CERTIFICAZIONE CISCO CCNA

---

strato fisico(bits)-Realizza una pipe virtuale fra diversi nodi connessi fisicamente. connessione 1bit 0bit, voltaggio, linearità, corrispondenza segnale, pipe virtuale generato, comunicazione con dlc.
chiamato anche modem:
(modem) Modulo semplice per ogni NODO: Fa corrispondere i dati che vengono dal livello superiore. (con un segnale appropriato). Ovvero,
Far corrispondere al segnale che viene dal link fisico una sequenza di bit appropriata per lo strato superiore.Progettazione:Temporizzazione dei bit che entrano nelle pipe.

Pipe sincrona. Pipe asincrona ad intermittenza. Caratteri asincroni.

data lynk(frame) – DLC è modulo semplice (rende affidabili i pipe dibit tra diversi nodi connessi) (stringa di bit strato inferiore -pakketto error free che viene dallo strato superiore). trasporta dati error free al network, dlc correzione errori, aggiunta header e trailer alla stringa di bit strato superiore, per formare frame. Frame=dati integri. Usati algoritmi distribuiti, correzione errori bit ci controllo. MAC= Realizza pipe sincrona ad intermittenza, allocazione liink, trasmettere frame,senza interferenze..

Strato di Rete(paket header)- realizza link end-to end per connettere 2 sistemi.(error Free). Processi paritari=insieme di moduli. Modulo = tanti link to link. (Stringa di bit)=packet header, raggiunge il dlc e vengono aggiunti healer e trailer. (frame intero). Paket body, informazioni aggiuntive sull'indirizzamento dati, generate dallo strato superiore. packet body=informazioni sulla gestione pakketto. packet body passa e genera r
packet header.
Il routing è anche una soluzione al congestionamento.
Stili di routing: Nel virtual circuit routine (virtua routine serveice) (connection oriented) assegnazione percorso e fare in modo che venga rispettato (pakketti di controllo+funzioni paket header) (connection oriented service)
Nel datagram routine (connection less service)(distribuzione disordinata) non necessario specificare percorso.
Congestione: Routing,Gestione Buffer,Controllo Flusso
Lan: singolo canale multiaccesso(pakketto per ogni nodo). No probl routine. Problemi di congestione Causa strato MAC.
Strato di rete e inferiori = Un'unica Black-Box. Input =informazioni strato superiore, output=informazioni per strato inferiore
Sottostrato Internet- funzioni di strato di rete (a volte in diverse reti hanno algoritmi diversi). Algoritmi distribuiti in NODI DI RETE.Soluzione: identificare un nuovo sottostrato allo strato di rete: (sottostrato internet identifica nell'architettura questo nuovo strato)
Gateway: connette 2 reti sullo strato di rete E' detto anche SITO. Esite un sottostrato internet per ogni gateway. Gateway: MAN e WAN. Lan-Lan: Bridge. Connessione strato DLC (data lynk).

Strato di Trasporto (SEGMENT) (paket body)- realizza diverse funzioni fra 2 sistemi connessi link-link.

Stabilisce, mantiene e termina i collegamenti virtuali.
-Per ogni sito esterno, esiste un MODULO SEMPLICE – Suddivide in tanti pakketti. (sito sorgente) – Ricompone i pakketti (sito destinazione). Servizio connectionLess (situazione di disagio)
-Multiplexa diverse sessioni(che abbiano lo stesso sito sorgente, stesso sito di destinazione) (alla sorgente), in un'unica sessione. Ovviamente meno X lavoro di scambio fra strato sessione e rete.
-Può anche dividere più sessioni in un'unica, correggere tasso trasmissione.. (risolvere problema di congestione).
- Controllo di flusso end to End (difficoltà controllo congestione). (controllo errori)
- Pakketto spedito (aggiunta intestazione trasport header). packet+trasport header= packet body. Trasport header viene tolto dal packet body quando questo raggiunge modulo del nodo di destinazione.

Strato di Sessione- info su Diritti accesso sessioni. Servizi offerti rete.

Sincronizza il dialogo
Classe del servizio,data expedition, exception reported
Strato sessione: Interazione fra utenti connessi
Strato Trasporto: Informazioni per avviare una sessione
Strato di Rete: Gestisce aspetti sottorete,durante la sessione
Questi 3 strati comunicano ed hanno compiti delineati. Di solito si unificano in 1 solo strato.

Strato di Presentazione- Criptazione dati, Compressione, Conversione in codice.

Data transfer syntax.
Criptazione: I messaggi vanno a finire nello stesso recipiente
Compressione: Minor transito di dati
Conversione in Codice: Incompatibilità varie periferiche

Strato di Applicazione- Comunicazione con l'applicazione finale.

Domande:

1) Perché il routing non costituisce un problema per le LAN ?
2) La congestione, nelle lan, è un problema che riguarda il sottostrato MAC. Perché?

2.2.1 Strato fisico

Un modulo dello strato fisico realizza una pipe di bit virtuale tra diversi nodi che sono connessi da un link fisico.

Per ogni nodo, c'è un modulo semplice la cui funzione è quella di far corrispondere ai bit che provengono dallo strato superiore, un segnale appropriato per il link fisico, nel caso in cui il nodo trasmette un messaggio, e di far corrispondere al segnale che proviene dal link fisico, una sequenza di bit appropriata per lo strato superiore, nel caso in cui il nodo riceve il messaggio. Il modulo semplice appena descritto è detto "modem". Solitamente, un modem può funzionare solo da interfaccia tra il link fisico e il modulo dello strato del DLC.

Nella progettazione dello strato fisico si deve tenere conto di alcuni aspetti.

Il primo aspetto è la temporizzazione della sequenza di bit che entrano nella pipe. Principalmente, si adottano le seguenti strategie:

- Pipe sincrona.
- Pipe asincrona ad intermittenza.
- Caratteri asincroni.

Il secondo aspetto è l'interfaccia il modulo DLC e il modulo fisico. Infatti, bisogna considerare delle situazioni in cui si possono trovare ciascuno dei due moduli oltre al problema di stabilire degli standard per l'interfaccia.

2.2.2 Strato del DLC

Un modulo allo strato del DLC ha il compito di realizzare una pipe di bit virtuale affidabile tra diversi nodi che sono connessi da un link fisico.

Per pipe di bit virtuale affidabile intendiamo un link che connette diversi nodi, su cui viaggiano, in modo asincrono, stringhe di bit error-free.

Per ogni nodo connesso ad una pipe di bit virtuale, c'è un modulo semplice la cui funzione è quella di far corrispondere ad un pacchetto error-free che proviene dallo strato superiore, una stringa di bit appropriata per lo strato inferiore, nel caso in cui il nodo trasmette il messaggio, e di far corrispondere ad una stringa di bit che proviene dallo strato inferiore, un pacchetto error-free per lo strato superiore, nel caso in cui il nodo riceve il messaggio. Il modulo semplice appena descritto è detto "modulo DLC". Un modulo DLC opera asincronamente in diversi sensi. Nel senso che il tempo impiegato da un pacchetto per essere elaborato dal modulo DLC è variabile (a causa della necessità di correggere gli errori dello strato fisico e della lunghezza variabile dei pacchetti) e nel senso che l'intervallo di tempo tra due input consecutivi è variabile (a causa della mancanza di pacchetti da spedire da parte degli strati superiori oppure della necessità di ritrasmettere dei vecchi pacchetti in cui sono stati individuati degli errori).

Un modulo DLC associato al nodo da cui l'informazione parte, aggiunge alcuni bit di controllo all'inizio (header) e alla fine (trailer) della stringa di bit che proviene dallo strato superiore. Questi bit aggiuntivi, insieme ai bit che costituiscono la stringa di partenza, formano un frame e servono per determinare l'inizio e la fine del frame e ad individuare la presenza di errori. Al fine di eseguire questi compiti, sono utilizzati degli algoritmi distribuiti che hanno un certo grado di complessità dovuto al fatto che i bit di controllo sono soggetti ad errori di trasmissione.

Quanto è stato detto finora vale solo per i collegamenti point-to-point e non per i collegamenti multiaccesso. Infatti, per questi ultimi vi sono dei problemi dovuti al fatto che il segnale ricevuto ad un nodo è una funzione dei segnali trasmessi dagli altri nodi che stanno trasmettendo, e che ogni segnale può essere "ascoltato" da molti altri nodi. Nel caso di collegamenti multiaccesso, quindi, lo strato del DLC costituisce solo il sottostrato dello secondo strato (a partire dal basso) del modello OSI. Più precisamente, costituisce il sottostrato superiore. Il sottostrato inferiore, invece, è rappresentato dallo strato del MAC. Un modulo allo strato del MAC realizza una pipe di bit sincrona ad intermittenza. Il modulo semplice associato al generico nodo connesso al link

multiaccesso, ha la funzione di allocare il link per il nodo in modo che possa trasmettere il frame senza subire interferenze dagli altri nodi.

2.2.3 Strato di rete

Un modulo dello strato di rete realizza un link end-to-end virtuale ovvero un link che connette due siti esterni di una rete, su cui viaggiano stringhe di bit error-free.

Per ogni nodo di un link end-to-end virtuale c'è un modulo semplice e tutti questi moduli (processi paritari) lavorano insieme per l'implementazione del routing e del controllo del flusso.

La stringa di bit che giunge dallo strato del DLC, ovvero il frame senza l'header e senza il trailer, è costituita dal "packet header", di cui lo strato di rete si serve per eseguire le funzioni di routing e di controllo del flusso, e il "packet body", che contiene informazioni fornite dallo strato superiore (riguardo, ad esempio, la destinazione della rimanente parte di informazione) oltre al pacchetto vero e proprio che va a costituire, insieme ad altri pacchetti, un messaggio generato da un utente durante una qualche sessione.

Si osservi che la parte di packet body che contiene informazioni su come gestire il pacchetto, è passata allo strato di rete dallo strato superiore come un insieme di parametri rispettando un protocollo di interfaccia tra i due strati. Lo strato di rete utilizza questi parametri, secondo il protocollo tra processi paritari dello strato di rete, per generare il packet header.

Consideriamo due tecniche di routing.

Nel virtual circuit routing, la funzione di routing eseguita dallo strato di rete consiste nel selezionare un percorso e nell'assicurare che ogni pacchetto segue il percorso assegnato (per tutta la durata della sessione).

In una rete che usa il virtual circuit routing (rete virtual circuit), la prima parte della funzione di routing può essere eseguita in diversi modi (per esempio, in modo distribuito da parte di tutti i nodi oppure a partire da un particolare nodo attraverso il quale l'informazione deve passare). Qualunque sia il nodo che è attraversato da una path che deve essere seguita dall'informazione per giungere alla destinazione, è necessario un considerevole scambio di informazioni riguardo i ritardi e il livello di traffico nella rete.

Tali informazioni vengono fornite attraverso dei pacchetti di controllo generati appositamente dallo strato di rete. La seconda parte della funzione di routing è eseguita eseguendo delle funzioni appropriate nel packet header ad ogni nodo, in modo che la stringa di bit venga inoltrata sul link corretto.

Nel datagram routing, invece, non è necessario determinare un percorso che l'informazione scambiata in una sessione deve seguire (fase di connessione). Tuttavia, l'applicazione di questa tecnica non è affatto semplice al punto che molte WAN utilizzano il virtual circuit routing per eseguire il routing.

Visto che in una rete virtual circuit l'ordine dei pacchetti viene preservato al momento del rilascio, utilizziamo il termine "virtual circuit service" per denotare un servizio offerto dalla rete in cui i pacchetti vengono rilasciati mantenendo l'ordine in cui sono stati inviati. Viceversa, utilizziamo il termine "datagram service" per denotare un servizio offerto dalla rete in cui i pacchetti possono essere rilasciati in modo disordinato. Poiché nel virtual circuit routing c'è una fase di connessione, ci riferiremo al virtual circuit service con il termine "connection-oriented service". Analogamente, ci riferiremo al datagram service con il termine "connectionless service".

L'altra funzione importante che è realizzata allo strato di rete è il controllo del flusso, o meglio, il "controllo della congestione". Infatti, se vediamo il controllo del flusso come la funzione per evitare che i dati siano spediti ad una velocità superiore a quella supportata dal sito destinazione e se vediamo il controllo della congestione come la funzione per evitare l'intasamento nella rete (nel senso che molti pacchetti sono bufferizzati in un nodo e aspettano di essere trasmessi sul link) allora, sicuramente, il controllo della congestione implica il controllo del flusso.

Pertanto, descriveremo come opera lo strato di rete per realizzare il controllo della congestione.

Fondamentalmente, la congestione capita quando gli utenti della rete richiedono insieme più risorsa di quanto la rete può offrire. Per avere uno spreco di risorsa minimo, lo strato di rete deve realizzare il routing, la gestione dei buffer e il controllo del flusso (nel vero senso della parola) in modo efficiente.

Si potrebbe pensare che portando la capacità dei link in una rete a livelli molto alti, si potrebbe evitare di realizzare il controllo del congestione. Tuttavia, ammesso che ciò avverrà in futuro, è pur vero che aumenteranno gli utenti della rete e, anche se gli utenti aumenteranno molto più lentamente della capacità dei link, si potrebbero avere dei seri problemi anche per piccoli malfunzionamenti di un nodo.

La trattazione appena conclusa è valida principalmente per le WAN. Risulta, invece, meno valida per le LAN. Infatti, le LAN sono, in genere, costituite da un singolo canale multiaccesso e, conseguentemente, un pacchetto è ricevuto da ogni nodo. Così, il routing non costituisce un problema per le LAN. Non è proprio così anche per la congestione. Infatti, è possibile che si verifichi una congestione in una LAN, ma questo è un problema

che riguarda il sottostrato MAC. In definitiva, quindi, lo strato di rete in una LAN non ha tutta l'importanza che ha in una WAN. Tale importanza è, invece, assorbita dallo strato del MAC.

In generale, comunque, lo strato di rete è concettualmente il più complesso della gerarchia in quanto tutti i processi paritari a questo strato devono lavorare insieme. Per gli altri strati (ad eccezione del MAC nelle reti multiaccesso) i processi paritari sono accoppiati e, per ogni coppia, ciascuno è associato ad una estremità di un link nel caso di strati inferiori dello strato di rete, mentre ciascuno è associato ad una estremità di una sessione, nel caso di strati superiori allo strato di rete.

In termini di black-box, lo strato di rete e gli strati inferiori appaiono come un'unica black-box. L'input per questa black-box è un pacchetto che arriva dalla black-box associata al sito sorgente allo strato superiore. Lo stesso pacchetto è rilasciato in output alla black-box associata al sito destinazione allo strato superiore.

2.2.4 Sottostrato di internet

Le funzioni di routing e il controllo della congestione possono essere realizzate in molti modi diversi, utilizzando algoritmi diversi. In genere, reti diverse utilizzano algoritmi diversi per realizzare le funzioni dello strato di rete. A complicare ulteriormente le cose, c'è il fatto che tali algoritmi sono distribuiti tra diversi nodi della rete. Come risultato si ha che non è così semplice connettere tante reti per ottenere una rete di reti. Una soluzione tipica per questo problema consiste nell'identificare nell'architettura a strati di una rete un nuovo strato o, meglio, un sottostrato dello strato di rete. Questo sottostrato è detto "sottostrato di internet".

Per connettere due sottoreti si usano i "gateway". Una rete che è interfacciata da un gateway ad un'altra rete, considera quel gateway come un sito esterno.

Ad ogni gateway sarà associato un modulo del sottostrato di internet che sta al di sopra dei moduli dello strato di rete associati alle singole reti.

I gateway, comunque, sono usati per connettere MAN e WAN. Per connettere LAN, invece, sono usati i bridge. I bridge si differenziano dai gateway in quanto connettono due sottoreti allo strato del DLC piuttosto che allo strato di rete. Da cui è chiaro che i bridge sono utilizzati per connettere LAN in quanto le LAN realizzano il routing e il controllo della congestione allo strato del DLC. D'altra parte, i bridge sono preferiti ai gateway per connettere LAN per via dell'economicità di tali dispositivi.

2.2.5 Strato di trasporto

Un modulo allo strato di trasporto ha il compito di realizzare diverse funzioni tra due siti esterni connessi da un link virtuale end-to-end.

Per ogni sito esterno connesso da un link virtuale end-to-end esiste un modulo semplice la cui funzione è quella di suddividere un messaggio in tanti pacchetti nel caso in cui il sito esterno è un sito sorgente, e di ricomporre i pacchetti per ottenere il messaggio nel caso in cui il sito esterno è un sito destinazione. La funzione realizzata da un modulo semplice associata ad un nodo destinazione può presentare delle difficoltà nella sua realizzazione nel caso lo spazio del buffer che deve accogliere i pacchetti che viaggiano sul link virtuale sia limitato oppure deve essere condiviso tra molti circuiti virtuali. Una situazione peggiore si ha quando la rete offre un servizio connectionless.

In realtà, lo strato di trasporto potrebbe realizzare anche altre funzioni. Infatti, potrebbe multiplexare diverse sessioni (tutte con lo stesso sito sorgente e lo stesso sito destinazione) in un'unica sessione dello strato di rete. In particolare, lo strato di trasporto potrebbe multiplexare tutte le sessioni con lo stesso sito sorgente e lo stesso sito destinazione. Tale realizzazione richiederebbe un minor # informazioni che lo strato di sessione dovrebbe scambiare con lo strato dei rete. Analogamente, lo strato di trasporto potrebbe suddividere una sessione in più sessioni per lo strato di rete. Ciò potrebbe essere richiesto per rendere possibile il controllo della congestione in modo equo per tutte le sessioni anche se una soluzione migliore, in questo caso, sarebbe quella di correggere il tasso di trasmissione della sessione allo strato di sessione. Inoltre, lo strato di trasporto potrebbe eseguire il controllo del flusso end-to-end. La realizzazione di quest'ultima funzione da parte dello strato di trasporto è frequente sebbene renda difficile il controllo della congestione.

Quando un pacchetto è spedito allo strato di trasporto è aggiunta una intestazione (trasport header) e la stringa di bit risultante costituisce il packet body che abbiamo introdotto nello strato di rete. Il trasport header viene levato dal packet body una volta che questo giunge al modulo paritario associato al nodo destinazione.

2.2.6 Strato di sessione

Lo strato di sessione fornisce informazioni sui diritti di accesso alle sessioni e, più in generale, sui servizi offerti dalla rete.

Ricapitolando, il modello OSI prevede che lo strato di sessione gestisce le interazioni tra utenti connessi (nel senso che hanno avviato una sessione) mentre lo strato di trasporto fornisce informazioni per avviare una sessione e lo strato di rete gestisce gli aspetti della sottorete durante una sessione.

In pratica, la suddivisione dei compiti per la gestione di una sessione tra lo strato di sessione, lo strato di trasporto e lo strato di rete non sono ben delineati al punto che molte reti considerano questi tre strati come un unico strato.

2.2.7 Strato di presentazione

Le principali funzioni realizzate da un modulo allo strato di presentazione sono la criptazione dei dati, la compressione dei dati e la conversione del codice.

La criptazione dei dati è necessaria in quanto, sebbene una rete è realizzata in modo che i messaggi vadano a finire nel giusto "recipiente", non è garantito che non si verifichino dei malfunzionamenti.

La compressione dei dati è richiesta per avere una minore quantità di dati che devono essere trasmessi.

La conversione del codice è necessaria quando c'è incompatibilità tra le varie periferiche.

2.2.8 Strato di applicazione

Le funzioni realizzate allo strato di applicazione sono tutte quelle che non sono state realizzate agli strati inferiori. Più precisamente, mentre agli strati inferiori sono forniti i programmi che sono richiesti per l'esecuzione di ogni applicazione, allo strato di

applicazione sono realizzati dei compiti specifici per l'esecuzione di singole applicazioni.

strato fisico- connessione 1bit 0bit, voltaggio, linearità, corrispondenza segnale, pipe virtuale generato, comunicazione con dlc
chiamato anche modem.

data lynk – DLC è modulo semplice (stringa di bit strato inferiore -pakketto error free che viene dallo strato superiore). trasporta dati error free al network, dlc correzione errori, aggiunta header e trailer alla stringa di bit strato superiore, per formare frame. Frame=dati integri. Usati algoritmi distribuiti, correzione errori bit ci controllo. MAC= allocazione liink, trasmettere frame,senza interferenze..

Strato di Rete- realizza link end-to end per connettere 2 sistemi. Processi paritari=insieme di moduli. Modulo = tanti link to link. packet header, raggiunge il dlc e vengono aggiunti healer e trailer. (frame intero). Paket body, informazioni aggiuntive sull'indirizzamento dati, generate dallo strato superiore. packet body=informazioni sulla gestione pakketto. packet body passa e genera r packet header.
Stili di routine: Nel virtual circuit routine (virtua routine serveice) (connection oriented) assegnazione percorso e fare in modo che venga rispettato (pakketti di controllo+funzioni paket header) (connection oriented service)
Nel datagram routine (connection less service) non necessario specificare percorso.
Congestione: Routing,Gestione Buffer,Controllo Flusso
Lan: singolo canale multiaccesso(pakketto per ogni nodo). No probl routine. Problemi di congestione Causa strato MAC.
Strato di rete e inferiori = Un'unica Black-Box. Input =informazioni strato superiore, output=informazioni per strato inferiore
Sottostrato Internet- funzioni di strato di rete (a volte in diverse reti hanno algoritmi diversi). Algoritmi distribuiti in NODI DI RETE.Soluzione: identificare un nuovo sottostrato allo strato di rete: (sottostrato internet identifica nell'architettura questo nuovo strato)
Gateway: connette 2 reti sullo strato di rete E' detto anche SITO. Esite un sottostrato internet per ogni gateway. Gateway: MAN e WAN. Lan-Lan: Bridge. Connessione strato DLC (data lynk).

Strato di Trasporto- realizza diverse funzioni fra 2 sistemi connessi link

Networks

Topology FISICO- Cavo
Topolocy LOGICO- Definisce le apparecchiature che permettono ai dati sul cavo di passare

Bus Topology: Singolo backbone (grosso cavo) che connette tutti i nodi
Ring Topology: Crea un anello fisico tramite il cavo e connette gli host via via.
Star Topology: Connette i cavi in un punto centrale di connessione. Questo punto può essere "hub" o "switch"
Exteended star Topology: E' una stella estesa grazie a hub o switches.
Hierarchial Topology: simile alla stessa estesa, ma esistono computer che linkano il traffico.
Mesh Topology: Usata quando non devono esserci assolutamente delle interruzioni. Ogni host contatta tutti gli altri host. E' simile alla struttura di internet.

La tipologia Broadcast consiste nell'inviare informazioni a tutti i nodi del CAVO.
Non esiste un ordine. La prima che invia i dati è denominata primo pc a servire.

La tiplogia Tocken passing consiste in controlli Per ogni nodo passante. Quando i dati passno su un nodo, questo risponde.

In una rete le periferiche sono connesse ad una rete tramite un segmento di cavo oppure esse sono il diretto riferimento come host. Possono avere diversi compiti.
Per una connessione di rete è usata la NIC. La nic, funziona sul livello di rete 2.
IL MAC E' utilizzato per CONTROLLARE la comunicazione dei dati, sulla rete.
Ci possono essere diversi tipi di periferiche, in questo caso possono essere considerate LIVELLO 1 di rete.
Le nic non sono assolutamente standardizzate, possono esistere diversi tipi di nic. O tipo nic.

Il cablaggio può avere delle simbologie molto varie. E' considerato il livello 1 del modello osi ed ha il compito di trasportare dati. Si può costruire le reti con ogni tipo di cavo. Alcuni cavi sono avvantaggiati e disavvantaggiati, i fattori sono i seguenti:

Costo,Coodità di installazione,Lunghezza del cavo.

Il cavo CAT5 Utp ha lo svantaggio della lunghezza. Non può superare i 100 metri.Se vogliamo estendere la rete ci serve un REPEATER.
Il repeater funziona sul LIVELLO 1 del modello OSI.
Per una 10megabit: 5-4-3. 5 Segmenti di rete, 4 Ripetitori, 3 Hosts.

HUB: periferica a livello 1. Rigenera e ritemporizza il segnale di rete. Rigenera il segnale e lo broadcasta su tutte le sue porte. Ci sono hub attivi e hub passivi. Gli **hub attivi** hanno un'alimentazione, gli **hub passivi** non vengono alimentati e non rigenerano la lunghezza del cavo. Esistono **I DUMP** e gli **hub intelligenti**. Gli hub intelligenti sono programmabili per poter gestiere il traffico. I dump prendono il segnale e lo ripetono, senza la possibilità di gestirlo. Nella rete Token ring, l'hub è chiamato MAU.

BRIDGE: periferica a livello 2. Connette 2 segmenti di rete LAN. Lo scopo del bridge è quello di **mantenere Locale** il traffico tramite un filtraggio sulla lan E di **permettere lo scorrimento** del traffico sulla rete che il bridge connette.
Il bridge connette le reti basandosi sul MAC ADDRESS delle periferiche.
Molti switch e routers svolgono la funzione dei Bridge che restano comunque importanti nelle reti.
Il simbolo è generalmente quello di un ponte sospeso. Ha 2 o 3 porte. Il bridge applica un filtraggio ai FRAME. E' livello 2 dell'osi model. E' raffigurato come un ponte rovesciato

SWITCH: Lavora a Livello 2. E' anche definito multi port REPEATER. Lavora tramite l'indirizzo MAC. E' una decisione che rende la rete più efficiente. E' migliore degli hub. La differenza è caratterizzata da ciò che accade all'interno della periferica. Ha la **Connettività di un Hub e la capacità di regolare il traffico come un BRIDGE**. Switcha i frame dalle porte in entrata, verso le porte in uscita. Ogni porta ha la propria **BANDA indipendente.** E' raffigurato come un rettangolo con freccette.

ROUTER: Il router lavora a livello 3. NETWORK. Ha la possibilità di connettere varie periferiche di livello 2. Può portare direttamente il backbone sulla rete internet. Il router esamina i pacchetti e sceglie la MIGLIOR DESTINAZIONE per essi sulla rete. Sono importanti per regolare il traffico

su reti di grandi dimensioni. Abilitano un computer a connetterne un altro dall'altra parte del mondo..! Router può eseguire anche funzioni avanzate. Le funzioni principali: **Path selection. Switching packet to the route.** Può avere diverse connessioni. Wan,Lan,Ethernet, Aui.

CLOUD: LE nuvolette sono connessioni che portano a reti o internet ma delle quali non si conosce i dattagli. E' un'insieme di pc o periferiche che viaggiano secondo tutti e 7 i modelli osi. Esiste un modo per connettersi ad una rete senza fornire i dettagli: Internet.

UN SEGMENTO, collega la rete a livello1. E' una parte di rete comune sul percorso di rete. Quando viene applicata una periferica che provvede ad allungare la rete per limitazione di capienza del cavo, automaticamente si definisce un nuovo segmento. Un segmento è definito come un INTERVALLO. Come una piccola rete lan che fa parte di una grande rete. Non bisogna fare confusione con le altre 2 definizioni: Si definisce anche come COLLISION DOMAIN. I segmenti sono i frammenti dati del livello 4.

HUB, a livello 1, nic livello 2, Cablaggi e struttura (patch, cablaggio, pannelli), livello1.
Ogni periferica a livello 2, chiaramente ha anche parte di struttura che funziona a livello1, come la trasformazione di dati in bit.
I router sono a livello3, per la scelta del path di rete, ma l'interfaccia interna opera a livello 2 e 1.
Le nuvole di rete, possono comprendere varie apparecchiature per cui il loro livello di rete varia da 1 a 7.

I bridge funzionano **esaminando il MAC address del frame in arrivo.** Se il frame è **locale** (col MAC address nello stesso segmento di rete della porta di arrivo del bridge), il frame **non è inoltrato** al bridge. Se il frame **non è locale** (col MAC address non nello stesso segmento di rete della porta di arrivo del bridge)allora **è inoltrato** al seguente segmento di rete. Siccome queste decisioni dei circuiti del bridge sono fatte **in base al MAC Address**, il bridge, nel diagramma, riceve il frame, rimuove il frame, esamina il MAC address, e poi lo inoltra o meno, a seconda del caso.

ELETTRONICA E SEGNALI

Reazioni elettriche: Protoni (carica+) Neutroni (carica neutro). = Nucleo. Elettroni=carica-

Elio. Numero atomico 2. Peso4. Sottraendo 2, si ottiene 2 neutroni
Forse opposte creano un'attrazione.

Colomb's LAW= Cariche opposte si attraggono.
Bohr's Model= Protoni positivi, Elettroni negativi.

LA Perdita di Elettroni, provoca carica negativa. E' chiamata **Elettricità STATICA**. Se questa corrente ha la possibilità di riversarsi su un condottore, si parla di **ELECTROSTATIC DISCARGE**. (scarica elettrostatica).
Un ESD può essere disastroso per un sistema informatico, anche se per l'essere umano è innocuo.
Atomi o gruppi di atomi sono chiamati **MOLECOLE** e si riferiscono a materiali.
Vengono classificati in base alla loro faclitià di elettrificazione, Elettroni liberi o flussi che li attraversono.

Electrical Insulator: Si tratta di materiali che **permettono agli elettroni di attraversarli con difficoltà o per niente.** Esempi: plastica,vetro,carta, gas elio. Questi materiali hanno una struttura chimica molto stabile. Gli elettroni viaggiano ermeticamente con il gruppo degli atomi.

Electrical Conductors: Si tratta di materiali che **permettono facilmente il passaggio degli elettroni**. Gli elettroni sono poco legati al nucleo. A temperatura gli atomi di questo materiale hanno un gran numero di elettroni che possono provvedere alla conduzione. L'introduzione di tensione causa il movimento degli elettroni liberi, e la corrente Fluisce. I migliori conduttori sono il metallo, argento ed oro. (copper (Cu), silver (Ag), and gold (Au).) . Altri conduttori: (solder (a mixture of lead (Pb) and tin (Sn), and water with *ions)* Il corpo umano è attorno al 70% acqua e ioni. E' un conduttore.

Electrical Semiconductors: I semi conduttori sono materiali **che fanno passare la corrente in maniera precisamente controllata**. (carbon (C), germanium (Ge), and the alloy, gallium arsenide (GaAs).).
Il miglior **semiconduttore è il SILICIO**. San jose è chiamata anche Silicon Valley, l'industria dei componenti parte da lì.

La classificazione di Isolanti, conduttori e semiconduttori è molto importante.

Ci sono molti modi per descrivere **l'attività Elettrica all'interno di un Media**:

Voltaggio: Pressione elettrica che separa 2 cariche. E' una forza che si verifica quando gli elettroni e protoni, vengono separati. La carica generata viene Spinta verso la forza di polarizzazione opposta. Questo accade nella batteria. Chimicamente vengono isolati gli elettroni ed una carica si sposta da una parte all'altra della batteria attraverso un circuito esterno. La FORZA della carica della separazione è espressa in VOLTAGGIO. (o meglio la PRESSIONE) Può essere creato **dalla FRIZIONE (strofinamento), dal Magnetismo, O dalla luce (celle solari). Il voltaggio è indicato con "V".**

Corrente: E' il flusso creato dal movimento degli elettroni. Nei circuiti elettrici la corrente è causata dal flusso di elettroni. Quando c'è applicato il voltaggio, una corrente si muove dal polo negativo (spingente) a quello positivo (attrazione) su di un perocorso (media). La corrente è raffigurata **con il simbolo "I"**. **La misura della corrente è "AMPERE"**. Il numero delle cariche per secondo che passano per un punto del percorso

Resistenza: I materiali sui quali viaggia la corrente offrono vari tipi di Opposizione, al movimento degli elettroni. I materiali che non danno resistenza sono CONDUTTORI. I materiali che offrono resistenza sono ISOLANTI.
L'ammontare della resistenza dipende dalla **Composizione Chimica dell'elemento**. La resistenza **è rappresentata come "R" o OHM**. Come "omega".

Corrente Alternata: E' una delle 2 direzioni in cui la corrente viaggia. La corrente e la polarità **variano ogni volta ke avviene un'inversione**. La corrente alternata viaggia in Una direzione. E' positiva da un lato e negativa dall'altro, quindi inverte la sua direzione e ripete il processo. Il terminale positivo diventa negativo e viceversa.. In processo si ripete continuamente.

Corrente Diretta: In questo caso la corrente viaggia solo in 1 o 2 direzioni, senza variare. Circola nella stessa direzione, spesso il voltaggio (DC),

manitiene la stessa polarità. **Un terminale è sempre posito e l'altro terminale è sempre negativo. Non avvengono cambiamenti.**

Impedenza: L'impedenza è la totale opposizione al flusso corrente. La resistenza è riferita alla corrente diretta (DC). **E' la capacità di NON FAR PASSARE la corrente**. Si riferisce alla non disponibilità al passaggio di correnti ALTERNATE.

Voltaggio e Corrente, Resistenza: La corrente circola soltanto in un circuito chiuso tramite materiali conduttori, deve esistere un voltaggio. Il voltaggio causa il circolo della corrente, l'impedenza lo ostacola. Ci sono diversi fattori per cui si è imparato a controllare il flusso di corrente. Ovviamente ricordati sempre che la corrente scorre solo a CIRCUITO CHIUSO.....
Ricordati sempre la Differenza fra TENSIONE (misurata dalla d.d.p. a circuito aperto) e la CORRENTE che indica la quantità di elettroni che stanno scorrendo nel conduttore.
La tensione si misura in Volt, o in MilliVolt, emisura la d.d.p., la CORRENTE si miusura in AMPERE o MilliAMpere e misura la "Forza" della tensione

Ground: Può essere inteso come il riferimento in termini di misurazione, di ZERO VOLTS,Per intenderci, è LA TERRA. Sta per terra..... La terra di un qualsiasi conduttore!
Quando si parla di corrente a radiofrequenze, come quella elettrica o quella che scorre lunho un cavo di rete, non si parlà di Polo Positivo e Polo Negativo, ma di POLO CONDUTTORE e TERRA.
La terra serve a creare la d.d.p. DIfferenza di Potenziale nel conduttore, e quindi a permettere algi elettroni di circolare...

Oscilloscopio: Periferica elettrica usata per studiare segnali elettrici. La misurazione è effettuata creando delle onde (in senso grafico). Queste onde sono pulsanti. Secondo il grafico, X rappresenta il tempo e Y rappresenta il voltaggio. Normalmente ci sono più assi Y così possono essere misurate 2 onde allo stesso tempo. La corrente può essere ALTERNATA (AC), ed è trasportata dalle linee di corrente. E CONTINUA (DC) e può essere trovata in batterie e alimentazioni da computer.

Gounding Equipment: Esistono materiali conduttori, utilizzati per trasportare la corrente, ma esistono anche materiali non conduttori usati per la SICUREZZA, per proteggere dalla corrente.
La corrente è convogliata ad un trasformatore che RIDUCE i volts della corrente. Generalmente 120 o 240Volts. La terra, CENTRALE, nei cavi, protegge le persone da scosse elettiche, ed è chiamato: the safety ground connection.
Anche nei case dei pc esiste quaclosa di simile.

Segnale Analogico: (SINE WAVES) E' ondeggiante, Ha un grafico che indica un continuo variare del voltaggio in relazione al tempo, E' tipico della natura, è usato da più di 100 anni per le telecomunicazioni.
Si deve tener conto dell'Amplitude (A)=Nel grafico è antezza e profondità. e del Period (T)=Nel grafico è il tempo completo di 1 ciclo.
La FREQUENZA (F) si calcola con: F=1\T

Segnale Digitale: (SQUARE WAVES) Ha dei notevoli salti di Voltaggio, rispetto al Tempo, nel grafico. E' raro in natura. Tipico della Tecnologia. Ha

un’amplificazione FISSA. Costante. (bit 0 e bit1). Ma la frequenza di pulsazione può variare.
Nei grafici, il segnale digitale è caratterizzato da impulsi che vanno instantaneamente da tensioni basse a tensioni basse, senza alcun intermedio.
Segnali Analogici\Digitali: E’ possibile trasformare i segnali analogici in segnali digitali. La scoperta è stata fatta da Jean Baptiste. Esso afferma che che SQUARE WAVES o le Pulsazioni (Square) possono essere costruite utilizzando una combinazione di onde analogiche (sine waves).
La base delle sine Waves può caratterizzare segnale digitale. Questo è importante per osservare il viaggio delle pulsazioni digitali attraverso cavi di rete analogici.

Rappresentare un bit su un media fisico: Le reti sono per la maggior parte digitali. Le pulsazioni costruiscono 1 pulsazione digitale. Corrisponde a 1 oppure 0. LA differenza fra 0 e 1 è di voltaggio. +5volts per l’esattezza. Il ground è utile per stabilizzare la differenza fra 0 e 1.Esso rappresenta gli ZERO VOLTS. E’ la parità o TERRA.
Devono funzionare su un circuito chiuso e deve esserci una TERRA.
Nel caso dei segnali ottici, lo 0 è rappresentato da una luce scura. 1 invece è una luce chiara ed intensa.
Nel caso dei segnali Radio, lo 0 è rappresentato da un’onda corta, 1 invece è un’onda lunga.
In 1 bit bisogna tener conto dei seguenti fattori:

- Propagazione
- Attenuazione
- Riflessione
- Disturbi
- Problemi di tempo
- Collisioni

Propagazione dei segnali di rete: LA propagazione va immaginata come un “viaggio”. Quando un’interfaccia di rete emette un segnale, esso si PROPAGA tramite delle square waves. **La propagazione rappresenta** 1 Salto di energia da un punto ad un altro. **La velocità** della propagazione dipende dal materiale e dalla struttura geometrica di questo dalla frequenza delle pulsazioni.
Il tempo impiegato da una pulzazione per raggiungere la fine del “MEDIA” e tornare indietro **è definito “round trip time” (RTT)**
Il tempo per raggiungere semplicemente la fine del tragitto è RTT\2.
Se si verificano dei ritardi nel tempo , possono esserci dei problemi.
La mancanza di conoscenza del tempo di propagazione è un problema.
Bisogna considerare che secondo la teoria della relatività di einsein, nessuna cosa può viaggiare più veloce della luce, per cui il tempo di RTT\2 non può essere ZERO. Esiste sempre un tempo da considerare per cui l’arrivo della pulsazione non è instantaneo.
Se il tempo è troppo lungo bisogna rivalutare la struttura di rete, se il tempo è troppo breve è necessario utilizzare un BUFFER (buffering).

Tempo=Zero Tempo di tragitto=RTT\2. Formula RTT\2=X\Speed

Attenuazione: L'attenuazione è **la perdita di forza del segnale**, ad esempio quando il cavo è più lungo del dovuto. Quando un segnale passa da un cavo si attenua per cui è consigliato usare Materiali Conduttori.
Nelle fibre ottiche, il materiale assorbe un po' della luce che essi trasportano..Questo può modificare la lunghezza delle onde, o\e il colore..Può incidere anche il tempo, la situazione atmosferica, i risultati possono rendere illeggibile i dati.
Nelle radio, Le onde radio possono essere assorbite da specifiche molecole nell'atmosfera. L'attenuazione può influire sulla lunghezza della rete, sul tragitto delle onde.
Puoi risolvere tutto questo utilizzando strutture con bassa attenuazione.
Soluzione 1: cambiare il tipo di MEDIA. Soluzione 2: Ripetere il segnale dopo una certa distanza. I ripetitori sono ottici, radio e elettrici.
Riflessioni: LA riflessione è il **Rimbalzare dei Bit e può interferire con i BIT seguenti**. Può contrastarli. La riflessione può non essere un problema se si tiene conto di questo fattore e comunque dipende molto dal tipo di cablaggio utilizzato**. LA riflessione è un rimbalzo**, dipende fortemente, nel caso delle onde radio, dalle condizioni atmosferiche.
Nelle reti **è importante** che l'impedenza del materiale (cablaggio) sia tarata con la potenza del trasmettitore. Se non c'è una correta impedenza, il segnale può riflettere e può venir creata un'interferenza.
Si può risolvere questo problema accoppiando tutti i componenti ad un'adeguata impedenza.

Disturbi: Il disturbo **è un'Inattesa aggiunta di voltaggio, luce ottica o segnale elettromanetico**. Non esiste segnale elettrico senza disturbo, per cui **è opportuno tener conto** del rapporto che può avere il disturbo con il segnale (NOISE) S\N (signal\Noise).
Si divide la forza del segnale con la forza dei disturbi. Si riceve segnali Inattesi da sorgenti Variabili. I disturbi possono corrompere i segnali 0 e 1 e quindi DISTRUGGERE il messaggio.

Next A- Next B: Quando il disturbo è generato da un Cavo all'interno della struttura del cablaggio, si parla di CROSSTALK. Quando un cavo è vicino ad un altro, **si possono causare disturbi** che arrivano fino alla fine del cavo, soprattutto nei terminatori (al termine del filo).

"NEXT can be addressed by termination technology, strict adherence to standard termination procedures, and use of quality twisted pair cables.NEXT-A is Near End Crosstalk at computer A and NEXT-B is Near End Crosstalk at computer B."

Il disturbo può anche essere causato da anomale condizioni Termiche.

Disturbi AC rapportati alla Terra: I disturbi possono essere causati da tutte le apparecchiature che utilizzano la corrente alternata, se non controllati, questi disturbi possono provocare problemi sulle reti. I case dei pc hanno una terra propria ed un riferimento alla terra dell'alimentazione. C'è un link fra la terra dei case e la terra di alimentazione. La terra di alimentazione può causare problemi al sistema. Sono problemi difficili da individuare. Spesso non si tiene conto della lunghezza necessaria alla TERRA.

I disturbi possono provenire da hard disk, monitor o apparecchiature vicine. Questo problema di solito si verifica in computer che hanno una connessione non troppo protetta e perfezionata.
Disturbi elettrici sono definiti anche **EMI (electronic magnetic interference) o RFI (radio frequency interference).**
Ogni cavo può fungere da Antenna. Quando ciò avviene il cavo assorbe l'energia di un altro cavo a se stesso, Se il livello di disturbi è abbastanza alto, può risultare difficile, per la nic, distinguere il disturbo dal segnale vero e proprio.
Molte lan **utilizzano una frequenza che rientra nei 100Mhz**, propria di apparecchiature come TV, radio ecc.ecc.
Le tecnologie ottiche e radio hanno in comune alcune problematiche dei cavi di rete, ma sono esenti da altre.
Ad esempio, le fibre ottiche sono immuni ai problemi NEXT e AC, ed i sistemi radio sono particolarmente immuni a EMI E RFI. La causa di ciò sta nel fatto che i cavi di metallo e materiali comuni sono particolarmente immuni a tale disturbo.
Per risolvere i problemi di AC è **importante stare non troppo distanti dalla propria centrale elettrica**..Questo comporta l'avere una linea di terra molto più breve (è un vantaggio)
CANCELLATION è una tecnica usata per proteggere i cavi da interferenze esterne.
E' importante avere un BOX di alimentazione separato per ogni ufficio.
E' importante isolare motori elettrici che possono provocare interferenze, controllare accuratamente le prese di corrente per ogni pc nella LAN.
Installare un generatore elettrico per ogni postazione riduce la distanza dalla TERRA.
Tipicamente per eliminare i distubi EMI e RFI si aumenta **la dimensione** del cavo e dei connettori.
Seguire le specifiche di lunghezza del cavo evitando nodi.
Utilizzare cavi di massima qualità.
Incrementare **il diametro** del cavo, e del connettore.
Quando si usano i cavi bisogna curarne l'integrità.
E' importante **individuare LA DIREZIONE** secondo la quale la corrente affluisce, quando si usano 2 cavi vicini è importnte verificare che la corrente affluisce **nelle 2 direzioni diverse** per cui il potere elettromagnetico di uno, va a cancellare quello dell'altro. Questo canella anche altri eventuali campi elettromagnetici al meglio.

Dispersione, Latenza, Jitter: Sono tre differenti cose che possono capitare ad un bit. Sono raggruppate perché l'effetto è simile.
La Dispersione, riguarda un problema in cui **il bit non raggiunge la destinazione in determinato tempo**. Il bit che viene dopo può quindo confondersi con il bit precedente.
Per evitare la dispersione si sceglie un cavo appropriato, si fa caso alla lunghezza del cavo, e si cerca l'impedenza appropriata. La disperasione può essere limitata dalla frequenza usata per trasmettere.
Jitter, Per ogni operazioe sul pc, fino a quello sulla nic per i dati, la cpu deve fare dei calcoli. Se questi calcoli non sono sincronizzati con il pc host di destinazione, si causa un tempo jitter. **Il bit dunque arriva con un lasso di**

ritardo rispetto al previsto. I jitter sono corretti da una serie complicata di calcoli.
Latenza, definita anche come RITARDO. Qui dobbiamo rammentare la teoria della relatività. Nessun corpo viaggia più veloce della luce in un ambiente privo d'aria. (3.0×10^8 meters/second)
I segnali radio viaggiano molto più lentamente rispetto alla luce nel vuoto.
I segnali di rete sul ferro (1.9×10^8 m/s to 2.4×10^8 m/s.)
I segnali sulla fibra ottica (2.0×10^8 m/s)
Viaggi più lunghi possono portare via una piccola parte di tempo in più in quanto cablaggi ed apparecchiature elettroniche generano LATENZA.
La soluzione è usare varie codifiche, differenti strategie di encoding, e vari layer protocols.
La trasmissione delle interfacce varia da 1 a 1000Mbps. Se si verificano errori, 1 può essere inteso come Zero. Se si verificano errori di intestazione, il pacchetto può andare perduto e si penalizza l'operazione con perdita di tempo, Possono anche verificarsi errori per cui il pc che riceve i dati ha difficoltà a riassemblare il pacchetto. Possono andar persi milioni di bit per secondo.

Collisioni: Le collisioni si verificano quando le periferiche **non sono disponibili al dialogo nello stesso momento e ci sono degli scontri**.. Si può verificare **una sovrapposizione del voltaggio** per cui il Bit è nullo (corrotto). E deve ripetersi l'invio poiché non c'è modo di interpretare l'informazione, in quel caso. Es. 5 volts,10volts.. 0-1. In caso di collisione..picchio di 15 volts. (si accende la luce COLL, per sovravvoltaggio). Il bit è distrutto.
Alcune collisioni rientrano nella naturalità di alcune strutture di network.
Eccessive collisioni rallentano la rete, e possono addirittura arrestarla.
Molte strutture di rete vanno ad individuare e localizzare le collisioni di rete.
La collisione avviene in T=RTT\4, a metà del tragitto del media.
Per prevenire le collisioni è necessario fare in modo che un pc trasmetta con sincronia rispetto ad altri pc, per realizzare questo è necessario avere diverse apparecchiature, chiamate TOKEN per trasmettere in token –Ring e FDD.

Trasmissioni dati a lunga distanza: Quando bisogna inviare un messaggio a lunga distanza ci sono dei problemi a cui bisogna pensare. Che metodo utilizzare **per codificare** il messaggio e che metodo utilizzare **per inviarlo**.
Encodando si può convertire dei dati in BINARI e possono viaggiare tramite un mezzo fisico.
Si devono utilizzare i calcoli binari per manipolare un'onda modulata.

Modulazioni e Codifica: La codifica deve avvenire quando i dati sono convertiti in 1 e 0 all'interno di qualcosa di fisico. Che può essere:
Un impulso elettrico in un cavo, Un impulso di luce su una fibra ottica, Una pulsazione elettromagnetica all'interno di uno spazio.
2 Metodi per completare questo sono: **TTL ENCODING e MANCHESTER ENCODING**.
TTL (Transistor-Transistor Logic) : La codifica è semplice, (often +5 or +3.3 V for binary 1 and 0 V for binary 0). Nell'ottica 1 è rappresentato da un laser chiaro e 0 da un laser scuro. Nelle onde radio 1 è rappresentato da una Portante e 0 è rappresentato da niente.

Manchester Encoding: E’ molto più Complessa, ma **più immune ai Distubi e più facilmente singronizzata**. I segnali sono codificati da alcuni transistor per cui il tutto è molto più stabile e controllato. Questa codificazione ha la forma di un’onda continua. Come una portate continua che cambia con il variare dei segnali (0 e 1).
Ci sono vari tipi di modulazione:
AM: (amplitude modulation) L’altezza delle onde o della portante è variabile, si tratta di onde analogiche che portano informazioni.
FM: (frequency modulation) L’altezza delle onde è variabile in base alla frequenza. Essa varia e vengono portate le informazioni.
PM: (phase modulation) La fase o i punti di inizio e fine dell’impulso generano una sorta di Circolo che porta l’informazione.
Esistono altre forme complesse di modulazione, al mondo.

I CABLAGGI Più CONOSCIUTI

Cavo Stp: (100 METRI) E’ un cavo che combina la tecnologia di **schermo protettivo (shielding) , cancellazione dei disturbi (cancelling), e protezione da altri fili (schermato).**
Ogni paio di cavetti è avvolto da un rivestimento METALLICO.
I 4 cavetti (2 ciascuno) sono a loro volta rivestiti da una pellicola metallica, solitamente di 150 Ohm.Sono tipicamente usati per le installazioni di reti Ethernet, sono protetti da EMI e FRI, riducono i fastidi elettrici, il Crosstalk.
Hanno diversi VANTAGGI e SVANTAGGI rispetto al classico cavo UTP non schermato:
STP protegge di più, ma costa molto ed è difficile da installare.
Twisted pair= i 2 fili interni singoli
Pair Shields=Protezione per i 2 fili, li raggruppa in 1 unico cavo. In genere ci sono 4 pair shields.
Overall shields=Protezione raggruppa a sua volta questi 4 gruppi.
Outer racket=E’ la gomma esterna

Esiste il tipo ScTp che sarebbe un UTP schermato, conosciuto come FTP (Foil Twisted Pair)
FTP= Una via di mezzo fra stp e utp. E’ schermato fra i 100 ed i 120Ohm. Non hanno i PAIR SHIELDS.

Questi cavi, sia stp che ScTp hanno bisogno della terra, verso la fine, se non sono propriamente collegati alla terra, possono subire molti problemi di “NOISE”, o Disturbi.
Non tutti i disturbi vengono annientati, ma la maggior parte, caratterizzati da onde elettromagnetiche. Questi cavi **non possono coprire una notevole distanza senza che il segnale venga ripetuto**, bisogna quindi considerare un costo aggiuntivo non indifferente. Se si aumenta la dimensione del cavo, il costo aumenta.

Cavo Utp: (10-100mbps)(100 Metri) Sono i più comuni. Sono composti da 8 cavi rivestiti da materiale isolante. Sono molto comuni, nella maggior parte delle reti esistenti in circolazione. Questi cavi, **hanno la cancellation effect**, che producono i cavi interni, **Limitano i disturbi RMI e RFI**.

Riduce il Cross Talk. Il numero di Microfili nei TWISTED paird è variabile. Esistono delle specifiche per cui si consideri il numero di micro fili all'interno del cavo.
Quando si usa un cavo di tipo UTP, si devono consierare dai 22 ai 24 micro fili. Il cavo utp ha un'impedenza di 100Ohm. Alcuni possono essere utilizzati per cavetteria telefonica. L'installazione di UTP comporta VANTAGGI in quanto hanno un diametro di soli 43mm, ed è facile da installare.
Il costo di UTP per metro è inferiore rispetto a qualsiasi tipo di altro cavo di rete.
Con il cavo UTP **è possibile usare una connessione RJ**, che è SALDA**, sicura, ed isolante, elimina i disturbi**.
Gli SVANTAGGI sono. **Interferenze con altri tipi di cavi di rete, Corta distanza che questi cavi possono coprire**, rispetto al Coassiale e Fibre ottiche. E' considerato il più veloce cavo a base metallica.

Cavo Coassiale: (10-100mbps)(500 metri) Consiste in un cilindro, dentro il quale ci sono 2 metalli conduttori. Il primo di questi è al centro del cavo. Un piccolo filo di metalo conduttore. All'esterno di questo c'è un'isolante flessibile.All'esterno di questo c'è un altro strato di metallo usato per **RIDURRE LE INTERFERENZE.** Poi c'è il Cable jacket che sarebbe la plastica che rivese il tutto.
Ovvre molti VANTAGGI. Viaggia a Lunghe distanze senza ripetitori, per cui va molto più lontano rispetto a STP e UTP. I ripetitori possono quindi generare GROSSI SEGMENTI per cui **è possibile coprire NOTEVOLI DISTANZE**.
E' stato utilizzato per molti anni, in vari tipi di comunicazioni. E' un cavo molto economico.
Il cavo è di GROSSE dimensioni per cui è scomodo. Va fatto passare in una conduttura già esistente, Possono esistere di grosse dimensioni, utilizzati normalmente per i BACKBONE. Sono spesso chiamati anche "thicknet". Questo nome suggerisce il tipo di cavo in quanto esso è RIGIDO ed utilizzabile in qualsiasi situazione. Questo cavo ha bisogno di buoni connettori e terminatori. Possono esistere **interferenze elettromaghetiche** e disturbi, Esistono infatti problemi di questo tipo legati a questo cavo. Per questo motivo, il piccolo diametro di un tempo, non è più utilizzato.
Piccolo 10Base2, 50ohm. Grosso 10base5.

Cavo Fibra Ottica: (100mbps e oltre) (2000-3000m)Questi cavi possono **condurre la modulazione con la "LUCE".** Sono molto dispendiosi rispetto agli altri tipi di cavi di rete, Non sono sensibili alle interferenze elettromagnetiche e sono in grado di avere un RANGE molto più elevato rispetto a tutti i cavi di cui si è discusso.
Si tratta di segnali ottici o ONDE ELETTROMAGNETICHE che viaggiano attraverso fibre ottiche, dunque NON SONO Considerate "wirless".
Ha portato molti benefici alle più diffuse apparecchiature di comunicazione, in particolar modo è applicata nelle comunicazioni a lunga distanza.
Le fibre consistono in **2 FILI di materiale Firbra di VETRO** e "cladding", isolati da rivestimenti protettivi di plastica.
Esiste poi una fibra esterna di **KEVLAR che ha il compito di Rinforzare** il FRAGILE cablaggio in firbra di vetro. Qualche volta è richiesta l'aggiunta di un fil di ferro per rinforzare ulteriormente il cavo. I 2 cavetti in fibra di vetro interni, sono chiamati anche "The core and the Cadding", di solito si tratta di vetro

MOLTO PURO con un indice di REFRAZIONE altissimo, per cui la luce viene INTRAPPOLATA nella fibra di vetro, **Il processo è chiamato TOTAL INTERNAL REFLECTION**, E permette alla fibra ottica di attuare una piccola “pipe” , guidando la luce ad una distanza enorme.

Comunicazioni Radio: Nelle comunicazioni radio, gli impulsi **viaggiano nell’aria**. **Non hanno bisogno di cablaggi** per essere strasmessi.Le onde radio possono dividersi in tante categorie: Radio,Ifrarosse,RaggiX, Raggi Gamma.
In tutte queste categorie di emissioni radio esiste **un Generatore di Onde** o un punto dove essi fuoriescono, **Viaggiano tutte alla Velocità della luce** c = 299, 792, 458 in Vacuum. Questa velocità è molto accurata, è chiamata Velcoità delle onde elettromagnetiche. Esiste l’equazione (frequenza) x (lunghezza d’onda) = C,
Tutte queste onde viaggiano nel Vuoto (vacuum), ma hanno interazioni diverse con Diversi tipi di metalli. **Varia la lunghezza d’onda e la frequenza**.
Le frequenze basse hanno delle onde LUNGHE. (Lunga distanza) Le frequenze alte, hanno onde Corte. Dalla lunghezza d’onda si può risalire alla frequenza e vice versa.
Sono state costruite delle periferiche di rete Wirless a 2,4 Ghz, e onde infrarosse, 820 nano metri, esse rappresentano il futuro del networking.

Le specificazioni dei media(cablaggi): Nel 1980 molte compagnie produssero numerosi tipi di comunicazioni. **Queste erano però tutte diverse fra loro**. Poco più tardi, l’organizzazione ISO, per la standardizzazione, **crea il modello OSI. Esso serve per rendere compatibili le reti**.
Il modello osi rende compatibili le comunicazioni mondiali. Alcune compagnie hanno creato degli **standard per quanto riguarda i cablaggi** utilizzati. Vennero realizzati ciò, **anche per rispettare norme compatibili per la sicurezza. Del fuoco, degli edifici e della sicurezza in generale**. In fase di progettazione di una rete, bisogna tener conto di ciò. Ci sono molte opzioni attuali per costruire delle reti, per cui bisogna guardare molto **anche alle performance**.
Gli standard dei cablaggi sono stati imposti e **concepiti da parte dei seguenti gruppi di persone**:

IEE: Istituto per gli ingegneri elettrici (ethernet, token ring)
UL: Laboratori sottoscritti (security, twisted pair)
EIA: Alleanza dell’industria elettronica (standard structures for support media)
TIA: Associazione dell’industria della telecomunicazione (standard structures)

Gli ultimi 2 di questi hanno anche creato degli standard, si sente più volte parlare di EIA\TIA standards. Hanno inoltre creato **delle strutture per il supporto specifico** di questi loro cablaggi.
L’istituto IEE ha invece lavorato molto sugli **standard ethernet e token ring**.
La UL punta molto sulla sicurezza e sulla **performance dei piccoli fili all’interno dei cavi**.
Le UL hanno messo appunto degli standard per **controllare la Protezione e Schermatura** dei cavi.

Gruppi TIE\EIA: Ebbero un grosso impatto sull'industria del netowking. Soprattutto per gli standard TIE\EIA-568-A e TIE\EIA-569-A.
Specifiche di TIE\EIA

568-a: Edifici commerciali. Comunicazioni e cablaggi standard.
569-b: Edifici per le comunicazioni tramite dei percorsi specifici o spazi
570-a: Residenziali e LeggereTelecomonicazioni commerciali. Cablaggio standard.
606: Amministrazione standard delle infrastrutture commerciali, di comunicazione
607: Commercializzazione di apparecchiature di terra e di sicurezza per le telecomunicazioni.

Essi specificano l'indispensabile per la produzione e la vendita multipla. Essi permttono lo sviluppo di LAN senza necessariamente utilizzare GLI STESSI equipaggiamenti, esiste la possibilità di abbinare più cablaggi per creare reti più efficenti. Questo campo è tutt'ora in espansione.

I dettagli dell'TIE\EIA 568-A: La TIE\EIA fa attenzione a diverse cose, in fase di cablaggio:
Cablaggio Orizzontale,Armadi per le Telecomunicazioni , Cableggi Backbone, Stanza specializzate, Aree di lavoro, Entrate Facilitate.
Il 568-A per ORIZZONTAL CABLING, intende un cavo che percorre un percorso che porta una comunicazione con connettività **su superficie orizzontale**. Cavi che percorrono un determinato percorso e che vanno a **ricollegarsi a speciali "armadi" o centraline che contengono un terminatore meccanico**. Il cablaggio orizzontale include il cavo che si usa **tipicamente per collegare un armadio di fili ad una workstation**.
IL 568-A Contiene delle specifiche governative sulla propria performance. E' utilizzato per installare 2 cavi, uno per la voce, un altro per i dati. Dei 2 cavi, uno per la voce può essere composto da 4 paia di UTP.
Le specifiche del 568-a **si dividino in 5 categorie di cablaggio**:
CAT1, CAT2,CAT3,CAT4,CAT5. **La categoria 5 è utilizzata generalmente per le LAN**. E' tutt'ora una categoria in fase di implementazione.
Possono esistere diversi cavi inclusi in qs categorie: Shields Twisted Pair, No Shields Twisted Pair, Fiber Optical Cable, Coaxial Cable.

Shield Twisted, Cavo a 150Ohm,
Unshield Twisted 100Ohm,
Fiber optical 62,5\125 Cavo Multi-Modo
Coassiale, 50Ohm

Il coassiale a 50Ohm, fa parte del 568-a, ma è possimo ad essere rimosso dalla categoria. Tutt'ora **non è consigliato**. **Verrà tolto quando lo standard sarà Rivisto**.
Secondo lo standard 568-a **sono necessari almeno 2 Sbocchi** per connettere **ogni area**. Questo tipo di sbocco\connettore, è supportato da 2 cavi. Il primo dev'essere un cavo (Two Pairs) da 100Ohm, CAT3 o maggiore. Cavo UTP con un appropriato connettore. IL secondo, può essere uno dei seguenti:

- 4 Paia di TWISTED-PAIR non schermati con gli appropriati connettori
- Un 150ohm schermato TWISTED-PAIR con gli appropriati connettori

- Un cavo coassiale con gli appropriati connettori
- Due fibre ottiche 62.5\125 con gli appropriati connettori

Secondo lo standard 568-a, un cavo che sale in orizzontale non può superare la distanza di 90 metri. Questo vale per tutti i cavi di Categoria 5 UTP riconosciuti. Il cavetto-PATCH sul punto orizzontale di connessione, **non può eccedere i 6 metri** di lunghezza.
568-a **permette una lunghezza massima di 3 metri per connettere una patch all'interno di un'area di lavoro**. La lunghezza totale dei cavi di connessione alle patch, non può superare i 10 metri, Infine, la 568-a, richiede le norme di "DEPOSITO" e di "TERRA" conforme al 607.
L'industria ha già realizzato architetture di classe 5e, 6 e 7 che offrono miglioramenti rispetto alla classe 5.

Cablaggi e connettori: Possono esserci vari tipi di terminatori al cablaggio e vari tipi di cavi, questo invoglia la ricerca, lo sviluppo e lo studio del cablaggio.
IL FLUKE è un Tester per i cavi.
I cavi possono essere invertito o Diretti. Si usano quegli diretti quando si raggiunge un device con un invertitore all'interno.
Cavi invertiti: Per collegarsi ad una console, ad un router o Switch. (rollover Cable). Pc-pc.
Cavi normali: Per gli hub.

Corrispondenza 8 fili: RTS, DTR, TxD, GND, GND, RxD, DSR, CTS.
1) RTS = Request To Send,
2) DTR = Data Terminal Ready,
3) TxD = Transmit Data,
4-5) GND = Ground (One for TxD and one for RxD),
6) RxD = Receive Data,
7) DSR = Data Set Ready,
8) CTS = Clear To Send.

Le ethernet sono generalmente composte da 4 FILI. Utilizzano 1,2,3,6.
Il cavo Roll-Over è anche chiamato A CONSOLE CABLE.

Ethernet 10 Base-T: E' una delle 3 tecnologie di rete. (ethernet, token ring, fdd). Il trasporto avviene, con medi tratti di terra, per lunghe distanze a velocità bassa. E fra centrali di computers ad alta velocità per brevi distanze. Si utilizzano cavi non troppo costosi. Le seguenti **periferiche sono PASSIVE**, richiedono energia per operare:
Pannelli Patch, Plugs, Cablaggio,Connettori.
Ci sono inoltre le **periferiche ATTIVE**,richiedono energia per offrire il loro lavoro:
Trasmittenti, Ripetitori,Hubs.
Il connettore standard è REGISTRED JACK 45 o RJ45. Riduce disturbi, la riflessione ed i problemi di stablità meccanica. Ha 8 conduttori. E' considerata una periferica passiva, E' solo un percorso di conduttura per i BITS. Non è considerato un DEVICE.
Lo standard 10BaseT è Categoria 5. E' composto da TWISTED PAID cable, è poco costoso, e facile da installare. La sua funzione è quella di trasportare bits. **Questo CABLAGGIO, E' livello1**.

Il connettore RJ45, è composto da 8 conduttori, che si collegano assieme al plug rj45. Sotto ci sono delle vie che separono i Twisted Pairs in una specie di forca chiamata Punch-down-tool che si collega ai ferretti conduttori. Fa parte della categoria di LIVELLO 1.
I pannelli Patch, sono una serie di "spazi" per l'alloggiamento dei jack rj45, sotto troviamo i punch-down-blocks con conduttori. Le patch appartengono al livello1.
Trasmittenti, sono un comabinazione di ricevitori e trasmettitori. Servono per converitre il segnale sotto un'altra forma. Trasformano da 10base2,10base5,10baseT o 10\100base-fx.
Esiste la possibilità di convertire il segnale AUI-Rj45. Sono in questi casi di livello1. Le trasmittenti sono a volte LOCATI all'inerdno di NIC, in questo caso si parla di LIVELLO2 e sono chiamati signaling components.
Ripetitori, Rigenerano il segnale per poterlo far arrivare a lunga distanza. Solo di livello1.
Possono incrementare il numero di nodi connessi alla rete e ovviamente la distanza che la stessa rete può coprire.I ripetitori rigenerano il tempo reale il sergnale prima di spedirlo di nuovo.
Lo svantaggio di questi apparecchi è il non poter filtrare il segnale. Il segnale passa e viene risputato. Niente di più.
Ripetitori multiporta (HUBS), Sono delle centraline che possono connettere 4,8,12 o 24 jack rj45, hanno bisogno di alimentazione e servono per ripetere il segnale. Sono l'ideale per costruire una rete velocemente **senza spendere grosse cifre**. Sono periferiche livello 1
Tutte queste periferiche, di livello 1 hanno **SOLO IL COMPITO di trasportare BITS**. Nessun indirizzo, nessun routing. I maggiori problemi di rete sono generati da problemi di collegamento fisico.

Collegamenti e condivisione di Media: Possono esistere vari mezzi di comunicazione:
Mezzo di comunicazione condiviso, numerosi host hanno accesso al medesimo pezzo di cavo, Possiamo disporri vari pc sullo stesso cavo, ma esso deve essere CATEGORIA 5UTP con almeno paia di cilo (PAIRS WIRES).
Mezzo di comunicazione condiviso Esteso, E' una tipologia di cavo in cui la rete può essere estesa, può ospitare più accessi, più utenti, Ci sono come sempre aspetti positivi e negativi.(tramite 1 repeater ad esempio)
Mezzo di comunicazione POINT to POINT, Consiste nel connettere solo una periferica via link. E' comunemente usato nelle attuali connessioni telefoniche ad internet (DIAL UP).
Molte reti **non sono connesse direttamente**, spesso sono separate da apparecchiature varie, alcune di alto livello di rete. Si può parlare di:
Circuit Switched: E' una rete non direttamente connessa, in cui gli attuali circuiti sono mantenuti per tutta la durata della connessione. Gli attuali collegamenti telefonici sono in parte di tipo "CIRCUIT SWITCHED",
Packet Switched: E' una connessione sempre indiretta, Un pacchetto viene inviato, esso contiene delle informazioni poiché altri server o nodi, effettuando routing, possano consegnarlo, nella destinazione scelta. Il vantaggio è che questa tecnica è facilmente applicabile, molti host possono condividere questa informazione. Lo svantaggio, a volte possono verificarsi degli errori.

Collisioni e Collision Domains: Una situazione che si verifica quando 2 bit propagano lo stesso segnale sulla rete. Avviene una Collisione. In un collegamento con soli 2 pc, **questo può non risultare un problema**, l'invio viene ripetuto e la connessione va avanti. **Il problema può essere più grave** nel caso in cui pc, connessi in grandi reti, devono scambiarsi milioni di bit per ogni secondo.

Se **c’è un solo cavo** che connette molti pc alla rete, la possiiblità di una collisione esiste. E’ anche possibile che si verifichino delle collisioni in **segmenti di rete “NON FILTRATI”,** ad esempio prolungati sono da REPEATERS.
Ethernet **consente il circolo di un solo pacchetto per volta**.Se più di un nodo prova a trasmettere allo stesso tempo, avviene una COLLISIONE, Ed i dati possono subire un danneggiamento.
Il punto dove ha origine la collisione, è chiamato “collision domain” (è un gruppo di più pc..ad esempio) e include tutto il tratto di cavo condiviso. Un altro cavo può essere collegato tramite 1 patch. Tutte queste interconnessioni di livello1 fanno parte del collision domain.
Quando avviene una collissione il pacchetto viene DISTRUTTO, bit per bit. Per superare questo problema, la rete deve avere una parte che si occupa della gestione del transito dei pacchetti, **questo fenomeno è chiamato CONTENTION**.
Un impulso non può occupare lo stesso punto, nello stesso momento, di un altro impulso, altrimenti avviene una collisione.
Si pensa che le collisioni vadano a peggiorare le performance delle reti. **In realtà un certo numero di collisioni è normale**, questo avviene perché molti pc, cercano di comunicare con altri, nello stesso tempo tramite lo stesso filo.
C’è **un protocollo chiamato Aloha** che è tutt’ora in studio, per eliminare il problema delle collisioni.

Accessi condivisi sulla collision Domain: E’ una situazione che si verifica spesso, **se si connette molti sistemi su un singolo cavo** senza altre periferiche di rete. Si verifica una collisione. Il tratto di file è un collision domain. Dipende da caso a caso, talvolta una situazione critica può **limitare il numero di computer** che possono utilizzare quel tratto di rete, chiamato SEGMENTO.
I ripetitori possono RIGENERARE e Ri-Temporizzare i bit, **ma non sono in grado di applicare** una correzione al flusso (FLOW) al transito dei bits sulla rete, Usare un ripetitore può essere sbagliato, in quanto spesso **si rischia di Estendere** i collision domains.
Un hub è un multiport repeater, per cui, esso **può estendere il collision domain** ad un largo numero di computers, da ciò ne deriva una notevole diminuzione delle Performance dell’intera rete.
Sia gli hub che i ripetitori sono di livello 1 per cui non possono correggere questi problemi. L’utilizzo di ambedue le periferiche comporta un enorme aumento del collision domain.

Il caso in un collision domain con 4 Ripetitori: Non possono esserci più di 2 ripetitori ogni 2 computer sulla rete. Per fare in modo che una rete10BaseT funzioni correttamente, **il ritardo complessivo di (Ripetitori, Cavo e Nic), dev’essere inferiore rispetto al Round-Trip Delay**.
Il ritardo dei ripetitori della rete 10baseT è di 2 millisecondi, il ritardo del cavo è di 0.55 millisecondi per ogni 100 metri, il ritardo di una scheda di rete(NIC) è di 1 millisecondo, delay (the 10BASE-T bit time of 0.1 microseconds times the minimum frame size of 512 bits), è 51,2 microsecondi.
Per 500 metri di cavo UTP connesso tramite 4 Ripetitori, e 2 NICs, il ritardo è sotto il massimo consentito. Latenza del Repeater, ritardo della propagazione,

contribuiscono con il problema dei 4 ripetitori. Andare oltre questo limite vuol dire violare il DELAY limit.
Quando questo limite è superato **il numero di collisioni aumenta drammaticalmente**!!!
Una collisione da ritardo (late collision), avviene **dopo che i primi 64byte del messaggio** sono stati trasmessi. Quando c'è una collisione da ritardo, l'interfaccia di **rete non sente di dover RISPEDIRE il pacchetto** automaticamente.
Questi frame sui quali avviene la collisione, caratterizzano il Consumo Differito. (consumption delay). La latenza aumenta e le prestazioni del network diminuiscono. Questa regola dell'ethernet è definita **regola del 5-4-3-2-1. : 5 sezioni di cavo, 4 Ripetitori, 3 sezioni miste (con hosts), 2 sezioni link, 1 largo collision domain.**

Limitare le collisioni in segmenti: La migliore soluzione per evitare le collisioni è di eliminare il carico eccessivo sui segmenti. A tale scopo è possibile dividere i segmenti con BRIDGE oppure con SWITCH o con Router. Questo processo è chiamato. SEGMENTATION.
Il bridge elimina il traffico, lo filtra, lo divide in segmenti, elimina il lavoro superfluo. Il traffico che va in collisione non passa dal bridge e non va ad influenzare il resto della rete.
Il bridge è usato quando c'è troppo traffico. **RISOLVE il problema della collisione**.

Tipologie di rete e problemi: Abbiamo visto che esistono le tipologie FISICHE e le tipologie LOGICHE. LE tipologie fisiche comprendono il cablaggio e la struttura base di rete, le tipologie logiche sono determinate dagli apparecchi che consentono lo scorrere dei dati.
In caso di collisione, si tiene presente della tipologia LOGICA.
Una rete può avere toplogia fisica e topologia Logica completamente differente l'una dall'altra. 10BaseT (phisical extended star topology, logical bus topology)

Linear Bus Topology: Secondo una prospettiva matematica, tutti i nodi sono connessi direttamente ad un cavo, e non ci sono altre connessioni fra il nodo.
Secondo la prospettiva fisica, Ogni cavo di ferro è collegato al cavo principale, **Permette a tutte le macchine** di allacciarsi al singolo cavo caondiviso,
Vantaggio:Ogni host è connesso a se stesso e possono comunicare.
Svantaggio: **Una rottura di questo cavo comporta la rottura** di tutte le connessioni.
Prospettiva Logica, Abilita tutte le periferiche a vedere il segnale delle altre periferiche, E' un vantaggio **se si vuole che le informazioni vadano a tutti gli hosts**. E' uno Svantaggio poiché **possono verificarsi Collisioni**.

Ring Topology: Secondo una prospettiva matematica, Questa tecnologia consiste in **un anello circolare che collega vari link,** Ogni nodo è connesso solo dai 2 nodi adiacenti. Prospettiva Fisica, Questo schema mostra tutte le periferiche collegate fra loro come una catena (margherita), Prospettiva Logica, Per controllare l'informazione ogni host deve passarla a quello adiacente.

Dual Ring Topology: Secondo la prospettiva matematica, Questa tipologia **consiste in 2 anelli concentrici con diversi host collegati**, ognuno di

questi è linkato solo con il proprio esterno, i 2 anelli non sono collegati. Prospettiva fisica, E' lo stesso schema del ring topology per eccezione di un anello adiacente, interno che connette le stesse periferiche, Nel mondo, per manetener estabilità, ogni macchina è parte di un anello indipendente. Prospettiva Logica, Questo modello comprende 2 anelli, solo uno di essi alla volta è utilizzato.

Star Topology: Secondo la prospettiva matematica, **Un link centrale ed altri link connessi direttamente**. Non sono permessi altri link. Prospettiva Fisica, Un link centrale con tanti link radiati da esso. Il VANTAGGIO, Permette ai nodi di comunicare con tutti gli altri, convenientemente, Svantaggio, Se il nodo centrale si rovina, la rete crolla. E dipendentemente dal tipo di periferiche usate, **la COLLISIONE può essere un problema**. Prospettiva Logica, Il flusso di tutte le informazioni viene lanciato su di una sola periferica, Questo **può essere buono per la sicurezza** o per i casi in cui c'è bisogno di restrizioni. Ma **il nodo centrale può avere dei problemi**.

Extendeed Star Topology: Prospettiva matematica, E' la stessa cosa della tipologia a stella, **unica differenza ogni link diventa a sua volta il nodo centrale di un'altra stella**. Prospettiva Fisica, E' una prospettiva CENTRALE, per cui ogni link esterno è a sua volta interno ad altri. Il vantaggio sta nel fatto che il cablaggio per l'interconnessione è corto e liminta le periferiche che si deve mettere in mezzo per portare la connessione.Prospettiva Logica, Le informazioni vengono dirottate sulla stella centrale. E' l'attuale struttura del sistema dei telefoni.

Tree Topology: Prospettiva matematica, E' simile all'extended star. Prima differenza sta nel fatto che qui **non c'è un solo nodo centrale, ma dei nodi troncati che si estendono per altri nodi**, Possono dividersi in Binary Tree ed in Backbone Tree. Prospettiva Fisica, Il tronco è un cavo che ha diversi rami. Prospettiva logica, Il controllo di informazioni è HIERICHAL.

Irregular Topology: Prospettiva matematica, **Non esiste nessun collegamento ovvio e logico** con i nodi, Prospettiva Fisica, Il cablaggio è inconsistente. Esistono vari nodi concatenati fra loro, di solito **sono reti in fase di costruzione o progetti poveri**. Prospettiva Logica, Non esiste alcuna logicità nei collegamenti.

Complete Mesh Topology: Prospettiva matematica, **Ogni nodo è linkato DIRETTAMENTE** con gli altri nodi. Prospettiva Fisica, Questo tipo di cablaggio ha distingamente dei vantaggi e degli svantaggi, Un vantaggio è che **ogni nodo è direttamente collegato con tutti gli altri**,se l'informazione fallisce da una parte può trovare altre strade per arrivare a destinazione, Un altro vantaggio **questo schema consente all'informazione di essere controllata da diversi nodi** e poi di essere rimandata indietro con facilità. Lo svantaggio sta nel fatto che l'ammontare di connessioni per Links diventa ECCESSIVO (ogni nodo riceve per tutti).Prospettiva Logica, Il comportamento di questa tipologia di rete, dipende molto dalle apparecchiature utilizzate.

Tipologia di RETE CELLULARE: Prospettiva matematica, coniste in più aree circolari,compongono una struttura esagonale, ogni area, all'interno, ha un

nodo al centro.Prospettiva Fisica, E' una struttura geografica che si divide all'interno delle regioni in CELLE (cells), **Non ci sono collegamenti fisici, bensì SOLO onde elettromagnetiche**. Spesso i nodi riceventi si muovono(car cell phone), ed anche i nodi trasmittenti (satellite). Il Vantaggio primario è che **non c'è bisogno di alcun cavo**, le onde passano attraverso l'atmosfera. Lo svantaggio primario sta nel fatto che **le onde sono suscettibili a distruzioni e possono nuocere alle persone**. Prospettiva Logica, Le strutture cellulari comunicano fra di loro direttamente (entro le dovute distanze), oppure comunicano con le cellule adiacenti, il che è inefficiente. Le cellular base topologies sono integrate con le altre tipologie anche se usano l'atmosfera o i satelliti.

Livello di rete 2

Livello2 considerazioni: Il livello 1 ha la funzione di trasportare i dati, ma **da solo non sarebbe sufficiente**, esso non può comunicare con gli altri livello, per cui a tale scopo le NIC operano su livello2. **Per le limitazioni del livello 1, c'è il livello 2**. Il livello 2 ha il Logical **Link Control (LLC)**, per cui si risolve il problema del livello1 che non può comunicare con gli altri livelli. Il livello1 non può identificare i computers, Il livello 2, crea i frame e raggruppa i bits. **Il livello 1 non decide** quale computer deve trasmettere in un grande gruppo, per cui trasmetterebbero allo stesso tempo, **il livello 2 ha il MAC (media access control), che è la soluzione** per questo.

802,2= definisce l'LLC, ed il transito verso strati SUPERIORI.
802,5= definisce il tipo fisico di rete.(ex token ring)
802,3= definisce il livello 1, la porzione di canale di accesso del data link.

Comparare il livello 2 con livello 1 in reti standard: L'istituto per gli ELECTRICAL e ELECTRONICAL INGENeering, è l'organizzazione **che definisce le reti standard. (IEEE),** includendo 802,3 e 802,5**. IEEE 802,3 definisce il livello1, e la porzione di canale di accesso** del data link su livello2. Il modello osi ha 7 Lati. IEEE riguarda solo i 2 lati inferiori, **il livello data link è DIVISO in 2 parti**. La tecnologia indipendente 802,2 LLC standard. La specifica tecnologia dipendente che include il livello 1.
La IEEE divide l'osi layer di livello 2 in 2 sottostrati. I sottostrati riconosciuti sono:
MEDIA ACCESS CONTROL (MAC). Transita i dati sotto, sul media (con livello1).
LOGICAL LINK CONTROL (LLC). Transita i dati verso l'alto (con livello3).
Questi sottostrati sono attivi, **per rendere compatibili** le comunicazioni con computer e periferiche.

Comparare IEEE Con il modello OSI: IEEE è la prima garanzia contro la violazione del modello OSI. **Esso definisce il proprio livello (LLC)**, incluso il proprio protocollo di trasmissione (PDU), che sono i frames. **Secondo, dopo LLC esiste MAC.e 802,3, 802,5 che definise il nome**, il frame ed il media access control attorno al quale specifica tecnologia è costruita. **L'osi è un indice per indicare i processi di rete**. IEEE interviene quando i problemi si sono già verificati. E' importante vedere nei dettagli le funzioni di mac e LLC**. La differenza fra gli standard OSI e gli standard IEEE risiede nella periferica di rete NIC** dove c'è anche il MAC (livello2). Molte nick comprendono anche un transceiver di livello1, situate all'interno e connesse direttamente al cavo. Molte cose possono essere viste **DAL punto di vista standard IEEE al punto di vista OSI**.

Logical Link Control (LLC): Lo standard IEEE ha creato un sottostrato Logico, per permettere ad **una parte del data link di funzionare indipendentemente**. Questo livello porta **versatilità** all'intera rete, **soprattutto ai protocolli che si trovano sopra di lui**, nel frattempo comunicano

efficaciamente con varie tecnologie sotto di lui. **L'LLC partecipa al processo di Incapsulamento**, ciò che viene creato da LLC, è definito LLC PACKET.
LLC prende i dati dal protocollo di rete ed aiuta IP. Aggiunge **ad esso, maggiori informazioni** per dirottare i pacchetti ip alla destinazione finale. Esso aggiunge 2 indirizzi appartenenti alle specifiche 802,2. **Il Destination Service Access Point (DSAP) e Source Service Access Point (SSAP) e richiede maggiori informazioni allo strato mac**, per poter inviare il pacchetto a destinazione, inoltre include le informazioni relative alla tecnologia di rete. (token ring, fdd,e cc.ecc). Il sottostrato LLC **gestisce le comunicazioni delle periferiche Sopra il singolo livello**, sulla rete. **LLC è definito IEEE 802,2** e funziona con ConnectionLESS e Connection ORIENTED definiti ovviamente nei livelli superiori. IEEE 802,**2 definisce un numero di campi** nel data lynk layer frame, che abilitano multipli livelli alti, a condividere un singolo data lynk fisico.
Il livello di sottostrato MAC, tratta tutti i protocolli che un host segue per arrivare a comunicare con il media fisico (cavo).

Concetti del livello 2: Comunica con i livelli più alti tramite un controllo logico, Utilzza una magra conversione dei nomi per l'identificazione. Utilizza i FRAME per organizzare i gruppi di dati, Utilizza il MAC per decidere quale computer deve trasmettere i dati, in un gruppo di vari computer.

Il formato dell'indirizzo MAC: La numerazione decimale è BASE10, Ed i numeri binari sono Base2, Un'altra numerazione esiste. **L'esadecimale (HEX), che è un sistema Base16**.
Hex è di fatto un metodo più BREVE per rappresentare il sistema degli 8Bit. E' possibile rappresentare il sistema di 8bit utilizzando solo 2 numeri esadecimali.
Esadecimale=4 BIT.
L'indirizzo **mac è 48BIT,** è espresso in 12 Esadecimali. **LE prime sei cifre sono rappresentate da IEEE**, Gli identificativi sono la marca del venditore, e OUI (organizzation unique identifier).
Le rimanenti 6 cifre del numero esadecimale rappresentano il numero seriale dell'interfaccia o un altro valore inserito dal venditore.
L'indirizzo mac è stampato sulla base dei BURNED ip ADRESSES, (BIAs). Il mac è impresso su ROM ed è copiato su RAM quando la NIC è inizializzata.

OUI=24 Bits	**NIC, vendor assignment= 24 BITS.**	**Totale MAC 48BITS.**
6 Cifre	**6 Cifre**	**Totale 12 Cifre.**
00 60 2F	**3A 07 BC**	
Cisco	**Particular Device**	

Numeri Esadecimali HEX: I numeri Esadecimali che compongono il MAC ADDRESS, hanno BASE 16, **Sono riferiti alla BASE di 16 perchè utilizzano 16 simboli**.
Possono rappresentare tutti i numeri possibili. Consideriamo che per i numeri bastano solo 10 cifre per cui **i restanti 6 sono rappresentati da lettere, A,B,C,D,E,F**.
I numeri sono moltiplicati per 16 e vengono elevati alla cifra esponenziale, il conteggio parte dall'ultima cifra fino alla prima.
Esempio:
4F6A = (**4** x 16^3)+ (**F**[15] x 16^2)+ (**6** x 16^1)+ (**A**[10] x 16^0) = 20330 (decimal)
0,1,2,3,4,5,6,7,8,9 poi A=10 B=11 C=12 D=13 E=14 F=15

Convertire Decimali a EsaDecimali: E' chiamato REMAINDER METOD. **Dividi i numeri decimali ripetutamente per 16**. Si divide. la rimanenza ogni volta per 16.

24032/1 = 1502, with a remainder of **0**
6
1502/16 = 93, with a remainder of 14 or **E**
93/16 = 5, with a remainder of 13 or **D**

5/16 = 0, with a remainder of **5**

Il risultato è 5DE0

Convertire Da Esadecimali a Decimali: E' necessario moltiplicare per 16 ogni numero.
E l'esponente dev'essere progressivo. Si parte dall'ultima cifra, eleveando il numero alla 0,1,2,3 ecc.ecc

Convert the hex number **3F4B** to a decimal number. (Work from right to left.)

3 x 16^3 =	1228	
F(15) x 16^2 =	3840	
4 x 16^1 =	64	
B(11) x 16^0 =	11	
	1620	= decimal
	3	equivalent

Computer senza nome e MAC: Senza mac avremo un gruppo di computer "senza nome" sulla rete, quindi, al livello data lynk, un header ed un trailer può essere aggiunto ai dati destinati allo strato superiore. L'header ed il trailer contengono informazioni che servono allo strato superiore, per cui il MAC è indispensabile. Questi dati indispensabili vengono incapsulati.

Indirizzo MAC sulla NIC: Ogni computer ha un unico modo di identificare se stesso, Ogni computer, collegato alla rete o meno **HA UN INDIRIZZO FISICO**. E' situato sulla scheda di rete. In fase di costruzione è assegnato un indirizzo fisico per ogni NIC. E' programmato dentro L'eprom, all'interno della nic. Se la scheda di rete è sostituita, ne viene messa un'altra, il pc rileverà il cambiamento sul nuovo mac address. Il mac è scritto usando numeri esadecimali (Base16), Ci sono 2 formati di mac address, 0000,0c12.3456 oppure 00-00-0c-12-34-56

Utilizzo del mac da parte delle nic: Ethernet e le lan 802,3 sono reti BroadCast. Ogni stazione esamina Ogni frame per determinare dove si trova la stazione di destinazione.
Quando una periferica vuole comunicare con un'altra, questa si apre una via di percorso, in relazione al MAC Address, Quando una periferica invia dati fuori dalla rete, **viene trasportato il mac address** nella destinazione desiderata.Durante il trasporto di questi dati,**le nic dei pc, analizzano il mac** e verificano **se questo indirizzo mac gli appartiene**. Se non gli appartiene non viene preso.
I dati passano attraverso il cavo**, le schede di rete di ogni stazione li controllano**. Le schede di rete **verificano l'indirizzo di destinazione nella testata del frame**, per vedere se il pacchetto è propriamente intestato a se. Quando il pacchetto passa alla stazione di destinazione, la scheda di rete se ne fa una copia, estrapola i dati, li trasforma e li da al computer.
E' importante l'INCAPSULAMENTO ed il DECAPSULAMENTO, includere l'informazione MAC. Senza di essa non sarebbe possibile inoltrare il pacchetto.

Limitazioni dell'indirizzo MAC: L'indirizzo mac ha funzioni vitali in una rete di computers, fornisce una via per l'identificazione delle macchine. **Gli host hanno un nome unico e permanente**. Le combinazioni di indirizzi mac non vanno ad esaurirsi subito, poiché sono 2 TRILIONI di combinazioni!

Gli indirizzi MAC hanno anche Svantaggi**, non hanno una propria strtuttura solida**, sono considerati “flat address space”, Differenti venditori hanno impresso sulle schede di rete, **differenti codici OUIs**, sono come un numero personale di identificazione.
Se la rete cresce, questo può diventare uno svantaggio di maggior influenza.
nessuno ne garantisce l'unicita' e poi il meccanismo che fa uso del mac address non è il massimo in termini di local security.

Perché la Framizzazione è necessaria: L’encoding dei bit su un cablaggio rappresenta oggi un grande progresso che permette di avere dei vantaggi, ma questo processo da solo, purtroppo, non è unicamente sufficiente affinchè avvenga una vera e propria comunicazione, **I Frame aiutano ad ottenere delle informazioni che non si avrebbero con il solo passaggio di bits**.
Quando si lavora con i bit, bisogna guardare il diagramma **tenendo conto di unità di misura come VOLTS in relazione al TEMPO**. Se si lavora con grandi quantità di dati, questo grafico può ingrandirsi ed assumere delle proporzioni ridicole.
Si può usare il FRAME FORMAT DIAGRAM, che è sempre basato sul voltaggio\tempo, in un grafico. La lettura va effettuata da sinistra verso dentra, proprio come il grafico di un oscilloscopio. Visualizza diversi gruppi di bits (fields) ed effettua altre funzioni.

Analogie e specifiche dei Frames: Picture Frame Analogy: LA creazioen del frame avviene come se fosse il disegno di una fotografia, Viene creato questo disegno per trasportare i dati con sicurezza. Nella comunicazione il frame è in realtà “un disegno di frame”, Mentre “i colori” si possono paragonare ai dati. Il frame inserisce un header ed un trailer per rendere facilmente trasportabili i dati.. Il frame aiuta i dati a proteggersi da errori..
Packaging\Shipping Analogy:,Movies Television Analogy
Possono esserci Vari tipi di frame. Il frame singolo ha delle sezioni interne chiamate **FIELDS.**
Ogni fields è composto da bytes. I nomi di questi Fields sono i seguenti:
A=Frame Start Field,
B=Address Field,
C=Lengt-Type-Control Field,
D=Data field,
E=Frame check sequence field,
F=Frame stop field.

Quando i computer sono collegati ad un media fisico, **c’è un modo per avvisare “broadcasting” che il frame sta arrivando**, Ci sono varie tecnologie e vari modi per far ciò, questo riguarda l’inizio della sequenza di dati.
Tutti i frames contengono informazioni relative a NOME del mittente, Inteso come MAC ADDRESS, e nome del destinatario (mac del destinatario)
Per la maggior parte dei casi **la lunghezza globale dei FIELDS compone la lunghezza globale del frame**, Alcuni hanno dei fileds che specificano le richieste del livello 3.Ci sono anche delle tecnologie dove NESSUN fields è utilizzato.
Data Fields dei Frames: LA ragione per cui è indispensabile inviare frame, è semplicemente ottenere un livello(layer) alto di dati, e finalizzare l’invio di dati dal pc origine al pc destinazione.**Il pacchetto di dati che vuoi far arrivare a destinazione, si divide in 2 parti**, 1) il messaggio che vuoi inviare, 2) i byte incapsulati che tu vuoi arrivino al pc di destinazione, ci sono inoltre altri dati da spedire, **Essi sono chiamati PADDING BYTES**, e vengono aggiunti cosicchè il globale del frame raggiunga una dimensione minima, per scopi di tempismo e di performance dell’operazione.
LLC è incluso del data fields dei frames standard IEEE.
Ricordiamoci che **LLC inserisce l’ip ai dati** ed aiuta gli stessi a raggiungere la destinazione. Esso comunica con il livello3.

Tutti i frames sono Suscettibili ad errori da parte di varie sorgenti. Bisogna conoscere gli effetti di questo. **LA soluzione, può essere spedire 2 volte la cornice del frame** (frame twice) poiché siamo sicuri che esso arrivi integro. Quando arriva il pc di destinazione ci manda indietro la coda del frame, per farci capire che possiamo inviarne un altro.
Esiste però un modo più EFFICIENTE per trasmettere i dati. **Ogni volta che il frame viene visto come "bacato", esso viene SCARTATO**, e ritrasmesso.
IL field **(frame check sequence),** contiene un numero **che viene calcolato dinamicamente** dal pc sorgente, è basato sul tipo di dati all'interno del frame, Quando il pc di destinazione riceve il frame, **viene RICALCOLATO** il Frame check sequence, e lo paragona a Check Sequence contenuto nel frame. **Se c'è una diversità, vuol dire che il frame è BACATO**, per cui viene scartato, E viene chiesto alla sorgente di ritrasmetterlo. Ci sono vari modi per calcolare un Frame Check Sequence:

- Circle Redunancy Check (CRC) (effettua un calcolo polinominale) , - Two-dimensional parity (crea una sequenza di 8 bit), -Internet checksum (aggiunge i valori di tutte le data ke arrivano a destinazione).

Infine parlando di STOP FRAME, Per inviare i dati il pc chiede l'attenzione degli altri pc, invia i dati, dopo di che, esso proclama la fine, E' considerata la fine del Frame Check Sequence, **Lo stop E' una normale sequenza di dati riservata alla finalizzazione** del frame.

Definizioni di MAC: il mac **determina QUALE Computer**, sul tratto di cavo condiviso, è autorizzato alla trasmissione dei dati. Con LLC comprende la versione IEEE del livello2. Ci sono 2 categorie di mac, **DETERMINISTIK (taking runs) e NON-DETERMINISTIK** (first come, first served). Nel primo caso, il deterministik, utilizza una forma chiamata "prendi il tuo giro" o take your turn. Ci riferiamo alla tecnologia Token Ring. **Chiunque ha il "GETTONE", può parlare**. Host individuali sono situato attorno ad un anello (cablaggio ad anello,circolare), Speciali forme di dati chiamate TOKEN affluiscono tramite il cablaggio, Quando un host vuole trasmettere, **afferra un token e trasmette** i dati per un tempo limitato, poi **rimette il token in gioco sull'anello, fino a quanto questo token non viene ripescato da un altro pc**..
Nel secondo caso, il Non-Deterministik, **si utilizza l'approccio (primo arrivato primo servito). STRATEGIA FIFO (first in, first out).** O FCFS. Nel 1970 nell'unversità delle away fu inventato un protocollo di comunicazione radio **chiamato ALOHA** che connetteva varie isole awaiane ☺
Il protocollo usato permetteva la trasmissione di una persona. C'era un led che rilevava le radio collisioni, durante la trasmissione. Dal livello Aloha siamo arrivati al moderno protocollo basato su MAC, **chiamato, CSMA\CD Carrier Sense Multiple Access \ Collision Detected**
CSMA\CD è un sistema semplice. **Ogni macchina ascolta sulla rete**. **Quando possibile, trasmette**. Se più persone parlano allo stesso tempo e si **verifica una collisione, nessuno può trasmettere**. **Ogni host nel sistema può Rilevare la collisione**, aspettare il silenzio e poi trasmettere.

Tre specifiche implementazioni del MAC: Il livello 2 comprende varie tecnolgie, token ring, fdd, ethernet. **Tutte queste tecnologie** includono processi di NAMING, FRAMING ed è comune a tutti l'identificazione MAC.

- Ethernet: Logical Bus topology (le informzioni circolano su un cavo centrale), star o extended star (a stella).
- Token ring: Exteendeed ring topology (l'informazione è controllata in un anello) e pshichal star topology
- FDDI: Logical ring topology, Psichal dual ring topology

La tipologia TOKEN RING e le sue VARIANTI: Ibm ha costruito la tipologia token ring nel 1970. E' seconda solo ad ethernet 802,3 IEEE.
La specifica 802.5 è per la maggior parte uguale **e perfettamente compatibile** con IBM Token ring. Lo standard 802,5 è stato progettato dopo ibm token ring e sta continuando tutt'ora il suo sviluppo.

Per token ring oggi si intende una specifica che comprende sia IEEE 802.5 che IBM Token Ring.

Il formato del Frame nella Token Ring: Tokens, I tokens hanno dimensione di 3 bytes, e **sono divisi in "start delimiter", "access control byte" e "end delimiter"**. Lo start delimiter, avverte le stazioni che sta arrivando il token, Questo segnale si distingue da tutti gli altri segnali sulla rete. All'interno del token **esiste una violazione del sistema di encoding**..
Access Control Byte: Gli access control byte contengono campi di **Priorità e Riservatezza**, ed un bit di Token e Monitoraggio. Il token bit **distingue il token dal Data command frame**, il bit monitor determina se un frame è sempre circondato da un anello.
The End Delimiter, **determina la fine del token** o del data control\frame. Esso contiene un bit che indica il frame danneggiato, ed un frame che è l'ultimo della sequenza logica.

Data\Command Frames: Smart delimiter, Access Control, Frame control, Destination Address, Source Address, Data, FCS, End Delimiter, Frame Status.
Hanno una lunghezza variabile, dipendente dalla lunghezza dei FIELDS. **Data Frames, Portano le informazioni al livello superiore**. **Command frames, contengono informazioni di controllo**, e non hanno dati per il livello superiore. Nel Data\Command Frames, **un frame di controllo**, Controlla l'access control byte. **Il frame control byte** indica se il frame contiene un'informazione di controllo o dei dati. Nel frame di controllo questo bit specifica il tipo di informazione di controllo.
Alla coda del frame di controllo ci sono 2 FIELDS, che identificano la destinazione e la stazione sorgente. Come succede con IEEE 802,5, questi indirizzi hanno una lunghezza di 6 bytes. A seguito dell'addess field **troviamo il DATA Field.** La lunghezza di questo FIELD è limitata dal token che sta tenendo in quel momento, Si definisce il tempo massimo per cui può essere tenuto un token. Dopo il data fields troviamo il famoso nonché importantissimo FRAME CHECK sequence. Viene calcolato dal pc che invia il frame, e dal pc di destinazione. Queste 2 numerazioni devono coincidere altrimenti il pacchetto è Scartato automaticamente.
End Delimiter, delimita la fine del command\data frames.

Token Passing: La Token ring e IEEE 802,3, sono 2 modelli sui quale funziona il Token Passante. Durante il processo, un token (un piccolo frame), attraversa la rete.
Il possesso del frame garantisce agli host **la possibilità di trasmettere**. Se la stazione riceve un token che non porta l'informazione MAC identica a quella situata sulla propria NIC, **il token passa al nodo successivo**. Ogni host può tenere il token per un massimo periodo di tempo, dipende dalla tecnologia impiegata.
Quando il token viene ricevuto da una macchina, quest'ultima lo prende ed altera 1 bit di questo. **Il token diventa la partenza della sequenza di frame**. Poi l'host aggrega l'informazione da trasmettere al token e lo trasmette all'host seguente. Mentre l'informazione circola attorno al RING, **non c'è nessun'altro token**, a meno che il RING non supporti la liberazione di altri token.
Tutti gli altri host non possono trasmettere allo stesso tempo. Esso devono attendere finchè il token non diviene disponibile. Le reti token ring non hanno collisioni. Quando la trasmissione del frame è completa, un nuovo token è rilasciato.
Le informazioni sotto formato Frame circolano attorno all'anello, **fino a che non raggiungono il pc di destinazione**, che riceve ed elavora l'informazione per processarla.
Il token poi continua a viaggiare finchè non ritrova l'host di partenza.Quì esso è rimosso.
L'host che invia il token può verificare quando esso è giunto a destinazione.
Le reti CSMA\DC sono deterministike. Questo permette di sapere il tempo che passa affinchè le stazioni potranno di nuovo Trasmettere. Questa funzionalità è particolarmente indicata per reti in cui la previdibilità dei ritardi è molto importante ai fini della robustezza di rete.
Per quanto riguarda il **Priority System**, la token ring assegna una priorità alle macchine che usano frequentamente la rete. Ci sono 2 FIELDS che controllano la priorità: **Priority Field e Reservation**

Field. Solo le stazioni con priorità uguale o più alta di quella contenuta nel token possono afferrarlo. Il prossimo token che viene generato include priorità riservata per quel determinato pc. Dopo la ricezione del token, **la stazione resetta la propria piriorità**.
Sui Meccanismi di Menagement, Token ring utilizza molti sistemi e tecnologie per rilevare e risolvere difetti di rete. Un meccanismo è selezionare un pc nella rete token ring da essere attivamente monitorata.Il token ring **centralizza il tempo di comunicazione** con una stazione e performa numerose funzioni di mantenimento.
L'active monitor può potenzialmente essere ogni pc in rete, Una funzione di queste può essere **cercare di eliminare i frame "BROKEN**" e generare un nuovo token.. Ciò viene rilevato da **Active Monitor.** La tipologia a STELLA, nel token ring, contribuisce ulteriormente al perfezionamento delle performance sulla rete. **Active MSAUs (Multi Station Access Units),** può **visualizzare tutte le informazioni contenute**, eventualmente per risolvere problemi ed eliminare il singolo pc dal RING se necessario. **Una formula chiamata Beaconing** rileva e **cerca di riparare** eventuali difetti nella rete. Quando vengono rilevati seri errori, viene inviato un beaconing frame, **esso prende il nome di Failure Domain**. Il failure domain include il nome del pc che è riporta l'errore, (NAUN) Nearest Active upstream neighbor ed ogni cosa nel mezzo. **Beaconing inizia un'operazione chiamata Autoconfiguration**, dove i nodi nei quali si presenta l'errore automaticamente performano una diagnositica. Avviene una Reconfigurazione della rete attorno all'area Danneggiata, MSAUs completa questa operazione.

Segnalazioni del Token Ring: L'encoding è una via di mezzo fra Temporizzazione e tipologia di trasporto dati che sono spediti tramite un mezzo. L'encoding Manchester combina dati e tempo, in **bit simbolici, che si dividono in 2 parti, La polarità della seconda metà è sempre invertita** rispetto alla polarità della prima metà. **Secondo la Manchester**, 1 è rappresentato in un transito ALTO-INTENSO di dati, e lo zero, in un transito BASSO-INTENSO di dati. 1 e 0 è recuperato da una Transizione di segnale. La temporizzazione può essere ripristinata e stabilizzata dal ricevitore. La 4\16Megabit Token Ring, **usa diversi tipi di Manchester Encoding**, (delle varianti del manchester encoding), Esse si differenziano dalla temporizzazione, e dalle informazioni inserite nei simboli. Es: 1 è rappresentato da una polarità e 0 è rappresentato da una polarità diversa che cambia ad ogni intervallo.

Token Ring and Psichal Topology: Le reti ibm token ring, solitamente cablate utp, sempre collegate a MSAUs i quali possono essere collegati tutti assieme attorno ad un grande anello. MSAUs e MSAUs sono collegati tramite una patch e sono adiacenti ad essa.

Lo standard FDDI e le sue varianti: Nel 1980 la tecnologia ethernet esistente fu spinta al limite. C'era **la necessità di una nuova tecnologia** che rispondesse alle sempre più esigenti domande di utilizzo. **L'ANSI X3T9.5 ha risolto questi problemi distribuendo la FDDI**. (Fiber Distribuited Data Interface). Dopo aver ampliato e completato le specificazioni FDDI, ANSI **ha deciso di proporre questo sistema allo standard (ISO)** ed è stato deciso di **creare una versione internazionale dell'FDDI, che è completamente compatibile con la versione standard dell'ANSI**.
Benchè le FDDI non siano Comuni quanto Ethernet o Token Ring, FDDI ha fatto notevoli progressi,i costi per un sistema del genere si stanno via via riducendo..FDDI è usata frequentemente come Tecnologia BACKBONE per connettere i pc ad altissime velocità.Le specifiche di FDDI sono le seguenti:

- MAC definisce come accedere al media. Formato Frame, Fermata Token, Indirizzamento, Algoritmo per calcolare un ciclo di redundanza nel meccanismo di Controllo e Recupero errori.
- Physical Layer Protocol (PHY), definisce le caratteristiche di codifica. Clocking Requirement, Framing, Ed altre funzioni

- Physichal Layer Medium (PLM), definisce le caratteristiche di trasmissione sul media. Fiber Optipc Link, Power Levels, connectors
- Station Management (SMT), definisce la configurazione FDDI, ring configuration, ring control features, station insertion and removal, inizialitation, fault isolation and recovery, scheduling

IL Formato del frame nel FDDI: Preamble: prepara ogni stazione all'inizio frame, Start delimiter: indica l'inizio frame, Frame Control: indicano la dimensione del campo di indirizzo,se i dati sono Sincroni o Asincroni, Destination Address: Unicast o Broadcast Indirizzi (uno o più di uno) di macchine di destinazione. L'indirizzo di destinazione ha 6 byte. Source Address: indirizzo macchina sorgente. 6byte. Data: dati di controllo, destinati al livello superiore. Frame Check Sequence (FCS): calcolato il Cylic redundancy Check, (CRC). Calcolato valore del frame, paragonato con calcolo a destinazione. Se i conti non coincidono, il frame viene scartato, End Delimiter: Determinano la fine del frame e contengono simboli no-data, Frame Status: Permette al pc sorgente di sapere se si è verificato un errore e se il pacchetto è stato consegnato.

Nota: IL FORMATO DEL TOKEN nelle token ring: PREAMBLE-START DELIMITER-FRAME CONTROL-END DELIMITER.

Il MAC nelle FDDI: Nell'FDDi vengono usate strategie del tutto simili alla TOKEN RING. Un token passa per la rete, Chi ha il token trasmette. Quando una stazione prende il token e non ha niente da trasmettere, passa alla stazione successiva. Quando una stazione prende il token, trasmette ed il token diviene la testata del frame che verrà trasmesso. Ogni stazione deve attendere affinchè il token non è disponibile. Nelle reti FDDI non esiste la possiblità di una collisione.
Nella fddi tutto funziona come nel token ring anche considerando CSMA\CD, dobbiamo però far presente che **nella FDDI abbiamo 2 ANELLI**.
Per cui se per qualunque ragione il primo anello è danneggiato, noi possiamo usare il secondo "come backup". Questo rende la FDDI molto affidabile.
FDDI Supporta allocazione in tempo reale della banda sulla rete, E' molto utilizzata per differenti tipi di applicazioni, **FDDI offre questo supporto per definire 2 tipi di traffico**, SINCRONOUS e ASINCRONOUS.
Sincronous: Il traffico sincrono può **consumare una parte dei 100megabit** e **l'asincrono può consumarne il resto**. La banda sincronous residente ha la capacità di trasmettere continuamente, **ideale per comunicazioni di voce**, e video.La specifica **FDDI SMT**, definisce uno schema delle risorse offerte e le distribuisce.
Asincronous: La banda asincrona **è distribuita secondo otto livello distinti**, di priorità. Ad ogni stazione è assegnato un livello di priorità asincrono. FDDI permette dialoghi estesi fra pc che usano temporaneamente tutta la banda asincrona. FDDI può impedire a delle stazioni di non utilizzare affatto la banda asincrona**. Abbassa la priorità di asincrona**.

FDDI Encoding 4B 5B: FDDI usa uno schema di encoding chiamato 4B\5B. Ogni 4 bit di data, sono inviati 5 bit di codice. I segnali sorgenti nei ricevendi FDDI sono LEDs oppure Laser.

FDDI Media: Fdd specifica una rete Token passing, 100 megabit, 2 anelli, utilizza fibre ottiche, Definisce un livello fisico ed una partizione dell'accesso al media sul livello link. Questo è simili a IEEE 802,3 e IEEE 802,5, in relazione al modello OSI. Oltretutto essa viaggia ad alte velocità ed è simile al token ring. In comune hanno la token passing e la forma (ring). La **caratteristica di FDDI è quella di usare le Fibre ottiche per le trasmissioni**. Esse hanno dei vantaggi,
Non emettono dei segnali elettrici, sono immuni ad interferenze elettriche, Hanno un potenziale di portata maggiore rispetto ad altri cavi.

Ci sono specifiche sulle fibre ottiche. **SINGLE MODE (mono mode) o MULTI MODE**. Gli impulsi di luce viaggiano attraverso le fibre ad un'angolazione particolare**. Nel Single Mode, permette solo in un modo, alla luce di propagarsi**. Nel modo multiplo la luce può propagarsi nelle fibre in diversi modi. Nel multi mode, la luce può viaggiare a distanze diverse, dipende dal suo angolo di entrata. Questo causa il problema per cui i dati arrivano a destinazione in tempi differenti, questo fenomeno è chiamato **MODAL DISPERSION**. La modalità **SINGLE mode garantisce banda più alta e copre distanze maggiori** rispetto alla multi mode. In un esampio, la single mode può essere usata per sotterraneo, la multi mode può essere usata per costernare un edificio.
FDDI specifica l'uso di 2 anelli nel collegamento fisico, **Il traffico su ciascuno anello viaggia in direzioni opposte**, **Gli anelli hanno un collegamento fra loro in punti adiacenti**. **Uno dei 2 anelli è quello primario**, usato per trasmissione dati, l'altro è **quello secondario, è utilizzato per portare indietro i dati**.
Classe B, o SAS (single attachment stations), si attacca ad un anello, Class A o DAS (dual attachment stations), si attacca ad entrambi gli anelli.Sas sono attaccati al primo anello tramite un CONCENTRATOR, che offre la possibilà di collegamento per multipli SAS.
Il concentrator garantisce che in caso di spegnimento di uno dei SAS, la rete non va giù.
Particolarmente indicato per pc che vanno frequentemente giù nella rete. **Ogni DAS ha 2 porte, A e B, che si connettono al ring**. Essi provvedono alla connessione per il Primario e Secondario anello.

Comparazione Fra Ethernet e IEEE 802,3: Ethernet **è la tecnologia più usata e diffusa**, Si usa per lunghe distanze sotto terra, oppure per brevi distanze in uffici ed edifici strutturati ad alta velocità. Nel 70 venne sviluppato il primo ethernet, e fu usato come base dall'associazione di ingeneri elettrici ed elettronici. IEEE. E' stata rilasciata nel 1980 IEEE 802,3.
Successivamente, intel, xerox, rilasia Ethernet versione 2.0. Sostanzialmente compatibile con IEEE 802,3. Ethernet e IEEE 802,3 detengono il più grande record di mercati condivisi nei protocolli di rete. Tutt'oggi il termine ethernet è usato per definire il CSMA\CD, che sono conformi alle specifiche di funzionamento IEEE 802.3.
IEEE 802.3 supporta delle tecnologie simili in tal caso CSMA\CD..
Ethernet e IEEE 802.3 sono Broadcast Networks, ogni stazione può vedere i frames che essi siano o no destinati a loro. Ogni stazione lo esamina. Il frame passerà al livello superiore solo dopo gli appriopriati processi.
La differenza tra Ethernet e IEEE 802.3 è sottile. L'Ethernet fornisce servizi corrispondenti al Layer1 e al Layer2 del modello OSI. IEEE 802.3 specifica il livello fisico, il Layer 1, e la componente di accesso al canale (?) del Layer 2, ma non definisce un protocollo di Logical Link Control. Sia la IEEE 802.3 sono implementate attraverso l'hardware. TIpicamente la componente fisica di questi componenti è una scheda di rete in una macchina host ....**(ma che cazzo vuol dire??)**
LA differenza fra Ethernet e IEEE 802,3 è molto sottile, Ethernet provvede a gestire servizi che corrispondono con il livello 1 e 2 dell'osi model. IEEE 802,3 specifica il livello 1, e la partizione del canale di accesso al data lynk layer, ma **non definisce un LLC! (logical link control)**
Ambedue sono implementate via hardware, sono racchiuse all'interno dei circuiti delle interfacce.
Ci sono 18 tipi di ethernet..

Il formato del frame Ethernet e IEEE 802,3: La suddivisione del frame ethernet e IEEE 802,3 si articola nel seguente modo:
Preamble: la parte iniziale, L'alternanza di 0,1, dice alla stazione ricevente **che si tratta di un frame ethernet o ethernet 802,3.** Il frame ethernet include un byte addizionale che è l'equivalente del campo del frame di partenza, (SOF),IEEE802.3.

Start Of Frame: Il delimiter 802.3 finisce con due "1" consecutivi che servono per sincronizzare la porzione di ricezione frame, su tutti i pc nella rete, SOF è una specifica esplicita in ethernet.
Destination and Source Addresses: L'indirizzo di destinazioen raggruppa informazioni del produttore (per i primi 3 bytes), può essere unicast, multicast, o broadcast (tutti i pc)
Type (Ethernet): Specifica il livello superiore che deve ricevere i dati quando il processo ethernet è completo. Lenght (IEEE 802.3) La lunghezza il numero di byte che sono permessi in questo campo.
Data (ethernet): dopo che il processo Phisical e link layer sono completi, i dati vengono spediti al livello superiore, che è identificato in questo campo.
Data IEEE 802,3: Dopo che il processo phsical e link sono completi i dati vengono spediti al livello superiore, e devono essere definiti entro questo campo, se i dati nel frame, sono insufficienti per occupare il frame per un minimo di 64byte, dei dati aggiuntivi sono aggiunti per occupare a pieno il frame.
Frame check sequence: E' il classico controllo degli errori, nel frame, si tratta di una sequenza di bit, particolare. Questa sequenza contiene 4 bytes, Viene fatto un conto in fase di invio frame e di ricezione così si può scoprire se il frame è danneggiato.

Ethernet MAC: Ethernet racchiude la condivisione **di media e BROADCASTING**, Il metodo di accesso CSMA\CD, utilizza ethernet per performare 3 funzioni:
Trasmettere e ricevere pacchetti, Decodificare i pacchetti e controllare se sono integri prima di farli passare a livello superiore, Rilevare errori, nei pacchetti sulla rete.
Nel Metodo d'accesso CSMA\CD, le periferiche di rete, con i dati da trasmettere, **prima ASCOLTANO poi eventualmente trasmetton**o.
Una periferica, prima di trasmettere, deve controllare se un'altra è occupata, Si controlla se ci sono altri segnali sulla rete, quando c'è via libera, si inizia a trasmettere. Mentre trasmettete la periferica ascolta, Esso deve rendersi conto se altre stazioni stanno trasmettendo i dati allo stesso tempo, Dopo aver finito di trasmettere, la periferica torna nel LISTENING MODE.
Ethernet **è in grado di rilevare la collisione** poiché in questo caso c'è un netto aumento della tensione. Le periferiche rilevano la collesione e smettono di trasmettere pe run po', poi riprendono. La periferica coivolga nella collisione è l'ultima che riprendere a trasmettere.
Nella ethernet tutte le periferiche possono vedersi attraverso il cavo (broadcasting). Tuttavia non tutte le periferiche della rete processano i dati. **Essi sono rivolti solo alla macchina che ha il MAC address e l'ip corrispondente**, questi dati vengono trasportati con il pacchetto.
Dopo che la periferica ha verificato MAC ed IP, effettua il controllo degli errori. Se si rilevano gli errori, il pacchetto è distrutto. La macchina di destinazione non notifica alla sorgente se il pacchetto è arrivato o meno. Ethernet è un sistema a ConnectionLESS.

I segnali ethernet: E' una via di mezzo fra tempo e dati, in uno stream di dati sul un MEDIA (cavo). Manchester encoding definisce uno 0 Come segnale ALTO per la prima metà del periodo, e basso per la seconda metà. Si definisce 1 come un segnale che è basso per la prima metà, del periodo ed alto per la seconda metà.
Ethernet è designato per trasmetter e ricevere segnali tramite un segmento che consiste in 4 FILI. Un paio per trasmettere ed un Paio per ricevere.

Ethernet 10BaseT media e Tipologie: Nella **tipologia a stella** un hub centrale connette tutte le macchine, Le comunicazioni delle macchine sono **POINT TO POINT**, il traffico passa attraverso un hub. L'hub riceve su una porta, quindi trasmette sulle altre porte, **Gli hub o multiport repeater sono chiamati anche CONCENTRATORS.** Gli hub passivi non rigenerano il segnale, mentre gli hub attivi sì. La star topology è facile da installare. Nella tipologia a stella, la gestione è molto semplice, ed è semplice capire i problemi. Se una macchina non va il resto della rete continua a funzionare, è assai facile aggiungere altre macchine alla rete.Lo svantaggio, L'hub rappresenta un punto singolo di FAILTURE, se salta quello la rete è giù.

TIE\EIA 568-A specifica gli orizontal cabling, o la tipologia utilizzata per orizzontal cabling. Può essere la star topology.Quì ci riferiamo alla tipologia di connettori che vanno all'armadio del cablaggio, per cui ogni sbocco è indipendnete e collega ad un pannello. Nel TIE\EIA la massima **lunghezza del cavo orizzontale è 90 Metri (dalla patch alla cassetta fili)**. La massima lunghezza delle patch cord all'uscita del connettore è 3 metri (dal pc alla patch). La massima lunghezza orizzontale del cavo che va ai connettori è 6 metri (dentro la cassetta fili).
Il totale è quindi 99 metri, per cui diciamo 100 metri:P Per la star topology ci sono delle distanze che vanno rispettate secondo lo standard 568-A, per esempio in un edificio di 200 metri tutta la superficie non deve essere occupata, Le distanze ad esempio da considerare sono quella MASSIMA del cavo che NON Deve superare i 100m altrimenti la dispersione impedisce alle macchine di interpretare il segnale che a loro arriva.
Se un cavo supporta una lunghezza molto estesa, in mezzo ad esso possiamo inserire anche periferiche che non amplificano il segnale, E' possibile usare ulteriori repeaters per estendere ulteriormente il cavo. In questo modo è pure possibile costruire una EXTEENDED star topology.

Le Nics: E' inserita nella scheda madre e **gestisce la connessione di rete**. Può essre designata come Ethernet Card, FDDI card o Token Ring Card. E' collegata al pc via seriale, parallela, richiede Indirizzi interni IRQ, e I\O per windows xx, Nella scelta di una scheda di rete, bisogna tener conto di: **Tipologia di Rete, Tipologia di Cavo, Tipo di System Bus**.

Funzioni Livello 2: Importanti funzioni del livello 2 sono. LLC(comunica al livello superiore), Framing (compone i frame con le informazioni di recapito), Naming (ha un mac identificatore), Media Access Control (struttura all'accesso al media), Signaling(segnali con altri transceivers).

I Bridge: Il bridge collega più segmenti di rete, eliminando il traffico superfluo, Divide i segmenti di rete, **basandosi sul MAC** address delle periferiche ed Elimina il Traffico sulla stessa rete. Non sono apparecchi compliacti. Analizzano i frame in arrivo e prendono la decisione basandosi sulle informazioni contenute nel frame, e forwardano il frame a destinazione.
i bridge servono per passare i pacchetti per esempio **tra una token ring ed una ethernet**
Ci sono 2 tipi di Bridges, Trasparent o Source Route.

Le operazione a livello2 dei Bridge: Il bridging avviene a livello 2, sul data link, controlla il flusso dei dati, controlla errori sulla trasmisisone datie reindirizzamenti sul media fisico. Il Bridge svolge questi compiti tramite diversi protocolli livello link, che indicano**. Controllo di Flusso, gestione errori, indirizzamento ed algoritmo**.
La **Trasparenza con il livello superiore** è il primo vantaggio del bridge. Il Bridge **NON RICHIEDE** di analizzare i dati del livello 3 poiché esso opera solo ed esclusivamente a livello2. I Bridge, filtrano il traffico solo Filtrando il traffico in base al MAC, non ai protocolli. I Bridge agiscono sul traffico **basandosi sul MAC** per cui possono AGEVOLMENTE dirottarlo su un altro segmento, si parla anche di traffico che rappresenta un livello network.
Per il filtraggio del traffico, **in base al mac address vengono costruite delle Tavole**, di tutti gli indirizzi MAC allocati, **nei segmenti direttamente connessi**.
Se un dato transita tramite il cavo, il bridge, **paragona l'indirizzo mac** del frame con quello nella propria Tabella.Se si vede che l'indirizzo mac appartiene ad una periferica sullo stesso segmento, ovviamente non viene forwardato, Se il frame appartiene ad una macchina con mac su un altro segmento, **il bridge lo trasporta all'altro segmento**. Il bridge **riduce drasticamente** il traffico eliminando quello in eccesso, una sorta di semaforo. I Bridges sono periferiche che possono essere usate per ridurre il collision domain, riducono il traffico in piccoli segmenti per cui eliminano il numero di pacchetti in collisione. Operano al livello 2 e **si riferiscono solo ed esclusivamente al mac address**. Il bridge lavora al meglio quando c'è un bASSO flusso di traffico, **Quando il flusso di traffico diventa eccessivo, il bridge, diventano un ostacolo** e rallentano la comunicazione.

Esiste un altro potenziale problema nell'utilizzo di un bridge. LE periferiche inviano **uno speciale pacchetto** nel momento in cui tentano di raggiungere una periferica sulla rete, ma **non ne conoscono la destinazione**. Quando avviene questo errore, la periferica sorgente, invia un Broadcast sulla rete verso tutti i pc. Da ciò ne deriva attenzione per tutte le periferiche. Il **bridge forwarda ciò**. Se vengono inviati **troppi broadcast**, il risultato può essere un **BROADCAST STORM**. Questo può causare dei TimeOut, Rallentamenti di traffico, e la rete può operare al di sotto delle accettabili performance.

Gli Switches: E' una tecnologia che **diminuisce la congesione** nelle reti Ethernet, **Reducendo il traffico ed incrementando la banda**, Spesso si sostituiscono agli hubs. Oggi tutte le periferiche di switching e routing, effettuano **2 operazioni basilari**: Switching Data Frames, il processo ricevuto riguarda un frame che transita su un MEDIA di entrata ed ESCE su un MEDIA di uscita. Maintenence of Switching Operations, Costruzione e mantenimento di tavole con MAC, e ricerca per esse. I router invece si occupano sia delle tavole fisiche che delle tavole dei servizi.
Utilizzano la TAVOLA DEI MAC per switchare i datagrams. Operano ad una velocità più alta rispetto ai bridge. C'è un'ottimizzazione notevole della banda. Lo switch può essere adattato al cablaggio esistente per cui rappresenta una grande soluzione.

Operazioni Livello2 switch: Gli switch **sono considerati bridge multiports** senza collision domain con possibilità di segmentazione. I dati sono analizzati a livello2, e transitano ad alta velocità, una velocità maggiore rispetto ai bridges. Il **frame entra direttamente** nello switch. Da ciò ne deriva bassa latenza ed alta velocità nelle prestazioni. Lo switching **aumenta la banda** disponibile sulla rete, **crea delle segmentazioni dedicate, virtuali**. E' chiamato **VIRTUAL CIRCUIT**. Viene creato quando necessario. Lo switching **riduce drasticamente il collision domain**, Tutte le periferiche connesse con lo switch **si definiscono entro un BROADCAST DOMAIN**. Anche gli switch si basano sul mac, come gli switch, per le periferiche e per regolare il traffico, Si avvia quindi il processo di micro segmentation.
Note: BROADCAST DOMAIN. Enable Dedicated Access, Support Multiple conversion at time, Enables dedicated Access.

Segmentazione delle Lan Ethernet: Ci sono diversi motivi per cui **conviene creare una segmentazione**. Il primo motivo **è isolare il traffico tramite Segmenti**, ed ottimizzare la banda creando quanto più piccoli collision domains, **Senza segmentazioni le lan gestiscono male il traffico** e viene a crearsi zona di collisione molto facilmente. **E' quindi possibile usare** routers, bridges, switches, per risolvere questo problema. Alcune periferiche, come ad esempio firewall possono danneggiare la rete. Si usa invece dei bridges per ridurre il collision domain. Si ha la possibiltà di estendere la rete e collegare macchine a distanza.
Gli switch supportano **il CUT-TRHOUGHT** switching, che riduce la latenza ed il ritardo sulla rete, mentre il bridge supporta il **Store and Forward Traffic switching**, **Lo switch riduce le collisioni ed incrementa la banda**, sul segmento di rete, Esso fornisce **Banda Dedicata** per ogni segmento. La **segmentazione By routers**, ha questi vantaggi ed altri. Ogni interfaccia sul router connette ad una rete separata, quindi l'inserimento di un router su una LAN, crea piccolissimi collision domain e broadcast domains. Questo accade perché i router **non fanno Broadcasting** a meno che essi non siano programmati per farlo. Router **può eseguire funzioni di Bridging e Switching**. Il router inoltre esegue path selection. Router può essere usato per connettere differenti cavi e differenti periferiche di rete e differenti tipologie di rete. La tipologia di funzionamento dei router è Ethernet, FDDI, Token ring. Può connettere le lan tramite vari protocolli, IPX, appletalk, ecc.ecc ed hanno connessioni seriali alle WAN.

Segmentazione BRIDGE, in un Collision Domain: Ethernet usa la segmentazione bridge, nel caso in cui ci siano molti utenti su un unico tratto di lan. Il bridge permette il passaggio solo dei dati

che hanno un mac corrispondente ad una macchina fuori dal segmento. Il bridge costruisce una tabella in cui sono memorizzati tutti i mac delle stazioni e **LA porta usata** per raggiungere le periferiche.I bridges sono diversi dai router xkè viaggiano a livello 2 e sono totalmente indipendenti dal livello3. I bridge passano i frame a livello 2, riguardanti o meno il livello 3. Essi sono trasparenti rispetto ad altre periferiche nella rete.
I Bridge incrementano la latenza del 10\30%. Il bridge effettua una comparazione CRC sul frame. Una periferica bridge è considerata Store and Forward device. Il tempo per eseguire queste operazioni genera comunque un ritardo e le prestazioni sulla rete ne risentono.

Segmentazione by Switch in un Collision Domain: La rete **che usa una tipologia Switches performa solo 2 nodi. Uno in entrata ed uno in uscita**. Sending node and receiver node. Tutta la bnada è disponibile per i dati, i 2 nodicondividono Xmegabit. Una switched lan è veloce ed efficiente, delle standard lan ethernet poiché l'uso della banda è più efficiente. Nelle switched lan l'implementazione della banda usata può avvicinarsi al 100%.. **Le reti ethernet tradizionali** sfruttano al massimo 30\40% della loro capacità..Questo è dovuto alla capacità di ethernet, soprattutto alla CSMA\CD. Se c'è **un eccesso della banda, aumentano le collisioni**. Lo scopo della lan è quello di diminuire la velocità per cui gli errori sono inferiori.

The purpose of LAN switching is to ease bandwidth shortages and network bottlenecks, such as that occurring between a group of PCs and a remote file server. A LAN switch is a high-speed multi-port bridge that has one port for each node, or segment, of the LAN. A switch segments a LAN into micro-segments, thereby creating collision free domains from one formerly larger collision domain.

Lo switch è basato **sullo standard ethernet**, Ogni nodo è connesso ad una delle porte dello switch, oppure ad un segmento che va ad una delle porte dello swtich. Questo crea una **connessione FULL BAND fra ogni nodo ed ogni segmento dello switc**h. Un computer è connesso direttamente ad uno switch ethernet, **rappresenta il suo collision domain** e l'accesso avviene a full band. Un frame entra nello switch e lì trova la sua destionation address. Lo switch a sua volta sa che cosa fare, **basandosi sulle informazioni contenute** nel frame. Se il frame deve andare in un pc su un altro segmento, **lo switch effettua l'operazione di SWITCHING** adeguata.

Segmentazione Router in un Collision Domain: Un router è **molto più avanzato** di un tipico Bridge, Il bridge è PASSIVO, è **trasparente per quanto riguarda il suo livello di rete**. Opera sul Data Link. Il router lavora al livello3 e basa le sue decisioni sul livello3. **Esso esamina la destinazione sulla sua tavola quindi calcola il routing** per la destinazione. Crea una **segmentazione di alto livello**, determina dove deve arrivare esattamente il pacchetto. Il router opera con un **alto livello di latenza perché compie molte più operazioni di un bridge**. Esamina i pacchetti per determinare il percorso della loro migliore destinazione. Questo processo **impiega tempo e latenza**

Teaching Topology: Contengono esempi di segmentazione, da Bridge, Switches e Routers. Molte periferiche circondano il router. Il bridge divide l'ethernet E1 in 2 segmenti. Il traffico è filtrato dal bridge, è ridotto il potenziale di collisione e la psychal estende il dominio di collisione.

Design of Networks

General Design: Bisogna tener conto innanzitutto della **tecnologia da utilizzare**. Bisogna progettare lo schema di rete da usare, per cui tutte **le periferiche di livello1**, eventualmente hub o switches. Successivamente bisogna pensare a ciò che **ci manca per il LIVELLO 2**, in tal caso è

possibile mettere switch per ridurre le collisioni. **Il livello3 infine** prevede l'applicazione dei routers per il processo di routing, e per altri compiti di gestione livello 3 che connettono lan a wan e viceversa.

Specifiche di Design: E' necessario pianificare **vari step**, per la realizzazione di una rete funzionale. E' necessario raggruppare varie informazioni; Orgranizzazione storica e corrente, Progetto di crescita, policies e procedure gestionali, sistemi dell'ufficio, persone che useranno la rete. Bisogna **identificare i problemi sui quali indirizzarsi**, Analizzare il necessario per il progetto, secondo i requisiti delle persone. Bisogna conisederare le risorse dell'organizzazione, Risorse HARDWARE, SOFTWARE e risorse Umane. Considerare quante persone sono necessarie e quanto training è necessario per la LAN. 1) Quante risorse necessarie sono disponibili?2) Quante di queste risorse Orientate o condivise? 3)Quante persone useranno la rete ? 4) Qual è lo skill delle persone che useranno la rete? 5) Come si comportao queste persone sui computer e sulle applicazioni?
Queste informazioni aiuteranno a fare un bilancio per la progettazione di una lan.

Il processo generale di Design: Il processo di design include varie figure: Designer(persona che apporta il design), Client (persona che richiede e paga il design), Users(persone che useranno il prodotto), Brainstorming(il generatore dell'idea creativa del design), Specification Developement(numeri che serviranno per capire se e quanto lavora bene la rete), Building and Testing(raggiungimento obiettivi cliente, e rispettare certi standard).
Il **Problem solving Cycle** ti permette di capire come risolvere un problema di design. Un processo che devi seguire per svolgere un design. Un modo usato dagli ingegneri per organizzare le proprie idee è applicare il **Problem Solving Matrix.** E' un elenco di procedure ed opzioni che è possibile seguire in fase di realizzazione rete.

Documentazione design di rete: Per creare un design di rete è necessario disporre di una certa documentazione: engineering journal logical topology physical topology cut sheets problem-solving matrices labeled outlets labeled cable runs summary of outlets and cable runs summary of devices, MAC addresses, and IP addresses

Bisogna standardizzare la documentazione del progetto con ANSI\EIA\TIA, OSI\IEC.

La cassetta dei cavi: Una decisione importante durante il design della rete è DOVE INSTALLARE la cassetta dei cavi. **Bisogna rispettare gli standard, Main Distribution Facility (MDF), e (IDF).** Infine bisogna sapere come progettare la propria rete, tener conto soprattutto degli effetti negativi che la corrente ALTERNATA può avere sulla rete.

La dimensione delle Cassetta-Cavi: Lo standard TIA\EIA-568 – A, specifica che il cavo orizzontale deve essere collegato in posizione centrale per quanto riguarda una topologia STAR, **Nel punto centrale bisogna posizionare la cassetta cavi, e qui bisogna installare il PATCH panel e l'hub**. La cassetta di cavi dev'essere abbastanza larga da accogliere l'occorrente ed anche future aggiunge. Naturalmente le dimensioni di questa cassetta variano in relazione alla dimensione della LAN. TIE\EIA 568 A prevede **una cassetta di fili per ogni 1000Metri quadrati di cavo, quando l'area servita eccede i 1000 metriquadri, e quando il cavo orizzontale supera i 90 metri.**

Specificazioni Ambientali: Bisogna seguire determinate specifiche ambientali, per posizionare la cassetta dei fili, Alimentazione supplementare, aria condizionata per caldo\freddo, postazione sicura da accessi non autorizzati, e devono essere applicabili misure di sicurezza. Poi considerando la scatola di cavi e l'ambiente bisogna concentrarsi su: Materiale del muro, Umidità, Temperatura, tipo di luce, Uscite di energia, Stanze ed equipaggiamento di accesso di sicurezza, Accesso al cablaggio.

Muri, pavimenti e soffitti: Se c'è una sola scatola di fili, in un edificio, o se la scatola di fili funge come MDF, **il pavimento** della stanza dove è situata questa scatola di fili**, deve supportare delle specifiche**. Deve supportare 4.8KPA, Se la scatola di fili serve come IDF, la porta deve supportare un carico di 2.4KPA. Quando possibile, si preferisce avere un aumento della pavimentazione, per poter alloggiare cavi, Si può avere un'intelaiatura scalare di circa 30.5 centimetri, per supportare tutti gli equipaggi proposti ed i cavi. Il tutto dev'essere accuratamente protetto dall'elettricità statica. **Se l'armadietto (il REC o come lo chiamano) fa anche da MDF** nell' edificio, allora il POP deve trovarsi nella stanza. In questo caso la pareti interne della stanza del POP, dietro il PBX, dovrebbe essere ricoperte dal pavimento al soffitto con 20mm di "plywood", con un minimo di 4.6 m di spazio tra le pareti (?) per le terminazioni e l'equipaggiamento. Poi, materiali antincendio dovrebbero essere usati nella costruzione degli armadietti (plywood, vernici ignifughe ecc). Le stanze non dovrebbero avere finti soffitti ('dropped' non lo so, 'a discesa', forse). Il non rispetto di queste regole crea una struttura insicura.

Temperatura ed umidità: La cassetta di cablaggio dovrebbe essere abbinata ad un impianto per mantenere la stanza a temperatura di circa **21 GRADI in piena operatività.** Non ci devono essere **TUBI d'acqua** che passano attraverso l'edificio,ad eccezione del sistema di spruzzatore anti incendio.**L'umidità deve mantenersi attorno al 30\50%.** Se non si segue queste specifiche, il materiale di ferro contenuto nel cablaggio UTP e STP.

Apparecchiatura D'illuminazione e sbocchi di alimentazione: Se c'è una sola scatola di cablaggio in un edificio o se essa funziona come MDF, ci devono essere, come minimo**, due uscite di corrente, dedicata, non switchabili, ognuna con un circuito separato**. Ci deve essere un'uscita di corrente, duplex, **ogni 1.8Metri**, nel muro, per ogni muro della stanza. Esse devono **essere posizionate a 150MM dal pavimento**. Dietro la porta deve esserci **un piccolo switch** che controlla l'illuminazione principale della stanza. L'illuminazione dev'essere utilizzata con installazioni particolari evitando di avvicinare troppo le luci Fluorescenti al passaggio dei cavi poiché potrebbero provocare interferenze..L'illuminazione richiesta, specifica un minimo di 500LX, ed il fissaggio della luce, deve essere installato ad almeno 2.6metri, sopra il pavimento.

Stanze ed equipaggiamento d'accesso: La porta della cassetta di fili deve essere larga almeno 9 metri ed apribile verso l'esterno, da permettere la facile

uscita dei lavoratori. L'uscita dev'essere situata all'esterno della porta ma permettere a chiunque si trova dentro, di uscire. Una bobina porta cablaggio può essere installata su un muro, provvisto di cardinature, Ci dev'essere uno strato di legno compensato fra il muro e gli agganci della bobina,

trd

Struttura del cablaggio orizzontale: possono essere necessari: Unshielded Twisted pair. Fibra ottica. Telecommunication outlet.
Sono permessi multi cable unit, secondo lo standard, TIE\EIA 568 A-3. La Grounding dev'essere applicabile, secondo lo standard ANSI\TIE\EIA-697, Un minimo di 2 Comunication OUTLET sono requisiti; la prima 100Ohm UTP, cat5e. Seconda 100Ohm utp 5e. Due fibre multimode 62,125-50,125. Un trasmission point, TP, è permesso. 50 Ohm coassiale e 150ohm STP non sono raccomandati per la prima installazione. Uscite addizionali sono consigliate. Il bridge non è permesso,
50,125 multimode è permesso in ansi\tie\eia 568b. iso\eic11801 è 120utp e 50,125 fibra ottica multimode. La definizione transition point, iso\eic 11801 e 568 a. include transizioni sotto-tappeto come ottimi punti di connessione. ISO 11801 è l'equivalente di orizzontal cross connect cablig. (HC), è anche chiamato Floor distributore (FD).
La prossimità di un cavo orizzontale può essere fonte di interferenze elettromagnetiche (EMI)

Accesso ai cavi e supporti: Se la cassetta di fili serve come MDF, tutti i cavi passano da essa.Se serve come IDF, Computer, stanze di comunicazione e pavimenti devono **essere protetti da un condotto di 10.2cm.** Anche il cablaggio dev'essere protetto. L'esatto ammontare di condotto necessario è determinato dal globale complessivo cavi che alloggeranno all'interno della scatola di cavi. Sarebbe opportuno creare un condotto con larghezza superiore al necessario in previsione di una crescita futura. Bisogna inoltre tenere dei condotti di riserva nell'armadio.
La cavetteria che va all-armadietto deve passare un sotto il pavimento. Se non possibile la cavetteria **deve esser fatta passare in manicotti di 10.2cm** sopra il livello ella porta. Il cavo deve esser fatto passare dal manicotto su {ladder [la scala, rack non so}. Se usata in questo il ladder rack dovrebbe essere installato in una configurazione che supporta l-equipaggiamento.

Infine, ogni apertura sul soffitto deve essere sigillata con materiali **che ritardano gli incendi**

Tipologia del pavimento base: Secondo lo standard TIE\IEA 568 A, nella tipologia a stella, un hub centrale collega tutte le periferiche .Quì è situata anche la cassetta di cavi. Per calcolare la posizione esatta di questa cassetta di fili, **bisogna disegnare una FLOOR PLAN-**
I potenziali posti dove **alloggiare una cassetta di fili** sono luoghi asciutti, al riparo dalla luce e dalle intemperie, che possono conettersi con l'edificio facilmente, disponibili verso vie di accesso alla struttura.
Dopo aver **disegnato il FLOOR PLAN**, il passo successivo è determinare quante cassette di fili ci dovrano essere nella rete. **Si traccia un cerchio sulla superficie della pianta, il cui raggio dev'essere di 50 metri**. Al di là di questa distanza è necessario, il più delle volte, inserire altre cassette di fili.
Il percorso massimo per un UTP è90 metri ma considerando le curve di un edificio si pianifica una distanza di 50 metri
Oltre questa si inserisce un hub o altro per rigenerare la distanza.

Specifiche dell'MDF: **Mdf è generalmente situato**, in una struttura a più piani, **AL piano INTERMEDIO**. (armadio centrale). IDF **invece, è l'armadio che sta su ogni piano**, **E' utilizzato un cavo backbone per connettere MDF e IDF**. Gli orizzontal cabling,escono da essi.
In grandi reti è possibile connettere più IDF a un MDF e POP, tramite bakbone. Dall'MDF e pop, parte un altro BACKBONE che collega altre reti o internet.
IL BACKBONE è definito anche VERTICAL CABLING. Ed ha i seguenti requisiti. Backbone Cabling, principali ed intermediati cross connettori, terminazioni meccaniche, patch cords usate per connessioni backbone to backbone, Media di networking verticale fra le varie wirin closet, Networking media fra l'MDF ed il POP. E' usato per connettere multi edifici o campeggi.
Come componenti di backbone, possono essere usati: 100OHM UTP (4pair), 150OHM STPA (150OHM), 62.5,125Multimode fibraottica, SingleMODE fibra ottika.
Lo standard TIE\IEA 568 A non raccomanda il 50OHM coassiale per nuove installazioni. Molte installazioni usano il 62,5\125 Multimode fiber optipcal.

SE la distanza fra l'HORIZZONTAL cross connect e idf (ICC) è inferiore al massimo consentito, LA distanza fra ICC e MC può essere INCREMENTATA. L'importante è ke la distanza globale non ecceda le specifiche.

La terra deve rispettare gli standard relativi ad ANSA\TIE\EIA 607, il collegamento fra le varie periferiche deve rispettare uno schema di eXTENDED STAR topology.

Nella IDF La lunghezza della PATCH cord e jumpers è limitata a 20metri, nella MMC la patch cord è limitata a 20 metri.

Requisiti TIE\EIA 568 A per il cablaggio BACKBONE: Quando è necessaria più di una wiring closet si usa la extended star topology ma per motivi pratici spesso si usa anche la HIERARCHAL TOPOLOGY.
Nella extended star topology ci sono 2 modi per connettere idf con mdf. **Il primo modo è connettere IDF direttamente a MDF**. siccome l'IDF è dove la cablatura orizzontale si connette al pannello dell'armadietto, la cui connessione principale connette all'hub nell'MDF, l'IDF è talvolta detto HCC (orizzontal cross connnect). MDF ha un cablaggio che va direttamente ad internet, di solito e si chiama MCC. **Nel secondo caso**, si conette **il primo IDF ad un altro IDF, quindi all'MDF**. Da idf a idf si usa un orizzontal cross cabiling (HCC) e dall'ultimo idf a MDF si usa IIC intermediate cross cabiling ed il connettore con MDF è detto MAIN CROSS CONNECT.
Per impedire eventuali errori, lo stard TIA\EIA 568 A non prevede più di un ICC (intermedio) per arrivare a MDF.

Massime distanze per un BackBone: La massima distanza per un cavo varia da un tipo di cavo ad un altro. Solitamente **si usa un Single mode** fibra ottica, per cui la connesione dall'ulimo HCC a MDF può essere di 3000 METRI. HCC-MCC =3000Metri. HCC-ICC \ ICC-MCC, la distanza è 3000 metri e può essere splittata. Esempio. Da hcc-icc500 metri, icc-mmc 2500 metri.
HCC-MCC=2000metri. HCC-ICC=500 metri ICC-MMC=1500 metri. (distanze consigliate).

Differenza fra Corrente Continua ad Alternata: La corrente alternata rispetto alla continua ha la capacità di invertire di polarità, in base al principio della calamita, si nota che con una inversione della polarità è possibile creare MOVIMENTO. All'inizio c'è una polarità che obbliga 1 tipo di movimento, il cambio di tensione completa la ROTAZIONE.
Una povera connessione provoca dei problemi per cui il segnale trasmesso può essere difficilmente interpretato.

ESD è l'electrstatic discarge può essere una soluzione per questo. **ESDs è il fenomeno per cui, con l'umidità si hanno dello shock** i cui effetti possono essere disastrosi, per le apparecchiature elettroniche..
ESD è un buon Grounding.
Equipaggiamenti di terra per prese di corrente: E' richiesto un circuito completo per controllare il circolo di corrente fra il positivo ed il negativo, Il metallo garantisce il circolo della corrente con una resistenza molto bassa, Plastica e vetro, invece, hanno una resistenza molto alta. Sono usati per prevenire lo shock e per interrompere circuiti. Una resistenza può fornire il supporto di terra necessario per scaricare la corrente elettrostatica. **Il GFCIs *Ground Fault Circuit Interrupters* fornisce la protezione necessaria** per eventuali danni da corrente elettrostatica.
Interrompe automaticamente i circuiti, riduce il campo dei danni dello shock elettrico; Gli **UPS uninterruped power supplies garantiscono corrente continuata per protezione** di apparecchiature informatiche.
Si collega la terra alle parti metalliche del computer per fare in modo che correnti estranee possano provocare degli SHOCK colpevoli di danneggiare le apparecchiature.
Un esempio, una periferica all'interno del pc, ha una connessione accidentale; Il suo cavo Caldo viene a contatto con il case del pc. Se la terra è connessa alla periferica, può esistere un bilanciamento della tensione per cui, essa serve come resistenza negativa, ed è sufficiente a prevenire la costituzione di una corrente elettrica ANOMALA.

Problemi di SICUREZZA di TERRA: Si dovrebbe sempre , per impianti di rete su vari edifici, **usare impianti di terra separati** per le varie apparecchiature informatiche. Sfortunatamente si usa quasi sempre lo stesso impianto di terra. Ci sono comunque **vari svantaggi** nel separare i 2 impianti di terra. Quando **le terre stanno in luoghi separati, hanno separato potenziale**. Per cui il loro contatto può dare luogo a grossi squilibri di tenzione.
Per 2 pc che hanno una messa a terra separata con diverso potenziale c'è il pericolo di uno shock, in questo caso è necessario adottore **ONE HAND RULE**, toccando il pc con una sola mano, si evita ogni shock.
Secondo gli accordi internazioni relativi agli standards IEEE, **non deve esistere alcuna differenza di voltaggio** fra il CASE del pc e la periferica di rete, le conseguenze possono essere degli shock e dei problemi a livello globale. Se ad esempio si tocca con una mano il case e con una mano la scheda di rete si ha uno schock..
Gli standard TIE\EIA 568 A possono essere usate bene le fibre ottiche quanto i cavi utp, il vetro è isolato elettricamente e **non permette l'afflusso di corrente**, l'elettricità non viaggia sulle fibre ottiche, per cui è preferibile, per edifici non cablati, usare fibre ottiche come BACKBONE.
Si raccomanda di **installare fibre ottiche per connettere Wiring Closet su diversi soffitti**,ancora meglio in edifici separati. Differenti messe a terra possono creare diversità di potenziale. **Le fibre ottiche eliminano il problema perché non conducono elettricità.**
Si raccomanda di installare fibre perché il cavo utp di metallo, che conduce elettricità, può ripetere un problema che si verifica in 1 edificio, anche per gli edifici comunicanti. Creando così un MULTI-PROBLEMA Elettrico. Le fibre ottiche non comportano questi disagi.

Problemi di Alimentazione: In un cavo ci sono vari fili, se esiste un problema elettrico ad un filo, questo può essere facilmente debellato. Se il problema interessa il polo caldo ed il neutral, si parla di **Normal Mode Problem**, se il problema interessa il caldo, il neutral e la terra, si parla di **Common Mode Problem**. I normal mode problem, sono i più comuni, e **solitamente non danno dei problemi**, che si riflettono sul pc o sull'uomo;Vengono corretti direttamente dallo stabilizzatore di alimentazione. Invece i Common Mode problem, va ad ainteressare direttamente il case del computer, per cui **possono provocare dei notevoli danni**.

Problemi Tipici di Linea Alimentazione: I tipici disturbi che derivano da problemi di alimentazione, possono essere..SURGES, SAGS, SPIKES e OSCILLATIONS. Un altro problema può essere la perdita totale di alimentazione. SURGE: E' una **Perdita di voltaggio**, che si verifica per **un tempo che va da 2 secondi a 2 minuti**.. Può esistere anche di 100 volts, un'apparecchiatura che funziona a 220v può scendere a 100v, per cui si danneggiano le apparecchiature; **Gli hubs sono particolarmente sensibili** a questo fenomeno, possono subire dei gravi danni. SAG\BROWNOUT: E' una **perdita** di voltaggio, anche dell'80%,**dura meno di 1 secondo**.Si possono verificare a causa di sovrccarichi di circuiti, sono la causa della maggior parte dei problemi di alimentazione sulle periferiche di rete. SPIKE: Sovraccarico di corrente, dura da 3 a 100millisecondi, quando accade uno spikes la linea elettrica raggiunge tensioni di almeno 240v. OSCILLATION\NOISE: Viene a crearsi un antenna effect. Le oscillazioni sono derivate da armonici o disturbi.
Ciò che CAUSA gli spike ed i surge, **è comunemente causata da fulmini**. La corrente del fulmine può affiancarsia quella in circolo per cui si verificano alte tensioni. E' anche possibile generare spikes e surges artificialmente tramite switches che regolano la tensione.
Il danno può verificarsi in apparecchiature elettriche ed elettroniche, comprese ovviamente le apparecchiature di rete, Possono esserci severe conseguenze a seguito di spikes e surge, **perdita di memoria, isolamento**, **problemi nel leggere i dati, dati alterati, garbling.**
Le protezioni, possono essere un valido aiuto per combattere i danni derivati dal diretto contatto con discariche elettrostatiche o fulmini. **LA primaria protezione**, per edifici e persone, è situata nell'edificio stesso, la protezione per le apparecchiature elettriche, funziona nel seguente modo; Quando si verifica un altissimo voltaggio sul cavo, esso, viene SCARICATO A TERRA, Se la protezione non effettua questa operazione abbastanza velocemente, questa si rivela non abbastanza efficace da proteggere le apparecchiature.
La Seconda protezione, installata dietro la prima protezione, Stoppa le correnti che passano attraverso la prima protezione, ed evita il danno all'apparecchiatura.
Per proteggere l'apparecchiatura installare un surge protector, tra l'entrata di corrente all'edificio ed il sistema.Puoi anche installare fra il Sistema e l'area di lavoro, una protezione..
Puoi anche usare il LEC (Local Excnahge Caarier) collegarlo fra il backbone e l'aria d'ufficio.
Una soluzione comune può essere una **SURGE REPRESSOR**. Quando una scarica di corrente si abbatte su un'apparecchiature, il SURGE REPRESSOR la dirotta verso Terra. E' anche vero che **un'errata installazione del surge repressor può aumentare** le probabilità di problemi elettrici; AD esempio se l'equipaggiamento non è propriamente messo a terra, quando il surge devia la scarica a terra, viene aumentato il potenziale di terra. LA risultante DIFFERENZA di potenziale può creare delle tensioni che invadono il circuito di terra, questo flusso di corrente può danneggiare apparecchiarture non protette. E' buona regola proteggere tutte le apparecchiature con un Surge Suppressor, SE il pc è collegato **ad una linea telefonica**, anch'essa **dev'essere protetta.** Le linee telefoniche sono vulnerabili agli spikes. Quando un fulmine colpisce delle linee telefoniche, le apparecchiature non protette vengono distrutte. Come ruolo generale, si considera l'apparecchiatura telefonica, parte di rete. Se vuoi proteggere bene la tua rete devi pensare **anche alla linea telefonica**. Se il surge suppressor può risolvere problemi dovuti a SPIKES e SURGES, **può NON ESSERE utile contro i BrownOuts**. A volte una totale assenza di corrente improvvisa può provocare devastazione ai dati. Quando ad esempio si copiano o si uploadano dei files e manca la corrente, questi file possono andar persi.
Con l'UPS puoi avere una corrente continuata per cui proteggere il sistema da BROWN OUTS. Il solo modo, invece, per poter **azzerare le oscillazioni è il re-cablaggio**. (rewire). Sebbene possa sembrare una soluzione estreme e costosa, è il modo più affidabile per assicurare connessioni al suolo sicure (direct power da interpretare).

Installazione e specifiche Surge suppressor: Il surge suppressor normalmente è installato su muri, Questa periferica è anche chiamata **Metal Oxide Varistor** (MOV), ed è usata come surge suppressor. Ha la possibilità di assorbire controllare correnti di vario voltaggio, dai 120 volts ai

330volts.. Sfortunatamente il MOV non è la miglior soluzione per proteggere le apparecchiature di rete; Questo perchè "la terra" serve come punto di riferimento comune per i segnali di dati in entrata e in uscita dal computer. Lo scaricamento di voltaggio in eccesso nella linea di alimentazione, vicino al PC può creare problemi.
Anche se questo tipo di voltaggio può evitare danni all'alimentazione, può avere come effetto dei dati corrotti. Se è collegato alla stessa terra, può **provocare differenza di potenziale** alle apparecchiature della rete, Può, a seguito di ciò verificarsi una perdita di dati o danno del circuito. Questo apparecchio ha una vita l'imitata. Dipende dal calore al quale è sottoposto e dall'uso. Per tutti questi motivi **questo tipo di SURGE SUPPRESSOR non è la migliore soluzione** per la rete.
Per risolvere questi problemi, è possibile installare un **surge suppressor di qualità** (anziché installare un surge suppressor per ogni workstation). Essi dovrebbero essere situati in prossimità di prese di alimentazione, anziché vicino alle stesse apparecchiature di networking. Mettendo un **SURGE SUPPRESSOR** di qualità, vicino ad ogni presa di corrente, lontano da apparecchiature di networking, si hanno risultati migliori.

La soluzione UPS: Grazie agli UPS, **uninterruptible power supplies**. Per installare un ups, bisogna vedere quanta corrente serve, quanto è il budget di spesa, e qual è il consumo delle apprecchie che si vuole collegare. Bisogna collegare a questi ups, switch,hub, router, **ed ogni periferica necessita alimentazione**. Un ups può aumentare la rete **per poco tempo** perché si pensa che in caso di black out, basti poco per tenere in piedi l'intera rete elettrica, **se si necessita più tempo** per tenere su le periferiche, è consigliabile **usare un GENERATOR**.
Le componenti di un ups sono. Carica battaria, Batteria ed Inverter.
Possono esistere **Continuos UPS o Switched UPS**. Nei continuos la batteria è Sempre collegata. Negli switched quando il voltaggio cade, si usa la batteria. I vari UPS si differenziano dal Tipo di Batteria, LA potenza dell'inverter, lo schema operativo..

Operazioni di funzionamento UPS: Come da proprio ruolo, un sistema UPS, offre molte possibiità a basso costo, è usato per mettere i sistemi in stand by. Essi **monitorizzano la linea di alimentazione**, Quando c'è un problema, **l'ups entra in azione con l'inverter**, e prende alimentazione dalle proprie batterie. Qando entra in azione questa procedura si parla di **TRANSFER TIME**. Questo periodo è molto breve, fino a quanto le batterie non sono esaurite. I moderni computer non hanno di questi problemi, possono restare molto accesi, almeno 1000millisecondi..**Le periferiche UPS che offrono molte possibiità** costano di più, **ed operano tipicamente online**. Questo consente di **operare COSTANTEMENTE con INVERTER**, che è alimentato dalle proprie batterie.Le batterie continuano sempre a caricarsi dalla corrente ed a trasmettere corrente all'inverter. Il funzionamento è a **CORRENTE Alternata(AC)** per cui si eliminano problemi di SPIKES, questo tipo di ups riduce il tempo di trasferimento necessario a ZERO. **Altri ups rientrano nella categoria ibrida**. Mentre possono apparire sempre online, essi non utilizzano sempre l'inverter, **Un buon ups comunica al pc quando le proprie batterie si stanno scaricando** così esso compie le operazioni di SHUTDOWN necessarie per salvagardare tutti i dati.

Procedure di sicurezza per installazione Rete: Il processo di installazione di un arte richiede **costanti procedure di sicurezza**. Devi considerare le condutture elettriche, lavori effettuati da elettricisti e costruttori di edifici. Elettricità: Non lavorare mai su una periferica elettrica mentre la **linea di corrente è collegata**, NON lavorare mai su una periferica elettrica **mentre il case è aperto e la linea di corrente è collegata**. Testa i connettori elettrici con il voltometro o tester,Localizza tutte le ocondutture elettriche ed i cavi di alimentazione prima di installare un cavo di rete. Devi **mettere a terra** tutti gli equipaggiamenti di rete. Costruzione: Usa dei vetri di sicurezza ogni qual

volta ti trovi a lavorare o tagliare lame. Misura attentamente prima di tagliare o forare permanentemente materiali da costruzione. MISURA prima, Tagilia dopo. (OSHA=Occupational Safety and Healt Administration).

Documentazione di rete: I tuoi progetti di strutturazione cablaggi saranno completi, a richiesta del cliente che ti chiederà di strutturare una stanza o un'edificio. LA tua responsabilità, come designer, consiste nella **SCRITTURA della DOCUMENTAZIONE**, Questo includerà tutti i vari accertamenti, la progressione del lavoro, il report finale ed i test. **Il tuo primo obiettivo** come designer di rete, sarà quello di avere in mano la specificazione del cliente, la spesa che questa persona dovrà affrontare per il progetto. La documentazione iniziale richiesta, sarà: Il giornale ingeneristico, la topologia logica, topologia fisica, la matrice di risoluzione dei prblemi, rivestimento delle uscite, rivestimento dei cavi passanti, il sommario di queste 2 cose, ed il sommario delle periferiche con MAC ed indirizzo ip. Questo, in relazione agli standard ANSI\TIA\EIA e ISO\IEC. **Un metodo efficiente** per lavorare in una rete con **un team di installazione**, è **dividere il team** in piccoli gruppi che consistono in 1 o più persone. Occasionalmente alternerai il lavoro con altri membri, ed avrai la possibiità di compiere un'incredibile varietà di operazioni. Ecco le formazioni dei gruppi, nell'intera squadra. Project Manager, procedure di sicurezza,documentazioni,specifiche su altri membri della squadra, comunicazioni con istruttore. Materials and tool manager: responsabile dei tool, cavi e tester. Cable runner: il responsabile della pianificazione e cablatura, sicurezza dei cavi, e specifiche per il test dei cavi, Jack and patch panel terminator: Responsabile per garantire la qualità dei jack durante l'installazione.

Flusso di lavoro: Per essere sicuro che il progretto vada a buon file**, è necessario creare un FLOWCHART**. Il FLOWCHART deve includere **ogni fase del lavoro**, deve essere completo ogni azione dev'essere orinata CRONOLOGICAMENTE **secondo una linea del tempo**. Deve includere i seguenti TASKS: Installazione uscite, installazione jacks, passaggio di cavi, inserimento dei cavi nei pannelli patch, testing dei cavi, documentazione dei cavi, installazione schede di rete, installazione hub, switch, bridge e routers, configurazione routers, installazione e configurazione pc.. Per quanto riguarda la strutturazione dei cavi, si può anche non seguire tutti questi task, a discrezione della particolarità del progetto.

Schedulazione materiali per il progetto: Per costruire una rete è necessario **utilizzare una varietà di materiali, qindi si usa anche vari strumenti per effettuare la costruzione** di materiali e componenti, Necessiteremo di diversi materiali, per iniziare il progetto ed ALTRI, quando il progetto sarà già partito e starà progredendo. Ad esempio: Data e tempo che verrà richiesto per la costruzione, strumenti usati, fornitori, specifiche sulla costruzione materiali di rete. **Secondo gli standard TIA\EIA 568-A**, abbiamo imparato che un computer si connette ad una Uscita tramite un horizzontal cross-connect, si utilizzano i jack a muro, ed un cavo Categoria 5, collegato ai jack. TIA\EIA 568-a specifica che nello schema di cablatura orizzontale, tu puoi usare **il jack RJ-45 per effettuare la connessione ad un cavo categoria5** che poi va all'uscita. Su un lato**, il cavo RJ45 contine 8 COLORI** corrispondendi a degli slots. Il filo individuale, all'interno del cavo cat5 viene inserito in uno di questi slot, relativamente al colore. **L'altro lato del jackrj45, è Femmina,** come un normale cavo telefonico, ad ecccezione delle dimensioni.

Il cavo di rete è più grande ed ha 8 PINS. La telecomunication outleet è creata secondo uno schema di cablatura orizzontale, è di solito installata sul miro. TIE\EIA 568-A, specifica due tipo di montaggi a muro che puoi usare per **inserire il jack-rj45 a muro**. **Il SURFACE MOUNT, e il FLUSH MOUNT.** Ci sono **2 TIPI** DI BOX che si può usare per il **surface mount** dell'rj45 al muro. Il primo è un **Box con montaggio a VITI**. Il secondo tipo di box che si può usare è il Box con **montaggio Adesivo**. Se si sceglie questo metodo, bisogna considerare che una volta installato il box, questo non può essere rimosso. Nel primo caso invece basta svitare le viti. Prima dell'installazione, è necessario: Scegliere il luogo giusto per rj45, Far passare il cavo, dentro il miro o sulla superficie tramite una canaletta, montare il box nella desiderata locazione, far passare il cavo all'interno del box, passare il cavo nel jackRJ45, Inserire l'rj45 nella FACEPLATE, dopo la faceplace nel box.

Molti installatori **preferiscono usare il montaggio superficiale dell'Rj45** jack perchè è **facile** da installare. Non devi bucare il muro, devi semplicemente montare il jack sulla superficiale del muro, questo metodo è anche veloce da eseguire. Per quanto riguarda il casto questa è un'importante considerazione. Il montaggio superficiale **spesso è l'unica scelta disponibile** in molte situazioni.

Fattori da considerare dopo aver montanto RJ45: Devi considerare **numerosi fattori** prima di decidere di effettuare un montaggio di un RJ45 Flush nel muro. **Per esempio le tecniche** che usi per tagliare **dentro il muro** sono diverse da quelle che usi per tagliare **l'intonaco**, è importante determinare prima il tipo di muro con il quale bisognerà lavorare. L'intanoco è un materiale con cui è difficile lavorare perché si sgretola facilmente. Quindi non è sempre possibile inserire saldamente delle viti. In questo caso è necessario installare un connettore **jack superficialmente**. Se ci sono dei battiscopa sul muro, tu puoi decidere di installare le prese per i jack qui, perché il legno è un materiale molto solito, più solido dello stesso muro. Se deciderai di mettere la presa jack nel battiscopa,., prima dovrai **scavare una parte di legno per 5CM** sulla superficiel del battiscopa. Il sottostrato di muro bloccherà l'inserimento del jack per cui non bisogna andare troppo a fondo. E' necessario non interferire porte e finestre, limitarsi quindi ad installare il tutto, attorno ad esse. Inine l'ultimo step è determinare se il jack andrà montato in un box o in un bracket a basso voltaggio.

Montaggio di un BOX a muro: Dopo che hai preparato l'apertura nella quale posizionare il jack, potrai inserire esso nel muro. Se stai usando un box per montare il jack, prendi il cavi e fallo passare dentro uno slot, all'interno del box, quindi premi il tutto verso l'apertura nel muro. Usa le viti per assicurare il tutto al muro, Se stai montando un jack dentro un mounting Braket a basso voltaggio, inserisci ancora il Bracket nell'apertura del muro. la faccia lisia verso l'esterno. Premi i bordi superiori e inferiori all'indietro, cosìcchè il supporto si attacca al muro. Poi spingi un lato verso l'alto e l'altro verso il basso, per montare il supporto in modo sicuro. Per montare un box nell'intonaco è necessario scartare l'intonaco così da vedere la parte sottostante, in legno, dopo di che, fare 2 buchi, e prendere le misure, scavare quindi con una lama, una figura geometrica tanto grande da permettere al box di alloggiare. Inserire il box, dopo di che, fissare il tutto con delle viti.

Inserimento dei cavi nel jack: La performance, in una rete è strettamente legata alla qualià delle connessioni. Quando si usa **un jack rj45**, in uno schema di comunicazioni orizzontali, la sequenza di fili è tanto critica da influire molto sulle **peroformance** della rete. Sequencing si riferisce al processo di abbinamento dei cavi ai propri terminali sul jack. Per capire come questo

lavora, esaminiamo un jack rj45 più da vicino. NOTATE che il **rj45 è codato con 4 colori**.(4 per lato, totale 8 FILI) I colori, BLU, verde, arancio e nero, corrispondono ai colore dei fili all'interno del cavo categoria 5. **Per pressare i cavi dentro il jack** tu devi usare un tool. Il tool è una device che utilizza un'azzione di carica premendo i cavi tramite una pinza metallica. Mentre preme, taglia la parte restante dei cavi (la parte inutile). Questo garantisce che il cavo abbia una buona connessione. Quando usi un **Punch Tool**, devi iniziare a posizionare la lama all'esterno del jack. Se posizioni la lama all'interno del jack tu taglierai i cavi ad una distanza troppo corta dal contatto. In tal caso, può non esserci alcuna connessione elettrica. Dopo aver collegato i cavi, è necesario prendere il jck, girarlo dal lato inferiore e chiuderlo con l'apposito coperchio. Dopo il montaggio è necessario far passare il cavo in eccesso tramite degli spiragli così da inserirlo all'interno del muro.

Installazione del cavo UTP: Per connettere i cavi ai jack seguire le seguenti procedure:1) **Sbuccia i cavi,** in piccola parte, maggiore è la parte di metallo esposta, maggiore è la perdita di segnale. 2) Assicurarsi che i cavi **si mantengono suddivisi a coppie**, il più possibile, fino a raggiungere il punto di terminazione. Questo è un tipo di cavo che produce cancellazione, per la categoria 4 utp il massimo consentito, in termini di vicinanza è 25mm, per i cavi a categoria 5utp la distanza massima per il cancellamento è 13mm. 3) Se durante il percorso del cavo deve avvenire una rotazione, assicurarsi che questa **non superi MAI i 90 Gradi**. 4) Si dovrebbe evitare di **TIRARE il cavo con una forza maggiore a 11.3 kg**. Le fibre interne potrebbero SFIBRARSI e generare CROSSTALK 5) Se cavi multipli devono passare per **lo stesso percorso**, **utilizzare delle fascette**, posizionarle ad intervalli casuali senza stringerle troppo. Questo può danneggiare il cablaggio. 6) Cercare di **minimizzare la torsione del cavo**. La torsione comporta diminuzione della banda e calo di prestazioni sulla rete. 7) In fase di determinazione della quantità del **cavo che dovrà essere utilizzati, è sempre meglio essere più "GENEROSI**"; Alcuni cavi, non devono tirare troppo per cui è richiesta una ulteriore estensione di 60\90cm, per tale motivo è meglio avere un cavo più lungo del previsto, in generale è sempre meglio avere un paio di metri in più di cavo. 8) Quando si assicurano i cavi **utilizzare le appropriate e raccomandate tecniche per utilizzo** di cavi sicuri, Barre di supporto cavi, Pannelli segmentati, e supporti di connessione in velcro. Mai usare delle Graffe, possono forare il cavo e creare perdita di connessione.

Documentazione del cablaggio: Quando si installano dei cavi, è importante **documentare le proprie azioni**. Tu puoi fare questo usato un voglio di caarta nel luogo dove instalera i cavi, in questo voglio ci dovrà essere uno schema, **una sorta di diagramma** che mostra la posizione dove i cavi sono passati. Più tardi tu puoi riferirti a questo foglio di carta per **piazzare i numeri corrispondenti alle uscite di telecomunicazione ed ai pennelli patch nella cassetta-fili**. Tu puoi usare una pagina, nel tuo giornale per documentare il passaggio dei cavi, tu dovrai avere uno strato addizionale di documentazione per ogni installazione di cavi. **Lo standard TIE\EIA-606, specifica che ogni unità di terminazione hardware ha un identificativo**. Questo identificativo è marcato **su ogni unità di terminaziona hardware, o sulla sua etichetta**. Quando gli identificatori vengono usati in zone di lavoro, i terminatori devono avere un'etichetta sulla facciata. Questa etichetta **può essere inseribile o adesiva**. Deve essere leggibile, indistruttibile, e l'adesibilità richiesta dev'essere specificata nel UL969.

Tipi di Etichette: Spesso sui cavi e sulle uscite di telecomunicazioni e sui pannelli patch c'è **un'etichetta con la scritta MR ZIMMERMAN** MATHclass o MR THOME'S ART class. Questo **può creare confusione**, per cui negli anni successsivi a quelli **non sono stati più usati nomi di persone**,Molti amministratori di rete, hanno incorporato il numero delle stanze nelle informazioni di liveli. Essi assiengavano lettere ad ogni cavo **in relazione alla stanza**. Molti sistemi di etichettatura, particolarmente usati il reti molto grandi, incorporavano anche codifica di colore. Per esempio un'etichetta blu identifica una cablatura orizzontale mentre una etichetta verde può identificare un cablaggio che va all'area di lavoro. Per capire come funziona, immagina che 4 cavi hanno da passare 1012 stanze. Sul foglio di carrta questi cavi saranno etichettati come 1012°, 1012B, 1012C, e 1012D. Tu puoi anche **etichettare ogni connessione al patch panel**. Si deve piazzare le etichette con un certo ordine, numerate in ordine crescente, così da facilitare la **diagnosi e l'ubicazione dei problemi**, se dovessero, in futuro, accadere. E' consigliabile etichettare direttamente anche i connettori oltre al cablaggio in generale, L'etichettatura, in ordine crescente, deve riguardare cavi e connettori. Così da risolvere futuri problemi, in caso dovessero presentarsi.

Preparazione cavo per Routing ed etichettatura: Per passare i cavi occorre tempo, se si considera il passaggio di 4 cavi, si può pensare ad un vantaggio nel momento in cui si passano **tutti e 4 i cavi allo stesso** tempo piuttosto che passarne 1 alla volta. Si necessita di un **GOMITOLO di cavi**, ogni gomitolo dovrà essere approssimativamente di 304.8 metri. Il cavo viene fornito all'interno di una scatola, dalla quale non va mai separato. **MAI riavvolgere il cavo**. Se si prova a riavvolgere il cavo, **questo subirà una torsione**. Anche qui serve una documentazione per cui per aiutarsi è necessario assegnare un foglio di carta con relativa documentazione a questo gomitolo di cavo. Per aiutarsi a passare e documentare il cavo, è necessario, come sempre, **assegnare delle etichette progressive allo stesso cavo**. Bisogna usare un Marcatore permanente, resistente all'acqua. In questo caso, i cavi sono 4 per cui, 1012-A,1012-B,1012-C,1012-D. Il cavo andrà marcato per 3 volte, assicurarsi che non sia tirato, legarlo con delle fascette, in modo che non stringano troppo.

Etichettatura del Cablaggio: Dopo aver fatto passare il cavo lungo il percorso scelto precedentemente, portarlo nella stanza, Permettere abbastaza lunghezza **da far raggiungere al cavo, tutti i jack** della stanza, estendere altri 60\90 cm di cavo in più, per questo. Tornare indietro e raggiungere il gomitolo, utilizzare il classico foglio di Documentazione e marcare il cavo**. Non tagiare il cavo senza prima avergli assegnato un'etichetta**. Per i migliori risultati, tagliare il cavo, con una cesoia particolare, questo creerà un taglio netto senza perdite di segnale né rischio di rovinare il cavo stesso. Dopo aver seguito queste istruzioni, l'horizzontal cable **va marcato sia all'inizio che alla fine.**

Procedure semplici per far passare il cavo: Il modo più facile per far passare un cavo è essenzialmente **farlo passare sopra un muro**. Solitamente questo metodo va usato solo in situazioni dove siamo sicuri che il cavo non è stato tirato o non ha subito urti. Bisogna pensare a possibili locazioni dove queste tecnica può essere utilizzata. Per passare il cavo sopra il

muro, devi **scegliere un oggetto che sia sicuramente attaccato alla parete**. Un oggetto può ad esempio **essere un TIE-TRAP. Se il tie trap deve essere rimosso, si può usare un Tie-Trap Adesivo. E' facile da usare, ricordati** che non può essere mosso o riposizionato in seguito. Se tu pensi che esso debba essere rimosso in futuro, usare il supporto **tie-trap standard con le viti a muro**. Se si usa un tie trap con edlle viti, bisogna per prima cosa scavare dei buchi nel muro, spesso questo può comportare dei problemi. Devi scavare **dei fori di 9.5mm** di diametro, puoi usare un trapano elettrico. Se hai bisogno di 9.5 mm di diametro, il trapano probabilmente creerà dei buchi eccedenti, Quindi è necessario usare un Trapano Martello, che ridimensiona i buchi. **Non bisogna mai usare delle cuciture**, altrimenti non si rientra nello standard TIA\EIA-568-A.

Montaggio dei cavi nelle Canalette: Tu puoi anche far passare il cavo **montando delle canalette**, sono dei canali a muro, con coperchio smontabile. Possono esistere vari tipi di canalette (recaway). DECORATIVE RACEWAY: Presentano **più rifiniture apparenti**, sono usate per far passare il cavo in una stanza dove esso è visibile. GUTTER RACEWAY: Sono meno attrattive e decorative, il loro primario vantaggio è che esse **sono grandi abbastanza da poter permettere il passaggio di diversi cavi**. Generalmente l'utilizzo di queste canalette è ristretto a spazi ad esempio Attici, o soffitti caduti. Le canalette possono essere di plastica o metallo e possono essere montate sia con viti che **con materiale ADESIVO**. Puoi pensare ai possibili Vantaggi e Svantaggi delle canalette adesive? **Svantaggi:** Look non gradevole, utilizzo singolo, può allentarsi o venir tirato via. **Vantaggi:** Facile da installare, Facile da rimuovere. Dopo aver installato la canaletta, fai passare il cavo all'interno di essa, ed attacca la canaletta al muro. Questo aiuterà a proteggere il cavo. Le canalette possono essere usate per condurre vari tipi di cavi, è possibile utilizzare delle canalette già esistenti, bisogna considerare il tipo di cavo che già passa attraverso le canalette esistenti, prima di farci passare il nostro cavo di rete categoria 5utp.

Misure di sicurezza per installazione cavo: 1) Quando capita di lavorare su muri, soffitti o attici, la prima cosa da fare è **disattivare tutti i circuiti di corrente nei pressi dell'are di lavoro**. Se non sei sicuro di aver disattivato la zona in cui lavori, disattiva la corrente all'intera area. 2) Prima di iniziare il lavoro, informati **sull'esatta posizione degli Estintori.** 3) **Usare appropriate pinze da lavoro, proteggersi con adeguati Guanti**, e guardarsi attorno con sufficiente illuminazione. 4) Se hai la necessità di tagliare **proteggi i tuoi occhi** con protezioni di vetro di sicurezza, è una buomna idea proteggersi gli occhi quando si lavora su soffitti o ambienti bui. 5) Consulta l'ingegnere dell'edificio per le varie regolamentazioni 6) **Mantenere il luogo di lavoro pulito**, non lasciare attrezzature in luoghi di passaggio, Attenzione ai mezzi ingombranti o dotati di corda, la gente potrebbe inciampare :P

Sicurezza dell'edificio: Bisogna sempre sapere in anticipo ciò che **dicono i codici in relazione alla struttura locale**. Alcuni codici di edifici **possono proibire le forature** o le scavature di buchi in certe aree di muri o soffitti. L'amministratore o l'ingegnere addetto può aiutarti ad individuare questi limiti. Quando si installa un cavo, se tu trovi un'area **danneggiata**, **non passare il cavo in quest'area**. In alcune situazioni se tu scavi un buco in un muro, i **buchi non possono essere utilizzati**. Ancora un ingenere può aiutarti ad identificare le locazioni giuste per effettuare le forature. Dopo aver fatto ciò, è possibile passare il cavo.

Supporto per cablatura Orizzontale: Molti installatori preferiscono far passare il cavo in attici o soffitti poiché in questo modo esso non è particolarmente in vista, Quando si fa passare il cablaggio, bisogna sempre fare **in modo che il cavo resti in alto** rispetto alla superficie del muro, eventualmente utilizzare supporti per il cavo. Come mensionato precedentemente esistono **diversi**

supporti per il cavo, si può usare :gutter, attach tie-warps o ladder rkack, che sarebbe il miglior tipo di supporto per il cavo. **Attici e soffitti** non sono luoghi molto confortevoli ed **è difficile lavorarci**, luoghi bui, con poca circolazione d'aria. Particolarmente duro, lavorarci d'estate a causa della temperatura. **Il TELEPOLE offre una semplice e facile soluzione**. il telepolo **è un palo con un gancio ad un capo**..per sistemare cavi per esempio sconnessi su un soffitto.

Pescare un cavo e tirarlo su per un muro: Quando devi passare il cavo per un muro, solitamente per tirarlo su, si ricorre ad un altro cavo chiamato **FISHING CABLE**, serve **appunto per PESCARE il cavo, dal basso verso l'alto**.

Wiring Closet: La Wiring closet serve come **punto di funzionalità centrale** per il cablaggio, usato per connettere periferiche in una lan. **E' il punto centrale della tipologia a stella**, Può essere costituita una stanza apposta per questa wiring closet, la wiring closet include: Pannelli patch, Hubs, Bridges, switches, routers. Nelle grandi reti abbiamo **più di una WIRING CLOSET**, Una wiring closet **è designata come MAIN DISTRIBUTION FACILITY (MDF)** e le altre **sono designate come INTERMEDIATE DISTRIBUTION FACILITY (IDF),** sono dipendenti dalla prima. La topologia descritta è una Exteended star topology.

Pannello Patch: Nella topologia Ethernet STAR la cablatura orizzontale passante che proviene da aree di lavoro **sfortunatamente termina al patch panel**. La patch panel **è una periferica di interconnessione** tramite la quale un cavo orizzontale può essere connesso ad altre periferiche di rete, come hubs o repeater. Più **specificatamente la patch panel è dotata di locazioni di PIN o PORTE** dove collegare i cavi. Una patch pannel ha **ruolo di SWITCHBOARD** quando il cablaggio orizzontale proviene da una workstation e deve connettere altre workstation in una rete. In diversi circostanze una patch panel **può anche essere un luogo per periferiche che si connettono a una WAN**, o ad internet. Questa connessione è descritta da TIA\EIA 568-A come **ORIZZONTAL CROSS CONNECT (HCC)**

Struttura del Panello Patch: Per capire come un patch panel serve per connesioni orizzontali che raggiungolo altre periferiche, esaminiamo la sua struttura. Molti collegamenti tipo **gli Rj45** sono localizzato **su un lato del patch panel** e proprio come i jack, essi sono codati con dei colori. **Per effettuare le connessioni elettriche ai pin, bisogna utilizzare un PUNCH TOOL**, sotto i cavi. **Questa è una proecdura importante**, da eseguire accuratamente ai fini delle PERFORMANCE di una rete. Bisogna **inoltre fare attenzione ai fili**. Devono corrispondere i **colori giusti**, è molto importante, i fili ed i pin **non sono intercambiabili**. Sul lato opposto del patch panel **ci sono delle porte**. Esse **assomigliano a sbocchi di comunicazioni**, come quelle nelle aree di lavoro. Le porte RJ45 e le porte sul patch panel portano pugs della stessa dimensione. Le Patch cords che connettono a queste porte possono essere possibili mezzi di intercomunicazione fra computer di altre reti ed altre periferiche (hub, repeaters, routers.ecc.ecc), **collegati anch'essi al patch panel**.In ogni sistema di rete, i connettori sono linkati. **Se non propriamente installati**, i connettori, **possono creare disturbi elettrici**, intermittenze elettriche fra i cavetti ed i pin. Quando questo accade, la trasmissione dei dati sulla rete può essere distrutta, o può essere ridotta la portata del cavo, per essere sicuri che il cavo sia installato correttamente, è necessario, come sempre, seguire gli standard TIE\EIA.

1) Quando si collega diversi cavi CAT5 passanti per un patch pannel bisogna **passare il cavo in ordine ascentende By Numero**. Bisogna prendere un foglio di carta ed appntare le operazioni da

fare, dopo si possonoa ggiungere delle etichette. Utilizzare **la numeratura dei cavi** per assegnare il passaggio di cavi dalla stanza di lavoro alla wiring closet, il numero del cavo deve corrispondere al numero della stanza dove le workstation sono situate, Dividendo i cavi in ordine Ascendente al patch panel **diventa facile localizzare e risolvere problemi** fuguri. 2) Come tuo lavoro è importante **portare la fine del cavo nell'esatta posizione dei pin**. Se non stai attento, i cavi possono essere schiacciati, questo può causare una perdita di portata del cavo, quadno la rete è connessa completamente. 3) Devi essere sicuro di **tenere il jack entro 6.4 mm dalla locazione dei pin** sui quali stai lavorando per non esporre troppo il cavo. Un buon metodo per effettuare ciò, è **misurare il cavo prima di sbucciarlo**. 38-50 mm possono essere sufficienti. Se tu esponi troppo cavo, le conseguenze possono essere, riduzione di capienza sulla rete. 4) **Non devi sbucciare i cavi più del necessario**, la sbucciatura eccessiva del cavo riduce la portata della rete e **può portare CROSSTALK**.

Il punch Tool: Il tipo di patch panel utilizzato determina quando usare **un punch TOOL da 110**, chiamato anche **KRONE PUNCH TOOL**. Il punch ha azioni di spinga caricata. (**SPRING-LOAD ACTIONS**). Questo permette ad esso di eseguire di funzioni allo stesso tempo. Premendo il cavo **due pinze di metallo sbucciano il cavo ed una lama taglia la parte di cavo non necessario**. Occasionalmente il punch tool può fallire nell'esecuzione di un taglio perfetto. Quando ciò accade, tagliare la parte di cavo che è venuta male, rimuoverla e ripetere l'operazione. Quando si usa un punch tool, bisogna essere sicuri di posizionare esso con la faccia delle lame dietro rispetto alla fine del cavo. Se non si prende questa preocauzione il taglio del cavo può risultare troppo corto per le connessioni elettriche da eseguire.

Montaggio di una Patch Panel: Puoi montare i patch panels **a muro, con l'aiuto di BRACKETS**, puoi piazzarli **in contenitori** (cabinet). Uno dei pezzi più comunemente utilizzati per equipaggiare il patch panel è il **DISTRIBUTION RACK**. puoi montare pannelli a muro con l'aiuto di mensole, puoi metterli in uno scaffalino o in armadietti (equipaggiati con file interne e sportellini). Uno dei pezzi + usati è **uno scaffalino di distribuzione** che contiene patch panels, repeaters, hubs e routers. ...Può variare in altezza da 1 a 1,9m**. Il vantaggio** è che offre facile **accesso sia frontalmente che posteriormente**. Per assicurare stabilità una lamiera fissa lo scaffalino di distribuzione al suolo. Anche se alcune compagnie vendono scaffali di ampiezza .5m, lo standard dal 1940 è sempre stato .48m

Testare i cavi usando un Flukkettone: IEEE e TIE\EIA hanno stabilito gli standard che permettono a te **di testare la tua rete** e stabilire se essa funziona **ad un livello accettabile**. Se la tua rete passa il test essa **è certificata per gli standard**, puoi usare queste misure per stbilire una linea base di funzionamento. **La baseline è un record** del tuo punto di partenza con il networking, il record delle tue possibilità di installatore e progettatore di reti. Conoscere le misure della baseline è assai importante. I test possono non essere sufficienti alchè la tua rete sia conforme agli standard, deviquindi **continuare a testare la tua rete** su una base regolare per essere sicuro che la sua performance migliori e sia accettabile. Puoi paragonare le correnti misurazioni con quelle che hai registrato manualmente. **Ripeti i test e paragonali ancora con le BASELINE**.Ciò può aiutarti a capire e rislvere numerosi problemi. **Un attrezzo che è possibile utilizzare** per testare la "SALUTE" della propria rete **è il FLUKE. Il FLUKE Network's NETTool**, permette di avere una visione delle cause sui **problemi di connettività Destkotp-to-network**, combinando le capacità di un tester di rete, un tester di configurazione pc ed un test base per il cavo. **NetTool si connette fra il pc ed il jack al muro**. Una volta connesso il nettool ascolta, colleziona ed organizza informazioni

riguardanti: Le risorse di rete disponibili, Le risorse di rete che il pc è configurato per utilizzare, la vita dei segmenti di rete, **includendo ERRORI, collisioni, utilizzo, e vita della scheda di rete, e rete locale**. Puoi Anche usare il NET TOOL per effettuare test base sul cavo per rilevare aperture, tratti troppo corti, difetti del cavo e lunghezza aperta sull'rj45, cavo terminato. E pin to pin è possibile testare l'installazione del cablaggio sulla patch. **Il net tool ha le seguenti caratteristiche**: Service identification (identifica un jack come ethernet, token ring Telco o non attivo). Link Reporting, (Rileva e riporta le precedenti negoziazioni di hub\switch-pc). Inline mode (visualizza l'ip del pc e le risorse utilizzate sulla rete, il default router, il server email, dns, ed i servizi web ai quali si ha accesso). Basic Cable Testing (Effettua dei test base dal cavo, visualizza i punti aperti, corti, cavi invertiti, lunghezza, e la mappatura dei pin con la connessione ai cavi)

Equipaggiamenti per Test dei cavi: Tu puoi pensare che testare un cavo, è semplice quando sostituirne uno con un altro. Non è così, comunque esso **fornisce una prova certa di un problema** che può riguardare i cavi della lan. Per questa ragione **è raccomandato usare il tester** per misurare le performance di una rete. Un cable tester è un apparecchio palmare. **Certifica che il cavo soddisfa i requisiti IEEE e TIA\EIA standard**. Il cable tester **varia** a seconda del tipo di funzioni che esso fornisce. Alcuni possono fornire stampati, altri possono essere collegati al pc e generare file di diagnostica. **Non è necessario uno speciale training** per utilizzare l'apparecchio che è facilmente reperibile sul mercato di oggi. Molti amministratori di rete competenti, o installatori, trovano nel manuale operativo dei tester sufficienti istruzioni per poterlo utilizzare perfettamente.

Test effettuati dal Cable tester: I tester dei cavi hanno una vasta gamma di possibilità. Tu puoi determinare quali funzionalità ti servono e fare la tua scelta economicamente più adeguata,. I cable tester hanno le seguenti funzioni. Determinare la distanza del cavo, localizzare cattive connessioni, effettuare una mappatura dello schema dei cavi per individuare crossed pairs, misurazione dell'attenuazione segnale, misurazione del crosstalk, rilevazione cavetti invertiti, rilevazione disturbi sulla rete, tracciare cavi vicino al muro.

Cable tester e misure delle Distanze: E' molto importante **misurare la totale lunghezza del cavo** in uso. **La distanza può incidere** sull'abilità delle periferiche sulla rete che condividono la parte del cavo. Come abbiamo già imparato in precedenza i cavi che **eccedono** la massima distanza, **secondo lo standard TIA\EIA 568-A, causano degradazione del segnale**. I tester dei cavi, spesso riferiti a **"TIME DOMANIN REFLECTOMETERS" (TDRs), misurano la distanza** del singolo cavo, Essi fanno ciò, inviando un impulso elettrico tramite il cavo, la periferica quindi temporizza la riflessione del segnale. Questo test è chiamato **TIME DOMAIN REFLECTOMETRY** e puoi fornire **la distanza con un'accuratezza di 61CM**.

Tdr: In una installazione di una lan che usa cablaura UTP **la misura delle distanza può farci capire se la connessione al patch panel o all'uscita può essere buona**. Per capire meglio questo avoro bisogna capire come il TDR lavora. **Il tdr misura le distanza** sul cavo inviando un segnale elettrico tramite il cavo, il segnale è riflesso quando esso raggiunge la magigore distanza in cui il cavo è aperto. **Per determinare una connessione** fallita bisogna attaccare il TDR ala patch cord al patch panel. **Se esso riporta** la distanza al patch panel inteso **come una distanza a più punti**, puoi quindi

capire che ci c'è un **problema** di connesssione. Puoi usare la stessa procedura sulla apposita fine del cavo per prendere le misure tramite il connettore RJ45 locato nella uscita di comuniazione.

Mappatura dei fili: I tester per i cavi **usano una funzionalità** chiamata **WIRE MAP**. Per indicare **quale filo è connesso** ad uno specifico pin o lugs e socket. Il test indica quando l'installatore connette propriamente i fili al plug o jack o quando esso li connette in modo invertito. **Quando i fili sono connessi in modo invertito**, essi sono riferiti a **"CROSSED PAIRS**", Unicamente sull'installazione dei cavi di tipologia UTP, **questo può essere un problema comune.** Quando dei cavi crossati sono rilevati nella rete UTP LAN cabling system, la connessione non sono buone e **devono essere rifatte**.

Splittatura dei cavi: L'ispezione **visuale e la misura del crosstalk è il solo modo** per poter rilevare una condizione di SPLIT PAIRS. Come conosci la cablatura nei filettini di ferro, **ripara essi da interferenze esterne**, da segnali che passano vicino a questi fili. Quindi **questo scudo** può funzionare **solo se i fili sono parte dello stesso circuito**. Dunque la corrente può passare nel circuito, far funzionare il sistema apparentemente senza problemi, anche se **il cavo non ha schermatura**. Conseguentemente a ciò, il segnale **non è protetto**. In questa eventualità, un **crosstalk può diventare un vero problema**. Un **Wire MAP non può rilevare una splitconnection** perché nei cavi splittato un circuito deve essere presente. **Un cavo è disturbato da un altro tramite interferenze**.

Attenuazione del Segnale: Vari fattori **possono ridurre la potenza del segnale** che passa attraverso i cavi utilizzando la cablatura UTP. Questa **riuzione in potenza è chiamata ATTENUAZIONE**. Se ciò avviene, **il segnale perde energia** sul cavo. Il tester **può misurare la riduzione di energia** di un segnale ricevuto da una periferica chiamata **"SIGNAL INJECTOR**", **un piccolo box**, approssimativamente di dimensioni simili ad una scatola di carte da gioco, è attaccata **alla fine del cavo**. Il tester del cavo generalmente misura l'attenuazione a diverse frequenze. I tester di cavi categoria 5 generalmente misurano più di 100 MHZ. Controlla le specifiche TIA\EIA 568-A per vedere l'ammontare di perdita permesso per il tipo di cavo usato nella specifica lan.

Le cause di un CrossTalk: Diversi fattori possono contribuire al crosstalk. La causa più comune è un cavo Crossato. Come menszionato precedentemente, **tu puoi rilevare ciò con la wire map**, una funzione del cable tester. Il crosstalk può anche essere causato da **fili scoperti** subito dopo l'attaccatura di connessione a periferiche come patch panels. Se intendi misurare il cross talk dovrai effettuare un check visuale della cablatura orizzontale per vedere se esiste tale possibilità. Se non si trova niente, gli split pairs possono rappresentare una delle maggiori cause di questo problema. **Un tester** di cavi, **misura il cross talk** analizzando il segnale del cavo su varie frequenze, **sopra i 100 mhz**. **Numeri alti sono buoni. Numeri bassi indicano problemi sulla ret**e.

Rilevazione problemi da un test di rilevazione rumori: Molti fattori esterni possono contribuire alle **interferenze** sulle periferiche di rete. Molti

esempio di **sorgenti** che producano segnali esterni che si impongono sulla cablatura di rete utp: Luci Fluorescenti, caloriferi, radio, condizionatori d'aria, televisori, computers, radar, motori, switch, apparecchiature elettriche di bambini, ecc.ecc Fortunatamente il signale prodotto da **queste sorgenti esterne** spesso occupa speciali frequenze. **Questo provoca un disturbo elettrico** che non è sempre rilevato da tutte le interferenze esterne, ma **permette di capire più o meno che cosa le provoca**.

Utilizza il cavo per rilevare le interferenze esterne: Usando un cable tester **si apporta una lettura sul cavo,** è però necessario disconnettere tutti i cavi dall'equipaggiamento informatico (Computers). **Un alto livello di lettura**, di solito indica **un problema**. Un modo sempre per localizzare la precisa sorgente **è UNPLUGGARE ogni periferica** elettrica finchè la sorgente dei disturbi è rilevata. Bisogna comunque essere consapevoli del fatto che ciò, **non sempre funziona**.

Procedure di Test dei Cavi:

Your instructor will demonstrate some of the tests that can be performed with a cable tester. In some instances, the tests will indicate that problems exist. You will be asked to outline how you would determine what the problems are, and describe how you would fix them.

During the second half of the lab, you will be asked to demonstrate your ability to use a star topology to set up a simple Ethernet LAN. Your instructor will evaluate you on your ability to handle the cable correctly, and to lay, and punch down wires, in a jack, and at a patch panel, so that there are good connections.

After you complete the connections for your star topology LAN, you will be asked to test it. If tests indicate problems, you will be asked to diagnose and troubleshoot those problems. The goal in this series of lab exercises is to produce a completely functional star topology LAN that meets TIA/EIA and IEEE specifications

gIP e Routing

Identificazione: Il lato Network (3), è resposabile per lo spostamento dei dati **tramite una quantità di reti.** Lo schema di indirizzo è usato dalle periferiche per determinare la destinazione dei dati che si muovono attraverso la rete. **I protocolli che non hanno il lato NETWORK possono essere usati SOLO per fare piccoli spostamenti** di dati all'interno di reti limintate. Questi protocolli, di solito **utilizzano il mac** per identiticare il pc nella rete. **Il problema** con questo tipo di approccio è la cresciuta della rete per cui diventa **difficile** organizzare **tutti nomi**. Bisogna inoltre essere sicuri che più di 1 computer **non utilizzi lo stesso nome**. I protocolli che supportono il lato **network**, usano un **schema di indiirizzamento HIERARCHICO** che permette **per un unico indirizzo il viaggio attraverso la rete**. Il **mac** address inveec utilizza una schematura di indirizzo piatta che lo rende **difficilmente localizzabile** in altre reti. Lo schema di indirizzamento Hierarchico permette alle informazioni di **attraversare INTERNETWORK** con un metodo di ricerca destionazione molto efficiente. LA rete telefonica è un esempio di utilizzo di hierirchal addressing. Il sistema telefonico usa un codice di area che designa un'area geografica per il primo CALL STOP. Il prossimo albero di numeri rappresenta il secondo step per la seconda area (HOP), i numeri finali rappresentano l'individuale destinazione (il telefono). Le periferiche della rete **necessitano uno schema di indirizzi che permette ad esse di essere forwardate** attraverso altre

reti, (a set of network composed of multiple segment using the same type of addressing). Ci sono **diversi livelli di rete** con differenti schemi di indirizzo che permettono alle periferiche di forwardare i dati sulle reti.

Segmentazione e sistemi Autonomi: Ci sono **2 PRIMARIE ragioni per cui** sono necessarie multiple reti. La **crescita di taglia di ciascuna rete e la crescita del numero stesso delle reti**. Quando una lan, man, o wan cresce, **può diventare necessario**, per il controllo del traffico, **dividere la rete in piccoli pezzi chiamati NETWORK SEGMENT**. Questo può risultare, nella rete, un aggiunta di gruppi di piccole reti che richiedono **INDIRIZZI SEPARATI**. Ci sono già un vasto numero di reti esistenti, separate reti di computer sono comune in uffici, scuole, compagnie di lavoro..ec.ecc. E' **conveniente far comunicare tutte queste reti con internet**. Essi devono far ciò con **un sensibile schema di indirizzi** e con più perferiche di internetworking. In caso contrario il flusso di reti, verrebbe ostacolato dalle ALTRE RETI, per cui non si avrebbe una comunicazione globale. Una analogia può aiutarci a capire la necessità della segmentazione di rete. Immaginiamo una strada e il numero di veicoli che la utilizzano. A seguito dell'incremento della popolazione dell'area circostante, la strada aumenta di dimensioni, diviene quindi **INTOPPATA con troppi** veicoli nel mezzo che non riescono a circolare. La rete opera in questo modo. La crescita di rete, l'ammontare del traffico..Un'altra **soluzione** può essere **usare le periferiche che segmentano la rete** e controllano il flusso del traffico. Allo stesso modo un astrada può usare periferiche come SEMAFORI che controllano il movimento del traffico.

Comunicazioni Fra reti Separate: Internet è una **connessione di segmenti di rete** che sono collegati fra loro e **comunucano** per facilitare la condivisione delle informazioni. Possiamo di nuovo fare l'esempio dell'anologia con la strada per cui varie stradine comunicano **grazie al collegamento di tratti intermedi** in regioni geografiche. Le reti operano per la maggior parte, nello stesso modo. Con compagnie di fornitori servizio internet (ISP) offrono servizi che permettono di raggiungere contemporaneamente multipli segmenti di rete.

Periferiche di Livello 3: I **routers** sono **periferiche di intercomunicazione**. Essi **operano al livello 3** OSI (network layer). Essi comunicano assieme o interconnettono segmenti di intere reti. Essi fanno passare i pacchetti di dati basandosi sul **livello3 Network e sulle informazioni contenute** in esso. I router effettuano **una decisione logica** per l'appropriata **uscita sulla porta VERSO un determinato segmento**. I routers prendono pacchetti da periferiche di rete, e basano le prorpie decisioni sul livello3, **forwardando il pacchetto** a destinazione. Infatti il termine **routing è riferito al livello3 (switching).**

Determinazione del Percorso: La determinazione del Percorso, avviene al Livello 3. Essa **permette al router di valitare il percorso disponibile** per la destinazione, e di stabilire la intestazione preferita per il pacchetto. Il servizio di routing usa le informazioni provenienti dalla tipologia di rete mentre valuta il percorso di rete. La determinazione del percorso è il processo tramite il quale un router **sceglie la prossima (HOP)** sul percorso, che permette al pacchetto di arrivare a destinazione. Questo processo è anche chiamato **ROUTING THE PACKET**. La determinazione del percorso per un pacchetto può essere paragonata ad una persona che guida una macchina e che viaggia da un lato all'altro della città. Il guidatore ha una mappa e vede le strade che necessita di percorrere per raggiungere la destinazione. La guida da una intersezione all'altra è **chiamata HOP**. Similarmente, **un router usa la mappa** per vedere le strade possibili che consentono di raggiungere la destinazione. **I routers possono anche eseguire decisioni basate sulla densità del traffico**, e sulla velocità del link (bandwidth), quindi un guidatore può sceglire un percorso più veloce ad esempio "l'autostrada" ☺

Rete e lato di Indirizzamento: L'indirizzo di rete **aiuta il router ad identificare** il percorso **all'interno della nuvola di rete**. Il router usa l'indiirszzo di rete per identificare la rete di destinaziona di un pacchetto **all'interno di una internetwork**.
In aggiunta all'indirizzo di rete, il protocollo di rete **usa anche altre informazioni** provenienti dall'host, dal nodo o dall'indirizzo. Per molti protocolli basati sul livello network, un amministratore di rete **assegna un indirizzo host** di rete in accordo con il piano di internetwork di indirizzi, precedentemente determinato. **Per gli altri** protocolli su lato network, l'assegnazione dell'indirizzo host **è parziale o completamente automatica\dinamic**.
L'**indirizzzamento** avviene nel **LAYER NETWORK**. Analogamente al lato network telefonico, esso include porzioni di numero di telefono. **Le rimanenti 4 cifre** del numero telefonico dicono alla compagnia telefonica di far squillare uno specifico telefono. Questo è simile alla funzione della porzione di indirizzi IP di un host. La porzione dice al router che la periferica specificata è situata in una determinata posizione per grazie a queste informazioni, viene forwardato il pacchetto. Senza il lato NETOWORK di indirizzamento, il routing non può esistere. Senza le strutture HIERARCHICHE proprie dell'indirizzo, il pacchetto non potrebbe viaggiare tramite una INTER-Network. Allo stesso modo, senza questa struttura hierarchica, il sistema telefonico, gli indirizzi postali o i sistemi di trasporto non potrebebro organizzare il loro sistema di trasporto.

Layer3 e Mobilità: L'indirizzo **MAC** può essere paragonato **al tuo nome**, e **l'indirizzo di rete** può essere paragonato al tuo **indirizzo email**. Per esempio **se tu ti sposti** in un'altra città, **il tuo nome non cambia**, ma **il tuo mail address può cambiare** per indicare la tua **nuova posizione**. I router hanno la gestione dei dati su IP e MAC, il mc è fisso. Quando si muove fisicamente **un computer in un'altra rete**, il computer **MANTIENE lo stesso mac**, ma **l'ip viene cambiato**, ne viene assegnato uno **secondo le specifiche della nuova rete**.

Comparazione dell'indirizzo Hierarchico e Piatto: La funzione del livello di rete è trovare il miglior percorso sulla rete. Per completare questa operazione v**engono usati 2 metodi di indirizzamento**. Il **flat** addressing ed **il hierchical** addressing. Lo schema del FLAT addressing assegna alla periferica il prossimo indirizzo disponible. Non c'è, purtroppo, nessun pensiero che può rendere idea della struttura dello schema di indirizzi.Un esempio di indirizzi FLAT è il numero di identificazione militare, o il numero identificativo di un compleanno. Il mac address funziona allo stesso modo. Un venditore assegna un blocco di indirizz. La prima metà di essi sono per il venditore (vendor code), il resto degli indirizzi mac sono numeri assegnati con sequenza. Il mac è un **identificativo FISSO**. (indirizzo piatto: Ip fisso o mac) **Il codice postale**, è invece un buon **esempio di indirizzi Hierchale**. Il codice è determinato dall'area in cui si trova l'edificili. Non da una sequenza casuale. **Lo schema di indirizzamento**, che si userà per questo processo **è chiamato IP (internet protocol) adressing. IP ha una struttura specifica** e non è assegnato a caso.

Diagramma di Rete e Livello: L'iP **internet protocol**, è **una implementazione** molto popolare dello **schema indirizzo delle reti HIERARCHICHE**. IP è il protocollo internet, **che usa internet**. Una informazione circola sui livelli del modello Osi, i dati **vengono incapsulati ad ogni livello**. Al lato network i dati **sono encapsulati in pacchetti**, chiamati anche **DATAGRAMS**, IP determina la forma del pacchetto **ip**, **in particolare L'intestazione**. Include l'indirizzo del destinatario e le informazioni di controllo. Esso non riguarda i dati all'interno del pacchetto. IP **accetta qualsiasi cosa che è passata dai livelli più alti**. (quando i dati transitano dall'alto verso il basso, non c'è ragione di INTESTARE.. ☹)
Un ip è a 32 bit. Diviso in 2 parti. La prima relativa a NETWORK, la seconda a HOST.

I Fields del lato Network: Il datagramma dei pakketi del livello 3 **rivece i dati del livello2** che sono **incapsulati** dentro il frame (precedentememte). Simlarmente, il pacchetto ip consiste **in dati dal lato superiore più un ip HEADER** che consiste in: Version (indica la versione di ip usato, 4

bit). Ip header lenght (HLEN). (La lunghezza del datagramma in 32 bit words, 4bit), Ttype of service (l'importanza che è assegnata da un particolare protocollo di alto livello,8bit). Total leght (lunghezza del pacchetto ip, includendo l'header,16bit). Identification (identificazione del datagramma,16bit). Flags (è un field di 3 bit, 2 di basso ordine contengono la frammentazione. Un bit specifica quadno il pacchetto può essere frammentatoed il secondo è l'ultimo frammentato, 3bits). Fragment OffSet (il field che è usato per aiutare i pezzi di dati a frammentarsi,13bit), Time to Live (TTL, mantiene un contatore che diminuisce gradualmente a 0, al qual punto il datagramma è eliminato evitando che i pacchetti circolino all'infinito (8 bits)), Protocol (indica che la ricezione da parte dei livelli alti, del processo ip è completa). Header Checksum (aiuta ip a mantenere l'integrità,16bit) Source Address (specifica il nodo di invio) Destination Address (specifica il nodo di ricezione) Options (permette ad ip di supportare varie opzioni di sicurezza, lunghezza variabile) Data (contiene informazioni di alto livello, lunghezza variabile, max 64kb) Padding (sono aggiunti extra zero a questo field per essere sicuri che ip header sia sempre un multiplo di 32 bit)

IP header Field di sorgente e destinazione: L'indirizzo ip **contiene informazioni necessarie** per **fare il routing** del pacchetto attraverso la rete. Ogni field di sorgente e destinazione **contiene un indirizzo di 32 bit**. L'indirizzo del sorgente contiene **l'ip della periferica che invia** il pacchetto. Il field di destinazione **contiene l'ip address della periferica che riceve** il pacchetto.

Indirizzo ip come un numero binario a 32 BIT: Un ip address **rappresenta un numero binario** a 32 bit. A seguito di un rapido review, ricorda che ogni cifra di numero binario **può essere solo 0 oppure 1**. **in un numero binario... il bit più a destra è quello meno significativo...(come nel sistema decimale peraltro) e che il valore di ogni bit raddoppia mano a mano che da destra si va verso sinistra..**Gli ip address **sono espressi in 12 numeri decimali**. E' un indirizzo di 32 bit, 4 gruppi da 8. Il massimo numero per 1\8 è 255. Il numero a 8bit più grande è 11111111. Questi bits , da destra verso sinistra, hanno un valore di 128,64,32,16,8,4,2. Aggiunti assieme, fanno 255.

I Fields componenti dell'ip Address: Il numero della rete di un ip **identifica la rete** a cui il pc è collegato. La **porzione host** di un indirizzo ip, **identifica la specifica periferica** sulla rete. L'indirizzo ip consiste in **4 octet separati da punti**, uno, due o tre di questi octects può essere usato **per identificare il numero della rete**. Similarmente queste 3 ottave superiori possono essere usate **per identificare la partizione host** dell'indirizzo ip.

Classi di indirizzi IP: Ci sono tre classi di Indirizzi IP, che un'organizzazione può ricevere da "america registry for internet numbers" (ARIN) o l'organizzazione dell'ISP. Ci sono. Classe A, B e C. Arin reserva **Classe A** per aziende di **enormi dimensioni**, **Classe B** per **aziende medie**, **Classe C** per tutti gli altri **piccoli sistemi di network**.

Classe A: Scritta in **formato binario**, la numerazione di questa classe ha come primo bit, **sempre 0**. Un esempio di classe A è 124.95.44.15. **Il primo ottavo**, 124, identifica la rete **assegnata da ARIN**. L'**amministratore** interno della rete, **assegna i restanti 24 bit**. Un facile modo per riconoscere se la periferica è parte di una rete di classe A, è guardare alla prima ottava dell'indirizzo ip, che **deve essere da 0 a 126**. Il 127, sotto forma binaria, è

riservato a funzioni speciali. Tutti gli ip di classe A utilizzano **solo la prima ottava per identificare la rete** a cui l'indirizzo appartiene. Le rimanenti 3 ottavo possono essere usate per la porzione di host dell'indirizzo.A ogni rete che usa un indirizzo di classe A può essere assegnato 2 alla 24 indirizzi, meno 2, o sono possibili 16.777.214 indirizzi ip ai dispositivi ccollegati a questa rete. (2097150 RETI)

Classe B: **I primi** 2 bit della classe b sono **sempre 1 e 0**. Un esempio di classe B è 151.10.13.28. **LE prime** dueottave identificano **il numero della rete assegnato da ARIN**. L'amministratore nterno assegtna le restanti 2 ottave (16bit). Un modo facile per identificare quando una periferica è parte di una rete di classe b è guardare il primo ottavo della rete, **deve essere fra 128 e 191**. Tutti gli indirizzo di classe b utilizzano i primi 16 bit per identiificare la rete le 8 ottave che rimangono identificano la porzione di host. Ad ogni rete può essere assegnato 2 alla 16 meno 2 di indirizzi, sono possibili 65,534 indirizzi collegati alla rete. (16382 RETI)

Classe C: Le prime 3 cifre binarie della classe c sono 1, 1 e 0. Un esempio di classe C è 201.110.213.28 le prime 3 cifre identificano il numero della rete assegnato da ARIN. L'amministratore interno della rete assegna il restante octect. Un buon modo per **riconoscere un ip di classe 3 è guardare l'octect iniziale, dev'essere fra 192 e 223**. Nelle classi C per identificare le rete sono assegnati 24 bit di indirizzo, l'ultimo ottavo è per la partizione di host. Ogni rete che usa la classe C può avere assegnato 2 alla 8 meno 2, con **254 possibili indirizzi** ip per le periferiche che sono collegate alla rete. (126 RETI)

Classe D: La prima OCTECT è da 224 a 239. E' riservata al MULTICASTING.

Indirizzi ip e numeri decimali: L'indirizzo ip **identifica una periferica sulla rete** e **la rete a cui essa è collegata**. Gli indirizzi ip**, sono solitamente scritti in ottave**, su base decimale. Gli ip sono **4 numeri** decimali, separati da punti. Tieni presente che un numero decimale **è sempre BASE 10**,il tipo che noi usiamo nella vita di ogni giorno.

Convertire decimal ip a binari: E' necessario conoscere il valore decimale di ogni 8bit, partendi con il bit sulla sinistra, il valore parte a 128 è ridotto di metà ogni volta che muovi unbit sulla sinistra, continuando a valire di uno sulla destra.

Network id e Indirizzo: Se il tuo computer vuole comunicare con tutte le periferiche sulla rete, tu devi stare attento a scrivere l'ip di questa periferica con esattezza. **Un indirizzo ip finisce con il binario zero** in tutti gli host questo è presente. Un indirizzo di classe A, ad esempio, è 113.0.0.0 contiene l'host 113.1.2.3. Il router usa l'ip di rete quando deve forwardare i dati su internet. Un indirizzo di classe B può essere 176.10.0.0. Il numero decimale che si trova nelle prime due ottave della classe B è designato per indicare il numero della rete. Le ultime 2 ottave contengono Os, perché sono 16bit di cifre che corrispondono all'host number, e sono suate per le periferiche**. L'ip usato per la rete NON DEVE ESSERE USATO PER 1 PERIFERICA. MAI**. Se tu vuoi chiamare tutte le periferiche su una rete, tu devi usare un **BROADCAST ADDRESS**. Il broadcast avviene quando una sorgente invia dei dati a tutte le periferiche della rete. Per essere sicuri che tutte le periferiche della rete facciano attenzione al broadcast, colui che invia, deve usare un indirizzo ip di destinazione che includa tutte le macchine. La fine del broadcast ip è 1s, nell'intera parte dell'host degli indirizzi (host field). Per esempio nella rete

176.10.0.0 dove gli ultimi 16 bit sono riservati all'host, il broadcast chesi invia a tutte le periferiche della rete deve includere l'indirizzo di destinazione **176.10.255.255 (dove 255 è il valore decimale per la octect che contiene 11111111).**

ID di rete: E' importante capire il significato di **una porzione di rete (NETWORK ID).** L'host su una rete **può comunucare soltanto con periferiche che hanno lo stesso network ID**. Essi possono condividere anche lo stesso mezzo fisico ma **se non sono di stessa rete (classe ip netowork), non possono comunicare**. Hanno bisogno di un'altra periferica che faccia da Router (routing). Il codice postale, ad esempio è simile al netowrk ID. Il codice postale abilita il sistema postale ad indirizzare la tua posta all'ufficio locale. Il network id abilita il router ad inviare il pacchetto, verso l'appropriato segmento di rete. L'host ID aiuta il router a trovare il percorso sulla rete LAYER3.

Analogie di Broadcast: L'indirizzo Broadcast **è un indirizzo che ha tutti "1" nel field dell'host**. **Quando** tu invii un pacchetto broadcast sulla rete, tutte le periferiche della rete, **vedono esso**. Per esempio, su una rete con id di **176.10.0.0**, il broadcast che può ragggiungere tutti gli host è **176.10.255.255**. Un indirizzo broadcast è molto simile al sistema postale. Il codice postale direziona la posta all'appropriata area, ed il broadcast address "current resident" devia ogni email sullo specifico indirizzo.L'indirizzo ip broadcast usa lo stesso concetto. Il numero di rete designato dal segmento, e il resto dell'indirizzo, dice ad ogni host che questo è un messaggio broadcast, e dice di fare attenzione al messaggio. Tutte le periferiche della rete, **riconoscono quello come host proprio**, come broadcast per la propria rete.

Host per le classi di IP: Ogni classe di rete ammette un fisso numero di host. Nella **CLASSE di rete A,** il primo ottavo è assegnato, escludendo gli altri tre ottavi (24bits), che sono assegnati agli host. Il numero massimo di host in una classe di rete A è 2 a 24, meno 2 (riservati per l'indirizzo di rete e l'indirizzo broadcast). O 16.777,214 hosts. In una rete a **CLASSE B** i primi 2 ottavi sono assegnati, lasciando gli ultimi 2 ottavi a disosizione degli host (16bit). Il massimo numero di host che la classe b può supportare è 2 a 16 meno 2. O 65,534 hosts. In una rete di **CLASSE C** i primi tre ottavi sono assegnati. Il restante octect è assegnato all'host. Il massimo numero di host è 2 a 8 meno 2. O 254 Hosts. Ricorda che **il primo indirizzo, in ogni rete è RISERVATO** all'attuale indirizzo di rete (network number) **e l'indirizzo finale in ogni rete è riservato per il broadcast.**

Classico indirizzamento IP: Gli amministratori di rete spesso **hanno bisogno di dividere le reti**, specialmente quelle larghe in piccole reti. Queste **piccole divisioni sono chiamate SubNetworks** ed hanno il compito di flessibilizzare la rete. La maggior parte delle volte, i **SubNetworks sono semplicemente riferiti al SUBNET**. Similarmente alla porzione di host, per le reti di classe A,B e C, il subnet sono assegnati Localmente, usualmente dall'amministratore di rete. Come l'indirizzo ip, **ogni subnet è unico.**

SubNetworks: Gli indirizzi subnet **includono la classe della porzione di rete A,B e C** più un subnet field ed un host field. Il subnet e l'host field sono

creati **dall'originale parzione dell'host per l'intera rete**. L'abilità di decidere come dividere l'originale partizione dell'host nel nuovo subnet e host fields apporta flessbilità di indirizzi per l'amministratore di rete. **Per creare il subnet address un amministratore prende in prestito dei bit dall'host originale e designa esso come subnet field**. Per creare un indirizzo subnet, un amministratore di rete prende dei bit dal field "host" e designa esso come "subnet field". Per creare un indirizzo subnet, un amministratore prende dei bit dal field dell'host e designa un subnet field. Il minimo numero di bit che possono essere presi, è 2. Se vuoi prendere solo 1 bit, per creare una subnet, avrai un numero di rete,0, ed un numero broadcast,1. Il massimo numero di bit che possono essere presi non c'è- Si possono prendere anche tutti ma bisogna lasciare le 2 cifre restanti per il numero host.
Motivazioni di subnetting: La prima ragione per ridure usare il subnet è **ridurre la dimensione del broadcast domain**. Il broadcast è inviato a tutti i nodi della sottorete. Quando inizia il traffico generato dal broadast esso consuma molte risorse e banda sula rete. Gli amministratori scelgono di ridurre il broadcast domain.

Subnet Mask: Il subnet mask (termine formale: **prefisso di rete esteso**), non è un indirizzo ma **determina quale parte dell'ip addres è network field e quale è host field**. Il subnet mask è un numero a 32 bit, diviso in 4 OCTECTS, separato da punti, proprio come gli indirizzi ip. Per determinare il subnet mask per una particolare rete, bisogna seguire questi procedimenti:1) **Esprimi il SubNetwork in formato Binario 2) Sostituisci la porzione di subnet dell'indirizzo con tutti "1" 3) Sostituisci la porzione di host dell'indirizzo con tutti "0". 4) Come ultima operazione riconverti tutti i numeri in decimale**. Per estendere il prefisso di rete, bisogna includere il numero di rete di classe A,B o C pià il campo del subnet (o numero subnet). Che è usato per estendere l'informazione di routing.

Operazioni Boolean, And, Or e Not: Il termine "operazioni" in matematica si riferisce a quelle regole che definiscono come un numero si combina con altri numeri. Le operazioni di numeri decimali includono addizioni, sottrazioni, moltiplicazioni e divisioni. Non sono relazionati ma differenti operazioni per lavorare co le numerazioni binarie. Le operazini base BOOLEAN sono AND, OR o NOT. **AND è una Moltiplicazione, OR è un'addizione, NOT cambia 1 e 0 su 0 e 1**.

Utilizzo della funzione AND: La più bassa numerazione nella rete ip è l'indirizzo di rete. Questo è anche applicabile al SUBNET. Il più basso numero dell'indirizzo è il numero del subnet. Per routeare il pacchetto, il router deve prima determinare l'indirizzo della rete di destinazione (subnet), performando un logico "AND" usando i'ip di destinazione ed il subnet mask. Il risultato sarà l'indirizzo subnet\ di rete.
Ip destinazione AND(moltiplicato) subnet mask = Indirizzo rete\subnet.

Range di Bit necessari per creare un Subnet: Per creare un subnet tu devi estendere la porzione di routing dell'indirizzo. Ad Internet la tua rete è nota nel suo insieme, ed è identificata come indirizzo di classe A, B, C, definiti in 8,16 o 24 bit di routing (numero rete). Il subnet field diventera un bit addizionakle, i routers riconosceranno vari subnet

come varie reti. Il numero minimo di BIT che può essere preso dall'host field per formare ils ubnet è 2. Il field subnet viene immediatamente dopo il network number.

1. destination. The minimum number of bits that you can borrow is 2, regardless of whether you're working with a Class A, B, or C network[1]. Because at least 2 bits must remain for host numbers[2], the maximum number of bits borrowed varies by address class.

Address Class	Size of Default Host Field	Maximum Number of Subnet Bits
A	24	22
B	16	14
C	8	6

Determinare la dimensione del Subnet MASK: Il subnet mask usa lo stesso formato dell'indirizzo ip. Esso **è lungo 32bit** ed è diviso da 4 punti, scritto in formato decimale. Il subnet mask **contiene tutti 1 nella posizione di rete** (determinato dalla classe di indirizzo), e **contiene tutti 0 nella restante posizione** designata per gli host. Di default se tu non prendi un bit, il subnet mask di classe b sarà 255.255.0.0, che è l'equivalente decimale di 1, nei 16 bit della porzione di rete di classe B. Se 8 bit venissero preso dal campo SUBNET, il subnet mask includerebbe 8 addizionali 1 a diventerebbe 255.255.255.0. Per esempio, il subnet mask 255.255.255.0 è associato all'indirizzo di classe B 130.5.2.144, il router saprà di dover forwardare il pacchetto alla sottorete 130.5.2.0, piuttosto che sulla rete 130.5.0.0. Un altro esempio nell'indirizzo di classe C 197.15.22.131, con subnet mask 255.255.255.224. Con il valore di 224 sulla ottava finale(111000000 binario). La classe C di 24 bit network portion è stata estesa di 3 bit per fare un totale di 27 bits. Il 131 nella ottava rappresenta il terzo host utilizzabile nella sottorete 197.15.22.128. I routers in internet che non conoscono il subnet mask, si preoccuperanno solo di portare queste in formazioni sulla rete di classe C 197.15.22.0, mentre il router dentro la rete, conosce il subnet mask e vedrà i 27 bit per effettuare la decisione finale di routing.

Subnet ed IP address: Quando prendi i bits dal campo dell'host, è importante notare che **il numero addizionale di subnet è creato ogni volta che prendi un bit in più**. Tu hai già imparato che non puoi prendere solo un bit bensì un minimo di 2. Prendendo 2 bit, crei 4 possibili subnet 2alla2. (ma devi sempre ricordarti che ce ne sono 2 riservati ed inutilizzabili). **Ogni volta che tu prendi un altro bit dal field dell'host, il numero del subnet aumenta** di ESPONENTE 2. Le otto possibili subnet che sono create prendendo 3 bit sono uguali a 2 ALLA 3. Le 16 possibili subnet create vengono fuori, prendendo 4 BIT, cioè 4 ALLA 4. Per questi esempi è facile vedere che **ogni vlta tu prendi un altro bit dal campo host, il numero di possibili subnet, RADDOPPIA**.

Host per SubNetworks: Ogni volta che tu prendi un bit dal campo host, c'è un bit in meno in tale campo che può essere usato per la numerazione host. Specialmente ogni volta che prendi un altro bit dal campo host, **il numero di host address che puoi assegnare, diminuisce di POTENZA2** (viene diviso

a metà) Per aiutarti a capire come funziona, usa un indirizzo di rete di classe c, come esempio. Se non c'è submask, tutti gli 8 bit nella octect sono usati dal campo host. Quindi ci sono 256 (2 alla 8) possibili indirizzi assegnabili all'host -2. Immagina che in questo caso, la rete di classe C è divisa in sottoreti, tu prendi 2 bit dal campo di 8bit di default, e la dimensione del campo host diminuisce fino a 6bit. Se tu scrivi tutte le possibili combinazioni nei restanti 6 bit, vedrai che il numero dei possibili host che si possono comporre è ridotto a 64. 2 alla6. Il numero effettivo quindi è 62. Nella stessa rete di classe c, si prende 3 bit, il campo host decresce fino a 5 bits il il nmero di host che è possibile ottenere è 32 2 alla 5. Che poi sarebbero 30. Il numero dei possibili indirizzi host che possono essere assegnati alla sottorete è relazionato al numero di sottoreti che sono state create. Nella rete di classe C, per esempio se il subnet mask di 255.255.255.224 è applicato, si ha 11100000. (3 bit), i restanti 5 bit sono per gli host. Quindi 5alla2, 32, 30 usabili. Sottoreti create=6.

Operazioni Boleand: Come hai già imparato la più bassa numerazione ip, è lo stesso indirizzo di rete. Il numero di rete nei campi network e nel campo host, zero. Questo può anche essere applicato nelle subnet. Il più basso numero di indirizzi, è l'indirizzo del subnet. Per fare il routing dei pacchetti, il router prima determina la rete di destinazione (subnet). Per completare questa informazione il router **esegue un ANDing utilizzando l'ip di destinazione ed il subnet mask della rete.** Immagina che hai un arete di classe B, l'indirizzo di rete è 172.16.0.0. Dopo aver assegnato il necessario per la tu rete, tu decidi di prendere 8bit per creare un subnet.. Come abbiamo imparato in precedenza, prendendo 8 bit, in una rete di classe B, il subnet mask è 255.255.255.0. Esternamente la rete invia i dati all'ip 172.16.2.120. Per determinare dove portare i pacchetti, il **router fa l'Anding di questo indirizzo con il subnet mask**. Quando questi 2 numeri sono ANDed, la porzione di host che ne risulta è sempre ZERO 0. Il restante è il numero di rete, includendo il subnet. Quindi i dati vengono inviati al subnet 172.16.2.0 e solo la parte finale dice al pacchetto che deve essere trasportato all'host 120 di tale rete. Immagina di avere la stessa rete 172.16.0.0. Questa volta decidi di prendere 7 bit dal campo subnet. Il numero binario sarà 11111111.11111111.11111110.00000000 Che cosa potrebbe avere questo in annotazione decimale? Ancora qualocuno fuori dalla rete invia i dati all'host 172.16.2.120. Per determinare dove i dati andranno a finire di preciso, il router AND questo indirizzo con il subnet mask. Quando i numeri sono stati "ANDed", la risultante porzione di host è 0. Qual è la differenza in questo secondo esempio..? Bisogna vedere la cosa dal punto di vista decimale. LA differenza è nel numero di subnet disponibili. E nel numero di host che possono esserci in ogni subnet. Tu puoi solo vedere questo pargonando i 2 differenti subnet mask. Con 7Bits nel campo subnet, ci sono solo 126 sottoreti. Quanti host possono esserci in ogni subnet? Quanto è lungo il campo host? Con 9 bit per i numeri host, ci possono essere 510 hosts in ognuna delle 126 subnet.

Configurazione ip su un diagramma di rete: Quando tu configuri i routers, devi connettere ogni interfaccia ad un diverse segmento di rete. Quindi ognuno di questi segmenti avrà una separata SUBNET. Tu puoi selezionare un indirizzo da ogni differente subnet per assegnarla all'interfaccia del router che connette

tale subnet. Per ogni segmento di rete, cavo o links, ci sono vari MEMBRI di un subnet\network.

Schemi dell'host\subnet: Una decisione importante che devi prendere quando decidi di creare subnet è determinare QUANTI subnet vuoi creare e quanti host ci sono sulla rete.Determinare un numero ottimale. Hai già imparato che non puoi usare il primo e l'ultmo subnet. Tu non puoi anche usare il primo e l'ultimo indirizzo all'interno di ogni rete. Uno è l'indirizzo Broadcast per quel determinato subnet, e l'aaltro è la parte di indirizzo della rete. Quando tu crei un subnet, tu perdi un po' di potenziali indirizzi. Per questa ragione, gli amministratori di rete **dovranno fare molta attenzione**, considerando il numero degli indirizzi che si perderanno creando le subnet. Esempio, tu puoi prendere 2 bit in una rete di classe C. Puoi creare 4 subnet. Ognuna di esse con 64 hosts. Solo 2 di queste subnet sono utilizzabili e solo 62 hosts sono utilizzabili per la subnet, restano quindi 124 host utlizzabile su 254 possibilità che si avevano prima di scegliere la subnet. Stai quindi perdendo il 51 percento dei tuoi indirizzi utili. Immagina, questa volta, di prendere 3 bits. Adesso tu hai 8 subnet, di cui solo 6 solo utilizzabili, con 30 host utilizzabili per rete. Questo da a te un totale di 180 hosts, contro i 254 che avevi prima di scegliere di usare il subnet, perdi quindi il 29 percento dei tuoi indirizzi. Quando tu crei un subnet, tu devi fare considerazione futura, sulla crescita, in percentuale della rete e sui pc che perderai. (percentuale)

Indirizzi privati: Ci sono certi indirizzi in ogni classe di indirizzi ip che **non sono assegnati**. Questi ndirizzi **sono chiamati INDIRIZZI PRIVATI**. Gli indirizzi privati, possono **essere usati** dagli host cheusano Tanslazioni degli indirizzi di rete **(NAT), o server proxy**, per connettersi a reti pubbliche, o dagli host non connessi ad internet. Molte applicazioni hanno bisogno di connettività solo all'interno di un arete, e **non necessitano di connettività esterna**. In reti di grandi dimensioni, il tcp\ip, è spesso usato, sempre quando la connettività lato network esterna non è necessaria. Ottimi esempi possono essere le Banche. Esse possono usare tcp\ip per connettersi automaticamente **macchine richiedenti (automatic taller machines) (ATMs).** Queste macchine non si connettono a reti pubbliche, gli indirizzi privati sono utili a questo.

Routers: Nel networking ci sono 2 schemi di interizzi. Il primo è il mac address o data link, di livello 2. Il secondo è livello 3, NETWORK. **Un esempio di livello 3 è l'ip address**. Il router è un tipo di periferica di int3ercomunicazione che **passa i pakketti da rete a rete basandosi su indirizzo di livello 3**. Il router ha **un'abilità intelligente** di decidere per forwardare le info sulla rete.

Layer 3 Indirizzi: I bridge e gli switches usano tipicamente il mac per decidere. Il routersi utilizzano lo schema di indirizzo di livello 3 per prendere decisioni. Essi usano ip o indirizzo logico, anziché il mac address. Ip è implementato via software, e si riferiscono alla rete su cui sono installati. Questi indirizzi livello 3 sono riferiti ai protocolli di indirizzi o indirizzi di rete. Un indirizzo fisico o mac address è usualmente assegnato dai produttori della NIC, ed è codato nella stessa nic. L'amministratore di rete, usualmente assegng li indirizzi ip. Infatti spesso gli amministratori di rete **raggruppno assieme le periferiche, per ip, dividendole a seconda della posizione geografica,**

ufficio, edificio. IP è implementato via software ed è facilmenre modificabile. Il bridge e lo switch è primariamente usato per connettere segmenti di rete. I routers sono usati per connettere separate reti e per accedere allo worldwide internet. Essi servono ad attuare, un END to END routing.

Numero unico di rete: I routers connettono 2 o più reti, ognuna di queste deve avere **un numero unico di rete** poiché il routing abbia successo. Il numero unico di rete è incorporato **all'interno dell'indirizzo ip** che è assegnato ad ogni periferica **collegata alla stessa rete**.

Interfaccia router\port: Il collegamento della rete **è chiamato INTERFACCIA**.Può essere riferito **alla stessa porta**. Nell'ip routing **ogni interfaccia** può avere un **separato** ed unico **indirizzo** di rete (o subnetworks).

Metodi per l'assegnazione degli indirizzi ip: Dopo che hai determinato lo schema di indirizzi per una rete, tu devi scegliere il metodo **per assegnare gli indirizzi ai pc**. Ci sono essenzialmente due metodi per assegnare gli indirizzi. **STATIC ADDRESSING e DINAMIC ADDRESSING**. Riguardo o meno lo schema di assegnazione che usi, **il pc DEVE avere un indirizzo ip e 2 macchine non possono avere lo stesso ip**. STATIC ADDRESSING: Se tu assegni un ip statico, tu devi andare su ogni individuale macchina e configurare essa con l'indirizzo ip. Questo metodo richiede di appuntarsi meticolosi records, perché usando due ip sono uguali possono verificarsi gravi errori sulla rete. Molti sistemi operativi con win95,winNT, inviano una richiesta ARP per controllare gli ip duplicati, quando essi vanno ad inizializzare TCP\IP. Se essi trovao un duplicato, il sistema operativo non inizializza TCP\IP e genera un messaggio di errore; Tenere dei record è assai importante perché non tutti i sistemi operativi indentificano doppio ip. DYNAMIC ADDRESSING: Ci sono molti differenti metodi per assegnare l'indirizzo ip dinamicamente. **Reverse address resolution – RARP**. **Combina gli indirizzi mac agli indirizzi ip**. Questa combinazione permette a molte periferiche di rete di encapsulare **i dati prima di spedirli sulla rete.** Una periferica di rete come ad esempio una workstation senza disco, può conoscere il proprio mac ma non il proprio IP. LE periferiche che utilizzano RARP hanno **bisogno che il RARP server sia presente sulla rete per rispondere alle loro richieste RARP**. Quando una periferica **vuole inviare un pacchetto** ad un'altra periferica, nel nostro esempio la periferica conosce il proprio mac address, ma non è in grado di localizzare il proprio ip nella tabella ARP. Per permettere alla periferica di destinazione, il retrieving dei dati, passa esso ad un livello più alto del modello osi e risponde alla periferica. La risposta deve includere il mac e l'ip address. La sorgente inizia un processo chiamato **RARP REQUEST**, che aiuta a rilevare il proprio ip address. La periferica costruisce un RARP request packet ed invia esso fuori sulla rete. Per essere sicuri che tutte le periferiche vedano la rarp request è usato un broadcast di ip. RARP usa lo stesso formato di pakketto dell'ARP. Ma in RARP, la richiesta, il mac header , l'ip header e l'operazion code sono diversi dalla richiesta ARP. Il pacchetto RARP contiene parti del MAC address per destinazione e sorgente.Il campo ip sorgente è vuoto. Il broadcast raggiunge tutte le periferiche della rete, quindi l'ip di destinazione delle periferiche sarà settato secondo tutti binari "1".I pc che stanno usando RARP hanno codato le

informazioni in rom che direzionano essi verso la start del processo e la localizzazione dell'RARP server. **BOOTSTRAP protocol - bootp:** Una periferica usa BOOTstrap Protocol quando essa inizia ad ottenere un indirizzo. BOOTP **usa l'udp** per portare il messaggio. Il messaggio UDP è incapsulato all'interno di un datagramma IP. Un computer usa BOOTP per inviare un broadcast ip datagram- Im bootp server riceve il broadcast e quindi invia un broadcast. Il client riceve un datagramma e controlla il MAC ADDRESS. Se esso trova il proprio max nella destinazion address field, esso prende l'ip in quel datagramma. Come il RARP, anche il BOOTP opera in , classico sistema Client-SERVER, e richiede solo lo scambio di un singolo pacchetto. RARP invia indietro solo i 4 octect dell'ip address, BOOTP datagrams può includere l'ip address, l'indirizzo ip delo router (gateway), l'indirizzo del server, ed il campo specifico del venditore. Uno dei problemi con il BOOTP è che esso **non è designato per fornire indirizzi dinamici**. Con il BOOTP tu crei una configurazione che specifica i parametri per ogni periferica. **Dynamioc HOST configuration PROTOCOL – DHCP:** DHCP è stato proposto come successore al BOOTP, per sfortuna di Bootp, **dhcp permette ad un host di ottenere un indirizzo ip rapidamente** e dinamicamente. Per fare ciò è richiesto un dhcp, un range definito di indirizzi da assegnare, ed un dhcp server. **Gli host che arrivano online, contattano il dhcp server e richiedono l'indirizzo**. Il dhcp server sceglie un indirizzo e lo assegna all'host. **Con il dhcp l'intera configurazione di un computer può essere ottenuta con 1 messaggio**. (il server può anche trasmettere il subnet mask).

Sequenza di inizializzazione del Dhcp: Quando un dhcp client parte,**boost**, esso inizia ad inizializzare il proprio stato (**initialize state**). Esso invia un **DHCP-DISCOVER** broadcast message, che è un pacchetto UDP con il numero della porta settato dal BOOTP port. Dopo aver inviato un DHCPDISCOVER packet , il client si sposta in un **SELECT STATE**, e raccoglie la **DHCP OFFER** responde dal dhcp server. A questo punto entra in **Request state**. Il cliente che ha scelto la prima riposta, riceve e negozia con il dhcp server inviando una **DHCPREQUEST** packet. Il dhcp server conferma la richiesta. Il client richiede un **DHCPACK** packet. Il client a questo punto si sposta in **Bound State** ed inizia ad usare l'indirizzo.

Componenti chiave IP: Per permettere alle periferiche di comunicare, la periferica che invia ha bisogno sia dell'indirizzo ip che del mac address della periferica di destinazione. Quando essa priva a comunicare con l'ip address che conosce, essa può determinare il mac address. **Il tcp\ip ha un protocollo chiamato ARP, che può automaticamente ottenere il mac address**. ARP abilita un computer a trovare il mac address di un altro computer che è associato ad un indirizzo ip.L'unità base di trasferimento, **nell'ip è IP PACKET**. Packet preccessing avvieene in software. Il pacchetto è diviso in 2 maggiori componenti. **Heade**r che include sorgente e destionazione (Addresses), e la data. Altri tipi di protocollo hanno i propri formati. Il pacchetto IP è unico con IP. Un altro maggiore componente dell'ip è INTERNET **CONTROL MESSAGE PROCOL (ICMP).** Questo protocollo è usato da una periferica per riportare il problema all'inviatario del messaggio. Per esempio se un router riceve un pacchetto che non è deliverabile, esso invia un messaggio indietro all'inviatario del pacchetto. Una delle numerose funzioni **del'ICMP è ECHO REQUEST\ECHO REPLY** che è un modo per testare se il pacchetto può arrivare a destinazione, pingando la destinazione.

Funzione di ARP: Il protocollo di livello 3 determina il passaggio dei dati dal layer network ai livelli più alti nella rete. Un pacchetto deve contenere il mac e l'indirizzo ip di destionazione. Se

qualcosa manca, il dato non passa dal layer3 ai livelli superiori. In questo modo l'indirizzo mac, e l'ip controllano per un bilanciamento di se stessi. Tutte le periferiche determinano l'indirizzo ip della periferica di destinazione, inoltre essi aggiungono alla tavola di indirizzi anche il mac address. C'è una varietà di modi per cui una periferica può determinare il mac. Essa necessita di esso per effettuare l'encapsulation. Le tavole ARP (address resolution protocool), fanno corrispondere ogni ip al pc. Le tavole ARP sono una sezione della memoria ram. Una sorta di cache mantenuta dalle stesse periferiche. Occasionalmente puoi inserire la tavola ARP manualmemnte. Ogni computer sulla rete mantiene la propria tavola ARP. Quando una periferica, sulla rete vuole inviare tramite la rete essa usa la informazioni prese dalla tabella ARP. Per determinare il mac dall'indirizzo ip, si consulta la tabella ARP.

Operazioni ARP con il Subnet: Se un host vole inviare dei dati ad un altro host, esso deve conoscerne l'indirizzo ip. Se esso non è in grado di localizzare il mac addres per la destinazione **nella sua Tavola ARP, l'host inizializza un processo chiamato AN ARP REQUEST**. An Arp richiede di abilitare esso a scoprire il mac address di destinazione. L'host **costruisce la richiesta ARP packet** e la invia a tutte le periferiche sulla rete. Per essere sicuro che tuttte le periferiche vedrano l'arp request, la sorgente effettua **un broadcast MAC ADDRESS**. Il broadcast in mac address scheme, ha tutte posizioni in esadecimali F. Quindi un mac broadcast avrà la forma **FF-FF-FF-FF-FF-F**F. Poiché il pacchetto di richiesta ARP possa viaggiare in modalità broadcast, tutte le periferiche della rete locale, ricevono il **pacchetto e lo possono al livello di rete successivo** per esaminarlo meglio. Se un indirizzo ip di una periferica coincide con l'ip richiesto da ARP, questa periferica risponde inviando il proprio MAC address. Questo processo è chiamato **ARP REPLY**. ESEMPIO:-La periferica sorgente 197.15.22.33 sta chiedendo il mac address di destinazione con l'ip 197.15.22.126. La periferica di destinazione prende la richiesta ARP e rispode con un ARP REPLY indicando il proprio mac. Da quando la periferica origine, **riceve l'ARP REPLY, essa estrae l'indirizzo mac dal mac header e aggiorna la propria tabella ARP**. La periferica di orgine può organizzare l'ip ed il mac in una tabella. Subito dopo viene eseguito un LAYER2 e LAYER3 encapsulation dei dati prima che essi possano essere buttato fuori oltre la rete. Quando i dati arrivano a destinazione, il livello data lynk, effettua un paragone, divide il mac header e lo trasferisce al livello di rete.La rete esamina i dati e vede che questo indirizzo ip è uguale all'indirizzo ip di destinazione contenuto nell'ip header. Il livello NETWORK, divide l'ip header e trasferisce i dati incapsulati nel prossimo livello più alto del modello osi. (LIVELLO4). Questo processo è ripetuto fino a che il resto del pacchetto non ha parzialmente decasulato i dati, tant da raggingere l'applicazione dove essi verranno letti.

Gateway di default: Per comunicare con altre apparecchiature sulla rete tu devi effettuare ciò con un **DEFAULT GATEWAY**. Un default gateway è un indirizzo ip di un interfaccia sul router che **connette il segmento di rete** sul quale gli host che si vogliono raggiungere sono locati. Il L'ip del default gateway **può essere nello stesso segmento** della periferica **SORGENTE**. **Se non è definito nessun default gateway** la comunicazione è possibile **solo sulle periferice di quella determinate rete** (segmento logico) Il computer che invia i dati non trova paragone fra l'inidirizzo ip della destinazione e **la propria ARP TABLE**. Dunque non trova la macchina. **Senza** il default gateway, **non si riesce a determinare il MAC** della macchina ed il pacchetto è inconsegnabile. Uno dei maggiori problemi nel networking è COME comunicare con le periferiche che non si trovano sullo stesso segmento di rete. Ci sono 2 problemi. Il primo è ottenere l'indirizzo mac della macchina di destinazione. Il secondo è trasferire i pacchetti da un segmento ad un altro, della rete. **ARP utilizza BROADCAST packets** per completare la propria funzione. **I router comunque non forwardano i broadcast**. Quindi per una periferica, inviare dati ad un indirizzo di una periferica che è su un altro segmento di rete è possibile, ma **deve esistere un default gateway**. Il gateway è l'ip della periferica che fa ROUTING sull'altra rete. La sorgente host **paragona l'ip di destinazione con il proprio ip**

e determina se i 2 ip sono locati sullo stesso segmento. Se i 2 ip sono su **2 segmenti diversi, vengono inviati i dati al GATEWAY.**

Il proxy ARP: E' una variante del protocollo ARP. In questo caso una periferica intermedia (un router ad esempio) invia una risposta ARP nell'interesse di un nodo finale. **Il routers che esegue PROXY ARP, cattura gli ARP packet**. Essi rispondono con il mac address di questi pc che non sono alla portata del singolo segmento di rete. Nella precedente desrizione su come i dati possono essere inviati **ad host di differenti segmenti o sottoreti**, **il defaulg gateway è configurato**. Se la sorgente non ha un default gateway configurato Essa invia una ARP REQUEST. Tutti gli host del **segmento incluso il router, riecvono questa ARP REQUEST**. **Il router paragona l'indirizzo ip di destinazione con l'indirizzo subnet e determina se questo indirizzo e nello stesso segmento di rete o meno. Se il segmento di destinazione è lo stesso, il router SCARTA IL PACCHETTO**. La ragione per cui il pacchetto è scartato è **xkè l'indirizzo ip è nello stesso segmento**. Questo permette alla periferica di **rispondere DIRETTAMENTE** alla richiesta ARP. L'eccezione su questo è quando l'idirizzo ip non è al momento ASSEGNATO, per cui ciò genera un errore. Se il subnet è differente il router risponderà con il mac della periferica che è direttamente connessa al segmento dove il router è locato. **Questo è PROXY ARP**. Dal momento in cui il mac address non è disponibile per la **destinazione il router ripara a questo inconveniente inserendo il mac nel pacchetto. Dunque il router FORWARDA la richiesta ARP** sulla adeguata sottorete. (badandosi sull'ip)

Routed Protocols: Ip è un protocollo lato NETWORK (3) e poichè è livello 3, esso **può essere Forwardato** su altre reti. Di rete in rete. I protocolli **che hanno questa possibilità sono chiamati ROUTED e ROUTABLE PROTOCOLS**. Il protocollo più comune e più usato è IP.Spesso ci si concentra su ip ma è importante conoscere **tutti i ROUTABLE protocols. Due sono IPX\SPX e AppleTalk**. I protocolli come ad esempio, ip, IPX\SPX e apple talk, forniscono un supporto per livello3 e sono routabili. Comuque ci sono protocolli che **non supportano ufficialmente il livelo3.** Questi sono chiamati **Non-Routable-Protocols**. Il più comune dei non routable protocols, sono NETBEUI. NETBEUI è piccolo, veloce ed efficiente, limitato ad un solo segmento.

Caratteristiche dei protocolli Routabili: Un protocollo, per essere **ROUTABILE** deve avere l'abilità di **detenere un Indirizzo di rete, un indirizzo di host, per ogni individuale periferica**. Molti protocolli come ad esempio **IPX, hanno bisogno solo del numero di rete**, perché essi **usano host's mac address** per il numero fisico. Altri protocolli come ip **vogliono un completo indirizzo, della rete e dell'host, e chiedono anche un SUBNET MASK**. L'indirizzo di rete è ottenuto con l'operazione di ANDING fra l'indirizzo ed il subnet mask.

Esempi di protocolli di Routing: I protocolli di routing (non confondersi con ROUTED PROTOCOLS) determinano il percorso che il Routed protocols deve seguire per raggiungere la destinazione. Esempi di routing protocols includono il Routing Information Protocol (RIP) l'interiore gateway routing protocol (IGRP), L'enhanced interiore gateway routing protocol (EIGRP) e Open Shortest path First (OFPF). I routing protocols abilitano i router che è connetto a creare una mappa, internamente degli altri ruters della rete su intenet. Questo permette il ROUTING, selezionando il percorso migliore. Tali mappe fanno parte della routers routing table.

Le funzioni del Routing Information Protocol: I routers utilizzano il protocollo per scambiare le tavole di routing e condividere le informazioni di

routing. Dentro la rete il protocollo più comune per trasferire le informazioni di routing fra routers è locato nella stessa rete ed è chiamato ROUTING INFORMATION PROTOCOL (RIP). Questo INTERIORE GATEWAY PROTOCOL (IGP) calcola le distanze dalla destinazione per sapere QUANTI HOPS un pacchetto deve passare. RIP abilita i routers a ipdatare la propria tabella di routing ad intervalli programmabili, ogni 30 secondi. Uno svantaggio del router che utilizza RIP è che esso è costantemente connesso agli altri routers nelle vicinanze, per updatare le routing tables, per cui ciò crea un enorme ammontare di traffico sulla rete. RIP permette ai routers di determinare quale parte della rete trasmette i dati. Esso effettua ciò usando un concetto conosciuto come DISTANCE-VECTOR. Quando i dati passano attraverso i router, attraversando nuove reti e passando per nuovi network numbers, questo è considerato un HOP. (uguale ad un hop). Un percorso ha un conteggio degli hop, per indicare che i dati stanno viaggiando attraverso un percorso che passa da routers, prima di raggiungere la destinazione finale sulla rete. Se ci sono miltipli percorsi per arrivare a destinazione il percorso con l'ultimo numero di hops dovrà essere un percorso scelto dal router. Il conteggio degli hop è solamente un misurazione utilizata da RIP. Non è necessario selezionare il percorso più veloce per arrivare a destinazione, La METRIC è la misurazione per effettuare le decisioni. Altri routing protocols usano numerose altri conteggi di hop per scegliere il miglior percorso per i dati.RIP resta molto popolare ed implementato. E' uno dei protocolli che è stato sviluppato più presto. Un altro problema è sull'uso di RIP. La destinazione spesso può essere locata troppo altrove ed essere irraggiungibile. Usando RIP il numero massimo di hop che i dati possono percorrere è 50. La rete di destinazione è considerata irraggiungibile se per arrivare all'host finale bisogna passare più di 50 hops.

Sequenza di incapsulamento e routing: Al livello data lynk, un pacchetto ip **è incapsulato in frame**. Il datagram (packet) include ip header ed i dati. Il router riceve i frame, spoglia il frame header, e controlla l'ip di destinazione nell'header dell'ip. Il router quindi cerca l'indirizzo ip di destinazione nella propria tabella dei routing, incapsula i dati nel data lynk frame e li invia all'appropriata interfaccia. Se non trova l'indirizzo ip, il pacchetto è distrutto.

Routing multi protocollo: I routers sono capaci di supportare protocolli di routing multipli ed indipendenti, e mantenere tavole per diversi routed protocols. Questa possibilità permette al router di portare pacchetti a diversi routed protocols al di là della stessa data lynk.

Servizi di ConnectionLESS: Molti servizi di rete utilizzano il sistema di delivery ConnectionLESS. Esso tratta ogni pacchetto separatamente ed invia esso tramite un percorso sulla rete. Il pacchetto può percorrere differenti percorsi tramite la rete, ma è reassemblato quando esso arriva a destinazione. Nel sistema delle connessioni la destinazione non è informata che il pcchetto è inviato. Una buona analogia per il connectionLESS system è il sistema postale. Il recipiente non è contattato dopo che la lettera è inviata da una destinazione all'altra. La lettera è inviata su quella via ed il recipiente saprà che essa arriva quando è già arrivata.

Servizio di ConnectionORIENTED: Nella connession oriented, una connnessione è stabilita quando l'inviatario ed il destinatario hanno stabilito la

connessione ed hanno trasferito alcuni dati. Un esepmpio, nel sistema telefonico, tu fai una chiamata, la connessione è stabilita quando la comunicazione avviene.

ConnectionLESS e ConnectionORIENTED: I processi di rete ConnectionLESS sono quasi sempre riferiti ai PACKET SWITCHED, in questi processi un pacchetto passa dalla sorgente alla destinazione, esso può switchare da differenti percorsi fino a che non arriva alla destinazione. Le periferiche creano la determinazione del percorso, per ogni pacchetto, basandosi su una varietà di criteri. Alcuni criteri, possono differenziare pacchetto da pacchetto (banda). Il processo di rte per connectioORIENTED, invece, è quasi sempre riferito a CIRCUIT SWITCHED. Questi processi stabiliscono la connessione con la destinazione e poi effettuano il trasferimento. Tutti i pacchetti viaggiano in sequenza sullo stesso circuito fisico o più comunemente sullo stesso CIRCUITO VIRTUALE. Internet è una delle tante CONNECTIONLESS, in cui i pacchetti sono guidati da IP. TCP aggiunge servizi di connection oriented sulla cima di IP. Il segmenti sono incapsulati in pacchetti ip per trasportare i dati attraverso internet. TCP provvede sessioni connectionORIENTED, per assicurare la consegna dei dati.

IP, utilità di TRASPORTO: IP è un sistema ConnectionLESS. Esso tratta ogni pacchetto indipendentemente. Per esempio se tu usi un programma FTP per scaricare un FILE, ip non invia il file in un lungo flusso di dati. Esso tratta ogni pacchetto indipendentemente. Ogni pacchetto può viaggiare per differenti percorsi. Alcuni possono essere persi per sempre. IP conta sul protocollo dell stato di trasporto quali pacchetti sono stati persi e richiede di nuovo la trasmissione. Il livello TRANSPORT è anche responsabile per il reordino dei pacchetti.

Periferiche di rete e TABELLE ARP: Un’interfaccia o la porta che risiede dove il router si connette alla rete, è considerata parte della rete. Quindi l’interfaccia router, connessa alla rete, ha un indirizzo ip per ogni rete. I routers e le altre periferiche sulla rete, inviano e ricevono dati sulla rete e COSTRUISCONO delle Tabelle ARP, che associano gli ip con i mac address.

Tabelle ARP: I routers possono essere collegati a reti multiple o sottoreti. Generalmente parlando con periferiche di rete, mappa l’ip addres ed il mac, che essi vedono su base regolare. In questo modo, ogni periferica contiene la mappa delle informazioni relativa solo alle periferiche che stanno in quella determinata rete. Essi conoscono molto poco sulle periferiche al di là della propria rete. I routers costruiscono tavole che descrivono la rete connessa ad esso. Le tavole ARP possono offrire ai router la possibilità di tenere informazioni su IP e MAC anche di altri pc collegati alla rete interna, di altre RETI.E’ importante per il router conoscere informazioni di altri pc su altre reti al fine di raggiungerli quando viene loro inviato un pacchetto.

Altre Tavole di indirizzi per i routers: Che cosa accade se un paccheto raggiunge un router che è destinato ad una rete che non è connessa? Oltre all’indirizzo ip ed al mac, delle periferiche localizzate sulla rete, esso connette anche router che posseggono ip address e mac di altri routers. Esso usa questi indirizzi per portare i dati fino a destinazione. **Se un router riceve un pacchetto la cui destinazione non è nella routing table, esso forwarda**

tale indirizzo ad un altro router che può contenere l'informazione riguardo la destinazione di routing table per quell'indirizzo.

Richieste ARP e Risposte ARP: ARP è usato solo sulla rete locale. Che cosa accade se un router locale vuole chiedere ad un router nn locale, il servizio di ROUTING indiritto, ma non conosce il mac di questo router non locale? Quando un router non conosce l'indirizzo mac del router sul Prossimo HOP, il router sorgente instaura una richiesta ARP. Il router che è connesso allo stesso segmento, della sorgente riceve la richiesta ARP. Il router quindi risponde alla richiesta arp. Questa risposta contiene l'indirizzo mac del NON LOCAL router.

Proxy ARP: Una periferica su una rete non può inviare una richiesta ARP ad una periferica su un'altra rete. Puoi immaginare la ragione di ciò? Che cosa accade nel caso di una sottorete? Può una periferica su una sottorete trovare il mac address di una periferica su un'ALTRA sottorete? La risposta è Sì. La sorgente effettua una richiesta al Router. Questo servizio di informazioni ARP che il router fornisce, è chiamato PROXY ARP, e permette al router di diventare il default GATEWAY.

Routing indiretto: Spesso una sorgente risiede su una rete che ha un numero differente da quello della destinazione desiderata. La sorgente non conosce l'indirizzo mac della destinazione. Essa deve quindi usare un servizio dal router. Con il router che richiede i dati alla destinazione è possibile attuare comunque una comunicazione. Il router che è usato per questa funzine è definito DEFAULT GATEWAY. Per ottenere un servizio, da un default gateway, una sorgente encapsula i dati che contengono il mac address del router di destinazione. La sorgente può usare l'ip di destinazione della macchina di destinazione, non quello del router, perché il pacchetto dev'essre inviato alla periferica host non al router! Quando il router prende i dati, esso li spoglia, preleva le informazioni DATA LINK che sono usate per l'incapsulazione. Esso quindi passa i dati al lato network mentre esamina l'ip di destinazione. Esso paragona l'indirizzoo ip, con l'informazione contenuta nella taella di routing. Se il router localizza localizza la mappatura MAC\IP, esso sa che la LOCATIONS di destinazione è collegata ad una delle sue porte, esso encapsula i dati con con l'indirizzo mac e li forwarda alla corretta destinazione. Se il router non può localizzare la destinazione mappata dell'indirizzo MAC della macchina, esso localizza l'indirizzo su un'altra tabella do routing di altri router e forwarda i dati sull'altro router. Questo tipo di routing è chiamato INDIRECT ROUTING.

Routed Protocols e routing protocols: I protocolli sono come il linguaggio. IP è un protocollo che appartiene a livello NETWORK. IP ha la possibilità di essere ROUTATO sulle reti per cui è chiamato ROUTED PROTOCOL. Altri esempi: Ipx\appletalk. I routers usano i routing protocols per scambiare tavole di routing e condividere informzioni di routing.In poche parole, o routing protocols determinano come i routed protocols sono routed. Esempi di routing protocols. RIP-Routing information protocol,IGRP interiore gateway routing protocol,EIGRP-enhanced interiore gateway routing protocol,OSPF-open shortest path first.

IGPS e EGPS: I tipi di routing protocols sono Exteriore Gateway Protocols (EGPs) e interiore gateway protocols (IGPs). L'exterior, routa i dati tramite sistemi autonomi. Esempi di EGP è BGP

(border gateway protocol), il primario esteriore routing protocol di internet. Esempi di IGPs sono: RIP,IGRP,EIGRP,OSPF.

RIP: Il metodo più comune per trasferire le informazioni di routing fra routers che sono locati sulla stressa rete è RIP. Questo Interiore Gateway Protocols, calcola la distanza a destinazione. RIP permette ai routers che usano questo protocollo di UPDATARE la propria tavola routing, ad intervalli programmabili. Tipicamente questo ogni 30 SECONDI. Poiché esso è costantemente connesso ai router, può causare molto traffico. RIP permette ai router di determinare quale percorso verrà usato per inviare i dati, basandosi sul concetto di conoscenza DISTANZA-VETTORE. Quando i dati viaggiano su di un router ed attraversano un'altra rete (altro numero di rete), è considerato che essi hanno viaggiato un HOP. Il percorso ha un conteggio degli hop (esempio 4) per indicare che i dati viaggiano attraverso un percorso, per cui 4 routers sono stati passati prima di arrivare alla destinazione finale. Se ci sono moltipli percorso per la destinazione, usando RIP, viene selezionato il percorso con il numero minimo di hop. Viene utilizzato il conteggio degli hop, che conta soltanto il "routing metric", usato dal ripo, quindi non è necessario scegliere il percorso più veloce. RIP resta il protocollo più più utiilizzato e perfezionato, è stato tirato fuori prima. Un altro problema, usando rip, è la destinazione. Essa può essere locata troppo lontana perché i dati possano raggiungerla. Con il RIP, il massimo numero di hop passabili è 50. Se la destinazione supera questo numero di hops è considerata non raggiungibile.

IGRP e EIGRP: Sono dei routing protocols inventati da CISO SYSTEMS, essi sono considerati routing protocols proprietari. IGRP è stato realizzato specificatametne per i problemi di indirizzi associati con routing su grandi Multi-Vector Networks, è vicino allo scopo di protocolli come RIP. Come RIP, IGRP è un distanza-vettori protocollo.Quando determina il percorso migliore esso tiene anche in considerazione molte altre cose come la banda, il carico, il ritardo e la riability. L'amministratore di rete può determinare l'importanza data ad uno di questi METRIC, o permettere a IGPRS di calcolare automaticamente il patch migliore. EIGRP è una versione avanzata di IGRP, specificatamente, EIGRP, fornisce una efficienza operativa superiore e combina i vantaggi dello stato link protocol con i protocolli di distanza-vettore.

OSPF: Significa, determinazione del percorso ottimale. Questo INTERIOR gateway protocol usa diversi criteri di scelta per determinare il route. Criteri metrici, Hop count, banda, delay, carico, affidabilità, sicurezza.

Come il routers riconosce le reti: L'amministratore di rete può inserire manualmente queste informazioni nel router, i router possono anche imparare informazioni da altri router al volo. Gli inserimenti manuali, nelle tavole dei routers sono chiamati "static routes". Le tavole routing che vengono apprese automaticamente sono chiamate "dynamic routes".

Static Routing: Se il router può apprendere le informazioni di routing automaticamente, può sembrare inutile settarle a mano. Ad ogni modo non è così. Spesso conviene settare il routing manualmente per ottimizzare la connettività, la banda, per esaminare un collegamento particolare nella rete. Questo tipo di rete, è riferita ad una SUBNETWORKS. (qui si consiglia config

manuale). E’ preferibile lo static routing quando c’è un solo path per la rete di destinazione. E’ importante lo static routing al fine di prevenire delle scelte che possono portare a connessioni su punti non praticabili. Per cui in tal caso la connessione fallirebbe.

Dynamic Routing: Il routing adaptive, o dinamico, avviene quando il routers invia periodici messaggi di update routing ad altri routers. Utilizzando il routing dinamico, i router possono modificare le proprie condizioni di routing sulla rete. Prima dell’avvvento del updating dinamico delle tavole di routing, molti venditori mantenevano le tavole di routing per i propri clienti. Quindi il venditore inseriva automaticamente nel router, il numero di rete, che associava con la distanza, con il numero delle porte nelle tabelle router di tutte le periferiche vendute. Le reti si allargavano per cui ciò richiedeva impiego di tempo e operazioni dispendiose per riconfigurare, ogni volta, i routers. Il dynamic routing è la soluzione. Elimna le necessità di rete da parte degli amministratori ed i commercianti non devono più inserire informazioni nella tabella di routing. Il routing dinamico, lavora al meglio su reti “tranquille” dove c’è BANDA e non esiste un ammontare eccessivo di traffico sulla rete. RIP,IGRP,EIGRP, e OSPF sono tutti esempi di Dynamic Routing. Essi permettono a questo processo di funzionare. Senza il dynamic routing, internet, non potrebbe esistere.

Come il router usa RIP per routare i dati sulla rete: Tu hai una rete di classe B divisa in 8 Sottoreti, che sono connesse con tre routers. HOST ha vuole inviare i dati all’host Z. Esso passa i dati secondo l’osi model, dall’application al data lynk, dove l’host A incapsula i dati con le informzioni fornite da ogni livello OSI. Quando i dati raggiungono il lato NETWORK (3), la sorgente A, usa il proprio indirizzo ip di e quellodi destinazione dell’host Z. Perché è proprio qui che vuole inviare i dati. Quindi passa i dati sul livello DATA LYNK. Al livello DATA LYNK, la sorgente A inserisce il mac di destinazione del router a cui è connesso ed il proprio mac address nel mac header. A fa questo perchè essa vede 8 sottoreti come reti separate. Ess sa che non può inviare i dati direttamente a differenti reti, ma può passare esse al proprio default gateway. In questo esempio il gateway di A è il router numero 1. I pacchetti dati viaggiano attraverso la sottorete. Gli host di passaggio non copiano il frame perché il mac di destinazione nel mac header non corrisponde ad esso.I dati continuano a viaggiare nella sottorete finchè non raggiungono il router1 (gateway). Il router uno vede il pacchetto, lo prende è riconosce che il proprio mac addressè lo stesso mac di destinazione. Il router 1 spoglia il mac header dei dati e li passa al livello di rete (3), dove viene visto l’indirizzo ip e l’ip header. Il router quindi ricerca nella sua tabella di routing, per mappare un percorso per l’indirizzo di rete di destinazione ed il mac address del router che è connesso alla sottorete 8. Il router sta utilizzando RIP (routing information protocol). Con esso esso determina il miglior percorso per cui i dati possano raggiungere la destinazione che è solo 3HOPS distante. Quindi il router determina che i dati devono essere inviati tramite la porta collegata alla sottorete 4 per permettere ai pacchetti di raggiungere la propria destinazione sul percorso selezionato. Il router passa i dati al proprio livello data link dove inserisce un nuovo mac address del pacchetto. Il nuovo mac header contiene il mac di destinazione del router 2, ed il mac address del primo router che diventa la nuova sorgente. L’ip header resta lo stesso. Il primo router passa i dati tramite la porta che esso a scelto,

sulla sottorete 4. I dati passano attraverso la sottorete 4. Gli host non copiano il frame perché il mac di destinazione non coincide con essi. I pacchetti continuano a viaggiare sulla sottorete 4 fino a che non raggiungono il router2. Le altre periferiche sulla sottorete 4 ed il router 2 vedono il pacchetto. A questo punto il router 2 prende il pacchetto poiché esso riconosce che il mac specificato ed il proprio mac coincidono. Al livello data lynk, il router spoglia il mac header e passa il tutto sul livello NETWORK (3). Qui avviene l'esame dell'ip di destinazione, nella tavola di routing. Il router usa RIP e l suo routing protocol, e scopre che la destinazione è distante 2HOPS. Quindi il router determina che i dati devono essere spediti sulla sua porta collegata alla sottorete 5 per far raggiungere ai dati la destinazione tramite il percorso corretto. Il router passa i dati al livello data link, dove viene inserito un nuovo mac header sul data packet. Il mac header contiene il mac header del router 2(source) che diviene il router dei destinazione. Viene utilizzato il rip e viene verificata di nuovo la routing table. IP header resta non mutato, il primo router passa i pacchetti sulla sottorete 5 tramite la sua porta. I dati passano sulla sottorete 5. I dati continuano a viaggiare sulla 5 finchè non raggiungono il ROUTER 3. Le altre periferiche su rete5 vedono il pacchetto, lo vede anche il router 3. Il router 3 prende il pacchetto perché riconosce che il mac gli appartiene. Al data link il router estrapola il mac header e lo passa al lato network, l'ip di destinazione è collegato ad una rete a cui esso è collegato. Quindi il router determina che deve inviare i pacchetti alla porta attaccata alla SOTTORETE 8. Esso inserisce l'indirizzo mac nei dati, questa volta il nuovo mac header contiene direttamente il mac della destinazione Z e la sorgente mac del router 3. L'ip header resta SEMPRE IMMUTATO. Il router 3 invia i dati tramite la porta a cui è collegata la sottorete8. I pacchetti dati viaggiano attraverso la sottorete 8. Gli host non copiano il frame xkè il mac address non coincide con il loro, finalmente il pacchetto raggiungere l'host Z, che LO PRENDE perché il mac è uguale a quello suo (mac header). HOST z apre il mac header e lo passa al lato network, al livello network, l'host Z vede che l'ip address e l'ip header coincide. Host z, quindi apre anche l'ip header e lo passa al livello Transport, del modello OSI. Zeta continua ad analizzare i dati secondo i livelli di incapsulamento, e raggiunge i vari livelli del modello osi. Questo continua fino a che non arriva all'application layer del modello osi. Il dato è consegnato.

Layer 4-5-6

Livello transport: La frase **Qualità di servizio** è spesso usata per descrivere il lavoro del livello 4. IL livello di trasporto. Il compito primario **è il trasporto e la regolazione delle informazioni** e del traffico dalla sorgente alld estinazione, con **sicurezza ed accuratezza**. Il controllo Fine to Fine effettuto **tramite finestre scorrevoli** (sliding winodows)in sequenza e conferma è il lavoro primario del livello 4. Per capire come funziona il controllo di flusso, pensa ad uno studente che studia una lingua per un anno. Adesso immagina esso che visita una località dove questa lingua è usata. In una conversazione esso cheide agli altir di ripetere le parole (reliability) e di parlare lentamente, quindi esso può capire le parole (Flow control).

Protocolli di livello 4: L'enfasi di questo curriculum è sulle reti ethernet TCP\IP. Il protocollo TCP\IP nella sua rappresentazione OSI di livello 4, **comprende 2 protocolli TCP e UDP**. **Tcp crea dei VIRTUAL CIRCUIT fra l'utente e l'applicazione**. Le caratteristiche di questo protocollo. Connection Oriented, affidabile, divide le comunicazioni in segmenti ed intervalli, riassembla I

messaggi alla stazione di destinazione. Re-invia messaggi non ricevuti. Riassembla messaggi da sorgenti in entrata.
Il trasporto UDP, si occupa di trasportare dati Inaffidabilmente fra host. Le seguenti caratteristiche di UDP:
ConnectionLESS, Inaffidabile, Trasmette messaggio (chiamata usata datagrams), non ha software di controllo per il delivery del messaggio, non utilizza riconoscimenti, non ha un controllo di flusso, non riassembla messaggi in entrata.

Paragonare TCP e IP: TCP Ip è la combinazione di 2 protocolli individuali. **TCP e IP**. IP è un **protocollo di Livello 3.** Un servizio di **ConnectionLESS che offre un BEST-EFFORT** sulla rete. **TCP è un protocollo di livello 4**. Un servio **connectionORIENTED** che fornisce controllo di flusso al meglio per garantire **affidabilità**, Insieme possono fornire un'enorme varietà di servizi. Assieme essi rappresentano l'intera suite, per cui **INTERNET FUNZIONA con TCP e IP**, 2 protocolli di livello 3 e 4.

Funzionamento TCP: TCP è **Transmission Control Protocol**, è un servizio di CONNECTIOn Oriented di livello 4 (transport) che offre, affidabilità, e trasmissioni in full duplex. Tcp è parte dello stack TCP\IP. Nel segmento TCP\IP ci sono varie fields.
Porta sorgente (il numero della porta)
Porta Destinazione (Il numero della porta)
Numero Sequenza (Numero usato per assicurarsi della corretta sequenza di arrivo dei dati)
Numero Riconoscimento (attende il prossimo octect)
Hlen (numero di 32 bit nell'header)
Riservato (settato a Zero)
Codici in Bit (Controllo funzioni, setup di terminazione della sessione)
Finestra (Numero di ottetti che l'inviatario sta accettando)
CheckSum (Calcolo complessivo dell'header e data)
Urgent Pointer (Indica la fine dei dati urgenti)
Option-one Option (Massima dimensione di un segmento TCP)
Data (dati per il protocollo di livello superiore)

Formato del Segmento UDP: UDP (**user datagram protocol**) è un protocollo di tasporto **CONNECTIONLess**, nello stack TCP\IP. UDP è un protocollo semplice che **scambia datagrammi senza riconoscimento né garanzia di consegna**. Il processo degli errori e la ritrasmissione deve essere **fatto da altri protocoll**i. UDP **non usa tecnica di finestre né riconoscimento**, quindi è il protocollo di application garantisce l'affidabilità. UDP è designato per applicazioni che **non necessitano di mettere i segmenti assieme in sequenza**. I protocolli che usano UDP includono:
TFTP (Trivial File Transfer Protocol)
SNMP (Simple Network Management Protocol)
DHCP (Dynamic Host Control Protocol)
DNS (Domain Name System)

I field di un segmento UDP:
Porta Sorgente, Porta Destinazione, Lunghezza, CheckSum,Data
Non esiste alcuna sequenza di riconoscimento.

Numero delle porte nel TCP: Sia TCP che UDP utilizzano **numeri di porte** (o sockets) per passare informazioni ai livelli superiori. I numeri delle porte **sono usati per tener traccia di differenti conversazioni** sulla rete allo stesso tempo. Gli sviluppatori di applicazioni software hanno accettato di usare **numeri di porta conosciuti che sono definiti in RFC1700**. Ogni

conversazione per FTP ad esempio, utilizza la porta numero 21 cme stanzard. Le conversazioni che non involvono le applicazioni ad utilizzare le porte standard, sono assegnate a numeri di porta selezionati (RANDOM) in uno specifico RANGE di numerazioni. **Questi numeri di porta sono usati sia per la Sorgente che per la Destinazione**, nel segmento TCP. Molte porte sono riservate, sia in TCP che UDP, comunque applicazioni possono non essere scritte per supportare esse, i numeri delle porte hanno i seguenti RANGES.
Numeri di porta fino a 255 (Per applicazioni Pubbliche)
Numeri di porta da 255 a 1023 (assegnati da compagnie per applicazioni di mercato)
Numeri di porta oltre il 1023 (non sono regolati)

I sistemi usano i numeri delle porte per selezionare le proprie applicazioni. **Il numero di porta originario (interno) è dinamicamente assegnato dall'host sorgente**. Usualmente questo numero è più grande di 1023.
La porta sta in mezzo all'APPLICATION LAYER ed il TRANSPORT LAYER.

Handhsake Open Connection: Il servizio di **connectionORIENTED si divide in 3 FASI**: Nella fase di **Stabilire la connessione** è determinato un singolo percorso fra la sorgente e la destinazione. Le risorse sono tipicamente riservate, questa volta, per assicurare un costante **grado del servizio**. Durante il trasferimento dei dati, essi sono trasmessi in sequenza oltre il percorso stabilito, arrivando a destinazione, nell'ordine con cui sono stati inviati. **La fase di terminazione connessione**, consiste nel terminare la connessione fra la sorgente e la destinazione, quando non è più necessario.
L'host TCP stabilisce una sessione di connection ORIENTED con un altro host, usando un **"Three WAY handshake"**. Una three way handshake\open connection consiste **in una sequenza che sincronizza la cnnessione nelle 2 parti finali**, prima che i dati siano trasferiti. Questo scambio di **sequenza introduttiva** numerica durante la sequenza di connessione, è importante. Esso **garantisce che nessun dato sia perso**, se ciò è dovuto ad alcuni problemi di connessione, il dato può essere recuperato.
Inizialmente un host **inizializza una connessione** inviando un pacchetto che indica la sequenza di numeri di X con un certo bit nell'hader che indica una richiest di connessione. **SECONDA fase**, l'altro host riceve il pacchetto, registra la sequenza di numeri X, risponde con una conferma di X+1, e include le prime iniziali del numero di sequenza Y.La conferma diX+1 sta a significare che l'host ha ricevuto tutti gli ottetti, ed include, nella sua risposta, X e l'eccezione X+1.
Conferma POSITIVA e retrasmssione, o **PAR, è una tecnica comune** che molti protocolli possono usare **per garantire affidabilità**. Con PAR, la sorgente invia un pacchetto, **parte un timer, ed attende per la risposta** mentre sta inviando il prossimo pacchetto. **Se il timer ESPIRA**, prima che la sorgente possa ricevere la conferma, **essa retrasmette il pachetto** e starta il timer ancora una volta, da capo.
La **dimensione delle finestre** determina **l'ammontare** di dati che tu puoi trasmettere in una volta prima di ricevere la conferma dalla destinazione. La larghezza maggiore di numero di finestre, La rappresenta il maggior ammontare di dati che un host può trasmettere. Dopo che l'host ha trasmesso il numero della dimensione-finestra in bytes, l'host **deve ricevere una conferma** che i dati sono stati ricevuti prima di poter inviare un messaggio. Per esempio con un Windows SIZE1, ogni segmento individuale(1), deve essere confermato prima che tu possa inviare il prossimo SEGMENTO. Il TCP usa **EXPECTATIONAL AKNOWLEDGE** (conferma attesa), durante il numero di attesa riferito agli ottetti che sono prossimamente attesi. La parte SLITTANTE di finestra slittante, si riferisce, di fatto, alla dimensione della finestra che è negoziata dinamicamente durante la sessione TCP. Da ciò ne risulta un'inefficiente uso della banda da parte dell'host. **Il WindowWING è un megganismo di controllo di flusso**, che rechiede che la periferica sorgente riceva **una conferma** dalla destinazione dopo la trasmissione di un certo numero di dati. Per esempio con uno Windows SIZE di 3, la periferica sorgente può inviare 3 Ottetti a destinazione.

Essa deve quindi Attendere la risposta. Se la destinazione riceve tutti e 3 gli OCTECTS, essa invia una **Conferma alla SORGENTE**, che può adeso trasmettere altri 3 ottetti. Se per vari motivi, la destinazione non riceve i 3 ottetti, per esempio, a causa di un sovraccarica di buffers, essa non invia una conferma. Poichè la sorgente non riceve la conferma essa è a cnoscenza che gli ottetti devono essere ritrasmesssi, e la velocità di retrasmissione deve essere rallentata.
Il TCP fornisce una sequenza di segmenti con una referenza di FORWARD\conferma. Ogni datagramma è numerato prima della trasmissione. Al ricevimento, tcp riassembla il segmento in un completo messaggio. Se il numero di sequenza è mancante, nella serie, tale segmento è Ri-TRASMESSO. I segmenti che non sono confermati nel dato periodo, devono essere ritrasmessi.

Il Livello SESSIONE: I procesi di rete spesso avvengono in meno di un secondo, sono quindi difficili da "vedere". Usando analogie tu puoi capire più chiaramente che cosa succede durante questi processi. L'anologia seguente aiuta a spiegare il livello SESSION.
Tu hai intrapreso un cattivo argomento con un amico. Tu stai adesso comunicando (rap session o session) con esso, discutendo lo stato della vostra amicizia. Tu stai usando, ipotizziamo AOL o IRC. Ci sono 2 problemi che interferiscono con la tua "sessione". **Il primo problema** è che il tuo messaggio **può sovrapporsi** a quello del tuo amico durante la conversazione. Tu puoi inviare il messaggio contemporaneamente al tuo amico,questo può interrompere altri (lui). **Il secondo problema** è che **tu necessiti una pausa** (per salvare la tua corrente conversazione su un file) o **controllare la conversazione dell'altra persona o re-sincronizzare** la tua comunicazione dopo l'interruzione. Per **risolvere il PRIMO problema**, tu usare e stabilire **un protocollo** o settare un protocollo che detta **le Regole** per la comunicazione con altri. Questo significa che tu devi Essere D'accordo con queste linee guida da usare durante la conversazione (regolare la conversazione in modo da evitare interruzioni). Questo è riferito al **TWO-WAY ALTERNATE COMMUNICATION**. **Un'altra soluzione** è che ogni persona debba scrivere quando desidera, **facendo continuamente attenzione** a chi trasmette. Questo è riferito a **TWO-WAY SIMULTANEOUS COMMUNICATION.**
Per risolvere il secondo problema, tu deve inviare un CheckPoint ad ognuno, significa che **ogni persona deve salvare la conversazione come un file, quindi ogni persone deve Ri-LEGGERE** l'ultima parte della propria conversazione sullo stesso file. Questo processo è chiamato **SYNCRONIZATION**. **Due checkpoints** molto importanti sono –Come la conversazione parte –Come la conversazione termina. Questo è chiamato anche **INITIATION e TERMINATION** CONVERSATION. Per esempio tu puoi instantaneamente inviare una mail o comunicare via IRC, GOOD-Bytes sono di solito scambiati prima di terminare la sessione. L'altra persona può capire che tu stai terminando la sessione. x aiutarti a comprendere cosa fa il session layer, usiamo la stessa analogia in un altro modo
Immagina di comunicare con un pen pal via servizio postale. i messaggi potrebbero passare dall'uno all'altro (??) perchè non hai acconsentito ad usare la comunicazione simultanea bidirezionale piuttosto che una comunicazione bidirezionale alternata. O puoi avere risultati scarsi di comunicazione perché non hai sincroizzato il soggetto con la tua conversazione.

Analogie sul livello SESSIONE: Il livello Sessione, **Stabilisce, mantiene e termina le sessioni** fra applicazioni. Questo include. **La partenza, lo stop, la re sincronizzazione** di 2 computer che sono in **"rap Session**". Il livello sessione coordina le applicazioni in modo che esse possano interagire con 2 host comunicanti. La comunicazioni dati, **viaggia su packet-switched networks**, non come il telefono che viaggia su Circuit-Switched networks. Comunicazione fra 2 computer, crea molte mini-comunicazioni, questo garantisce che i 2 pc possano comunicare effettivamente. Un requisitio per queste mini conversazioni è che ogni host giochi 2 ruoli. **Richiesta di Servizio**, -Come se fosse un client. **E risposta con servizio** –Come se fosse un server. La determinazione del roule che è "playng" dall'una all'altra parte è chiamato **DIALOGUE CONTROL**.

Controllo del Dialogo: Il livello session decide quando usare **TWO-WAY simultaneos** communications, opppure **TWO-WAY alternate** communication. Questa decisoone è riferita ad un controllo di dialogo. **Se è permessa la Two-way simultanoius communication**, il **livello sessione fa poco per gestire la conversazione.** In questi casi, altri livelli di comunicazione fanno ciò. E' possibile **avere collisioni sul livello sessione**, comunque questi **sono molto diversi rispetto alle media-collisions che avvengono al livello1**. A questo livello le collisioni possono avvenire quando due messaggi passano assieme e causano confusione negli host comunicanti. **Se queste collisioni sul livello sessione, sono intollerabili, il controllo del dialogo opta per un'altra opzione: TWO-WAY alternate communication**. Two-Way alternate **communication involve l'uso del livello sessione data token che permette ad ogni host di attendere il proprio turno**. Questo è simile al sistema che si ha sul livello 2 token ring handel livello2, rispetto alle collisioni sul livello1.

Separazione Dialogo: La separazione consiste, nell'ordine: **Inizializzazione, terminazione e gestione** della comunicazione. Per cui vengono fatti: **Backup** di file particolari, **salvataggio** impostazioni di rete**, salvataggio** impostazioni di **clock**,**prendere nota della fine conversazione**. Una **maggiore** sincronizzazione porta a maggiori "**back-and-fort" steps**, Il check point è simile, in un certo senso ad un applicativo tipo word, situato in un computer, che **compie una pausa per l'autoSAVE** del documento corrente. Questi checkpoint sono usati per **separare parti della sessione** precedente riferiti a dialoghi passati.

Protocolli di livello 5: Il livello 5 ha un numero importante di **protocolli**. Devi essere abile da riconoscere questi protocolli **quando essi appaiono nella procedura di login** o in una applicazione. Esempi di protocolli livello 5.
NFS (network file system)
Structure Query Language (SQL)
Remote Procedure Call (RPC)
X-Window System
AppleTalk Session Protocol (ASP)
Digital Network Architecture Session Control Protocol (DNA SCP)

Livello Presentazione Funzioni e Standards: Il livello **presentazione** è responsabile per la **presentazione dei dati** in un form che riceve la periferica e che può comprendere. Per comprendere il concetto di presentazione utilizzare l'anologia di 2 persone che parlano differenti lingue. L'unico modo per dialogare è tradurre ciò che si dice. Il livello presentazioen serve **come traduttore per periferiche** che necessitano di comunicare oltre la rete. Il **lievello 6**, presentation layer, effettua le seguenti funzioni. **DATA FORMATTING, DATA ENCRYPTION, DATA COMPRESSSION**.Dopo aver ricevuto i dati dal livello applicazione, il livello presentazione, esegue una o tutte le sue funzioni sui dati prima di inviarli al livello sessione. Alla stazione ricevente il **livello presentazione porta i dati dal livello sessione** ed effettua le necessarie funzioni prima di passare esso al livello applicazione.
Per capire come I dati **vengono preparati al lavoro**, immagina due sistemi non simili. Il primo sistema utilizza un extendend binary coded decimal interchange code, per rappresentare i caratteri sullo schermo. Il secondo sistema utilizza American standard code for information interexchange per la stessa funzione. **Il livello 6 si occupa della traduzione** fra questi 2 tipi di codici. Gli standard di livello 6 determinano anche come le immagini grafiche sono presentate. Questi standard sono i seguenti: PICT (picture format Quick Draw, mac operating system). TIFF (taggef image file format), JPEG (joint photographic experts group)
Ci sono anche altri standard di livello 6:
MIDI(Musical intruments Digital Interface) Mpeg (motion picture experts group) QuickTime(standard video MAC).

-

COMPRESSION – ENCRYPTION – DATA FORMAT.

Formato File: **ASCII e ebcdic** sono usati per il **formato testo**. Il testo asci contiene **semplici caratteri** e mancano di sofiticati comandi di formattazione (es.sottolineatura). Il notepad èun esempio di applicazione che usa e crea i file di testo. Solitamente hanno estensione txt. **Ebcdic è molto simile ad ascii** esso non usa formattazione **sofisticata**. La principale differenza fra i 2 è che **EBCDIC è usato fondamentalmente per i mainframes ed ascii è usato sui personal computers**. Un altro file comune è il BINARY FORMAT. I file binari contengono codici speciali che possono essere letti solo da specifiche applicazioni software. I programmi come FTP usano il tipo di file binario per trasferire files. Le reti usano molti differenti tipi di files. Una precedente sezione menzionava i file di tipo grafico come jpeg. Internet usa 2 file binari per visualizzare le immagini, GIF e JPEG. Ogni computer con un lettore per gif o jpeg può leggere questi tipi di files, indipendentemente dal tipo di computer. I readers sono software designati per visualizzare questi tipi di files, immagini di tipo particolare. Molti programmi possono leggere molteplici tipi di immagini e convertirle in altri formati. Il browser web ha l'abilità di visualizzare questi 2 formati, GIF e JPEG senza software addizionali. Il formato **file multimediale è un altro tipo di file binario** che contiene suoni, musica e video. I file sonori generalmente operano in 2 modi. Essi possono essere completamente scaricati e poi eseguiti o essi possono essere eseguiti mentre vengono scaricati. L'ultimo metodo è chiamato **STREAMING audio**. Windows utilizza gli WAVE, e gli AVI. Alcuni video meno comuni sono Mpeg,Mpeg2,E machintosh quicktime (mov).
Un altro formato file è il Markup Language **HTML**. Questo formato è composto da una serie di **direttive** che dicono al browser come visualizzare e gestire i documenti. HyperText Markup Language, HTML, è il linguaggio di internet. Le istruzioni html dicono al browser come visualizzare il testo, o un collegamento ad un altro url. HTML **non è un linguaggio di programmazone** ma è un set di istruzioni per visualizzare una pagina.

Encryption e Compressione: Il livello 6 è anche responsabile **dell'encryption** dei dati. L'encription **PROTEGGE informazioni** durante la loro trasmissione. Transazioni finanziarie, usano l'encryption per proteggere informazioni delicate durnate il loro viaggio in internet. Una chiave di encription **è usata per encryptare i dati alla sorgente e decriptarli alla destinazione**. Il livello presentazione è anche responsabile per la compressione dei files. La compressione lavora utilizzando **algoritmi o formule matematiche** complesse che riducono loa dimensione dei files. L'algoritmo cerca ogni file per ripetere il processo di modello bits, e **sostituisce essi con un Token**. Un token è **una corta combinazione di bit** che rappresenta il lungo modello. Una semplice analogia più essere il nome CATHY il token si riferisce ad ogni persona il cui nome è catherine.

Il livello Applicazione: Nel contesto del modello osi, il livello applicazione (7) **supporta i componento di comunicazione** di un'applicazione. Il livello applicazione è responsabile di: Identificare ed estabilire possibili ed intesi partner di comunicazione, sincronizzare applicazioni cooperanti, stabilire procedure di recupero errori, controllare l'integrità dei dati.
Il livello applicazione è **vicino ai sistemi finali**. Questo determina **se esistono sufficienti risorse per la comunicazione fra sistemi**. Senza il livello applicazione, non ci sarebbero supporti di comunicazione per la rete. Il livello applicazione **non fornisce servizi per altri livelli del modello osi.** Esso **fornisce servizio** per processo di **applicazioni esterne** di livello esterni. Esempi di questi processi di applicazioni, può essere Word Processing, banking terminals programs. In aggiunta, il livello applicazione, fornisce **una interfaccia diretta per il resto del modello osi**, usando applicazioni che viaggiano sul networks. Clients **FTP, EMAIL, TELNET** o un'interfaccia indiretta utilizzando applicazioni standalone con un redirector di rete.

Applicazioni Network Dirette: Molte applicazioni che lavorano sul network sono classificate come **Client o Server applications**. Queste applicazioni come ad esempio ftp, browser, e email,

hanno **2 componenti** che permettono di funzionare. **Il lato Client e Il lato Server**. Il lato **client** è locato sul computer ed è il **richiedente** del servizio. Il lato **Server** è locato sul remoto computer e **fornisce** servizi in risposta alla richiesta del client.
Una client-SERVER application lavora ripetendo constantemente la seguente routine in Loop: **Client-Request, Server-Response,Client-Request,Server-Response**, ecc.ecc. Per esempio un browser web accede ad una pagina web richiedendo un resource locator (URL), su un web server. Dopo aver localizzato l'url, il server web che ha identificato l'url, risponde alla richiesta. Quindi basando le informazioni ricevute dal web server, il client può richiedere maggiori informazioni dallo stesso server web, o può accedere ad un'altra pagina richiedendola ad un differente web server.
Netscape ed internet explorer sono le più **comuni** applicazioni usate come applicazioni di rete. Un modo facile per capire il funzionamento dello web browser è paragonare esso al controllo remoto di una televisione. Il Telecomando ci da la possibilità di controllare la tv direttamente per quelle che sono tutte le sue funzioni: volume, canali, brightness, ecc.ec. Per far sì che il telecomando funzioni bene, tu non devi capire come esso funzioni elettronicamente. La stessa cosa è uguale per un browser, esso offre a noi la possibilità di nvigare tramite il web cliccando su un hyperlinks. Per fare in modo che esso funzioni correttamente, non è necessario capire come il livello i livelli osi più bassi ed i protocolli lavorano ed interagiscono con il sistema.

Supporto di rete Indiretto: All'interno della lan, **il supporto delle indirect applications**, è basato sulle **funzioni client-server**. Se un cient vuole salvare un file da word processor su un server di rete**, il redirector abilita il word procesing a diventare un client di rete per quella determinata operazione**. Il redirector è un protocollo che lavora con sistemi operativi e clients di rete dedicati a specifici programmi o applicazioni. Esempi di redirector sono: Apple File protocol, NETBIOS extended user interface (NETBEUI), Novel IPS\SPX protocols, Network file system (NFS) della suite tcp\ip.
I processi redirector sono i seguenti: **Un client richiede** che il file server di rete, permette ai dati di essere immagazzinati, **Il server risponde salvando il file sul proprio disco**, o rejettando la richiesta del client. Se la richiesta del client che la rete invia al server, permette al data file di essere inviato dalla rete, **il server processa la richista** inviando il file ad una delle sue periferiche, o respinge la richiesta. **Redirector** permettono agli amministratori di rete di **assegnare risorse remote** a nomi logici su client locali. Quando tu scegli uno di questi nomi logici per eseguire una operazione come ad esempio salvataggio file o stampa file, il redirector di rete invia i file selezionati alla propria risorsa remota sulla rete per il processo. **Se la sorgente è sul computer locale il redirector ignora la richiesta e permette al sistema operativo locale di processarla** direttamente. Il vantaggio dell'utilizzo di un network redirector su un client locale è che l'applicazione sul client non ha mai da riconoscere la rete. In aggiunta, l'applicazione che richiede il servizio è locata sul computer locale ed il redirector gira la richiesta alla propria risorsa di rete mentre l'applicazione tratta essa come una richiesta locale.I **redirectors espandono le possibilità di un software che non è propriamente designato per la rete**. Questo può anche essere usato per condividere documenti, templates, database,stampante, e molti altri tipi di risorsa, senza avere il supporto di uno speciale software oapplicazione. Il networking ha avuto una grande influenza sullo sviluppo dei programmi come work processor, database programs e software di produttività. Molti di questi pacchetti software sono andesso NETWORK-Integrati, su network-aware. Essi hanno possibilità avanzate di lanciare browser integrati o tools per interent e di pubblicare i loro risultati su html per facile integrazione con web.

Effettuare e tagliare connessioni: E' importante notare che nei precedenti esempi, la connessione del server è mantenuta solo **quanto basta per la transazione**. Nell'esempio WEB, la connessione è mantenuta a sufficiente per il download della pagina corrente. Nell'esempio delle stampanti, la connessione è mantenuta fin quanto non sono stati inviati i documenti al server di stampa. Dopo che

il processo è completato, la connessione è Interrotta, e deve essere ri-ristabilita per il prossimo processo. Più tardi, in questo capitolo, tu imparerai approposito del secondo metodo in cui avviene il processo di comunicazione. Questo è illustrato **da telnet ed esempi FTP**, che stabiliscono una connessione con il server e **mantengono la connessione fino a che tutti i processi non sono stati eseguiti**. Il client termina la connessione quando l'utente determina di aver finito. Tutte le attività di comunicazione si raggruppano in queste 2 categorie.Nella prossima sezione, si imparerà a conoscere il Domain Name Server che è un processo supportato dal livello applicazione.

Problemi con l'uso di indirizzi IP: Nel capitolo del livello network abbiamo imparato che internet è costruito su indirizzi a schema hieriarchico. Questo permette il routing che è basato su classe di indirizzi, opposti ad indirizzi individuali. Il problema che viene a crearsi per gli utenti è associare il corretto indirizzo con il sito internet. La sola differenza fra l'indirizzo 198.151.11.12 e 198.151.11.21 è una digitazione di trasporto. E' molto facile dimenticare un indirizzo di un particolare sito, perché i numeri non sono associati con i siti e con il proprio address. Allo scopo di associare il contenuto del sito con il proprio indirizzo, è stato creato un **DOMAIN NAME SYSTEM.** Un dominio è un gruppo di computer che sono associati dalla loro posizione geografica o dal loro tipo di lavoro\operatività. Un domain name, è una stringa di caratteri e\o numeri usualmente un nome\abbreviazione che rappresenta l'indirizzo numerico di un sito internet. Ci sono più di 200 livelli di dominio su internet. Esempi di questi includono. .US-united states, .uk-united kingdom. Ci sono anche nomi generecici, esempi di questi includono i seguenti. .edu (educational),.com(commerciali),.gov(governativi),org (no profit),.net (servizi di network).

IL Domain Name Server: Il dns è **un servizio** di rete. Esso risponde alle richiede dai client e consiste nella traduzione di nomi in ip associati. Il sistema dns è settato in struttura hierarchy che crea differenti livelli di server DNS. Se un **dns locale** è abilitato alla translazione di un domain name, nel proprio ip associato esso effettua l'operazione e **ritorna il risultato al client**. Se non può tradurre l'indirizzo esso passa la richiesta al prossimo livello più alto di dns nel sistema che prova a tradurre l'indirizzo. Se il **dns a questo livello è abilitato** a translare il domain name nell'ip associato, esso effettua l'operazione ed il risultato torna al client. Questo livello **è ripetuto fino a che il nome non è tradotto, al livello top del dns raggiunto**. Se il domain name **non può essere trovato** nel livello più alto del dns, **questo è considerato un errore**, ed il messaggio corrispondente di errore, torna indietro. Ogni tipo di applicazione che usa domain names per rappresentare indirizzi ip, **usa anche il dns per tradurre il nome**,nel corrispondente ip address.

Applicazioni Internet: Tu selezioni le applicazioni di rete, basate sul tipo di lavoro che devi compiere. Un completo set di livello applicazioni è disponibile ed interagisce con internet. Ogni tipo di **applicazione è associato con un prorpio protocollo**. Quindi ci sono molte applicazioni e molti programmie protocolli disponibili. Alcuni esempi:
Lo world wide web utilizza http protocol.
I programmi di accesso remoto usano il protocollo TELNET per connettersi direttamente alle risorse remote
I programmi di email supportano le applicazioni di livello POP3 per posta elettronica
Un programma di utilità file, usa il protocollo FTP copiando e spostando files a siti remoti
I programmi di rete per esaminare i dati, usano il protocollo SNMP
E' importante enfatizzare che il livello APPLICATION rappresenta **un altro livello di protocollo nei modelli OSI e TCP\IP**. Il livello di PROTOCOLLO o Interfaccia con le applicazioni.
I client email (eudora,outlook, pegasus, netscape mail), lavorano con il protocollo POP3. La stessa cosa succede con i Browser Web. 2 browser popolari sono Internet Explorer e Netscape.
All'apparenza le operazioni di questi due programmi è molto differente ma essi lavorano entrambi con il livello APPLICATION del protocollo http.

Messaggio EMAIL: La posta elettronica ti abilita ad inviare **in messaggio fra computer connessi**. La procedura per l'invio di documenti email si convoglia in 2 processi separati. **Il primo è inviare** l'email al **post office** dell'utente. **Il secondo è deliverare l'email** dal post office alla mail dell'utente (**recipient**). Negli indirizzi email alexxz@tin.it, consiste in 2 parti: Il mnome del recipiente locato prima della @ e il post office @tin.it. Il nome del **recipiente è importante solo per il final delivery**, per cui inizialmente si tiene sempre conto del post office. Grazie al DNS si raggiunge il post office server.

Funzione DNS: Quando un email client **invia una lettera**, esso **richiede al dns** connesso sulla rete, di tradurre i domain names, negli ip associati, questa informazione torna indietro ai richiedenti, ed abilita propriamente il trasport layer alla segmentazione ed encapsulazione. **Se il DNS non traduce i nomi, la richiesta è passata finchè il nome non è tradotto**. La parte dell'indirizzo email che contiene **il nome del recipiente** diviene importante, a questo punto. **IL SERVER estrae essa dal messaggio, e controlla se esso è membro del proprio post office**. Se il recipiente è membro, esso archivia il messaggio i quella determinata mailbox, fino a quando nessuno la scarica. Se il recipient non è member di quel post office, viene generato un errore ed inviata l'email indietro al mittente. LA seconda parte del mailing proces, è il processo di ricezione. Un utente deve usare un software client email sul proprio pc per stabilire la richiesta con il post office. Quindi quando andiamo su RETRIEVE MAIL, viene chiesta una password. Dopo aver inserito la password, diamo OK, il mail software fa la richiesta al post office server. Esso **estrae la configurazione del client,** utilizza un altro processo di ricerca DNS per trovare l'ip del server, **la richiesta è segmentata e sequenziata dal livello transport.** I pacchetti viaggiano attraverso il resto del modello OSI **(network, data link, physical),** e sono quindi ritrasmessi tramite internet, al post office di destinazione. A questo post office i packets sono **reassemblati in una propria sequenza** e controllati per errori di trasmissioni dati. Al post office, user name e password sono verificati. Se questi dati sono corretti, il post office trasmette le email al pc richiedente, le email sono quindi **SEGMENTATE, SEQUENZIATE ed incapsulate in frame per essere inviate al client computer corrispondente a quel determinato recipient**. Dopo che il messaggio email è arrivato al computer, l'utente può aprirlo e leggerlo. Se si decide di rispondere alla mail, il processo riparte da capo, ancora. Le email sono normalmente inviate in formato ASCII, ma gli attachment sono solitamente incluse con esse (audio, video, graphics). Per ricevere correttamente gli attachment, lo schema di encoding deve essere lo stesso dell'invio messaggio. **I due formati più comuno per gli email attachment sono il Multipurpose Internet Mail Extension (MIME) e Uuencode (unix utility)**

Telnet: Emulazione Terminale (telnet), fornisce l'abilità di **controllare da remoto un altro computer**. Esso permette di **loggarti ad un host ed eseguire comandi**. Un cliente TELNET è riferito ad un local host, e ad un telnet server che usa **uno speciale software chiamato DAEMON**, riferito ad un host remoto. Per effettuare una connessione da un client TELNET tu devi prima selezionare una opzione di connessione. Un box di dialogo ti chiederà **l'host name, ed il tipo di terminale**. L'host name è la destinazione del computer remoto che vuoi connettere. Il tipo di terminale descrive il tipo di **emulazione terminale** che vuoi far eseguire al computer. L'operazione telnet non usa potenza di processo del pc per trasmettere. Essa trasmette battute di testo al remote host ed invia il risultato sullo screen, quindi sul monitor locale. **La lavorazione ed i processi prendono luogo sul computer remoto.** Telnet inizia il processo di email. Quando tu inserisci un nome dns per una locazione telnet, il nome dev'essre tradotto nell'ip associato prima che una connessione venga stabilita. L'applicazione **telnet lavora unicamente ai 3 livelli top del modello osi. Session, presentation, application. Il livello applicazione (comandi), il livello presentazione (formato, ascii) ed il livello sessione (trasmissione). I dati quindi passano dal livello trasport e sono segmentati, poi viene addata una porta ed effettuato un check degli errori. I dati quindi passano dal livello network dove un ip header (contiente sorgente e destinazione ip address) è aggiunta. Poi il pacchetto viaggia e raggiunge il livello data lynk, che encapsula i dati packet**

in data frame, aggiunge la sorgente e destinazione del mac address ed il frame trailer. Se il computer sorgente non ha il mac del computer di destinazione esso esegue una arp request. Quando il mac è stato determinato, il frame viaggia attraverso il cavo (binary form), e raggiunge la prossima periferica. Quando i dati raggiungono l'host computer remoto, **il data link, network e trasport, riassemblano l'originale data command**. Il remote host computer esegue il comando e trasmette il risultato indietro al local client computer, usano lo stesso processo di encapsulamento e delivery dell'original command. Questo processo viene ripetuto per intero inviando comandi e ricevendo risultati fino a che il local client non ha completato il lavoro che necessita. Quando questo lavoro è ok, la sessione viene terminata.

File Transfer Protocol: FTP è designato per **il download dei file (ricevuti da internet, es), o upload dei files.** L'abilità di uploadare e downloadare file è una delle numerose possibilità che internet, offre. Questo può specialmente essere d'aiuto per persone che **hanno bisogno di file su computer, driver, ecc.ecc**. Gli amministratori di rete possono raramente aspettare giorni per avere files immediatamente. Internet può fornire questi files immediatamente utilizzando FTP. FTP è **un'applicazione client-server, come email e telnet. Essa richiede un software che è in esecuzione sul server ed è accessibile by Client software**. Una sessione FTP è stabilita **nello stesso modo della sessione telnet**, e come telnet anche ftp la mantiene fin oa **quando il client non ha terminato le proprie operazioni** O la comunicazione ha generato un errore. Dal momento in cui si stabilisce una connessione ad un demone ftp, devi fornire username e password. Normalmente tu puoi usare anonymous login ed il tuo indirizzo email come password. Il tipo di connessione così descritto è chiamato ANONYMOUS FTP. **Da quando viene stabilita la tua identità, un link di comando apre la comunicazione fra la tua macchina client e l'ftp server. Questo è molto simile alla sessione TELNET, in cui i comandi sono inviati ed eseguiti sul server** ed i risultati vengono re-inviati al client. Questo possibilità ti permette di creare, cancellare directory, files, ed eseguire molte funzioni associate alla gestione files. Il proposito principale dell'ftp è **TRASFERIRE files da un computer ad un altro,** compiando e spostando files Dal SERVER al CLIENT, e Client-SERVER. Quando tu copi files dal server, **FTP stabilisce una seconda connessione, un DATA Link fra il computer attraverso il quale i dati vengono trasferiti. Il trasferimento dei dati, avviene in ASCII mode, o Binary MODE**. Queste 2 modalità determinano come i data files sono trasferiti fra le stazioni. Dopo che il trasferimento è terminato, **la connessione dati è terminata automaticamente**. **Dopo che tu hai completato l'intera sessione di copiare,spostare files, tu puoi decidere di fare LOG OFF chiudendo il command data links e terminando definitivamente la session**e. Un altro protocollo che ha l'abilità di **scaricare files è http (hypertext transfer protocol),** del quale parleremo nel prossimo paragrafo. Una limitazione dell'**http** è che tu puoi solo usare esso per scaricare file, **non per fare UPLOAD**.

HyperText Transfer Protocol: HTTP lavora con lo **World Wide Web che è la parte più grande ed usata di internet.** Una delle principali ragioni della straordinaria crescita del web è che essa permette l'accesso ad un immenso numero di informazioni. Un browser web è una applicazione **Client-SERVER** il che vuol dire che essa richiede sia un compoennte client che un componente server per poter funzionare. Un browser web presenta i dati in formato multimediale su pagine web che usano **TESTO, GRAFICA, suono e video**. Le pagine web sono stato create con un linguaggio il cui formato è chiamato **HyperText Markup Language (HTML**). Html **da istruzioni** un browser web su una particolare pagina web, a produrre la pagina stessa in uno specifico modo. HTML specifica la Locazione del testo, dei files, grafica, oggetto,ed il modo in cui essi debbano essere trasferiti dal web server al web browser. Gli **hyperlink** rendono lo world wide web facile da navigare .Un hyperlink è un oggetto (testo, frase, disegno), su una pagina web, che, quando cliccato, ti trasferisce ad un'altra pagina web. La pagina web, contiene, inolte, descrizioni in thml

(NASCOSTE), e l'indirizzo coosciuto dell'url (resource locator). Nell'esempio seguente, il simbolo http://, dice al browser, quale protocollo usare. La seconda parte "www", dice al browser quale tipo di risorsa si desidera cntatare. La terza parte "cisco.com", identifica **il dominio** del web server ed il suo indirizzo ip. L'ultima parte, "edu" identifica la specifica cartela di locazione (sul server) che contiene la pagina web. Esempio: http://www.cisco.com/edu/
Quando tu apri un browser web, la prima cosa che solitamente vedi, è **la starting page**, o HOME page. L'indirizzo della home page è già memorizzato nella configurazione del browser, e può essere cambiato in ogni momento. Dalla pagina di partenza, tu puoi cliccare uno degli hyperlink web o digitare l'url nella barra degli indirizzi. Il web browser, quando esamina il protocollo, determina se è necessario aprire un altro programma e determina l'indirizzo ip del web server. Dopo ciò, il livello **TRANSPORT, NETWORK, DATA LINK e phisicha, inizializzano la sessione con il web server**.
I dati sono trasferiti al protocollo http che contiene il nome della directory della locazione o web page. (può anche contenere un nome specifico di un file html o pagina). Se nessun nome è dato, il server usa il nome **di default**, di solito è index.htm ma è specificato nella server configuration.
Il server risponde alla richiesta inviando files di testo, audio, videoe grafica come specificato nelle istruzioni HTML al client web. Il server **risponde alla richiesta** inviando tutto il testo, grafica, audio e video come specificato nelle istruzioni HTML, al client web. Il browser riassembla tutti i files ai fini della creazione pagina. Quindi termina la sessione. Se tu clicchi un'altra pagina che è locata sullo stesso o differente server, questo processo si ripete da capo.

SEMESTRE 2

REVIEWS

Modelli di rete Livellati (layered): Nuove pratiche di lavoro hanno comportato **cambiamenti sulle reti.** Uffici, enti lavorativi, case, enti privati, **necessitano di un accesso immediato** ai dati. Essi necessitano. Di reti interconnesse che forniscono accesso ai computer \fileserver situati in altre locazioni. Ampia banda sulla rete per soddisfare le necessità degli utenti. Supportare tecnologie che possono essere applicate su servizi WAN. Per sfruttare la comunicazione con altri partners si sta **implementando nuove applicazioni** come COMMERCIO ELETTRONICO, videoconferenza, voce tramite ip ed adddestramento a distanza. Il lavoro sta emergendo su VOCE, video, data, tutte cose che si appoggiano sull'attuale sistema di networking. Le reti sono designate per supportare correnti e future applicazioni**. Per permettere aumento di BANDA, scalabilità ed affidabilità**, i venditori introducono **protocolli** e tecnologie di rapida applicazione. Gli "architetti" delle reti devono creare reti sempre **più moderne e funzionali** anche se il concetto di moderno cambia su base mensile se non settimanale. Dividendo l'organizzazione del networking ed i tast in separate funzioni\livelli, nuove applicazioni possono esssre create senza problemi. **Il modello OSI** organizza le funzioni di rete in SETTE categorie. Il controllo dei dati dai livelli superiori a quelli inferiori, riguardanti i bit che vengono trasmessi sul media. Il compito dei managers che lavorano su grandi reti, **è configurare i tre livelli inferiori**. Le funzioni Peer To Peer usano l'encapsulation ed il de-encapsulation come interfaccia per i livelli. Esistono livelli nel modello OSI, ognuno di questi ha funzioni distinte e separate. IL TCP\IP model invece, si divide in 5 livelli. Questa separazione delle funzioni di rete è chiamata **LAYERING.** Riguardo o meno il numero di livelli, spesso la ragione della divisione delle funzioni include:
Dividere gli aspetti inter-relazionati su operazioni di rete, **in meno complessi elementi**.
Definire interfacce standard, per compatiblità Plug and Play ed integrazione di multi-venditori.

Abilitare gli ingegneri a focalizzare il proprio design e lo sforzo di produzione **su particolari funzioni di livelli.**
Prevenire cambiamenti di un'are a seguito di effetti derivati da altre aree, quindi ogni area si può evolvere più velocemente.
Dividere le complesse operazion di networking in facili iperazioni **subnet facilmente apprendibili**.

Livelli osi: **Ogni** livello, nel modello osi, **fornisce una specifica funzione**. Le funzioni sono definite da OSI e possono essere usate da ogni venditore produttore di apparati di networking.
Applicazione: Questo livello applicazione fornisce alla rte **servizi per applicazioni**. Per esempio una **word processing** application è servita dal file transfer service di questo livello.
Presentazione: Questo livello fornisce **rappresentazione dei dati, codifica e formattazione**. Esso **garantisce** che i dati che arrivano dalla rete, possano essere usati dall'applicazione, esso garantisce inoltre, che le informazioni inviate dall'applicazione possono essere trasmesse sulla rete.
Sessione: Questo livello **stabilisce, mantiene e gestisce le sessione fra applicazioni**.
Trasporto: Questo livello segmenta e riassembla i dati in **data stream**. IL Tcp è una dei livello del protocollo usato con IP.
Network: Questo livello determina il miglior **modo per muovere i dati da una posizione ad un'altra**. I routers operano a questo livello. Si può trovare lo schema di indirizzi di IP.
Data Link: Questo livello **prepara un datagramma** per trasmissioni fisiche sul media. Esso comunica errori di comnicazione, tipologia di rete, e controllo di flusso. **Questo livello usa il MAC**.
Physical: Questo livello pensa **alle procedure Elettriche, Mecceniche e funzionali**, i mezzi per attivare, mantenere i link psychici fra sistemi. Questo livello usa **il media fisico** come Twisted Pair, Coassiale, e fibra ottica.

Comunicazioni Peer To Peer: Ogni livello **usa il proprio protocollo** per comunicare con il "peer" di un altro sistema. **Ogni layer's** protocol scambia informazioni ed è chiamato **PDU**. Un livello può usare un nome più specifico per il PDU. Per esempio in tcp\ip il livellotrasporto del TCP comunica con il Peer **TCP usando SEGMENTI**. Ogni livello usa il servizio del proprio livello pari, per la comunicazione Peer to Peer. Il servizio **di livelli inferiori usa informazioni di livelli superiori** come **parte dei pdu** che scambia con il proprio Peer. Il **segmento TCP diventa parte del network** layer packets (datagrams) che sono scambiati mediante il Peer IP. A turno i pacchetti IP vanno a far parte dei Data link frames che sono scambiati mediante connessioni DIRETTE alle periferiche. In fine, questi frames diventano bit ed i dati sono trasmessi dall'hardware che è usato dal livello Phisical. **Ogni livello dipende dal servizio superiore** dell'osi refernce model. Per fornire questo servizio i livelli inferiori, usano l**'encapsulation** per inserire il **Protocol Data unit (PDU)** che provengono dal lato superiore **in dei DATA FIELDS**. Dunque vengono aggiunti header, trailers, ed altri per performare le funzioni desiderate.
Per esempio il livello Network fornisce un servizio al livello trasporto, ed il livello trasporto, presenta i dati al sottosistema di internetwork. Il livello rete ha il compito di spostare i dati tramite l'internetwork. Esso completa questa operazione encapsulando i dati in pacchetti. Questi pacchetti includono HEADER contenenti informazioni che sono necessarie per completare il trasferimento, come la sorgente e la destinazione di indirizzo logico.. Il livello Data link, al fine di fornire un servizio al network layer, encapsula i pacchetti network in frame, il frame header contiene informazioni che sono necessare per completare le funzioni data link. In fine il livello fisico fornisce un servizio al Datalink layer. Esso encoda i frame in una serie di 1 e 0 per la trasmissione tramite il media, tpicamente un cavo.

I 5 steps dell'incapsulamento dei dati: Come le reti forniscono servizi per gli utenti, il controllo e l'impachettamento delle informazioni degli utenti è sottoposto a numerosi cambiamenti. In questo esempio di internetworking, ci sono 5 steps di conversione.

Step1: Un computer converte un messaggio email **in caratteri alfanumerici**, che possono essere usati dal sistema di internetworking. Questo è DATA.
Step2: Questo messaggio data è quindi segmentato per essere trasportato **sul sistema di internetworking dal livello trasporto**. Il livello trasporto garantisce che il messaggio possa arrivare a destinazione e che la comunicazione avvenga in entrambe le fini.
Step3: I dati sono quindi **convertiti in pacchetti o datagrammi per livelli di rete**. I pacchetti contengono anche un header di rete che include la sorgente e la destinazione dell'indirizzo logico. L'indirizzo aiuta le periferiche di rete ad inviare i pacchetti tramite la rete lungo un percorso chiuso.
Step4: Ogni livello di data lynk inserisce i pacchetti **in FRAME**, il frame abilita la periferiche a connettere la prossima periferica direttamente connessa al link.
Step5: Il frame è trasformato in **una serie di 1 e 0**, per la trasmissione sul **media**. Una funzione di clock abilita la periferica a distinguere i bit nel proprio viaggio sul media. Il media può variare, lungo il percorso. Per esempio un messaggio email può avere origine su una lan, tramite un backbone passare un campo e continuare il viaggio tramite la WAN fino a che non raggiunge la propria destinazione in un altro pc all'interno della LAN remota.

Periferiche di rete e Tecnologie: Le maggiori caratteristiche della lan sono le seguenti. La rete opera all'interno su **pavimenti o in edifici**. La rete fornisce multiple connessioni ai servizi di desktop (di solito pc) con accesso a media che supportano banda ELEVATA. Per propria definizione, la rete connette **computer e servizi ad un medium** di alta capacità (ampia banda).
Per propria definizione, la lan connette computer e servizi ad un media comune di livello 1. Le periferiche di lan sono: **BRIDGES connessi alla LAN, che aiutano a filtrare** il traffico. **HUB** che concentrano le connessioni di lan e permettono l'uso di Twisted-Pair copper media. Switches ethernet che offrono la possiblità di avere banda Full duplmex e segmentano il desktop traffic. **ROUTERS** che offrono molti servizi, inlclusi gli **internetworking** ed il controllo del traffico su broadcasting. Possono esistere diverse tecnologie: **ETHERNET**, la prima delle maggiori tecnologie di lan essa comprende il più vasto numero di reti attualmente prodotte.**TOKEN RING**, da IBM, ha seguito ethernet ed è attualmente, usata in un largo numero di reti ibm.
FDDI, utilizza anche i tokens ed è attualmente una lan da campo molto popolare.
Su una rete il livello fisico fornisce accesso al **MEDIA**. Il livello data lynk fornisce supporto per la comunicazione oltre diversi tipi di data links, come ad esempio **ethernet\IEEE 802.3 media**. Tu studierai lo standard IEEE 802,3. Lo schema di indirizzi come ad esempio MAC ed IP fornisce un metodo molto strutturato per trovare e consegnare i dati a computer o host sulla rete.

Gli standar Ethernet IEEE\ 802,3: Ethernet e gli standar IEEE 802,3 **definiscono il bus topology** ed operano ad una banda base di 10 MEGABIT.

10BASE2 (thin Ethernet)—Permette il cablaggio coassiale su segmenti di rete di **186m**
10BASE5 (thick Ethernet)—Permette cavo coassiale, segmenti di **500m**
10BASE-T—Trasporta i frame ethernet su cablaggio **inespensivo twisted-pair wire**.

10 Base 5 e 10Base 2 **forniscono accesso a diverse stazioni sullo stesso segmento** LAN. Le stazioni sono collegate al segmento da un cavo **che passa dall'unità di attaccamento (AUI)** nella stazione al transceiver che è direttamente collegato con l'ethernet cavo coassiale.
Poiché 10BaseT possa fornire accesso ad una singola stazione, **tutte le stazioni che sono collegate alla ethernet lan da 10BASE T** devono sempre essere connesse ad un hub o ad uno switch. In questo arrangiamento, l'hub o lo switch è nello stesso segmento ethernet.
Ethernet a 820,3 data links **preparano i dati** per il trasporto, sul link fisico che congiunge due periferiche.
Il broadcasting è uno strumento molto potente che può inviare un frame a **molte stazioni**, allo stesso tempo. Broadcasting utilizza le destinazioni data link (1) (FFFF.FFFF.FFFF in esadecimale).

Se la stazione A trasmette un frame con indirizzo di destinazione costituito da tutti 1, le stazioni B,C e D riceveranno tutti lo stesso, e lo passeranno al livello superiore per processarlo.
Se impropriamente usato, il broadcasting può avere seri effetti sulla performance delle stazioni, e può causare interruzioni non necessarie. Il Broadcast può essere usato solo quando il MAC address della destinazione è Sconosciuta, o quando si vuole INVIARE un messaggio a tutte le stazioni.

CSMA\CD: Sulle LAN ethernet **solo una trasmissione è permessa allo stesso tempo**. L'ethernet LAN è riferita al **CARRIER SENSE MULTIPLE ACCESS** con **Collision Detection** (CSMA\CD). Questo vuol dire che ogni nodo di trasmissione invia dati che sono ricevuti ed esaminati da **OGNI NODO**. Quando il segnale **raggiuge la fine del segmento**, **i terminatori assorbono esso** e prevengono un ritorno indietro sullo stesso segmento. Quando una stazione vuole trasmettere un segnale, **essa fa un check** sulla rete per vedere se un'altra stazione sta già **trasmettendo**. Se la **rete non è già attualmente utilizzata** da un'altra trasmissione**, la STAZIONE PROCEDE con la trasmissione**. Mentre invia il segnale**, la stazione monitor** la rete per assicurarsi che nessuna altra stazione stia trasmettendo allo stesso tempo. E' possibile che 2 stazioni verifichino che non ci siano trasmissioni e decidano di trasmettere approssimativamente **allo stesso tempo**. **Questo causa una collisione**. Quando vieen rilevata uan collisione, il nodo la riconosce**, esso trasmette un segnale (JAM)** che fa in modo che tutti gli altri nodi riconoscano la collisione. Tutti i nodi trasmittenti quindi smettono di inviare frame per un periodo random selezionato, prima del quale nessuno riprende a trasmettere. Se i seguenti tentativi danno per risultante una nuova collisione, il nodo può provare a retrasmettere tante volte **fino a 15 tentativi**, dopo i quali, smette. L'orologio indica i vari TIMERS di trasmissione.I momenti di non trasmissione delle stazioni. Se 2 TIMERS sono sufficientemente differenti, una stazione può "succeed the next time".

Indirizzamento IP Logico: Un componente essenziale in ogni sistema di network è il processo che permette alle informazioni di **localizzare uno specifico computer sulla rete**. La varietà di indirizzi e schemi è usata a questo scopo, essa dipende dalla famiglia di protocollo inizialmente usata. Per esempio AppleTalk addressing è differente dal TCP\IP addressing che a sua volta è differente da IPX addressing. Due importanti tipologie di addressing sono DATA LINK aaddress e NETWORK address**. Il data link** address è anche chiamato indirizzo fisico hardware address o **MAC**. Sono tipicamente unici per ogni connessione di rete, infatti per molte lan, il **data link address è localizzato sulla NIC**. Poiché un tipico computer ha una sola connessione fisica, esso ha anche un singolo **indirizzo fisico**. I routers ed altri sistemi che sono connessi a molti phisichal network devono avere **multipli indirizzi data link**. Come dice lo stesso nome, gli indirizzi data link esistono a livello 2 del modello OSI. I network addresses, chiamati anche **indirizzi LOGICI o IP ADDRESSES** dell'internet protocol suite, esistono a livello 3 del modello OSI. Diversamente dal data link, che usualmente esiste con un indirizzo **di tipo FLAT**, gli indirizzi livello network sono di tipi HIERARCHICO. In altre parole essi fungono come un indirizzo postale, che decide la locazione di una persona, indicando la contea, stato, zip code, città strada, indirizzo casa, e nome. Un esempio di indirizzo FLAT è US Social Security number. Ogni persona ha un unico social security number, le persone possono muoversi attorno alla contea e ottenere un nuovo indirizzo logico dipendendo dalla propria città, strada, o zip code. Ma il loro numero resta invariato.

Indirizzo MAC: Per permettere a **multiple stazioni di condividere lo stesso MEDIA**, e la stessa identità, IL MAC definisce l'hardware o data link address chiamato **MAC ADDRESS**. Ogni interfaccia di rete ha un indirizzo **unico MAC**. Nella maggior parte delle nic, il mac address è BURNATO all'interno della ROM. Quando la nic si inizializza, questo indirizzo è copiato nella ram.
Prima che le periferiche direttamente connesse alla stessa lan possano scambiare i **DATA FRAME**, la periferica che INVIA deve avere il loro destination MAC ADDDRESS. Un modo in cui l'inviatario può **accertarsi del mac address è usando l'ARP (address resoluzion protocol).**

PRIMO ESEMPIO: Host Y ed host Z sono sulla sterssa lan. Host Y fa un broadcast per una ARP REQUEST alla LAN, cercando l'host Z. Tutte le periferiche vedranno la richiesta (è un broadcast), ma solo l'host Z risponderà con il proprio MAC ADDRESS. L'host Y riceve il messaggio con il mac nella propria local memory chiamata ARP CACHE. La prossima volta che y deve comunicare direttamente con Z userà le informazioni presenti nella stored ARP CACHE riguardo al mac della periferica Z.
SECONDO ESEMPIO: Nel secondo esempio l'host Y e l'host Z sono su differenti LAN ma possono comunicare tramite il ROUTER A. Host Y fa un broadcast della propria ARP REQUEST per l'host Z. Host A determina che l'host Z non può ricevere direttamente la richiesta perché l'ip di Z appartiene ad un'altra rete. Router A quindi determina che il pacchetto dev'essere ROUTATO. Router A fornisce le informazioni che Y richiede. Y riceve ciò che router A gli ha fornito, e salva il mac address nella propria ARP CACHE. La prossiam volta che Y tenterà di comunicare con Z, esso utiizzerà le informazioni memorizzate nella propria ARP cache.

L'ambiente TCP\IP: Nell'ambiente TCP\IP, **le stazioni comunicano con SERVER** o altre stazioni. Questo può accadere perché **ogni nodo** che usa TCP\IP protocol suite, ha **un indirizzo unico, logico di 32 BIT**. Questo indirizzo è conosciuto come **IP ADDRESS**. Ogni compagnia o organizzazione connessa ad una internetwork, è concepita come una singola unica rete, **che deve essere raggiunta, prima che un host all'interno di essa possa essere contattato**. **Ogni compagnia** di rete ha **un indirizzo**, l'host che vive su tale rete condivide il medesimo indirizzo di rete ma ogni host è identificato con un **UNICO indirizzo HOST** sulla rete.

SottoReti: I subnet **migliorano l'efficenza** dell'indirizzamento di rete.L'aggiunta di Subnets non cambia come le periferiche esterne vedono la rete, ma all'interno dell'organizzazione viene a crearsi una struttura addizionale diversificata. L'indirizzo di rete 172.16.0.0 è suddiviso in 4 subnets. 172.16.1.0, 172.16.2.0, 172.16.3.0 e 172.16.4.0. routers determinano la rete di destnazione usando l'ndirizzo di subnet.che limita l'ammontare del traffico sul segmento di rete. Da un indirizzo o un punto statico, i subnet rappresentano una **ESTENSIONE del numero di rete**. Gli amministratori di **rete determinano la dimensione dei subnet basandosi sulla presunta espansione dell'azienda**. Le periferiche di rete usano il **SUBNET MASK per identificare quale parte dell'indirizzo è per la rete e quale rappresenta l'indirizzo degli host.**

Application,Presentation,Session: Livello Applicazione, nel contesto con il modello osi, il livello applicazione, SETTIMO, supporta i **componenti di comunicazione dell'applicazione**. Esso non fornisce servizi ad altri livelli OSI. Quindi esso fornisce servizi ad applicazioni processandole dall'esterno. Un'applicazione può funzionare completamente usando solo l'informazione che risiede sullo stesso computer, in locale. Comunque un'applicazione può anche avere dei compoenti di comunicazione che possono connettersi con applicazioni di rete.
Un esempio può essere, un'applicazione che può includere un trattamento testo (WORD), che incorpora **un componente di trasferimento file che permette al documento di essere trasferito elettronicamente tramite la rete**. Il componente del trasferimento files, qualifica l'applicazione come facente parte del contesto OSI e la classifica come applicazione LIVELLO 7 osi model. Un altro esempio di applicazioe per computer può essere il componente di trasfermento dati che caratterizza uno web browser come netscape navigator, ad esempio. Quando si visita il sito, esso è trasferito sul computer.
Livello Presentazione, Il livello presentazione LIVELLO6, è resposabile per **presentare i dati** in una forma in cui la periferica che li riceve possa comprenderli. E' come un TRADUTTORE che si occupa **dell'interpretazione dei dati**. Per periferiche che necessitano di comunicare oltre la rete, fornendo formattazione e conversione. Questo livello di presentazione **formatta e converte i dati** delle applicazioni di rete in TESTO, GRAFICA, VIDEO, AUDIO e qualsiasi altro formato per cui **la periferica ricevente possa COMPRENDERE ciò che riceve**.

Il livello di presentazione non riguarda solo il formato e la presentazione dei dati, am anche la **STRUTTURA dei dati** e dell'uso del programma. Il livello 6 porta i dati al livello 7. Per capire come lavora questo livello, immagina di vedere 2 sistemi. Un sistema usa EBCDIC ed il router usa ASCII per rappresentare i dati. Quando i 2 sistemi necessitano di comunicare, il livello 6 converte e **traduce** i 2 differenti formati. Un'altra funzione del livello 6 è **l'ENCRIPTION dei dati**.
L'encription è usata dove c'è la necessità di proteggere le informazioni trasmesse da accessi non autorizzati. Per completare questa procedura, i processi e le codifiche locate nel livello 6 **devono convertire i dati.** Altre routenes locale nel livello presentazione, comprimono il testo e **convertono i grafici in BIT STREAM** che possono essere trasmessi sulla rete. Gli standard di livello 6 guidano la modalità di presentazione dell'immagine. Ecco alcuni esempi:
PICT- Un formato di disegno, usato per trasferire Disegni come testo, grafica fra machintosh o powerPC
TIFF-Alta risoluzione, immagini, grafica.
JPEG-Per immagini di qualità fotografica, compresse
Altri standar di livello 6 possono essere..
MID- Musical instruments
MPEG-Video in movimento compresso, con un bit rates superiore a 1.6mbit.
QUICKTIME-Standar video per machintosh o power pc.
Livello Sessione, **Stabilisce, gestisce e termina le sessioni fra applicazioni**, coordina le richieste di servizio e le risposte che avvengono quando l'applicazione stabilisce comunicazioni fra differenti host.

Livello Trasporto: Il livello trasporto è responsabile per il trasporto e per la **regolamentazione del flusso delle informazioni** dalla sorgente alla destinazione, con sicurezza ed accuratezza. Le proprie funzioni includono: **Sincronizzazione della connessione, Controllo di Flusso, Recupero Errori, affidabilità tramite il Windowing**.
Il livello trasporto (LIVELLO 4), abilita le periferiche dell'utente a segmentare le applicazioni di livelli superiori per inserirle nel modello trasmissivo dello stesso livello 4, e da la possibilità alla periferica ricevente di **riassemblare il segmento** di applicazione superiore. La comunicazione di livello 4 è una connessione logica fra punti indipendenti sulla rete, e fornisce **servizi di TRASPORTO** dall'host alla destinazione. Il servizio è spesso riferito ad un Fine to FINE service.
Il livello di trasporto invia i propri dati **come segmenti, garantendo l'integrità dei dati**. Questo trasporto è **CONNECTION-ORIENTED**, relazionato fra i sistemi comunianti. Alcuni delle ragioni per cui il trasporto viene completato con affidibilità… Garantisce che l'inviatario **riceve una conferma del delivery del segmento**. Esso fornisce, **la possibilità di RETRASMETTERE i segmenti che non sono stati confermati**. Fornisce **controlli del traffico** in caso di congestione.
Uno dei problemi che può avvenire, durante il tasporto dei dati, è **il superamento del buffer** sulle periferiche di ricezione. Questo può essere un serio problema che può risultare i perdite di dati. Il livello transport utilizza un metodo chiamato **FLOW COTROL** che **risolve** questo problema.

Funzioni del livello Transport: Ogni livello superiore **esegue una propria funzione**. Queste funzioni **dipendono** dai servizi dei livelli **inferiori**. Tutti i 4 livelli superiori, application,presentation, session e trasport, possono encapsulare i dati in fine-fine segmento.
Il livello trasporto, presume che iesso può usare la rete come una NUVOLA per inviare i pacchetti, dalla sorgente alla destinazione. Se tu esamini le operazioni che partecipano al processo di CLOUD, puoi notare che una delle funzioni che la coinvolge, è la selezione del miglior percorso per il routing. Si inizia quindi a vedere il ruolo che il router esegue in questo processo.
Segmentazione di applicazioni ALTO LIVELLO: Una ragione per usare un modello multi-layers come ad esempio l'osi model è che multiple applicazioni possono condividere la stessa connessione e lo stesso trasporto. La funzionalità di **trasporto** è completata **segmento per segmento**. Questo vuol dire che segmenti differenti che provengono da differenti applicazioni, possono essere inviati

alla stessa destinazione o a diverse destinazioni, sono inviati sul modello FIRST**-COME, First SERVED** baasis. Per capire come questo sistema lavora**, immagina che tu stai inviando una email e trasferendo un file (FTP)** ad un'altra periferica sulla rete. Quando tu invii il tuo Email, prima che l'attuale trasmissione abbia inizio, il software all'interno della tua periferica, **effettua un settaggio su SMTP**, in base al numero della porta. Quindi ogni applicazione invia **un DATA STREAM segmenti,** esso utilizza il numero di porta precedentemente definito. Quando la periferica di destinazione riceve il data stram, **essa separa ed individua il segmento** che il livello trasporto può passare, per indirizzarlo verso la corrispondente applicazione di destinazione.
TCP stabilisce la connessione: Poiché il trasferimento dei dati possa iniziare, il livello trasporto deve stabilire una connection-oriented con il **proprio** Peer-System. Quindi entrambi, l'applicazione inviataria ed il ricevente **devono informare i rispettivi sistemi** operativi che la connessione ha avuto inizio. Contettualmente una periferica effettua una chiamata all'altra periferica che deve accettarla. **Il software del protocollo situato nei 2 sistemi operativi comunica inviando messaggi tramite la rete,** per verificare che il trasferimento sia autorizzato e che entrambi **le periferiche siano PRONTE**.
Dopo che la sincronizzazione è avvenuta, **una connessione viene definitivamente stabilita** ed inizia il **trasferimento dei dati**. Durante il trasferimento, **le due periferiche continuano a comunicare** con i loro protocolli, per verificare se i dati che ricevono **sono integri\corretti**.
Il primo **HANDSHAKE richiede la sincronizzazione**. **Il secondo ed il terzo HANDSHAKE confermano la richiesta** iniziale di sincronizzazione e sincronizzano i parametri nella direzione opposta. Il semento di **HANDSHAKE finale, invia una conferma alla destinazione** comunicando che da entrambi le parti, la connessione è stabilita. Quando **la connessione è stabilita** e tutto queste procedure sono state completate, **il trasferimento inizia**.
TCP invia i dati con Controllo di Flusso: **Mentre il trasferimento** dei dati è in atto, **può avvenire una congestione** a causa di 2 differenti motivi. PRIMO, un computer di **alta velocità** può generare **traffico troppo veloce**, più di quanto la rete possa trasferire. SECONDO, se **numerosi computer inviano datagrammi simultaneamente** ad una singola destinazione, può verificarsi una **congestione** di traffico. Quando i datagrammi **arrivano troppo velocemente al gateway**, esso sono temporaneamente allocati in memoria. Se il traffico continua con tale rimo, il gateway **esaurisce la propria memoria e scarta i datagrammi** addizionali che arrivano.
Anziché permettere la perdita dei dati, la funzione trasporto può effettuare **un "NOT READY"** come segnale per l'inviatario. Questo segnale o indicatore,.ha la funzione di Segnale che dice all'inviatario di STOPPARE l'invio dei dati. Quando il ricevente è invece **Abilitato ad accettare i dati, esso invia un "READY" sull'indicatore** di trasporto che corrisponde ad una disponibilitàù ad accettare i segnali per cui i segmenti vengono **RESUMATI** e riprende il trasferimento.
TCP offre affidabilità con il sistema Windowing: La diponiiblità di un trasferimento di dati **Connection-Oriented**,.sta a significare che grazie ad essa**, i pacchetti arrivano nello stesso ordine in cui sono stato inviati**. La **funzione del protocollo, fallisce** se qualche pacchetto dati è perso, danneggiato, duplicato o ricevuto nell'ordine sbagliato. Per garantire l'affidabilità del trasferimento, **le periferiche riceventi devono confermare la ricezione**, di ogni segmento ad ogni pc.
Se una periferica INVIANTE **deve attendere una conferma** dopo l'invio di ogni segmento, è facile capire che il Troughput potrebe in questo modo essere piuttosto basso. Comunque poiché c'è **un periodo di tempo disponibile**, non utilizzato dopo ogni trasmissione di pacchetto e dopo il processo di ogni conferma, **questo INTERVALLO o lasso di tempo**, può essere usato per trasmettere più dati. Il numero di pacchetti che l'inviatario è abilitato a trasmettere senza ricevere una conferma, **è indicato all'interno della WINDOW**.
Il sistema windowing è **un accordo fra l'inviatario ed il ricevente**. E' un metodo di controllo dell'ammonta delle informazioni che possono essere trasferite dall'inizio alla fine. Molti protocolli **misurano queste informazioni in termini di numeri pacchetti**. **TCP\IP misura le informazioni in termini di numeri di Bytes**. Un esempio può essere caratterizzato da una workstation che invia

ed una che riceve. La prima ha uno windows size 1 e l'altra ha lo windows size 3. **Con il windows size 1, l'inviatario deve attendere per ogni pacchetto trasmesso**. Può inviare solo un pacchetto alla volta. **Con lo windows size 3, invece, l'altro può inviare tre pacchetti alla volta, TRE PACCHETTI prima che debba ricevere una conferma**, quindi ripetere l'invio di altri 3 pacchetti.
La tecnica della conferma TCP: L'affidabilità della consegna è garantita poiché **uno streaming di dati che sono inviati da una periferica,** vengono trasportati tramite un data link ad un'altra periferica, SENZA duplicazioni o perdite di dati. Conferma positiva, con retrasmissione è un processo che garantisce l'affidabilità di consegna dello straming di dati. Esso necessità di un RECIPIENTE dove inviare la Conferma dell'avvenuta ricezione messaggio, in modo che l'inviatario la riceva.
L'inviatario mantiene una registrazione di ogni pacchetto dati che invia e quindi attende la risposta, PRIMA di inviare il prossimo pacchetto. Quindi l'inviatario **fa partire un timer**, nello stesso momento in cui invia il segmento. **Se questo timer Expira, prima che la CONFERMA sia giunta a destinazione il segmento viene reinviato**.

Wan e Routers

Wan e Periferiche: Una Wan (wide area network), **opera al livello fisico e data link** del modello osi. Essa **interconnette LANS** che sono solitamnte separate da **aree geografiche**. Wan fornisce la possibilità di **scambiare pacchetti\frames fra routers\bridges**.
Le meggiori caratteristiche delel wan sono:
Esse operano oltre lo scopo delle lan. (non sono limitate a piccoli spazi come le lan). Esse usano servizi di trasporto come Regional Bell Operating Companies (RBOCs), e Sprint,MCI.
Esse usano connessioni seriale di vario tipo per accedere alla banda di aree dati oltre l'area geografica locale. Per definizione, le WANS collegano periferiche che sono separate da Aree Geografiche, queste periferiche sono: Routers: che offrono molti servizi come ad esempio internetworking e porte di interfaccia WAN, switches: connettono le wan per voce, data e video comunicazioni, modems: Servizio di unità canale\servizio unità digitale (CSU\DSUs) che interfacciano servizi T1\E1. Adattatore Terminale\Terminatore di rete (TA\NT1s) che si interfacciano a Integrated Services Digital Networks (ISDN). Server di comunicazione: Concentrano comunicazioni di Dial-IN e Dial-OUT.
PAN=Personal Area Network.(millimetri) CSN=Computer System Network (metro) LAN=Local Area Network (metri) WAN=Wide Area Network (km)

Gli standards Wan: I protocolli fisici della WAN descrivono come fornire meccanismi elettrici e funzionali per quanto riguarda le connessioni WAN ed i servizi coorelati ad esse. Questi servizi sono molto spessi ottenuti dagli WAN PROVIDERS come ad esempio (RBOCS), alternate carriers, post-telephone, e agenzie telegrafiche. (PTT).
I protocolli data link delle WAN descrivono come i frame sono trasportati attraversi sistemi su una singolo link di dati. Essi includono protocolli designati per operare oltre delicati Point to Point, multiporta e servizi multi accesso (switched), come ad esempio il Frame relay. Gli standards WAN sono definiti e gestiti da un numero di autorità riconosciute:
Internetional Telecomunication Union-Telecomunication Standardization Sector (ITU-T), che forma il comitato internazione di telegrafia e telefonia (CCITT)
International Organization for Standardization (ISO)
Internet Enginering Task Force (IETF)
Electronic Industriesl Association (EIA)

Gli standards Wan tipicamente descrivono sia il livello FISICO (1) che I requisiti in termini di data link (2). Il livello FISICO WAN descrive l'interfaccia fra il l'equipaggiamento a livello terminale (DTE), e il circuito di terminazione dell'equipaggiamento (DCE). Tipicamente il DCE è il Service provider ed il DTE è la periferica wan collegata. In questo modello il servizio offerto al DTE è creato reso possibile da un modem o CSU\DSU.

Livello data link : Router ----- CSU\DSU --- CSU\DSU ----- Router

Livello Fisico Router (DTE) ---------- CSU\DSU (DCE)

Wan tecnologies: ROUTER ---------- ROUTER (PPP) ROUTER---------ISDN (frame relay)

Tecnologie WAN: La seguente, è una descrizione breve delle tecnologie più comunemente utilizzate dalle WAN. Esse sono raggruppate in **Switched-Cricuit, Cell-Switched, Dedicated-Ditigal e Analog Services.**

Circuit-Switched Services: **POTS (plain OLD telephone Service).** Non un servizio di dati computer, ma è incluso per 2 ragioni: Molte delle sue tecnologie fanno parte di un'infrastruttura dati sempre crescente. E' un modello di incredibile affidabilità, facilità d'uso, per le comunicazioni di livello WIDE. Il media usato è il classico Twisted-Pair Copper-Wire. **Nawwowand ISDN:** (integrated services digital network), una tecnologia importante e versatili. E' stata la prima di quelle digitaliy. Utilizzabile da paese a paese, dal costo moderato, la cui massima banda è 128kps BRI (basic rate interface) e 3 MEGABIT per una PRI (primary rate interface) il classico cavo è twisted-pair copper wire.

Packet Switched Services: **X25** , una tecnologia vecchia ma ancora usata, ha un error checking esteso ed è usata da quando le wan erano molto sensibili agli errrori. Può essere utile usare x25 ma la correzione errori provoca un limite di banda. La banda può essere al massimo di 2 MBPS ed il costo moderato-alto. Il cavo mediamente usato è il twisted-pair copper wire. **Frame Relay**: Una versione packet switched dell'isdn. E' diventata estremamente popolare come tecnologia WAN. E' più efficiente di X25, ha dei servizi molto simili ad esso. La banda massima è 44,736MEGABIT, 56kps, 384kps. E' estremamente popolare negli US. L'utilizzo è vasto. Il costo è medio-Basso il cavo utilizzato può essere twisted-pair copper wire o fibra ottica.

Cell-Switched Services: **ATM** (asynchronous transfer mode) Recentemente affiancata ad ISDN, è diventata molto importante per WAN quanto per LAN. Utlizza piccoli frame di 53 byte per il trasporto dei dati. La banda massima è di 622MEGABIT. Il classico cavo è Twisted-pair commer e fibra ottica. Il costo è ALTO, ma l'utilizzo è in constante aumento. **SMDS** (switched multimegabit data services). Recentemente affiancata ad ATM, tipicamente usata nelle MANS. La banda massima è 44.736Megabit, il cavo classico è Twisted-pair copper wire o fibra ottica. Il costo è relativamente Alto, l'utilizzo non è molto frequente.

Dedicated-digital services: **T1,T3,E1,E3**. I servizi di serie T negli stati uniti, e quelli di serie E nell'europa, sono estremamente importanti per le WAN. Essi usano la divisione del multiplexing temporizzata "slice up" ed assegnano degli slot temporali per la trasmissione, la banda è: T1-1,544Megabit, T3-44,736Megabit, E1-2,048Megabit,E3-34,368Megbit. Sono disponibili anche altre bande. Il media usato è tipicamente il Twisted-Pair copper e la fibra ottica. L'utilizzo è MOLTO frequente, il costo è Moderato. **Xdsl** (digital subscriber line and x for family technologies). Una nuova tecnologia LAN creata per l'utilizzo da casa. HA una banda che diminuisce ed aumenta con le distanze dalla centrale telefonica. La velocità top è 51,84Megabit, è

possibile vicino ad una compagnia telefonica. Più comuni sono i casi di banda ridotta (da 100kps a diversi megabits). L'utilizzo è per ora ridotto ma si sta incrementando significativamente. Il costo è moderato ma in discesa. Le varie Xdsl sono: Hdsl (hi bit rate dsl) –Sdsl(single line dsl) –Adsl(asymmetric dsl)-Vdsl(very high bit rate dsl)-Radsl(rate adaptive dsl) **Sonet** (synchronous optical network). Una famiglia di tecnologie il cui mezzo fisico è dotato di alta velocità, designate per le Fibre ottiche ma possono anche funzionare con il copper wire. Hanno una serie di data bit variabili per le varie esigenze di mercato. Sono stati implementati vari livelli di OC (optical carrier), da 51,84Megbit (OC-1) da 9,952Megabit (OC-192). Può raggiungere questi livelli stupefacenti, utilizzando il multiplexing in divisione della lughezza d'onda (WDM), il cui laser è settato per produrre differenti colori (lunghezza d'onda varibile) per inviare grandi quantità di dati sulla fibra ottica. L'utilizzo è frequente fra i backbone internet. Il costo è alto.

Altri servizi per WAN: **Moedm Dial UP** (switched analog) Velocità limitata, molto versatile, lavora con una linea telefonica esistente, la banda è sui 56kps, il costoè basso, l'utilizzo è frequentissimo, il cavo è il Twisted-pair phone line. **Cable Modems** Mettono il signale sullo stesso cavo televisivo. La sua popolarità è stta incrementata in regioni dove si ha un'enorme quantità di cavi televisivi (coassiali, 90% in usa). La banda massima è di 10Megabit, per cui si possono collegare molti utenti (per esempio delle lan). Il costo è relativamente basso, l'utilizzo non è molto frequente ma si sta incrementando. Il media usato è il cavo COASSIALE. **Wireless** Non è necessario nessun MEDIA. Il segnale è elettromagnetico e viaggia nell'aria. ***Terrestrial,*** La banda è tipicamente di 11 MEGABIT, il costo è relativamente basso, è richiesto un collegamento lineare, l'utilizzo è moderato. ***Satellite***, può servire gli utenti mobili (cellulari), e gli utenti remoti tramite un cavo. L'utilizzo è frequente, il costo è ALTO. Alcuni standard utilizzati per mezzi fisici per questa tecnologia. Eia\tia-232, eia\tia-449,v.24,v.35,x.21,G.703,eia-530. **High-Lievel Data Link Control (HDLC)** è uno standard IEEE non può essere compatibile con differenti venditori poiché ogni venditore sceglie una diversa implementazione su esso. HDLC supporta sia le connessioni Point to point che le multiport con minimo carico (overhead). **Frame Relay** Utilizza facilitazioni digitali di alta qalità, usa frame semplici senza correzione di errore. Esso può inviare dati a livello 2 molto più rapidamente degli altri protocolli WAN. **Point-to-Point protocol (PPP)** Descritti da RFC 1661, due standard fatti da IETF contengono fields che identificano il livello di rete. **Simple Data Link Control Protocol (SDLC)** Un protocollo data link per wan designato da IBM. Per system network architecture (SNA). E' sostituito dall'hdlc che garantisce maggiore versatilità. **Serial Line Interface Protocol (SLIP)** E' un protocollo data link per le WAN estremamente popolare che il trasporto dei pacchetti IP. In molte applicazione è sostituito dal più versatile PPP. **Link Acess Procedure Balanced (LAPB)** Un protocollo data link usato da X25. Ha la possibilità estesa di controllare gli errori. **Link Access Procedure D-Channel (LAPD)** E' uno protocollo Wan Data link usato per segnalazioni e chiamate setup su line isdn D-channel. La trasmissione dei dati prende luogo sul canale B dell'isdn. Link **Access Procedure Frame (LAPF)** Per i servizi che si basano sulla modalità frame (riparazione). E' un protocollo data link WAN simile al LAPD, usato con le tecnologie Frame Relay.

Le basi sui Routers: I computers hanno 4 componenti base: CPU,memoria,interfacce e BUS. Un router ha anch'esso 4 COMPONENTI. Anch'esso può esser definito computer. E' un computer con degli speciali compiti. Invece di avere componenti che sono deducati all'audio ed al video, ed hanno periferiche di output quali mouse o tastiera, il router è dedicato solo al ROUTING. I computer necessitano di sistema operativo per eseguire le applicazioni software. Il router necessita di un Internetworking operating software (IOS) per eseguire i file di configurazione. Questi file di configurazione controllono il flusso dati ed il traffico dei routers. Specificatamente utilizzando i routing protocols per direzionare i ROUTED protocols e le tavole di routing. Essi effettuano le decisioni riguardanti il miglior percorso per i pacchetti. Per controllare questi protocolli e per prendere queste decisioni, il router DEVE essere configurato. Verrà speso molto tempo in questo

semestre per imparare come Costruire dei files di configurazione da comandi IOS per permettere al router di eseguire le funzione di rete che si desidera. Ad un primo sguardo la configurazione dei routers potrà sempbrare complessa, ma verso la fine del semestre saremo in grdo di leggere e di comprendere essa. Il router è computer che seleziona il miglior percorso e gestisce gli switching di pacchetti fra reti differenti. La configurazione del router è la seguente:

RAM\DRAM memorizza le tavole di routing, la cache arp, la fast switching-cache, il packet buffering (shared ram) e le queue per i pakketti vecchi. La ram fornisce anche energia temporane per il file configuration del router, mentre esso è Acceso. Il contenuto della RAM è perduro quando il router viene spento o riavviato.

NV\RAM E' una ram non vlatile che memorizza i backup\dati del router e la configurazione file e NON VA VIA quando il router viene riavviato o spento.

FLASH E' una memoria Cancellabile e riprogrammabile (ROM). Tiene l'immagine del sistema operativo e del microcodice. Puoi fare l'update del software senza rimuovere o sostituire il chip nel processore. Il contenuto della flash resta anche quando si spegne o si riavvia. Possono esser contenute molte versioni di IOS nella memoria FLASH.

ROM Contiene la diagnostica di accensone, il programma di Bootstrap ed il software del sistema operativo. L'upgrade del software nella rom, richiede la sostituzione del chip sostituibile Sulla cpu.

INTERFACE La connessione di rete attraverso la quale pacchetti entrano ed escono nel router, essa può essere sulla motheboard o su un modulo separato.

Le funzioni del router in una lan: Mentre i routers possono essere usati per segmentare la lan, non dobbiamo dimenticare che il loro uso più frequente è con le WAN devices. I routers hanno sia LAN che WAN interfaces. Infatti le tecnologie WAN sono usate frequentemente per collegare routers. Essi comunicano con altre periferiche con connessioni WAN, e creano sistemi autonomi per i collegamenti backbone ed internet.I router sono periferiche di backbone per ampie intranet facenti parte di internet, essi operano a livello 3 del modello osi, effettuano decisioni in base all'indirizzo network (IP). LE 2 funzioni principali dei router sono la selezione del miglior percorso per paccketti in entrata e lo switching di packetti sulla propria interfaccia di uscita. Router completano ciò, costruendo delle routing tables e scembiando le informazioni di rete contenute in esse, con altri routers. E' possibile configurare le routing tables a mano, ma disolito esse sono mantenute dinamicamente usando un routing protocol che cambia la topologia di rete (path) con altri routers.

Se per esempio tu vuoi che un computer (x) sia abilitato a comunicare con altri computer (y), e con altri sulla terra sulla terra (z) e sul sistema solare. Tu puoi includere una funzione di routing per flusso di informazioni e affidabilità di percorso. Molte reti designano decisioni e tecnologia che possono tracciare i computer x,y,e z per abilitarli a comunicare su internetworks. Le internetwork possono anche includere: End to end addressing, indirizzo che rappresenta la tipologia di rete, la migliore selezione di percorso, dinamic routing e switching.

Tipologia del Laboratorio di Routing: La topologia di laboratorio del semestre è può essere interpretato come un sistema per mezzo del quale si possa imparare ad implementare wan e collegare uffici nel mondo. La wan può non essere collegata ad internet. Può essere una compagnia privata..Nel mondo. Tuttavia la topologia, come mostrato, non è ridondante. Un guasto in qualche router, potrà interrompere le comunicazioni. Questa wan, nonché RETE di reti, è controllata da una amministrazione comune, chiamata sistema autonomo.

Internet è la rete di Sistemi Autonomi, ognuno dei quali ha un router che gioca un proprio Ruolo, importante.
Router interni (interni ad una determinata area), Area border routers (connettono due o più aree), Backbone routers (percorso primario per il traffico, è molto spesso usato come sorgente per molte altre reti). Sistemi autonomi (AS) boundary routers.(Comunicano con i routers in sistemi autonomi) Quindi nessuna entità lì controlla. Le entità tipiche sono:
Corporazioni (MCI world com,sprint,AT&T,Qwuest,UUNET,France Telecom)
Università (university of illinois, stanfort university)
Instituti di ricerca (CERN in swizerland)
Internet service provider (ISPs).
Quanto spiego nel semestre è non riguarda il modello internet ma il modello di una tipologia che può rappresentare un sistema autonomo. Il protocollo che è routed universalmente è IP, il routing protocol BGP è largamente usato negli internet routers.
Router A in kuala, RouterB in san francisco, Router C a new york, Router D e E a parigi. Oguno dei router connette un ufficio o un lan campus. Le connessioni fra A-B, B-C, C-D sono basate su T1, che sono collegate sulle interfacce seriali dei routers. Ogni router della rete è enthernet è collegato ad essa. Topicamente le periferiche sulla rete ethernet e gli host sono mostrati attraverso un console cable che va al routers, grazie al quale è possibile vedere la configurazione interna del router. Questi 4 routers hanno, fra loro, una serial wide area connection.

ROUTER CLI

Utente e modalità privilegiate: Per **configurare** i routers cisco, è possibile **accedere all'interfaccia utente** sul router con un terminale o accedere al router via remoto. Quando si accede ad un router, **si deve inserire il login**, prima di inserire altri comandi.
Per sicurezza il router ha **2 livelli di access commands**.
USER MODE (tipicamente opeazioni che includono **il controllo dello status del router**, in questa modalità il cambio delle configurazioni non è permesso).
PRIVILEGED MODE (operazione tipica che iclude anche **il cambio delle configurazioni del router**)
Quando ci logghiamo sul router per la **prima volta**, possiamo vedere il router **PROMPT**. I comandi disponibili a questo livello utente sono caratterizzati da un **subset di comandi disponibili** solo al livello privilegiato. Per maggior parte, questi comandi ti permettono di **visualizzare informazioni senza cambiare i settaggi** e le configurazioni del router.
Per accedere ai **pieni set di comandi**, bisogna prima abilitare il **PRIVILEGED mode**. Al prompt è necessario scrivere **"ENABLE".** Alla richiesta di password **si deve inserire una parola chiave** che è stata precedentemente settata con il comando **"ENABLE SECRET"**. Da quando hai completato lo step di login, il prompt **cambia la visuale aggiungendo una #.** Questo vuol dire che siamo in privileges mode. Nella modalità privilegiata tu puoi accedere a modalità come ad esempio la GLOBAL configuration mode o altre specifiche modalità.
Interfaccia, sottointerfaccia, linea, router, route-map, configurazioni addizionali dei routers..
Per **uscire**, infine, è necessario digitare **EXIT**.
La schermata di uscita varia con **specifici software IOS** della configurazione router.

Lista di comandi su USER MODE: Digitando il punto **interrogativo (?)** nella user mode o nella modalità privilegiata, si visualizza **una lisa di comandi usati**. Il comando **"—More—"** infondo allo stesso display mostra **un continuo** delle informazioni disponibili. Se sei preme un tasto è possibile **continuare a vedere** il prossimo screen di informazioni (premere barra spaziatrice). Per visualizzare la prossima linea si deve premere il tasto invio. Si preme ogni altro tasto per tornare al prompt.

Lista dei comandi in PRIVILEGE MODE: Per accedere alla modalità privilegiata **è necessario scrivere "ENABLE".** Verrà chiesta la password. Successivamente **digitando il punto interrogativo (?) si potrà avere la lista di comandi** proprio come avviene nella modalità user. **L'abbreviazione di enable si ha con il comando "ENA".**

Le funzioni HELP del router: Supponiamo che si voglia vedere il CLOCK del router. Se **non si conosce** il comando da usare, allora digitiamo **"HELP"** e **controlliamo la sintassi** per il settaggio del clock. Dunque impareremo a conoscere **il comando HELP**. Dunque settiamo il clock del router. Ipotizziamo che **non si conoscano i parametri**del comando Clock.

1) Utilizziamo **help per verificare la sintassi** del settaggio CLOCK. L'Help è necessario per vedere i comandi di clock.
2) **Controllare** la sintassi per cambiare il **TIME**.
3) **Inserisci** quindi i dati, utilizzando ORE, Minuti e secondi, come mostrato dall'help. In sistema indica che tu devi fornire informazioni addizionali per completare il comando. Il comando "SET" è necessario.
4) Verifica la sintassi inserendo il tempo, le ore, minuti e secondi.
5) Se non si ha inserito tutto con completezza, il sistema ci dirà che i dati forniti non sono sufficienti per cui si preme CNTRL+P per ripetere ciò che è stato scritto precedentemente. Si può aggiugnere un **"PUNTO INTERROGATIVO" per chiedere al sistema di completare gli argomenti, quindi è possibile vedere COME completare il determinato** comando. Quando si ha un errore, si visualizza il simbolo ^, si può capire che proprio qui c'è l'errore.Quindi si Re-inserisce il comando corretto nello stesso punto in cui compare il simbolo di errore. Oppure si scrive un ? per saperne di più.
6) Quando **si trova la sintassi corretta**, basta digitarla e premere invio.

L'interfaccia utente fornisce la sintassi di controllo inserendo **il simbolo ^ dove si verifica l'errore**. **Il simbolo ^ appare nel punto della stringa dove si ha inserito un comando incorretto**. L'indicatore di error location e l'aiuto interattivo, sono un aiuto per trovare facilmente la corretta sintassi di utilizzo dei comandi.

Utilizzare i comandi IOS di editing: L'interfaccia utente include una modalità **editing avanzata** che fornisce un set di **chiavi di editing** e funzioniche ci permettonodi editare le linee di comando per come esse sono scritte.
Si utulizzano determinate chiavi a sequenza per **muovere il cursore attorno alla command line** per eventuali **correzioni o cambiamenti**. La modalità di editing avanzata è **attivata automaticamente**. Per **disabilitare** questa possibilità dovremo scrivere **"TERMINAL NO EDITING"**, **nella modalità privilegiata**. Per editare i comandi esistono varie funzioni di **scrolling** che estendono quelli standard (linea singole sulla sinistra dello skermo). Quando il cursore raggiunge il margine di destina, il cursore torna indietro **di 10 spazi**, non è possibile visualizzare 10 caratteri sulla linea, ma si può scrollare indietro e correggere la sintassi e l'inizio del comando. Per scrollare in dietro si **preme "CTRL-B" o la freccia sinistra, ripetutamente** finchè non si arriva all'inizio del rigo di comando. O premere **"CTRL-A" per andare direttamente all'inizio linea**. Vediamo il caso in cui un comando si estende oltre una linea. Quando il cursore raggiunge la fine della linea, contuniamo a scrivere sotto per cui il cursore torna di nuovo indietro di 10 spazi, sulla sinistra. **Il dollaro ($) indica che la linea è stata scrollata a sinistra. Ogni volta che si arriva alla fine, il testo continua sotto e si torna indietro di 10 spazi sulla sinistra**.

Utilizzo dell'history con comandi IOS: L'interfaccia utente fornisce **una history**, di comandi che hai inserito. Questa funzione è **particolarmente utile** per **richiamare** i lunghi e complessi **comandi**. Con la history puoi completare le seguenti operazioni: **Settare l'history buffer**, richiamare comandi, disabilitare la funzione di history.

Default la histotry command è attivata ed il sistema **registra** nel proprio buffer **10 commands line**. Per cambiare il numero di linee comando che il sistema può registrare durante una sessione terminale, utilizzare **"terminal hystory size", o "history size". Il numero massimo di comandi è 256**.
Per richiamare i comandi che sono situati nel buffer dell'history si inizia dal più recente, si preme **"CTRL-P" o il tasto UP ripetutamente** per richiamare i successivi comandi in ordine **dal più recente al meno recente**. Per **tornare al comando più recente** nel buffer storico, dopo aver premuto CTRL-P o UP, **si preme "CTRL-N" o DOWN ripetutamente** per richiamare comandi in ordine dal più vecchio al più recente. Mentre si digitano i comandi, per far prima, **si può inserire un unico carattere per il comando e premere TAB**. L'interfaccia **completerà** il comando. La lettera unica indica il comando, **la funzione TAB effettua semplicemente un riconoscimento visuale**, sempre che il router abbia inserito tale comando nelle sue entries.
La maggior parte dei computer può avere funzioni di copia e select addizionali**. Puoi colpiare un precedente comando ed incollarlo come tua attuale entry.**Premendo **RETURN**. Infine puoi **usare "CTRL-Z" per uscire** della modalità configurazione.

ROUTER COMPONENTS

Sorgenti esterne di configurazione Router: In questa sezione, si impareranno a conoscere i **componenti** del router che hanno un ruolo chiave nel processo di configurazione. Conoscendo quali componenti sono coinvolti nel processo di configurazione, potremo capire al maglio, come il router memorizza ed usa i comandi di configurazione. Essere consapevole di quelli che sono i passi durante l'inizializzazione del router, ci aiuterà a determinare che cosa può accadere e dove i problemi possono verificarsi, mentre il router si avvia.
E' possibile **configurare** il router **da locazioni esterne**, incluse le seguenti:
Dal terminale console (un computer connesso tramite la porta console) durante la sua installazione.
Via modem utilizzando la porta Auxiliary. AUX.
Via Terminale virtuale 0-4, dopo che il router è installato sul netowork.
Da un **TFTP** server sulla rete.

Componenti interni del Router: L'architettura interna di un router cisco, supporta componenti che giocano un ruolo importante nell'avvio del router. I componenti interni del router, sono i seguenti:

RAM\D-RAM – Memorizza le routing **TABLES, L'arp Cache, Fast Switching cache**, il packet buffering (shared), e le vecchie queues di pacchetti. La ram inoltre fornisce **temporanea memoria per una configurazione** file di un router, mentre questo è alimentato. Il contenuto della ram è perso quando il router viene spento o riavviato.
NVRAM – E' una ram **non volatile**. Memorizza i **files di configurazione** per backup e startup.Il contenuto della NVRAM è trattenuto durante lo spegnimento ed il restart del router.
FLASH – Cancellabile e Programmabile ROM che contiene **l'immagine del sistema operativ**o ed il microcodice. La memoria FLASH abilita il software a fare **gli update** senza rimuovere né sostituire il chip sul processore.Il contenuto della flash non è perso quando si riavvia o si arresta il router. La memoria flash può memorizzare **versioni multiple di IOS**.
ROM – contiene la **diagnostica** per il POWER ON, **il programma di BOOTSTRAP** ed il sistema operativo (software). L'upgrade del software in rom, necessita la rimozione e la sostituzione del chip sulla cpu.
INTERFACES – Le connessioni di rete **sulla scheda madre** o sui moduli separati tramite i quali i pacchetti entrano ed escono dal router.

Ram per lo Storage del Router: LA Ram è **un'area di memorizzazione** del router. Quando si accende il router, **la ROM esegue il Bootstrap** program, questo programma effettua **alcuni test** e quindi **carica** il software cisco **in memoria**. Il comando esecutivo, o **EXEC, è una parte** del cisco software IOS. **EXEC riceve ed esegue comandi** che tu inserisci nel router.
Il router usa anche la **ram per memorizzare un file attivo di configurazione** e mappare tavole di rete, e liste di indirizzi di routing. Puoi visualizzare il file di configurazione sulla console remota o terminale. **Una versione salvata di questo file è memorizzata sulla NVRAM**. Ad esso avviene un accesso e **viene caricato in memoria ogni volta** che il router inizializza. Il file di configurazione contiene i processi globali e le informazioni d'interfaccia che riguardano direttamente le operazioni del router e le proprie porte di interfacciamento.
Un'immagine di sistema operativo non può essere visualizzata su uno screen di terminale. Una immagine è eseguita spesso dalla ram principale e caricata da diverse sorgenti di input. Il software operativo, è organizzato in routines che **direzionano** i task associati **con differenti protocolli**, come movimenti di dati, tavole e gestione buffer, updates del routing ed esecuzione di comandi.

Le modalità del Router: Quando si **accede** dalla console o da un'aplicazione telnet, o ancora, da una tty port, **il router può essere posizionato** in diverse posizioni. Ogni modalità **fornisce diverse funzioni:**

User Exec mode – E' una modalità che ti permette di **vedere info del router**.
Privileges EXEC mode – E' una modalità che **supporta il debugging** ed il testing command, esame dettagliato del router, **manipolazione dei file di config** ed accesso alla modalità config
Setup Mode – Questa modalità rappresenta un **prompt interattivo di dialogo** alla console che aiuta il nuovo uternte a creare la configurazione per la prima volta
Global Config MODE – Questa modalità **implementa i comandi powefu**l online che eseguono tastk **semplici di configurazione**.
Other Config MODE – Queste modalità forniscono **maggiori dettagli** sulle multiple line configurations.
RXBOOT Mode – Questa modalità può essere usata per fare **un deleting della password** e recuperarla, è utile in caso il sistema si sia cancellato dalla flash.

Esaminare lo STATUS del Router: In questa sezione impareremo i comandi base che possiamo usare per determinare lo stato corrente del router. Questi comandi ci aiuteranno ad ottenere informazioni vitali che si necessitano quando si monitorizza e si fa il troubleshooting delle operazioni del router. E' importante essere in grado di monitorare lo stato di salute in ogni momenti. I router cisco hanno una serie di comandi che ci permettono di determinare quando il router funziona correttamente o quando si sono verificati dei problemi. I comandi di status del router e le loro descrizioni sono i seguenti:

SHOW VERSION – Visualizza la **configurazione del sistema hardware e la versione software**, il nome e la sorgente del **file di configurazione** e l'immagine **di boot**.
SHOW PROCESSES – Visualizza informazioni sui **processi attivi**.
SHOW PROTOCOLS – Visualizza i **protocolli configurati**; Mostra lo stato di tutti i **protocolli di livello 3** configurate.
SHOW MEMORY – Visualizza le **statistiche sulla memoria** del router, includendo le statistiche sul memory free pool.
SHOW STACKS – Monitorizza **l'utilizzo dello stack dei processi** e gli interrupt routines, e visualizza **la ragione dell'ultimo boot** di sistema.
SHOW BUFFERS – Fornisce **statistiche sul buffer** pools nel router.
SHOW FLASH – Mostra **informazioni sulla flash** memory

SHOW RUNNING-CONFIG (scritto in termini Cisco dalla release 10.3 o precedenti), visualizza i file di configurazione **attualmente attivi**
SHOW STARTUP-CONFIG (cisco 10.3 o precedenti) Visualizza **i file backup di configurazione** (NVRAM)
SHOW INTERFACES – Visualizza le **statistiche per tutte le interfacce** configurate sul router.

I comandi show-running config e show startup config: Fra i cisco, il comando di EXEC più usato è **SHOW RUNNING-CONFIG** e **SHOW STARTUP-CONFIG**. Essi permettono ad un amministratore di **vedere il la configurazione corrente** sul router, o i comandi di **startup** che il router userà al prossimo restart. E' necessario eseguire questo comando **da ENA**.
I comandi **WRITER TERM** e **SHOW CONFIG** sono usati da cisco release 10.3 o inferiori, sono stato **sostituiti** da nuovi comandi. Questo comandi hanno continuato a sostituirsi, l'attuale documentazione non ci fornisce degli aggiornamenti, e cambiamenti che potranno riguardare il futuro. Puoi riconoscere il file configuration attivo tramite la digitura **CURRENT CONFIGURATION**. Puoi riconoscere un backup di file configurazioe quando vedi il messaggio sul TOP che ti dice Quanta memoria **NON-Volatile** hai utilizzato.

Show Interface, Version, Protocol: Il comando **SHOW INTEFACES** visualizza **i parametri configurabili e le statistiche** in tempo reale riguardo **tutte le interfacce configurate sul router**. Il comando **SHOW VERSION** visualizza informazioni sulla **versione software** del cisco IOS che è attualmente in esecuzione sul router.
E' anche possibile usare **SHOW PROTOCOLS** per visualizzare **il protocollo configurato** sul router. Questo comando visualizza **lo status globale** di un'interfaccia specifica e di ogni protocollo di livello3, configurato. (IP,DECnet,IPX,AppleTalk).

Ottenere l'accesso ad altri router, usando CDP: il **Cisco Discovery Protocol (CDP)** fornisce un comando singolo e proprietario che **abilita gli amministratori** di rete ad accedere ad un sommario dei dati similari, nelle **configurazioni di altri router direttamente collegati**.
CDP funziona tramite il livello **DATA LYNK** che connette i bassi livelli (1) ed i livelli di rete (3). Poiché esso possa operare a questo livello, le periferice CDP che supportano differenti livelli di rete, possono apprendere luna dall'altra e **settarsi automaticamente** sul corretto livello di funzionamento.
Quando una periferica cisco che ha in esecuzione CISCO IOS 10.3 o precedente, **fa il boot**, **il CDP parte automaticamente** e **rileva** nelle vicinanze, **altri router** o periferiche **che utilizzano CDP**. Questa estensione avviene su tutte le apparecchiature oltre **l'utilizzo del TCP\IP** (non solo tcp\ip!) ed include le apparecchiature **direttamente connesse**, della cisco, riaguardo o meno il livello dei protocolli che essi usano, **siano di livello 3 o livello 4.**

Visualizzazione delle CDP entries: L'uso primario del CDP è **scoprire le piattaforme e protocolli** nelle periferiche che si trovano nelle **vicinanze**. Utilizza il comando **SHOW CDP NEIGHBORS** per visualizzare i CDP **updates sul router locale**. Ogni router sta eseguendo CDP e **scambiando** informazioni riguardo ogni entries nei protocolli, **con i router nelle vicinanze**. L'amministratore **può visualizzare i risultati del CDP** information Exchange **su una console** che è **connessa ad un router**, configurato per esseguire CDP su queste interfacce. L'amministratore di rete usa il comando **SHOW** per visualizzare informazioni **sulle reti direttamente collegate** al router. CDP fornisce informazioni **su ogni periferica CDP nelle vicinanze**. I valori sono i seguenti:

Device Identifiers – **L'host name** configurato del router, ed il **domain name** (di ognuno)
Address List – Almeno un indirizzo per SNMP, fino ad **un indirizzo per ciascun protocollo** supportato
Port Identifier – Identificativo **porta**. Ethernet0,Ethernet1,Serial0.. Ecc.ecc

Capabilities List – Se la periferica ha **un ruolo di Sorgente** verso un bridge, o router.
Version –Informazione **che viene fornita dal computer locale** « show version »
Platform –La **piattaforma** sulla periferica (hardware). Es. Cisco 7000.

Per **ottenere le CDP** informations da routers **non direttamente** connessi **è necessario Telnettarli**.

Un esempio di configurazione CDP: CDP **si inizializza automaticamente** dopo che una periferica si è avviata. Il CDP funziona normalmente e **parte, di default**, quando un product cisco, parte con release 10.3 o successiva. **Solo i router direttamente connessi** nelle vicinanze possono scambiare i CDP frames. Un router **inserisce in cache** le informazioni che riceve da **un altro devices con CDP nelle vicinanze**. Se nella sottosequenza del frame CDP è indicato che una delle **informazioni** riguardanti il router nelle vicinanze è **cambiata**, il router **scarta altre informazioni e le sostituisce con le nuove**.
Utilizzare il comando **SHOW CDP INTERFACE** per vedere i valori del CDP timers, lo **status** dell'interfaccia e **l'encapsulation utilizzata** da CDP per il suo **annuncio** e la scoperta di trasmissione frame. I valori di default per i timer **settano la frequenza per gli update** CDP e per l'**invecchiamento** delle entry CDP. Questi timers sono **settati automaticamente**, a 60 secondi e 180 secondi rispettivamente. Se la periferica **riceve un update più recente, o se il time-hold espira**, la periferica **deve scartare il CDP entry**.

Visualizza CDP entries, per una periferica e CDP vicini: CDP è stato **designato ed implementato** come un protocollo **molto semplice e di basso peso**. Un Frame CDP **può essere piccolo** e **recupera moltissime informazioni** utili sui routers nelle vicinanze. Si può utilizzare il comando **SHOW CDP ENTRY** (device name) per visualizzare **una singola entry** CDP. Nota che l'effettuarsi di questo comando, include tutto lo **strato 3 di indirizzi**, presenti nel router B (vicino). Un amministratore può **vedere gli indirizzi ip** CDP (routerB) con un singolo comando inserito (entry), sul router A. Il tempo di attesa durante ilquale viene conteggiato il timer, si intende come tempo trascorso da quando il frame CDP arriva con questa informazione. Il comando include versioni abbreviate delle informazioni sul router B.
Si usa il comando **SHOW CDP NEIGHBORS** per visualizzare i **CDP updates** ricevuti sul computer locale. Per ogni porta locale il display mostra le seguenti cose:

ID della periferica vicina.
La **porta** locale, TIPO E NUMERO.
Il tempo in **DECREMENTO timer**, il valore è espresso in secondi.
Codice di **Capienza** della periferica vicina.
Piattaforma hardware della periferica vicina
Numero **della porta e Tipo di porta** della periferica vicina

Per visualizzare questa informazione al meglio nella stessa forma del **SHOW CDP ENTRY**, si può usare il comando opzionale **SHOW CDP NEIGHBORS DETAIL**.

Se si sta usando una IOS cisco release 10.3 o più nuova, è necessario abilitare il CDP su tutte le interfacce della periferica, usando il comando **CDP ENABLE**. Usando il comando **SHOW CDP INTERFACE** si avrà accesso al gruppo di informazioni CDP usate per **annuncio** e scoperta della trasmissione frame. Utilizzare **SHOW CDP NEIGHBORS e SHOW CDP NEIGHBORS DETAIL** per visualizzare gli **updates CDP** ricevuti dal router locale.

Test dei processi che usano il modello OSI: Il problema maggiormente comune che può avvenire nelle reti IP è il **risultato di Errori nello schema di addressing**. E' importante **testare** la propria configurazione di **indirizzi prima di continuare con steps di configurazioni future**. Il test base di

una rete deve avvenire in una forma sequenziale basata sul modello osi. **Livello per Livello**. **Telnet, Ping, Trace, Shop Ip Route, Show Interfaces e Debug**, sono comandi che ci permettono di testare la rete. **SHOW INTERFACE (Layer 1,2,3). PING, TRACE,IP ROUTE (Layer 3), TELNET (Layer7).**

Test del Livello Applicazione usando Telnet: Un altro modo per **apprendere** sui router remoti è **connettersi ad essi**. Telnet, un protocollo basato su **terminale virtuale**, che è parte della suite TCP\IP, permette connessioni eseguite verso l'host. E' possibile settare una connessione fra il router e la periferica connessa. Telnet ci permette di **verificare il livello applicazione** fra sorgente e destinazione. Questo è un test dal meccanismo **molto completo**. Un router può avere **più di 5 connessioni telnet** contemporanee.
Iniziamo il test mettendo a fuoco **il livello superiore** osi (applications). Il comando telnet **fornisce un terminale virtuale** che gli amministratori possono usare **per le operazioni telnet** per connettersi ad altri router **su cui gira TCP\IP**. **Con l'implementazione** cisco TCP\IP, **non è necessario inserire il comando CONNECT o TELNET per stabilire una connessione Telnet**. Se preferiamo, possiamo **solo inserire l'host name**. Per **chiudere** una sessione Telnet, utilizzare Il comando EXEC "**exit**" o "logout".
La lista seguente comprende i comandi alternativi per operazioni:

Inizializzare una sessione da denver

```
Denver> connect paris
Denver> paris
Denver> 131.108.100.152
```

Resumare una sessione (inserisci il numero sessione o nome):

```
Denver>1
Paris>
```

Terminare una sessione:

```
Paris> exit
```

Come abbiamo imparato l'applicazione telnet **fornisce un terminare virtuale** per cui tu **puoi connettere altri host** su cui sta girando **TCP\IP**.
E' possibile utilizzare Telnet per **eseguire un test** che determina **se o no si può accedere ad un router remoto**. E' possibile, successivamente utilizzare Telnet per connettere Il router YORK al router PARIS, quindi eseguire un test base di comunicazioni di rete.
Se puoi accedere **da remoto ad un altro router** tramite telnet, tu sai che **almeno una delle applicazioni TCP\IP** può raggiungere il computer remoto. Una connessione telnet che ha successo, indica che **il livello superiore** di applicazione (e **quindi i livelli inferiori**, ovviamente) funzionano **propriamente**. Se noi possiamo telnettare un router ma non un altro router, è probabile che ciò fallisca a causa di uno specifico errore sull'addressing name, o a causa di un problema di permissions. Questi problemi possono esistere sul router SORGENTE o sul router di destinazione che non si riesce a connettere. Il **prossimo step** è provare a **PINGARE il router**. Questo comando ti pemetterà di **testare** il collegamento **a livello network**.

Test della rete usando il comando PING: Come aiuto per la diagnostica della connettività base di rete, molti protocolli di rete supportano il protocollo ECHO. **Echo è usato per controllare** se i pacchetti in un determinato protocollo sono indirizzati (being routed). In comando **ping, invia** un pacchetto ad un host di destinazione e quindi **attende per la risposta** dell'altro host. I risultati da questo echo protocol **possono aiutare per valutare l'affidabilità** nel collegamento **PATH-TO-HOST**, il **ritardo** nel percorso, e , se l'host può essere **raggiunto o meno**. (funzionalità host).

Puoi usare il comando **Ping USER EXEC** per diagnosticare **connettività** di rete a livello Base. Il ping usa **ICMP** (Internet Control Message Protocol).

Test della rete usando il comando TRACE: Il comando trace **è il tool ideale** per vedere **dove** i dati sono inviati sulla rete. Il comando TRACE è **simile al ping**, eccetto la connettivistà END-to End, il TRACE **testa ogni step** lungo il percorso, questa operazione può essere performata sia nella modalità user che privilegiata (EXEC).
Il comando trace porta visione degli **errori generati** dai router quando il pacchetto eccede il tempo limite per il TTL. Il comando tracert **invia molti pacchetti** e visualizza **il tempo di round-trip** per ognuno. Il beneficio di trace è che esso dice **quale router nel percorso è l'ultimo ad essere raggiunto, questo è chiamato FAULT ISOLATION**.
In questo esempio noi stiamo tracciando un percorso da YORK a ROMA. Lungo il percorso,bisognerà passare da Londra a Parigi. Se uno dei routers è irraggiungibile, si segna un asterisco accanto al nome del router. Il comando TRACE continua a cercare di raggiungere il prossimo obiettivo, finchè non si preme CTRL-SHIFT-canc.
Testare la rete con il comando SHOW IP ROUTE: Il router **offre molti strumenti** potenti in questo punto della ricerca, puoi prendere visione delle **routing tables** nelle direzioni in cui il router determina **come il traffico dev'essere diretto** sulla rete. Il prossimo test baso, si focalizzerà sul livello network (3). Usando il comando **SHOW IP ROUTE** per determnare **se una entry, su routing table, esiste per la rete che vogliamo connettere**. Ad esempio Roma 131.108.33.0 è raggiungibile da parigi, 131.108.16.2 tramite **l'interfaccia ethernet1**.

Utilizzo comando SHOW INTERFACE Serial per testare livello Fisico e Data link:
L'interfaccia ha 2 componenti, quella FISICA (hardware) e LOGICA (software).
HARDWARE , possiamo parlare di cavi, connettori ed interfacce, per **effettuare la connessione** attuale fra periferiche.
SOFTWARE è contenuto nel messaggio , un messaggio che tiene **viva la connessione**, **informazioni di controllo**, ed informazioni utente che passa alle applicazioni adiacenti, i dati sono trasferiti fra router connessi ed interfacce.
Quando si testa il **livello Fisico e data link**, bisogna porsi queste domande:

C'è un **segnale** rilevato?
E' di buona **qualità il link fisico** fra le periferiche?
Abbiamo ricevuto **il messaggio** di KEEPALIVE?
I pacchetti **possono passare** sul mezzo fisico?

Uno dei compiti può importanti del comando di uscita **SHOW INTERFACE SERIAL** è **visualizzare le linee dello status protocollo data link**. La linea di status è indicata da **un segnale di portante** e si riferisce allo **status sul mezzo fisico**. Può anche essere indicata dai keepalives frames, in questo caso **si riferisce al data link framing**.

Il comando Show Interface e Clear Counter: Il router traccia le **statistiche** che forniscono informazioni sull'interfaccia, è possibile usare il comando **SHOW INTERFACE** che visualizza **varie statistiche**. LE statistiche riflettono le operazioni del router **dall'ultima volta in cui il contatore si è esaurito**. Utilizzare il comando **CLEAR COUNTERS** per **resettare** il contatore a Zero. Partendo da zero si ha una facilitazione visiva dello stato corrente della rete.

Controllo in tempo reale del traffico con il DEBUG: L'apparato router comprende hardware e software; Possiamo prendere in considerazione questi 2 elementi per effettuare il tracking dei problemi, su di esso e sugli host all'interno della rete. L'exec command **DEBUG PRIVILEGED**, fa partire la console e visualizza gli **eventi della rete specifici** nel parametro del comando.

Utilizzando il comando **TERMINAL MONITOR** si può fare un **forward dei dati** di debug **ad una sessione telnet di terminale.**
In questo esempio abbiamo ricevuto un broadcast da un router. Utilizzando il programma **UNDEBUG ALL** (nessun debug), si **disabilita il debug** quando non se ne ha necessità. Il debug è concepito per risolvere problemi, **quando non è necessario, va disabilitato**.
Bisogna fare ATTENZIONE: Il debugging **può creare traffico** sulla rete e rallentamenti significativi. Non lasciare il debug su ON. Utilizzarlo solo per diagnosticare i problemi e quindi reimpostarlo su OFF.
Per default, il router invia al sistema messaggi di errore del comando exec DEBUG, alla console**. I messaggi possono essere ridirezionati ad un host unix**, nel suo buffer interno. Il comando **TERMINAL MONITOR** ti da al possibilità di **redirezionare questi messaggi ad un terminale**.

Router Setup e Startup

Routine di startup del Router: Un router si **inizializza facendo il BootStrap**, caricando il sistema operativo ed i file di **configurazione**. Se il router **non può trovare** un file di configurazione, esso entra nella modalità **setup**. Il router memorizza nella **NV-RAM una copia di backup** del file di configurazione dalla modalità setup.
Lo scopo delle routine di startup per il cisco IOS software, è far partire le operazioni del router. Il router deve rilasciare una performance affidabile sul proprio lavoro, connettendo gl utenti ad internetworks, ed a server configurati. Le routine di startup devono:

- Assicurarsi che il routers si avvi ed abbia **esaminato l'hardware**
- Trovare il **cisco IOS locale** che il router utilizza come sistema operativo principale.
- Trovare ed applicare le **regole di configurazione** sul router, incluse le funzioni rel protocollo e gli indirizzi delle interfacce

Quando un router cisco si avvia, esso esegue un auto test **POST (power on self test).** Durante questo auto test, il router esegue la **diagnostica da rom**, su tutti i moduli hardware. Questa diagnostica verifica le operazioni base della cpu, memoria e interfacce di rete\porte. Dopo la verifica delle funzioni hardware il router procede con l'inizializzazione del software.

Sequenza di Startup del Router: A seguito dell'auto test, si verificano i seguenti eventi:
STEP1 – **Il boostrap generico**, dei dati che sono sulla rom, eseguiti dalla cpu. Il bootstrap è una semplice operazione di preset che serve per caricare istruzioni che sono state copiate in memoria, può a questo punto entrare nella modelità configurazione\setup.
STEP2 – **Il sistema operativo** può essere trovato in una delle possibili posizioni. La posizione è indicata nel campo boot del registro di configurazione. Se il campo boot indica una flah o la rete, per caricare il BOOT SYSTEM, nel file di configurazione viene anche indicatio l'esatto percorso dove si trova l'immagine.
STEP3 – L'immagine del **sistema operativo è caricata**. Quindi, quando essa è caricata ed è operativa, il sistema **operativo inizia a localizzare i componenti hardware e software** e la lista dei risultati sulla console del terminale.
STEP4 – Il file di configurazione che è **salvato nella NVRAM**. **E' caricato nella memoria principale** e esegue una linea per volta. Questi comandi di configurazione **eseguono il processo di routing**, di indirizzi per interfacce, caterristiche media e successivi processi.
STEP5 – Se **non esiste una configurazione valida nella NVRAM**, il sistema operativo esegue una domanda derivante dalla routine di configurazione, derivata dal sistem configuration, anche chiamata **SETUP DIALOG**.

Il setup non è inteso come una modalità per **entrare nelle impostazioni** relative alle complesse funzionalità **del protocollo** che usa il router.
Si dovrebbe usare il **SETUP** per apportare modifiche al sistema per quanto riguarda le configurazioni **minime**, quindi si usano i comandi di **VARIOUS configurtion-mode**, per la maggior parte delle configurazioni relative ai tasks del router.

Comandi relazionati allo Startup del Router: I 2 comandi **SHOW STARTUP-CONFIG e SHOW RUNNING-CONFIG** visualizzano l'attivo file di **configurazione e quello di backup**. Per cancellare lo Startup-Config si usa **ERASE STARTUP-CONFIG**. Questo comando cancella i file di configurazione di backup presenti nella NVRAM. Il comando **RELOAD, fa il reboot del router**, causa un ripetersi dell'intero processo di startup. Il comando **SETUP è usato per entrare nella modalità setup dalla pozione PRIVILEGIATA-**EXEC (enable).

Utilizzo del comando setup: Una delle routine della configurazione iniziale è la modalità SETUP. Come hai già imparato in questa lezione, il proposito principale della modalità SETUP, **è trasportare** una **configurazione minima** per un altro router che non può trovare la configurazione da altre sorgenti. Per molti dei suggerimenti, nella schermata di configurazione sistema del comando setup, **le risposte di default appaiono fra parentesi**. (premi return per usare i settaggi di default). Se il sistema è stato precedentemente configurato, il default che appare, sarà APPLICATO correntemente. Se questa è la prima volta che configuriamo il sistema, fornirà i dati base. Se non ci sono dei dati di default, come password, ad esempio, non è visualizzato niente dopo il punto interrogativo. Durante il processo di setup, **è possibile premere CTRL+C per terminarlo** e ripartire da capo. Quando il setup è terminato, tutte le interfacce saranno riavviate.Quando avremo completato il processo di configurazione nella modalità setup, lo screen visualizzerà la configurazione che hai appena creato, Tu verrà chiesto se tu vuoi usare questa configurazione. **Inserisci yes e la configurazione verrà eseguita e salvata nella NVRAM**. Se rispondi NO, la configurazione non sarà salvata ed ho il processo reinizierà ancora da capo. Se appare il **MORE**, premi **barra spaziatrice** per continuare.

Settaggio dei parametri Globali: Dopo aver visto il corrente sommario, un prompt apparirà sul tuo monitor, indicando che tu stai per accedere ai **GLOBAL PARAMETERS** del router. Questi parametri sono i **valori di configurazione** che si scelgono. Un prompt appare sul monitor ed indica che abbiamo avuto accesso ai parametri che si settano per il router. Questi parametri sono i valori di configurazione che abbiamo deciso. Permettono inanzitutto di **settare l'hostname del router**. Il nome host sarà **parte del CISCO IOS** prompt per tutte le modalità di configurazione. Nella configurazione iniziale, il nome del router, come **default**, è visualizzato, fra parentesi quadrate **"ROUTER**".
Si utilizza la prossima schermata di configurazione globale, per settare le varie passwords usate sul router. Bisogna inserire una password per **"enable".** Quando si inserisce una stringa di password **"ENABLE SECRET",** i caratteri sono processati da una encryption proprietaria cisco. Questo aumenta la sicurezza della stringa di dati che compongono la password.Quando qualcuno tenterà di fare un listato del contentuto del file di configurazione router, questa password apparirà come una stringa di caratteri incomprensibili.
Il comando **setup** non richieda che si setti una "ENABLE PASSWORD", bensì una **"ENABLE SECRET WORD"**. Quest'ultima è una parola crittografica "one-way" che viene usata al posto di e"enable passoword" quando essa Esiste. **"enable password" è usata quando non esiste nessuna "enable secret word"**. Essa è anche usata **con vecchie versioni** di IOS. Tutte le password devono essere **alfanumeriche.** Quando ti verranno chiesti i parametri per ogni interfaccia installata, si devono utilizzare dei valori precedentemente scelti per il router. Quindi si risponderà YES alle richieste addizionali riguardanti il protocollo.

Settaggio dei parametri dell'interfaccia: Quando ci verranno chiesti i parametri per ogni interfaccia installata si dovranno usare i valori di configurazione che si sono determinati per l'interfaccia al prompt

Settaggio SCRIPT , review ed utilizzo: Quando si **completa il processo di configurazione** per le interfacce che sono installate sul router, il comando **SETUP visualizzerà la configurazione** che si è creata. Il comando SETUP quindi **chiederà se tu vuoi utilizzare questa** configurazione. Se rispondi **di sì** la configurazione **sarà eseguita e salvata nella NVRAM**. Se si risponde NO, la configurazione non verrà salvata ed il processo ricomincerà ancora. Non esiste la possibilità di tornare ad un default prompt, **c'è solo la possibilità di rispondere YES o NO**. Dopo aver inserito YES all'ultima domanda, il sistema sarà pronto per essere usato. Se si desidera modificare la configurazione che si è da poco effettuata, bisognerà fare ciò manualmente. Lo script ti chiederà di usare la modalità configurazione per cambiare ogni comando DOPO CHE sarà usata la modalità setup. **Il file script generato dal setup, è aggiuntivo**. Puoi abilitare le features con setup ma non puoi disabilitarle. Inoltre **setup non supporta diverse features del router**, o operazioni che richiedono **configurazioni più complesse**.

CONFIGURAZIONE ROUTER 1

Informazioni File di configurazione Router: In questa sezione si imparerà come lavorare con i files di configurazione, che possono venire dalla console, dalla NVRAM o da un TFTP server. Un router utilizza le seguenti informazioni dal file di configurazione mentre esso parte:
Versione software IOS
Identificazione Router
Locazione dei file di BOOT
Informazione sul Protocollo
Configurazione Interfaccia
Il file di configurazione contiene i comandi per customizzare le operazioni del router. Il router utilizza queste informazioni **in fase di partenza**. **Se non ci sono** file di configurazione disponibili, il sistema **ti giuda con un setup wizard per la creazione delle config** mancanti.

Lavorare con file di configurazione Release 11.x: Le informazioni di configurazione del router, possono essere **generate in diversi** modi. E' possibile usare il comando **PRIVILEGED EXEC configure, da un terminale virtuale (remoto), una connessione modem o una console**. Questo ci permette di accedere **alle configurazioni** e cambiarle in ogni momento. Si può anche usare **il comando EXEC CONFIGURE** per caricare una configurazione **dal TFTP server** che ci permette di mantenere e caricare le informazioni da un sito centrale. L'elenco seguente descrive brevemente alcuni dei **comandi di configurazione**:

Configure Terminal –Configura manualmente **dalla console** terminale
Configure Memory – Carica la configurazione **dalla NVRAM**
Configure Tftp Running-Config – Carica le informazioni di configurazione **da un TFTP SERVER alla ram**.
Show Running-Config – **Visualizza** la configurazione corrente **nella RAM**
Show Running-Config Startup-Config – Memorizza la configurazione corrente **dalla RAM alla NVRAM**.
Copy Running-Config TFTP – Memorizza la configurazione corrente **dalla RAM al TFTP server**.
Show Startup-Config – **Visualizza** la configurazione salvata, che è contenuta **nella NVRAM**
Erase Startup-Config – **Cancella** il contenuto della **NVRAM**

Lavorare con le PRE-RELEASES 11.0 dei file di configurazione: Alcuni dei comandi della versione 10.3 **sono vecchi**. E sono stati sostituiti con nuovi comandi. I vecchi comandi che sono stati sostituiti, continuano ad eseguire le normali funzioni, ma non sono supportati dalla documentazione. Quest'ultima verrà ricreata nelle future releases.
I vecchi comandi:
Config Term, Write Term, Config Mem, Write Mem, Config Net, Write Net, Show Config, Write Erase.

Coping Running-Config TFTP, e Copy TFTP Running-Config: E' possibile memorizzare una copia corrente della configurazione sul server TFTP. Si usa **COPY RUNNING-CONFIG TFTP** per memorizzare la configurazione corrente in ram **Su un server TFTP** di rete. Quindi completare i seguenti steps:

1) Inserisci il comando **COPY RUNNING-CONFIG TFTP**.
2) Inserisci l'indirizzo **ip** dell'host che vuoi usare per memorizzare il file di configurazione
3) Inserisci **il nome** che vuoi assegnare al file di configurazione
4) **Confermare** le tue scelte dando YES ogni volta

E' possibile configurare il router, caricando **il file di configurazione memorizzato in un server** di rete, quindi completare i seguenti task:

1) Entra nella modalità configurazione inserendo **COPY TFTP RUNNING-CONFIG**
2) Al prompt di sistema, **seleziona** un file di configurazione situato su un host. Il file di configurazione continee i comandi che si applicano a tutti i routers, ed ai terminali server sulla rete. Il file di configurazione sull'host contiene dei comandi applicabili particolarmente al router, al propt di sistema inserire l'indirizzo io (opzionale) dell'host dal quale si desidera prendere il file di configurazione. In questo esempio, il router è configurato da un server TFTP il cui indirizzo ip è 131.108.2.155
3) Al prompt di sistema inserire **il nome del file di configurazione o accettare il nome di default**. La conversione del nome file, è convertita su base unix. Il nome del file di default è **HOSTNAME –CONFIG** per il file host e **NETWORK –CONFIG** per il file di configurazione di rete. Nella metodologia dos, il nome del file, è limitato ad 8 caratteri, più 3 caratteri di estensione. Conferma il file di configurazione e l'indirizzo del server che il sistema supporta.

Notice in the figure that the router prompt changes to `tokyo` immediately. This is evidence that the reconfiguration happens as soon as the new file is downloaded.

Utilizzo della NVRAM con release 11.x: Questi comandi gestiscono il **contenuto della NVRAM**.
Configure Memory –**Carica** le informazioni di configurazione **dalla NVRAM**
Erase Startup-Config –**Cancella** il contenuto **della NVRAM**
Copy Running-Config Startup-Config –**Memorizza** la configurazione corrente **dalla Ram** (configurazione corrente) **alla NVRAM** (startup o backup configuration)
Show Startup-Config –**Visualizza** la configurazione salvata, che è il conenuto **della NVRAM**.

Utilizzare NVRAM Con le release precedenti alle 11.0 IOS: I comandi utilizzati con release 10.3 o precedenti **sono vecchi**, questi sono stati sostituiti con nuovi comandi. I comandi che sono stati sostituiti continuano ad eseguire la loro normale funzione nella versione corrente ma non sono molto documentati. Il supporto per questi comandi verrà rilasciato in versioni successive. I comandi vecchi sono i seguenti:
Configure Memory, Write Erase, Write Memory.

Utilizzare le modalità di configurazione del Router: La modlità di **Esecuzione**, **interpreta i comandi** che vengono digitati e **trasporta i risultati** delle corrispondenti operazioni. E' possibile **loggarsi** sul router prima di inserire un comando EXEC. Ci sono 2 Modalità EXEC. I comandi EXEC **disponibili un USER mode** ed i comandi **disponibili in Privileged Mode**. Dalla modalità **privilegiata**, puoi accedere alla configurazione globale e specificare le modalità di configurazione, alcune di queste sono le seguenti:
Interface
SubInterface
Controller
Map-List
Map-Class
Line
Router
IPX-Router
Route Map
Se si scrive **EXIT, il router tornerà indietro di un livello**. Eventualmente si avrà la possiiblità di loggarsi fuori. In generale, digitando EXIT da una delle specifiche configurazioni, si ritorna alla global configuration mode. **Premendo CTRL+Z si esce completamente** dalla global configuration mode **e si ritorna alla modalità EXEC privilegiata**.

Modalità di configurazione Globali: I comandi di configurazione globale, si utilizzano sulle caratteristiche che riguardano il sistema nel suo insieme. Si usa il Privileged Exec command **"CONFIGURE"** per entrare **nella global configuration mode**. Quando si inserisce questo comando, l'exec ci chiede un comando di configurazione.
E' possibile qundi specificare su, **NVRAM o un file memorizzato su un server di rete**, come sorgente. Il settaggio di default è scritto sulla console terminale. Premere RETURN per iniziare la configurazione. I comandi per abilitare **un particolare routing o funzione di interfaccia**, **si inizializzano con i comandi di global configuration**.
Per configurare **un protocollo di routing** utilizzare il comando **CONFIG-ROUTER** (prima entrare nel global router protocol command type)
Per configurare **una interfaccia** utilizzare il comando **CONFIG-IF** (prima inserisci il numero interfaccia ed il tipo)
Per terminare digitare EXIT.

Configurare i Protocolli di Routing: Dopo che il **protocollo di routing è abilitato** da un comando globale, la configurazione router **ROUTER (CONFIG-ROUTER)#** è visualizzato. Quindi digitare ? per avere la lista dei subcommands per il protocollo.

Comandi di configurazione Interfacce: Poichè tutte le interfacce del router siano settate automaticamente in down mode, molte funzionalità devono essere **abilitate sulla base dell'interfaccia**. **I comandi** di configurazione intefacce **modificano l'operazione dell'ethernet**, token ring, o seriale. In aggiunta, **i subcommand dell'interfaccia seguono sempre i comandi dell'interfaccia** poiché i comandi interfaccia definiscono solo il TIPO di interfaccia.

Configurare una interfaccia Specifica: Il primo set di comandi **è associato all'interfaccia**. Sulla seriale, **una parte fornisce il segnale di clocking**, questo riguarda la **DCE**. L'altro l'altro è DTE per default. I cisco routers **sono periferiche DTE per default**, ma inalcuni casi **possono essere usati come periferiche DCE**. Se si sta usando una interfaccia che fornisce il clocking, bisognerà

specificare il CLOCKRATE. (comando). **Il comando BANDWIDTH** sovrascrive il Bandwidth di default che è mostrato in **"show interface"** ed è usato da alcuni protocolli di routing come **IGRP**. Il secondo set di comandi è associato alla serie 4000 dei router cisco. Sul cisco 4000, ci sono 2 connessioni all'esterno del box dell'interfaccia (collegata alla aui), ed al connettore 10baseT. Il default port è AUI, ma **bisogna specificare media-type 10BASE-T**, se desideri utilizzare questa anziché la AUI.

Metodi di configurazione per relase 11x: Entrare nelle statistiche di configurazione, **esaminare i cambiamenti che sono stati fatti**, se necessario modificare o rimuovere le statistiche di configurazione, salvare **i cambiamenti su un backup nella NVRAM che il router userà in fase di partenza**.

Metodi di configurazione per le PRE-Relases 11.0: I comandi della versione 10.3 sono vecchi, essi sono stati sostituiti con nuovi comandi, i vecchi comandi che sono stati sostituiti continuano ad eseguire le normali funzioni nella corrente relase ma non sono molto documentati, il supporto per questi comandi verrà illustrato nelle future release.

Metodi di configurazione Password: E' possibile dare sicurezza al sistema usando **la password per la restrizione di accesso**. Le password possono essere settate **sia per linee individuali che per la Privileged Exec Mode.**
Line **Console 0** –**Setta una password** sulla console del terminale
Line Vty 0 4 –Setta **la protezione password** per connessioni **Telnet**
Enable Password –Setta la password per la **modalità** privilegiata
Enable Secret Password –(dai parametri globali,system config dialog, una un sncryption proprietario cisco per alterare la stringa di caratteri)
Tu puoi comunque **proteggere la password** utilizzando il **SERVICE PASSWORD-ENCRYPTION**. Questo encryption non combacia con gli standard **"data encryption srtandard"** (DES)

Configurazione Ident Router: La configurazione delle periferiche di rete, **determina il comportamento della rete**. Per gestire la configurazione delle periferiche, è necessario **listare e comparare i file di configurazione delle periferiche**, quelli in esecuzione e quelli memorizzati sui server di rete per accesso condiviso ed effettuare le installazioni del software,quando necessario, per upgrade.
Una delle operazioni base **è dare un nome al router**. Il nome del router **è considerato l'host name** ed è anche il nome visualizzato nel prompt di sistema. Se non si configura un nome il sistema assegnerà un nome di default al router, **per cui sarà "Router".** Puoi nominare il router in una modalità di configurazione.
E' possibile **settare il messaggio del giorno** che verrà visualizzato **su tutti i terminali connessi**, questo messaggio **verrà visualizzato al login**, è utile per indicare messaggi ed info sul router, per configurare questo messaggio usare il comando **"BANNER MOTD" nella global config mode**.

Immagini di IOS

Localizzare il software IOS: La **sorgente** di default per i cisco IOS e lo startup, **dipende dalla piattaforma** software. Ma più comunemente il router cerca il **sistema di BOOT** salvato nella NVRAM. Comunque esiste la possibilità di scegliere per **varie alternative**. Puoi specificare **un'altra sorgente** per il router nella quale cercare il software, il router userà queste impostazioni

per localizzare e caricare il software. I settaggi nel registro di configurazione, permettono le seguenti alternative..:

E' possibile **specificare il sistema di boot** della global configuration-mode, per entrare. Il settaggio nel registro di configurazione offre le seguenti alternative.

- E' possibile **specificare i comandi** di boot system che il router usa in **sequenza**. **Salva** queste (statements = affermazioni ???) **in NVRAM** per usarle al successivo avvio con il comando **COPY RUNNING-CONFIG STARTUP-CONFIG**. Il router **userà** questi comandi quando ne ha bisogno, in successione, **al riavvio**.

- Se la NVRAM non contiene comandi per il boot system, il router può utilizzare, **in alternativa**, il **default cisco IOS nella memoria FLASH**.

- Se la **flash è vuota**, il router può provare con **l'alternativa TFTP**. Il router utilizza questa configurazione registrata da un file dal quale il router fa il boot e carica l'immagine, opportunamente memorizzata su un server di rete.

Valori di configurazione: Poichè il router possa rilevare le **informazioni di boostrap**, esse devono essere settate **nel campo BOOT**, all'interno del registro di configurazione.
E' possibile **cambiare** il settaggio di default applicato al registro di configurazione con il comando **CONFIG-REGISTER** nel global config mode. Bisogna usare numeri esadecimali come opzione per questo comando.
Un esempio, il registro di configurazione è settato in modo tale **da esaminare il file startum nella NVRAM** per trovare un sistema di **boot**. Il **registro è a 16BIT** nella NVRAM. **Gli ultimi 4 bit**, quelli inferiori, all'interno del registro di configurazione sono riservati **al campo BOOT**.
Per effettuare delle variazioni al campo boot, e lasciare tutti i bit nell'impostazioni originale, (inizialmente il registro contine 0x010x), seguire le seguenti istruzioni:

- Settare il valore del registro a 0x100 **se si necessita di entrare nel rom monitor**. Dal rom monitor, far partire il sistema operativo utilizzando il B command al prompt del rom monitor. (questo valore setta i bit di partenza 0-0-0-0.
- Settare il registro di configurazione su **0x101 per configurare il sistema di boot** automatiamente **dalla rom** (Questo valore, nel campo boot 0-0-0-1)
- Settare il registro di configurazione ad ogni valore patendo da 0x102 **fino a 0x10F per configurare il sistema** per utilizzare il sistema di **boot nella NVRAM**. Questo è il settaggio di default. (Questi valori nel campo boot, rappresentano i bit da 0-0-1-0 a 1-1-1-1)

Per verificare i settaggi nel campo BOOT, utilizzare il comando **CONFIG-REGISTER** e poi **SHOW VERSION**.

Il comando SHOW VERSION: Il comando **show version** visualizza informazioni relative al **software cisco IOS** che sta girando sul router. Questo include il **registro** di configurazione ed il settaggio relativo al **campo BOOT**. (vedere sulla configurazione di questo esempio nelle prossime righe). In questo esempio, la versione di cisco IOS e l'informazione descrittiva, è accentuata sulla seconda linea di output. Lo screen catturato mostra una versione sperimentale della release 11.2. La linea mostra in nome dell'immagine di sistema.

"`System image file is "c4500-f-mz", booted via tftp from 171.69.1.129`"

`Impareremo di più in seguito riguardo alla release 11,2 cisco IOS. Per adesso, analizzamo la porzione del file che indica che questa immagine è designata per una piattaforma cisco 4500.`

A seguito di un continuo di output, il comando **SHOW VERSION**, visualizza **informazioni relative al tipo di piattaforma** su cui la versione del cisco IOS sta girando attualmente. Il testo evidenziato fornisce i risultati del comando **CONFIG-REGISTER 0x10F** che è usato per entrare **nei valori di configurazione** del registro.

Comando di Boot Sistema: I seguenti esempi mstrano come **è possibile inserire comandi multipli di boot system**, per specificare la **sequenza di ricerca** dei cisco IOS software durante il boot. I tre esempi mostrano le entries del sistema di boot che specificano che l'immagine IOS verrà inizialmente caricata **dalla memoria FLASH**, poi **da un server TFTP** di rete ed alla fine, in minima parte, **dalla ROM**.

- **Memoria Flash** – E' possibile caricare una immagine di sistema dalla EEPROM. Questo vantaggio è che le informazioni memorizzate nella flash memory (eeprom), **non sono vulenrabili ad errori di rete**, cosa che può verificarsi nel caricamento dell'IOS dal TFTP server.
- **Server di RETE** – Nel caso in cui la **flash** memory sia **corrotta**, si esegue un backup dopo di che si specifica che l'immagine dell'ios dev'essere caricata **dal TFTP server**.
- **ROM** – Se la memoria Flash è corrotta e il server TFTP fallisce nel caricare l'immagine, il **boot dalla rom è il tentativo finale** nel software. Comunque l'immagine del sistema situata all'interno della rom, è una **sottoversone** dell'intero cisco IOS software. In questa versione ridotta **mancano i protocolli, le caratteristiche e le configurazioni** che però sono presenti nella versione completa. Se si è fatto un update del router, solo l'ultima volta che si è acquistato, può esistere in questa sezione una vecchia versione del cisco IOS software.

Il comando **COPY RUNNING-CONFIG STARTUP-CONFIG salva i comandi** all'interno della NVRAM. Il router esegue i comandi di boot per sua necessità, in modo che essi siano situati dove erano originariamente, nel momento in cui siamo entrati nella modalità di config.

Preparazione per usare il TFTP: La produzione delle internetworks solitamente **copre una vasta area**, e include **multipli routers**. Questi, sono distribuito geograficamente e necessitano **di una sorgente di backup**, dove allocare le immagini software. UN **TFTP server** permette di far **transitare tutte le immagini di configurazione** di cui c'è bisogno, tramite la rete. Un server tftp **può essere** direttamente **un altro router**, o un sistema **HOST**. Esempio: UN server TFTP può essere una **workstation su cui gira UNIX**. L'host TFTP può essere rappresntatoda un qualsiasi sistema che abbia **caricato il software TFTP** e sia abilitato a ricevere comunicazioni TCP\IP dalla rete. La copia del software TFTP avverrà **sulla FLASH** del router. Prima di effettuare tale operazione bisognerà preparare le condizioni per cui essa possa esssere effettuata. Controllare le seguenti condizioni preliminari:

- **Dal router**, verificare di esser sicuri di avere **accesso al server TFTP** sulla rete TCP\IP. Il comando ping, è un ottimo strumento per verificare ciò.
- **Sul router** è necessario assicurarsi che esso possa scrivere **e leggere dalla flash memory** interna. Verificare se il router ha **sufficiente spazio** in memoria per accogliere **l'immagine IOS.**
- **Sul server TFTP** bisogna assicurarsi di avere **spazio per l'immagine cisco IOS**, per upload e download, **è necessario specificare il nome file e percorso**.

Questi steps di controllo garantiranno una copia perfetta. Se si interferisce (rush??) nella copia del file, questa può vallire ed è necessario effettuare un troubleshooting sulla causa del fallimento del processo.

Il comando SHOW FLASH: Utilizzare il comando **SHOW FLASH** per verificare **se si ha sufficiente memoria** sul sistema per ospitare il cisco IOS. Un esempio. Abbiamo un router che ha 4 MB di memoria flash, tutti e 4i mb sono disponibili. E' necessario paragonare tale spazio con la **dimensione dell'immagine cisco IOS**. Lo spazio generato dall'immagine **deve includere il**

software documentativo o i dati di uscita dall'applicazione di configurazione software relativi al collegamento online (CCO) o comandi del tipo DIR o LS situati sul TFTP server.
Se **NON c'è sufficiente spazio** in memoria, non si potrà copiare o caricare l'immagine, il che vuol dire che si potrà **soltato** caricare **una versione ridotta\inferiore del cisco IOS**. In alternativa è possibile amentare lo spazio disponibile sul router.
E' considerata una buona idea, tenere una copia di backup dell'immagine IOS, per ogni router. Si dovrà quindi fare il backup, con costanza, prima di updatare sul router nuove versioni di IOS.

Convenzioni di nomi del Cisco IOS: I prodotti cisco hanno **subìto un'espansione** oltre i generici router. Possiamo trovare **molte piattaforme** o prodotti per le reti e l'analisi di spettro.
Per ottimizzar questo concetto per cui il software CISCO IOS opera con questa grande varietà di piattaforme, si deve innanzitutto sapere che cisco lavora per **Creare differenti tipi di IOS** a seconda della necessità. Queste immagini sono **perfettamente compatibili** con le varie piattaforme,le quali dispongono di **memoria e funzionalità adeguate** per ospitare le IOS.
La conversione nominativa della cisco 11.2 IOS è composta da 3 parti:

- La piattaforma **su cui** l'immagine viene eseguita
- **Una lettera o una serie di lettere** che identificano le speciali **possibilità e funzionalità** settate per essere **supportate dall'immagine**.
- Specifiche sul luogo dove l'immagine sta girando e se essa è **stata compressa o zippata**.

La conversione nominativa del cisco IOS, e le convenzioni standard ad essa legata, contenuti, immagini, ed altri dettagli sono soggetti a cambiamenti.

Il comando COPY FLASH TFTP: E' necessario copiare un'immagine di sistema, in blocco su un server di rete. Questa copia dell'immagine di sistema può servire come **copia di backup** ed **è anche utilizzata per verificare** che la copia presente sulla flash **sia integra** allo stato originale.
Un esempio: Un amministratore sta facendo il backup della sua corrente immagine situata nel router, su un server TFTP. Esso utilizza il comando **SHOW FLASH** per visualizzare **il nome dell'immagine** (xk09140z) ed il comando **COPY FLASH TFTP** per copiare l'immagine **sul server TFTP**. I files possono essere **rinominati durante il trasferimento**.
Una ragione per questo upload sul server è **fornire una sicurezza alla corrente immagine** prima di fare un update con una nuova versione. Quindi se con questa nuova versione si verificassero dei problemi, l'amministratore può di nuovo ripristinare la vecchia immagine, scaricandola dal TFTP server.

Il comando COPY TFTP FLASH: Dopo aver effettuato una copia di backup del corrente IOS, si può caricare una nuova immagine. **Si scarica la nuova immagine dal TFTP server**, usando il comando COPY TFTP FLASH.
Questo comando inizia **richiedendo l'ip address** dell'host remoto che funge da TFTP server. Poi verrà chiesto **il nome dell'immagine IOS**. E' necessario inserire il nome corretto del file per fare un update dell'immagine come nominata sul server TFTP.

Come caricare un'immagine IOS di backup: Se c'è necessità di caricare una versione di **backup dell'ios**, usare il comando **COPY TFTP FLASH** che ci permette di scaricare l'immagine precedentemente uploadata sull'TFTP server.
Dopo aver inserito il comando **COPY TFTP FLASH** il sistema chiederà **l'indirizzo ip o l'host del server TFTP**. Con ciò si può **anche** intendere **il nome di un altro router** che renderà **servibile** la propria **ROM o FLASH**. Il sistema quindi chiederà il nome del file dell'immagine IOS. Se sulla flash esiste un'immagine con nome C4500-I e si chiede di copiarci sopra un file image con lo stesso nome, il sistema ci dirà che l'immagine con quel nome, esiste già. Quindi **rispondendo di sì** alla domanda overwite, il file sarà **cancellato e sostituito** con la nuova copia. **Se** esistono **2 copie di ios** nella flash memory, **la vecchia copia è resa inutilizzabile in favore della nuova versione** e verrà

listata **con la proprietà DELETED** (parentesiquadre) quandos i esegue il comando **SHOW FLASH**.
Se si annulla il processo di copia il nuovo file **sarà marcato come deleted perché non è stato copiato per intero e quindi non è valido\utilizzabile**. In questo caso il sistema **continuerà ad utilizzare il primo fil**e.

Configurazione Router 2

Processo di configurazione Router e recupero passw:

Just as the router configuration file has different parts to it, the router configuration process also has different parts.
A common procedure that technicians perform on routers is the password recovery procedure. The Figure shows the procedure for both the 1600 and 2500 Series routers. This procedure/series of commands is also a good review of the IOS.

Processi di configurazioen router:

- Loggarsi sul router
- Entrare in modalità Privilegiata
- Inserire la password
- Configurare le interfacce (int E0, S0 ecc.ecc)
- Configurare i protocolli di routing (Router Rip, Aigrip, ecc.ecc)
- Configurare i dns (Ip,Host)
- Esaminare la configurazione
- Show RUN
- Tirare su le interfacce
- OK-PARTENZA
- Salvare i dati dalla Ram alla NVRAM

Router (CONFIG-IF) “ip address”
Router (CONFIG-ROUTER) “network”
Router (CONFIG-LINE) “password”

Se il router non può avviarsi fare il BOOT (ctrl+BREAK).
Se è un 25xx, 0x2142
Se è un 16xx, 0x2142

1) entrare nel router
2) Enable
3) Configure Terminal
4) Hostname LAB_A
5) Enable secret CLASS
6) Line console 0
7) Login
8) Password Cisco
9) exit
10) interface ethernet 0
11) ip addresss 192.5.5.1 255.255.255.0
12) no shutdown
13) interface ethernet 1
14) ip address 205.7.5.1 255.255.255.0
15) no shutdown
16) interface serial 0
17) ip address 201.100.11.1. 255.255.255.0
18) clock rate 56000
19) no shutdown
20) exit
21) router rip
22) network 192.5.5.0
23) network 205.7.5.1
24) network 201.100.11.1
25) exit
26) ip host lab_a 192.5.5.1 205.5.5.1 201.100.11.1
27) ip host lab_b 219.17.100.1 199.6.13.1 201.100.11.2
28) ip host lab_c 233.8.151.1 204.204.7.1 199.6.13.2
29) ip host lab_d 210.93.105.1 204.204.7.2
30) ip host lab_e 210.93.105.2
31) show running config
32) copy running-config startup-config
33) reload

TCP\IP

La suite del protocollo TCP\IP ed il modello OSI: La suite del protocollo CP\IP è stata creata come parte di ricerca costituita dall'agency DEFENCE ADVANCHED RESEARCH PROJECT (DARPA). Esso originariamente è stato architettato per fornire comunicazioni **tramite DARPA**. Più tardi, il tcp\ip è stato incluso con le distribuzioni di unix. Adesso il tcp\ip è fattore standard delle comunicazioni di internetworking e server come protocollo di trasporto per interent, permettendo a milioni di computer di comunicare globalmente.
Questo paragrafo su basa su tcp\ip, esso è molto importante, i motivi sono molteplici.

- Tcp\IP **è un protocollo universalmente disponibile** che viene usato per lavoro
- Tcp\IP **è usato come referenza per comprendere altri protocolli** poiché esso include elementi che possono rappresentare altri protocolli
- Tcp\IP è **importante poiché il router lo utilizza come tool di configurazione**

La funzione dello **stack** del tcp\ip è **trasferire** informazioni da **una periferica di rete ad un'altra**. In questo procedimento viene citato il modello osi che sostiene tutto lo standard fisico nei protocolli

più bassi e collega i protocolli. I Livelli osi **più frazionati e complessi sono LIVELLO 7 (application), Livello 4 (Transport) e Livello 3 (Network).** Inclusi in questi livelli ci sono altri tipi di protocolli con una varietà di funzioni. Tutti questi sono relazionati al trasferimento delle informazioni.
TCP\IP permette comunicazioni attraverso **reti interconnesse** e funziona equamente sia per comunicazioni LAN che per WAN. TCP\Ip include non solo specifiche di livello 3 e 4 (come ad esempio Tcp e IP), ma **anche specifiche per applicazioni comuni**, come **email, remote login**, emulazione terminale e trasferimento file (**FTP**).

Lo stack del TCP\IP ed il livello Applicazione: Il livello applicazione supporta **indirizzamento di protocolli** e gestione della rete. Esso inoltre ha **protocolli per trasferimento**, email e remote login.
DNS – Domain name server. E' un sistema usato in internet per **tradurre i nomi** di domini e per la loro pubblicizzazione attraverso nodi\indirizzi.
WINS – Windows Internet Naming Service. E' un progetto Microsoft standard per Windows NT che automaticamente **associa workstation NT con nomi di dominio Internet**.
HOSTS – E' un file creato dall'amministratore di rete e mantenuto sul server\s. **E' usato per fornire una mappatura statica fra indirizzi ip e nomi** di computer.
POP3 – Post Office Protocol. E' uno standard Internet per **memorizzare email su un server mail fino a che non si accede e si scaricano sul proprio computer**. Esso permette agli utenti di ricevere email dalla propria casella INBOX utilizzando vari livelli di Sicurezza.
SMTP – Simple Mail Transport Protocol. **Governa la trasmissione di email** attraverso computer sulla rete. Esso non fornisce supporto per la trasissione di altri dati, all'infuori del testo (text plan).
SNMP – Simple Network Management Protocol. E' un protocollo che fornisce un metodo per **monitorare e controllare le periferiche di rete**. Effettuare configurazioni, raccogliere statistiche, ai fini della performance e sicurezza.
FTP – File transfer Protocol. **E' una connessione affidabile** (conn-oriented), che **usa il TCP** per trasferire files fra sistemi che supportano FTP. Esso supporta Binario Bi-Direzionale e trasferimenti di file in ASCII.
TFTP – Trivial File Transfer Protocol. E' un servizio **prettamente inaffidabile, basato su Connection-Less che usa UDP** per trasferire file fra sistemi che supportano TFTP. E' utilizzato in molte lan poiché esso **opera più velocemente di FTP** in un ambito statico.
HTTP – Hypertext Transfer Protocol. E' uno standard di internet **che supporta lo scambio di informazioni** sul **World Wide Web** o su reti interne. Esso **supporta molti tipi** di files differenti, incluso Testo, grafica, suono e video. Esso **definisce il processo** che ha origine sul browser web ai fini di inviare informazioni ai server WEB.

Protocolli per risoluzione problemi (troubleshooting).

TELNET – **Un'emulazione terminale** standard. Protocollo usato dai clients al proposito di effettuare connessioni remote via terminale e servizi di accesso telnet. Abilita gli utenti a **collegamenti remoti con routers** e ad entrare in comandi di configurazione.
PING – Pocket Internet Groper. E' una **utility di diagnostica** usata per determinare quando un computer è propriamente connesso ad una periferica o ad internet.
TRACEROUTE – E' un programma che è disponibile su molti sistemi ed **è simile al ping**, eccetto che il traceroute **fornisce più informazioni** rispetto al PING, il traceroute **traccia il percorso** che un pacchetto compie **per arrivare a destinazione**. Esso è usato per risolvere i problemi di routing.

Protocolli Familiari Basati su windows

NBTSTAT – E' una utility usata per **Controllare la risoluzione** dei nomi NETBIOS. (troubleshooting). Utilizzata per vedere e rimuovere entries dalla cache-nomi.
NETSTAT – E' una utility che **fonisce informazioni sulle statistiche TCP\IP**. Può essere usata per reperire informazioni sullo **status delle connessioni TCP\IP**, ed un sommaro di quelle ICMP, TCP, e UDP.
IPCONFIG\WINIPCFG – Utility utilizzata per **visualizzare i settaggi di rete correnti** per tutti gli ip delle perferiche di rete (nic). Può essere utilizzato per visualizzare il MAC address, il gateway e l'indirizzo IP.

Stack del protocollo TCP\IP e Livello Trasporto: Il **livello trasporto** permette ad una periferica sorgente di **segmentare** molti dati-applicazioni che viaggiano a livelli alti, per posizionarli in **streaming a livello 4**, ed abilitare la periferica ricevente **al riassemblamento** ed il riposizionamento dei segmenti sul livello superiore **(all'arrivo).**
Il data stream di Livello 4 è una connessione logica fra end-points di rete e fornisce servizio **di trasporto da un host a destinazione**. Questo servizio è riferito qualche volta ad "servizio End-To-End".
Il livello **trasporto** comprende 2 protocolli
TCP – Un protocollo **connection-oriented**, affidabile, fornisce **controllo di flusso** con le sliding windows e effidabilità data dai numeri di sequenza di conferma. **TCP re-invia tutti i pacchetti che non sono stati ricevuti**, fornisce un circuito virtuale fra applicazioni end-user. Il vantaggio del TCP è che **esso fornisce garanzia di consegna** dei segmenti.
UDP – Connection-LESS. Non affidabile. Responsabile di trasmettere messaggi **senza checking** software di consegna. **Il vantaggio** che fornisce **udp è la velocità**. Poiché udp non fornisce di conferma di conseguenza meno traffico superfluo è inviato, per ciò il trasferimento dei dati è più rapido.

Formato del Segmento TCP e UDP: Il segmento tcp\ip contiene i seguenti campi:
Source Port – Il **numero della porta** chiamante
Destination Port – Il **numero della porta** chiamata
Sequence Number – Il numero usato per assicurarsi della **corretta sequenza** di arrivo dei dati
Aknowledgment Number – Il prossimo ottetto TCP **atteso**
HLEN – Il numero di 32 Bit words nell'**header**
Reserved – Settato a Zero
Code Bits – La funzione di **controllo, setup e terminatore** di **sessione**
Window – Il numero di ottetti che l'inviatario **potrà accettare**
Checksum – Il checksum calcolato con **header e data fields**
Urgent Pointer – Indica la fine dei dati urgenti
Option – La massima **dimensione per il segmento TCP**
Data – Dati per i protocolli di **livello superiore**

I protocolli di livello applicazione devono **fornire affidabilità**, se necessario. UDP non usa lo windowing né l'aknowledgment. Esso è disegnato per applicazione che **non necessitano** di inserire assieme segmenti **in sequenza**. In effetti **l'header di UDP** è relativamente **corto**.
I protocolli che usano UDP sono i seguenti
TFTP
SNMP
Network File System (NFS)
Domain Name System (DNS)

Numeri delle porte TCP e UDP: Sia il TCP che l'udp **usano numeri delle porte** (o sockets) per passare informazioni ai livelli superiori. I numeri di **porte** sono usati per **mantenere traccia delle differenti conversazioni** che passano attraverso la rete allo stesso tempo.
Gli sviluppatori di applicazioni software hanno acconsentito ad usare porte conosciute il cui **standard è definito in RFC1700**. Per esempio, ogni conversazione riguardante un'applicazione FTP usa la porta standard 21.
Le **conversazioni che non convogliano in applicazioni**\porte conosciute, assegnano porte in maniera **random**, la cui scelta avviene **secondo un Range**. Queste porte sono usate come **sorgente e destinazione** per il segmento TCP.
Molte porte sono riservate sia per TCP che per UDP, quindi alcune applicazioni non devono essere scritte per appoggiarsi su di esso.
I range di porte assegnati sono i seguenti:

- Le porte Sotto la 255 sono usate per applicazioni **Pubbliche**
- Le porte fra 255 e 1023 sono assegnate ad applicazioni per **compagnie di pubblicità**
- Le porte Sopra la 1023 **non sono regolate**

I sistemi finali usano i numeri delle porte scelte a cura delle proprie applicazioni che le utilizzano. Il numero della porta sorgente solitamente è al di sopra della 1023, ed è dinamicamente assegnato dall'host sorgente.

Connessione TREEWAY HANDSHAKE Tcp: Poichè una connessione venga stabilita I due sistemi finali **devono sincronizzarsi tramite una sequenza TCP** iniziale numerica **(ISNs).** Il numero di sequenza è usato per **tracciare l'ordine** di pacchetti ed assicurarsi che **nessuno** di essi **vada perso** durante la trasmissione. Il numero di **sequenza** iniziale è un numero di **partenza usato** quando una connessione **TCP è stabilita**. Lo scambio dati **avvia un numero di sequenza**, durante la sequenza di connessione garantisce che i dati persi vengano recuperati.
La sincronizzazione **è completa quando** vengono **scambiati segmenti** trasportanti **il ISNs ed il bit di controllo chiamato SYN** che è addetto alla **sincronizzazione**. (I segmenti che trasportano il Syn sono chiamati anche SYNs). Una connessione di successo **richiede un appropriato meccanismo** per la chiusura della **sequenza iniziale e un handshake** leggermente obbligato **per scambiare i ISNs**. La sincronizzazione richiede che **ogni lato invii la propria ISN** e riceva una **conferma** e l'ISN di ogni lato per la connessione.
Ogni lato deve ricevere il L'ISN del lato opposto ed inviare **un aknoledgment (ACK)** di conferma in un ordine specifico, evidenziato nei seguenti steps:

A ->B SYN -- My sequence number is X.
A <- B ACK --Your sequence number is X.
A <- B SYN -- My sequence number is Y.
A ->B ACK -- Your sequence number is Y.

Poichè **il secondo ed il terzo** step possono essere combinati in **un unico messaggio**, lo scambio è chiamato **THREE-WAY HANDSHAKE\Open Connection**. Entrambi **i lati** della connessione **sono sincronizzati** con una **sequenza** THREE-WAY HANDSHAKE\Open Connection.Una sequenza Three-Way Handshake è necessaria poiché TCP può usare **differenti meccanismi** per raccogliere l'ISN. Il ricevitore del primo SYN **non sa se il segmento è uno vecchio** (arrivato con ritardo) oppure no. Esso **ricorda** l'ultimo **numero di sequenza** usato nella connessione, che non sempre è possibile, quindi esso **richiede all'inviatario di verificare il Syn**. A questo punto ogni lato **può iniziare** la comunicazione ed **ognuno può stopparla** poiché **TCP è un metodo di comunicazione Peer-To-Peer (bilanciato).**

Semplice Aknowledgment e Windowing TCP: Per **governare** il flusso di dati fra periferiche, TCP usa il meccanismo di **controllo Peer-To-Peer**. L'host ricevente che riporta il livello TCP, **invia un window size** alla sorgente sul livello **TCP**. Lo windows size **specifica il numero di byte**, di partenza con il **numero di conferma** che l'host ricevente TCP è pronto a ricevere.
La windows size si riferisce **al numero di byte** che sono trasmessi prima **di ricevere un aknowledgment.** Dopo che un host ha trasmesso il numero di byte relativo allo windows-size, esso deve **ricevere un acknowledgment** prima che altri dati vengano trasmessi.
Lo windows size determina **quanti dati alla volta** può accettare la stazione ricevente. Con windows **size di 1**, ogni segmento porta **solo un byte** di dati che devono essere confermati (acknowledged) prima che un altro segmento venga trasmesso. Questo risultato **non è efficiente** per l'uso della **banda** da parte dell'host.
L'obiettivo dello windowing è **migliorare il controllo di flusso** e l'affidabilità. Sfortunatamente, con windows size di 1, si ha un uso altamente inefficiente della banda.

TCP sliding window

Tcp usa EXPECTATIONAL AKNOWLEDMENT, per il numero di acknowledgment riferico **all'ottetto prossimamente atteso**. La parte **slittante della sliding window**, si riferisce al fatto che la window size **è negoziata dinamicamente** durante la sessione TCP. Una sliding windows risulta in **un più efficente uso della banda** da parte dell'host poiché **uno window size più ampio** permette a più dati di **essere trasmessi prima della conferma**.

TCP sequence and acknowledgment numbers

Il TCP fornisce **la sequenza dei segmenti con una referenza** di forward acknowledgment. Ogni datagramma **è numerato prima della trasmissione**. Alla stazione **ricevente,** TCP **riassembla** il segmento **in un messagio completo**. **Se** il numero di sequenza arriva e **manca qualcosa**, tale segmento **è ritrasmesso**. Se il segmento non è confermato **entro un determinato tempo**, avviene una **retrasmissione**. Il numero di sequenza e la conferma **sono Direzionali**, il che vuol dire che la comunicazione avviene in **entrambi le direzioni**.
La sequenza e la conferma con il mittente, prendono **una direzione ben precisa**.

TCP\IP ed il Livello INTERNET: Il **livello internet dello stack TCP\IP** corrisponde al livello di rete riferito al modello OSI (**livello3**). Ogni livello è responsabile **dell'invio di pacchetti** attraverso la rete utilizzando software di indirizzamento. Molti protocolli operano al livello TCP\IP-Internet che corrisponde al livello OSI 3 (network).
IP – Fornisce **connection-LES**, delivera **best-effort**, routing di datagrammi. Non è riferito al contenuto dei datagrammi. **Sceglie un percorso** per portare i datagrammia destinazione.
ICMP – Fornisce **controllo** e possibilità di **messaging**
ARP – Determina l'indirizzo di livello 2 (data link) per indirizzi ip conosciuti.
RARP – Determina l'indirizzo di livello 3 (network) per indirizzi data link conoscuti.

Il Diagramma IP: Un **datagramma** IP contiene **IP header e dati** ed è formato dal **Layer MAC e dal Trailer MAC**. Un messaggio può essere trasmesso **come una serie di datagrammi** che sono **riassembla**ti in un messaggio ove vengono ricevuti.
I fields del datagramma IP sono i seguenti:
VERS – Numero versione
HLEN – Lunghezza Header in word di 32 bit
Type of Service – Come il datagramma deve essere gestito
Total Length – Lunghezza totale (header + data)
Identification,Flags, Flag Offset – Fornisce frammentazione di datagrammi, così da permettere differenti MTUs nella internetwork.

TTL – Tempo di vita
Protocol – Il livello superiore (livello 4 TCP) che invia datagrammi
Header CheckSum – Un controllo di integrità nell'header
Source IP address e Destination IP address – Indirizzi a 32 bit
IP option – Testing della rete, debugging, sicurezza ed altre opzioni

Il campo PROTOCOLLO, determina che il protocollo di **livello 4 debba essere trasportato assieme al datagramma IP**. Spesso il traffico IP utilizza TCP, ed **altri protocolli possono usare IP**. Ogni header **IP deve identificare il protocollo relativo al livello di destinazione** per il datagramma (LIVELLO 4). Il livello di **trasporto è numerato**, similarmente al **numero della porta**. IP include il numero di protocollo nel campo PROTOCOL.

Internet Control Message Protocol (ICMP): Tutti gli Host TCP\IP **implementano ICMP**. I messaggi ICMP **sono trasportati in datagrammi ip** e sono utilizzati per inviare **messaggi di controllo e di errore**. ICMP usa i seguenti tipi di messaggi predefiniti. Altri esistno e non sono inclusi in questa lista.

- Destinazione Irraggiungibile
- Eccesso di TIME TO LIVE
- Problemi di Parametri
- "source quench"
- Redirect
- Echo
- Echo Reply
- TimeStamp
- TimeStamp Reply
- Information Request
- Information Reply
- Address Request
- Address Reply

Come lavora ICMP:

Se **un router riceve** un pacchetto che **non può trasportare** alla destinazione finale, **il router invia un messaggio ICMP** in cui viene scritto che **la destinazione è irraggiungibile**, alla sorgente. Il messaggio può essere **Irraggiungibile poiché non si conosce il percorso** di destinazione. Una **risposta Echo** è confermata con successo da un comando **PING**. Il risultato **può includere altri ICMP messages** come ad esempio "irraggiungibile" o "timeout".

Come lavora L'ARP: L'arp è usato per **risolvere o mappare un indirizzo ip conosciuto ed ottenere il MAC address**, per favorire **multi comunicazioni su un media multi accesso** come ad esempio Ethernet. Per determinare un Mac address di destinazione per un datagramma, **una tavola, chiamata ARP cache è verificata** prima dell'invio. **Se** l'indirizzo **non è nella tavola, ARP invia un broadcast** che viene ricevuto **da ogni stazione sulla rete**, con l'intento di trovare la stazione di destinazione.
Il termine **"local ARP"** è usato per descrivere la ricerca di un indirizzo in **cui il richiedente e la stazione di destinazione condividono lo stesso MEDIA**. Prima di ricorrere all'ARP **è consultata la subnet mask**, in alcuni casi, il mask può determinare che i nodi non sono sulla stessa rete.

IP ADDRESSING

Il Proposito dell'indirizzo ip: Nell'ambiente tcp\ip, stazioni finali comunicano con servers ed altre stazioni. Questo può avvenire poiché **ogni nodo utilizza la suite** del protocollo tcp\ip ed ha un unico **indirizzo logico a 32bit**. Questo indirizzo è conosciuto come **IP ADDRESS** ed è specificato in forma a 32bit in formato esa decimale. L'interfaccia **router deve essere configurata** con un indirizzo **ip**, se **il suo ip è "routed" dall'interfaccia**, I comandi **ping e trace** sono usati per verificare la configurazione dell'indirizzo ip.
Ogni azienda o organizzazione situata su internet è vista come **una singola rete** che può essere raggiunta **tramite un host** individuale per mezzo del quale tale compagnia può essere contattata. Ogni rete aziendale **ha un indirizzo**. L'indirizzo situato su tale rete fa parte dello stesso indirizzo di rete, ma ogni host è identificato con un unico indirizzo host sulla rete.

Il ruolo dell'HOST address in una "routed network": In questa sezione si impareranno i concetti base, necessari, prima di **configurare un indirizzo** ip. Esaminando i vari requisiti di rete, è possibile scegliere **la corretta classe di indirizzi** e definire come **stabilire una subnet**. Ogni periferica o interfaccia deve avere **un numero HOST** che non può contenere **tutti 0 nel campo host**. **Un indirizzo** host è riservato per un **broadcast ip** all'interno di una rete. Un valore host in cui sono presenti **tutti 0, rappresenta "la rete"** o l'indirizzo di rete. (es.172.16.0.0). Un valore di zero è anche usato, **in rari casi, per il broadcast ip**, in diverse recenti implementazioni del tcp\ip. La **tavola** di routing, contiene le **entries della rete e gli indirizzi delle periferiche** che si appoggiano sul media. Di solito **non** contiene **informazioni sugli hosts**.
Un indirizzo ip, e una subnet mask, su di una interfaccia, raggiunge 3 propositi:

- Abilitano il sistema a **processare la ricezione e la trasmissione** dei pacchetti
- Specificano **l'indirizzo locale** della periferica
- Specificano **un range di indirizzi** che condividono il cavo con la periferica

Il ruolo dell'indirizzo BROADCAST in una "routed network": Il broadcasting **è supportato** dall'ip. Il messaggio è costituito per essere visto **da ogni host** sulla rete. L'indirizzo **Broadcast** è formato **usando tutti "1"** all'interno della **porzione** di indirizzo HOST.
I software IOS cisco supportano **due tipologie di Broadcast**. Il ***direct broadcast ed il Flooded broadcast***. Direct: I broadcasts si direzionano **all'interno di una specifica rete o subnet**, sono permessi e **forwardati** dal router. Questi direct broadcast contengono **tutti "1" nella porzione host** di indirizzo.
I **flooded** broadcast (255,255,255,255) **non sono propagati**, ma sono considerati **broadcast locali**.

Assegnazione dell'intrfaccia router e dell'ip address di rete: Il numero dei bit di routing (network e subnet) in ogni subnet mask può essere indicato in formato "/n"
In una piccola rete sono stati assegnati indirizzi per le interfacce, subnet mask e risultanti numeri subnet.

Esempio:

/8 = 255.0.0.0

/24 = 255.255.255.0

Il comando IP Address: Utilizzare il comando IP ADDRESS per stabilire un **indirizzo** di rete **logico** per un interfaccia.
Utilizzare il comando **TERM IP NETMASK-FORMAT** per specificare il **formato** della **maschera** di rete per la versione corrente. Le opzioni di formato sono:

- Conteggio dei Bit
- Punto-Decimali

- Esadecimali

Utilizzare il comando **IP HOST per creare un host statico** nella entry del file di configurazione del router.

Il comando IP-NAME server: Il comando **IP NAME-SERVER** definisce **quali host** debbono **fornire il servizio del nome**. E' possibile specificare **un massimo di sei indirizzi ip** e server nomi in un **singolo** comando.
Per mappare gli ip name server, è necessario **identificare l'host name**, specificare un server name ed **abilitare il dns**. Ogni volta che il sistema software riceve un host name che non riconosce, esso **si basa sul dns interno e l'ip di tale periferica**.

Come Abilitare e Disabilitare il DNS su un router: Ogni **indirizzo ip** unico può avere un **host** name **associato** ad esso. Il software cisco IOS mantiene **una cache degli host name**, mappandoli per l'uso con i comandi EXEC. Questa cache, **velocizza il processo di conversione** dei nomi in indirizzi.
L'indirizzo **ip** definisce **il nome degli schemi** che permettono ad una periferica di essere **identificata e localizzata**. Un nome, come ad esempio ftp.cisco.com identifica **il domino nell'ftp** di cisco. Per mantenere traccia del nome di dominio, **ip identifica un server name** che gestisce la cache dei nomi. DNS (Domain Name Service) è necessario per default con un indirizzo server di 255.255.255.255 che è un local broadcast. Il comando **Router (config)#no ip domain-lookup disabilita la translazione** dei nomi\indirizzi **all'interno del router**. Questo vuol dire che il router non **genererà o forwarderà i pacchetti broadcast verso il domain system**.
Il comando **show host** è usato per visualizzare **una lista di host** names ed **indirizzi**.

Comandi di Verifica: I problemi di indirizzamento sono **i più comuni** che avvengono in reti IP. E' importante verificare la propria **c**onfigurazione di indirizzi, prima di continuare con i futuri steps di configurazione.
Esistono 3 Comandi che ci permettono di **verificare la configurazione** di indirizzi all'interno di una internetwork:

- **TELNET** – Verifica **il livello applicazione** fra stazioni sorgenti e destinazione, è il test più completo attualmente disponibile.
- **PING - Utilizza il protocollo ICMP** per verificare la connessione hardware e l'indirizzo logico al livello internet. **E' un test molto basilare**
- **TRACE** – Utilizza **i valori TTL** per generare **messaggi da parte di ogni router** usati lungo il percorso. E' **molto potente**, e la sua ablità, è **localizzare errori\problemi nel percorso**, dalla sorgente alla destinazione.

I comandi Telnet e Ping: Il comando **TELNET** è **un semplice comando** che si può usare in caso sia possibile connettersi al router. Se non è possibile usare TELNET sul router, ma è possibile pingarlo, si deduce che il problema sia di un livello più alto, di funzionalità relativo al router. A questo punto è necessario fare il reboot al router e usare TELNET ancora.
Il comando **PING invia pacchetti ICMP** echo ed è supportato **sia in user che in privileged** exec modes. In questo esempio, un ping time out come riportato dal punto, e 4 sono ricevuti con successo, come mostrato dal punto esclamativo.
Questi sono i risultati del test ping.
L'estensione del comando PING è supportata solo **nella Privileged Exec Mode**. E' possibile usare il comando Ping per **specificarare una opzione** di supporto internet header. Per entrare nell'extended mode, **digitare PING e quindi Y alla domanda di Excentend command**.

Character	Definition
!	Ricezione con successo di un reply

	echo
.	Tempo scaduto nell'attesa del datagramma
U	Destinazione Irraggiungibile
C	Congestione pacchetti
I	Ping interrotto (e.g. Ctrl-Shift-6 X)
?	Tipo di pacchetto sconosciuto
&	TTL ecceduto

Il comando Trace: Quando si usa il comando TRACE, **host names sono visualizzati** se l'indirizzo **è tradotto dinamicamente** o tramite **tavole** di host **statiche**. Il tempo mostrato, rappresenta il tempo necessario per il ritorno di ciascuna delle 3 sonde.
Trace è **supportato da IP, CLNS, VINES, e AppleTalk**. Quando il trace **raggiunge il primo target** di destinazione, **è riportato un ASTERISCO**. Questo è causato normalmente da un time out in risposta, di uno dei pacchetti-sonda.
Le risposte al trace sono le seguenti:

!H -- The probe was received by the router, but not forwarded, usually due to an access list.

P – Il protocollo è Irraggiungibile

N – La rete è irraggiungibile

U – La porta è irraggiungibile

***** -- Time out.

11 Routing

Determinazione del Percorso(path): La **determinazione** del percorso per il traffico che passa attraverso una nuvola di rete, avviene al **livello 3**, network. La funzione di determinazone percorso permette **al router di valutare** i percorsi possibile per la destinazione e stabilire la handing preferita dei pakketti. I servizi di routing usano le informazioni della **tipologia di rete**, in fase di **valutazone** del percorso. Questa informazione **può essere configurata** dall'amministratore di rete, oppure aggiunta tramite un processo dinamico che gira sulla rete.
Il livello network,3, **fornisce una consegna best-effort** end-to-end tramite reti interconnesse. Il livello rete usa la tavola di routing per inviare pacchetti dalla rete sorgente alla rete di destinazione. Dopo che il router ha **determinato** il percorso da usare esso procede forwardando i pacchetti. Esso tiene i pacchetti che sono accettati **su una interfaccia** e li forwarda su **un'altra interfaccia** o porta che reflette il **miglior percorso** sull'intestazione del pacchetto per la destinazione da raggiungere.

Come vengono trasportati (routed) pacchetti a destinazione: Per essere veramente pratica, una rete deve rappresentare nella propria consistenza un punto del percorso disponibile fra routers, ogni linea fra router ha **un numero che utilizza un indirizzo** di rete. Questi indirizzi devono trasportare informazioni che possono essere usate per il **processo di routing**, per passare pacchetti da una sorgente fino a destinazione. Usando questi indirizzi il livello di rete può fornire una connessione ripetitiva che interconnette reti indipendenti.
La consistenza degli indirizzi di livello 3 sopra l'intera internetwork **evita** anche l'uso della **banda** da parte di **broadcast non necessari**. Il broadcast invoca un processo non essenziale dall'alto di vasta capacità, su tutte le periferiche o link che non devono ricevere il broadcast. Usando l'indirizzamento consistnete end-to-end, per la rapresentazione del percorso e delle connessioni

media, il livello di rete **può trovare la destinazione evitando** di opprimere le periferiche o links o internetwork con il **broadcast.**

Indirizzi di rete e indirizzamenti host: Il router usa **l'indirizzo di rete** per identificare la rete **di destinazione** (LAN) di un pacchetto all'interno di una internetwork. **Per molte protocolli** che funzionano su livello 3, la relazione **è stabilita dall'amministratore** di rete che assegna un indirizzo host di rete in accordo ad una rete o progetto pre-determinato. **Per altri** protocolli di livelli di rete, l'assegnazione di indirizzi host **è parzialmente o completamente dinamica**. Molti schemi di protocolli di rete utilizzano **diversi host o indirizzi di nodi**.

Selezione di percorso e Switching di pacchetti: Un router generalmente **rilascia un pacchetto** da un data link ad un **altro usando 2 funzioni** basilari:

- Funzione di **determinazione percorso**
- Funzione di **Switching**

Il router **usa la porzione di rete** dell'indirizzo per effettuare la **selezione del percorso** per passare il pacchetto al **prossimo router** lungo il percorso. La funzione di **switching** permette al router di **accettare un pacchetto da un interfaccia e forwardarlo tramite una seconda interfaccia**. La funzione di determinazione percorso permette al router di scegliere **l'interfaccia più appropriata** per il **forwarding** del pacchetto. La **porzione del nodo dell'indirizzo è usata dal router finale**. (Il router **connesso alla rete di destinazione**) di fare il deliver del pacchetto all'host corretto.

Routed e Routing protocols: Vista la similarità di questi 2 termini, la **confusione** spesso può esserci**.** Routed protocol e routing protocol. **Routed** protocol è ogni protocollo di rete che **fornisce sufficienti informazioni nel proprio livello di indirizzo**, da **permette al pacchetto** di essere **forwardato da un host ad un altro host**, basandosi sullo schema di indirizzi. I **ROUTED** protocols definisce il formato del campo all'interno del pacchetto. I pacchetti sono generalmente convogliato da un end system ad un altro end system. Il protocollo **internet (IP)** è un esempio di Routed Protocol.
I **Routing** protocol, invece, **supportano un routed** protocol fornendo meccanismi per **condivisione** delle informazioni di routing. I messaggi del protocollo di routing sposta messaggi fra routers. Un **routing** protocol **permette al router di comunicare** con altri router per updatare e mantenere tavole. Esempi TCP\IP di protocolli di routing, sono:

- RIP (Routing Information Protocol)
- IGRP (Interior Gateway Routing Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)
- OSPF (Open Shortest Path First)

Operazioni sul protocollo, livello Network: Quando un'applicazione host **necessita** di **inviare** un pacchetto a destinazione **su una differente rete**, l'indirizzo host **del frame link del router**, usa **l'indirizzo di un'interfaccia router**. Il processo router di livello di rete, **esamina** l'entrante **packet header** per determinare **la rete di destinazione**, quindi fa referenza sulle tavole di routing che associano le reti alle interfacce esterne. Il pacchetto **è Incapsulato ancora** in un data link frame che è appropriato per l'interfaccia selezionata ed è richiesto il **delivery sul prossimo HOP** nel percorso. Questo processo avviene **ogni volta** che il pacchetto è forwardato tramite un altro router.
Nel router che è connetto alla rete dell'host di destinazione, il pacchetto è **encapsulato nel frame** diretto **verso la rete** di destinazione e trasportato **all'host** di destinazione.

MultiProtocollo di Routing: I routers hanno la capacità di **supportare molti routing** protocols indipendneti e mantenere **tavole di routing per molti routed** protocols. Questa capacità permette al router di fare il deliver di pacchetti da diversi routed protocols sullo stesso link.

Routing Statico e Routing Dinamico: Il route **statico** è amministrato **manualmente dall'amministratore** di rete che inserisce la configurazione all'interno del router. L'amministratore deve fare **manualmente l'update** di questo router statico ogni qual volta il campo di tipologia di rete richiede un update.
Il Route **dinamico lavora diversamente**. Dopo che un amministratore di rete ha inserito i **comandi di configurazione** per far partire il dinamic routing, il route è **automaticamente updatato** dal processo di routing ogni qual volta una nuova informazione è ricevuta dall'internetwork.
Il cambio, nella modalità dinamica, è scambiato fra routers come **parte di processo di update**.

Perchè usare lo Static Routing: Il routing statico **si adatta a molte applicazioni** utili. Il routing dinamico **attende** di rivelare tutto il nodo di una internetwork, per ragioni di sicurezza si deve nascondere una parte dell'internetwork. Lo static routing ci permette di **specificare** le informazioni che devono e possono essere rivelate **su reti ristrette**.
Quando una rete è accessibile solo da un percorso, lo static routing **può essere sufficiente**. Questo tipo di rete è chiamata **STUB NETWORK**. Configurando lo statico routing per una Stub Network, **si evita l'overhead di routing dinamico**.

Quando è usato un Route di Deafult: Una entri di una routing table, **direziona pacchetti al prossimo hop** quando l'hop **non è esplicitamente listato** sulla tavola di routing.E' possibile selezionare le **routes di default** come parte di una configurazione **statica**.
In questo esempio, i routers della compagnia X processano la specifica modalità di routing, della tiplogia di rete della compagnia X, ma non di altre reti. Mantenendo la tipologia di ogni altra rete, accessibile tramite l'accesso Cloud non è necessario ed è impossibile. Mantenendo una specifica metodologia di routing, ogni router all'interno della company X, è informato del route di default che esso è usato per raggiungere ogni destinaziona sconosciuta, direzionando il pacchetto ad internet.
Quando è necessario il routing Dinamico: Static routing permette ai routers di fare il route dei pacchetti da una rete ad una rete **basandosi su informazioni configurate**. Il router si riferisce alla propria **tavola di routing** e segue la modalità statica residente, e rilascia i pacchetti al router D. Il router D fa la stessa cosa e rilascia il pacchetto al router C. Il router C trasporta ilpacchetto all'host di destinazione.
Se il percrso fra Router A e Router D fallisce, il Router A non è abilitato a rilasciare il pacchetto al Router D utilizzando la Static Route.Fino a che il Router A non è configurato manualmente da rilasciare pacchetti nella direzione del router B, la comunicazione con la rete di destinazione, è impossibile.
Il routing **dinamico offre grande flessibilità**. In acordo con le tavole di routing generate dal router A, i pacchetti possono raggiungere la destinazione tramite la Route preferita, attraverso il router D. Comunque un secondo percorso per arrivare a destinazione è disponibile tramite il router B.
Quando il router A riconosce che il link del router D è Down, esso **aggiusta la propria tavola di routing**, modificando il percorso tramite il router B, come il preferito per la destinazione. I routers continuano ad inviare pacchetti attraverso questo link.
Quando il percorso fra il router A ed il router D e restorato a pieno servizio, il router A può di nuovo cambiare la sua routing table per indicare la preferenza per la counterclockwise sul percorso tramite il router D e C per arrivare alla rete di destinazione. I protocolli di routing dinamico possono direzionare il traffico dalla stessa sessione a differenti percorsi per una migliore performance **Questo processo è chiamato LOADSHARING**.

Operazioni di Routing Dinamico: Il successo del routing dinamico **dipende da 2 funzioni** basilari del router:

- **Mantenimento delle tavole** di routing

- La **distribuzione temporale dei routing updates** ad altri routers

Il routing dinamico si appoggia su un protocollo di routing per condividere la metodologia di routing con altri routers. Un protocollo di routing **defiisce le regole** usate dal router mentre esso **comunica con i router nelle vicinanze**. Per esempio un protocollo di routing descrive:

- **Come inviare gli updates**
- Che tipo di **metodologia è contenuta** in questi **updates**
- **Quando** inviare questa **metodologia**
- Come **localizzare il destinatario** degli updates.

Come viene determinata la distanza sulla rete tramite i sistema METRICI: Quando un **algoritmo** di Routing fa l'**update** delle tavole di routing, il **suo primo obiettivo** è Determinare la **migliore informazione** da includere **nelle tavole**. Ogni algoritmo di routing interpreta qual è la migliore **nel proprio modo**. **L'algoritmo genera** un numero chiamato **METRIC VALUE** per ogni percorso attraverso la rete. Tipicamente **il più piccolo numero metrico è il miglior** percorso per cui anche quello più breve.
E' possibile calcolare il Metric Semplice, basandosi **su una singola** caratteristica del percorso. E' possibile calcolare metrics più comlessi, basandosi **su diverse caratteristiche**. I metrics più comunemente utilizzati dai routers, sono i seguenti:

- *bandwidth* – La capacità di un Link; (normally, a 10 Mbps Ethernet link is preferable to a 64 kbps leased line)
- *delay* -- La lunghezza di tempo necessaria per spostare un pacchetto lungo ogni link dalla sorgente alla destinazione.
- *load* -- L'ammontare di attività su una risorsa di rete come ad esempio router o link
- *reliability* -- Solitamente si riferisce alla quantità di errori di ogni link di rete.
- *hop count* -- Il numero di Routes che un pacchetto deve attraversare prima di raggiungere la propria destinazione.
- *ticks* -- (approximately 55 milliseconds). Il ritardo sul data link utilizzando un ibm pc clock ticks
- *cost* -- Un valore arbitrario, solitamente basato sulla banda, sulla spesa montaria o altra misurazione che è assegnata dall'amministratore di rete.

Tre Classi di Routing: La maggior parte degli **algoritmi di routing** sono classificati come uno dei 2 algoritmi base:

- **DISTANCE VECTOR**
- **LINK STATE**
- **HYBRID**

Il routing **Distance-Vector** determina la direzione (vettore) e la **distanza di ogni link nella internetwork**. Il **link-State (chiamato anche Shortest path first), ri-crea l'esatta tipologia dell'intera intenetwork** (o almeno la porzione su cui il router è situato).
L'equilibrio **ibrido** solutamente **combina** aspetti degli algoritmi Link-State e del Distance-Vector. Prossimamente tratteremo **procedure e problemi per ognuno** di questi algoritmi di routing e presenteremo **tecniche per minimizzare** i problemi.

Tempo di Convergenza: L'**algoritmo** di routing è **fondamentale** per il Dynamic Routing. Quando la tipologia di una rete cambia a seguito di una crescita, o di un "failure" e problematiche varie, il

Knowledge (tipologia di routing), deve riflettersi su una **nuova accurata visione** della tipologia acquisita. Questo processo è chiamato **CONVERGENCE**.
Quando tutti i routers in una internetworks, stanno operando con le stessa Tipologia, l'internetworks è detta **COVERGED**. Una **rapida Convergence è preferita nelle** reti poiché **riduce** il eperiodo di tempi nel quale i routers devono continuare ad eseguire **decisioni di routing incorrette**.

Distanza Vettore nel Routing: La distanza vettore basa i propri al goritmi sul **passaggio di copie multiple** della tabella di routing. **Router to Router**. Questi **regolare update** fra routers comunicano eventuali cambi di tipologia di rete.
Ogni router riceve una tabella di routing **dal suo routers direttamente connesso** situato nelle vicinanze. Per esempio il router B riceve informazioni dal Router A. Il router B **aggiunge** un numero di **distanza-vettore** (come un numero di hops), che va ad incrementare, la stessa distanza vettore e quindi passa questa nuova tabella di routing **aggiornata ad un altro router nelle vicinanze**, il router C. Questo processo, **step-by-step**, avviene in tutte le direzioni fra i router direttamente collegati, nelle vicinanze.
L'algoritmo eventualmente **eccumula la distanza** di rete, quindi esso può mantenere un database della topologia di rete sempre aggiornato. L'algoritmo del Distance-Vector, comunque, **non permette ad un router** di **conoscere l'esatta tipologia** di una internetwork.

Come i protocolli di Distanza Vettore scambiano le Tavole di Routing: Ogni router che usa il distance-vector **inizia identificando le periferiche vicine**. L'interfaccia che pesa su ogni rete **direttamente** connessa, deve avere una **distanza di 0**. Una rete basata su distance-vector scopre processo dopo processo, e trova il **miglore percorso** per la rete di destinazione, basandosi sulle informazioni che riceve dai router **nei dintorni**.Per esempio, il Router A impara da altri router basandosi su informazioni che riceve su router B. **Ogni entry** di rete nella tabella di routing, ha un **accumulo di distance vector per visualizzare la distanza percorsa e percorribile in ogni distanza.**

Come i campi di topologia si propagano tramite la rete ed i routers: Quando una tipologia **cambia** in distanza-vetore, le tabelle di routing **devono fare un update**. Con il processo di scoperta-reti (**discovery**), avviene un update **step per step, router\router**. **L'algoritmo** di distanza vettore fa chiamata per ogni router nelle vicinanze inviando **l'intera tabella di routing**. Le tabelle di routing includono informazioni sul **costo totale del percorso** (definizione specifica **metrica**) e dell'indirizzo logico **del primo** router del percorso di ogni rete **contenuta** nella tabella di routing.

Il problema dei LOOPS di Routing: Il loop di routing può avvenire se una **lenta convergenza** o una nuova configurazione **causa inconsistenti entries**.

- A seguito di un FAILURE da parte della rete 1, tutti i router hanno effettuato un adeguamento alla tecnica di routing. La rete è quindi Converged (già effettuata la convergenza), riguardo a questo, il router C preferisce il percorso della rete 1 passando per il router B e la distanza dal router C alla rete1 è 3.

1. Just before the failure of Network 1, all routers have consistent knowledge and correct routing tables. The network is said to have converged. Assume for the remainder of this example that Router C's preferred path to Network 1 is by way of Router B, and the distance from Router C to Network 1 is 3.

2 Quando il Network 1 cade, il router E manda un aggiornamento ad A. Il router A cessa di mandare pacchetti al Network1, ma i routers B, C, D

continuano perchè non sono stati informati del crash. Quando il router A manda l'aggiornamento, i routers B e D smettono di instradare verso il Network 1. Però il router C non ha ricevuto l'aggiornamento. Per il router C il Network 1 è ancora raggiungibile attraverso il router B.

3 Adesso il router C manda aggiornamenti periodici al router D, indicando un percorso per il Network 1 attraverso il router B. Il router D cambia la sua tabella di routing per 'riflettere' questa giusta ma incorretta informazione e inoltra questa l'informazione al router A. Il router A la inoltra as B e E e così via.
Tutti i pacchetti per il Network 1 adesso faranno loop da C a B a A a D e di nuovo all'indietro verso C.

Il problema del Couting all'infinito: Continuando l'esempio del paragrafo precedente, l'update invalido della rete 1, **continuerà con i loop affichè altri processi non lo stopperanno**. Questa condizione è chiamata **COUNT TO INFINITY**, i pacchetti che vanno in loops continuamente attorno alla rete, a dispetto della trasmissione, in questo esempio, la Network1 è down mentre i routers stanno **continuando all'infinito a fare il count**, le informazioni invalide fanno in modo che possa esistere un **loop continuo**.
Senza contromisure che arrestino il processo, la distanza vettore (**metric**) degli hop **continua ad incrementarsi** ogni volta che un pacchetto passa **attraverso ad un altro router**. Questi pacchetti vanno in **loop** sulla rete poiché **esistono informazioni errate** sulle tavole di routing.

La soluzione di Definire un Massimo: L'**algoritmo** di routing della **Distanza-Vettore** ha la capacità di **auto correggersi**, ma un problema di routing loop può dar luovo ad un count to infinity.Per comprendere questo problema, è necessario sapere che i protocolli di distanza-vettore **definiscono l'ifinito come un numero massimo** e specifico. Il numero si riferisce a Routing Metric.
Con questo approccio il protocollo di routing permette al loop di continuare **fino a quanto il metric eccede** il proprio **valore massimo**. **Quando ciò avviene, il pacchetto è Scartato** dal router. In ogni caso, quando il valore massimo del metric, **eccede**, la rete in questione (network1) **è considerata irraggiungibile**.

La soluzione "split Horizon": Un'altra possibile sorgente o **causa del routing Loop** può essere **una incorretta informazione che è rispedita indietro ad un router**, contraddicendo la corretta informazione che esso ha inviato. Ecco come ciò accade:

- Il router A passa un update al router B ed al router D indicando che la rete1 è down. Router C trasmette un update al router B indicando che la rete 1 è raggiungibile ed è ad una distanza metrica di 4 dal router D. Questo non viola le regole slit-horizon.
- Router B conclude, incorrettamente, che il router C ha un valido percorso per la rete1, per cui è possibile passare di lì, raggiungendo la destinazione in una distanza inferiore. RouterB invia un update al router A avvidansolo che una nuova Route su Network1 è disponibile.
- Router A adesso determina che può inviare dati alla rete1 tramite il Router B, Router B determina che può inviare dati alla rete 1 tramite il Router C, ed il router C determna che può inviare dati alla rete 1 tramite Router D. Ogni pacchetto introdotto in questo schema andrà in loop fra i routers
- **Split-Horizon inizia a valutare la situazione**. Se una tabella di network sulla rete 1, arriva dal Router A, Router B, Router D non possono inviare informazioni alla rete1 dietro il router A. **Split-Horizon quindi riduce le informazioni di routing incorrette e riduce l'overhead di ruting**,

La soluzione Hold-Down Timers: E' possibile **risolvere il problema di count to infinity utilizzando HOLD-Down Timers**, che lavorano nel seguente modo:

- Quando un router **riceve un update** da un altro router nelle vicinanze, indicando che una rete, precedentemente accessibile, è adesso, **inaccessibile,** in router **marca la route come "inaccessibile", e fa partire un hold-down timer**. Se **prima che il tempo espiri**, viene **ricevuto un messaggio** da parte dello stesso router che ha passato l'info in precedenza, in cui si dice che **la rete è di nuovo accessibile**, il router in questione **marca la rete come "accessibile" e viene rimosso l'hold-down timer**.
- Se un update arriva **da un router differente con un migliore prospetto metrico** dell'originale, il router **marca la rete come accessibile** e rimuove l'hold-down timer.
- Se prima che il timer scada, **arriva un mezzaggio da un router differente, con un metric meno buono**, **l'update è ignorato**. Ignorando l'update **con il metric peggiore**, quando l'hold-timer ha effeto, **permette un tempo maggiore** per poter cercare ed eventualmente effettuare un cambio di route per propagarsi sulla rete.

Il link-State del Routing: Il secondo algoritmo base usato per il routing è il **Link-State**. Il link-state basa l'algoritmo di routing, anche chiamato **SPF (shortest path first),** di mantenere un **complesso** database delle informazioni di *topologia*. Mentre l'algoritmo di distanza-vettore non specifica informazioni sulla distanza di rete e non conosce i router distanti, l'algoritmo di routing Link-State, **mantiene piena conoscenza della distanza di router** e come essi sono collegati.
Il link state routing utilizza:

- **Annunci** del collegamento Link-state (LSAs)
- Un **database** della tipologia
- **L'algoritmo SPF ed il risultato dell'albero SPF**.
- Una tabella di routing **dei percorsi e delle porte** di ogni rete

Gli ingegneri hanno impelementato il concetto link-state nel OSPF (Open Shortest Path First) routing. RFC 1583 contiene una descrizione del concetto OSPF Link-State ed operazioni.

Come i protocolli LINK-STATE, scambiano le tavole di Routing: La scoperta del Link-State routing utilizza i seguenti processi:

- I routers **scambiano LSAs** con altri routers. Ognuno di essi inizia **con reti direttamente connesse** per cui comunica con informazioni dirette
- Ogni router in parallelo con altri, **costruisce un database** di topologia formato da tutti gli LSAs che vengono dalla rete.
- **L'algoritmo SPF calcola l'accessibilità** della rete. Il router costruisce questo database di tipologia logica come un Albero, con se stesso alla ROOT. Ciò raggruppa tutte **le possibili percorrenze** su ogni rete, della internetwork su cui gira il protocollo link-state. Quindi queste percorrenze vengono ordinate, dalla più breve alla più lunga (SPF) Short path first.
- Il router **mostra i migliori percorsi**, e le **porte** di queste reti di destinazione, nella tabella di routing. Esso mantiene, inoltre database di **tipologia** e dettagli di status.

Due tipi di Link-STATE: Fondamentalmente esistono **2 Fattori** concerni al link state: Requisiti di **Memoria e Processing e Requisiti di Banda**.

Requisti di Memoria e Processing
Facendo girare protocolli di routing con Link-State, in molte situazioni, viene richiesto che il router **utilizzi più memoria** ed esegua più processi di quanti ne possa fare con protocolli di routing basati su Distance-Vector. L'amministratore di rete, **deve essere sicuro che il router scelto sia capace** di fornire queste necessarie risorse.

Il router **tiene traccia** di tutti gli **altri router nel gruppo** e della rete che essi possono raggiungere direttamente. Per il link-state routing, la **memoria** deve essere in grado di **mantenere informazioni di vari databa**se, delle tabelle di **routing** e di **alberi topologici**. Utilizzando DIKSTRA'S ALGORITHM, per eseguide la SPF, è necessario un processing task proporzionale al numero di links sulla internetwork, moltiplicati al numero di router nella internetwork.

Requisiti di Banda:
Un'altra causa per quanto riguarda il **coinvolgimento della banda**, può essere determinata dal **flooding** causato dall'iniziale **pacchetto di link-state**. Durante la procedura iniziale di **scoperta,** tutti i routers, utilizzano i protocolli di link-state routing, inviando **pacchetti LSA** a tutti gli altri routers. Questa azione provoca un **Flooding** per la internetwork e quindi i routers, in questo caso **hanno bisogno di banda** e temporaneamente la banda per il traffico dei router viene ridotta, così quella per il trasporto dei dati. **Dopo questo** flooding iniziale, i protocolli di link-state **rechiedono solo la banda minima** per inviare infrequenti o event-triggered **pacchetti LSA** che si riflettono sul campo di tipologia.

Annunci di Link-State non sincronizzati (LSAs) provocano Decisioni di percorso Inconsistenzi by Routers: L'aspetto più complesso ed importante del Link-State Routing è **essere sicuri** che **tutti** i router **ricevano** i necessari **LSA packets**. I router con **differenti sets di LSAs**, calcolano le routes in base a **differenti topologie**. Quindi la rete diventa **irraggiungibile** con il risultato di disagi sui router e sui link. Seguiamo questo esempio di informazizone percorso inconsistente:

- Fra il router C ed il D, rete 1 è risulta DOWN. Entrambi I router, costruiscono un LSA packet per riflettere questo status.
- Più tardi la rete1, raggiunge lo status UP. Un altro pacchetto LSA reflette la prossima tipologia creata, quindi varia, in questo caso è indispensabile
- La rete origiale, numero 1 è Irraggiungibile. Un messaggio del tipo "unreachable", dal router C utilizza un percorso lento per l'update ed arriva più tardi. Questo pacchetto LSA può arrivare al router A dopo che è arrivato al router D. Il messaggio è il seguente: Network1, Backup Now. LSA.
- Con l'LSA non sincronizzato, il router A può avere dei problemi con il proprio SPF costruito. Il problema è questo: Deve usare un percorso che includa la rete1, oppure un percorso in cui la rete uno non ci sia a causa dell'aggiornamento che l'annunciava irraggiungibile?

Se la distribuzione dell'LSA a **tutti i routers non è efficiente, il LINK-STATe routing, può risultare INVALIDO**. Su reti di **grosse dimensioni**, un problema di questo tipo sul link-state può **espandere il problema**, per cui la distribuzione dei pacchetti LSA può avere delle conseguenze molto serie. Se **una parte** della rete Si attiva **(UP)** prima, ed **altre parti vengono su più tardi**, **l'ordine** di distribuzione dei pacchetti LSA **deve variare**. Questa variazione può può alterare o **impareggiare la convergenza**. I router devono apprendere differenti versioni di tipologia prima di costruire la propria SPF e le routing Tables. Su una internetwork di ampie dimensioni, la parte che si UPDATA più rapidamente può causare problemi per le parti che subiscono l'update più lentamente.

Distanza vettore V.s Link-State di protocolli Routing: E' possibile paragonare il distance-vector routing con il Link-state routing in diverse aree chiave:

- **Distance-Vector** routing **invia dati topologici dalle informazioni** contenute nelle tabelle di routing dei **routers vicini**. Il **link-state** routing ottiene **una vasta visione dell'intera topologia di rete** accumulando tutti i necessari LSAs.
- Il routing **Distance-vector** determina **il percorso migliore** aggiungendo dei **valori metrici** che riceve come informazioni di routing e che passa da **router a router**. Per il **Link-State**

routing, **ogni router lavora saparatamete** per calcolare il proprio percorso migliore per arrivare alle reti di destinazione.

- Con molti protocolli di routing basati su **Distance-vector**, l'update per la topologia va a cambiare per mezzo di tavole **periodiche**. L'informazione passa **da router a router**, spesso, ciò provoca una **lenta convergenza**. Con i protocolli **LINK-STATE** routing, **l'update** è solitamente **avviato da cambi di topologia**. Gli **LSAs,** relativamente **piccoli**, vengono passati a **TUTTI i routers** solitamente ciò ha come risultante **una rapido tempo di convergenza**, per cui rapidamente ogni router è a conoscenza del cambio di topologia.

Protocolli Ibridi di Routing: Un emergente terzo tipo di routing protocol, combina gli aspetti sia del **distance-vector che del link-state in un'unica tipologia**. Questo terzo tipo è chiamato **BALANCED-HYBRID ROUTING.** I protocolli balance-hybrid routing, utilizzano **distance-vector** con **più accuratezza** in termini di **distanza metrica** per determinare il miglior percorso per la rete di destinazione. Comunque essi si differenziano dalla maggior parte dei protocolli distance-vector ottenendo **aggiornamenti del cambio di topologia, solo quando avviene un update.**
Il balance-hybrid routing protocol, effettua **una convergenza rapida come il Link-State**. In sostanza, La differenza dal distance-vector el link-state **si evidenzia nell'utilizzo di varie risorse come Banda, memoria e processore**. Vari esempi di protocoli hybridi possono essere **ISI's IS-IS** (Intermediate System-to-Intermediate System), e Cisco **EIGRP** (Enchanced Interior Gateway Routng Protocol)

Routing Lan-to-Lan: Il livello di rete deve essere compreso ed interfacciato con vari livelli inferiori. I routers devono essere **capaci di gestire**, maneggiare ed incapsulare i pacchetti in vari frames di livello inferiore **senza cambiare l'address** di livello 3 del pacchetto.
La rete HOST dipende dal router e dal suo indirizzo, per poter trovare il miglior percorso che gli consente di **raggiungere una determinata destinazione**.
Quando il **router fa un check** sulle sue tavole di routing interne, esso **scopre che il miglior percorso** per la destinazione di rete2, **utilizza la porta To0**, interfacciata ad una rte Token-Ring. Quindi il livello più basso di framing deve cambiare al passaggio dati da ethernet, rete1 a token-ring sulla rete2. L'indirizzamento di livello 3, dalla sorgente, alla destinazione rimane sempre lo stesso. L'indirizzo di rete, per fare un esempio, resta NETWORK2, HOST6, riguardo o meno la differente encapsulation di basso livello.

Routing Wan-to-Wan: Il livello network deve **relazionarsi ad un'interfaccia** e con vari livelli di traffico LAN-To-WAN. A seguito di una crescita dell'internetwork, i percorso fornito dal pacchetto, può subire diversi punti di ripetizione, ed una varietà di tipologie di data link oltre le lan. Per esempio,

- Un pacchetto dalla workstation con indirizzo 3.1 deve attraversare un data link per raggiungere il file server all'indirizzo 2.4
- La workstation invia un pacchetto al file server, prima di far ciò, lo encapsula in un Frame token-ring indirizzato al router A
- Quando il router A riceve il frame, esso rimuove il pacchetto dal frame tocken-ring e lo encapsula in un frame di tipo FRAME-RELAY, dopo di che lo invia al router B.
- Il router B rimuove il pacchetto dal Frame Relay Frame e lo forwarda al file server in un nuovo ethernet frame.
- Quando il file server con indirizzo 2.4 riceve il frame ethernet esso estrae e passa il pacchetto all'appropriato processo di livello superiore.

I routers **permettono il passaggio dei pacchetti LAN-to-WAN** inserendo **l'indirizzo End-To-End** sorgente e di destinazione **durante l'encapsulamento del pacchetto in data frames**, nel modo più appropriato ed **adeguato**, per la tipologia di lan, che caratterizza il prossimo HOP lungo il percorso.

Selezione Percorso e Switching di protocolli Multipli e media: I Routers sono periferiche che **implementano** i servizi di rete. Essi forniscono interfacce per un **range vasto** di link e sottoreti e grantiscono **ampio range e velocità**. I routers sono **attivi ed intelligenti** nodi di rete che possono partecipare al managing della rete. I router gestiscono la rete, **fornendo protocolli dinamici** oltre le risorse e supportando i task per effettuare con successo la **connettività fra internetwork**.
Forniscono performance **affidabile**, controllo di gestione e flessibilità.
In aggiunta allo switching ed al routing, i routers hanno una varietà di features addizionali che aiutano a migliorare il rapporto costi-efficacia sulla internetwork. Queste Features includono il **traffico in sequenza** basato su Priorità e filtering del traffico.
Tipicamente, i router hanno bisogno di **supportare stacks di protocolli multipli**, ognuno con il proprio routing protocols, e permettono a questi differenti ambienti di operare in parallelo. In pratica, i routers **incorporano** anche le **funzioni di Bridging** e qualche volta servono, limitatamente, da hub.

12Protocolli di Routing

Modalità setup: Dopo aver **testato l'hardware** ed aver **caricato l'immagine IOS** del sistema operativo, il router trova ed **applica le regole di configurazione**. Queste entries forniscono al router, con i dettagli del router specifico e gli attributi, **le funzioni di protocolli, e gli indirizzi delle interfacce**. Comunque**, se un router non può** localizzare una valida configurazione di startup, esso entra nel setup iniziale di configurazione, chiamato **SETUP MODE**.
Con la modalità setup, è possibile, con facilità **rispondere alla domande**, nel system config dialog. Questa agevolazione, ci permette di rispondere a delle informazioni basilari di configurazione. Rispondendo si da la possiblità al router di usare quei parametri minimi, appena sufficienti per la gestione dell'apparato. Le entries a cui l'utente può accedere sono:

- Un inventario delle interfacce
- Una opportunità di entrare nei parametri globali
- Una opportunità di entrare nei parametri d'interfaccia
- Un review dello script di setup
- Una opportunità di indicare quando si desidera che il router debba utilizzare questa configurazione

Dopo aver approvato le entries della modalità setup, il setup **usa queste entries** per la configurazione "running". Il router inoltre **memorizza la configurazione in NVRAM** come "new startup-config", ed è possibile startarla utilizzando le funzioni del router. Infine per protocolli addizionali e vriazioni sull'interfaccia, è possibile usare la modalità **ENABLE** (enable mode) ed inserire il comando "configure".

Come il router prende informazioni sulla destinazione: Per default, i routers scelgono un determinato percorso, in differenti modi:

- **STATIC ROUTES – Manualmente** definita dall'amministratore di sistema, **dal prossimo hop** alla destinazione, utilizzate per la Sicurezza e riduzione del traffico
- **DEFAULT ROUTE – Manualmente** definita dall'amministratore di sistema, come il percorso da scegliere **quando non si conosce** la Route per la destinazione.

- **DYNAMIC ROUTING** – Il router **apprende** il percorso per arrivare a destinazione, ricevendo periodici update da altri routers.

Il comando IP ROUTE: Il comando **IP route** è una sorta di **Setup per lo static Route**.
La **distanza amministrativa** è un valore di **fedeltà** applicata alla **sorgente di routing**, espressa in **valori numerici, da 0 a 255**. Più **alto è il numero, più bassa è la fedeltà** della sorgente di routing.
Un route statico permette la configurazione **manuale delle tavole** di routing. Non avverrà quindi nessun cambiamento dinamico lungo il percorso. Un route statico può riflettere molte knowledge speciali, di sutazioni di rete, conosciute dall'amministratore di rete. Gli inserimenti manuali dei valori relativi alla distanza per le static routes sono solitamente dei numeri BASSI (1 per default). Gli updates di routing non sono inviate su un link se esso sono SOLO definiti come Route statici, quindi essi conservano la banda.
Con assegnazione del route statico, ad esempio, per raggiungere la STUB NETWORK 172.16.1.0 è cosa fattibile solo dal Router A poiché è l'unica possibilità che si ha di raggiungere tale rete.
E' inoltre possibile l'assegnazione del route statico per collegare il Router B con la NUVOLA di rete.Comunque un'assegnazione statica è indispensabile per ogni rete di destnazione, in tal caso il route di default può rappresentare valida decisione.

Il comando IP Default-Network: Il comando IP Default-Nework stabilisce un **route dinamico**, in una rete utilizzando i protocolli di rounting di default.
I default Routes mantengono le **tavole** di routing **quanto più Corte possibili**; **Quando non esiste**, nella routing table, **un entry che permette ad un pacchetto di raggiungere la rete di destinazione**, il pacchetto **è inviato alla rete di DEFAULT**. Poiché un router non ha una conoscenza completa della rete di destinazione, esso può usare un numero di una rete di default, per indicare la locazione dalla quale identificare il numero di rete sconosciuto. **Si usa il default** network number quando **c'è la necessità di localizzare un route ma si ha solo informazioni parziali** sulla rete di destinazione. **Il comando IP DEFAULT-NETWORK deve essere aggiunto a tuti i router** nella rete, per essere utlizzato con il comando addizionale **REDISTRIBUTE STATIC**, per cui tutti i routers saranno a conoscenza della candidata rete di default.
In questo esempio, il comando globale **IP DEFAULT-NETWORK 192.168.17.0** definisce la rete di classe C 192.168.17.0 come **il percorso di destinazione per i pacchetti che non hanno entries** nelle tavole di routing. L'amministratore della company X non vuole fare un update che provenga da una rete Pubblica. Router A necessita di un firewall per gli update di routing. Router A necessita di un mecanismo per raggruppare queste reti che condivideranno la strategia di routing della compagnia X. Per quanto riguarda il meccanismo di tale sistema, questo è definito, numero di sistemi autonomi.

Sistemi Autonomi: Un sistema autonomo consiste in router, **gestiti da più di un operatire**, che **rappresenta una consistente visione di routing** per il mondo Esterno. Il Network Comunication Center (NIC) assegna un unico sistema autonomo ad enterpries. Si tratta di un sistema autonomo a 16 bit. Un protocollo di routing come ad esempio **Cisco IGRP necessita la specifica di un unico sistema autonomo** nella propria configurazione.
I protocolli di routing esteriori, sono usati per **comunicazioni fra sistemi autonomi**. I protocolli di routing Interiori, sono invece usati con un singolo sistema autonomo.

Protocollo di Routing IP Interiore: Al livello Internet della Suite di protocolli TCP\IP, **un router può usare il protocollo di routing** ip per compleatare il routing **attraverso** l'implementazione di uno specifico **algoritmo di routing**, Esempio di routing ip protocols:

- **RIP** – Un protocollo di routing basato su Distance-Vector
- **IGRP** – Un altro protocollo di distance-vector
- **OSPF** – Un routing protocol Link-State

- **EIGRP** – Un protocollo Hibrido

TaskS di configurazione IP: La selezione di un protocollo di routing ip, comporta il settaggio **sia a livello global che a livello di interfaccia**. La Global Task include la **selezione di un protocollo di routing, RIP o IGRP**, ed offre la possibilità di **indicare indirizzi ip di rete** con specifici valori di Subnet. La Interface Task permette di assegnare Indirizzi Network\Subnet e l'appropriata subnet mask. **Il Dynamic routing utilizza il Broadcast** ed il Multicast **per comunicare con gli altri routers**. Il Routing **metric aiuta i routers** a trovare il **miglior percorso** per ogni rete e subnet.

Utilizzare i comandi Router e Network: Il comando ROUTER esegue il processo di Routing. Il comando **NETWORK**, è indispensabile poiché esso **attiva il processo di routing**, che determina quale interfaccia parteciperà all'invio ed alla ricezione degli updates di routing.
Il numero di rete **deve esser basato sulla classe della rete**, non può essere un indirizzo subnet o host individuale. La maggior parte delle LAN sono limintate a numerazioni di reti appartenenti alle Classi A,B o C.

Elementi chiave del Rip: Il RIP è stato originariamente specificato in RFC 1058. La sua caratteristica chiave include:

- E' un routing protocol **basato su Distance-Vector**
- Il **conteggio degli hop** è usato come **"metric**" per la selezione del percorso
- Se il conteggio degli hop raggiunge **un numero maggiore di 15, il pacchetto è scartato**
- Gli **update** di routing per **broadcast**, avvengono **ogni 30 secondi**.

Utilizzare comandi Router Rip e Network per abilitare RIP: Il comando **Router RIP seleziona il RIP come protocollo di Routing**. Il comando di rete assegna un NETWORK CLASS address, **a cui il router sarà direttamente connesso**. Il processo di routing **associa interfaccce con l'indirizzo di rete** ed inizia ad usare in RIP sulla rete specificata.
NOTA: Nel rip, **tutte le subnet mask devono essere le stesse**. Il RIP non condivide informazioni di Subnetting nell'update dei routers.

Abilitare Rip su Reti Ip-Addresses: In questo esempio la descrizione dei comandi è la seguente:

- **ROUTER RIP** – Seleziona rip come Routing protocol
- NETWORK 1.0.0.0 – Specifica una rete direttamente connessa
- NETWORK 2.0.0.0 – Specifica una rete direttamente connessa

Una interfaccia Router A della cisco che è connessa alla rete 1.0.0.0 e 2.0.0.0, invia e riceve UPDATES RIP. Questi Update di routing permettono al router di apprendere la tipologia di rete.

Monitoraggio del flusso di pacchetti, usando il comando Show IP protocol: Il comando **SHOP IP PROTOCOL visualizza i valori, riguardo al Routing** Timers ed informazioni di rete che sono assciate interamente con il router. Usare questo informazioni **per identificare un router** che **si sospetta** possa effettuare il delivery di informazioni **non corrette**.
Generalmente, il router **invia gli update** (tavole di routing) **ogni 30 secondo** (intervalli configurati). Se passano 70 secondo dall'ultima volta che esso ha inviato l'update, il prossimo verrà inviato fra 13 secondi. Seguendo la linea "routing for networks", il router specifica le routes per le reti listate. L'ultima linea mostrata mostra che la distanza amministrativa del rip è 120.

Il comando Show IP Router: Il comando **SHOW IP ROUTE** visualizza il **contenuto delle tavole** di routing ip **che contengono entries** per tutte le reti conosciute e le sottoreti, per mezzo di un codice che indica quante e che informazioni sono state apprese e memorizzate.

Caratteristiche chiave dell'IGRP: IGRP è un protocollo di routing **basato su DISTANCE-VECTOR e creato da Cisco**. IGRP **invia gli updates** di routing, ad **intervalli di 90 secondi**, pubblicizzando reti o particolari sistemi autonomi. Molte delle caratteristiche chiave di IGRP..

- **Versatilità** che permette automaticamente **handle indefinti, complesse tipologie**.
- **Flessibilità** per segmenti che hanno diversa capienza (banda) e **caratteristiche di ritardo**
- **Scalabilità e funzionalità** in reti di **grandi dimensioni**

Il protocollo di routing IGRP **utlizza 2 misurazioni metric**. **BANDA E RITARDO**. IGRP **può essere configurato** per utilizzare **una combinazioni di variabili** che compongono il metric, queste variabili sono:

- **Banda**
- **Ritardo**
- **Carico**
- **Affidabilità**

Utilizzare i comandi IGRP e Network per abilitare IGRP: Il comando **ROUTER IGRP** permette **di scegliere IGRP come protocollo di routing.**
Il comando **NETWORK** specifica **ogni rete direttamente connessa** che deve essere inclusa. Come RIP, **tutte le subnet mask devono essere ugali**. IGRP non condivide le informazioni di SUBNETTING negli updates di routing.

Abilitare IGRP su reti IP-Addressing: IGRP è selezionato come **ROUTING PROTOCOL** per **sistemi autonomi 109**. Tutte le interfacce connesse alla rete 1.0.0.0 e 2.0.0.0 saranno usate per inviare e ricevere tavole di update IGRP. In questo esempio:

- **ROUTER IGRP 109** – Seleziona IGRP come routing protocol per sistemi autonomi 109
- NETWORK 1.0.0.0 – Specifica una rete direttamente connessa
- NETWORK 2.0.0.0 – Specifica una rete direttamente connessa

Monitorare il flusso di pacchetti usando il comando Show IP Protocol: Il comando **SHOW IP PROTOCOL** visualizza parametri, filtri ed informazioni di rete **su tutti i protocolli di routing** (RIP, IGRP, ecc.ecc), in utilizzo sul router. **L'algoritmo usato per calcolare** il routing metric, per IGRP è raffigurato in questa finestra. Essso definisce il valore di K1-K5 metrics, ed il massimo conteggio degli hop. Il metric K1 rappresenta la banda ed il metric K3 rappresenta il ritardo. Per default i valori del metric K1 e K3 sono settati ad 1. K2,K4,K5 metric sono settati a Zero.

Il comando Show Ip Interface: Il comando **SHOW IP INTERFACES visualizza lo status** ed i parametri globali associati alle interfacce IP. **Il cisco IOS SOFTWARe automaticamente inserisce un route directly-connected** nella tabella di routing se l'interfaccia è quella tramite la quale il software può inviare e ricevere pacchetti. Se l'interfaccia è marcata **come UP è utilizzable**, Se l'interfaccia è **DOWN o Inutilizzabile, è rimossa dalla tabella di routing**. Rimuovendo l'entry è possibile permettere l'uso delle routes di backup, sempre che queste siano esistenti.

Il comando Show Ip Route: Il comando **SHOW IP ROUTE** visualizza il contenuto **delle routing tables ip**. Le tavole contengono **una lista di tutte le reti conosciute**, delle subnets e dei metrics associati ad ogni entry. Nota: In questo esempio le iformazioni **sono trasportate da IGRP** (I) o da connessioni dirette ©.

Il comando Debug Ip Rip: Il comando **DEBUG IP RIP visualizza gli updates di routing ip**, nello **stesso modo** in cui essi sono stati **inviati e ricevuti**. In questo esempio l'update è inviato da 182.8.128.130. Esso è stato rilevato da tre routers, uno di questo è inaccessibile poiché per

raggiungerlo occorre effettuare più di 15 HOPS. Gli updates vengono quindi **Broadcastati** dall'indirizzo 183.8.128.2.
E' indispensabile **fare attenzione** quando si usa il comando DEBUG. Il comando DEBUG è un **processo intenso**, e può causare un **peggioramento delle performance** di rete, in alcuni casi perdita di connettività. **Utilizzare solo quando la rete è poco usata**. **Disabilitare** il comando quadno si ha finito digitando **NO DEBUG IP RIP o NO DEBUG ALL.**

SEMESTRE 3

MODELLO OSI e ROUTING

Il modello Osi e la divisione in Livelli: I modelli di rete utilizzano **i livelli per semplificare** le funzioni di rete. La **separazione** delle funzioni di rete è **chiamata Layering**. Per capire l'importanza del layering, bisogna considerare il modello osi come un modello stratificato per comprendere l'implementazione della comunicazione fra computer. Utilizzando i livelli, il modello OSI, **semplifica le procedure** necessarie al fine della **comunicazione** fra 2 computers. Ognuno può contrantersi su una specifica funzione, permettendo al designer di rete di scegleire la periferica e la funzionalità specifica per quel determinato livello. Nel modello Osi, Oguno dei sette livelli indica una funzione distinta. Il motivo di questa divisione delle funzioni di rete include:

- I livelli dividono gli aspetti delle operazioni di rete **in elementi meno complessi**
- I livelli definiscono interfacce **standard per compatibilità plug and play**
- I livelli abilitano gli ingegneri a specielizzarsi e **designare funzioni modulari**
- I livelli si promuovono **simmetricamente** in diverse funzioni modulari di rete, e possono **lavorare contemporaneamente**.
- I livelli prevengono cambi in un'area per effeto di cambi su un'altra area, quindi ogni area si può **evolvere più velocemente**.
- I livelli dividono la complessità del networking in **separate operazioni facili da imparare**.

Livelli del modello OSI: Ogni livelli del modello osi, assolve ad **una specifica funzione**:
APPLICAZIONE- Livello 7: Questo livello **fornisce servizi di rete alle applicazioni** per l'utente. Una applicazione di word processing è servita, per il trasferimento file, da questo livello.
PRESENTAZINE- Livello 6: Questo livello fornisce la **presentazione dei dati e la formattazione in codice**, lungo la negoziazione dei dati e la sintassi di trasferimento. Esso garantisce che i dati che arrivano dalla rete possano essere usati dall'applicazione, e garantisce che le informazioni inviate dall'applicazone possano essere trasmesse lungo la rete.
SESSIONE- Livello 5: Questo livello stabilisce, mantiene e gestisce **le sessioni fra applicazioni**.
TRASPORTO- Livello 4: Questo livello **segmenta e riassembla i dati in un Data Stream**. Il livello trasporto ha la potenzialità di **Garantire una connessione ed offrire affidabilità** di trasporto.
NETWORK- Livello 3: Questo livello **determina il miglior percorso** per il trasporto dei dati da una posizione ad un'altra. Il router OPERA a questo livello. Questo livello usa l'indirizzamento Logico, in uno schema che può essere gestito da un'amministratore. Questo livello utilizza lo schema del protocollo internet IP e Apple-Talk, DECnet,VINES, e gli schemi di IPX
DATA LINK- Livello 2: Questo livello fornisce la **trasmissione fisica** sul media. Esso gestisce la **notifica degli errori**, la tipologia di rete ed il controllo di flusso. Questo livello utilizza l'indirizzo Media Access Control (MAC), che è anche riferito come indirizzo fisico o Hardware.

FISICO- Livello 1: Questo livello fornisce il **meccanismo elettrico e procedurale** per attivare e mantenere il link fisico attraverso più sistemi. Questo livello utilizza un media come ad esempio Twisted-Pair, Coassiale, e Fibra ottica.

Comunicazioni Peer To Peer: Il modello osi descrive come le informazioni create da un software attraversano un media di rete. Affinchè le informazioni inviate, attraversino i livelli di rete di un dato sistema devono essere composte da Zero e UNO. Ogni livello utilizza il proprio livello di protocollo per comunicare in maniera peer to peer con altri sistemi. Questo **scambio di unformazioni utilizza il PDU**, in cui avviene una comunicazione fra stessi livelli. Ogni livello di protocolo scambia le informazioni con lo stesso.
Il layering del modello osi, **proibisce comunicazioni dirette fra livelli (peers) in differenti host**. Ogni host deve **rispondere al servizio fornito dell'host adiacente**. Il segmento TCP fa parte del pacchetto di livello 3, il quale è uno scambio fra ip peers. A sua volta, il pacchetto ip diventa parte del frame data link scambiato con la periferica direttamente connessa. Infne questi frame devono diventare bits e finalmente trasmessi al livello fisico utilizzando l'hardware.

Encapsulation: La richiesta specifica è memorizzata come **informazione di controllo** che è passata tramite livelli (peers), nel blocco dell'header che è attaccato all'attuale informazione di applicazione. **Ogni livello dipende dalla funzione del servizio sottostante**. Per **fornire** questo servizio **il livello inferiore utilizza l'encapsulation** per inserire il PDU del livello superiore nel proprio campo data, quindi esso può aggiungere headers e trailers che eseguiranno la funzione.
Il concetto di Header e data è relativo, dipende del livello corrente di analisi dell'unità di informazione. Per esempio. Nel livello 3 l'informazione consiste nel Livello 3 header, e nei dati che seguono. I dati del livello3, **quindi, possono potenzialmente contenere gli headers** del livello 4,5,6 e 7. Più **specificatamente l'header del livello 3 ha la funzione di semplificare i dati per il livell2**. Questo concetto è illustrato in seguito. **Non tutti i livelli** hanno la necessità di **appendere gli headers al livello inferiore**. Diversi livelli eseguono **una semplice traduzione** dei dati attuali che ricevono per renderli leggibili dal livello adiacente.
Per esempio il livello network fornisce un servizio al livello transport, ed il livello transport presenta i dati al livello network. Il livello network quindi encapsula i dati all'interno di un header. Questo header contiene informazioni necessarie per completare il trasferimento del file, dalla sorgente alla destinazione ,secondo l'indirizzo logico. Il livello Data Link a sua volta, fornisce un servizio al livelli network encapsulando le informazioni contenute in esso, all'interno del frame. Il frame header contiene informazioni necessarie a completare le funzioni del data link. Per esempio l'header del frame contiene l'indirizzo fisico. Il livello fisico fornisce un servizio al livello data link, econdando il frame data link in una quntità di UNO e ZERO per la trasmissione sul cavo. Per esempio Per l'invio di una email sono necessari diversi step di conversione.
STEP1-Un utente invia un messaggio email, i cui caratteri alfanumerici sono **convertiti in DATA**, la partenza avviene a livello 7 e attraversa il livello 5 prima di essere inviata alla rete
STEP2-Utilizzando i segmenti al livello 4, **la funzione di trasporto**, **impacchetta i dati** per il transport (4), e garantisce che il messaggio possa essere leggibile dall'inizio alla fine e possa avvenire una comunicazione sicura.
STEP3-I dati **sono posizionati in pacchetti (o datagrams), al livello 3, che contengono network header con sorgente e destinazione** dell'indirizzo logico. Quindi la periferica di rete invia il pacchetto attraverso la rete, lungo il percorso scelto.
STEP4-Ogni periferica di rete **inserisce il pacchetto in un frame, al livello 2, il frame permette la connessione con le periferiche di rete direttamente connesse al link**. Ogni periferica, all'interno della rete selezionata e del percorso, richiede il framing per connettersi con la prossima periferica.
STEP5-Il **frame deve essere convertito in una serie di UNO e ZERO per la trasmissione sul media**. Spesso si tratta di cavo o fibra ottica. Al livello 1. La funzione di clocking abilita la periferica a distinguere i bits affinchè essi possano attraversare il media. Il media, sulla rete fisica,

può variare lungo il percorso. Per esempio il messaggio email può essere originato, su una lan, appoggiandosi ad un backbone, ed uscire su un link WAN finchè non raggiunge la destinazione, su un'altra LAN.

Tre Categorie di Ethernet: Ethernet ed Ethernet 802.3 comprendono **la più nota varietà** di protocolli LAN utilizzati. Attualmente il termine **Ethernet** è spesso usato come **rifericomento** al Carrier Sense Multiple Access Collision Detect **(CSMA\CD)** che generalmente **è anche conforme alle specifiche ethernet, incluso IEEE 802.3**.
Quando esso fu progettato, ethernet ebbe lo scopo di attraversare il terreno per **medie-lunghe distanze, reti a bassa velocità, e stanze specializzate in cui , per distanze limitate, i dati viaggiano a velocità molto elevate**. Ethernet è ottimo per applicazioni dove il media per **comunicazione locale** dove il traffico **non è molto intenso**.
Il termine **Ethernet** si riferisce **alla famiglia di implementazioni LAN** che includono tre categorie principali:

- Ethernet e IEEE 802.3 – Specifica per lan che **opera a 10 Megabit** al di là di coassiale e cavo Twisted Pair.
- 100-Mbps Ethernet – Anche conosciuta come Fast Ethernet, **l'ethernet a 100Megabit** specifica una lan che opera a 100 megabit tramite un Twisted Pair Cable
- 1000-Mbps Ethernet – Anche conosciuta come GigaByte Ethernet, **1000-Mbps Ethernet** specifica una LAN che opera ad 1 gigabit, attraverso fibra ottica o Twisted Pair Cable.

Ethernet è sopravvissuta come **tecnologia Essenziale** poiché essa è estremamente flessibile e perché essa è **semplice** per quanto riguarda la sua implementazione e comprensione. Altre tecnologie sono state promosse come ottimi rimpiazzi, ma i managers di rete hanno scelto ethernet e suoi derivati come effettiva soluzione per reti di dimensioni **fino al "campus**" e relativa implementazione. Per risolvere le **limitazioni** dell'ethernet, le organizzazioni hanno creato **grandi condutture per il cablaggio**. Dal punto di vista critico si potrebbe considerare ethernet come una tecnologia che non è in grado di crescere, nonosante ciò, lo schema i trasmissione ethernet continua ad essere **uno dei principali mezzi di trasporto** per lan e campus applications.

Tre Tipi di Ethernet a 10Megabit: Il cablaggio standard di ethernet e ethernet 802,3 **definisce una Bus topology** LAN che opera a **10 megabit**. Ci sono 3 tipo di standard:

- 10Base2 – Conosciuta come **Thin Ethernet o ThinNET**, 10Base2 consente di avere segmenti la cui grandezza in termini di distanza **supera gli 185 metri** su cavo coassiale.
- 10Base5 – Conosciuta come **Thick Ethernet**, 10Base5 permette segmenti di rete di distanza superiore a **500 metri sul cavo coassiale**.
- 10Base-T – 10base-T trasporta i framese ethernet in **un twisted pair** economico. Il cablaggio individuale non può superare i **100 metri**.

Gli standards di cablaggio **Ethernet e IEEE 802,3 specificano una rete di BUS topology** con connessione fra stazioni end\to end. Il mezzo di comunicazione fisico è anche chiamato **Transceiver cable**.Il transceiver è collegato con il media fisico. La configurazione dell'IEEE 802,3 è quasi sempre la stessa cosa, ma il connecting cable è considerato come Attachment Unit Interface **(AUI)**, ed il **transceiver** è chiamato **Media Attachment Unit (MAU)**. In entrambi i casi, il cavo di connessione si collega con una **interface board**, all'interno della stazione finale.
Le stazioni sono collegate al segmento con un cavo che passa dall'aui nella stazione al mau, che è direttamente collegato al cavo coassiale ethernet. Poiché il 10Base-T fornisca accesso ad un'unica stazione, le stazioni collegate alla lan tramite la 10base-T debbono essere sempre connesse ad un hub o ad uno switch.

Analogia di "NIC": L'accesso al media di rete avviene **al livello Data Link** del modello OSI. Il data link, **dove il mac è situato**, è adiacente al livello Fisico. Non possono esistere due indirizzi

mac. Così su una rete, la scheda di rete, è situata nello stesso punto in cui la periferica stessa si connette al media fisico. Ogni Scheda di rete **ha un unico indirizzo MAC**.
Ogni scheda di rete che lascia la fabbrica riporta **l'indirizzo mac con le sigle di assegnazione** del manufacturer. Questo indirizzo è programmato **all'interno di un chip** sulla scheda di rete. Poiché il mac address è locato sulla scheda di rete, se una scheda di rete è sostituita, l'indirizzo fisico della stazione cambia. Il mac address è scritto utilizzando la numerazione **BASE 16, con numeri ESADECIMALI**. Ci sono **2 formati** di indirizzi MAC. 0000.0c12.3456 e 00-00-0c-12-34-56.
Sulle reti ethernet, quando una periferica vuole inviare i dati ad un'altra periferica, essa può aprire una comunicazione verso l'altra periferica, utilizzando il proprio indirizzo MAC. Quando i dati **sono inviati all'esterno** sulla rete, dalla sorgente, essa **trasporta l'indirizzo mac della destinazione**. Quindi questi dati attraversano il media, le schede di rete di ogni periferica controllano se il mac address coincide con quello ricercato e trasportato all'interno del frame.
Se non ci sono uguaglianze, la scheda di rete ignora il frame ed esso continua lungo la rete, per giungere alla prossima stazione. Quando avviene **un riconoscimento** del mac, la scheda di rete, **fa una copia del frame** che è posizionata nel computer dove essa risiede al livello data link. **Dopo che** il frame è stato **copiato**, **esso continua il suo viaggio** alla ricerca di un altro riconoscimento.

Trasporto tramite Mezzo fisico e connessione a periferiche: L'ethernet e 802.3 data link, fornisce il **trasporto dei dati**, tramite un link fisico, fra 2 o più periferiche. Per esempio le tre periferiche possono essere direttamente connesse, l'una con l'altra, tramite una LAN Ethernet. Un router centrale che collega più networks utilizza il mac address di entrambi le periferiche delle reti collegate.

Protocolli Livello 3 dello stack TCP\IP: Molti protocolli operano al livello network del modello OSI:

- IP – Fornisce **connectionLess, consegna di Best-Effort, e datagrammi di routing**. Questo non riguarda il contenuto dei datagrammi o pacchetti. Esso si occupa di **portare i datagrammi** a destinazione.
- ICMP – Fornisce un controllo **a livello di messaggistica**.
- ARP – Determina **l'indirizzo data link** per indirizzi ip conosciuti
- RARP – Determina **gli indirizzi network** quando il livello data link (MAC) è conosciuto.

Reti e Sottoreti di Indirizzi IP: Nell'ambiente TCP\IP **tutte le stazioni comunicano** con i server gli host ed altre stazioni. Questo avviene poiché ogni nodo che **usa la suite del tcp\ip** ha un unico **indirizzo logico a 32 bit**. Conosicuto come **Ip Address**. In aggiunta all'ambiente tcp\ip, ogni rete è vista come un **singolo ed unico indirizzo** ip. Tale indirizzo può essere raggiunto prima che un'host individuale facente parte dello stesso, possa essere contattato.
Le reti possono essere **segmentate in una serie di piccole reti**, chiamate **SUBNETWORKS**. Quindi un ip address è **frazionato** in network number, **subnetwork** number e **host** number. Subnet sono **indirzzi unici a 32 bit**, creati prendendo i bit dal campo host. Gli indirizzi subnet sono **visibili da altre periferiche** sulla stessa rete ma **non sono visibile fuori dalla stessa rete**, poiché le informazioni dettagliate sullo schema di subnetting è normalmente **non condiviso all'esterno** con i router vicini. Le subnets permettono un **utilizzo più efficiente degli spazi riservati** agli indirizzi ip. **Non esiste differenza** per come **l'esterno vede la rete**, ma all'interno della struttura ci sono delle strutture addizionali, visualizzabili. La rete 172.16.0.0 è divisa in 4 subnets: 172.16.1.0, 172.16.2.0, 172.16.3.0 e 172.16.4.0.

Determinazione percorso nel contesto dei pacchetti e del routing: La **determinazione del percorso** indica **il path** che si dovrebbe seguire, attraversando la nuvola di rete. I routers valutano il **miglior percorso** per il traffico. La **determinazione del percorso** avviene a **livello 3**, livello di

NETWORK. I servizi di routing usano le **informazioni derivanti dalla tipologia** di rete in fase di valutazione del percorso. Questa informazione può essere **configurata da un amministratore** di rete o collocata **all'interno di un processo** dinamico in esecuzione sulla rete. Il livello network **connette le reti** e fornisce il best-effort ed il servizio di consegna end to end gestito dal livello trasporto. Il livello di network invia pacchetti dalla rete sorgente alla destinazione, **bsandosi sulle ip routing tables**. **Dopo** che il **router ha determinato quale percorso** usare, esso **può procedere con lo switching** dei pacchetti. Lo **switching** fa si che **i pacchetti siano accettati da una interfaccia e forwardati ad un'altra interfaccia o porta** che riflette il miglior percorso per la destinazione dei pacchetti.

Gli indirizzi di livello 3 devono contenere informazioni Path e Host: Affinchè le comunicazioni sul percorso siano pratiche, **una rete deve rappresentare** un percorso **consistente** costituito da routers. L'indirizzo di rete che rappresenta il network di questo percorso, contiene il percorso e la porzione di host. La **porzione del percorso** identifica **una parte di percorso** usata dal router all'interno della nuvola di rete. La **porzione dell'host identifica una specifica periferica sulla rete.** Il router usa **l'indirizzo network per identificare la rete sorgente o la rete destinazione** per i pacchetti. Il router **utilizza l'indirizzo di rete per identificare** la rete sorgente o la rete di destinazione dei pacchetti.
Per alcuni protocolli di livello 3, un **amministratore** stabilisce questa relazione **assegnando un indirizzo** di rete per un tempo assegnato in conformità con la pianificazione degli indirizzi di rete. Per altri protocolli su livello network, l'assegnazione degli indirizzi **è parzialmente o completamente dinamica**. La consistenza dell'indirizzamento di livello 3 sull'intera network, inoltre, **migliora ed ottimizza l'uso della banda** prevenendo broadcast non necessari. I broadcast causano traffico non necessario e disturbano qualsiasi dispositivo o connettore che non necessita del broadcast. Utilizzando **un addressing end to end** per rappresentare il percorso delle connessioni di rete, i livello network **può trovare il percorso** senza il bisogno di utilizzare periferiche non necessarie o link sulla rete. **Può funzionare in maniera autonoma**.

Tipi di messaggi ICMP: I messaggi ICMP sono **traportati in datagrammi IP** ed usati per inviare messaggi di **errore** e di **controllo**. ICMP utilizza i **seguenti tipi di messaggi definiti**. Altri possono esistere e non essere necessariamente inclusi in questa lista:

- Destinazione Irraggiungibile
- Tempo ecceduto
- Problemi di parametro
- Sequenza di sorgente
- Redirect
- Echo
- Echo reply
- TimeStamp
- TimeStamp reply
- Richiesta D'informazione
- Risposta D'informazione
- Richiesta D'indirizzo
- Risposta D'indirizzo.

Comando PING e ICMP: Un router **riceve** un pacchetto **che non è in grado di essere trasportato** fino alla destinazione ultima, dunque questo router **invia un messaggio** (icmp host unreachable) alla sorgente. **Il messaggio è "undeliverable" poiché non si conosce il percorso per la destinazione**.

A R P: Per comunicare su una rete ethernet, la stazione sorgente **deve conoscere l'indirizzo ip** della stazione di destinazione **e l'indirizzo MAC**. Quando la sorgente ha **determinato l'indirizzo ip della destinazione**, il protocollo internet sorgente, **guarda nella tavola ARP** per localizzare **l'indirizzo mac** per la destinazione. **Se il protocollo internet, localizza** una mappatura dell'ip address di destinazione ad un mac address nella propria tavola, **essi abbina l'indirizzo ip al mac** address e utilizza esso per encapsulare i dati. **Il pacchetto è quindi inviato** all'esterno oltre il media di rete, fino a che non raggiunge la destinazione. **Se l'indirizzo MAC non è conosciuto**, la sorgente **deve inviare fuori una richiesta ARP**. Per determinare l'indirizzo di destinazione per un datagramma, **è controllata la tabella ARP** sul router. Se l'indirizzo non è nella tavola, **arp invia un broadcast** cercando la stazione di destinazione. **Ogni stazione sulla rete riceve** questo broadcast.
Il termine ARP locale è usato quando **sia l'host richiedente che quello di destinazione** condividono lo stesso media.
Precedentemente alla tabella arp, è avvenuta una consultazione della subnet mask. Il mask ha determinato che tali nodi sono situati sulla stessa rete.

Il Routing in una Lan Mista: Il livello network **deve relazionarsi ad un'interfaccia** con vari **livelli inferiori**. I routers devono essere **capaci di riassemblare** l'handing dei pacchetti encapsulati in differenti **frame di basso livello senza** possa **cambiamenti all'header** del pacchetto, sull'indirizzamento di livello 3. **Quando il router controlla** la propria tabella di routing, esso scopre che il percorso migliore per la rete 2, mostra il passaggio dalla porta T0, sull'interfaccia collegata ad una LAN token ring.
Benchè **il livello inferiore di framing debba cambiare** a seguito dello **switching** dei pacchetti effettuato dal router, da una rete ethernet, ad una rte token ring, **l'indirizzamento di livello 3, resta lo stesso**. La rete di destinazione resta la stessa, l'host resta lo stesso. Cambia solo il tipo di encapsulation di livello inferiore.

Operazioni base che vengono eseguite dal Router: I routers generalmente **rilasciano un pacchetto** da un data link ad un altro. Per rilasciare un pacchetto, un router **usa 2 funzioni basilari**: La funzione di **determinazione percorso**, e la **funzione di Switching**. La funzione di switching, permette ad un router di **accettare un pacchetto su una interfaccia e forwardarlo su una seconda** interfaccia. La funzione di **determinazione del percorso** abilita il router a **selezionare l'interfaccia più appropriata per il forwarding** del pachetto. La porzione del nodo di indirizzo si riferisce **alla specifica porta del router** che si riferisce alla direzione **relativa al router adiacente**. Quando un'applicazione host ha la necessità di inviare un pacchetto ad una destinazione su una rete differente, un frame data link è **ricevuto su una delle interfacce del router**. Il livello network procede **esaminando l'header** e **determinando la rete di destinazione e la referenza della routing table** che associa la rete **all'interfaccia di uscita**. Il frame originale è spogliato e scartato. Il **pacchetto è ancora encapsulato nel frame data link per l'interfaccia selezionata** e memorizzato in **un'attesa** (queue) per il delivery **al prossimo HOP del percorso**.
Questo processo avviene ogni volta che il pacchetto è Switchato **attraverso ad un altro router**. Una volta giunto al router connesso alla rete che contiene l'host di destinazione, il pacchetto è ancora **encapsulato** nella lan di destinazione **tramite un frame** e trasportato all'host di destinazione.

Routing Statico e Dinamico: Il routing **statico** è **amministrato manualmente**. Un amministratore di rete **inserisce le route** nella configurazione del router. L'amministratore deve **fare l'update manuale** di questa route statica; Quando **la tipologia** di rete **cambia**, viene richiesto un **update**. Il routing statico riduce l'overhead perché i routing **updates non sono inviati**, come nel caso del rip, ogni 30 secondi. Il routing **Dinamico** lavora differentemente. Dopo che l'amministratore di rete ha inserito **i comandi di configurazione**, il comando di **partenza del dynamic routing**, la conoscenza

del percorso **è acquisita automaticamente**, da un **processo di routing**, quando una nuova informazione è ricevuta dalla rete. I cambiamenti sono **scambiati fra routers**, come parte del processo di **update**.
Il routing **statico** trova campo in diverse applicazioni. Esso permette ad un amministratore di **specificare che cosa deve essere propagandato su partizioni ristrette della rete**.
Per ragioni di sicurezza, l'amministratore **può nascondere parti di rete**. Il **dynamic** routing tende a **rivelare ogni cosa** conosciuta sulla rete. In più, quando una rete è accesssibile **solo da un percorso**, il **routing statico può essere sufficiente**. Questo tipo di partizione è chiamato **STUB NETWORK**.
Configurando lo static routing come una stub network, **si evita il carico** che si avrebbe con il **dynamic** routing poiché gli update non sono inviati.

La Default Route: Una entry all'interno della tabella di routing, è utilizzata per **direzionare i pacchetti, per i quali la prossima hop non è esplicitamente listata nella routing table**. Questa entry è chiamata Default Route.

Routed e Routing Protocols: Può esserci spesso confusione fra terminologie similari quali ad esempio **routing e routed** protocols:

- Routed Protocol – Ogni protocollo di rete che **fornisce sufficienti informazioni** al proprio indirizzo di livello di rete, sufficienti **da permettere ad un pacchetto di essere forwardato** da un host ed un altro host basandosi sullo schema di indirizzo. I routed protocols **definiscono il formato e l'utilizzo dei campi con il pacchetto**. I pacchetti generalmente sono convogliati da un end system ad un altro end system. IP è un esempio di routed protocol.
- Routing Protocol – Un protocollo che **supporta un routed protocol fornendo meccanismo per condividere le informazioni di routing**. I messaggi di routing protocol si **spostano fra routers**. Un routing protocol **permette al router di comunicare** con altri router di **updatare e mantenere le tavole**. Gli TCP\IP di routing protocols sono **RIP**: Routing Information Protocol, **IGRP**:Interior Gateway Routing Protocol, **EIGRP**: Enchanced Interior Gateway Routing Protocol, e **OSPF**: Open Shortest Path First Protocol.

Le informazioni che il router usa per eseguire il Routing Base: Il **successo** del dynamic routing dipende da **2 funzioni basilari**: Mantenimento della **Tabella di routing**, Distribuzione **temporale della conoscenza formalmente come Routing UPDATES ad altri routers**. Il Dynamic Routing confida nel **routing protocol** per condividere la consocenza di rete. Un routing protocol definisce un **set di regole** usate da un router quando esso comunica con i router vicini. Per esempio, un protocollo di routing descrive:

- **Come gli update sono INVIATI**
- **Che tipo** di conoscenza di rete è contenuta in questi updates
- **Quando inviare** questa conoscenza di rete
- **Come localizzare** i recipienti degli update.

I protocolli di routing **exterior** sono usati per **comunicare fra sistemi autonomi**. **Interior** routing protocols sono usati **con un singolo sistema autonomo**.

Protocolli di Routing: Al livello network del modello osi, un router **può usare il protocollo ip** di routing per **compiere il routing** attraverso **l'implementazione di uno specifico protocollo di routing**. Esempi di protocolli di routing ip includono:

- RIP-A – Distanza vettore Routing Protocol
- IGRP – Cisco Distanza vettore Routing Protocol
- OSPF-A – Link-State Routing Protocol
- EIGRP-A – Hibrido Routing Protocol

Molti **protocolli di routing** possono essere **classificati** fondamentalmente, per uno dei due tipi base. **Distance Vector o Link State**. Il routing protocol **Distance Vector** determina la direzione (vettore) e la **distanza di ogni link della rete**. Il **link State routing** protocol (anche chiamato Shortest Path First –SPF protocol) approssimativamente **ri-crea l'esatta tipologia dell'intera rete** (o dell'ultima partizione in cui il router è situato). Un terzo tipo di protocollo, è il **Balanced-Hybrid procol**, combina **gli aspetti dei protocolli distance vector e link state**.

Convergenza di Rete: I protocolli di routing che sono usati per **determinare la miglior "route"** per il traffico **da una particolare sorgente ad una particolare destinazione**, sono **fondamentali per il dynamic routing**. Quando la topologia della rete cambia, **deve cambiare la configurazione di tutti i routers**. La conoscenza di rete deve riflettersi **accuratamente** sulla **nuova tipologia**, per tutti gli apparati. Questa visione generica, che tutti i router acquisiscono è chiamata **CONVERGENZA** (convergence). Quando **tutti i router nella rete stanno operando con la stessa conoscenza del network, la rete è CONVERGED**. La convergenza **rapida è desiderabile**, in quanto **riduce fallimenti di rete, diminuendo il tempo di updating**.

Routing DISTANCE Vector: Nel **distance vector**, vengono passate **periodiche copie** della tabella di routing **da router a router**. Ogni router **riceve una routing table** dal proprio vicino. Per esempio, il router B riceve informazioni dal router A. Router B aggionge un numero di distanza vettore (come numero di hops), incrementando la distanza, e quindi passa la tabella di routing all'altro vicino, in questo caso, router C. Quando stesso step, **avviene in ogni direzione**, **fra router vicini**. In questo modo, il protocollo **accumula distanza** di rete, ed è possibile **mantenere un database** delle informazioni relative alla tipologia di rete; C'è da dire però, **che i protocolli di distanza vettore non permettono** ad un router di conoscere **l'esatta tipologia** della rete.

Routing Link State: Il secondo protocollo base usato per il routing è il **LINK STATE**. Il link state **mantiene un complesso database** delle informazioni relative **alla Tipologia**. Mentre il distance vector non specifica le informazioni sulle reti distanti e non conosce informazioni sui router distanti, **il link state, mantiene piena consocenze dei router distanti e su come essi sono interconnessi**.
Il link state utilizza **Link State Advertisements** (LSAs), un **database di topologia**, **il SPF protocol**, il risultante "albero" SPF tree e in fine, una una **tavola dei percorsi e delle porte dell'intera rete**. Gli ingegneri hanno implementato il concetto di link state **per l'OSPF routing**.

Differenza fra Distance Vector e Link State: E' possibile **comparare** il distance vector con il link state, in diverse aree chiave.

- **Distance vector** inserisce tutti **i dati di tipologia dalla tavola** di routing dei prorpi **router vicini**. Link state ottiene una **completa visione della topologia di rete** accumulando informazioni dell'LSAs **sia dai router vicini che da quelli distanti**.
- Distance Vector **determina il miglior percorso** , addizionando **i valori metrici** che riceve dalle tavole dei router. Per il link state routing, **ogni router lavora separatamente** per **calcolare il tragitto più breve** per le destinazioni.
- Con molti protocolli di **distance vector**, l'update della topologia **avviene tramite periodiche tavole di update**. Queste tavole vengono passate **da router in router**, il risultato di ciò, è una **lenta convergenza**. Con i protocolli di **link state, gli update avvengono solitamente a seguito di cambiamenti di topologia**. Gli LSAs che i router si passano sono **relativamente piccoli** per cui, **il tempo** di convergenza si **riduce notevolmente**, per ogni **cambiamento delle tipologia** di rete.

Processo di Routing IP: La scelta di IP come routed protocol, **richiede il settaggio di parametri globali**. I parametri **globali includono la selezione di un routing protocol**, che ad esempio **RIP i**

IGRP e l'assegnazione di un numero di network senza la specifica di subnets. La configurazione ip avviene **nel seguente modo**. Il comando **IP ADDRESS** stabilisce **l'indirizzo logico di rete** per una **determinata interfaccia**. E' possibile anche usare il termine **ip netmask-format** per specificare il **formato del mask** di rete per la sessione corrente. Se opzioni di formato sono BIT count, dotted decimal e hexadecimal.
La configurazione dinamica del routing invece funziona nel seguente modo: Quando si usa il **dynamic** routing, i routers inviano mesaggi **periodici di update ad ogni router**. Ogni volta che uno di questi messaggi è ricevuto ed **esso contiene nuove informazioni**, il router attua la nuova **miglior "route",** ed invia a sua volta nuovi update ad altri router. Utilizzando il comandi di configurazione router, un router **può modificare la propria condizione di rete**.Il comando **network** è necessario in quanto **permette al processo di routing di determinare quale interfaccia parteciperà all'invio ed alla ricezione delle tavole di updating**.

Configurazione RIP: Le caratteristiche chiave del rip sono:
- Esso è un **distance vector** routing protocol
- Il conteggo degli hop è utilizzato **come metric**, per la selezione del **miglior percorso**
- Il **massimo numero di hop permesso è 15**
- Gli updates sono broadcastati **ogni 30 secondi**, come default

Il comando **Router RIP** seleziona il RIP come protocollo di routing. Il comando **network** assegna indirizzi ip Base, relativi al **segmento di rete**, direttamente connesso. Il processo di routing **associa interfaccie con indirizzi propri** ed inizia il **processo di scambio** di pacchetti sulle reti specifiche. Esempio:
- Router Rip- Seleziona rip come protocollo di routing
- Nework 1.0.0.0- Specifica una rete direttamente connessa
- Network 2.0.0.0- Specifica una rete direttamente connessa

Un router cisco connesso alle reti 1.0.0.0. e 2.0.0.0 sta inviando e ricevendo pacchetti tramite gli udate rip.

Trasporto Affidabile: Per poter inviare i segmenti a livello trasporto, è necessario **garantire l'integraità dei dati**. Un metodo per far ciò, può essere il **FLOW control**. Il flow control **corregge il problema di flooding** e di **riempimento del buffer** sull'host di destinazione. Il flood (overflows) può **presentare seri problemi** poiché esso può comportare perdite di dati. Il servizio offerto dal livello **trasporto**, permette agli utenti di **richiedere un trasporto affidabile** di dati fra host e desintazione. Per ottenere un trasporto affidabile dei dati, una relazione di tipo **"connection-oriented" è stabilita fra sistemi comunicanti.** Il trasporto **"reliable"** può consistere in:
- **Segmentazioni** riguardanti applicazioni di **livelli superiori**
- **Stabilire** la connessione
- **Trasferire** i dati
- Fornire **affidabilità e windowing**
- Utilizzare tecniche di **Aknowledge**

Segmentazione Livello 4: Un motivo per usare il modello di rete stratificato è spiegato dal fatto che **diverse applicazioni** possono **condividere** lo stesso **mezzo di trasporto** e di connessione. La funzionalità di trasporto è effettuata **segmento per segmento**. Questo vuol dire che differenti applicazioni possono inviare segmenti al **"first-come, first-served".** Stessa cosa può essere intesa per la **stessa destinazione o per più destinazioni diverse** fra loro.

Tree Way HandShaking: Per stabilire una connessione, una stazione **effettua una chiamata** che deve essere **accettata da un'altra stazione**.Il modulo del protocollo, in questa situazione, deve

lavorare fra i 2 sistemi comunicanti, inviando un messaggio **attraverso la rete**, al fine di **verificare** che il **trasferimento** sia **verificato**, e tutto sia pronto da entrambi le parti. Dopo che questo processo di sincronizzazione **è avvenuto, viene stabilita una connessione**, ed il trasferimento **dei dati, inizia**. Durante questo trasferimento, **le 2 stazioni continuano a comunicare** con i propri protocolli (software) ed a verificare che i dati siano tutti ricevuti correttamente.Per far ciò, **è necessario un handshaking**. L'azione dello shaking che le 2 stazioni compiono in fase di comunicazione è **una sorta di saluto**.L'operazione **si divide in più fasi**, Distinte fra loro. **Il primo handshake è una sorta di saluto**. **Il secondo ed il terzo handshake, confermano la richiesta di sincronizzazione iniziale**.Infine c'è un **ultimo handshake che informa la destinazione, che le stazioni comunicanti vanno d'accordo e che il collegamento è stato stabilito** correttamente. **Alla fine** di questa operazione, **il trasferimento inizia regolarmente**.

La funzione del BUFFER nelle comunicazioni dati: Durante il trasferimento dei dati, **può avvenire una congestion**e. Questo per due differenti motivi. **PRIMO, L'alta velocità** di computer può generare traffico "veloce" per cui **la rete non è in grado di trasferire tutto**. **SECONDO, se molti computer, allo stesso tempo, hanno necessità di trasmettere** datagrammi ad una singola destinazione, tale destinazione, **può essere congestionata**, per cui in questo caso non è una singola sorgente a cusare il problema, bensì più di una.
Quando i datagrammi arrivano **troppo rapidamente** per essere processati, **essi sono temporaneamente allocat**i in memoria. Se il traffico continua, l'host di **destinazione può esaurire tale memoria e SCARTARE** datagrammi addizionali che arrivano. In questo caso, un indicatore agisce come "luce di stop" ed **informa l'inviatario che deve stoppare** l'invio dei dati. Quando la stazione ricevente è di nuovo in grado di ricevere dati, **essa invia un segnale, "READY",** (indicatore di trasporto), per cui la sorgente può di nuovo trasmettere resumando la trasmissione.

Sistema Windowing: Nella forma più basilare della connessione affidabile di tipo **"connection oriented"**, i pacchetti **devono essere consegnati** al recipiante **nello stesso ordine** in cui essi sono stati trasmessi. **Il trasferimento fallisce se qualche pacchetto è perso, danneggiato, duplicato o ricevuto in ordine differente**. Una soluzione è conoscere ogni pacchetto secondo il proprio "recipient".
Se l'inviatario non attende per la conferma, dopo la conferma la banda rallenta notevolmente. Poiché, dopo che l'inviatario ha finito di trasmettere e processare quelli ricevuti,avanza del tempo, questo viene usato per trasmettere altri dati. Il numero di pacchetti che l'inviatario **è abilitato a trasmettere prima di ricevere un aknowledgment**, **è chiamato anche "windo**w".
Lo windowing è **un metodo per controllare l'ammontare di informazioni trasferite END-To-END**. Molti protocolli misurano le informazioni in termini di numeri di pacchetti. **TCP\IP misura le informazioni in termini di bytes**.

Affidabilità via Aknowledgement: La garanzia di consegna è costituita **da quel metodo per cui uno stream di dati è inviato da un sistema e trasportato tramite un data link ad un altro sistema senza duplicazioni o perdite di dati**. Una acknowledgment positiva **richiede un recipiente** per comunicare con la sorgente, **inviando indietro un acknowledgment** quando esso riceve i dati.
L'inviatario **conserva una registrazione di ogni pacchetto** inviato ed **attende un acknowledgment** prima dell'invio del prossimo pacchetto. L'inviatario inoltre **fa partire un timer** quando esso invia un segmento e **retrasmette il segmento se il timer Espira** prima che l'acknowledgment sia arrivato.

Lan Switching

Fattori che incidono sulle Performance di Rete: Le lan attuali stanno diventando **sempre più congestionate e sovraccaricate**. C'è un aumento della popolazione e degli utenti che usano le reti. Molti fattori, questi, che combinati, devono **espandere le possibilità delle lan** tradizionali.

- L'ambiente di **multitastking** presente negli attuali sistemi operativi, tipo windows, permette **transazioni simultanee** di rete, ciò viene definito multitasking, questa possibilità comporta ad una **maggiore richiesta di risorse sulla rete**
- **Sistemi operativi più veloci** in combinazione con **i 3 sistemi operativi più comuni** (windows, unix, mac) sono in grado di **eseguire multitasking**, e gli utenti che li utilizzano hanno la possibibilità di **inizializzare comunicazioni** di rete simultanee. Dalla release di windows 95 in poi, gli utenti sono così in grado di **incrementare la loro domanda di risorse** di rete.
- Mentre l'uso delle applicazioni di rete si sta incrementando (world wide web ad esempio), le **applicazioni client\server permettono agli amministratori di centralizzare** le informazioni, per cui è facile mantenerle e proteggerle. Le applicazioni client\server eliminano le preoccupazioni, per cui tali applicazioni saranno sempre più utilizzate in futuro.

Elementi di Rete standard 802.3: L'architettura lan **più comune ed utilizzata e l'ethernet**. Ethernet è utilizzata per **trasportare dati fra periferiche sulla rete** come ad esempio computers, stampanti e file servers. Le periferiche, sono connesse **sullo stesso media**. Il media dell'ethernet **usa il metodo del data frame broadcast** per trasmettere e ricevere dati a tutti i nodi del media condiviso
La performance del media ethernet o ethernet 802.3 lan **può essere negativamente afflitta** da **diversi fattori**:

- Dal data frame broadcast e la natura di trasporto delle reti ethernet\802.3
- Dal metodo di accesso CSMA\CD **permette solo ad una stazione alla volta**, di trasmettere.
- Dalle applicazioni multimediali che **chiedono molta banda**, come audio\video, ed internet, accoppiate con la natura broadcast dell'ethernet, **possono creare congestioni** a livello network..
- Dalla **latenza del passaggio dei frame**, dal livelli, al livello 2\3 di rete, e la latenza dell'estensione dell'ethernet\802.3 **causata dai ripetitori**.
- Dall'estensione delle distanze delle reti ethernet\802.3 a livello 1, con l'utilizzo di ripetitori

L'ethernet che utilizza CSMA\CD ed un media condiviso, può supportare la trasmissione dati a velocità superiori ai 100Megabit. CSMA\CD è un metodo di accesso **che comunque permette ad una sola stazione di trasmettere allo stesso tempo**. L'obiettivo di ethernet è fornire il "best effort delivery service" e permettere a tutte le periferiche sul media condiviso, di trasmettere allo stesso modo. Uno dei problemi del la tecnologia CSMA\CD è la collisione.

Ethernet HALF Duplex: Ethernet è **una tecnologia HALF-Duplex**. Ogni host ethernet **verifica** la rete per vedere se i dati in quel momento vengono trasmessi, dopo di che trasmette dati addizionali. Se la rete è attualmente in uso, la trasmissione è ritardata. Malgrado la trasmissione abbia un ritardo, due o più host ethernet possono trasmettere allo stesso tempo, **con il risultato di una collisione**. **Quando avviene** una collisione, l'host che per primo rileva una collisione, **invia un segnale JAM**. Dopo aver captato il segnale jam, ogni host attenderà un periodo RANDOM di tempo prima di iniziare a ritrasmettere. La scheda di rete di ogni periferica, **fa partire un algoritmo backoff**, che genera un periodo random di tempo. Quanti più host sono aggiunto alla rete ed iniziano a troasmettere tante più probabilità ci sono ke la collisione avvenga.
Le lan ethernet possono **giungere alla saturazione** poiché utenti di rete fanno un uso intensivo di **software** a liello di client server che **causano trasmissioni per priodi più lunghi e più intensi**.

Congesione di RETE: La tecnologia avanza e vengono **prodotti computer sempre più veloci** e tecnologici. La combinazione di più computer dalle elevate prestazioni ed applicazioni dall'intensa

richiesta di risorse di rete, **è sicuramente sovrbbondante rispetto alla capacità di soli 10 Megabit** che sono quelli disponibili sull'ethernet\802.3. Le network attuali **stanno subendo lo stress di trasmissioni sovrabbondanti** come file grafici di ampie dimensioni, immagini, video in full motion, ed applicazioni multimediali, oltre all'incremento di utenti sulla stessa rete.
Tutto questi fattori **causano stress sulla ethernet** 10 mebabit.Per risolvere il problema della congestione **è richiesta più banda** e la banda attuale va usata più efficentemente. Discuteremo più avanti della soluzione al problema della congestione.

Latenza di RETE: La **latenza** spesso, chiamata anche **RITARDO**, è il tempo in cui un pacchetto o frame **compie un viaggio dalla sorgente (nodo) alla destinazione finale** sulla rete. E' importante **quantificare la latenza** locale del percorso fra la sorgente e la destinazione, per le lan e le wan. In casi specifici, di ethernet lan, **comprendere la latenza** ed i propri effetti sul tempo di rete, è di importanza cruciale al fine di determinare se il sistema CSMA\CD per la rilevazione delle collisioni funziona perfettamente. La latenza può essere **determinata** almeno da **tre fattori fondamentali**:
Il PRIMO, c'è **il tempo che impiega la sorgente NIC a posizionare gli elementi elettrici** (voltaggio) sul cavo (livello fisico) ed il tempo impiegato dalla NIC ricevente a ricevere questi segnali elettrici ed interpretarli. Questo fenomeno è solitamente chiamato DELAY (E' solitamente 1 microsecondo su una scheda di rete 10base-t).
Il SECONDO, c'è **il ritardo di propagazione** per cui il segnale impiega tempo a viaggiare sul cavo (556 microsecondi per 100 metri su categoria 5 utp). Più il cavo è lungo più il ritardo di propagazione aumenta. Quanto più lenta è la velocità di propagazione, tanto più ritardo c'è nella trasmissione dei dati.
Il TERZO, la latenza è accordata quando periferiche di rete sono aggiunte nel percorso fra 2 computer comunicanti. La periferica può essere di livello1,2 o 3. Da come le periferiche sono configurate può derivare la latenza. Il tempo attuale di trasmissione, può anche includere il tempo di acquisizione dei dati sulla rete.
La latenza non **dipende solo dalla distanza e dal numero di pc sulla rete**. Per esempio, se abbiamo 2 separate workstation su un unico nodo di rete, una delle 2 può avere "latenza" poiché il router che le separa non è configurato correttamente.
Questo avviene poiché generalmente i router effettuani decisioni più complesse ed in più tempo. (funzionamento livello 3 e livello 2)

Tempo di Trasmissione Ethernet 10Base-T: Tutte le reti sono **costituite dal "bit time" o "slot time"**. **Molte tecnologie** lan come Ethernet **definiscono il bit time** come l'unità base di tempo in cui un bit può essere inviato. Per far **riconoscere** alle periferica la comunicazione binaria **1 o 0, ci dev'essere una tempo minimo in cui il bit è On o OFF**.
Il **tempo di trasmissione eguaglia il tempo relativo numero di bit inviati per una determinata tecnologia**.Un altro modo di intendere il tempo di trasmissione è prendere in analisi un frame attualmente trasmesso (**piccoli frame impiegano poco tempo, grandi frame impiegano molto tempo**, per essere trasmessi).
Ogni ethernet da 10 megabit **ha 100 nanosecondi per window,** per trasmettere. Un byte eguaglia 8 bits. Un byte impiega un minimo di 800 nanosecondo per trasmettere.
Un frame di 64Byte, il più piccolo permesso nello standard 10base-t, affinchè il csma\cd lavori propriamente, impiega 51,200nanosecondi o 51.2 microsecondi per trasmettere (64bytes a 800ns per byte, equivalgono a 200,51ns e 51,200 ns divisi per 1000, equivalgono a 51,2 microsecondi). Il tempo di trasmissioni di un frame di 1000byte dalla sorgente richiede 800microsecondi, impiegati per completare lo stesso frame. **Il tempo in cui il frame, attualmente, arriva alla stazione di destinazione dipende dalla latenza** addizionale introdotta dalla rete. Questa latenza è dovuta al **ritardo della scheda di rete, al ritardo dovuto alla propagazione, al ritardo delle periferiche di 1,2,3 livello**.

Il beneficio dell'uso dei Ripetitori: La **distanza** che può essere **coperta in una lan** è **limitata all'attenuazione**. L'attenuazione consiste **nell'indebolimento del segnale** (che è attenuato), per cui esso **ha difficoltà a viaggiare** sulla rete. La **resistenza**, nel cavo, o media, **causa attenuazione**. Un ripetitore ethernet è **una periferica fisica posto sulla lan che velocizza o rigenera il segnale** sulla stessa LAN. Quando si usa un ripetitore ethernet, per **estendere la distanza** sulla lan, una singola rete può coprire una grande distanza e molti utenti possono condividere lo stesso media. Comunque usando un ripetitore, **conosciuto come HUB**, si **compromette la gestione del broadcast e si ha una più frequente collisione**, ciò ha effetti negativi sulla performance della rete.

Ethernet FULL DUPLEX: Le ethernet **full duplex permettono la trasmissione di pacchetti e la ricezione di altri pacchetti allo stesso tempo**.Questa trasmissione simultanea e ricezione, necessita dell'uso di due "wires pairs" nel cavo e **di una connessione "switched**" fra ogni nodo. Questa connessione è considerata **point to point** ed è **libera da collisioni**; Poiché entrambi i nodi possono trasmettere e ricevere allo stesso tempo, **non c'è negoziazione di banda**. Full duplex ethernet può utilizzare un media esistente lungo il media incontrando minimi standard ethernet.
Per trasmettere e ricevere allo stesso tempo, **è necessaria una porta dedicata per ogni nodo**. Le connessioni full duplex possono usare i media 10base-T,100Base-TX o 100Base-FX per creare connessioni punto punto. La scheda di rete di entrambi gli host end, **devono essere full duplex**. L'ethernet full duplex permette di usufruire del vantaggio dei "two wires" all'interno del cavo. Questo può essere fatto anche creando una connessione diretta dalla trasmittente (TX) alla "end to end", del circuito, e dalla ricezione (RX), sempre alla "end to end". Con queste 2 stazioni connesse a questo modo, abbiamo creato un esempio di "collision free domain", poiché la trasmissione e la ricezione avvengono in circuiti separati.
L'ethernet **solitamente può solo usare il 50-60 percento della banda** (10megabit) disponibile, poiché le collisioni e la latenza impediscono di utilizzare il restante 40percento. **L'ethernet full duplex offre il 100%** di banda in entrambi le direzioni. Questo produce un potenziale di 20Megabit di portata, 10Megabit TX e 10Megabit RX.

Segmentazione di LAN: Una rete può essere spostata in **una piccola unità chiamata SEGMENTO**. Ogni segmento usa il **metodo di accesso csma\cd** e mantiene il traffico fra utenti e segmenti.
Dividendo la rete in segmenti separati **un amministratore può diminuire la congestione** di ogni segmento. Trasmettendo dati con un segmento, **le periferice di ogni segmento**, stanno **condividendo** i 10 megabit di banda per segmento. In una ethernet lan segmentata, i dati passano fra segmenti che trasmettono su un backbone usando un router, un bridge o uno switch.

Segmentazione LAN con BRIDGES: Le lan che utilizzano un bridge per segmentare una rete, **forniscono molto banda per utente** poiché ci **sono pochi utenti per ogni segmento**. In contrasto a ciò, le lan che non **utilizzano i bridge per la segmentazione** forniscono meno banda per utente poiché ci sono molti più utenti in un punto non segmentato (intera lan).
I bridges **possono "acquisire**" le informazioni **relative alla segmentazione costruendo tavole di indirizzi** che contengono gli indirizzi di ogni periferica sulla rete e sanno che segmento dovrà usare per raggiungere altre periferiche. I bridge sono di livello 2 **e forwardano i frames** in base al **Media Access Control (MAC)**. In aggiunta c'è da dire che i bridge sono trasparenti nei confronti di altre periferiche sulla rete.
I bridge **aumentano** la latenza in una rete del 10\30 percenti. Questa latenza è causata dal tempo necesssario per la decisione del bridge e per la trasmissione dei dati. Un bridge è considerato **una periferica "store and forward"**. Esso deve calcolare **il "cycle redundancy check (CRC)** nel campo CRC del frame e comprare il frame con l'attuale dimensione risultante **prima del forward** dello stesso. **Se la porta di destinazione è occupata, il bridge può temporaneamente**

memorizzare il frame, finchè la porta non è disponibile. Il tempo che è impiegato per eseguire queste operazioni rallenta la trasmissione causando un incremento della latenza.

Il Pros e Cons della Segmentazione LAN con Routers: I router sono molto più avanzati dei classici bridge. Un bridge opera al livello Data Link. Il router opera **al livello network** e basa le tutte le proprie **decisioni sul forwarding fra segmenti sulla rete, sui protocolli di livello3**. Router crea un **alto livello di segmentazione**, forwardando i dati agli hub, ai quali le workstation sono connesse. Un router esegue le decisioni di **forwarding dei segmenti**, esaminando l'indirizzo di destinazione sul pacchetto e analizzando la prorpia **routing table** per istruzioni di forwarding. Un router deve **esaminare un pacchetto** per determinare il miglior percorso per il forwarding di tali pacchetti a destinazione.
Questo complesso processo **richiede TEMPO**. I protocolli che **richiedono una conferma** fra ricevente e trasmittente per ogni pacchetto inviato (conosciuto come aknowledgment oriented protocol), **causano il 30\40% di perdita** di banda. I protocolli che **richiedono un aknownledge** minimo (sliding window protocols) **causano un 20\30% di perdita della portata** sul media. Questo è causato dal fatto che c'è meno traffico fra l'inviatario ed il ricevente. Il restante è impiegato per l'acknowledgment.

Pros e Cons della Segmentazione LAN con Switches: Lo switching nella lan **aumenta la banda e riduce l'ingorgo** di rete, ciò può accadere a dverse pc come ad un server remoto. Uno switch **può segmentare la lan in microsegmenti**, considerati anche singoli "host segments". Questo **crea un tratto libero da collisioni**. Allo stesso modo il lan switching **elimina il dimini di collesione, tutti gli host connessi allo switch sono compresi nello stesso dominio di broadcast**. Dunque tutti i nodi connessi tramite lo switch, possono ricevere un broadcast diretto allo stesso nodo.
Switched Ethernet è basato su Ethernet. Ogni nodo è direttamente connesso ad una delle porte o segmenti i quali sono poi connessi allo switch. Ciò crea una connessione a 10 megabit di banda fra ogni nodo di ogni segmento dello switch. Un computer connesso direttamente allo switch ethernet è integrato nel collision domain ed accede alla banda piena di 10 megabit.
Una rete che usa la topologia switched ethernet, crea una rete che comporta, una portata paragonabile a quella di solo 2 nodi collegati l'un con l'altro. Questi due nodi condividono la banda di 10 megabit fra loro il che vuol dire che spesso la banda totale è disponibile per la trasmissione dei dati.Una lan switched usa la banda efficentemente, dunque essa fornisce più portata di una lan creata da bridges o hubs. Nell'implementazione dell'ethernet switched, **la banda disponibile può raggiungere circa il 100%**. Lo switching ethernet **aumenta la banda disponibile sulla rete creando un segmento di rete dedicato** (connessione point to point) e connettendo questi segmenti in una rete virtuale all''nterno dello switch. **Il "virtual network circuit" esiste solo quando i due nodi hanno necessità di comunicare.** Per questo si chiama "virtual"; Dunque esiste solo quando le stazioni hanno necessità di comunicare con lo switch ed una connessione con esso, è stabilita.
Un punto negativo degli switch. Essi costano di più degli hub; Comunque molte società sostituiscono gli switch agli hub un po' per volta, senza avere dei costi eccessivi.

Due operazioni base in uno Switch: La switching è una tecnologia che **diminuisce la congestione delle reti ethernet**, token ring e FDDI riducendo il traffico ed **incrementando la banda**. Gli switched di rete sono spesso usate per sostituire gli hubs condivisi. Essi sono designati per lavorare con infrastrutture di ampia capacità che esistono giù; Per cui è possibile installare questi apparecchi senza distruggere il traffico di rete esistente.
Attualmente nelle comunicazioni dati, tutto l'equipaggiamento di switching, esegue due operazioni basilari:

- **Switching Data Frames**, Questo accanto quando **un frame arriva** su un media(ingresso) **e viene ritrasmesso** su un altro media (uscita)
- **Mantenere le operazioni di Switching**, uno switch **costruisce e mantiene** tavole di routing,

Il termine **Bridging** si riferisce ad una tecnologia in cui una periferica, **conosciuta come bridge**, **connette due o più segmenti di rete**. Un bridge **trasmette datagrammi da un segmento ad altre destinazioni su altri segmenti**. Quando un bridge è acceso, ed inizia ad operare, esso **esamina l'indirizzo mac del datagramma che sta arrivando e costruisce una tavola** delle destinazioni conosciute. Se il bridge sa che la destinazioen del datagramma **è sullo stesso segmento** della sorgente, esso **lo scarta il datagramma** poiché non c'è bisogno di trasmetterlo. Se il bridge sa che la destinazione **è su un altro segmento**, **esso lo trasmette solo su quel determinato segmento**. **Se il bridge non conosce il segmento di destinazione, esso trasmette il datagramma su tutti i segmenti ad eccezione del segmento di sorgente** (questa tecnica è chiamata Flooding). Il beneficio primario del bridgin è che esso **limita il traffico su un certo segmento** di rete.Sia il bridge che lo switch connettono segmenti di rete, usano una **tabella di indirizzi mac** per determinare il segmento su cui un datagramma ha la necessità di trasmettere e riducono il traffico.
Gli switch sono **più funzionali dei bridge** poiché essi operano ad **una velocità molto più alta** e possono **supportare nuove funzioanlità** come ad esempio le **VLANS**. **I bridges** tipicamente eseguono **l'operazione di switching usando il software**. Gli **switches tipicamente eseguono lo switching usando l'hardware.**

Latenza di uno Switch Ethernet: Ogni switch usato sulla lan a 10 megabit, **contribuisce ad aumentare la latenza sulla rete**. Comunque la latenza dipende da **tipo** di switch e dal tipo di **tecnica** di switching utilizzata. Le **diverse modalità** di switching (store-and-forward, fragment-free, fast-forward) si **differenziano** quando la decisione di switching nei confronti di un frame in ingresso, è stata effettuato. La latenza dovuta al **tempo di "making decision"** si va a sommare al **tempo in cui in frame entra ed esce dalla porta** dello switch e determina la latenza totale dello switch.
Notare che un hub, che ha semplicemente lo scopo di **forwardare i frame**, senza filtraggio e senza prendere decisioni, **ha solo la latenza** relativa al port-to-port. Tutte queste frazioni di secondo non sembrano molto importanti, ma è necessario considerare anche le velocità di trasmissione. Per 10 megabit abbiamo 1 bit ogni 1 milioni di secondi, per 100 megabit, abbiamo 1 bit per ogni 100 milioni di secondi, per un gigabit abbiamo 1 bit ogni bilione di secondi. Le periferiche di rete attuali stanno operando ad un velocità incredibilmente alto per cui ogni nanosecondo può essere materialmente considerabile.

Switching di Livello2 e Livello3: Ci sono 2 metodi per lo switching di frames. C'è **lo switching a livello 2 e quello a livello 3**. Lo switching è un processo di **prendere un frame in arrivo da una interfaccia e di trasportarlo verso un'altra**. I routers utilizzano lo **switching di livello 3** per fare il routing dei pacchetti. Gli switch utilizzano il **livello 2 di switching** per forwardare i frames. La differenza fra lo switching livello 2 e quello di livello 3, **è il tipo di informazione** all'interno del frame è che usata per **determinare la corretta interfaccia di output**. Con lo switching a **livello2**, i frames sono switchati **in base al mac address**. Con lo switching a livello 3, i frames sono switchati **in base alle informazioni di livello network**.
Lo switching di livello 2, **non guarda** dentro al pacchetto **cercando l'indirizzo di rete**, che appartiene ad uno switching di livello 3. Lo switching di livello 2, **trova** la destinazione verificandola **all'interno del frame** e considerando **l'indirizzo mac**. Esso invia l'informazione **all'interfaccia appropriata** se la conosce l'indirizzo della destinazione. Lo switching di livello 2 **costruisce e mantiene tavole di switching** che tengono traccia degli indirizzi mac che appartengono ogni porta o interfaccia. Nel livello 2, lo switch **non sa dove invierà il frame**, esso **fa il broadcast del frame in tutte le direzioni, da tutte le porte, sulla rete, per acquisire informazioni** relative alla corretta destinzione. **Quando la risposta del frame torna indietro, lo switchi, apprende** la locazione del nuovo indirizzo ed **aggiunge questa informazione alle tabelle** di switching. Il costruttore dell'hardware determina il livello 2 di indirizzo. **Sono indirizzi unici divisi in 2 parti. La prima.."manufacturing" MFG, ed l'indentificatore unico "unique**

identifier". L'istituto degli ingegneri elettrici ed elettronici "electrical and electronic engineers **(IEEE) assegna il codice MFG** ad ogni venditore. **Il venditore assegna l'identificativo unico**. Gli utenti hanno **poco o nessun controllo** sul livello e (eccetto in system network architetture, SNA), poiché **l'indirizzamento di livello 2, è fissato con una periferica**. Al contrario gli indirizzi **di livello 3 possono essere cambiati**. In aggiunta, gli indirizzi di livello 2 assumono spazio di "flat address" definiti universalmente "indirizzi unici". Il livello 3 di switching opera al livello di rete, esso esamina le informazioni contenute nei pacchetti e lo forwarda in base al loro indirizzo di rete di terzo livello. Lo switching di livello **3 può supportare anche la funzionalità dei routers**. La maggior parte degli amministrator di rete determinano gli indirizzi di livelli 3. Protocolli come IP,IPX, e APPLETALK, **utilizzano l'indirizzamento di livello 3**. Creando indirizzamenti di livello 3, un amministratore **crea aree locali** che funguno da **singole unità di indirizzi** (analogamente a strade, città, stati e contee) ed **assegnano un numero** ad ogni entità localie. Se gli utenti si spostano su un altro edificio, le loro macchine ottengono un nuovo indirizzo di livello 3, ma i loro indirizzi di livello 2 restano gli stessi. Poiché i routers operano a livello 3 del modello osi, essi sono adiacenti e **creano una struttura (hierarchical) gerarchica di indirizzi**.
perciò una rete di instradamento può legare una struttura **di indirizzi logici ad una infrastruttura fisica**. Per esempio tramite le tcp\ip subnets o le reti IPX per ogni segmento. Il flusso del traffico in una switched network (flat), si diversifica molto rispetto al traffico che può esserci in una routed network.
Le reti hierarchiche, **offrono più flessibilità** nel controllo del traffico rispetto alle flat networks, poiché esse possono usare la rete per determinare il percorso ottimale e contenere i broadcast domains.

MicroSegmentation: La potenza incrementale dei processori desktop ed i requisiti del client server e delle applicazioni multimediali, hanno creato un incremento della **necessità di banda** in media tradizionali e condivisi. Questi requisiti hanno spinto i designers di rete **a sostituire gli hubs** contenuto nelle wirin closet, **con degli switch**.
Lo switching di livello2, utilizza la micro segmentazione per soddisfare la domande di più banda ed incrementa le **performance** ma i designersi di rete sono adesso concentrati all'incremento della domanda per comunicazione di intersubnet. Per esempio, ogni volta che un utente accede ad un server o ad altre risorse che sono situate su differenti subnet, il traffico deve passare attraverso una periferica di livello. Potenzialmente in tale situazione esiste un grave ostacolo che può minacciare la performance di rete. Per cercare di risolvere questo problema, gli amministratori di rete possono aggiungere delle possibilità alla rete per cui vengono **alleviati i carichi eccessivi suoi routers**. Perciò **uno switch migliora la gestione della banda separando domini di collisione e, selettivamente forwardando il traffico verso l'appropriato segmento sulla rete.**

Come uno Switch apprende Indirizzi: Uno switch ethernet può **apprendere l'indirizzo di ogni periferica sulla rete** leggendo l'indirizzo sorgente di ogni pacchetto trasmesso e non la porta dove il frame è entrato nello switch. Lo switch quindi **aggiunge questa informazioni al proprio database** di forwarding. Gli indirizzi sono **appresi dinamicamente**. Questo vuol dire che nuovi indirizzi sono letti, essi sono **acquisiti e memorizzati nel Content Addressable Memory (CAM).** Quando una pacchetto sorgente è letto e si è verificato che **non è presente in CAM, esso è Acquisito** e memorizzato per utilizzo futuro.
Ogni volta che un indirizzo è memorizzato, esso è stampato, questo permette agli indirizzi di esser memorizzati per un periodo di tempo determinati, ogni volta che un indirizzo è referentemente trovato nella cam, esso **riceve un nuovo "time stamp".** Gli indirizzi per cui **non è trovata referenza durante un determinato periodo di tempo, sono rimossi dalla lista**. Rimuovendo questi indirizzi, **la cam mantiene sempre un accurato e funzionale database di forwarding**.

Vantaggi del Lan Switching: Lo switching **porta molti benefici**. Uno switch è in grado di **permettere a molti utenti di comunicare** in parallelo attraverso **l'uso di circuiti virtuali e segmenti** di rete dedicati, **collision free**. Quando massimizza la banda possibile sul media condiviso, inoltre trasformare **la prorpia vecchia rete in una switching lan** non è molto costoso in quanto è possibile riutilizzare l'hardware ed il cablaggio esistente. Infine, la potenza dello switch, combinata con il software di configurazione della lan, **offre all'amministratore grande flessibilità nella gestione del network**.

Switching Simmetrico e Asimmetrico: o switching simmetrico è un modo di caratterizzare uno lan switch...facendo in modo di **accordare la banda allocata ad ogni porta sullo switch**. Un **Symmetric Switch fornisce connessioni "switched" fra porte, con la stessa banda,** ad esempio 10 megabit per porta o 100 megabit per porta. In una **lan Asymmetrica, lo switch fornisce connessioni "switched" fra porte di diversa banda come ad esempio 10 megabit e 100 megabit**. Lo switching **asimmetrico esegue il controllo del traffico a livello client\server** dove molti client stanno comunicando con un server allo stesso tempo richiedendo molta banda dedicata alle porte dello switch a cui il server è connesso in modo da prevenire un disagio su quella determinata porta. Il memory **buffering in uno switch asimmetrico è necessario per controllare il flusso** del traffico, **da 100 megabit si può passare a 10 megabit** senza causare congestione sulla porta più lenta a 10 megabit.

Buffering di Memoria: Uno switch ethernet **può usare una tecnica di buffering** per memorizzare e forwardare pacchetti **sulla corretta porta**. Il buffering **può essere usato quando la porta di destinazione è occupata**. L'area di memoria dove lo switch memorizza i dati è chiamata **"memory buffer"**. Il buffer può usare **due metodi per forwardare i pacchetti**. **Port** based memory e **shared** memory.
Nel Port base memory, i pacchetti sono **memorizzati in delle queues** che sono linkate **con specifiche porte**. Il pacchetto **è trasmesso** in uscita solo quando **tutti i paccheti a capo di esso nella queue sono stati trasmessi**. E' possibile per un singolo pacchetto, **ritardare la trasmissione** di tutti I pacchetti in memoria a causa della porta di destinazione che, in tal caso, può essere occupata. Questo ritardo avviene **anche se gli altri pacchetti possono essere trasmessi a porte aperte**.
Nello shared memory buffering si deposita tutti i pacchetti **in una memoria buffer condivisa da tutte le porte** dello switch. L'ammontare di memoria allocata per una porta è determinata da quanto è richiesto per ogni porta. Questo è chiamato **Dynamic Alocation of Buffer Memory**.
I pacchetti nel buffer sono quindi **linkati dinamicamente alla porta di trasmissione**. Il pacchetto è linkato all'allocazione di memoria della porta di trasmissione. Questo permette al pacchetto di **essere ricevuto su una porta e trasmesso su un'altra porta**, **senza metterlo in queue**.
Questo switch **mantiene una mappa delle porte per switchare** un pacchetto che necessita di essere trasmesso. Lo switch **Cancella questa mappa** delle porte di destinazione **solo dopo che il pacchetto è stato trasmesso** con successo.
Poichè il buffer di memoria è condiviso**, il pacchetto è ristretto dalla dimensione dell'intero buffer** di memoria, non solo dall'allocazione di una porta.
Questo vuol dire che pacchetti di grandi dimensioni possono essere trasmessi con meno scarti. Questo è importante per il 10\100 switching dove una porta a 100 megabit può forwardare un pacchetto ad una porta a 10 megabit.

Due metodi di Switching: Possono essere utilizzate 2 modalità di switching per forwardare un frame attraverso uno switch.

- Store and Forward – L'intero frame **è ricevuto prima che venga presa la decisione del forwarding**. La destinazione o\e l'indirizzo sorgente sono **lette, filtrate ed applicate**, prima che il frame venga forwardato La latenza sussiste durante il tempo di ricezione. La latenza è

maggiore con frame più grandi poiché l'intero frame impiega più tempo per esser letto. La rilevazione di errori è alta a causa del tempo a disposizione dello switch per controllare se ci sono errori nell'attesa dell'itera struttura del frame da ricevere.

- Cut Throught – Lo switch **legge l'indirizzo di destinazine prima di ricevere l'intero frame. Il frame è quindi forwardato prima che possa arrivare per intero**. In questo modo si diminuisce la latenza della trasmissione e si riducono gli errori di switching. Il fast-forward ed il fragment-free sono **2 forme di cut-trought switching**.

- Fast Forward Switching. Questo metodo di switching offre il più **basso livello di latenza forwardando immediatamente** un pacchetto dopo aver ricevuto i dati relativi alla sua **destinazione**. Poiché il fast switching **non controlla** gli errori, può succedere che qualche frames venga rilasciato **con errori**. Ciò avviene non frequentemente e la periferica della rete di destinazione, **scarta i frame con errori** dopo che essi sono arrivati.**Nelle reti, alti tassi di collisione, pssono avere negativi effetti sulla banda**. Utilizzare l'opzione fragment free per ridurre il numero di collisioni e di frame forwardati con errori. Nella modalità fast-forwarding la latenza è misurata dal primo bit ricevuto al primo bit trasmesso, First IN, First Out (FIFO).
- Fragment-Free Switching. Filtra le collisioni che sono la costituite, in gran parte da **pacchetti con errori**. Questo **filtraggio avviene prima del forwarding**. Secondo la propria funzionalità di rete, i frammenti di collisioni devono essere **più piccoli di 64 bytes**, ogni **frammento più grande** di 64 bytes, è considerato **un pacchetto valido ed è ricevuto senza errori**.Il fragment free switching **attende la riceziomne completa del pacchetto** (privo di collisioni), **dopo** di che, procede con il **forward**. Nel fragment free, **la latenza è misurata in FIFO**.

La **latenza** relativa ad ogni modalità di switching dipende **da come lo switch forwarda** i frame.Quanto più **rapida è la modalità di switching**, tanto più **scarsa è la latenza**. Compiendo un **rapido forwarding**, lo switch impiega **meno tempo per controllare** gli errori. C'è però da dire che che in questo caso c'è uno scarso checking degli errori, per cui ciò comporta la necessità di **aumentare il numero delle ritrasmissioni**, a causa di errori.

Come settare le VLANS: Uno switch ethernet fisicamente **segmenta una lan in un dominio di collisione individuale**. Dunque, **ogni segmento è parte di un dominio di broadcast**. Il numero totale di segmenti relativi ad uno switch, equivale al numero di broadcast domains. Questo vuol dire che tutti i nodi di **tutti i segmenti possono vedere un broadcast** da un nodo ad un segmento. **Una Vlan è un gruppo logico di servizi di rete, o utenti, che non sono ristretti\limitati ad un segmento fisico costituito da uno switch**. Le periferiche o utenti in una VLAN possono essere raggruppati per **funzione, divisione, applicazione**, e tutto ciò che riguarda, o meno la locazione fisica del loro segmento. Il setup delle **VLAN è eseguito sullo switch** via software. Le VLANS sono **standardizzate** secondo gli accordi con IEEE 802.1Q, ma la loro implementazione varia, a seconda del produttore\venditore.

Lo Spanning Tree Protocol: La funzione principale del protocollo Spanning-Tree è permettere di **duplicare percorsi relativi a switch\bridge senza incorrere in effetto di latenza e\o loops sulla rete**. I bridges e gli switches **effettuano decisione di forwarding**, su frame basati su Unicast in base all'indirizzo mac di destinazione del frame. Se il mac è sconosciuto, la periferica fa un FLOOD da tutte le sue porte al fine di raggiungere la destinazione desiderata. Questo fenomeno è un sorta di Broadcast Frame.
L'algoritmo di spanning-tree, implementato dal protocollo spanning-tree, previene loop, valutando una stabile tipologia chiamata **"spanning-tree network topology"**.
Quando vengono create reti di tipo fault-tolerant,è necessario che un percorso privo di loop, debba esistere fra tutti i nodi della rete. **L'algoritmo Spanning-treee è usato per calcolare i percorsi "free-loop"**. **I frames spanning-tree, chiamati "protocol bridge data unit" (BPDUs), sono inviati e ricevuti da tutti gli switch sulla rete ad intervalli regolari e sono usato per**

determinare la tipologia spanning-tree. Uno switch usa il **protocollo spanning-tree su tutte le ethernet** e le fast ethernet **basate sulle VLANs**. Il protocollo Spanning-tree **rileva e ferma i loops**, posizionando diverse connessioni in **modalità standBy**, che sono attivate da **eventi attivi di connessioni fallimentari**. Un'istanza separata del protocollo spanning-tree **gira con ogni VLAN** configurata, garantendo una portata standard sulla topologia ethernet.

I 5 Stati di Spanning Tree Protocols: Gli stati del protocollo spanning-tree sono i seguenti:

- Blocking-No frames forwarded, BPDUs heard
- Listening-No frames forwarded, listening for frames
- Learning-No frames forwarded, learning addresses
- Forwarding-Frames forwarded, learning addresses
- Disabled-No frames forwarded, no BPDUs heard

Lo sotto di ogni VLAN è inizialmente settato per quanto riguarda la configurazione e più tardi modificato **sotto l'aspetto del processo relavito allo spanning-tree protocol**. E' possibile determinare lo stato, il costo, e la priorità delle porte e delle VLANs usando il comando **show spantree**. Dopo che lo stato delle porte e delle VLAN è settato, lo spanning-tree protocol, determina **quando la porta forwarda o blocca il frame**. Le porte **possono essere configurate** immediatamente entrando nella **spanning-tree protocol forwarding mode**, quando la connessione è effettuata. Inteso come sequenza di bloccaggio, acquisizione e quindi forwarding.
La possibilità di passare rapidamente dallo stato di bloccaggio a quello di forwarding, che va ad agire sullo stato delle porte di transizione, è utile in situazioni dove l'accesso immediato ad un server è indispensabile.

VLANS

Configurazioni esistenti di Lan condivise: Una vlan è **un gruppo logico di periferiche** o utenti che possono essere **raggruppati per funzione, divisione o applicazione**, riguardo o meno la loro locazione sul segmento fisico. La Configurazione delle Vlan si effettua **via software** all'interno dello switch. Le Vlan **non sono standardizzate** e necessitano dell'uso di software proprietario che viene fornito dal venditore dello switch.
Una lan tipica è configurata **accordando l'infrastruttura fisica** alla quale si sta connettendo. Gli utenti sono **raggruppati** in base alla loro locazione in relazione all'hub su cui sono pluggati e per come il cavo è fatto passare per poi arrivare alla wiring closet. Il router **interconnette ogni hub** condiviso, tipicamente fornisce segmentazione e può attivare **un firewall per il broadcast**. I **segmenti creati dagli switch**, non sono segmentazioni tradizionali di lan che non raggruppano utenti, accordandosi con il loro workgroup, associato alla banda. Essi **condividono lo stesso segmento e si contendono la stessa banda** benchè i bisogni possano variare molto a seconda del WorkGroup o Divisione.

Gruppi di utenti, separati, in topologie Virtuali: Le lans sono divise **secondo una struttura crescente** in Gruppi di lavoro i quali sono **connessi tramite backbone** per poi formare delle Vlans. Le Vlans **segmentano logicamente** le infrastrtutture fisiche della lan, in **differenti subnets**. (o domini broadcast, nel caso dell'ethernet). I frames **broadcast** sono switchati sono fra **porte che apaprtengono alla stessa Vlan**.
L'implementazione iniziale delle Vlan offre **la capacità di mappare le porte** che stabiisce un dominio broadcast fra un grupo default di periferiche. I bisogni correnti richiedono spesso alle Vlan la copertura dell'intera rete. Questo approccio con Vlans permette di **raggruppare geograficamente** utenti separati in large tipologie virtuali di rete. Gruppi di configurazione VLAN.

La configurazione Vlan raggruppa utenti **tramite associazione logica** piuttosto che per associazione fisica. La maggior parte delle reti installate fornisce una segmentazione logica molto limitata. Gli utenti sono comunemente raggruppati **in base a connessioni ad hub** condivisi e router fra gli hubs. Questa tipologia fornisce segmentazione **solo fra hubs che sono tipicamente situati su piani separati** e non fra utenti connessi allo stesso hub. Per cui il merito è dei router. Questo impone costrizioni fisiche sulla rete e limiti per quanto riguarda il raggruppamento di utenti. Alcune architetture di hub\condivisi, hanno **possibilità di raggruppamento** ma essi sono ristretti per quanto riguarda la configurazione logica per definire gli workgroup.

Differenze fra "switched" tradizionali Lan e Vlans: In una lan che utilizza le periferiche di switching, la tecnologia Vlan è **un modo efficiente di raggruppare gli utenti di reti in gruppi virtuali**, riguardo o meno la loro posizione fisica sulla rete. Molte delle differenze fra lan e Vlan sono le seguenti:

- Le vlans **lavorano al livello 2 ed al livello 3** del modello osi
- La **comunicazione** fra vlans è fornita dal **routing di livello 3**
- Le vlans forniscono un **metodo di controllo dei broadcast** di rete
- L'amministratore di rete **assegna utenti ad una Vlan**
- Le Vlans possono **incrementare la sicurezza di rete**, definendo quale nodo di rete può comunicare con altri\o.

Utilizzando la tecnologia Vlan è possibile **raggruppare porte di switch e utenti** connessi ad esso in **gruppo logici definiti**, come ad esempio:

- Co-Operatori della stessa divisione
- Squadra di produzione
- Diversi gruppi di utenti che condividono la stessa applicazione di rete

E' possibile raggruppare queste porte ed utenti in **gruppi su uno switch** singolo su switch connessi. Raggruppando **le porte e gli utenti assieme su switch multipli**, le Vlans possono spannare una singola struttura, strutture interconnesse, o WANS, utilizzando bridges per collegare 2 segmenti della stessa Vlan.

Il trasporto Vlans sui Backbone: E' importante, in ogni architettura VLAN **abilitare il trasporto delle informazioni VLAN fra switch interconnessi e router** che risiedono sul backbone. Le specifiche di trasporto sono le seguenti:

- **Rimuovere i confini fisici** fra utenti
- Incrementare la **flessibilità di configurazione** della soluzione Vlan, **quando gli utenti si spostano**
- Fornire meccanismi per **interoperabilità fra componenti di sistemi su backbone**

La backbone comunemente ha la **funzione di punti di raccolta** per volumi di traffico elevati. Essa trasprta le **informazioni relative alle Vlan**, agli utenti ed indentificazioni fra switch, routers, e servers direttamente connessi. All'interno della backbone sono sclti link **dotati di ampia banda** ed alta capacità per il trasporto genrale del traffico per l'intera Rete.

Il ruolo dei Routers nelle Vlans: Il rouolo tradizionale del router nelle Vlans è **fornire protezione**, gestione del management e **gestione del ruoting** e distribuzione. Mentre le Vlan Switched possono eseguire solo alcuni di questi tasks, i routers rimangono **Vitali nell'architettura delle lan\vlan** poiché essi permettono l'interconnessione, nel casono delle Vlan, **permettono a più Vlans di dialogare**. Essi si connettono anche **ad altre parti sulla rete** che sono a loro volta segmentate logicamente con le tradizionali Subnet e richiedono accesso a siti remoti tramite links wan. Le comunicazioni di **livello 3**, che a loro volta sono commutate nello switch o fornite esternamente sono **parte integrante di ogni architettura switch** di alto performance. E' possibile effettivamente

integrare **routers esterni in architetture di switching** utilizzando una o più connessione backbone ad alta velocità. Queste connessioni sono tipicamente FAST ETHERNET o ATM e forniscono i seguenti vantaggi: 1) Incrementare la portata fra switch e routers,
2) consolidare complitamente il numero di porte fisiche del router, necessarie per la comunicazione fra vlans ed architetture, non solo fornite da segmentazione logica, ma con accurata pianificazione esse possono aumentare l'efficienza della rete.

Come i Frames sono usati nelle Vlans: Gli **switches** sono uno dei **componenti chiave** nelle comunicazioni Vlans. Ogni switch **ha una propria intelligenza** che gli permette di **effettuare filtraggio, decisioni di forwarding**, basandosi sulle metrics delle Vlans definite dal manager di rete. Lo switch può anche **comunicare le proprie informazioni ad altri switch o router**, all'interno della rete. L'approccio più comune per il raggruppamento logico di utenti in Vlans distinte è il **frame filtering** e **frame identification** (frame tagging).
Entrambi queste tecniche analizzano il frame quando esso è stato ricevuto o lo forwardano tramite gli switch. Basandosi su un set di regole definite dall'amministratore, queste tecniche determinano **dove il frame dovrà essere inviato**, filtrato o broadcastato. Questi meccanismi di controllo possono essere **amministrati centralmente** (con software di gestione rete) e con essi è facilmente possibile **implementare la portata della rete**. Il **filtraggio** del frame esamina informazioni particolari su ogni frame. Una **tavola di filtraggio** è costruita per ogni switch. Questo fornisce un alto **livello di controllo** amministrativo poiché esso esamina molti attributi dello stesso frame. Il tipo di lan switch usato,determina se gli utenti possono essere raggruppati in base al MAC od al protocollo ed al tipo di macchina.
Lo switch analizza i frame che filtra**, li paragona con le entries nella propria tavola** ed esegue le azioni appropriate basandosi sulle stesse entries.
*Prima, la VLAN **erano Filter-based** e gli utenti raggruppati **basati su una Filtering Table**. Questo modello **non scalava bene** perchè ogni Frame doveva essere riferito ad una Filtring Table.*
*Il Tagging del Frame unicamente **assegna un ID alla Vlan per ogni frame**. L'amministratore dello switch **assegna un Vlan ID ad ogni vlan** nella configurazione dello switch.*
*Questa tecnica fu scelta dall'istituto per ingegneri elettrici ed elettronici (IEEE) poiché essa è **estremamente scalabile**. Il tagging del frame è l'inserimento di una sorta di **"etichetta"** per cui avviene il **Riconoscimento**, come il meccanismo standard del Trunking. Paragonandolo al frame filtering, il tagging può fornire più soluzioni scalabili per l'implementazione di Vlans su vasti campi. L'etichettatura del frame da parte degli stati IEEE 802.1q è il metodo di implementazione delle VLAN*
*Il tagging dei frame sulle VLAN è una tecnica che è stata costituita per le comunicazioni "switched". Il tagging del frame, **posizione un identificativo unico nell'header di ogni frame, nel momento in cui esso è forwardato e posizioneto sul backbone di rete**. L'identificativo è compreso ed **esaminato da ogni switch**, prima di ogni broadcast o trasmissione da parte di altri switch, router o stazioni riceventi. Quando il **frame esce tramite il backbone, lo switch rimuove l'identificativo prima che il frame sia definitivamente recapitato** a destinazione. La funzione identificativa del frame, è di livello 2 e necessita di un piccolo processo amministrativo.*

La relazione fra Porte, Vlans e Broadcasts: Una vlan è composta da **una rete Switched** the è originariamente segmentata attraverso funzioni, teams di progetto o applicazioni, riguardo o meno la locazione fisica degli utenti. **Ogni porta di switch può essere assegnata alla Vlan**. Le porte assegnate alla stessa VLAN **condividono il broadcast**. Le porte che non appartengono alla stessa Vlan non condividono Broadcast. Le vlans **migliorano la performance** e la maneggevolezza della rete. Le seguenti sezioni riguardano Tre metodi **di implementazioni delle vlans** che possono essere usati per assegnare una porta dello switch alla vlan.
Essi sono:

- **Port centric**

- **Static**
- **Dynamic**

Una "port-centric" Vlan Rende facile lavoro all'amministratore: Nelle Vlans port-centric, tutti i nodi connessi alle porte in una stessa Vlan **hanno lo stesso Vlan ID**. Possiamo ottenere un grafico che mostri la membership della vlan suddividendola per porte che rendono il lavoro dell'amministratore più facile e la rete molto più efficiente poiché:

- Gli utenti sono **assegnati per porta**
- La Vlan **è facilmente amministrata**
- Essa fornisce un **incremento di sicurezza** fra Vlans
- I pacchetti **non raggiungono altri domini**.

Vlans Statiche: Le Vlan statiche consistono in **porte su uno o più switch che sono assegnate** staticamente ad una vlan. Queste porte mantengono le proprie configurazioni di vlans assegnate fino a che non avviene un cambiamento. Ciò nonostante le vlans statiche richiedono all'amministratore di eseguire cambi tramite una stazione di management della rete, **esse sono sicure, facili da configurare ed esaminabili senza difficoltà**. Le Vlans statiche lavorano bene in reti in cui avvengono spostamenti, controlli e gestione.

Vlans Dinamiche: Le Vlans dinamiche **consistono in porte, su uno switch che sono autumaticamente determinate** tramite un'assegnazione. Le funzioni delle dynamic vlan sono **basate sull'indirizzo mac**, **indirizzo logico o tipo di protocollo** con cui si gestisce i pacchetti. Quando una stazione è inizialmente **connesso ad una porta** dello switch, **non assegnata**, **esso esegue un controllo del mac address** nel **database della Vlan**. Lo switch quindi **configura dinamicamente la porta** con la corrispondente Vlan. Il vantaggio maggiore di questo metodo è **meno necessità** di amministrazione all'interno della wiring closet dove un utente è aggiunto, spostato quando generalmente si aggiunge alla rete per la prima volta. C'è più amministrazione durante il setup del database **con il software di management della Vlan** che mantiene un accurato database degli utenti sulla rete.

Come le Vlans eseguono facilmente Spostamenti e cambi addizionali: Le compagnie sono in continua re-organizzazione.Dal 20 al 40 percento della forza di lavoro fisica è spostata ogni anno. Questi spostamenti, addizioni e cambi sono una delle menate più grandi che un amministratore di rete può avere, ed una delle cause di spesa maggiore che una rete può comportare, per quanto riguarda, appunto, la propria gestione. Molti **spostamenti richiedono il ricablaggio**, e il gran parte tutti gli spostamenti richiedono **un nuovo addressing sui pc**, che, in una lan standard, conseguono alla **riconfigurazione dei routers** e degli hubs.
Le Vlans forniscono un meccanismo effettivo per controllare i propri cambiamenti e **ridurre in gran parte il costo associato alla riconfigurazione** di hub o\e routers.
Gli utenti, in una vlan, possono condividere lo **stesso spazio riservato agli indirizzi** di rete (che è la sotterete ip ((SUBNET)), riguardo o meno la loro locazione fisica. Quando utenti **in una vlan** sono **spostati** da una locazione ad un'altra, il loro indirizzo di rete **non deve cambiare**. Ciò è valido **fin quando essi rimangono all'interno della stessa Vlan** e sono connessi alla **stessa porta** sullo switch. Una cambio di locazione, può essere semplice con il plugging di un utente in una porta di uno switch in grado di sostenere Vlan e di configurare le proprie porte basandosi sulla stessa Vlan. Le vlans rappresentano un **miglioramento significativo della tipica lan**, basata su tecniche dirette applicate fisicamente sulla wiring closet. Le vlans richiedono **meno ripassaggi di cavo, meno configurazioni, e meno debugging**. La configurazione dei **router resta la stessa**. Un semplice spostamento di un utente da una locazione ad un'altra, non comporta alcuna modifica sulla configurazione del router, se l'utente è situato sulla stessa Vlan.

Come le Vlans Aiutano a controllare l'attività Broadcast: Il traffico **broadcast** esiste e può essere **generato in ogni rete**. La frequenza del broadcast dipende dal tipo di applicazione, dal tipo di server, dall'ammontare della segmentazione logica e da come queste risorse di rete sono usate. Le applicazioni sono settate, da qualche anno ormai, in modo da ridurre il numero di broadcast inviati. Nuove applicazioni multimediali sono state create, con funzioni intensive di broadcast e multicast. Le misurazioni hanno la necessità di **prevenire problemi relativi a broadcast**. Uno dei più efficenti sistemi di misurazione è **segmentare la rete con firewalls protettivi**. I firewalls possono prevenire problemi su un segmento per evitare il danneggiamento di altre parti della rete. Quindi un segmento può avere condizioni eccessive di broadcast, mentreil resto della rete è protetta con un firewall **la cui funzione è comunemente fornita da un router**. La segmentazione da parte del firewall fornisce **affidabilità e minimizza il sovraccarico di traffico generato dai broadcast**, offrendo maggiore portata al traffico riservato alle applicazioni.
Se i router non sono utilizzati fra switch, **i broadcast di livello 2, sono inviati ad ogni porta dello switch**. Quando fenomeno si riferisce comunemente ad una FLAT network. **In una flat network c'è un dominio di broadcast sull'intera rete**. Il **vantaggio della flat** network è la **bassa latenza** e la **alta performance**, ciò in relazione alla portata ed alla facile amministrazione. Lo **svantaggio** è che le flat network **incrementano la vulnerabilità al traffico in broadcast** che avviene sugli switch, sulle porte, links backbone ed utenti.
Le **Vlans** possono effettivamente **estendere il firewall dal router allo switch**, proteggendo la rete da problemi di broadcast. Addizionalmente le Vlans mantenegono tutti i benefici, in termini di performance e benefici di switching.
I firewalls furono creato assegnando porte di switch o utenti a specifici gruppi di vlan sia con singoli che con multipli swich. Il traffico **broadcast** all'interno di una lan **resta contenuto** e non si trasmette all''sterno di essa. Le porte adiacenti quindi, non ricevono niente del traffico broadcast generato da altre VLANS. Questo tipo di configurazione sostanzialmente, **riduce il peso del traffico**, libera la banda per l'utilizzo e abbassa la vulnerabilità a broadcast storms.
Quanto più piccolo è il gruppo di Vlan, tanto più piccolo è il numero di utenti affetti da broadcast, all'interno dello stesso gruppo. Le **Vlans** possono anche essere **assegnate in base al tipo di applicazione ed all'internsiivtà del broadcast** che una determinata applicazione può generare. Gli utenti che stanno condividendo un'applicazione "broadcast intensive", possono essere posizionati nella stessa vlan e distribuiti sul campo.

Come le Vlans Possono aumentare la Sicurezza di rete: L'uso della lan si è incrementato moltissimo rispetto agli scorsi anni. Il risultato è che le lan spesso si trovano in situazioni critiche per quanto riguarda lo spostamento dei dati.La trasmissione di dati **"confidential" richiede sicureza tramite accesso ristretto**. Un **problema delle** lan condivise è che esse sono relativamente **facili da penetrare**. Inserendo un Plug, un utente intrusivo, può avere accesso a tutto il traffico all'interno del segmento. Quanto più largo è il gruppo, quanto più grande è il potenziale d'accesso. Una semplice tecnica amministrativa per aumentare la sicurezza è segmentare la rete in multipli gruppi di broadcast che permettono al manager di:

- **Ristringere il numero di utenti nella Vlan**
- **Impedire ad un altro utente di penetrare senza prima ricevere l'approvazione dal manager** della vlan.
- Configurare **tutte le porte non usate** per un servizio di default a **BASSA priorità** di Vlan.

Implementare questo tipo di segmentazione è relativamente **facile.** Le porte dello switch sono raggruppate assieme, e basate su tipo di applicazione e privilegi di accesso. Applicazioni ristrette e risorse sono comunemente inserite in un **gruppo sicuro di Vlan**.
Ai fini della sicurezza, nelle vlan, **lo switch ristringe l'accesso ai gruppi**. Le restrizioni possono essere attuate in base ad indirizzi di stazioni, tipi di applicazioni e tipi di protocolli.

E' possibile **aggiungere maggiore sicurezza** utilizzando le **ACCESS CONTROL LIST**. Esse sono utili specialmente nelle **comunicazioni fra Vlans**.
Per quanto riguarda altre possibilità di sicurezza sulle Vlan, il **router ristringe l'accesso alla vlan** come configurato su switch e routers. E' possibile creare restrizioni in base a indirizzi ip, tipo di applicazione, tipo di protocollo e anche orario della giornata.

Come le Vlans possono far risparmiare: Durante il passato gli amministratori di rete hanno installato un numero significativo di hubs. Questi hubs eseguono funzioni utili in molte installzioni già esistenti quando essi sono utilizzati con switched. **Molti hubs sono sostituiti con nuovi switch**. Gli amministratori di rete possono **risparmiare** denaro **connettendo hubs esistenti a switch**. Nel momento in cui ogni porta dello switch può costituire una Vlan, **ogni segmento relativo all'hub connesso a questa porta, può essere assegnato SOLO a quella specifica VLAN**.
Le stazioni che condividino un hub segment, sono tutte assegnate allo stesso gruppo di VLAN. Se una stazione individuale necessita di essere RIASSEGNATA ad un'altra VLAN, la stazione dev'essere riallocata **al corrispondente Hub**. Lo switch interoconnesso gestisce la comunicazione fra le porte dello switch ed automaticamente determina il segmento appropriato di ricezione. Se un hub condiviso è diviso in un piccolo gruppo, la microsegmentazione aumenta. Ciò garantisce maggiore flessibilità assegnando utenti individuali a Vlan.
Connettendo hubs a switch, gli **hub** possono essere usati come **parte dell'architettura della VLAN**. Questo permette la **condivisione del traffico** e delle risorse di rete direttamente connesse alla porta di switching con la stessa Vlan.

Design di Rete

Gli obiettivi del design di una Lan: Designare una rete può essere un'operazione non semplice che va oltre la semplice connessione di più computer assieme. Una rete **deve includere molte caratteristiche**, per poter essere scalabile e maneggevole. Per designar una rete **scalabile** ed **affidabile**, i designers di rete devono realizzare ognuno dei maggiori componenti di rete con requisiti e tecniche distinte.Anche una rete che consiste in soli 50 nodi può portare a problemi complessi e\o risultati incalcolati. Per cui di conseguenza tentare di disegnare una rete che contiene 1000 elementi può essere ancora più complesso.
Il primo step per quanto riguarda il design di una lan è stabilire **quali documenti serviranno** per poter completare il design e per raggiungere gli obiettivi prefissati. Questi obiettivi **possono variare** a seconda dell'organizzazione o della situazione in cui ci si trova. Comunque i seguenti requisiti vengono prefissati nella maggior parte dei design di rete:

- Funzionalità- La rete deve lavorare, essa deve **permettere agli uetnti** di andare in contro alle **necessità lavorative**. La rete deve fornire, utente per utente, utente per applicazione, **connettività con una velocità ragionevole** ed affidabilità.
- Scalabilità- La rete dev'essere in grado di **crescere**. Deve permettere una crescita **senza cambi di componenti**, in ogni sua parte.
- Adattabilità- La rete dev'essere designata con **un occhio alle tecnologie future**. Essa **non deve** includere elementi che possono in qualche modo **limitare l'implementazione** delle nuove tecnologie o di quelle che verranno
- Maneggevolezza- La rete dev'essere designata in maniera tale da **facilitare il controlllo e la gestione**, e da garantire stabilità in tali operazioni.

Questi requisiti sono specifici per **certi tipi di rete** o più in generale, in altri tipo di reti. Questo capitolo parlerà di come indirizzarsi verso questi requisiti.

Componenti critichi in un design di rete: Con l'emergere **di tecnologie ad alte velocità** come ad esempio **ATM** e le complesse architetture lan che usano **VLANS**, molte organizzazioni hanno

upgradate le reti esistenti a **Nuove reti più veloci**. Per un design di reti ad alta velocità e basate su applicazioni multimediali, i designers di rete, devono indirizzarsi verso is seguenti componenti critici, del design di una lan:

- La **funzione** e **la posizione dei server**
- **Rilevazione di collisione**
- **Segmentazione**
- **Banda e Domini di Broadcasts**

Inserimento di server durante il design di rete: Uno dei componenti chiave nel design di successo è comprendere **la funzione e la posizione dei server** necessari per la rete. I servers forniscono la c**ondivisione** di file, **la stampa la comunicazione, ed i servizi di applicazione**, come ad esempio word processing. I server tipicamente **non funzionano come le workstations**. Esso dispongono di specifici sistemi operativi come ad esempio NET WARE, windows NT, unix e linux. Ogni server solitamente è **dedicato ad una funzione**, come ad esempio gestione email o condivisione files. I servers possono essere divisi in **2 distinte categorie**. **ENTERPRISE servers e WORKGROUP servers**. Un **Enterprise** server supporta **tutti gli utenti della rete** offrendo servizi come ad esempio email, dns e tutto ciò che l'organizzazione ha necessità di usare. **Workgroup** server supporta **uno specifico set di utenti** offrendo servizi che assolvono le necessità di un particolare gruppo. Il dipartimento di vendita, per esempio può avere frequentemente la necessità di consultare un inventario o database ed il dipartimento di ingegneria può avere la necessità di specializzarsi su un'applicazione di disegno.
Gli Enterprises server devono essere posizionati **come MDF** (main distribution facility), in questo modo **il traffico sui server enterprise è situato in una posizione intermedia** e non vi è necessità di trasmettere per tutta la rete al fine di poterlo raggiungere.
Gli workgroup serevrs devono essere posizionati **come IDF** (intermediate distribution facilities), **vicino agli utenti che accedono alle applicazioni** di quei determinati servers.
Spesso è necessario **collegare** direttamnete **server all'MDF ed all'IDF**. Posizionando **workgroup server vicina ad utenti**, il traffico, viaggerà solo tramite l'infrastruttura di rete diretta all'idf e non ingluenzerà altri segmenti di rete destinato al traffico usato per altri utenti. **Con MDF e IDF è possibile utilizzare switched lan da 100 MEGABIT per la comunicazione** con questi server.

Intranet: Una opzione configurazione piuttosto **comune** per le lan è la **creazione di una intranet**. I server web intranet privati **si differenziano da quelli pubblici**. I server **pubblici, non hanno accesso all'intranet**. Le intranet sono designate **per avere accesso da parte di utenti che hanno privilegi all'interno** della rete, tramite, i server web installati sulla rete. La tecnologia **Browser** è usata per **acceder alle informazioni**, come ad esempio dati finanziari, I dati basati su grafici, testi ed altro,salvato su questi servers.
L'ggiunta di una **intranet**, alla rete, può causare una **necessità aggiunta di banda**. Poiché intranet necessita di banda extra sul backbone di rete, gli amministratori di rete devono anche considerare di acquistare dei **computer veloci** per l'accesso a queste intranet. I nuovi computers e server possono supportare velocità di 10\100 e 1000 megabits, tramite apposite NIC (network interface card), per fornire una maggiore flessibilità nella configurazione, quindi permettendo agli amministratori di rete di dedicare banda a stazioni individuali, secondo le necessità.

Che tipo di contesa è stabilita con ethernet: Dei buoni progetti di rete richiedono attenzione sulla **selezione ed il posizionamento delle periferiche di rete**, poiché conflitti e collisioni possono avvenire anche a causa di una minima disattenzione.
Un nodo ethernet effettua **l'accesso al cavo** assieme **ad altri nodi ethernet**. Quando le reti sono ingrandite **aggiungendo più nodi sul segmento** condiviso, ogni nodo è ha accesso in minor parte alla condivisione dello stesso media. La **performance** di rete quindi **deteriora**, anche a causa

dell'aumento di **collisioni**. Ethernet non può evolversi o scalare a causa di una inabilitazione degli avcessi al "Contention-based".
Quanto più **il traffico si incrementa** sul media condiviso, quanto più le **collisioni aumentano**. Le collisioni sono **eventi normali in ethernet**, tuttavia un eccessivo numero di esse, riduce notevolmente la banda. In molti casi, la banda attuale è **ridotta ad una frazione di 10 megabit**, ipoteticamente disponibili.
La riduzione della banda può essere un fenomeno **Rimediabile, utilizzando i bridges, switch o router, per rendere più efficiente un segmento** di rete.

Perché i domini broadcast si relazionano con la segmentazione: La segmentazione è il processo di **splitting di un singolo dominio di collisione in 2 o più** domini di collisione. I **bridges** o gli **switches** possono essere usati al livello data link per **segmentare una tipologia bus**, logica e creare un dominio di collisione separato.
Il risultato è **più banda** disponibile per ogni stazione, individualmente. **Switches e bridges** non forwardano collisioni, bensì pacchetti.
Tutti i **broadcast** che provengono da ogni host sullo stesso dominio broadcast **sono visibili da tutte le altre stazioni** nello stesso **dominio di broadcast**. I broadcast **devono essere visibili** da tutti gli host nel dominio broadcast al fine di stabilire la connettività.
La scalability della bandwidth domain dipende dal totale ammontare di traffico e la scalabilità del broadcast domain dipende dall'ammontare del traffico broadcast. E' molto importante ricordare che normalmente **switched e bridges, forwardano i broadcast (FF-FF-FF-FF-FF) mentre i router li bloccan**o.
La differenza fra Banda e domini di collisione: Una **bandwidth domain** è ogni cosa **associata con una porta su un bridge o su uno switch**. Nel caso dello **switch** ethernet il **bandidth domain** è anche conosciuto come **Collision Domain**. Tutte le workstations all'interno del Bandwidth domain competono per le **stesse risorse di banda** della rete. Tutto il traffico da ogni host verso il BandWidth domain è visibile da tutti gli altri hosts. Nel caso dell'ethernet collision domain, due stazioni possono trasmettere allo stesso tempo, causando una collisione.

Raduno ed analisi di tutto l'occorrente: Poiché una lan sia effettivamnete funzionante e possa fornire servizio ad utenti ed assolvere alle loro necessità, dev'essere **propriamente designata ed impelementata**. Esistono **una serie di steps** da completare per poter arrivare a ciò

- Raggruppare **i bisogni** degi utenti
- Analizzare i **requisiti**
- Designare la **struttura delle periferiche** di livello 1,2,3 e la **tipologia** di rete
- Documentare **l'implementazione** della rete dal punto di vista **logico e fisico**

Il primo step nel design di una rete può essere **raggruppare i dati** sull'organizzazione della struttura. L'**history** dell'organizzazione, lo **stato corrente** ed eventuali **progetti** di crescita devono essere inclusi. Le **policies** operative, le procedure di **management**, i sistemi di ufficio, le **procedure interne** ed i punti di vista di persone che useranno la lan, sono punti ugualmente importante. E' necessario quindi rispondere alle seguenti domande:

- **Chi** sono le persone che **useranno la rete**
- **Qual è** il loro livello di **skill?**
- Quale sono le loro **attitudini di utilizzo del computer e delle applicazioni per computer?**

Rispondendo a queste ed a domande similari ci aiuterà a determinare **quanto training** sarà indispensabile e **quante persone saranno necessarie** per il supporto della LAN.
Raggruppando le informazioni ci si avvantaggia su eventuale scoperte e identificazioni dei problemi. Idealmente le informazioni dei processi raggruppati aiutano a chiarire ed identificare i problemi E' anche possibile determinare **se ci sono "policies" documentate sul posto**. Determinare se alcuni dati od operazioni sono stati dichiarati **"CRITIC". Mission-Critical data e operazioni**

sono considerati componenti chiave per il lavori. Accedere ad essi, è critico per lo svolgimento del **lavoro di ogni giorno**. Quindi bisogna determinare **quali protocolli sono permessi** sulla rete, e se tutti o solo alcuni **computer possono supportarli**. Raggruppando questa informazione ci aiuterà a determinare **quanto training sarà necessario** ed il numero di persone che dovranno supportare la LAN.
Poi è necessario determinare chi, nell'organizzazione, ha **l'autorità di determinare l'indirizzamento** , i nomi, la tipologia del design e la configurazione. Alcune compagnie hanno un **manger** centrale "management information systems" (MIS), che controlla ogni cosa. Altre compagnie hanno MIS molto ridotti e\o delegano autorità o divisioni.
Si deve Porre attenzione sull'identificazione e le limitazioni dell'organizzazione. Le risorse che possono influire su sull'implementazione di una nuova LAN, sono l'hardware e il software e le risorse umane. Computer e pacchetti software, già esistenti, devono essere **documentati**, sono quindi indispensabili identificativi hardware e software. E' inoltre importante sapere come queste risorse sono linkate o condivise, e conoscere le risorse finanziarie disponibili all'interno dell'organizzazione. Documentando questo tipo di cose, ci aiuta a fare **una stima dei costi e costruire un budget** per la lan.
E' necessario essere sicuri di comprendere la **performance di una rete già esistente**.

Fattori che hanno effetto sulla disponibilità di rete: Esistono Unità di misura che indicano **fattori indispensabili** per la rete, possiamo citarne alcune:

- **Portata (throughput)**
- **Tempo di risposta**
- **Accesso alle risorse**

Ogni cliente ha una diversa **definizione di Disponibilità**. Per esempio può essere necessario **trasportare voce e video** sulla rete. Comunque questi servizi richiedono **più banda** di quella che è effettivamente disponibile sulla rete o sul backbone. E' possibile **incrementare la disponibilità** aggiungendo più risorse, ma le risorse **comportano un costo**. I design di rete cercano di fornire **più banda possibile e risorse al minor costo**.
Dopo aver considerato **l'esigenza di disponibilità**, il prossimo step nel design di una rete è analizzare gli **elementi di rete necessari** e le informazioni utenti, raggruppate nell'ultimo step. Gli utenti di rete necessitano **costanti cambiamenti**. Per esempio quanto più **necessario** diventa usare **applicazioni basate su audio video**, tanto più la **pressione sulla** banda di rete diventa **intensa**. Un altro componente relativo alla fase di analisi è **l'assegnazione dei requisiti utente**. Una rete che non è capace di assolvere le necessità proposte dagli utenti, è destinata ad essere utilizzata poco. Perciò bisogna accuratamente analizzare e di conseguenza GARANTIRE che la rete **assolva** i bisogno delle persone che vi lavorano.

Tipologie fisiche usate nel networking: Dopo aver analizzato i requisiti della rete, possiamo determinare con esattezza **i bisogni e le necessità** per gli utenti. Successivamente dev'essere scelta una tipologia di lan che **soddisfi le esigenze degli utenti**. Ci concentreremo sulla STAR TOPOLOGY e sulla Extended star topology. Come già visto in precedenza, la star\extended topology utilizza ethernet 802.3 CSMA\CD. E' una **configurazione dominante** all'interno dell'industria. Il design della topologia di rete può essere diviso in 3 aree distinte. Queste aree sono definite dal livello fisico, dal data link e dal livello network del modello osi.
Le sezioni che seguiranno tratteranno gli elementi relativi al design della topologia di rete, in relazione a: phisichal, data link e network.

Design della tipologia di livello 1, metodo di segnale, tipo di media, e lunghezza massima: Esamineremo il livello 1 e la tiplogia a stessa estesa (extended Star). Il **cablaggio fisico** è uno dei componenti **più importanti** da configurare quando si effettua il design di una rete. I problemi relativi al design possono includere..**Tipo di cablaggio** usato, e **struttura del cablaggio**. Il livello 1

di cablaggio include spesso il tipo di categoria 5, "unsielded twisted-pair" (utp) ed il cavo a fibra ottica, insieme con lo standard TIA\EIA-568-A per il layout e gli schemi di collegamenti cablaggio. In aggiunta alle limitazioni di distanza è necessario valutare con certezza **la forza e la debolezza delle varie tipologie**, prima di poter tracciare il cavo. Molti problemi sono relativi al livello 1.Quindi se si prevede un significativo cambiamento sulla rete, è anche necessario fare una revisione completa del cablaggio, eventualmente ripassare i cavi dove necessario.
Se si sta progettando una nuova rete o si sta ricablando una già esistente, la fibra ottica è preferibile per l'utilizzo su backbone o rialzi, con cavo di categoria 5 UTP a scorrimento orizzontale.
L'upgrade del cavo deve avere una certa proprità.Le imprese dovrebbero garantire, senza alcuna eccezione, che i propri sistemi siano conformi agli standard industriali defiiti dalle specifiche TIA\EIA-568-A.
Gli standard **TIA\EIA-568-A specificano che ogni periferica connessa alla rete dev'essere linkata ad una locazione centrale con cablaggio orizzontale**. Le periferiche devono rientrare nei 100 metri di distanza, per un cavo di categoria 5 UTP ethernet, come specificato dagli standard TIA\EIA-568-A.

Diagrammare un cavo basato sullo standard ethernet, dalla workstation alla HCC, includendo le distanze: In una semplice tipologia a stella con una sola wiring closet, l'MDF include uno o più patch panels, cross-connet orizzontali (HCC).I patch cable HCC sono usati per collegare il cavo orizzontale di livello 1, con le periferiche richieste di livello 2. Lo switch di rete è connesso ad una porta ethernet sul router (livello3), usando un patch cable, di categoria 5 ethernet. A questo punto l'host finale ha completato la connessione fisica alla porta del router.

Hcc, Vcc, Mdf, Idf e Pop: Quando ci sono degli host, in reti di grandi dimensioni, che **eccedono la distanza di 100 metri,** relativi alla categoria 5 utp, non è insolito che vi sia **più di uno wirin closet**. Creando multiple wiring closet, possono essere create anche numerose aree in cui è possibile collegare periferiche di rete. La **Wiring Closet secondaria è chiamata IDF**. Gli standards TIA\EIA-568-A specificano che IDF **dev'essere connessa a MDF usando la cablatura vertucale**, chiamata anche **Backbone** cabling. Un connettore verticale (vertical cross-connect,VCC), è usato per **interconnettere vari IDF ad un MDF centrale**. Di norma si usa il cavo a fibra ottica poiché la lunghezza del cavo verticale supera i 100 metri, che rappresentano il limite per il cavo di categoria 5 UTP.

Ethernet 10Base-T e 100Base-TX: La **Fast Ethernet** è in realtà una ethernet upgradata a **100Megabit**. Essa utilizza lo standard **"broadcast-oriented"**, ethernet, con tipologia "logical bus topology, 10baseT", tramite **il metodo CSMA\CD** per il Media Access Control **(MAC)**. Lo standard Fast Ethernet comprende attualmente numerosi standards basati sul twisted pair wire (100BASE-T), e **altri cavi a fibra ottica (100BASE-FX) ed è utilizzato per connettere MDF a IDF**.

Elementi di un diagramma di tipologia Logica: Il *diagramma logico* mostra il **modello di** tipologia escludendo i dettagli di installazione **ed i percorsi del cavo**. E' una **mappa base per la descrizion**e di una lan. Il diagramma logico include:

- La **locazione** esatta **dell'MDF e dell'IDF**.
- Il tipo e la quantità di **cavi** usato per **interconnettere l'IDF con l'MDF**. E' anche incluso il numero idi cavi disponibili per incrementare la banda fra wiring closets. Per esempio se il **cablaggio verticale fra IDF1 e MDF** riesce a garantire l'80% di **assolvenza alla banda richiesta,** è possibile **aggiungere due pairs di cavi** per raddoppiare la **capacità**.
- La **documentazione dettagliata di tutti i cavi passanti**, i numeri di identificazione e le porte su cui HCC e VCC sono collegate e saranno terminate. Per esempio, la stanza 203 ha perso la connettività con la rete. Esaminando il Cutsheet, è possibile vedere che dalla stanza 203 sta

passando il cavo 203-1, che è collegato con hcc1 sulla porta 13. E' possibile testare se il cavo passante presenta un problema di livello1.

Periferiche comuni di livello 2 ed il loro impatto sulla rete: L'obiettivo delle periferiche di **livello 2**, in una rete è fornire **il controllo di flusso**, la rilevazione degli errori, la correzione degli errori e **rudurre la congestione** sulla rete. Le due periferiche più comuni, che appartengono a questo livello (oltre alle nic, che ogni rete ha), sono i **bridge e gli switch**. Le periferiche di questo livello **determinano la dimensione del dominio di collisione**. In seguito parleremo dell'implementazioni delle reti in relazione al livello 2.

Switching Asimmetrico: Le dimensioni delle Collisioni e dei domini di collisioni sono due fattori che influiscono negativamente sulla performance della rete. Utilizzando il **lan switching è possibile micro segmentare la rete**. Questo elimina collisioni e **riduce la domensione del dominio di collisione**. Un'altra caratteristica importante dl lan switch è come esso alloca la banda basandosi su "per-port". Tale allocazione permette più banda per la cablatura verticale, uplinks e server. Questo tipo di switching è riferito al **"asymmetric Switching**". Esso fornisce connessioni "switched" fra porte di diversa banda come ad esempio combinazioni di **10 e 100 megabit**.

L'ettetto che la microSegmentazione può avere su di una rete: La **micro segmentazione** si ottiene usando switch e bridge **eliminando domini di collisione** e di conseguenza congestione di rete. Ciò offre miglioramenti accellerando la performance di workgroups e backbones. Tipicamente l'accellerazione di performanche eseguita in questo modo, involve lo switching ethernet. Gli switch possono essere usati come hubs per fnire il livello appropriato di performance per differenti utenti e servers.
Determinazione del numero dei cavi: Mentre si effettua il design di una rete, uno switch posizionato in MDF e in IDF, va a collegarsi con la **cablatura verticale fra MDF e IDF**, ciò causa un trasporto di traffico fra MDF e IDF. La capacità di **questo collegamento deve essere maggiore** di quella fornita da un collegamento che, da IDF, raggiunge le Workstations. Il cablaggio **orizzontale** scorre utilizzando CATEGORIA 5 UTP e **non deve essere più lungo di 90 metri**, permettendo **link a 10 megabit o 100 megabit**. In situazioni normali, 10 megabit è una **banda adeguata** per la caduta del cablaggio orizzontale. Gli switch per lan asimmetriche, permettono un mix di 10 megabit e 100 megabit su ogni porta di un singolo switch. Il prossimo compito è determinare il numero di porte, da 10 o 100 megabit che sono necessarie per l'Mdf e per ogni IDF. Ciò può essere determinato andando ad analizzare, a posteriori, i bisogni degli utenti, seguento la cablatura orizzontale, ed analizzando l'area in cui essa trova connettività.
Il numero di cavi verticali passanti, dev'essere incluso. Per esempio, gli utenti dicono che per ogni stanza devono passare 4 cablature orizzontali. L'idf a cui il servizio è collegato, e che copre l'area interessata, interessa 18 Stanze. Per cui le calate di cavo devono essere 18. Il totale sarà 72 Porte di switch, per tutti gli utenti di tutte le stanze.

Determinazione della dimensione del dominio di collisione in reti con Hub o Switch: Per determinare la **dimensione del dominio di collisione**, è necessario determinare **quanti h**ost sono fisicamente connessi **ad ogni singola porta** dello switch. Ciò può essere fondamentale al fine di determinare quanta banda è disponibile per ogni host. Una situazione ideale possiamo averla connettendo **solo un host per ogni porta** di switch. Tale situazione andrebbe a **tagliare di netto** il **dominio di collisione** per cui ne derivva che in questo caso le uniche 2 cose che abbiamo solo l'host sorgente e l'host di destinazione. Effettivamente in questo caso, le collisioni dovrebbero praticamente essere **ridotte a zero**, durante la comunicazione fra gli host.
Un altro metodo per implementare lo switching sulle lan, è installare hub condivisi sulle porte degli switch e collegare molteplici host ad una singola porta dello switch. Tutti gli host connessi **sugli hub condividono lo stesso dominio di collisione** e la stessa banda.

E' da notare che molti switch di vecchio tipo come ad esempio il Catalyst 1700 non offrono un vero e prorpio supporto di condivisione dello stesso dominio di collisione e della stessa banda, poiché essi non mantengono mappature di multipli indirizzi fisici (MAC) per ogni porta. In questo caso, possono esserci molti broadcasts e richieste ARP.

Posizionamento degli hub in una extended-star topology: Gli **hubs condivisi** possono essere **usati con usuccesso** in una Switched lan, per coreare **molteplici punti di connessione** alla fine della cablatura orizzontale. E' però necessario assicurarsi che il dominio di collisione si mantenga ridotto. I requisiti di banda da parte degli host, devono essere accordati durante il processo di design della rete.

Migrazione di un arete da 10 Megabit a 100 Megabit: Quanto più la rete cresce, tanta più banda è necessaria. Nel cablaggio verticale fra MDF e IDF, fibre ottiche non utilizzate possono essere collegate dal VCC alle porte a 100Megabit sullo switch.
La cablatura orizzontale può incrementare il fattore di 10. Ciò viene effettuato portando un cavo che va **dall'HCC ad una porta a 100Megabit** sullo switch e cambiando **gli hub a 10 megabit, con hub a 100 megabit**. In fase di dimensionamento della lan switched è importante essere sicuri che vi siano sufficienti porte a 100 megabit per questa migrazione. E' importante documentare la velocità a cui ogni cavo attualmente installato, può viaggiare.

Utilizzare i router alla base del design di rete: Le periferiche di **livello 3**, come i router, ad esempio, possono essere usate per **creare segmenti di lan** unici. Le comunicazioni **fra segmenti** sono basate **sull'indirizzamento di Livello 3**, possiamo fare l'esempio dell'ip addressing o dell'ipx addressing. L'implementazione delle periferiche di **livello 3, permettono la segmentazione** di una lan, in una unica rete logica e fisica. **I routers permettono** anche **la connettività a WAN**, come ad **esempio internet**. Il **routing di livello 3**, determina il flusso del traffico fra **segmenti fisici di rete** basati sull'indirizzamento di livello 3. Il router è una delle periferiche può potenti nella tipologia di rete. Come precedentemente discosso**, un router forwarda i pacchetti badandosi sull'indirizzo di destinazione**. Un router **non forwarda i broadcast**, come ad esempio le richieste ARP.
L'interfaccia router è considerata **il punto di entrata e di uscita di un broadcast domain** e ferma i broadcast prima che essi possano raggiungere altri segmenti della lan. form

Come le Vlans possono creare piccoli domini Broadcast: Un problema importante nella rete è il totale numero di broadcast, comprese le ARP requests. Utilizzando le **VlanS è possibile limitare il traffico broadcast all'interno della VLAN** e creare un piccolo **broadcast domain**. La vlan può anche essere usata per **fornire sicurezza** creando un vlan group per una specifica funzione.
L'associazione fisica delle porte è usata per implementare le VLAN.

Come il router fornisce la Struttura ad una rete: I router **forniscono salabilità** poiché essi possono servire come firewall o broadcasts. Gli indirizzi di livello 3, tipicamente hanno una struttura che permette ai router di fornire grande stabilità dividendo la rete in subnets. Una notevole **scalabilità** è aggiunta **alla struttura di indirizzamento di livello3**.
Quando la rete è divisa in **subnet**, lo step finale è quello di realizzare e **documentare lo schema di indirizzi ip** che dovrà essere utilizzato nella rete. La tecnologia di routing **filtra i broadcast data-link ed i multicast**. Aggiungendo alla porta del router, subnet addizionali o indirizzi di rete, è possibile segmentare la internetwork a seconda delle necessità.
Gli indirizzi del protocollo di rete e il routing forniscono Built-in scaling (non l'ho capito). Quado si decide se usare router o switches, bisogna sempre ricordarsi, qualde problema si tenta di risolvere. Se il nostro problema è il protocollo, il router è appropriato. I **routers risolvono problemi** come ad esempio, **broadcast eccessivi**, protocolli non scalati bene, **mancanza di sicurezza, e problemi di**

indirizzamento. I routers comunque costano di più e sono più difficili da configurare rispetto agli switches.

Come una rete di grandi dimensioni necessita di incorporare Routers: I routers possono essere usati per **fornire subnet ed aggiungere struttura agli indirizzi**. Con i **bridges e gli switches**, tutti gli indirizzi **sconosciuti devono essere FLODDATi**, passando da ogni porta. Al fine di conoscere i mac sconosciuti.**I routers, usano protocolli** che possono risolvere il problema, identificando e trovando gli utenti, il flood quindi non è necessario. **Se l'indirizzo di destinazione è locale, l'host sorgente può incapsulare il pacchetto nell'header del data-link ed invhhhhhhhhiare un frame unicast, direttamente alla stazione di destinazione**.Il router non vede il frame e non ha la necessità di floddare il frame. L'host sorgente, deve usare ARP. Questo causa un broadcast, ma il broadcast è solo un broadcast locale, e non è forwardabile dal router. Se la **destinazione non è locale**, la stazione sorgente, **trasmette il pacchetto al router**. Il router **invia il frame alla destinazione o al prossimo hop, basandosi sulla propria tabella di routing**. Alla luce di ciò è ovvio che una rete,per essere scalabile, ha bisogno di molti routers.

Il diagramma di una rete Standard che utilizza Routers: Possiamo fare un esempio di implementazione di multiple reti fisiche.Tutto il traffico dalla rete 1, destinato alla rete 2, passa dal router. In questa implementazione, ci sono due broadcast domains. Le due reti hanno un unico schema di addressing sul network\subnetwork. In una struttura di cablaggio di livello 1, multiple reti fisiche sono facili da creare, semplici a collegare al cavo orizzontare ed a quello verticale, ed agganciare allo switch appropriato (livello2), utilizzando patch cables. Come vedremo nei capitoli futuri, questa implementazione fornisce ed implementa una robusta sicurezza. In aggiunta, il router è il punto centrale della lan, per la destinazione del traffico.

Mappa logica e fisica: Dopo aver realizzato lo schema di indirizzamento ip per il cliente, è necessario reperire documentazione per quanto riguarda i site e le reti all'interno dei site. Una convenzione standard può essere settata per indirizzi di host importanti sulla rete. Questo schema di indirizzi deve conservare consistente portata all'interno di tutta la rete. Creando mappe degli schemi di indirizzi, è possibile ottenere una sorta di istantanea dell'intera rete. Creando mappe fisiche della rete aiuta nel troubleshooting della rete stessa.

Protocollo di routing IGRP

Significato di Determinazione del percorso: Come già appreso in precedenza, ll livello network, **connette due interfacce e fornisce il best effort e la consegna end to end** agli utenti, tramite il livello di trasporto. Il livello network, invia macchetti dalla rete sorgente a quella di destinazione, **è necessario determinare un "path**" per poter far ciò, questa funzionalità è a **cura dei routers**.

Deterimazione Percorso: La funzione di **determinazine del percorso** permette ad un router di **valutare** i percorsi disponibili per la destinazione e di stabilire il **miglior percorso** per il **routing** dei pacchetti. Il routing si riferisce al **processo di scelta del miglior percorso** su cui inviare i pacchetti e come **attraversare molteplici reti** fisiche. Questo concetto è alla base delle comunicazioni internet. Molti protocolli di routing semplicemente usano i **percorsi più brevi** e quindi migliori. La sezione che seguirà spiega alcuni metodi per completare questa operazione. Il routing dei pacchetti nella rete è simile al viaggio di una macchina. I routers, tramite l'uso dei protocolli, effettuano decisioni di percorso basandosi sulle tavole di routing. Persone, che guidano auto, determinano il percorso migliore esaminando le mappe, analizzando le condizioni della strada e leggendo i segnali stradali.

Le operazioni delle Tavole di Routing: Nelle reti ip, **il router forwarda** i pacchetti dalla rete sorgente alla rete di destinazione basandosi sulla **tabella** di routing ip. Il router accetta i pacchetti su una interfaccia, determina quale percorso utilizzare e quindi procede a fare lo swiching dei pacchetti. Il router quindi **forwarda** questi pacchetti su un'altra interfaccia che è situata sul **prossimo hop** del miglior percorso per la destinazione dei pacchetti.
La tabelle di routing memorizzano le informazioni relative alle **possibili destinazioni** e come raggiungere queste destinazini. Le **tabelle** di routing possono memorizzare **solo la porzione di rete** dell'ip per il routing. Questo mantiene queste tabelle snelle ed efficenti;Non le appesantisce.
Le entries all'interno delle tabelle di routing contengono l'indirizzo ip del prossimo hop, lungo il percorso fino alla destinazione. Ogni entry specifica sono un hop ed il punto in cui il router è direttamente connesso. Si dice che un router è difettamente connesso se esso può raggiungere la determinata risorse tramite una rete singola.
I protocollo di routing permettono alle **tabelle di routing** di contenere una grande **varietà di informazioni**. Per esempio un router usa la tabella di routing, per verificare **il prossimo hop**, nel momento in cui esso riceve un pacchetto. Il router utilizza la propria tabella di routing per **verificare l'indirizzo di destinazione** e associare tale indirizo con il prossimo hop. L'indirizzo di destinazione ed il prossimo hop, informano il router che tale destinazione può essere raggiunta inviando il pacchetto ad un particolare router che rappresenta il prossimo hop sul tragitto per la destinazione.
Il router deve **comunicare con gli altri router** al fine di costruire un database o tavola di routing, attraverso l'uso dei protocolli di routing e tramite la **trasmissione di vari messaggi**. Il routing update, per esempio, è uno di questi messaggi. Il **routing update**, generalmente consiste in una porzione di **tabelle** di routing che aggiornano quelel in locale. Analizzando i **routing updates**, che provengono d altri router, il router può **costruire un dettagliato disegno della tipologia** di rete. Quando il router comprende la tipologia di rete utilizzata, esso può **determiare il miglior ROUTE** per la destinazione.

Metrics: E' assai importante che una tabella di routing sia **updatata con accuratezza** poiché il suo primario scopo è **fornire la miglior informazione** al router. Ogni protocollo di routing **interpreta il miglior percorso** a proprio modo. Il protocollo **genera un valore chiamato METRIC**, per ogni percorso sulla rete. Tipicamente, quanto **più piccolo è il metri, migliore è il percorso**.
Le tabelle di routing possono anche contenere **informazioni sulla desiderabilità** del percorso. I routers **paragonano i metrics** per determinare il miglior percorso. I metric si differenziano dipendentemente dal design del protocollo di routing che è usato. Una **varietà di metrics** comuni saranno descritti nel capitolo successivo.
Una varietà di metrics, possono essere usati **per definire il miglior percorso**. Molti procolli di routing come ad esempio Routing Information Protocol **(RIP), utilizzano solo un** metric. Altri protocolli di routing, come ad esempio Interior Gateway Routing Protocol (IGRP), **usano una combinazione** di metrics.

Decisioni di Forwarding by Router: Un router esamina il protocollo **relativo all'indirizzo della destinazione** del pacchetti. Quindi determina **se esso è in grado o meno di forwardare** questo pacchetto al prossimo hop. Se il router **non è in grado** di far ciò, e **non esiste una default** route, esso tipicamente **scarta il pacchetto**. **Se il router sa come forwardare** il pacchetto, esso **cambia la destinazione fisica (MAC) con quella del prossimo hop e trasmette il pacchetto**. Il prossimo hop può o meno essere direttamente connesso all'ultimo host di destinazione.
Se essono non è direttamente connesso, il prossimo hop, è solitamente un altro router. Il router esegue la stessa decisione di routing come il precedente. L'indirizzo network consiste in una porzione di rete ed in una porzione di indirizzi. La porzione network è usata dal router all'interno di una nuvola di rete. **La porzione di rete dell'ip di destinazione è estratta e comparata con l'indirizzo network sorgente**. Quando un pacchetto attraversa la rete, **l'ip sorgente e quello di**

destinazione non sono mai cambiati. Un **indirizzo fisico è determinato dal protocollo di routing** e via software, ed è lo stesso indirizzo fisico del prossimo hop.
La **porzione di rete** dell'indirizzo è utilizzata per **eseguire la decisione del per la selezione** del miglior percorso. Il router è responsabile del passaggio pacchetto alla rete successiva lungo il percorso. La funzione di **Switching** permette al router di **accettare un pacchetto su una interfaccia e forwardarlo su una seconda interfaccia**. La funzione di **determinazione percorso**, abilita il router a **selezionare l'interfaccia più appropriata** per il forwarding dei pacchetti.

Protocolli di Routing: Il termine Routed protocol e routing protocol sono spesso confusi. I **routed** protocols sono protocolli che vengono spostati sulla rete. Esempio di **routed protocols, sono TCP\IP** (transmission control protocol, internet protocol), **o IPX** (internetwork packet exchange**). I protocolli di routing** determinano il miglior percorso a cui inviare il routed protocols tramite la rete. Esempio di questi routing protocols. **IGRP, OSPF, EGP, BGP, RIP, APPN**. I computers (sistemi finali) usano i routed protocols, come ip, per esempio, per parlare con altri computers. I routers (sistemi intermedi) usano i routing protocols per parlare con altri, relativamente ai percorsi di rete.

Routing Multi Protocollo: I routers sono capaci del **routing multi protocollo**, che consiste nel **supporto di multipli** ed indipendenti **protocolli di routing** come ad esempio IGRP e RIP. Questa capacità permette ad un router di fare il **delivery dei pacchetti da alcuni** protocolli routed, come ad esempio Tcp\IP e IPX, **ad altri**, oltre lo stesso data link.

Differenza fra un protocollo di routing ed un altro: Il routing è il processo per determinare **dove inviare i pacchetti** destinati ad un indirizzo **al di fuori della rete** locale. I routers raggruppano e mantengono le informazioni di routing per permettere la trasmissione e rifiutare pacchetti. Le informazioni di routing prendono **il modulo di entry situato nelle tabelle** di routing ed una entry relativa ad ogni route identificata. I protocolli di routing permettono ad un router di creare e mantenere **tabelle di routing dinamicamente** e di effettuare cambiamenti della rete.
I protocolli di routing possono differenziare da altri in base a caratteristiche chiave:

- I particolari, obiettivo del protocol designer, avranno effetto sull'operazione del protocollo di routing risultante
- I diversi tipi di procolli di routing, possono generare differenti effetti sulla rete e sui routers

I **protocolli di routing sono solitamente divisi in due classi**. **Interior** Routing Protocols e **Exterior** Routing Procols. Gli **Interior** Routing Protocols sono usati per il routing delle informazioni all'interno di reti che sono **sotto un comune amministratore**, il complesso di questi sistemi è **definito Sistema Autonomo**.
Tutti gli IP interior protocols devono essere **specificati con una lista di reti associate**, prima che l'attività di routing possa iniziare. Un processo di routing cerca updates da altri routers e effettua un broadcast relativo alle proprie informazioni di routing su le stesse reti. **L'interior Protocol cisco, supporta il RIP ed IGRP**.
I protocolli **Esteriori** sono usati per **scambiare informazioni di routing** fra reti che **non** sono gestite da un **amministratore comune**, in altre parole, **fra sistemi autonomi**. I routing protocols esteriori, includono **EGP e BGP**. I protocolli di routing esteriori **richiedono le seguenti informazioni** affinchè il routing possa iniziare.

- Una **lista dei routers nelle vicinanze** (chiamati anche pers), con cui scambiare le informazioni di routing
- Una **lista delle reti da considerare** direttamente **connesse**.

L'obiettivo dei protocolli di Routing: LA ROUTE OTTIMALE- La route ottimale si riferisce **all'abilità da parte del routing protocol** di selezionare la **miglior ROUTE**. La migliore route

dipende dalla metric usata per effettuare il calcolo. Per esempio, un routing protocol può usare il numero di hops ed il ritardo, ma il calcolo del ritardo può essere più "laborioso".
SEMPLICITà ED EFFICIENZA- I protocolli di routing sono anche designati per essere **quanto più efficenti** possibili. L'efficienza è **particolarmente importante**, quando si usano protocolli di routing che devono girare **su periferiche con limitate risorse**.
ROBUSTEZZA- Per essere robusto, un routing protocol deve adempiere al suo scopo **in ogni circostanza**. Queste circostanze possono ad esempio essere Fallimenti hardware, condizioni di alto carico ed implementazioni incorrette. I routers possono causare **problemi considerabili se essi falliscono la loro operatività in prossimità di punti di congiunzione** sulla rete. Il migliore protocollo di routing è spesso quello che ha resistito più tempo. I protocolli di routing devono **sopportare molteplici varietà di condizioni** sulla rete.
RAPIDA CONVERGENZA- I routing protocols **devono convergere** rapidamente. La convergenza è la velocità e l'abilità di un gruppo di periferiche di rete che stanno facendo girare uno specifico protocollo di routing, di **unificarsi alla nuova tipologia** per quanto riguarda il cambiamento che si è verificato sulla stessa. **Cambiamenti** della tipologia di rete **causeranno problemi di routing**,per cui alcuni routers **non si renderanno disponibili** sul percorso. Quando ciò accade i **routers distribuiscono l'update** di routing tramite messaggi che vengono inviati sulla rete**.** Ne deriva **un ri-calcolo della route** ottimale; Ogni router aderisce a questa decisione. I protocolli di routing che provocano un rallentamento nella convergenza, possono causare il routing loop o inconsistenza sulla rete.
FLESSIBILITA': I protocolli di Routing devono anche essere **flessibili**. In altre parole, essi devono essere rapidamente ed accuratamente **adatti ad una serie di circostanze** di rete. Per esempio, ipotizziamo che un segmento di rete è andato giù. Molti protocolli di routing selezionano rapidamente il miglior percorso per tutti i routers che normalmente usano un determinato segmento. I protocolli di routing possono essere programmati per adattarsi ai cambiamenti sulla rete, per quanto riguarda la Banda, la dimensione delle queue, il delay ed altre variabili.

Il Routing Loops: Ipotizziamo il caso del routing Loop. Un pacchetto arriva al router 1, tramite una T1. Il router 1 è stato updatato e sa che il miglior percorso per la destinazione rimanda al router 2, che è il prossimo hop. **Il router1 quindi forwarda il pacchetto al router2**, il router **2 non è stato updatato** e sa che il prossimo hop è il router 1. Quindi **il router 2 forwarda il pacchetto al router 1**. Il pacchetto **continua a rimbalzare** fino a quando il router 2 riceve l'update o fin quando il pacchetto è forwardato per **il numero massimo di volte** consentito.
Routing protocols differenti hanno **diversi settaggi tipici** per quanto riguarda questo numero massimo consentito.
L'amministratore di rete solitamente **può definire un basso massimo**. Per esempio, IGRP ha un massimo count di hop, di 255, il prorpio default di 100 e solitamente setta 50 o meno.

Routing Statico e Dinamico: I protocolli di routing statico, sono i più Rigidi. L'amministratore di rete **configura le route** statiche prima che il routing abbia inizio. Queste routes non vengono cambiate affinchè non compia questa operazione l'amministratore, manualmente. I protocolli che usano le routes statiche sono semplici da designare. Essi **lavorano bene in situazioni dove il traffico è prevedibile ed il design di rete è semplice**. I sistemi di routing statico **non possono reagire a seguito di cambiamento** nella tipologia di rete, e sono generalmente considerati **inutilizzabili nelle reti moderne.** Oggi giorno il costante cambio delle configurazioni di rete, **richiede quasi sempre il Dynamic Routing**.
I protocolli di routing dinamico,**si aggiustano a seguito di cambiamenti sulla rete**. Questo accade **analizzando updates** di routing in arrivo. Se un messaggio indica che una rete ha subito un cambiamento, il software di routing, **calcola la route per spedire le nuove tabelle di routing** o aggiornamento. Questi messaggi **attraversano la rete**, e chiedono ai routers di **ricalcolare le loro tavole di routing** periodicamente ed in accordo globale.

I protocolli di routing dinamico, possono essere **supplementati** con le **routes statiche** appropriate. Per esempio, un gateway di ultima risorsa può essere **assegnato staticamente** (default gateway). Questo router **crea una posizione di memorizzazione** per tutti i pacchetti che non hanno una corretta ROUTE, garantendo che essi vengano inviati in quella determinata direzione.

Classificazione di Protocolli di Routing: Come già visto in precedenza **la maggior parte dei protocolli di routing possono essere classificati in 3 tipologie** base.

- Distance Vector- Il vettore del routing **determina la direzione, e la distanza di ogni link** sulla rete. Esempi di distance-vector, IGRP e RIP.
- Link-State- (chiamato anche shortest path first), **ricrea l'esatta topologia dell'intera rete** (o quantomeno l'ultima partizione in cui il router è situato). Esempi di routing link-state sono OSPF, IS-IS, e NetWare Link Service Protocol (NLSP).
- Hybrid- **Combinano gli aspetti del link state e del distant vector**.Un esempio di hybrid è EIGRP.

Configurazione del routing: Selezione di un protocollo di routing: Ogni protocollo di routing dev'essere **configurato separatamente**. Per ogni protocollo, è necessario seguire 2 steps basilari.

1) **Creare il processo di routing** con uno dei comandi di routing
2) **Configurare il protocollo** specifico

Come discusso tempo fa, i protocolli "interior", come ad esempio IGRP e RIP, **devono avere una lista di reti specificate** prima che il routing possa iniziare. Addizionalmente a ciò, il processo di routing **rileva gli updates da altri routers** su queste reti e fa un broadcast di queste informazioni. IGRP ha requisiti addizionali; **E' necessario specificare un numero relativo a sistemi\a autonomo**.

Con ogni protocollo di ip routing, è necessario **creare i processi di routing**, associare le reti con questi processi e customizzare i protocolli di routing per reti particolari. **Scegliere quindi un routing protocol** per completare il Task. Quando si sceglie un protocollo di routing, è necessario considerare:

- **Dimensione della rete** e complessità
- **Livello di traffico** sulla rete
- **Sicurezza** necessaria
- **Affidabilità** necessaria
- Caratteristiche di **ritardo** della rete
- **Policies** aziendali
- Accettazioni di eventuali **cambiamenti sulla struttura** aziendale.

Metric IGRP: IGRP è un protocollo proprietario cisco, e fu creato dopo RIP. IGRP è un distance-vector, interior routing protocol. I protocolli Distance-vector **cercano gli altri router per inviare loro tutta o parte della loro tavola di routing, in messaggi di update, inviati ad intervalli regolari**, SOLO ai router nelle vicinanze. L'informazione di routing attraversa la rete, **i router possono calcolare le distanze** di tutti i nodi all'interno della rete. IGRP utilizza una **combinazione di METRICS**. Il **ritardo** di rete, la **banda**, l'**affidabilità** ed il **carico** sono tutti fattori di decisione routing. Gli amministratori di rete, possono determinare i settaggi per oguno di questi metrics. IGRP utilizza i settaggi determinati dell'amministratore per quanto riguarda banda e ritardo per calcolare automaticamente la migliore Route.

IGRP fornisce **un vasto range di metrics**. Per esempio, l'affidabilità ed il carico possono rientrare nel range da 1 a 255. La banda può assumere valori che vanno da 1200bps fino a 10Gbps. Il ritardo

può quotarsi da 1 a 224. Questi range di metrics, molto vasti, permettono un **settaggio adeguato** delle **metric** stesse, in reti con **varie caratteristiche**, per quanto riguarda la **performance**. Logicamente, gli **amministratori** di rete possono **influenzare la selezione delle route** con scelte intuitive. Ciò è effettuato andando a **variare ognuna delle 4 metrics**. Viene dato al router **un valore per ogni metric**. I valori di default relativi ad IGRP **danno molta importanza alla banda**, ciò rende **IGRP superiore a RIP**. In contrasto, **RIP non ha bisogno di configurare metrics**, esso funziona solo con gli hop count.

Differenza fra Interior Routing ed Exterior Routing: L'obiettivo primario di cisco, nella creazione di IGRP fu fornire un **protocollo robusto** per il routing all'interno di sistemi autonomi. Un sistema autonomo è un gruppo di rete sotto un **comune amministratore** condividendo una **strategia di routing comune**. IGRP usa una **combinazione di metrics** configurabili dall'amministratore. Queste metrics sono, **Ritardo, Banda, Affidabilità e Carico**. IGRP incorpora 3 tipi di routes: Interior,System e Exterior.
Interior: Avvengono **fra rete subnettate che sono collegate ad un'interfaccia router**. Se ala rete collegata al router non è subnettata, igrp non utilizza le interior routes. In aggiunta, **le informazioni subnet non sono incluse negli updates IGRP**.
System: Si tratta di routes **esistenti nella maggior parte delle reti**, incluse quelle composte da sistemi autonomi. Le system routes **sono trasportate direttamente dall'interfaccia connessa**. Altro routers che usano IGRP forniscono informazioni di system route. Le system route, **non includono informzioni di subnetting**.
Exterior: Sono routes **relative a reti esterne ai sistemi autonomi**, cono considerate **identificativi di gateway** come **ultima risorsa**. Il router sceglie **un gateway come ultima risorsa** da una lista di routes esteriori, che fornisce IGRP. Il gateway come ultima risorsa **è usato se il router non ha una route migliore per il pacchetto** o la destinazione non è connessa alla rete. Se un sistema autonomo ha una o più connessioni ad una rete esterna, **diversi routers possono scegliere differenti exterior routes come gateway di ultima risorsa**.

Sequenza di comandi corretta per abilitare IGRP: Per configurare IGRP è necessario **creare un processo di routing IGRP**. Il comando router è **necessario per implementare IGRP** su un router. Questa sezione descrive i processi che eseguono i router per assicurarsi che altri routers, nelle vicinanze, siano informati ello stato delle reti nei sistemi autonomi. Questi status di report includono la frequenza con cui la tabella di routing (update), è inviata e l'effetto di queste operazioni sulla banda.

Descrizione di tre caratteristiche di IGRP che ne migliorano la stabilità: IGRP fornisce un numero di possibilità che sono designate per garantire la propria stabilità:
HOLDDOWNS: La **route** per una rete può essere **posizionata all'interno di una holddown**. Questo avviene **quando un router apprende che una rete è più distante rispetto a ciò che vi era descritto nelle tabelle di routing**, oppure **apprende la la stessa rete è Down**. Durante il periodo HoldDown, **la route è ridistribuita**. Di conseguenza informazioni che vengono trasmesse da altri router **riguardanti il vecchio metric, sono ignorate**. Questo meccanismo è spesso usato per **evitare i routing loops**, sulla rete. Ciò non ha effetto **sull'incremento del tempo di convergenza** sulla tipologa di rete.
Gli holdDowns sono usati per **prevenire messaggi di update irregolari atti a ristabilire vecchie route non più attive (fallite)**. Quando **un router va giù**, i routers nelle vicinanze **rilevano** ciò, tramite **la mancanza totale di comunicazione per quanto riguarda l'invio di updates**. Quindi calcolano **la nuova Route** ed inviano messaggi per informare gli altri router nelle vicinanze del cambio di route. Questa attività inizializza un'ondata di updates che vengono filtrati dalla rete. Questi updates (triggered) non arriva instantaneamente ad ogni periferica di rete. E' possibile per

una periferica (A) di inviare un messaggio di update ad una seconda periferica (B) indicando la route indicando la risorsa che è andata Giù.
HoldDowns **dice ai router di ignorare (hold down) ogni cambiamento che affligge le route in un determinato periodo di tempo**. Il perdiodo holddown è solitamente calcolato per essere maggiore del periodo necessario per l'update dell'intera rete con il cambio di rete. Ciò può prevenire i loop di routing causati da una lenta convergenza.
Split Horizons: uno split horizon si **verifica quando un router cerca di mandare indietro un'informazione su una route nella direzione da cui è venuta**. Per esempio consideriamo un grafico in cui il router1 inizialmente dichiara di non avere route per la rete A. Come risultato non ci sono ragioni, per il router 2 di includere questa route back al router 1, poiché router 1 è lontano dalla rete A. La regola dello split horizon dice che il router 2 deve bloccare questa route da ogni update che manda al router 1. La regola Split-horizon aiuta a prevenire i routing loops.
Per esempio consideriamo il caso in cui il router1 è interfacciato con la rete A e va giù. Senza lo split horizons, il router 2 continua a sapere che il router 1 può collegarsi alla rete A. Se il router 1 non ha sufficiente intelligente, esso può scegliere il route 2 come selezione alternativa, da ciò ne deriva un routing loop. Sebbene holdDown sia sufficiente a prevenire questo problema, si preferisce usare Split Horizons, perfezionato ed implementato in IGRP, per fornire extra stabilità al protocollo. Split Horizons deve prevenire i routing loops, fra routers adiacenti.
POISON REVERSE UPDATES: I posion reverse update sono intesi come **soluzioni per i routing loops**. **Un incremento esagerato del metrics nel routing, generalmente indica un routing loops**. Posion reverse update, geeralmente sono inviate per **rimuovere la route e posizionarla in holddown**. Un router **"avvelena" (posion) la route, inviandogli un update con un metric infinito**. Questo rende **la route irraggiungibile** dal router che originariamente ha acquisito dale route dalla rete. Il posioning **può incrementare la velocità di convergenza**.

Metrics IGRP ed updates: IGRP usa **diversi tipi** di informazioni metriche. Per ogni percorso passante **attraverso sistemi autonomi**, igrp registra il **segmento con minor ritardo** e\o carico, e con la maggior affidabilità e disponiblità di banda.
Mentre viene calcolato il miglior percorso **la banda è un valore molto importante** ed altre variabili sono utilizzate per far pensare ogni metric. Per una rete caratterizzata da un media singolo, come quelle tipicamente usate da tutte le ethernet,ci si riduce al singolo hop count per la valorizzazione in metrics.
Per esempio in un mix di ethernet e linee seriali, da 9600 baud a t1, la route con il più basso metrics, propone il percorso più desiderabile per la destinazione.
Un router sul quale sta girando IGRP, invia IGRP updates via broadcast ogni 90 secondi. Esso dichiara una route invalida o inaccessibile se non riceve un update dal primo router della route entro il periodo di update ripetuto 3 volte (270 secondi). Dopo un periodo pari a 6 volte quello di update (630 secondi), il router rimuove la route dalla propria tabella di routing. IGRP utilizza **il Flash update e il "posion reverse" per aumentare la velocità del processo di convergenza** del protocollo del protocollo di routing. Un **flash update**, consiste **nell'inviare un update più presto rispetto al periodo standard relativo all'intervallo prestabilito in cui vengono notificati eventuali cambi o update** sulle tavole di routing. I **"posion reverse updates**" sono intesi come default **routing loop di grandi dimensioni** che sono causate dall'ingremento di metrics. Gli updates "posion reverse" sono inviati per **sposare una route e posizionarla in holddown**.Holddown impedisce l'utilizzo delle nuove informazioni di routing per un certo periodo di tempo.

Il massimo conteggio degli HOP in IGRP: IGRP può **contare gli hop per un massimo di 255**. Il settaggio di default è 100.Poiché IGRP utilizza triggered (flash) updates, il conteggio a 100 può non essere troppo lungo. Il massimale per quanto riguarda gli hop, **dev'essere quanto più basso possibile**, a meno che non vi sia una rete grande. Esso **dovrebbe essere un numero largo quanto il**

massimo numero di routes che è possibile compiere attraverso la rete. SE IGRP routing è scambiato con una rete esterna il conteggio degli hop include sia i passi interni che quelli esterni. Quando si fa il conto dei salti (dei router), bisogna considerare cosa accadrebbe alla configurazione se un paio di linee andassero giù.Qui c'e' un esempio di router che usa tutte le caratteristiche spiegate in questa sezione:

Il Numero di rete 10.0.0.0 in questo caso è usato come esempio:

Router(config)# **router igrp 46**
Router(config-router)# **timers basic 15 45 0 60**
Router(config-router)# **network 10.0.0.0**
Router(config-router)# **no metric holddown**
Router(config-router)# **metric maximum-hop 50**

With this statement, routing generally adapts to change within 45 seconds. This is assuming that the keepalive interval, which is the period of time between messages sent by a network device, has been set to 4.

Access Control Lists (ACLs)

Che cosa sono le ACLs: Le acls sono **lista di istruzioni** o regole che è possibile applicare ad un'**interfaccia** router. Queste liste dicono al router **che tipo di pacchetto accettare e che tipo di pacchetto rifiutare**. L'accettazione o il rifiuto possono essere basati su **specifiche** particolari, come ad **esempio indirizzo di destinazione, e numero di porta**. Le ACLs sono usate per **gestire** il traffico e scannare specifici pacchetti applicando ACL ad un'interfaccia router. Il traffico passante per quella determnata interfaccia è testato e **comparato con le condizioni** definite nella ACL. Le ACLs possono essere **create per tutti i routed protocols**, come ad esempio IP, o ipx, per il filtraggio dei pacchetti che passano attraverso interfacce router. Le ACLs possono essere **configurate sul router** per controllare l'accesso alla rete o ad una determinata subnet. Per esempio nella scuola di washington, dev'essere usata una ACL per impedire che il traffico degli studenti influisca la rete amministrativa. ACLs filtrano il traffico, controllando i pacchetti che possono essere forwardati e quelli che devono essere bloccati verso una determinata interfaccia router. Il router esamina ogni pacchetto, per **determinare se forwardarlo o deletarlo**, basandosi **sulle condizioni** specificate nella ACL. Le condizioni ACL devono essere l'indirizzo sorgente, l'indirizzo di destinazione, informazioni relative al protocollo di livello superiore ed altro ancora..
Le ACLs devono essere defintite su "per-protocol basis". E' necessario **definire ACL per ogni protocollo abilitato** sull'interfaccia, se si vuole controllare globalmente il traffico globale della stessa. Molti protocolli si riferiscono alle ACL come "filtri". Per esempio se la nostra interfaccia router dove è configurato ip, appletalk e ipx dev'essere controllata, è **necessario definire** almeno TRE ACLs. Acls possono essere usate **come strumento per il controllo** della rete, aggiungendo **flessibilità nel filtraggio** dei pacchetti che affluiscono dentro e fuori ad un'interfaccia router.

Motivi per la creazione di ACLs: Ci sono **molte ragioni per creare ACLs**. Per esempio le ACLs possono essere usate per:

- **Limitare il traffico** sulla rete ed incrementare le performance di rete. Per esempio ACLs possono specificare che **un certo tipo di pacchetto debba essere processato dal router prima di tuttti gli altri**, sulla base del protocollo. Questo fenomeno è riferito al **Queuing,** garantendo che il router non processi i pacchetti che non sono necessari. Dunque la queuing regola il traffico di rete e controlla la congestione.

- **Fornisce il controllo del traffico**. Per esempio, ACL **può applicare restrizioni**, o **ridurre** il **contenuto degli updates di routing**. Queste restrizioni sono usate per **limitare le informazioni su una specifica rete,** per evitarne quindi la propagazione su altre reti.
- Fornisce **un livello base di sicurezza per accesso alla rete**. Per esempio ACL può **permettere ad un host** di accedere ad una parte della rete e **impedire** ad altri host, la stessa cosa, per la stessa area. HOST a è accettato per quanto riguarda l'accesso ad "human resources" network, mentre host B non può accedervi. Se non si configurano le ACL sul router, tutti i pacchetti che passano attraverso il router possono transitare sulle parti e su tutte le reti collegate ad esso.
- Decide che tipo di traffico **dev'essere forwardato o bloccato** ad una **determinata interfaccia** router. Per esempio è possibile permettere al traffico email di essere routato, ed al traffico telnet di essere bloccato.

Test dei pacchetti con ACLs: **L'ordine in cui si posizionano le statements ACL è molto importante**. Quando il router deve se **forwardare o bloccare** un pacchetto, il software IOL, testa i pacchetti e li **confronta con le condizioni** imposte nelle ACL (**statements**), nello stesso ordine in cui esse sono state create.
E' importante sapere che, **se viene rilevata una coincidenza** nelle statements, **non ne vengono ricercate e controllate altre**.
Logicamente, se si creano delle condizioni di statement in cui tutto il traffico è permesso, **nessuna statement successiva** sarà verificata.
Se si necessitano di **Statements addizionali**, è necessario **deletare l'acl** precedente e **ricrearla** con le **nuove condizioni**. Inoltre è una buona idea editare la configurazione del router, usando un text editor su un pc, e quindi inviare essa al router grazie al TFTP.
E' possibile creare **ACL per ogni protocollo** che si vuole **filtrare**, **su ogni interfaccia** router. Per diversi protocolli è possibile **creare una ACL dedicata al filtraggio** del traffico in entrata ed una ACL per il filtraggio del traffico in uscita.

Come lavora ACLs: Una Acl è **un gruppo di statements** che definisce come I pacchetti:
- **Entrano** in un'interfaccia
- Passano **attraverso** il router
- **Escono** da una interfaccia.

L'inizio del processo di comunicazione è un qualcosa che **resta invariato**, sia che si utilizzino le ACL sia che non si utilizzino. Un pacchetto entra passando per una determinata interfaccia, il router verifica **se il pacchetto è Routable oppure bridgeable**. Il router **successivamente** controlla **se l'interfaccia** sul quale il pacchetto è entrato **ha una ACL**. Se ne esiste qualcuna, il pacchetto è di nuovo **testato e paragonato alle condizioni presenti** all'interno della lista. Se il pacchetto è benvenuto, esso è **contrllato nelle tabelle di routing** per determinarne l'interfaccia di destnazione. Il router verifica se l'interfaccia di destinazione ha una ACL. Se non esiste alcuna acl, il pacchetto può essere inviato direttamente all'interfaccia. Gli **statements acl operano in ordine di sequenza** logica. Se una condizione coincide con quella interna del pacchetto, esso è accettato o rifiutato, ed **il resto delle statements acl non sono verificate**. Se il pacchetto non coincide internamente con nessuna delle acl, ma la acl finale è scritta per negarne il passaggio, il pacchetto non passerà.

Controllo di Flusso e test su ACLs: Se a seguito di un test con la prima ACL del gruppo, il pacchetto **trova coincidenza** con le statement inserite nella stessa ACL, esso **viene accettato o rifiutato**. Esso è scartato e lanciato nel "bit bucket", e non esposto ad test ACL successivi.
Se il pacchetto **non trova coincidenza** con il primo test, **esso passa al controllo sulla prossima** statement all'interno della ACL.

ACLs ci permettono di controllare quali client possono accedere alla nostra rete. Le condizioni nel file ACL possono essere:

- Stabilire se certi host **possono accedere o meno ad una parte della rete**.
- Garantire o negare il **permesso a certi tipi di servizi o traffico**, come ad esempio FTP o HTTP.

Creazione ACLs: In pratica, i comandi ACL possono espressi **lungo sequenze di caratteri**. Le operazioni chiave per la creazione della ACLs sono le seguenti:

- Si crea ACLs utilizzando la modalità di configurazione globale.
- Specifica **un numero ACL da 1 a 99**, istruisce il router ad **accettare gli statements standar ACL**. Specificare **un numero ACL da 100 a 199 istruendo il router ad accettare le statements estese acl**.
- E' necessario selezionare **attentamente e logicamente l'ordine delle ACL**. Gli ip **protocols permessi devono essere specificati.** Tutti gli altri dovrebbero essere ristretti.
- Si dovrebbe scegliere **quali protocolli ip**, verificare. Gli altri protocolli non sono verificati. Più tardi, nella procedura, è possibile anche **specificare una porta** di destinazione opzionale per avere una precisione maggiore.

  Raggruppare le ACLs ad interfacce: Ogni protocollo ha il proprio set di tastks e regole specifiche che sono necessarie per il filtering del traffico. Comunque, in generale, molti protocolli, necessitano di 2 steps base. Il **primo step** è creare una **definizione** ACL. Il **secondo step** è **applicare l'ACL all'interfaccia.**

  Le ACLs sono assegnate **ad una o più interfacce**. Esse possono filtrare il traffico **in ingresso o quello in uscita** in relazione alla configurazione. Le ACLs settate in **Uscita sono più efficenti di quelle in entrata**, e sono sempre preferite. Un router con ACLs inbound devono verificare ogni pacchetto per vedere se esiste una coincidenza con la condizione ACL prima di effettuare lo switching all'interfaccia esterna.

  Assegnare un numero unico ad ogni ACL: Quando si configura le ACLs su un router, è necessario identificare ogni ACL unicamente **assegnando un numero alla ACL** per protocollo. Quando si usa **un numero di identità come ACL**, questo numero deve rientrare nel **range** specifico di numeri validi per il protocollo.

  Dopo aver creato una ACL numerata, è possibile **assegnare essa ad un'interfaccia** per essere utilizzata. Per alterare una ACL numerata è necessario **deletare tutte le statements all'interno dell'ACL**. Ciò è eseguito utilizzando il comando "no access-list (numero lista)".

La funzione WildCard Mask Bits: Una wildcard mask è un numero di 32 bit diviso in 4 ottetti, ognuno dei quali contiene 8 BITS. Un **bit 0 vuol dire "controlla il valore del bit corrispondente**", un **bit 1, vuol dire "non controllare, o oginorare**" il valore del bit corrispondente.

Un wildcard mask è comparabile ad un indiriszzo ip. I numeri 1 e 0 sono usati per identificare come trattare il bit del corrispondente indirizzo ip. **Le ACLs utilizzano il wildcard masking per identificare un singolo o multiplo indirizzo per permettere o** negare i tests**. Il termine "wildcard masking" è un nickname per il processo di ricerca delle coincidenze nelle ACLs. Esso deriva dall'analogia delle wildcard che trovano coincidenza con tutte le altre carte nel gioco del poker. Benchè siano entrambi strutturati su una base di 32 bit, lo wildcard mask ed il subnet mask ip operano differentemente. Lo 0 e l'1 nel subnet mask determinano la rete, la subnet e la porzione di host dell'indirizzo ip corrispondente. Lo 0 e l'1 nello wildcard determina se il bit corrispondente dell'indirizzo ip dev'essere controllato o ignorato dai propositi ACL.** Il bit 0 in una ACL wildcard mask, fa in modo che ACL controlli il corrispondente bit, nell'indirizzo ip. Il bit 1 nella ACL wildcard mask fa in modo che ACL ignori il corrispondente BIT nell'ip Address**. Esempio: Si vuole testare un indirizzo ip, per cui esso verrà accettato o rifiutato. Ipotizziamo che questo ip sia di classe B e si vuole usare IP wildcard mask bits per permettere a tutti i pacchetti di un determinato host da 172.30.16.0 a 172.30.31.0. Inizialmente lo wildcard mask verifica i primi 2 ottetti (172.30) utilizzando i corrispondenti bit nello wildcard mask, per cui (0). Poiché non esistono interessi sull'indirizzo host individuale (i corrispondenti bit nello wildcard mask non hanno 00), lo wildcard mask ignora l'ottetto finale, utilizzando "1", in corrispondenza alle ottette non interessate. Nel terzo ottetto, lo wildcard mask è 15 (00001111) e l'indirizzo ip è 16 (00010000). I primi 4 "0" nello wildcard mask (0000), dicono al router di accettare le prime 4 cifre dell'indirizzo ip (0001). Poiché gli ultimi 4 bits sono ignorati, tutti i numeri facente parte del range da 16 (00010000) a 31 (00011111), saranno accettati poiché essi iniziano per 0001. Per i 4 bit finali nell'ottetto, il wildcard mask, ignore il valore poiché in queste posizioni, il valore dell'indirizzo può essere binario 0 o binario 1, ed il bit corrispondente nello wildcard mask è 1. In questo esempio, l'indirizzo 172.30.16.0 con lo wildcard mask 0.0.15.255 permette il passaggio delle subnets di range da 172.30.16.0 a 172.30.31.0. Lo wildcard mask non corrisponde ad ogni altra subnet.**

Il comando ANY: Lavorare con la rappresentazione decimale del wildcard mask bit **può essere noioso**. Per l'utilizzo più comune dello wildcard masking**, è possibile usare delle abbreviazioni**. Queste **abbreviazioni riducono l'ammontare di testo che bisogna inserire** quando si configurano le condizoni di test (statements). Per esempio, se si vuole specificare che **ogni indirizzo di destinazione sarà permesso sul test ACL, bisogna indicare tutti gli indirizzi** address..Per cui specificare 0.0.0.0, quindi per indicare quale acl si vuole ignorare (benvenuta senza alcun checking), il corrispondente wildcard mask per questo indirizzo deve avere tutti "1", quindi 255.255.255.255. E' possibile **usare l'abbreviazione Any per comunicare questa stessa condizione** di test al cisco ACL software. Invece di digitare 0.0.0.0 255.255.255.255, è possibile usare il termine ANY direttamente da tastiera.

Per esempio, invece di usare:
Router(config)# **access-list** 1 permit 0.0.0.0 255.255.255.255
E' possibile usare:
Router(config)# **access-list** 1 permit any

Il comando HOST: Un'altra condizione comune in cui il cisco IOL permette abbreviazioni nella ACL wildard mask è quando si vuole fare **una verifica di tutti i bit dell'intero indirizzo** host. Per esempio, se si vuole **specificare che uno specifico indirizzo host sarà** accettato dall'acl test. Per indicare un indirizzo host, è necessario **inserirlo per intero**, esempio 172.30.16.29. Quindi indicare che **ACL deve verificare tutti i bit nell'indirizzo**, ed il **wildcard mask corrispondente** per questo

indirizzo sarà 0.0.0.0. E' possibile utilizzare il comando abbreviato "host" per comunicare questa stessa condizione di test per il cisco IOS ACL software.

In questo esempio, digitando 172.30.16.29 0.0.0.0, è possibile utilizzare il termine **host** prima dell'indirizzo.

Anziché usare:
Router(config)# **access-list** 1 permit 172.30.16.29 0.0.0.0
E' possibile usare:
Router(config)# **access-list** 1 permit host 172.30.16.29

Che cosa sono le ACLs Standard: E' possibile utilizzare **ACLs standard** quando si vuole bloccare \ accettare **tutto il traffico proveniente da una rete**, o negare suites di protocolli. Gli ACLs standard controllano **l'indirizzo sorgente dei pacchetti** che devono essere Routati. Il risultato permette o nega l'accesso in uscita **per un'intera suite di protocollo**, basandosi sulla rete, sulla subnet e sull'indirizzo host.
Per esempio i pacchetti provenienti dalla E0 sono controllati per quanto riguarda il loro indirizzo sorgente ed il protocolli. Se essi sono permessi, avviene il loro smistaggio presso S0, che è inserita nella ACL. Se non sono permessi, vengono scartati.

Scrivere un comando ACL valido utilizzando tutti i parametri disponibili: Come precedentemente appareso, è possibile usare la versione standard del comando di configurazione globale per le "access-list" per definire **una ACL standard con un numero**. Questo comando è usato in modalità di configurazione globale.
La sintassi è:

Router(config)# access-list*access-list-number* {**deny** | **permit**} source [source-**wildcard**] [**log**]

E' possibile utilizzare il "no" per rimuovere l'ACL standard:

Router(config)# no access-list *access-list-number*

Come verificare le Access Lists: E' possibile usare il comando esecutivo **"show access-lists"** per **visualizzare il contenuto di tutte le ACLs**. In aggiunts si usa il comando esecutivo "show access-list" seguito dal NOME o Numero della ACL per visualizzarne il contenuto. L'esempio seguente di ACL, permette l'accesso per gli hosts su 3 reti specifiche:

access-list 1 **permit** 192.5.34.0 0.0.0.255
access-list 1 **permit** 128.88.0.0 0.0.255.255
access-list 1 **permit** 36.0.0.0 0.255.255.255

Tutti gli altri accessi sono Implicitamente negati.
In questo esempio gli WildCardBits vengono applicati alla porzione host dell'indirizzo di rete. Ogni host con un indirizzo sorgente che non coincide con le statements ACL sarà respinto. Per specificare **un ampio numero di indirizzi individuali più fcilmente, è possibile omettere lo wildcard se esso è composto da tutti 0.** Dunque i comandi della configurazione numero 2 avranno lo stesso effetto:

access-list 2 **permit** 36.48.0.3
access-list 2 **permit** 36.48.0.3 0.0.0.0

Il comando “ip access-group” assegna un’ACL esistente ad un’interfaccia. C’è da ricordare che solo una ACL per porta,per protocollo, per direzione, è consentita. Il formato del comando, è il seguente:

Router(config-if)#**ip access-group** access-list-number {**in** | **out**}

Scrivere un comando ACL per consentire il traffico da una rete: In questo esempio, il comando ACL **permette il forward** del solo il traffico dalla rete sorgente 172.16.0.0. Il traffico da reti non facenti parte della 172.16.00, è automaticamente bloccato. Come visto in questo esempio,inoltre, il comando “ip access-group 1 out”, applica l’acl all’interfaccia in uscita.

access-list 1 **permit** 172.16.0.0 0.0.255.255

Implicitamente ogni altro indirizzo è bloccato:

(access-list 1 **deny** 0.0.0.0 255.255.255.255)
interface ethernet 0
ip access-group 1 **out**
interface ethernet 1
ip access-group 1 **out**

Scrivere un comando ACL per negare l’accesso ad un host specifico: L’esempio seguente mostra come una ACL è designata per **bloccare il traffico** proveniente da un indirizzo specifico, 172.16.4.13, e permette a tutto il resto del traffico di essere forwardato sull’interfaccia ethernet 0.
Il comando “access-list” utilizza il parametro deny per impedire il traffico ad un host identificato.
L’address mask 0.0.0.0 richiede che il test coincida con tutti i bits.
Nel secondo comando Access-list il 0.0.0.0 255.255.255.255 la combinazione ip address\wildcard mask, identifica il traffico proveniente **da ogni sorgente**. Questa combinazione può anche essere scritta **con il comando “any”**. Tutti gli 0 nel campo indirizzo, indicano **una posizione di accettazione**, e tutti gli 1 nello wildcard mask indicano che tutti i 32 bits non verranno controllati nell’indirizzo sorgente (respinti).
Ogni paccheto che non trova una coincidenza (match) nella prima linea ACL verrà passato **all’analisi ed alla comparazione della seconda linea**. Se troverà coincidenza potrà essere forwardato.

Ecco come si nega l’accesso ad un host specifico:

access-list 1 **deny host** 172.16.4.13 0.0.0.0
access-list 1 **permit** 0.0.0.0 255.255.255.255

Implicitamente
(**access-list** 1 **deny** 0.0.0.0 255.255.255.255)

interface ethernet 0
ip access-group 1 **out**

Scrivere un comando ACL per negare l’accesso ad una specifica Subnet: L’esempio mostra come **ACL è designata per il blocco del traffico** proveniente da una subnet specifica, 172.16.4.0, e permette a tutto il traffico di essere forwardato. Notare che lo wildcard mask è 0.0.0.255. **Gli “0” nelle prime 3 ottette, indicano che tali bit saranno testati per riscontrare** una coincidenza, mentre l’ultimo ottetto, **composto solo da “1”, indica di non preoccuparsi** della condizione della cifra relativa all’ultimo ottetto dell’indirizzo ip (porzione host), per trovare eventuali coincidenze.

Notare che l'abbreviazione ANY è usata per l'indirizzo ip della sorgente:
Ecco come negare l'accesso ad una specifica subnet..
access-list 1 **deny**) 172.16.4.0 0.0.0.255
access-list 1 **permit any**
I
Implicitamente viene negato l'accesso ad ogni altro host:
(**access-list** 1 **deny any**)

interface ethernet 0
ip access-group 1 **out**

Che cosa sono le "extendeed ACLs": Le ACLs estese sono usate molto spesso per **testare le condizioni** pochè essi **forniscono un grande range** di controlli rispetto alle standard ACLs.
Le ACL estese sono usate per **permettere traffico web** ma **negare il traffico ad FTP o TELNET** da parte di una compagnia non facente parte della rete. Le ACL estese controllano **sia L'indirizzo sorgente che quello di destinazione** del pacchetto.
Essi possono anche controllare **per specifici protocolli**, **numeri di porta ed altri parametri**. Questo da molta flesibilità per descrivere che cosa ACL dovrà controllare. I pacchetti possono essere **accettati o rifiutati** basandosi su Dove il pacchettè è stato creato sulla destinazione prefissata. Per esempio l'extended ACL può **permettere traffico** Email dalla E0 alla specificata destinazione su S0, mentre blocca i logins remoti o i file transfers.
Possiamo supporre che all'interfaccia E0 è stata applicata una ACL estesa, create da **precise statements logiche**. **Prima che un pacchetto possa processato da tale interfaccia, esso è testato dall'ACL** associata con tale interfaccia.
Basandosi sul test dell'ACL estesa, il pacchetto può essere **accettato o rifiutato**. Per i bit in entrata, i pacchetti **continueranno con il percorso e saranno processati**. Per i bit in uscita, i pacchetti saranno **inviati direttamente all'interfaccia** E0. Se a seguito del test ne deriva una negazione di permesso, il pacchetto sarà Scartato. Il router ACL **fornisce controllo firewall** per negare l'uso dell'interfaccia E0. Quando i pacchetti **sono scartati**, diversi **protocolli re-inviano il pacchetto all'inviatario**, facendo sapere ad esso che la destinazione **non è raggiungibile**.
Per una singola ACL, è possibile **definire numerose statements**. Ognuna di queste statements deve fare referenza **allo stesso identificativo**, per quanto riguarda **il nome o numero**, per **legare le statements alla stessa ACL**.
E' possibile stabilire ed utilizzare **numerose condizioni secondo vari statements**, **limitandosi** solo alla **memoria** disponibile. Naturalmente, **più stantments** si hanno, più **difficile** sarà **comprendere e gestire le ACL**. Perciò è consigliabile **documentare le ACLs** al fine di prevenire confusione.
Le ACLs standard (numerate da 1 a 99), possono non fornire il controllo e filtraggio del traffico necessario. Le **ACL standard** si basano **sull'indirizzo sorgente e sul mask**. Le ACLs standard permettono inoltre di negare l'accesso all'intera suite IP. **Manca** quindi la possibilità di avere un controllo **più preciso** sul traffico e sugli accessi.
Per filtraggio e controllo del traffico **più preciso** è necessario usare le **Extended ACLs**. Lo statement delle Extended ACL controlla **l'indirizzo sorgente e quello di destinazione**. In aggiunta alla fine dell'acl ext statement, si può avere **maggiore precisione** grazie ad un campo che specifica **l'optional TCP o UDP ed il numero di protocollo**. Queste sono conosciute come **porte TCP\IP**.
E' possibile specificare le **operazioni logiche** che le ext acl eseguiranno su protocolli specifici. Le EXT acls, utilizzano un numero nel range da 100 a 199.

Parametri per ACL estese: Per completare il comando access-list, si usano i seguenti comandi:

Router(config)# **access-list** *(Numero access list)* {**permit**| **deny**} *protocol indirizzo sorgente mask-sorgenteindirizzo destinazione mask di destinazione* [*operator port*] [**established**]

Il comando **"ip access-group"** serve per **associare una ext acl ad un'interfaccia**. Ricordarsi che è possibile avere una ACL per interfaccia, per protocollo ed una per direzione. Il formato del comando è il seguente:
Router(config)# **ip access-group(numero di access list)** { **in**| **out**}

Numeri di porte TCP e UDP: L'indirizzo di sorgente e destinazione e lo specifico protocollo che utilizza le extended access lists, devono essere **identificati con un numero** il cui **range** dev'essere da **100 a 199** In aggiunta dev'essere definito **un livello superiore ed un numero di porta TCP ed UDP** per test ulteriori relativi alla stessa EXT ACL, c'è la necessità quindi di **assegnare un'identificazione**, con un numero che ha un range da **100 a 199**. Molte porte UDP e TCP sono riservate.

Scrivere ACL per negare conessioni FTP su un'interfaccia Ethernet: Ecco un esempio di EXT ACL che blocca il traffico FTP.
Il comando Interface **E0 "access-group 101",** applica **l'acl 101 all'interfaccia in uscita E0**.
Notare che **bloccando la porta 21** si previene comando di trasmissione **FTP** per cui trasferimenti FTP.
Bloccando la porta 20 si impedisco al traffico di essere trasmesso, ma non si blocca il traffico per quanto riguarda i comandi FTP. Gli ftp servers possono essere configurati con faclità per **lavorare su porte differenti**. Si deve conoscere le porte più conosciute in modo da bloccarle, per la sicurezza. **Non ci sono garanzie** che però il servizio verrà proposto su queste porte, che solitamente vengono usate.

Access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
Access-list 101 permit ip 172.16.4.0 0.0.0.255 0.0.0.0 255.255.255.255
Il deny implicito:
(access-list 101 deny ip 0.0.0.0 255.255.255.255 0.0.0.0. 255.255.255.255)
interface ethernet 0
ip access-group 101 out

Scrivere una ACL per negare l'accesso in uscita con TELNET su una porta ethernet e permettere tutto il resto del traffico: Questo esempio invece, nega il traffico sulla porta 23 dall'indirizzo ip 172.16.4.0 inviato fuori sull'interfaccia E0. Tutto il traffico che proviene da altre sorgenti o destinazione, è permesso, come indicato dalla parola chiave any. L'interfaccia E0 è configurata con il comando access-group 101 out. Questa è l'acl 101 cpplicata all'inrfaccia uscente E0. Ecco come negare solo le telnet da E0, e permettere tutto il resto del traffico:

access-list 101 **deny** tcp 172.16.4.0 0.0.0.255 any eq 23
access-list 101 **permit** ip any any
(implicito deny any)
(**access-list** 101 **deny** ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)
interface ethernet 0
ip access-group 101 **out**

Configurare "named ACLs": Le Named ACLs permettono a standard ed estese ACL ip **di essere identificate con stringhe alfanumeriche (nomi).** Possono essere ANCHE **rappresentati con la numerazione (1-199)**. Le Named ACLs possono essere usate per **cancellare entries individuali** da

una specifica ACL. Questo ci permette di **modificare la nostra ACL senza cancellarla** e quindi ricrearla. Si useranno le Named ACL quando:

- Si vuole **intuitivamente identificare** le ACLs utilizzando un nome alfanumerico
- Si hanno **più di 99 standard e 100 estese**. Le ACLs devono essere configurate in un router per poi essere assegnate ad un protocollo.

Esistono tuttavia degli **SVANTAGGI** nell'utilizzo delle Named ACL:

- **Non sono compatibili** con le releases Cisco prima della 11.2
- **Non** si può usare **lo stesso nome per ACLs multiple**. Neanche ACLs di tipi differenti possono avere lo stesso nome. Per esempio, è illegale specificare una ACL standard "george" ed una ext ACL con lo stesso nome "george". E' una cosa non possibile.

Per dare un nome alla ACL usare i seguenti comandi:

Router(config)# **ip access-list** {**standard** | **extended**} nome

Nella modalità di configurazione ACL, specificare **una o più condizioni permesse o rifiutate**. Questo determina quando i pacchetti passano oppure vengono scartati:
Router(config)# **deny** {source [source-wildcard] | **any**}
oppure
Router(config)# **permit** {source [source-wildcard] | **any**}.
The configuration shown in the Figure creates a standard ACL named Internetfilter and an extended ACL named marketing_group .

Il comando DENY: Utilizzare il comando "deny" ACL configuration per **settare le condizioni** per una Named ACL. La sintassi completa per questo comando è:

Router(config)# **deny** {source [source-wildcard] | **any**}

Si usano "no" in aggiunta a questo comando, per rimuovere una condizione DENY usando la seguente sintassi:
Router(config)# **no deny** {*source* [source-wildcard] | **any**}

Il comando PERMIT: Usare il comando di configurazione **access-list "permit"** per **settare le configurazioni per un Named ACL**. La sintassi completa di questo comando è la seguente:
Router(config)# **permit** {source [source-wildcard] | **any**}[**log**]

Usare in aggiunta a questo comando il **"no"** per **rimuovere una condizione da una ACL**, la sintassi per far ciò, è la seguente:
Router(config)# **no permit** {source [source-wildcard]| **any**}

Usare questo comando nella modalità di configurazione delle access lists, con il comando **"ip access-list"** per **definire le condizioni** per cui un pacchetto passa l'ACL
Il seguente esempio è **riferito ad una ACL standard** chiamata **"internetfilter":**

ip access-list standard Internetfilter
deny 192.5.34.0 0.0.0.255
permit 128.88.0.0 0.0.255.255
permit 36.0.0.0 0.255.255.255
(tutti gli altri accessi sono implicitamente negati)

In questo esempio,gli statements relativi ai prmessi ed alle negazioni **non hanno numero e nessuna rimozione di test specifici** dall'ACL nominata:
Router(config {std- | ext-}nacl)# {**permit** | **deny**} {**ip ACL test conditions**} {permit | deny} {ip ACL test conditions} no {permit | deny} {ip ACL text conditions}

Questo esempio attiva le IP NAMED acl, sull'interfaccia:
Router(config-if)# ip access-group {name | 1-199 {in | out}}

Protocolli su cui le ACLs possono essere create: ACLs possono **controllare molti protocolli** sui routers Cisco. Si inserisce **un numero nel protocol** (number range), come **prima cosa**, all'interno dello statement ACL. Il router **identifica quale ACL** software dev'essere usato basandosi su questa entry numerata.
Diverse ACLs sono consentite per un protocollo, selezionando **un numero differente** dal (protocol number range), **per ogni nuova ACL**. Tuttavia **solo una ACL** per **protocollo\interfaccia** può essere specificata. Per **molti protocolli, più di 2 ACLs possono essere graggruppate ed assegnate** ad un'interfaccia: Una ACL in **entrata ed una in uscita**. Con altri protocolli, solo una ACL controlla sia i pacchetti in entrata che quelli in uscita.
Se l'acl è settata all'ingresso, quando il router riceve un pacchetto, il cisco IOS software controlla la condizione delle statement ACL per trovare una riconoscenza valida. Se il pacchetto **è permesso**, il software **continua a processarlo**. Se il pacchetto è **rifiutato** il **software lo scarta** posizionandolo nel "bit bucket". Se l'ACL è settata in uscita, dopo averla ricevuta e routato il pacchetto all'interfaccia esterna, il software **controlla le condizioni ACL** e cerc una coincidenza. Se il pacchettè è permesso, il software lo trasmette finalmente in uscita. Se il pacchetto è rifiutato, il software lo scarta inviandolo nel "bit bucket".

Regola importante: Posizionare l'ACL estesa quanto più vicina possibile alla sorgente del traffico Negato: Le ACLs sono usate per **controllare** il traffico filtrando il pacchetto ed eliminando il traffico non desiderato alla destinazione. Il traffico **non necessario**, passa per la rete, ma può **essere evitato localizzandolo e specificandolo con attenzione ed esattezza nelle ACLs**. Il traffico che sarà negato, verrà **immediatamente bloccato**, per cui la destinazione remota non subità diminuzioni della performance; Non sarà utilizzata.
Supponiamo che una polici d'impresa desidera negare il traffico telnet o ftp ad un router A verso la switched lan sulla porta E1 del router D. Allo stesso tempo, **altro traffico dev'essere permesso**. Molte tipologie di approccio possono aiutarci nel completamento di questa policy. E' solitamente consigliato **utilizzare una Extended ACL.** Essa specifica sia **l'indirizzo sorgente** che quello di **destinazione**. Posizionare quindi, questa Ext ACL sul router A. Quindi i pacchetti che non attraversano la ethernet port sul router A, non passano sull'interfaccia seriale del router B e C, e quindi non entrano sul router D. Il traffico con indirizzi di sorgente e destinazione differenti è permesso.
E' consigliabile inserire le ACLs estese può vicine possibili alla sorgente del traffico che dev'essere negato. Le ACLs **standard non possono specificare l'indirizzo di destazione**, per cui è indispensabile inserire eventuali acl standard quanto più vicine possibili alla destinazione. Per esempio, è possibile posizionare sia una standard che una extended ACL sulla E0 di un router D, per filtrare il traffico sul router A.

Utilizzare ACLs in Firewall Routers: Le ACLs devono essere usate il **"firewall routers"**, che sono spesso posizionati **fra la rete interna e quella esterna**, come ad esempio internet. Il firewall router **fornisce un unico punto di isolamento**. Per cui il resto della rete interna non è affetto da ulteriori filtraggi. Una ALC su un **router** posizionato **fra 2 parti della rete**, può essere usata per **controllare il traffico in uscita ed in entrata da quella specifica parte della internetwork**.

Per fornire i benefici di sicurezza della ACLs, si deve configurare questa acl sulla parte più esterna del router. Queste **parti "esterne"** sono situate **sulle estremità dei routers**. Ciò fornisce una sicurezza base sulla rete uscente, o per una parte meno controllata della rete, in una o più reti private. Su queste estremità dei routers, possono essere **create le ACLs**; Una per ogni protocollo configurato sulle interfacce del router. Le ACLs possono essere configurate **sia per il traffico in entrata che per quello in uscita** o applicate per entrambi le cose, fungendo come un vero e proprio filtro sull'interfaccia.

L'architettura Firewall protegge dalle intrusioni: Un'architettura firewall è **una struttura che esiste fra il mondo esterno e reti private**, per poterle **proteggere** da intrusioni. In **molte circostanze**, gli intrusi **vengono da internet**, e da molte altre migliaia di reti che internet connette. Tipicamente un **Firewall** di rete consiste in **diversi e differenti apparecchi**.
In questa architettura, il router **che è connesso ad internet (exterior router), forza tutto il traffico in ingresso sul gateway** dell'applicazione. **Il router che è connesso alla rete interna (interior router), accetta i pacchetti solo dal gateway** di applicazzione. In effetti il **gateway controlla** lo spostamento dei servizi network-baset, sia all'interno che dell'interno della rete.
Per esempio solo certi utenti hanno la possibilità di comunicare con internet o solo certe applicazioni possono stabilire connessioni fra host interiori ed esteriori.
Se la sola applicazione che è permessa è la mail, solo pacchetti mail saranno accettati e passeranno dal router. Questo protegge il gateway di applicazione ed evita di sopraffarlo con pacchetti non utili, che comunque altrimenti dovrebbe scartare.

Come utilizzare ACLs ed interpretarne l'uscita: Il comando **show ip interface visualizza le informazioni ip relative all'interfaccia su cui sono settate le ACLs**. Il comando **Show access-list visualizza il contenuto di tutte le ACLs**. Inserendo un numero e nome di ACL come opzione per questo comando, è possibile visualizzare una specifica lista.

IPX

La suite del protocollo Novel Ipx: Cisco e novell hanno collaborato **per diversi anni**, per sviluppare e migliorare il networking basato su NetWare. Benchè molti dei protocolli NetWare furono **inizialmente** designati per essere usati **su piccole ed omogenee reti**, cisco ha **aggiunto** delle caratteristiche per **ottimizzare la performance** dei protocolli NetWare in vasti e diversei ambienti.Cisco supporta diverse implementazioni per la suite base di protocolli NetWare. Queste implementazioni sono parte del Cisco operating system **(IOS).**
Novel ha introdotto NetWare nel lontano 1980. NetWare utilizza un'architettura Client\Server.
I Clients, spesso chiamati anche Workstations, richiedono servizi, come ad esempio accesso per File e Stampanti, dal server. Diversamente dalle reti Windows NT, **I server NetWare sono dedicati e non possono essere usati come clients**. NetWare è **una suite proprietaria** di protocolli ed include le seguenti caratteristiche:

- **IPX** è un protocollo di **livello 3**, di tipo **ConnectionLess**, che non necessita di una aknowledgment per ogni pacchetto e definisce i nodi della rete e gli indirizzi.
- Il routing information protocol **Novel (rip),** che è differente dell'IP RIP, facilita lo **scambio di informazioni di routing**.
- Il Service Advertising Protocol (**SAP**), **pubblicizza servizi** di rete
- Il NetWare Core (centro) Protocol **(NCP**) fornisce **connssioni ed applicazioni a livello Client-Server**
- Il Sequenced Packet Exchange (**SPX**), è un servizio **di Livello 4 Connection-Oriented** Service.

Caratteristiche di Ipx: Ipx è un NetWare protocol di **Livello 3**, usato per **trasportare** i pacchetti tramite reti interconnesse. Ipx è **ConnectionLess** (simile ai pacchetti ip, nelle reti tcp\ip) ed ora all'interno della stessa implementazione di rete, come TCP\IP, nel multiprotocol Router. Le caratteristiche Ipx Sono le seguenti:

- Esso è usato in **un ambiente Client\Server**
- Esso **utilizza nodi di rete** con struttura di **Addressing** Ipx
- Il proprio **indirizzamento logico** contiene un'interfaccia con **Mac Address**
- La configurazione dell'interfaccia Ipx supporta **multipli Encapsulation data-link**
- Novel **Rip** utilizza il **metrics Distance-Vector** per gli hops
- Il Service Advertisement Protocol (**SAP**), ed il Get Nearest Server (**GNS**) broadcast, **connettono clients e servers ipx utilizzando Rip**, che è un distance-vector routin protocol oppure Netware Link Service Protocol (**NLSP**), che è un **link-state** Routing Protocol. L'IPX RIP invia gli updates di routing **ogni 60 secondi**. Il **RIP utilizza ticks** (ritardo di rete) ed il conteggio **hop** come routing Metrics. Se il conteggio Hop è **maggiore di 15**, il pacchetto sarà **scartato**.

Addressing del protocollo Ipx: Novel Ipx utilizza **due parti di indirizzi** creati **combinando il numero di rete, con il numero di nodo unico**. Il numero di nodo, è solitamente il **MAC address** per le interfacce di rete sul nodo finale. Ipx supporta **multiple reti logiche su una interfaccia individuale**, tuttavia **ogni rete** deve usare un tipo di **encapsulation differente**. Il **numero di rete** IPX, che è assegnato dall'amminstratore di rete **può essere superiore ad 8 Base 16** (hesadecimale) cifre in lunghezza.
Il nodo IpX è un numero di **12 cifre hexadecimali**. Questo numero è solitamente l'indirizzo mac ottenuto da un'interfaccia dotata di mac address. L'uso dell'indirizzo mac nell'indirizzamento logico ipx, **elimina la necessità di utilizzare ARP** per ottenere questo indirizzo. Le interfacce seriali utilizzano l'indirizzo mac per le interfacce ethernet per i loro indirizzi dei Nodi Ipx. Un esempio può essere dato dal nodo ipx 0000.0c56.de33 su la rete 4ald. Ad Ogni interfaccia router che partecipa all'Ipx routing dev'essere **assegnato un Ipx network Number**. Ad Un'interfaccia su un router cisco è assegnato lo stesso numero di rete IPX della periferica IPX che è cablata sull'interfaccia router. Il miglior modo per **ottenere un indirizzo di rete Novell è chiederne uno all'amministratore** di rete. Se non si può ottenere un indirizzo Novell Ipx dall'amministratore, è possibile **ottenerlo direttamente dal router** Vicino. Per poter far ciò, è necessario **Telnettare i router vicino usando i comandi Show Protocols, o Show Ipx Interface**.

Encapsulation dell'ethernet Netware: NetWare supporta **encapsulation Multiple** (tipologie di frames) per la famiglia ethernet di protocolli, tutti supportati dai routers Cisco.Xerox, Intel e Digital (cononosciuto collettivamente come DIX), hanno rilasciato **un primo standard per ethernet nel lontano 1980**, chiamato Ethernet **Version 1**. Due anni dopo, Dix sostituì questo standard con Ethernet Version II che è lo standard per l'encapsulation TCP\IP.
Quindi l'istitoti degli ingerneri elettrici ed elettronici (IEEE) ha iniziato il lavoro su frame ethernet migliorato, che verrà poi effettivamente **collaudato nel 1982**.
Novell ha chiamato questo tipo di frame 802.3 (ethernet 802.3). Questa specifica è spesso chiamata **ethernet Raw poiché IEEE non ebbe il tempo di completarla**. Due anni dopo, finalmente, IEEE ha rilasciato la **specifica finale per 802.3**, che include un Link di controllo logico (**llc**) logical link control header.
LLC contiene dei **campi che identificano il punto d'accesso per i servizi**, e questi questi campi rendono le specifiche IEEE **incompatibili con Novell's 802.3**. Poiché il frame IEEE 802.2 include servizio di punti d'accesso, il cisco IOS software si riferisce a 802.2 come Ethernet SAP (Novells chiama essa Ethernet_802.2).

La compatibilità distribuita fra 802.2 e 802.3 spinge gli sviluppatori di **tipi principali di frames**, chiamati **Ethernet SNAP**. La cosa più importante da ricordare riguardo a questi 4 tipi di frames, è che essi non sono compatibili fra di loro al 100%. Se un server Novell usa il framing 802.3, e il router cisco è configurato per encapsulare utilizzando 802.2, questi 2 nodi non possono parlare. Il cisco IOS software, ed i termini Novels di incapsulation sono i seguenti:

- Ethernet 802.3 è anche chiamata **RAW Ethernet**. E' il **default per le versioni NetWare 2 tramite 3.11**
- **Ethernet 802.2 o SAP** è anche chiamata **Novell Ethernet_802.2 o 802.3**. E' il formato frame IEEE standard, **includendo un header LLC 802.2.** Con la release NetWare 3.12 e 4.x, questa encapsulation diventa un nuovo standard di frame NoveLL per il routing osi.
- Ethernet II o **ARPA è anche chiamato Novell_Ethernet_II** o Ethernet Version II. E' usato per la versione standard **Ethernet header II con Tcp\IP**
- **Ethernet SNAP** o snap è anche **chiamato Novell Ethernet_SNAP** o snap. Esso **estende l'header IEEE 802.2 aggiungendo una header di "subnetwork access protocol**" (SNAP) che fornisce un tipo di encapsulation simile a ciò che è definito in Ethernet Version II specification ed è usato con TCP\IP e AppleTalk.

I nomi di encapsulation IOS per ethernet,Fddi e Token Ring: L'hardware cisco ed il software IOS, supporta tutte le **differenti encapsulation 802.3** utilizzati da NetWare.L'attrezzatura cisco può fare la differenza fra vari tipi di pacchetti, riguardo o meno la loro encapsulation. Su una **singola interfaccia lan sono supportate multiple encapsulation**, permettendo a **vecchi e nuovi nodi NetWare di coesistere sullo stesso segmento lan fin quando si configura la rete logica**. Il supporto per tipologie **multiple di encapsulation IPX** riduce la spesa per le apparecchiature, minimizza la complessità di configurazione e tranquillizza la migrazione fra l'encapsulation IPX ed altri.

Il formato del pacchetto Ipx: Il **pacchetto IPX** è **l'unità base del networking Novell NetWare**. La descrizione nella tavola, riepiloga i campi dei pacchetti IPX.

Novell Rip: Connettendo reti esistenti Novell e supportando un ampio numero di NetWare clients e Servers, rappresenta una grande sfida nell'area di installazione; Gestibilità e Scalabilità. Il cisco **IOS** fornisce molte caratteristiche chiave designate per **rendere le reti Novell quanto più larghe possibili.**
Il Cisco IOS software, supporta lo standard **Novell Rip**, che fornisce una soluzione base per il networking su reti Novell. Comunque, **frequenti messaggi di update, lenta convergenza e la limitazione di 15 hop count del Novell Rip**, rendono esso una **pessima scelta per reti di grandi dimensioni o reti connesse via Links WAN**.
Poiché Novell Rip è un routing protocol **Distance-Vector**, esso **utilizza 2 metric** per effettuare le decisioni di routing (**ticks)-Misurazione del tempo e (hop count)-conteggio degli hop** attraversati. Novell Rip controlla questi 2 metrics comparando come **prima cosa i ticks** con percorsi alternativi. Utilizzando ticks come metric si ha una migliore misurazione della velocità del link. **Se 2 o più percorsi hanno lo stesso valore tick, Novell RIP paragona l'hop count**. Se due o più percorsi hanno lo stesso hop count, il router carica "shares". **Il "load sharing", è l'utilizzo di due o più percorsi per trasportare pacchetti alla stessa destinazione** equamente per mezzo di routers multipli per bilanciare il lavoro e migliorare la performance di rete.
La **Novell RIP ROUTING TABLE**, in un router è **differente dalla IP routing Table** poiché il router **mantiene una routing table per ogni protocollo IPX** abilitato. Perciò **per ogni Ipx Abilitato, il router passa periodicamente copie del proprio** Novell RIP ai propri vicini. I router Vicini, contribuiscono a **sommare distanza vettori**, prima di passare le copie delle proprie Novell RIP table.

Una “migliore informazione” **Split-horizon protocol, previene il broadcasting dai router vicini**, delle Tabelle Novell Ipx. L’informazione torna indietro sulla rete da cui è stata ricevuta. **Novell RIP un meccanismo di “invecchiamento”** dell’informazione per testare le condizioni in cui Ipx permette ad un router di andar giù senza aver inviato alcun messaggio esatto ai router vicini. Update periodiche resettano di nuovo il timer. **Gli update delle tavole di routing sono inviati ogni 60 secondi**. Questa frequenza di update può causare eccessivo traffico su diverse reti.

Il service Advertising Protocol: Il **SAP NetWare**, permette alle risorse di rete, includendo File e server di stampa, di **pubblicizzare il proprio indirizzo di rete** ed il servizio che essi forniscono. Ogni servizio **è identificato con un numero, ed è chiamato SAP Identifier**. Gli updates **SAP** sono inviati **ogni 60 secondi**.
Periferiche intermediarie di rete, come router, **ascoltano gli update SAP** per costruire **una tabella di tutti i servizi** conosciuti ed associati con indirizzi di rete. Quando un Client Novell **richiede un particolare servizio di rete**, se un NetWare server è locato sul segmento, **esso risponde alla richiesta client**. Il Cisco router non responde alla richiesta. **Se il servizio richiesto non è disponibile** sulla rete locale, il router Cisco **risponde con un indirizzo dalla propria tabella SAP**. Il client può quindi contattare il servizio direttamente.
Tutti i **servers** su NetWare networks possono **pubblicizzare i propri servizi ed indirizzo**. Tutte le versioni di NetWare, supportano i **broadcast SAP** per annunciare e Localizzare servizi di rete registrati. Aggiungere, trovare e rimuovere servizi su una rete, è un’operazione dinamica che viene eseguita dagli **annunci SAP**. Ogni servizio SAP è un oggetto **identificato con un numero**. Esempio: 4-NetWare file server, 7 Print Server, 24 Remote Bridge Server.
Solo **i routers ed i servers tengono le Tables SAP**, non le workstation. Tutti i server ed i routers Tengono una **lista** completa dei **servizi disponibili** per tutta la rete nelle tabelle SAP. Come RIP, anche **SAP utilizza un meccanismo di invecchiamento atto ad identificare e rimuovere le tabelle entries nelle tabelle SAP che risultano invalide.**
Per default la pubblicizzazione del servizio avviene **ad intervalli di 60 secondi**. Comunque benchè i servizi di pubblicizzazione possano lavorare bene sulla lan, il servizio di **broadcasting può necessitare di molta banda** per essere accettato su larghe reti o su reti linkate da connessioni seriali Wan.
Per questo motivo, i routers ono forwardano i broadcast SAP. Ogni router costruisce la propria tabella SAP e forwarda essa ad altri router vicini. Per default, questo avviene **ogni 60 secondi** ma il router può **usare le Access Control List per controllare l’accettazione del SAP** o il forward.
Il cisco IOS software inoltre permette agli amministratori di rete, di **visualizzare le entries** contenute nelle tabelle SAP by nome e quindi identificativo SAP. Presentando informazioni di configurazione rete in un formato più leggibile, si rende le reti più affidabili e flessibili, diagnositcando i problemi con più facilità.

Il Get Nearest Server Protocol: I client NetWare**, automaticamente scoprono le reti e servizi** disponibili, poiché i Novell Servers e routers **annunciano il servizio utilizzando SAP** broadcast. Un tipo di pubblicizzazione SAP è **GNS**. **Che abilità un client a localizzare velocemente il server** più vicino per il Login.
L’interazione NetWare client\server inizia quando i clients si accendono ed eseguono i propri programmi di startup. Questi programmi usano l’adattator di rete sulla LAN per iniziare la sequenza di connessione per utilizzare il NetWare command shell. La **sequenza di connessione** è un broadcast che proviene dai clients che stanno usando **SAP**. Il più vicino file NetWare server, risponde con un’altra SAP. **Il tipo di protocollo è GNS**.
Da tal punto, il client può **loggarsi sul target server, effettuare una connessione, settare la dimensione del pacchetto e procedere ad utilizzare le risorse** del server.
Se un server NetWare è locato sul segmento, esso risponde alla richiesta del Client. Il cisco Router non risponde alla GNS request.

Se **non ci sono server NetWare sulla rete locale**, il **router Cisco, risponde con un indirizzo del server dalla propria SAP** Table.
Il cisco IOS permette ai Clients NetWare di essere localizzati sui segmenti lan dove non ci sono servers. Quando un client NetWare vuole localizzare un server NetWare, esso distribuisce **una richiesta GNS**. I cisco routers ascoltano il traffico NetWare, identificando servers e **forwardando le GNS request** specificatamente ad essi. Tramite il **filtraggio dei GNS packets**, è possibile esplicitamente **escludere i servers selezionati**, fornendo grande sicurezza e flessibilità, nel design del network.
In risposta alla richiesta GNS, il cisco IOS software, può anche distribuire clients uniformemente fra i servers disponibili. Per esempio, supponiamo che il client A ed il client B distribuiscano entrambi la richiesta GNS. Il route cisco Invia una risposta GNS al client A, dicendo ad esso di comunicare con il server 1, ed una risposta GNS al client B dicendo ad esso di comunicare con il server 2. Supportandosegmenti lan senza server, e distribuendo client uniformemente fra server disponibili, il cisco IOS software fornisce carico di rete e condivisione, migliora nel complesso la disponibilità di banda per applicazioni e minimizza la necessità di configurare e gestire un largo numero di servers locali, partendo dal presupposto che ogni server è identico agli altri.

I Tasks di configurazione Novell Ipx: Configurare un router per Ipx routing, coinvolge sia i task Globali che quelli **relativi all'interfaccia**.
La configurazione Globale Ipx include le seguenti fasi:

- Far **partire** il processo Ipx
- Abilitare il **"load sharing"** appropriato per la rete

La configurazione interfaccia Ipx include le seguenti fasi:

- **Assegnare un unico numero identificativo di rete** per ogni interfaccia. E' possibile assegnare multipli numeri di rete ad un'interfaccia, supportando differenti tipi di encapsulation.
- Settare l'opzionale **encapsulation Ipx type**, se essa è differente dal Dafult

I tasks di configurazione Ipx sono descritte in più dettagli, nelle seguenti sezioni.
Il comando **"ipx routing" abilita il Novell Ipx Routing**, se nessun nodo è specificato, il router cisco utilizza il mac address dell'interfaccia. Se un router cisco ha solo interfacce seriali, **un indirizzo dev'essere obbligatoriamente specificato**.
In aggiunta, il comando **"ipx maximum-paths" abilita il load sharing**. Come precedentemente specificato, questo è il numero massimo di percorsi paralleli per la destinazione, il default è 1, **il massimo è 512**.

Scrivere una valida sequenza di comandi per assegnare numeri di rete Ipx ad Inter Facce: Quando si assegna un numero di rete Ipx ad una interfaccia che supporta multiple reti Ipx, è possibile anche **configurare una rete primaria ed una secondaria**. **Il primo** indirizzo logico che configuriamo, sull'interfaccia è considerato quello **corrispondente alla rete primaria**.
Ogni rete addizionale è considerata **rete "secondaria**". Ipx network su **una interfaccia può** utilizzare una **encapsulation distinta**, e deve trovare **coincidenza con i clients e con i server** che usano lo **stesso numero di rete**. E' necessario assegnare **un secondo indirizzo di rete** se un tipo addizionale di encapsulation è liknato ad una rete individuale. Per assegnare numeri di rete ad interfacce che supportano multiple reti ipx, si usa normalmente le subinterfaces. Una subinterfaces è un meccanismo che **permette ad una singola interfaccia fisica di supportare interfacce logiche** multiple o reti. Dunque diverse interfacce logiche o reti, possono **essere associate con una singola interfaccia hardware**. Ogni **subinterfaccia** deve usare una **encapsulation distinta**, e questa encapsulation deve trovare **coincidenza con i client ed i servers che stanno utilizzando lo stesso numero di rete**.

Scrivere un comando valido per Monitorare e fare TroubleShooting su Ipx: Quando è configurato il routing ipx, è possibile m**onitorare e fare troubleshooting su Ipx** utilizzando il comando mostrato nella tabella : (omiss)

Monitorare lo stato di un'interfaccia Ipx: Il cisco IOS include una **varietà di strumenti** per configurare, monitorare e gestire la rete. Questi strumenti rendono le reti NetWare facili da settare. Essi possono essere essenziali quando sopraggiungono condizioni inaspettate sulla rete.
Il comando **"show ipx interface" mostra lo status dell'interfaccia Ipx** e dei parametri Ipx configurati per ogni interfaccia.
La prima linea mostra l'indirizzo Ipx, il tipo di encapsulation e lo status dell'interfaccia.
La seconda area mostra che i **filtri sap** non sono settati.
L'ultima mostra che il fast switching è abilitato. E' possibile settare manualmente il trick metric per configurare il ritardo tick su un'interfaccia. Usare il comando **"ipx delay(numero)**", in cui il numero è **un tick da associare ad una interfaccia**. Questo comando dice al router di ignorare ogni altro settaggio di default. I default settings sono i seguenti:

- Per le interfacce **LAN, 1 tick**
- Per le interfacce **WAN, 6 ticks**

Monitorare Tabelle di routing Ipx: Il comando **"show ip route"** mostra il **contenuto della tabella di routing Ipx**.
Nell'esempio, la prima linea fornisce informazioni di routing per una rete remota:

- R indica che l'informazione è stata **appresa da un update Rip**
- Il numero di rete è 20 30. La rete è locata a **6 tiks dall'hop circostante**. (Questa informazione è usata per determinare la miglior route. Se c'è un **legame fra ticks**, gli **hops sono usati per rompere questo legame**.)
- Il prossimo hop sul percorso è il router 3021.0000.0c03.13d3
- L'informazione è stata updatata 23 secondi fa
- Il prossimo hop è raggiungibile in uscita dall'interfaccia seriale 1.
- C'è una metric route uguale su differenti hop, raggiungibili tramite l'interfaccia seriale 0
- Il numero di rete è 3010
- Il tipo di encapsulation è NOVELL-ETHER.
- Il C indica che l'informazione è stata appresa da una rete primaria direttamente connessa.

Monitorare Servers Novell Ipx: Il comando **"show ipx servers" mostra i servers Ipx scoperti tramite la pubblicizzazione SAP**. Il comando in uscita **"show ipx servers",** mostra le seguenti informazioni:

- Il **serverzio appreso** da un server tramite **UPDATE SAP**.
- Il **nome del server, la locazione della rete, l'indirizzo della periferica ed il numero socket sorgente**
- I **ticks e gli hops per la Route** (presi dalla tabella di routing)
- Il **numero di hops** (presi dal protocollo SAP)
- L'**interfaccia tramite la quale** si raggiunge il server

Per visualizzare la lista dei servers Ipx scoperti tramite pubblicizzazione SAP, si usa il comando "show ipx servers", nella user exec mode. La sintassi completa per questo comando è:
show ipx servers (sorted (name | net | type))

Monitorare il traffico Ipx e descrivere molti campi opzioni per questi comandi: Si utilizza il comando **"show ipx traffic" per avere le informazioni sul numero e tipo di pacchetti ipx ricevuti e trasmessi dal router**. Notare che una larga percentuale del numero totale di pacchetti

ricevuti, sono a loro volta re-inviati via pubblicizzazione RIP. Ciò avviene poiché l'esempio in questione è stato preso da un laboratorio in cui non essenzialmente utenti utilizzano la rete e creano traffico. Questi dati ci permettono di vedere quando traffico in overhead ipx ha generato.

Scrivere un comando per il troubleshooting sull'ipx routing: Il comando **"debug" ed il comando "ping", permette ad amministratori di rete, di vedere e tracciare al meglio, ogni aspetto del traffico della rete.** Il supporto di **debug** cisco, può essere essenziale per gli amministratori di rete, per **monitorare, gestire e fare troubleshooting** su reti Novell.
Il comando **"debug ipx routing activity", visualizza le informazioni su i pacchetti ipx di routing update che sono trasmessi o che sono ricevuti**. Un router invia un **update ogni 60 secondi**. Ogni pacchetto di update può contenere più di 50 entries. Se ci sono **più di 50 entries sulla tabella di routing, l'update include più di un pacchetto**. In questo esempio, il router sta inviando update ma non ne sta ricevendo alcuno. Gli update ricevuti da altri router devono anche apparire nella listing.
Il comando **"debug ipx routing activity"**, deve essere usato con attenzione, con ogni comando di debug. Esso **utilizza molte risorse sul router** e può causare Crash e far andar giù la rete.

Comando per il troubleshooting Ipx SAP: Il comando **"debug ipx sap** (events|activity)" **visualizza le informazioni sui pacchetti IPX SAP trasmessi e ricevuti**.E' indispensabile scegliere fra "events o activity" alla fine del comando debug ipx sap. Si può utilizzare il comando **"debug ipx sap activity" per i dettagli** un uscita oppure **"debug ipx sap events" per dettagli meno approfonditi**. Come gli updates RIP, questi SAP updates sono **inviati ogni 60 secondi** e possono contenere **pacchetti multipli**. Come mostrato nell'esempio, ogni pacchetti SAP **si raffigura con linee multiple in uscita**, includendo un messaggio "sommario" del pacchetto, e un servizio dettagliato del messaggio. Le risposte SAP possono essere le seguenti:

- 0x1 -General query
- 0x2 -General response
- 0x3 -GNS request
- 0x4 -GNS response

In ogni linea della risposta SAP mostrata in esempio,è listato l'indirizzo e la distanza del risponditore o del Target router.

Il comando Privilegiato Ipx Ping: Il software cisco IOS, fornisce **una versione IPX del comando ping**, per aiutare al troubleshooting. Il comando Ping permette agli amministratori di rete di **verificare che un nodo particolare è capace di rispondere a richieste di rete**. Questa caratteristica aiuta a determinare quando un percorso fisico eisiste fra una stazione che sta causando problemi. Il comando **IPX ping è uno standard Novell** e **può essere usato con i clients e servers**.
Per verificare la raggiungibilità di un host e la connetticità, usare il comando Ping, in modalità di comando privilegiata:
La sintassi completa per il comando ping è la seguente:
"**ping (ipx) (network.node)"**
Questa informazione è una descrizione dei parametri usati con questo comando.
Il comando privilegiato ping fornisce una completa agevolazione ping per gli utenti che hanno privilegi sul sistema.
Il comando **privilegiato ping lavora solo con routers Cisco che montano la versione 8.2 o successiva**.**Le periferiche Novell IPX non possono rispondere a questo comando**.
Un router **non può essere pingato da se stesso**. Per annullare la sequenza ping, è necessario premere ESC. Per default ciò si ottiene anche con Ctrl-^-X o Ctrl-shift 6-X. Si inserisce questo simultaneamente premendo Ctrl, Shift, e 6. Andando avanti quindi e premere X.
L'informazione nella tabella descrive i caratteri visualizzati nel test del ping e delle risposte che ne derivano.

User Ipx Ping Command: Il ping è utilizzato per **controllare la raggiungibilità di un host** e la **connettività** della rete.
Il ping livello utente fornisce **un'agevolazione per utenti che non hanno privilegi di sistema**. Il comando privilegiato ping invece non serve a questo, esso **invia per 5 volte, 100 byte ipx echos Cisco**. La sintassi del comando è la seguente:
Ping (ipx) (host|address)
L'informazione nella tavola è la descrizione dei parametri usati nella sintassi.
Il comandi livello utente Ping lavora **solo su routers cisco che hanno la versione IOS 8.2 o successiva**. Le periferiche non rispondono a questo comando. Non si può pingare un router da se stesso. Se il sistema non mappa un indirizzo per l'host name, tornerà indietro un messaggio di "host sconosciuto".

Management di Rete

Diagrammi del Cut Sheet: Il **primo** ed il più **critico** componente per una buona rete è rappresentato dalla **documentazione**. La documentazione è **molto discussa**, è inoltre **il task più performato** in una progettazione di una rete. La documentazione rappresenta la memoria dell'amministratore di rete, Essa consiste, prima di tutto, in un **giornale ingegneristico** (engineering journal), ma non si ferma qui; La documentazione include anche:

- Un **diagramma che indica il percorso** del layout del cablaggio fisico.
- Il **tipo** di cavo.
- La **lunghezza** di ogni Cavo.
- Il tipo **di terminazione** per il cavo.
- La **locazione fisica** per ogni "wall plate" o patch panel.
- Uno **schema** disegnato per facile identificazione di ogni Cavo.

Layout IDF e MDF: Questo documento contiene **layouts** fisici e logici per il **Main Distribution Facility e tutti gli Intermediate Distrubtion Facilities**, sulla rete. Esso include il **layout Fisico** della "rack mounts", equipment ausiliario, e server in ogni Distribution Facility. Esso include inoltre **disegni** di patch panels per identificare le terminazioni dei cavi. I dettagli relativi alla identificazione d al la configurazione di tutte le apparecchiature locate in ogni distribution facility, devono essere incluse.

Dettagli di configurazione Server e Workstation: I **dettagli di configurazione** servers e workstations comprendono informazioni relative ad ogni host collegato alla rete.
Le informazioni contenute in questi fogli sono **standardizzate** e contengono diverse cose, come ad esempio: Modello del computer, numero seriale, floppy drives, hard drives, dvd\cd-rom drives, scheda sonora, adattatore di rete, ed ammontare della ram, ed ogni altro dettaglio fisico del computer. Questa informazione include anche **altri dettagli del computer**, IRQ, DMA e Configurazione della memoria Base e delle schede aggiuntive.
Infine, questo documento contiene la **locazione fisica**, gli utenti e l'identificazione di rete (indirizzo ip, mag address, subnet e tipologia), tutte informazioni, queste, relative al computer. Sono incluse anche la data di acquisto e la garanzia.

Listato Software: La documentazione di rete deve includere: Una **lista del software** standard e speciale usato per ogni computer sulla rete. La **configurazione standard per l'installazione**, nei dettagli e un listato di **ogni software che verrà installato**. Il **sistema operativo** e il software **applicativo.**

Mantenimento dei Records: E' anche valutabile l'idea di poter tenere **una lista** di tutte le **riparazioni che sono state effettuate** all'equipaggiamento che fa parte del network. Aiuteremo l'amministratore a **prevedere futuri problemi** con l'hardware ed il software esistente.

Misure di Sicurezza: Questo documento include **la sicurezza** Software e Hardware. La sicurezza software comprende Diritti utenti, definizione di **password** e supporto firewall. La sicurezza Hardware comprende cose facilmente identificabili come ad esempio la **chiusura di sicurezza** che riguarda **MDF ed IDF** e come essi sono resi **sicuri da accessi esterni**; Chi ha accesso in tali stanza e perché; Come gli host sono protetti (cablaggi di sicurezza, allarmi) e chi ha accesso fisico al sistema.

Policy Utente: Le **policies** sono documenti che possono essere **molto importanti** ed utili per l'amministratore di rete. Esse contengono informazioni su come **gli utenti possono interagire sulla rete**. Queste policies espongono che **cosa è permesso e che cosa invece non è permesso** sulla rete. Essi possono anche includere un elenco delle **conseguenze** della **violazione** delle policies. Altri aspetti delle policies utenti possono essere, il **requisito minimo** per la lunghezza nell'inserimento **dell'user ID e Password,** e le **regole** per il contenuto della password. Le policies necessitano di essere create dalla direzione del management della compagnia, per garantire che queste policy, siano messe in vigore. Come un amministratore di rete, è possibile creare la rete quanto più **sicura e funzionale** possibile per la propria azienda. Bisogna sempre esser sicuri che le policies di rete non vadano in **conflitto** con le policies aziendali o limitino gli utenti ad accedere alle risorse necessarie. Le informazioni registrate in questi documenti rappresentano la documentazione di rete relative al nostro sistema. Questa documentazione permetterà il **mantenimento e l'upgrade della rete** sotto molti aspetti e stili. Questa documentazione darà all'amministratore una posozione di partenza alla quale tornare se un upgrade dovese rivelarsi azione errata, o se si avesse bisogno di tornare indietro a seguito di un fallimento di rete. Uno degli ultimi punti sulla documentazione di rete è che essa deve **continuamente essere updatata** con gli ultimi cambi ed upgrade della rete. Se ciò non avviene, la documentazione non ha un grande **accordo di pertinenza** con l'implementazione corrente.
I **cambiamenti** devono per prima essere **annotati sul documenti**. Questi cambiameni devono quindi **produrre cambi** che sono usati come istruzioni per altri tipi di cambi nel sistema del network.

Accesso alla Rete: La **sicurezza** di rete involve 2 maggiori componenti: **Il primo è tenere la rete protetta** da accessi non autorizzati ed **il secondo è abilitare il recovery** dei dati da eventi catastrofici. La prima parte della sicurezza fa riferimento alla documentazione di rete. E' necessario rendere la **rete quanto più sicura** possibile contro accessi non autorizzati. Stabilendo **delle policies** di sicurezza si può far ciò. Le policy di sicurezza concistono in un minimo di lettere **per le password** di rete, scadenza, password unica (non permesso di ripetere la stessa password alla scadenza). Le plicy devono anche settare **uno specifico orario del giorno o giorno della settimana per cui un utente può loggarsi** sul network. Questi parametri possono essere direttamente controllati dall'amministratore di rete e rafforzati dal sistema operativo.La sicurezza spinge a conoscere le **policy di rete** aziendali ed a seguirle. Un esempio di queste policy può essere il Permettere ad utenti di usare nomi di famiglia o di animali della stessa famiglia per la password. Un altro esempio è essere sicuri che l'utente sia loggato fuori dalla rete, o che abbia uno screen saver protetto da password, attivato, quando la postazione non è utilizzata per un determinato tempo.

Questi tipi di regole devono essere seguite se l'utente ha capito l'importanza di queste network policies e se esso vuole, per la propria rete, una certa sicurezza.

Recupero Dati: Il **recupero dati**, la seconda parte della sicurezza di rete, permette il **recupero dei dati persi**. Ci sono metodi multipli per **prevenire la perdita** di dati. Solitamente c'è più di un metodo che può essere usato allo stesso tempo per proteggere i dati. Questi metodi, popolari, di protezione dati, **sono backup di dati**, fault tolerant configurations, ed utilizzano diversi **UPS per prevenire lo shutdown** dei pc, durante sbalzi di corrente o blackout. Si parlerà di questo metodi nei dettagli; Il **Tape Backup è il processo per fare i backup** dei dati su un supporto magnetico. La ragione per cui è usato il supporto **magnetico** (Tape) è il costo e la capacità. Le cartucce Tape sono molto meno costose e contengono più dati rispetto agli hard disk removibili. Lo svantaggio del tape, per uso generale, è che **esso memorizza i dati sequenzialmente**, proprio come la musica viene registrata sulle cassette. Localizzare un file specifico su un tape, può essere **difficile come localizzare una specifica** canzone su una cassetta.Tuttavia quando i dati sono backuppati e recuperati sequenzialmente, la ricerca non è realmente necessaria. Poiché questo processo può pesare sulle risorse di sistema, è importante effettuare il backup **più rapidamente possibile**. Per permettere all'operazione di backup di essere eseguita rapidamente ed efficentemente, sono stati realizzati diversi tipi di **dispositivi per il backup**. Molti di questi tipi, lavorano con un **flag o switch** chiamato **"archive bi**t". Questo archive bit è memorizzato in un file ed utilizzato **quando qualche file sul supporto è creato o modificato**. Questo Flag **suggerisce al processo di backup se il file necessita d'essere backuppato o no**. Se il file è memorizzato sul tape, **durante il processo** di backup, normalmente **la flag è OFF**, sapendo che il file corrente si sta copiando sul tape.
Molte aziende raccomandano che tape e backup siano memorizzati in diversi tipi di "fire safe", o saranno difficilmente utilizzabili in caso di eventi castastrofici on-site.

Operzioni di Backup: I 5 steps delle operazioni di backup sono le seguenti:

1. Backup completo: **tutti i files** sul disco sono memorizzati nel tape, r**iguardo o meno i settaggi dell'"archive bit",** dunque il **flag** di questi bit è settato sempre su **OFF.**
2. Backup Incrementale: Backup di tutti i files che sono stati **creati o modificati dalla data dell'ultimo backup**. Ogni backup **incrementale** è **dipendente dall'ultimo backup** full e da tutti gli interventi di backup incrementale. **L'"archive bit" è su OFF durante questo processo**. Per restorare il sistema in maniera completa, dev'essere installato l'ultimo full backup+l'eventuale backup incrementale.
3. Backup differenziale: Backuppa tutti i file che sono stati creati o modificati **dall'ultimo FULL Backup**. L'archive bit non è resettato durante un backup differenziale. Questo vuol dire che ogni volta, il backup differenziale, è eseguito, tutti i file modificati o creati **dall'ultimo full backup sono bakuppati di nuovo**.
4. Copia di Backup: Backuppa **tutti i file selezionati sul tape**. Questo backup non **resetta l'rchive bit su OFF**. Per restorare da capo il sistema, dev'essere prima installato l'ultimo FULL backup, seguito dall'ultimo backup differenziale.
5. Backup Giornaliero: Bakuppa i files **che sono stati modificati nel giorno del backup**. Questo backup non resetta **l'Archive bit su off**.

Le prime tre procedure di backup sono usate molto spesso. Può esserci un esempio per cui usare prima un backup incrementale poi un backup differenziale.
Grazie al backup **differenziale**, tutto il backup va per primo effettuato di lunedì. Questo resetterà tutti gli archive bit sui files. Martedì, un backup differenziale verrà effettuato per separare i tapes. Questo memorizzarà tutti i file modificati martedì sul tape, ma non resetterà il loro archive bit. Questo processo è ripetuto per tutti gli altri giorni della settimana, sempre con lo stesso tape e garantisce un completo backup dei dati\dati di rete. Il suo vantaggio è che esso richiede solo 2 Tapes per eseguire il restore ed il backup. Lo Svantaggio è che , se si vuole restorare il backup, è necessario prima passare il primo tape poi il secondo. Tutti i **backup incrementali sono restorati**

nell'ordine in cui sono stati creati. **Se uno dei 2 tape è corrotto, si perderanno tutte le informazioni.**
Un backup **FULL è eseguito ogni giorno**, e richiede un tape per il restore dei dati, ma non è molto pratico eseguire il backup full ogni giorno xkè si tratta di una operazione che **prende molto tempo**. Né le copie di backup né le copie giornaliere, resettano l'archive bit, e sono usate per fare il backup di files selezionati. Un'altra considerazione importante, quando si esegue il backup di sistema, riguarda i dati di utenti e workstations. I dati memorizzati sulle workstations sono spesse volte più importanti di quelli memorizzati sui server di rete. Un metodo particolare per fare il backup a workstations, dipende dalla situazione. **Ci sono diversi scenari per il backup delle workstations**. Il primo metodo deve essere usato per una workstation che crea e lavora con un grande ammontare i dati, che sono solo usati su quella determinata workstation. In questo caso, **un tape individuale** può lavorare meglio. Esso permette ad un ammontare ampio di dati di essere dedicati allo scopo e di **non creare impatto diretto sulla portata di rete**.
Il "downside" di questo metodo è che esso mette nelle mani **dell'utente la responsabilità del backup**. Un secondo modo per eseguire il backup delle workstation è copiare tutti i files in una periferica di memorizzazione removibile, come **ad esempio un floppy zip drive**. Questo sistema **è poco dispendioso, si risparmia tempo e si evitano le complicazioni del backup su tape**, ma le mani del backup sono sotto la responsabilità dell'utente.
Un altro metodo è creare delle **directories sul server** per tutti gli utenti che servono alla memorizzazione dei dati utente. Questa soluzione **rimuove la responsabilità dell'utente** per eseguire il backup, si elimina, in questo modo **periferiche speciali di backup situate nelle workstation**. Lo **svantaggio** di questa soluzione è che **le policy** sulla memorizzazione dei dati, **devono essere chiaramente definite**. L'utente deve comprendere dove esso sta memorizzando i dati per essere sicuro che l'operazione di backup avvenga correttamente. Inoltre se **c'è un problema di comunicazione sulla rete, i dati non possono essere copiati** fino a che l'utente non ha risolto questo problema.
Come abbiamo visto, dunque, **con ogni soluzione, esistono dei potenziali problemi**. Ogni situazione avrà un miglior caso per una migliore soluzione in rapporto al tempo ed allo spazio. L'unica soluzione errata è ignorare tutti i dati necessari sui sistemi e non eseguire il backup.

Tecniche di Redundanza: Il prossimo metodo per proteggere i dati, è tramite periferiche **"fault tolerant storage".** Questo tipo di devices **redundanti, è categorizzato per Raid** (Redundant Array Of Inexpensive Disks), ed è livellabile da 0 a 5. Tutti i tipi di raid verranno illustrati ma si guarderà in particolar modo i tre livelli di maggior importanza. I vari tipi di raid sono i seguenti:

1. RAID 0: Memorizza i dati **su dischi multipli**, nessuna parità, nessuna ridonanza.
2. RAID 1: Morroring di dischi (duplicazione dischi), scrive i dati **in 2 partizioni identiche** su dischi separati, dunque crea un **backup automatico**. Il duplexing usa un controller da **2hard disk**.
3. RAID 2: Scrive su dischi **multipli**, **con checking degli errori**. Questi sistema **non è usato** perché richiede dischi molto costosi e varie modifiche per lavorarci sopra.
4. RAID 3: Memorizza i dati di byte in byte, ed ha **un drive con parità, dedicato**. Questo sistema è buono, ma caratterizza una scelta ridondante e **costosa**. A causa della sua spesa, e dei suoi costi, questa soluzione **non è usata spesso**.
5. RAID 4: Memorizza i dati, di settore in settore, ed **ha un drive di parità dedicato**. Una scelta dispendiosa e redondante, che ha lo svantaggio di scrivere sui dischi **molto lentamente**, A causa della sua lentezza e dei suoi costi, questa soluzione **non è usata spesso**.
6. RAID 5: Memorizza data e parità **su dischi multipli** (al massimo 3 dischi, per raid5). Mixando la parità su tutti i dischi, **non è necessario un disco ulteriore di parità**. La scrittura dei dati sui dischi è **molo lenta, ma il costo non è alto**. Un altro importante fattore che riguarda il Raid 5, è che **su un sistema WindowsNT la partizione boot e quella di sistema non possono essere localizzate nell'ordine di dischi impostato sul raid5**.

Esistono altri livelli di raid ma già con questi possiamo capire la sostanza di ciò che interessa per Cisco. Non **tutti i sistemi operativi di rete**, supportano tutti i livelli raid menzionati. I tre livelli raid che sono supportati dalla maggior parte dei sistemi operativi, sono **RAID0, RAID1 e RAID5**. Il punto chiave da ricordare è che RAID0 è usato per velocizzare e per fornire nessuna redundanza dei dati (backup). Il RAID 1 fornisce **piena redundanza** di dati. Dunque esso **richiede molto spazio** per la memorizzazione, poiché tutti i dati sono scritti su dischi separati. **RAID1 ha un punto singolo di fallimento sul controller**. Questo problema è curato dalle altri varianti di RAID 1, che sono il Duplexing, dove anche il disk controller è duplicato.
Raid 5 richiede **un minimo di 3 dischi** e la dimensione della **partizione dev'essere la stessa** su ogni disco, In un sistema **winNT, il RAID5 richiede 4 dischi poiché la partizione di sistema e la partizione di boot, non possono esistere nel raid set**. RAID 5 è **popolare** poiché esso fornisce lettura dai dischi molto rapida, che offre una portata maggiore sulla rete. C'è un punto importante da esporre riguardo il Raid 5 su windows NT.
Per avere piena redundanza su WindowsNT, **almeno 5 dischi sono necessari**. I primi 2 funzioneranno da setup per raid 1 (disk mirroring), per gli altri 3 dischi si setterà il raid 5 che comprenderà il system boot e la partizione di sistema.Questo fornirà piena redundanza con il vantaggio di velocità che raid 5 fornisce. **RAID5 ha un vantaggio** addizionale, i **drives sono sostituibili a caldo**. Quando un drive fallisce il suo lavoro o si rovina, possiamo **continuare a lavorare poiché, sostituendo il disco, la parità verrà ricostruita**. Il disco rovinato può essere rimosso e sostituito senza spegnere il sistema. I dati mancanti verranno ricostruiti sul nuovo disco.

Corrente statica, polvere, sporco e Calore: Un'altra parte di un buon management di rete è dialogare con **fattori ambientali** che possono riguardare una rete. Controllando questi fattori, si crea una rete più stabile e flessibile. Quando si installa un nuovo equipment, bisogna sempre seguire le procedure riportate sul manuale di setup. Questo risolverà molti problemi che verranno fuori. Bisogna assicurarsi che tutti **gli equipaggiamenti siano switchati su OFF** prima di effettuare i collegamenti. E' necessario spengenere gli equipaggiamenti anche durante l'installazione di una nuova CARD. E' necessario essere sicuri **che il computer sia su OFF** prima di installare eventuale hardware e componenti e di non toccare cariche elettrostatiche formatosi all'interno del computer. Il miglior modo per proteggersi dalla corrente elettromagnetica, è usare una cinghia di terra (cavo di terra). Senza propri **scaricamenti a terra**, è possibile che **si formi una carica elettrica di oltre 20.000volts**. Questa carica elettrica può essere creata **camminando su tappeto o tessuto sintetico, con scarpe di pelle o tramite lo sfregamento in sedia di plastica**. Un'altra causa di questi fenomeni statici è **l'umidità formatasi nell'aria**. E' importante assicurarsi che la stanza in cui sono situati gli equipaggiamenti sia tenuta sotto controllo per quanto riguarda la temperatura e l'umidità. Le scariche elettrostatiche **provocano fenomeni a dir poco spregevoli**. E' possibile che si continui a non conoscere e ad ignorare la corrente statica, finchè essa non va a creare un danno. Una carica elettrostatica **danneggia irreparabilmente circuiti** intergrati sulla rete e sugli equipaggiamenti computerizzati. Per essere sicuri che questo problema sia eliminato, è necessario acquistare un anti statico che può non necessariamente essere una cinghia anti statica. E' necessario **Spolverare e pulire tastiere, disk drives ed altro equipaggiamneto dall'aria e dalle intemperie**. Tenere tutto il materiale informatico riparato da agenti esterni. La **nicotina è molto tossica** e si attacca sui componenti. Fumare nei pressi di componenti informatici può danneggiarli. Mai versare caffee o altri loquidi su componenti informatici o di rete. Se il liquido cade all'interno dell'apparecchiatura, può causare dei danni enormi, smesso causa un "burn UP" dei componenti.
Non permettere agli equipaggiamenti informatici di **surriscaldarsi**, computers ed altre apparecchiature di rete, hanno un Fan che provvede al dissipamento del calore, è necessario controllare che questo **dissipatore non venga accidentalmente bloccato**. Posizionare il proprio compute su supporti rigidi e resistenti. **Vibrazioni e shocks possono provocare dei danni** ai componenti all'interno del computer.

Condizionamento Energia: Proteggere i componento da **cablaggi elettrici** irregolari nell'edificio. Il miglior modo per proteggere la rete ed il network equipment, è inserire all'interno della struttura, **circuiti separati e dedicati**. Questo risolverà alcuni, ma non tutti i problemi correlati al cablaggio. Possono esssere usate altre periferiche per controllare irregolarità elettriche:

1. Trasformatori isolanti: **Controllono le spikes** di voltaggio e i disturbi di alta frequenza
2. Regolatori: Mantengono un **voltaggio** in uscita **costante** nonostante il voltaggio alla sorgente sia soggetto a frequenti ed irregolari cambiamenti per lunghi periodi di tempo. Esso **risolve problemi di browouts** e surges di voltaggio.
3. Condizionatore di Linea: Questo è un **regolatore con un trasformatore** isolante integrato.
4. Uninterruptibile Power Supply (UPS): E' fondamentalmente è un caricatore di batterie che carica una batteria la quale da energia al computer. Questa periferica permetterà al computer di **evitare disconnessioni brusche dalla rete** elettrica.

Interferenza Elettromagnetica e RadioFrequenza: Le interferenze elettromagnetiche, (EMI) e le Interferenze Radio (RFI), causano **problemi con le comunicazioni di rete**. Le sorgenti di questi problemi possono essere componenti computer come **alimentatori e monitors**, possono essere luci **fluorescenti o grandi motori elettrici, e cablaggio elettrico**.
EMI e RFI possono dare problemi ad equipaggiamenti con **cablaggio non propriamente schermato**. Componenti di una periferica possono dannegiarsi ed il danno causato a questi componenti può trasmettersi ad altre parti. Questo tipo di problemi sono **difficili da diagnosticare**, e sono solitamente scoperti, da diagnostiche software e hardware.

Virus Software: Tutti i precedenti problemi possono affliggere e compromettere la performance della rete, ma sono legati unicamente all'aspetto fisico della stessa. L'ultimo fattore che può influire **negativamente sulla performane della rete è il software**. Il solo ed unico **proposito dei virus** software è la **creazione di problematiche sui computers e le reti**. Ecco una lista dei virus e delle diverse e principali forme virali informatiche:
WORM : E' un programma che **si propaga tramite computers**, solitamente **creando copie di se stesso** in memoria. Uno worm si duplica in un computer, esso causa il **crash del pc**, spesso è **diviso in separati segmenti**, un verme è introdotto all'insaputa in un host o in una rete, per divertimento con l'intento di danneggiare (alterare, modificare) o distruggere informazioni.
VIRUS : Un programma che **infetta files** di computer, solitamente **programmi e files eseguibili**. L'invezione avviene quando il virus inserisce **una copia di se stesso nei files di un computer**, questo solitamente accade in molti modi, le copie sono eseguite **quando il file è caricato in memoria**, permettendo ad essi di infettare tutti gli altri file e così via. I virus spesso provocano dei danni in senso lato, spesso intenzionalmente, spesso non intenzionalmente. Ad esempio possono inviare questi virus in internet **tramite email attachments**.
TROJAN HORSE : E' un programma distruttivo camuffato da gioco, utility o applicazione**. Quando si esegue il file, spesso indirettamente sul computer, esso** appare come un'applicazione **spesso utile.I 3 capitoli precedenti descrivono certi tipi di software che possono danneggiare la rete o il computer. Ecco 3 step fondamentali per far si che un computer o la rete venga infettata da virus.**

1. **Fare attenzione** nel ricevere software, **senza conoscerne specificamente la provenienza**, molte volte il software è distribuito tramite canali illegali, questo è il primo step per la diffusione di un virus. Questo avviene poiché i sistemi non controllano il file system per rilevarne virus.
2. Essere **Diffidenti nei confronti di persone che usano il computer a proprio rischio**. Ogni file, anche il più innocente, ☺ può trasportare un virus. **Non necessariamente** dev'essere un **eseguibile**, può anche essere un file di dati che un virus ha infettato.
3. **Usare antivirus** costantemente su tutti i computers. Ci sono molte aziende che vendono o costriuscono software per la scansione dei virus.

Ci sono semplici cose che possono essere fatte per proteggere computer da virus. Ci sono molti altri modi per rilevare e prevenire intrusioni di virus che non possono essere scoperte.

Linea di base per la Rete, Updates e cambiamenti: Insieme alla sicurezza di rete ed alla redundanza, un'altra considerazione importante nel management della rete è **la Performance**. La performance di rete è **una misurazione della velocità e dell'affidaibilità di una rete**. Un buon paragone può esser fatto con una automobile.
Si vuole che la nostra macchina sia chiusa (security) ed abbia una ruota di scorta (redundancy), si compra solo questa parte dell'auto. Altri elementi dell'auto sono la rapidità (quickness), e la capacità di frenare (reliability). Questi aspetti di performance **necessitano di essere controllati** costantemente. Proprio come un'auto, anche la rete dev'essere controllata ed ottimizzata spesso. La differenza fra una rete ed un'auto, nell'esempio, è che per le auto ci sono vari livelli di perfornance, in relazione ai diversi modelli di auto. Per le reti non è così.
Ogni combinazione di computer, ed hardware di rete, software e cablaggio **ha una differente performance di rete**. Per sapere quando la rete è poco performante, **è necessario fare delle misurazioni e comparazioni**. Bisogna così **fissare una BASELINE**.
Una **baseline è stabilita** dopo che la rete è stata installata e **configurata propriamente**. In una condizione di perfetto funzionamento.
Per stabilire una baseline, bisogna **usare un monitor package o tool**. Due programmi sono il **FLUKE LANMeter o Windows NT network monitor**. Questi strumenti **registreranno diversi tipi di perfornce sulla rete**, includendo la percentuale di utilizzo della rete, il conteggio delle collisioni, errori sui frames e traffico broadcast.
Una misurazione Baseline è **stabilita quando il sistema** i rete è ad un livello di performance **ottimale**. L'amministratore di rete ha quindi **un valore di comparazione** per determinare la vita e la qualità della rete.
A seguito di una crescita o di **un cambiamento** della rete, la misurazione **baseline**, necessita di essere periodicamente **updatata**.
Quando l'hardware è upgradato è molto importante **upgradare i drivers** che controllano l'hardware. I vecchi drivers possono non essere compatibili e creare problemi e creare seri intoppi alla performance. Se un upgrade o un nuovo programam è installato, **il servizio o il repair pack supplementare dev'essere reinstallato**.
Quando si effettuano dei cambiamenti sulla rete, come ad esempio muovere una parte dell'equipment da una locazione ad un'altra, è molto importante verificare la propria operazione sia nella locazione sorgente che in quella di destinazione, prima di fare un update delle baseline . Questo è molto importante, in special modo quando si effettuano dei cambiamenti sulla riduzione del traffico si rete su un particolare segmento.
Anche se la periferica sta lavorando correttamente, sul vecchio segmento essa può non fare la stessa cosa sul nuovo segmento. E da ciò ne deriva un effetto negativo sulla performance generale di rete. Bisogna sempre verificare le operazioni di una periferica convolta nello spostamento (prima e dopo lo spostamento). Questo check includere la funzionalità di rete e tutte le applicazioni critiche.

Peer-To-Peer: Gli amministratori di rete devono essere consapevoli dell'esistenza di **2 tipi di reti**. I 2 tipo sono **Peer-to-Peer networks** e **Client-Server networks**.
La peer-to-peer networks è anche conosciuta come **WorkGroup network**. Essa è designata per un **piccolo numero** di workstations. Microsoft raccomanda di non utilizzare una rete **peer to peer con più di 10 computers**. I **vantaggi** di una peer-to-peer network sono che essa è **economica da creare e facile** per quanto riguarda la gestione. Essa permette agli **utenti di controllare le proprie risorse** e **non richiede un server dedicato** e nessuno software addizionale a parte il sistema operativo.
Ci sono molti **Svantaggi: Nessun punto centrale** di management è fornito e la **creazione di id's** per ogni utente che condivide risorse sulla propria macchina. Ogni volta un utente cambia la password, tutte le password sulla risorsa condivisa, tutto questo però avviene individualmente.

Se una **workstation condivisa è spenta**, le risorse di quel determinato pc **non sono inaccessibili** e non disponibili. Ricordarsi che se ci sono più di 10 utenti o se la rete cresce, la peer-to-perr network non è una buona scelta.
Esempi di **sistemi operativi peer-to-peer**, sono Windows per **Workgroups, windows 95, Windows 98 e LanTASTIC**.

Client-Server: L'altro tipo di rete è quella **client-server**. Cliente server network **tipicamente ha un server, periferica dedicata all'hosting** software e **gestione del traffico** di rete. I sistemi operativi di rete, sono il cuore delle reti client-server. Questi sistemi controllano le risorse e gestiscono la LAN. Un vantaggio delle reti client-server include un **punto centralizzato** per utente, sicurezza e gestione delle risorose. Server dedicati possono essere usati più efficentemente per fornire **specifiche risorse** ai clients. Essi forniscono inoltre accesso a risorse consentite con un **network ID ed una password**. Lo **svantaggio** è che esiste **un singolo punto di fallimento** per la rete. Se il **server va giù, tutte le risorse dei servers non sono disponibili** per i clients. I Clients **non** possono **operare senza il server**.
Le operazioni di rete ed il mantenimenti **richiede un personale addestrato**. Questo, in aggiunta con speciale software di rete, aumenta il costo di gestione della stessa.
Nonostante gli svantaggi, una rete client-server è realmente **l'unica scelta lavorativa**, quando si hanno **più di 10 utenti**. Esempi di **sistemi operativi client-server**, sono **Unix, Novell NetWare, Windows NT, e Windows 2000** Professional.
Il sistema operativo **Unix**, può esistere in varie versioni, implementato da diverse aziende. Le aziende che forniscono unix, sono Sun MicroSystem, IBM, Hewlett-Packard e Santa Cruz Operation (SCO). Ci sono anche versioni **Free di unix**, chiamate **FREEBSD, e Linux**, il quale ha un'enorme popolarità al giorno d'oggi.
Unix è un sistema operativo **multi-user** che supporta il **microprocessing, multitasking e multithreaded** applications. Il sistema operativo è basato sul Kernel, che isola il livello hardware del computer dalle applicazioni operative improprie e primariamente **utilizza NFS** (Network File System - Sun Microsystems's implementation)
NFS fornisce **sicurezza in accesso al server sia per file che per directory**. Unix fornisce **controllo utente, centralizzato** tramite il sistema operativo. Poiché sono in produzione multiple versoni di unix, è difficile contrastare le variazioni delle varie release di questo software. Questa descrizione descrive le caratteristiche comuni riscontrabili in tutti gli unix. I clients ce lavorano meglio con unix, sono solitamente specifici per gli sviluppatori di sistemi.
Riguardo a **NetWare e Windows NT**, possiamo dire che essi si presentano con differenti versioni create durante gli anni. Prima di tutto c'era Novell NetWare. La versione di **NetWare che è stata realizzata inizialmente è stata la Ver 3.13, Poi ver 4.11, infine la 5.00**.
Queste versioni si differenzaino, primariamente nella gestione dei servizi di directory.
NetWare **Versione 3.11 utilizza un oggetto chiamato "the bindery" per gestire utenti multipli** e risorse. Il servizo Bindery crea una "**service-centric network**". Una service centric network è focalizzata su un **server individuale** come punto di controllo. Questo crea un **problema con reti che hanno diversi server**. Ogni server deve avere un id individuale per ogni utente, quando la password è sincronizzata o **cambiata su un server, dev'essere cambiata anche su tutti gli altri** servers; Questo sistema **compete con il management centralizzato**.
La versione 3.12 è esistita prima della grande diffusione delle reti multi-server. Questo è uno dei motivi per cui nasce **NetWare 4.11**. NetWare 4.11 e 5.0 **usano un oggetto chiamato NDS** (Novell Directory Services) per gestire utenti e risorse. Il vantaggio, oltre la versione 3.12 è che il **DNS crea delle reti di tipo network-centric**.
Una rete nework-centric si focalizza **sull'intera rete come punto di controllo**. Questa focalizzazione consolita il management su un singolo punto ed i **server sono trattati come oggetti** nel contesto della rete. Questo permette **un singolo ID e Pasword** per autorizzare utenti per tutte le risorse sulla rete e fornire una **facile organizzazione e gestione** della rete.

Tutte le versioni di NetWare usano **una combinazione di 2 files servizi**. Il primo file è il **FAT** (File allocation Table), che è il file **usato per il DOS**. Il secondo è il (**DET**) Directory Entry Table, che è **proprietario Novell**, e fornisce **sicurezza server sia per file che per directory**.
I Clients che lavorano bene con **NetWare sono numerosi**, essi **includono tutte le versioni** di windows, **DOS, machintosh e OS-2**. La parte **negativa di NetWare** è la gestione utenti e risorse file.
Windows **NT** è **l'ultimo sistema operativo** discusso. Ci sono **2 versioni di Windows NT**. Windows NT versione **4 Server e Workstation**, furono costruite con l'interfaccia utente di windows 95. Questo fornisce una consistente interfaccia "**look and feel**" attraverso tutti i prodotti windows. Windows NT **gestisce utenti e risorse tramite l'uso del Dominio**. Un dominio è **un gruppo logico di utenti e risorse** sotto il **controllo di un server** chiamato **PDC** (Primary Domain Controller). I Domini possono anche supportare l'uso di servers secondari chiamati BDC (Backup Domain Controllers). Il Bdc può **bilanciare il carico** di lavoro del PDC e **fornire una redundanza** di utenti e risorse.
Un **terzo tipo** di server consentito nel dominio, è chiamato Stand-Alone Server. Il server è configurato **per supportare una particolare applicazione** e dedicare le proprie risorse a tale applicazione. Un'altra variazione di dominio è chiamata **Modello multi-domain**. In questo modello, **domini separati sono connessi con trusting**-trusted relationships. Questo permette agli utenti di attraversare domini per usare le risorse. La struttura gestione Windows 2000 Server **usa Active Directory** più spesso rispetto alla struttura standard di dominio.
Active directory è basato sul modello **network-centric**, che è come NDS, piuttosto che come un modello Domain Centered.
Windows **NT è come unix**. E' un sistema operativo **Multi-Utente che supporta il multi processing**, **multitasking e applicazioni multithreaded**. Questo sistema operativo è basato sul kernel, che isola il livello hardware del computer, da applicazioni operative improprie, ed usa sia la **Fat16** che il sisterma proprietario windowsNT, **NTFS**. Con la Fat16, windows NT fornisce il livello sicurezza directory (chiamata anche folder). Nessun file di sicurezza individuale è fornito. **NTFS fornisce sicurezza e permessi sia per file che per directory**.
La ragione per cui WindowsNT supporta entrambi queste strutture è che esso ha la **possibilità di coesistere con un altro sistema operativo** sullo stesso pc. Questo non vuol dire che entrambi i sistemi possono partire contemporaneamente, ma il computer può sostenere Windows NT o altri sistemi operativi. Per gli altri sistemi operativi, e per l'accesso ai files, è necessario usare FAT16. Windows 95 e 98 supportano FAT32 che windows NT non supporta. Dunque **fat 16** può essere una scelta che permette, sullo stesso computer, di far girare **Windows NT e Windows 95**. Windows NT lavora al meglio con altro clients Windows NT workstation, ma lavora bene anche con Windows per Workgroup, Windows 95, Windwos 95 e Machintosh.
Niente di materiale è usato come sistema operativo di rete, la principale funzione del **NOS è controllare la rete.** Per completare questo, è necessario **stabilire i diritti degli utenti** e creare tutti gli account, password e gruppi, appartenenti ad un particolare profilo di sistema, con l'aggiunta di eventuali policies. Parleremo di questo in maniera più dettagliata nei paragrafi seguenti.

Controllo della Rete: Un account di login, **identifica l'utente** su un sistema di rete. Questo account con la password **permette l'identificazione** e **fornisce l'accesso** alle risorse di rete. Questo account tiene la **responsabilità dell'utente per le azioni sulla rete**. Ciò è registrato in documenti di sicurezza identificati più tardi nel capitolo. Poiché un utente di rete dispone di quel solo ed unico account (tipicamente) tutte le risorse non necessariamente possono essere completamente disponibili per quell'utente. I **diritti attribuiti** all'utente ne determinano **le capacità d'accesso**.
I diritti sono **settati dall'amministratore** per permettere o negare accesso ad una particolare risorsa sulla rete. Sebbene un utente sia connesso alla rete e una stampante di rete possa ugualmente esser connessa alla rete, l'utente può NON essere in grado di stampare su quella stampante. **Se l'utente**

non ha i diritti di utilizzo per quella determinata stampante, **l'accesso alla risorsa verrà negato**. Se all'utente sono assegnati i diritti sulla risorsa, la stampante sarà disponibile. Questo vale per le stampanti, per i files, applicativi o altre "risorse" sulla rete.
Esiste **un problema amministrativo** nell'assegnazione di diritti agli utenti. Ciò avviene se ci sono **molti utenti** su una rete; Assegnando e modificando i diritti per ogni utente può portar via molto tempo all'amministratore. Questo problema **è risolto utilizzando i GRUPPI**.
I gruppi sono **raggruppamenti logici** di utenti sulla rete. I diritti ed **i permessi sono dati al gruppo** anziché all'utente individuale. (Stessa procedura).
Se un utente avrà quindi bisogno di questi diritti, esso **sarà assegnato ad un gruppo** e tramite questa azione acquisirà automaticamente i diritti di quel gruppo. Un cambiamento di diritti al gruppo **si rifletterà su tutti i membri** di quel determinato gruppo. Questo non vuol dire che i diritti NON possono essere assegnati ad utenti individuali. Il metodo più efficiente per gestire reti di grandi dimensioni, è **lavorare con Gruppi**. Le regle, **le policy ed i profili** non hanno a che vedere con le risorse del sistema bensì per come **l'utente interagisce** con la workstation.
I profili permetteranno ad un utente di **customizzare la propria interfaccia** utente su un computer e quindi abilitare all'uso del profilo di ogni computer che verrà connesso ad esso tramite la rete. Questo sistema è chiamato **Roaming Profile**. Un altro tipo di profilo è **mantenere la stessa interfaccia** utente per ogni accesso e **non permettere cambiamenti**. Questo sistema è chiamato **Mandatory Profile**, ed è usato in situazioni in cui **molte persone usano lo stesso computer** fisico. Se l'utente è sullo stesso computer tutto il tempo, e **non ha necessità di andare su altri computer**, esso può avere un **profilo Locale**. Un profilo Locale è memorizzato **non sulla rete**, come i primi 2 profili, ma **sul computer Locale**.
Le policies dialogano con il **controllo delle risorse** sul computer locale.
Una policty che non permette ad utente di memorizzare dati su un disco rigido di una workstation o su un floppy disk, può essere **utile ai fini della sicurezza**. Le policies possono anche **impedire ad utenti di eseguire cambiamenti** accidentali sulla configurazione del sistema operativo. Per esempio settaggi scheda video, configurazione hard disk e rete, sono aspetti della workstation che nella maggior parte dei casi, gli utenti vanno a cambiare. Se ciò viene fatto da tutti, ne deriva lavoro extra da parte di tecnici ed help desk per sistemare di volta in volta il problema.
Tutti gli aspetti su cui abbiamo gà discusso, possono essere riassunti in questo modo. I **Diritti** di rete, gli account di login, le password ed i gruppi, tramite i profili e le policies, **forniscono una strada grazie alla quale l'amministratore di sistema controlla gli accessi e le restrizioni sui servizi** di rete e cntrolla gli utenti locali sulle workstation. Essere un amministratore di rete, vuol dire dover fornire un **set completo di diritti e privilegi sulla rete**. Non tutti gli utenti hanno i diritti di cambiare privilegi e diritti **su altre utenze**. Questi **diritti sono riservati** a certi gruppi di persone che hanno ricevuto il privilegio di **amministrator**.

Metodo Scientifico: Il Troubleshooting di rete è un **processo simmetrico** applicato per **risolvere un problema** sulla rete. Un buon modo per iniziare può essere usare il **Dartmouth Design Matric**, che solitamente si usa **nella fase di design** della rete. E' uno strumento eccezonale, per stabilire un'analisi sistematica della tecnica per il troubleshooting. Un'altra tecnica di troubleshooting è il **metodo scientifico**. La prima lista rappresenta solo una spiegazione generale del metodo scientifico, La seconda lista mostra come il metodo scientifico viene applicato per il troubleshooting.
METODO SCIENTIFICO:

1. **Osservare** diversi aspetti dell'universo
2. **Inventare una teoria** che consiste in ciò che si ha osservato
3. Usare la teoria per **eseguire predizioni**
4. **Testare queste predizioni** sperimentandoli tramite osservazioni future
5. **Modificare la teoria** alla luce dei risultati ottenuti
6. Tornare allo Step3

METODO SCIENTIFICO PER IL TROUBLESHOOTING:

1. **Identificare il problema** di rete\utente
2. **Raggruppare i dati** che riguardano i problemi di rete\utenti
3. **Analizzare** i dati affinchè venga fuori la possible soluzione al problema
4. **Implementare la soluzione** per la rete, che consenta di attuare la correzione al sistema.
5. **Se** il problema **non è risolto**, **annullare i precedenti cambiamenti e modificare** i dati
6. Tornare allo step 3

Analisi della rete e TroubleShooting: Esiste un esempio di questo metodo per il **troubleshooting. Un utente** su una rete, chiama l'help desk per segnalare che il proprio computer **non può stare a lungo connesso ad internet**. L'help desk riempie il rapporto degli errori e lo inoltra a noi, che siamo nel dipartimento di supporto della rete. Poi possiamo parlare direttamente con l'utente e chiedere **se esso ha fatto qualcosa di differente** rispetto alle solite azioni di sempre, su internet. Si controlla **i log dell'hardware** relative alle interfacce di rete, e si trova che l'utente di tale computer è stato **upgradato la scorsa notte**. Si nota che i **driver** del computer sono stati configurati in modo non corretto. Si va quindi sul loco e si cntrolla la configurazione di rete sul computer. Essa sembra essere corretta, quindi si **pinga il server** sulla subnet ma non arriviamo ad una connessione.
La prossima soluzione è **controllare il plug** del cavo collegato alla workstation. Si verifica entrambi le **connessioni dei cavi** e quindi si prova di nuovo a **pingare il server**. Esso continua a non offrire connettività. Dunque proviamo a **pingare 127.0.0.1**, il lookback del computer. Il ping risulta attivo, quindi **si elimina possibili problemi fra il computer, la configurazione driver, e la scheda di rete**.
Si decide quindi che potrebbe esserci un problema con il server per questo segmento di rete. C'è un altro computer nella prossima scrivania, dnque si pinga l'indirizzo del server ed il risultato è Positivo. Questo elimina il problema sul server, sul backbone e sulle connessioni al server.
Quindi si va **sull'idf e si cambia le porte** relative alla workstation. Si torna sulla workstation e di nuovo si prova il ping. La soluzione **non sembra dare un risultato** soddisfacente. Questo ci fa capire che il problema **è situato lungo la cablatura orizzontale o sul cavo della workstation**.
Si torna indietro all'idf, si reinserisce il cavo nella porta originale, **sostituendo però il cavo che va dalla patch alla workstation**. Si prova di nuovo ad **eseguire un ping**. Questa volta il **risultato è soddisfacente**, dunque il problema **è risolto**.
L'ultimo punto è per **documentare la soluzione** del problema riguardo il **report di errore** e far ritornare all' Help Desk così che possa essere **segnato come caso risolto**.
Come è possibile vedere in questo esempio, è stato **relizzato un processo step-by-step** in cui sono state eliminate le **possibili cause** del problema di rete. Ogni possibile problema è stato centrato ed individualmente, eliminato. Se si eseguono **multipli cambiamenti** allo stesso tempo, il processo **può essere confuso e la soluzione non identificata e trascritta con sufficiente chiarezza**. Dunque la soluzione potrebbe esser **implementata senza trovare la soluzione** al problema; I dati in quel caso dovrebbero essere rivalutati e potrebbe esser **formulata una nuova soluzione** al problema. Questo processo continua finchè il problema attuale non è stato individuato e risolto. **Il problema verrà documentato per usi futuri**.
Non importa quali tipi di problemi si incontreranno in un sistema di rete, **il processo per la risoluzione sarà sempre lo stesso**. Quest'ultimo è il processo descritto precedentemente nel capitolo.

SEMESTRE 4

Wan e Wan Design

Servizi Wan: Una Wan è una rete di comunicazioni dati che opera oltre la portata **geografica**. La wan è una forma differente di lan. Per stabilire una connessione WAN ed usare i **servizi wan network carrier**, ci si deve iscrivere ad **una compagnia "regional Bell" (RBOC),** o Wan service provider. Una Wan utilizza **data link** per comunicazioni ISDN e frame relay. Queste sono fornite da **servizi carrier** per accedere alla banda oltre l'area geografica. Una Wan fornisce **connettività fra organizzazioni,** servizi e utenti remoti. Le Wans generalmente trasportano video, dati e voce. Le **funzioni Wan sono situate sui 3 livelli** più bassi del modello OSI. Dunque, livelli Fisico, data link e Network. I servizi dati e Telefonia sono più comumenente collegati ai Servizi WAN. I servizi Dati e Telefonia avvengono con collegamenti **dal POP all'ufficio centrale** provider WAN (CO). Il **CO** è la **compagnia locale di telefonia**; L'ufficio centrale che convoglia tutti i collegamenti di una determinata area il cui circuito **effettua uno Switching** delle vare linee. I servizi Wan possono dividersi in 3 Tipologie principali:

- Call Setup: Setta e **rende pulite le chiamate** fra utenti telefonici. E' anche chiamato "signaling", calls etup, usa un canale telefonico separato che non viene generalmente usato per altro trattico.Il call setup più comunemente usato è il **"signaling System 7"** (SS7), che usa il telefono per controllare messaggi e segnali fra il punto di trasferimento lungo il percorso relativo alla destinazione chiamata.
- Time-Division Multiplexing (TDM): Le informazioni che provengono da numerose sorgenti hanno allocazione di banda su un singolo media. Il Circuit Switching **usa il Signaling per determinare il route** della chiamata, a cui è dedicato un percorso fra inviatario e ricevente. Multiplexando il traffico in time slot dedicati, **TDM evita la congesione** ed i ritardi. Il sistema di telefonia base e ISDN utilizzano circuiti TDM.

- Frame Relay: Le informazioni contenute nei frames **condividono Banda** con altri utilizzatori\utenti frame relay WAN. Frame Relay è un servizio **multiplexed statico**, che a diffferenza di TDM, **usa identificatori di livello 2 e circuiti virtuali permanenti**. In aggiunta, il **packet switching** del frame relay utilizza il **router di livello 3** con l'indirizzo dell'inviatario e del ricevente contenuti nel pacchetto.

CPE, demarc, last mile, CO switch, e strumenti di rete: Providers di servizi Wan. L'avanzamento della tecnologia rispetto al passato, ha fatto in modo che nascessero numerose soluzioni addizionali per il design delle Wan. Quando si sceglie un'appropriata soluzione Wan, si deve discutere sui **costi e sui benefici** di ognuna con il nostro service providers. Quando una organizzazione sottoscrive un servizio Wan Esterno, il **provider fornisce la connessione** e **tutto il necessario** per la connettività. In questo caso, l'occorrente che viene fornito dev'essere **usato per Ricevere il servizio**, fra i più comuni possiamo ricordare:

- Customer premises equipment (CPE) – Periferiche fisicamente locate Localmente **in ambito del sottoscrittore.** Includono sia **periferiche**

che appartengono al sottoscrittore o affittate dal sottoscrittore al service provider.

- Demarcation (or demarc) – E' il punto su cui CPE finisce ed la **porzione locale in cui il servizio inizia**. Ciò avviene solitamente nei **dintorni del POP** dell'edificio.
- Local loop (or "last-mile") – Il cablaggio che si estende **dalla Demarc all'ufficio centrale del provider** Wan.
- CO switch – Uno switching facility che fornisce il **punto più vicino di presenza per il provider** di servizi Wan.
- Toll network – I collettivi switches e facilities (chiamati trunks), all'interno della nuvola di rete WAN del provider. Il traffico della persona che chiama può attraversare un trunk per poi arrivare ad un centro primario, successivamente ad un centro di sezione, quindi ad un REGIONAL, o interregional centro di chiamata, dunque la chiamata attraversa lunghe distanze per arrivare a destinazione.

Un'interfaccia chiave nel customer site, si trova **fra il DTE ed il DCE**. Tipicamente il **DTE** è il **router**. Il **DCE** è la periferica usata per **convertire** i dati utenti dal DTE in una forma più accettabile sulla Wan Service facility. Il **DCE è l'attacco modem**, il canale di servizio\unità (CSU/DSU), o un Terminal adapter\network adapter (TA\NT1). Il percorso Wan fra i DTE è chiamato, **Link, Circuito, Canale o Linea**. Il **DCE fornisce primariamente un'interfaccia per DTE** nel comunication link sulla nuvola Wan. Le interfacce DTE\DCE hanno **una limitazione**, ove la resposanbilità per il traffico è attribuita al passaggio dati fra il sottoscrittore WAN ed il provider WAN. Le interfacce DTE\DCE **usano vari ptoocolli** come ad esempio **HSSI e V 3.5.** Questi protocolli stabiliscono i codici che le periferiche usano per comunicare con altri. L'operazione di **setup ed i percorsi per il traffico** utente sono determinati per **mezzo di questa comunicazione**.

Circuiti Virtuali Wan: Un virtual circuit è un **circuito logico**, in sostanza è l'opposto del Point-to-point circuit. Esso è creato per garantire la **comunicazione affidabile** fra 2 periferiche. Esistono 2 tipi di circuiti virtuali. Essi sono, **Switched Virtual Circuits** (SVCs) e **Permanent Virutal Cirtuits** (PCVs).
Gli SVCs sono circuiti virtuali che sono stabiliti **dinamicamente su domanda e terminati quando la trasmissione è completa**. La comunicazione oltre un SVC consiste in 3 fasi. Esse sono: **Stabilimento** del circuito, **trasferimento** dati, e **terminazione** del circuito. La fase di stabilimento porta alla creazione di circuiti virtuali fra periferiche sorgenti e di destinazione.
Il trasferimento dati, porta a trsmettere dati fra periferiche tramite circuiti virtuali. La fase di circuit-termination, porta alla lacerazione del circuito virtuale fra periferiche sorgenti e di destinazione. Le SVCs sono usate in situazioni **dove la trasmissione dei dati fra periferiche è sporadica**. La fase di stabilimento e terminazione dell' SVCs crea un piccolo sovraccarico di rete, ma è sempre inferiore rispetto al sovraccarico generato dalla creazione di circuiti virtuali costantemente disponibili.
Un **PVC stabilisce permanentemente circuiti virtuali** che consistono in una **"modalità" definita** Data Transfer. PVCs sono usati in situazioni in cui i trasferimenti dati fra periferiche **sono costanti**. I PVCs **diminuiscono la banda** in associazione con lo stabilimento e la terminazione dei circuiti virtuali, ma **incrementano il costo** dovuto alla costante disponibilità dei virutal-circuit.

Tipi di linea Wan: I Links Wan sono disponibili dal provider di rete, **ad un certo BitRate** che specifica la **Capacità del Link**, misurata in bit per secondo. (BPS). Questa capacità determina quanto velocemente i dati possono essere mossi attraverso un link WAN. La banda Wan è spesso approvigionata dagli Stati Uniti utilizzando la hierarchia North American Digital

Fondamenti sulle Periferiche Wan: Le Wans usano numerosi tipi di periferiche, includono:

- **Routers** che offrono molti servizi, includendo **porte d'interfaccia WAN e LAN**.
- **Switch WAN** che **connettono WAN e forniscono banda** per Voce, Data e Comunicazioni video.
- **Modems** che interfacciano **voice-grade** services. I Modems includono **CSUs\DSUs** e periferiche TA\NT1, che si **interfacciano a servizi ISDN**.
- **Server di comunicazione**, che concentrano **comunicazioni utente Dial-In e Dial-Out**.

Router e Switch Wan: I **Routers** sono periferiche che **implementano servizi** di rete. Essi **forniscono interfacce** per un vasto range di Links e sottoreti con un vasto range di velocità. I Routers sono periferiche di rete **attive ed intelligenti** e possono partecipare nel management della rete. I Routers getiscono le reti, fornendo **controllo dinamico** oltre risorse e supportando i tasks e gli obiettivi delle reti. Questo obiettivi sono la **connettività, l'affidabilità, la performance, i controllo di management e la flessibilità**. Uno **Switch** è una periferica di networking **multi-porta**. Esso tipicamente **switcha** il traffico come **frame relay, x25** e Switched Multimegabit Data Service (SMDS). Gli switch lan, tipicamente **operano al livello Data Link**, del modello osi. Esempio, Due Routers possono esser connessi, su sistemi finali connessi **su switch WAN**.

Modem su una Wan: Un modem è un periferica che è usata **per connessioni fra reti digitali**, e line telefoniche Voice-grade. **Alla sorgente**, i segnali **digitali sono convertiti** appropriatamente per la trasmissione su comunicazione **analogica**. **Alla destinazione**, questi segnali analogici sono **di nuovo convertiti in forma digitale**.

CSU-DSUs su una Wan: Un CSU\DSU è una delle due **interfacce digitali**, o diverse separate periferiche digitali. Esso **adatta l'interfaccia fisica sulla periferica DTE** (come ad esempio un terminale), **e sulla interfaccia DCE** (come ad esempio uno switch), in una switched-carrier network.
Spesso **CSUs\DSUs sono integrati nel router Box**.

Adattori Terminali ISDN su una Wan: Una ISDN **Terminal Adapter** (TA) è una periferica usata per **convertire i segnali standard elettrici, in una forma usata da ISDN**, così anche le periferiche **non ISDN possono collegarsi** alla rete. Per esempio un TA può essere usato per **connettere una porta seriale di un router** ad una periferica BRI.

Organizzazioni che si occupano degli standard Wan: Wan come Lan, **utilizza** il modello **OSI** livellato per l'encapsulation. Tuttavia, le WANs sono concentrate soprattutto **sul livello phisical e data link**. Gli standard Wans descrivono sia il **delivery sul sistema fisico** che i **requisiti** per il **DATA-Link**., includendo **l'addressing, il controllo di flusso e l'encapsulation**. Gli wan standard sono definiti e gestiti da un numero di autorità riconosciute fra le quali:

- International Telecommunication Union-Telecommunication Standardization Sector **(ITU-T)**, formerly the Consultative Committee for International Telegraph and Telephone **(CCITT)**
- International Organization for Standardization **(ISO)**
- Internet Engineering Task Force **(IETF)**
- Electronic Industries Association **(EIA)**
- Telecommunications Industries Association **(TIA)**

Livelli fisici Wan Standard: Il protocollo di livello fisico WAN, descrive come viene **fornito il meccanismo elettrico** e come vengono **effettuate le operazioni funzionali** di connessioni per i servizi WAN. Molte wan **richiedono una interconnessione** che è fornita da una **comunicazione di service provider (Come RBOC**), un carrier alternativo (come ad esempio un internet service provider), un post telephon o un'agenzia telegrafica (PTT).
Il livello fisico Wan descrive inoltre **l'interfaccia fra DTE e DCE**. Tipicamente il **DCE** è il service **provider**, ed il **DTE** e la **periferica** collegata.
Esistono molti standard fisici i quali definiscono delle **regole** governative **sulle interfacce fra DTE e DCE.**

- **EIA/TIA-232** – Un livello standard **d'interfaccia fisica comune**, creato da EIA e TIA che supporta **circuiti non bilanciati** alla velocità di 64 kbps. Esso ricorda la specifica V.24, conosciuta come RS-232. Questo standard è stato utilizzato per molti anni.
- **EIA/TIA-449** – Un'interfaccia di livello fisico molto popolare, creata da EIA e TIA, Essa essenzialmente è una **versione più veloce di EIA\TIA-232** (Oltre 2 Megabit), capace di percorrere lunghe distanze.
- **EIA/TIA-612/613** – Uno standard relativo alle **High Speed Serial Interface** (HSSI), che **fornisce accesso ai servizi ad una velocità di** 45MBPS per T3, E3 a 34MBPS, e SONET STS-1 a 51,84MBPS

- **V.24** – E' un ITU-T standard per **interfacce di livello fisico fra DTE e DCE**.
- **V.35** – E' uno standard ITU-T che **scrive un protocollo di livello fisico**, synchronous, usato per **le comunicazioni fra periferiche** che accesdono alla rete e **packet network**. V.35 è usato molto comunemente negli Stati Uniti ed in Europa, ed è raccomandato per comunicazioni la cui velocità **supera i 48Kbps**.
- **X.21** – Uno standard ITU-T per le comunicazioni **seriali tramite digital lines** synchronous. Il protocollo X.21 è usato primariamente in Europa ed in Giappone.
- **G.703** – Una ITU-T specificazione elettrica e meccanica per connessioni fra compagnie telefoniche e DTE utilizzando British Naval Connectors (BNCs) ed **operando ad un data rate pari a quello di una E1**.
- **EIA-530** – Due **implementazioni elettriche** di EIA\TIA-449: RS-442 (**Per trasmissioni bilanciate**) e RS-423 (Per trasmissioni non-bilanciate)

Descrizione delle 6 Encapsulation Wan: Il livello Wan Data Link definisce **come i dati sono encapsulati** per la trasmissione a siti remoti. I protocolli Wan Data-Link descrivono **come i frames sono trasportati** fra sistemi su un singolo percorso.

- **Frame Relay** – Può **trasmettere** i dati **molto rapidamente** rispetto agli altri protocolli WAN. Utilizza **un'encapsulation semplificata** senza meccanismo di correzione di errori, e trasmette con un segnale digitale di alta qualità..
- **Point-to-Point Protocol (PPP)** – Rappresentata da RFC 16661, PPP **fu realizzata da IETF**. PPP contiene un campo di protocollo che identifica il **protocollo relativo al livello di rete**.

- **ISDN** – Un set di servizi digitali che trasmettono **voce e data sulle linee telefoniche esistenti**.
- **Link Access Procedure, Balanced (LAPB)** – Per reti di tipo packet-switched, LAPB è usata per **encapsulare pacchetti** al livello 2 sull'X.25 stack. Esso può anche essere usato su un point-to-point link se il link è inaffidabile o se c'è un ritardo inerente associato al link, come ad esempio un satellite link. Il LAPB fornisce **affidabilità e controllo di flusso** su base point-to-point.
- **Cisco/IETF** – Usato per **encapsulare il traffico** Frame Relay. Questa opzione cisco è proprietaria e può essre usata **solo fra routers Cisco.**
- **High-Level Data Link Control (HDLC)** – Uno standard ISO, HDLC può non essere compatibile con differenti venditori poichè ognuno di essi ha scelto una **differente implementazione**. HDLC supporta sia configurazioni point-to-point che multiport.

Linee seriali, Campi Frame: Due dei più comuni encapsulation wan Point-To-Point sono **HDLC e PPP**. Tutti gli encapsulation delle linee seriali hanno **in comune un formato frame**, che è composto dai seguenti fields:

- **Flag** – Indica **l'inizio del frame** ed è settato in Esadecimale (BASE 16), pattern 7E.
- **Address** – Un campo di 1 o 2 bytes che indirizza **la stazione finale** in multidrop environments.
- **Control** – Indica **se il frame è una informazione, un supervisory o un tipo di frame** non riconosciuto. Esso contiene anche specifiche funzioni in codice.
- **Data** – I dati Encapsulati.
- **FCS** - The frame check sequence (FCS).
- **Flag** - The trailing 7E flag identifier.

Ogni connessione Wan utilizza un **protocollo di livello 2** per encapsulare il traffico **durante il passaggio sul link WAN**. Per essere sicuri che venga usata un corretto encapsulation protocol, è necessario configurare il **tipo di encapsulation** a livello 2 **per ogni interfaccia seriale sul router**. La scelta del protocollo di encapsulation, **dipende dalla tecnologia wan** e dagli equipaggiamenti hardware di comunicazione. I protocolli di encapsulation che possono essere usati **con le connessioni wan, sono PPP e HDLC.**

PPP: PPP è uno standard **di encapsulation** su linea **seriale** (descritto in RFC 1332 e RFC 1661). Questo protocollo può, in altre parole, **controllare la qualità del link** durante la connessione (Quando essa è stabilita). In aggiunta esiste un **supporto di autenticazione tramite PAP e CHAP** (password authetincation Protocol e Challenge Handshache Authentication Protocol).

HDLC: E' un protocollo di livello **data link derivato dal SDLC** (synchronous Data Link Control, Encapsulation protocol. HDLC è una **encapsulation cisco** usata di default **per le linee seriali**. Questa implementazione è **molto semplificata**. **Non esiste windowing né flow control**, un codice di 2 byte proprietario è inserito dopo il field di controllo. Questo vuol dire che **il framing HDLC non è utilizzabile con altri tipi di equipment**. L'encapsulation HDLC è tipicamente usato quando **entrambi** le fini relative a connessioni di linee dedicate, **sono routers o access server**, sui quali sta girando **un sistema IOS** Cisco. Poiché il metodo di encapsulation **HDLC può variare**, PPP

dev'essere usato con **periferiche che non stanno utilizzando il software IOS**.

Due opzioni base del link Wan: In generale, esistono 2 tipi di Win Link. Queste opzioni sono **linee dedicate e connessioni "switched"**. Le **connessioni Switched**, a loro volta, possono essere **circuit switched o packet switched**.

Linee Dedicate: Le linee dedicate, sono chiamate anche **Leased Lines**, e forniscono un servizio **a tempo pieno** (NON STOP). Le linee dedicate sono tipicamente usate per **trasportare data ed occasionalmente anche video**. Nel design di rete, le **linee dedicate** tipicamente **forniscono Connettività CORE o BACKBONE** fra siti maggiori o campus, ad esempio, Connettività Lan-To-Lan. Le linee dedicate sono considerate le **opzioni ideali per il design** delle Wan.
Quando vengono create connessioni su linee dedicate, è **indispensabile una porta sul router**, per ogni connesione, fra il CSU\DSU e l'attuale circuito relativo al service provider. Il costo di una soluzione per linea dedicata **può diventare significativo** quando esse sono usate per la connessione **con numerosi sites**.

Leased Lines: La connettività Dedicata, full time, è fornita Point-To-Point **da link seriali**. Le connessioni sono eseguite utilizzando le porte synchronous seriali del router, con **utilizzo tipico della banda attorno ai 2 megabit** (E1), disponibile attraverso l'uso del CSU\DSU.
Differenti metodo di encapsulation al livello data link, forniscono **flessibilità e affidabilità** per il traffico utente. Linee dedicate di questo tipo sono ideali per ambienti in cui vi è **un ampio traffico**. L'utilizzo della banda disponibile è un INTERESSE, in qunato è necessario pagare per la disponibilità della linea, anche quando la connessione è in IDLE. Le linee dedicate sono riferite sempre a link point-to-point.Il **percorso stabilito è permanente** e **fissato per ogni rete remota** raggiunta tramite il carrier facilities. Un **link point-to-point fornisce una singola, comunicazione** wan pre-stabilita, sul percorso che va dal customer, alla rete remota. Il service provider fornisce link point-to-point per uso privato del customer. Point-to-Point è usato per connessioni link dirette e fisiche, o link virtuali che consistono in multipli link fisici.

Connessioni Packet-Switched: La Packet Switching è un **metodo di Wan Switching** in cui le periferiche di rete, **condividono un circuito virtuale** permanente (PVC) che **trasporta pacchetti dalla sorgente alla destinazione**, tramite una carrier network. Un PVC è similare ad un link Point-to-Point. Frame relay, SMDS, e X.25 sono tutti **esempi di tecnologie wan** di tipo packet-switched. Le reti di tipo switched **possono trasportare frames o pacchetti di varie dimensioni**, o celle di dimensione fissa. Il tipo di rete packet-switched più comune è la Frame Relay.

Frame Relay: Frame Relay è stata designata per essere usata su linee ad **Alta-velocità** con qualità digitale.
Come risultato, frame relay **non ha un grande error checking** e non è particolarmente affidabile. Frame-Relay attende i protocolli di livello superiore per la distribuzione dei dati.
Frame-Relay è una **tecnologia di comunicazione**, del tipo Packet-Switching. Essa può connettere multiple periferica di rete su una multiport wan. Il design del frame relay wan **può coinvolgere certi aspetti dei protocolli superiori** (come ad esempio split horizon), esempio IP, IPX, Apple-Talk. Frame Relay è chiamata non-broadcast, **multi-access tecnology**, poiché essa **non ha canali broadcast**. I broadcasts sono trasmessi tramite frame relay inviando pacchetti alla rete di destinazione. Frame-Relay definisce la connessione **fra un customer,DTE, ed un carrier, DCE**. Il **DTE è tipicamente un router, ed il DCE è uno switch Frame Relay**. (In questo caso, DTE e DCE si riferiscono al livello Data Link, non al livello fisico). L'accesso Frame-Relay è tipicamente a 56k, 64k o 1.544Megabit.

Frame Relay non è un'alternativa cost-effective al design wan point-to-point. Un sito può essere connesso ad altri **tramite un circtuito virtuale**. Ogni router necessita **solo di un'interfaccia fisica** per il carrier. Frame-Relay è spesso **implementato come servizio carrier-provided**, ma può anche essere usato per reti private. Il servizio Frame-Relay è offerto tramite un PVC. Un PVC è un data link non affidabile. Un identificatore Data-Link (DLCI) identifica un pvc. Il numero DLCI, è un **identificativo locale frame DTE e DCE**., che identifica il circuito logico fra la periferica sorgente e quella di destinazione. Il Service Level Agreement (SLA), specifica il Committed Information Rate (CIR), fornita dal Carrier, che è il Rate, in bit per secondo, a cui il frame relay conferma e switcha i dati (transfer rate). Possono essere usate due tipologie comuni di frame relay:

- **Fully meshed topology** – Ogni periferica Frame Relay ha **un PVC per ogni altra periferica** sul Multiport WAN. Ogni update inviate da una periferica **è visto da tutte le altre** periferiche, Se si utilizza questo design, **l'intera Frame Relay WAN, può comportarsi come se fosse un unico Data Link**.

- **Partially meshed topology** – Può essere chiamata anche STAR TOPOLOGY, o Hub-And-Spokes topology. In questa topologia non **tutte le periferiche sul frame relaty devono avere un PVC per ogni altra periferica**.

Connessioni Circuit-Switched: Il Circuit Switching è un metodo di Wan Switching, in cui vengono stabiliti **circuiti virtuali**, mantenuti, e terminati **tramite una carrier network per ogni sessione di comunicazione**.Molto frequentemente usati in reti di compagnie telefoniche, le circuit switching operano similmente alle normali chiamate telefoniche. **ISDN è un esempio** di una tecnologia WAN di tipi Circtuit-switched. Le connessioni Circuit-switched da un site ad un altro sono effettuate **quando è necessaria una Low Bandwith**. I servizi base di telefonia generalmente operano a velocità **non maggiori dei 56k**, e Basic ISDN Connection (**BRI**), forniscono linee a **velocità di 64 e 128kbps**. Le connessioni **Circuit-switched** sono usate primariamente per **connettere utenti remoti e utenti mobili a corporate Lan.**Essi sono anche usati come **backup line** per circuiti ad alta velocità, come Frame Relay e linee dedicate.

DDR (Dial On Domand Routing): Il dial-on-demand routing (**DDR**) è una tecnica in cui un router può **dinamicamente iniziare e chiudere una sessione di tipo circuit-switched**, quando una stazione **necessita di effettuare la comunicazione**. Quando il router riceve una chiamata di traffico destinata per una rete remota, il **circuito viene stabilito**, ed il traffico è normalment etrasmesso. Il router mantiene e **mette in idle un timer** che è resettato solo quando il traffico che interessa la rete esterna è ricevuto. Se il router **non** riceve il traffico interessato per il routing verso l'esterno, **entro il tempo impostato, il circuito viene terminato**. Al contrario se traffico non interessato è ricevuto e non esistono circuiti, il router elimina questo traffico. Quando il router invece, riceve traffico interessato, **esso inizializza un nuovo circuito**.
DDR permette una connessione telefonica **standard o una connessione ISDN** solo quando è necessario da **un flusso di traffico** di rete. DDR può essere **meno dispendiosa** rispetto ad una linea dedicata o una soluzione multiporta. DDR vuol dire che la connessione è stata realizzata **solo quando è stato inizializzato un trasferimento** di traffico specifico, o inizializzata una chiamata. DDR è una sostituta delle linea dedicata quando non è richiesta\supporta al disponibilità di traffico full time. In aggiunta, DDR può essere usata per **sostituire links point-to-point e servizi switched multi access WAN**. DDR può essere usata per fornire **backup load sharing** o backup delle interfacce. Per esempio molte linee seriali possono esistere, ma la seconda linea può solo essere usata **quando la prima linea è occupata** o **quando esiste un carico eccessivo** di richieste per la rete. Quando una linea WAN è usata **per applicazioni critiche**, una linea DDR può essere configurata per l'utilizzo **nel caso in cui la linea primaria vada giù**. In questo caso, appunto, la

linea secondaria si abilita e il traffico può proseguire attraverso essa. Comparandolo con le LAN classiche o Campus-base, il traffico che DDR **utilizza è tipicamente di "basso volume"** e sporadico. DDR inizializza **una wan verso un remote site** solo quando c'è traffico da trasmettere. Per configurare una DDR, si entra nella configurazioni comandi che indica quali pacchetti e protocollo ci interessano per inizializzare la chiamnata. Fatto questo, è inserita una access control list per identificare l'indirizzo della sorgente e della destinazione, e speficicare i criteri di protocollo per inizializzare la chiamata e concluderla.
Quindi **l'interfaccia su cui la chiamata DDR viene indirizzata, si inizializza**. Questo step riguarda un gruppo di Dialing. Il dialer group associa i risultati della specifica access control list, che interessa un pacchetto, ad un'interfaccia router per il dialing verso una chiamata WAN.

Descrizione dell'ISDN: Le compagnie telefoniche hanno **creato ISDN** con l'intenzione di **creare una rete totalmente digitale**. Le periferiche ISDN includono:

- Terminal Equipment 1 (TE1) – Indicano una periferica **compatibile con la rete ISDN**, Una TE1 connette una NT di tipo 1 o 2.
- Terminal Equipment 2 (TE2) -- Designates a device that is **not compatible with ISDN** and **requires a TA.**

- TA -- **Converte** segnali elettrici standard in una forma **usata da ISDN** per cui anche **periferiche non-ISDN possono connettersi con le reti ISDN**.
- NT Type 1 (NT1) – Connette il sottoscrittore con 4-cavetti ISDN al loop facility locale con collegamento tramite 2-Cavetti..

- NT Type 2 (NT2) – Direziona il traffico a e **da differenti periferiche subscriver**, e NT1. La NT2 è una **periferica intelligente** che esegue lo **switching** ed il concentrating.

- L'interfaccia S\T definisce l'interfaccia fra TE1 e NT. Il S\T è anche usato per definire l'interfaccia da TA a NT.
- L'interfaccia R definisce l'interfaccia fra TE2 e TA.
- L'interfaccia U definisce l'interfaccia a 2 cavi, fra NT e la nuvola ISDN.

Esistono 2 servizi ISDN: Basic Rate Interface (BRI) e Primary Rate Interface (PRI). La ISDN **BRI**, opera spesso **su cavo "copper twisted pair"** telefonico cablato attualmente in tutte le case. ISDN BRI trasporta **una banda totale di dati pari a 144Kbps** in **tre canali** separati. Due dei canali, **chiamati B (bearer) channels, operano a 64Kbps e sono usati per trasportare voce o traffico dati. Il terzo canale, il D (delta) channel,k è un canale a 16kbps, usato per trasportare istruzioni che dicono alla rete telefonica come indirizzare ognuno dei 2 canali**. ISDN BRI spesso è riferita a **2B+D.** ISDN fornisce grande flessibilità al designer di rete poichè ha la capacità di usare ognuno dei B channels per **separare applicazioni voce e dati**. Per esempio, una ISDN da 64kbps (b channel), può downloadare un grande documento dalla corporate network, mentre l'altro B channel fa il browse di una web page. Quando si designa una WAN, è necessario fare attenzione nella **selezione dell'equipaggiamento** che ha la proprietà futura di estendere la flessibilità ISDN.

WAN DESIGN

Requisiti per il WAN DESIGN: Le comunicazioni WAN avvengono **fra aree geografiche separate**. Quando una stazione finale locale vuole comunicare **con una end stazione remota** (locate su differenti Sites), le informazioni devono essere inviate **tramite uno o più links** WAN. I **routers** all'interno delle Wans rappresentano **punti di connessione** alla rete. Questi routers determinano il percorso più appropriato tramite il quale il traffico deve passare per la trasmissione dello stream di dati. Le comunicazioni Wan sono **spesso chiamate Servizi** poiché il network service provider (spesso la compagnia telefonica), danno agli utenti i servizi wan che essi chiedono. Due tipi di **servizi Wan sono Packet-Switching e Circuit-switching**, ognuno di queste 2 tecnologia ha vantaggi e svantaggi. Per esempio le reti di tipo **Circuit-switched** offrono agli utenti **banda dedicata** che non può influire (né negativamente né positivamente) con altri utenti, ma le risorse di rete possono essere **sotto-utilizzate durante il periodo di BASSo traffico**. Contrariamente a ciò, **packet switching** permette alle risorse di chiamata di essere **condivise da diversi utenti** poichè ogni pacchetto contenenti informazioni di indirizzo non permette lo switching sul percorso disponibile. Le reti di tipo Packet switched offrono **grande flessibilità** ed usano la **banda** di rete **più efficentemente** rispetto alle reti circuit-switched, ma se c'è un **sovraccarico** di rete, i pcchetti possono **ritardare o essere scartati**. Tradizionalmente, una bassa portata, un alto ritardo ed un ampio livello di errori, caratterizzano le comunicazioni WAN. Le connessioni WAN inoltre **caratterizzano un costo del cavo, dal service provider alla connessione** (campus).
L'infrastruttura è spesso presa in **affitto** dal service provider. Perciò una design di una WAN deve minimizzare il costo di Banda ed ottimizzare quello di banda\efficenza. Per esempio, tutte le tecnologia e le funzionalità, usate in WAN sono sviluppate per adattarsi ai seguenti presupposti:

- Ottimizzare la **banda** WAN
- Minimizzare il **Costo**
- **Massimizzare l'effettivo servizio** dato agli utenti.

Le reti tradizionali costituite da Media condiviso, sono state superate per le seguenti richieste relative alle nuove reti:

- L'utilizzo della rete è stato implementato **per l'utilizzo di Enterprise Client\Server**, multimedia, ed altre applicazioni di produttività avanzata.
- **Il tasso di cambiamento** in termini di necessità applicative continua ad accellerare con nuovi sviluppi quali ad esempio "internet Push" technlogies.
- Con l'aumentare dei servizi forniti agli utenti, **le applicazioni aumentano la domanda di servizi richiesti alla rete**.
- Un imprecisato **numero di connessioni** sono state stabilite presso uffici di tutte le dimensioni, utenti remoti, utenti mobili, siti internazionali, customer\suppliers e internet.
- La crescita esplosiva di corporate **intranets e di extranets** ha creato una grande domanda di banda.
- L'uso di **enterprise server continua a crescere** per servire le necessità lavorative delle organizzazioni.

Le nuove infrastruttura WAN devono essere **più complesse**. Esse sono basate su nuove tecnologie ed in grado di affrontare **ogni tipo di incremento**, e di applicazioni miste con livello di servizio Garantito. E' stato previsto un incremento del traffico pari al 300%, per i prossimi 5 anni, che **inciterà a contenere i costi delle Wan**. Le connessioni WAN sono generalmente usate per **trasportare informazioni importanti**, e sono ottimizzate nel rapporto costo\performance. I routers che connettono i campus, per esempio, generalmente applicazionо una ottimizzazione del trraffico, multipli percorsi per redundanza, dial backup per il recupero della distanza e **qualità del servizio (QoS)** per applicazioni critiche.

Integrazioni LAN\WAN: Le applicazioni distribuite necessitano costantemente di un **incremento di banda**. La diffusione **dell'uso di internet**, è una cosa che ha creato delle **problematiche** per molte architetture lan già esistenti. Le comunicazioni voce si sono incrementate significativamente, con o senza la dipendenza su un voice mail system per comunicazioni verbali. La rete è uno strumento **critico per il flusso delle informazioni**. Le reti devono costare meno affinchè supportino applicazioni emergenti, ed un largo numero di utenti. La **performance deve essere incrementata**. Fino a poco tempo fa le comunicazioni lan e le wan erano **logicamente separate**. La **banda disponibile è essenziale**, nelle lan e la connettività e limitata solo dall'hardware e dai costi di implementazione. La banda ha un **costo ignorabile** nelle Wan. Le applicazioni internet come ad esempio **la voce ed il video** in real time, devono essere **prevedibili**, per cui è necessaria una LAN o WAN di ampie performance. Queste applicazioni multimediali sono diventate rapidamente una parte essenziale nel peso delle produttività di lavoro. Le aziende stanno iniziando a considerare implementazioni per quanto riguarda nuove intranet lan dotate di ampia banda per le applicazioni multimediali. Dunque includiamo **video training, video conferenza, e voce over ip**. L'impatto di queste applicazioni sulle attuali infrastrutture di networking esistenti, può diventare una faccenda seria. Supponiamo che un'azienda faccia affidamento sulla propria rete per traffico di lavoro e voglia integrare applicazioni di video-training. La rete dev'essere in grado di fornire **QoS garantito** (Quality of Service). Questo QoS deve trasportare il traffico multimediale ma non permettere ad esso di interferire con il traffico lavorativo, il quale ha primaria importanza (critical). Consecutivamente a ciò, i designers di rete hanno bisogno di **grande flessibilità** per risolvere multipli problemi di internetworking senza creare numerose reti o tirare ulteriori cablaggi, evitando ulteriori spese.

Obiettivi LAN\WAN: Designare una wan può essere una grande sfida. Le discussioni che seguono esternamente le diverse aree interessate devono essere considerate **durnate la fase di progettazione** ed **implementazione** di una WAN. Questi steps, descritti qui, possono abbassare i costi delle Wan e migliorarne la performance. I Lavoratori possono continuamente mettere alla prova le proprie WANs, incorporando questi steps nel processo di progettazione. I 2 obiettivi primari per il design delle Wan ed implementazione sono i seguenti:

- Application availability – Le reti trasportano informazioni di applicazioni fra computers. **Se le applicazioni non sono disponibili** per gli utenti di rete, **la rete non svolge il suo compito alla perfezione**.
- Total cost of ownership - Information Systems (IS) department budgets spesso viene espresso in milioni di dollari. Molte aziende fanno affidamento su **calcolatori elettronici per la gestione dei dati** e le attività lavorative associandosi al **costo relativo alle risorse operative che continua ad aumentare**. Un buon design wan può aiutare a bilanciare questi obiettivi. Quando è propriamente implementata, una infrastruttura wan, può **ottimizzare la disponibilità dell'applicazione ed il costo effettivo delle risorse di rete esistenti**.

Il **design di WAN** generalmente ha la necessità di tener conto di **tre differenti fattori**:

- Variabili di Ambiente:
  - La **locazione degli hosts**, server, terminali ed altri nodi finali.
  - Il **traffico** progettato per l'ambiente.The
  - Il **costo** progettato per fare il delivery dei defferenti **livelli di servizio**.

- Performance:
  - **Affidabilità** della rete
  - **Portata** complessiva di traffico.
  - **Velocità di Host\Client Computer**. Per esempio NIC o Hard Drive.
- Variabili di Networking:
  - **Topologia** della Rete
  - **Capacità** della Linea
  - Packet traffic

La caratterizzazione del traffico di rete è **un'operazione critica**, e fondamentale per il successo della pianificazione di una Wan. Molti progettisti curano questo aspetto, e lo considerano come **componente "chiave".** L'obiettivo complessivo del design di una wan si divide in 2 parti. Il **Costo deve essere minimizzato** in base a tre generali fattori menzionati. Le 2 questioni primarie sono la **disponibilità ed il costo**. Queste distribuzioni sono essenzialmente in discordia. Un INCREMENTO della disponibilità deve generalmente essere riflettuto su un aumento di costo. Dunque è necessario fare attenzione sul peso relativo all'importanza delle **risorse disponibili** e sul **costo che si deve affrontare**. Il primo step nel processo di design è comprendere **i requisiti lavorativi**. I requisiti della WAN devono essere riflessi sugli **obiettivi, le caratteristiche, i processi di business**, e le policy del business in cui essi operano.

I Requisiti per la fase di Gathering delle Wan: Il primo step nel design di una WAN è **raccogliere dati** sulla struttura lavorativa e processarli. Successivamente, determinare chi è **la persona più importante** che potrà aiutarci nel design della rete. Parlare con gli utenti principali, ed informarsi sulla loro **posizione geografica**, sulla **applicazione corrente** che stanno svolgendo e sulle **necessità progettuali**. Il design finale della rete deve comunque riflettersi sui requisiti degli utenti. In generale, gli utenti vogliono la disponibilità di diverse applicazioni nella loro rete. Il primo componente per l'operatività di applicazione **è il tempo di risposta, la portata e l'affidabilità**.

- **Il tempo di risposta è il tempo fra l'inseriento di un comando, l'esecuzione sull'host e il delivery della risposta**. Applicazioni in cui la il tempo di risposta rapido è considerato critico, includono servizi interattivi, online come ad esempio sistemi di messaggistica automatica, e "point of sale"..
- La **portata richiesta** da applicazioni intensive, generalmente è composta da Trasferimenti file, tuttavia la banda occupata da **applicazioni che lavorano in maniera particolarmente intensa** possono comportare un peso ed in particolare una tempo di risposta piuttosto lento. Effettivamente essa può essere schedulata; E' possibile tener conto dei momenti in cui il tempo di risposta è basso a causa di traffico.
- **l'affidabilità** è un fattore assai importante, molte applicazioni hanno requisiti che eccedono le necessità classiche. Le organizzazioni che conducono tutte le attività lavorative,online, e tramite telefono **richiedono circa il 100% di uptime**. Servizi finanziari, **scambi di sicurezza, emergenza, polizia, operazioni militari**, sono degli esempi. Queste situazioni richiedono un alto livello di affidabilità e

redondanza. Determinare il costo del downtime è essenziale al fine di determinare l'affidabilità della stessa rete.

Le necessità dell'utente possono essare assegnate in vari modi. Più persone utilizzeranno la rete, quanto più accurata sarà la valutazione sulle necessità. In generale per ottenere tali informazioni si segue i seguenti metodi:

- La maggior parte degli utenti ha gli **stessi requisiti** in termini di **email**, possono avere **differenti necessità** per quanto riguarda la **condivisioni di stampanti**, e la gestione di **print server** nella propria area.
- Interviste e **focalizzazione sui gruppi utenti**, portano a determinare **una Baseline** che poi sarà d'aiuto per l'implementazione della rete. E' necessario comprendere che certi gruppi necessitano dell'accesso a server comuni. Altri, possono aver bisogno di accesso esterno ad una specifica risorsa. Alcune organizzazioni possono aver bisogno dell'IS support system per poter gestire, in certe situazioni, accordi con standard esterni.
- Il miglior metodo,formale, per ottenere informazioni, è effettuare **interviste con le figure chiave del gruppo**. La focalizzazione dei gruppi può anche essere usata per raccogliere informazioni e generare discussioni su differenti organizzazioni con interessi simili o meno.Infine, è possibile fare uno sguardo formale per reperire valide statistiche riguardo **un particolare livello di servizio**.
- I **test sui fattori umani**, sono **molto costosi**, è necessario molto tempo ed è possibile scoprire metodi per valutare le necessità degli utenti. Questo sistema è spesso applicato quando si va a valutare le necessità relative ai **tempi di risposta** degli utenti. Per esempio noi effettuiamo un test su un sistema che sta già funzionando ed eseguendo normali attività remote sulla rete del laboratorio. Valutando le reazioni degli utenti riguardo la performance dell'host e degli strumenti che utilizzano è possibile creare **un minimo standard che garantisca performance sufficienti.**

Dopo aver raccolto dati sulla struttura corporate, si deve determinare dove **avviene il flusso di informazioni all'interno dell'azienda**. E' necessario localizzare i **dati Condivisi** e soprattutto sapere chi ne ha l'accesso e chi li utilizza. Determinare inoltre se è possibile accedere esternamente ai dati dell'azienda. E' indispensabile esser certi sulla **corretta distribuzione della performance** derivata dalle risorse esistenti. Se esiste tempo analizzare attentamente la performance della rete esistente.

Analisi dei Requisiti: I Requisiti della rete, devono essere analizzati, inoltre è necessario tener **conto dei clienti** e delle specifiche relative agli **obiettivi tecnici**. Quali nuove applicazioni saranno implementate? Tali applicazioni sono basate su internet? Come possiamo sapere se i nuovi design avranno successo?
E' necessario misurare le **disponibilità Utili della rete**. Sono molti i fattori che hanno effetto sulla disponibilità, ad esempio **la portata, il tempo di risposta, e l'accesso alle risorse**. Ogni customer ha una differente definizione di disponibilità. La disponibilità può essere incrementata

aggiungendo più risorse. Le risorse tuttavia aumentano il costo. Il design di rete ha come obiettivo FORNIRE maggiore disponibilità **ad un costo ridotto**. L'obiettivo dell'analisi dei requisiti è determinare **una media ed un traguardo**, sul data rate per ogni risorsa, nel tempo. Definire le attività del normale lavoro giornaliero. In questa definizione è necessario includere **il tipo di traffico passato, il livello di traffico, il tempo di risposta degli host ed il tempo in cui avvengono i file transfer**. Osservare l'uso delle **apparecchiature** di rete per un periodo di test. Se le caratteristiche della rete testata sono prossime a **quelle della nuova rete**, i nuovi requisiti per questa rete possono essere stimati, in base al numero di utenti che è già stato progettato, applicazioni e tipologia. Questo è il miglior approccio per la stima del traffico in condizioni in cui mancano gli strumenti per misurare il comportamento del traffico, nei dettagli.
In aggiunta, è possibile **monitorare passivamente una rete già esistente**, misurare l'attività ed il traffico generato da un numero conosciuto di persone, collegate ad una rete test rappresentativa. Utilizzare quindi i risultati per **ipotizzare attività e traffico per la popolazione anticipata**. Un problema nella definizione del carico di lavoro sulle reti, è che non è facile localizzare con esattezza il carico relativo al traffico e le performance delle periferiche di rete, per quanto riguarda la loro funzionalità in rapporto al numero di utenti, al tipo di applicazione ed alla locazione geografica. Tutto ciò è valido se non si ha una posizione reale sul network. Considerare i seguenti fattori che influenzano la **dinamica della rete**:

- Il tempo che dipende **dalla natura dell'accesso di rete** durante il periodo di **picco**, può variare. Le misurazioni possono dare vari risultati, uno fra questi può essere il picco di domanda.
- Le differenze associate con il tipo di traffico come ad esempio **il Routed e lo Switched traffico, genera differenti domande** alle periferiche di rete ed ai protocolli.Molti protocolli sono sensitivi ai pacchetti scartati, **molte applicazioni richiedono una banda maggiore**.
- La casuale natura del traffico di rete, determina un esatto tempo di arrivo e specifica gli effetti del traffico non prevedibile.

Ogni sorgente di traffico **ha un proprio metric che deve essere convertito in bit per secondi**. E' necessario standardizzare la misurazione del traffico per ottenere i requisiti di traffico per utente in bit per secondo. In fine, un fattore deve essere applicato per conto del sovraccarico del protocollo, **fragmentazione del pacchetto, crescita traffico, e margine di sicurezza**. L'analisi può essere effettuata variando questi fattori. Per esempio, Microsoft Office deve essere eseguito da un server e quindi il volume del traffico generato dagli utenti che condividono l'applicazione sulla rete, può essere analizzato. Questo volume aiuterà a determinare la banda ed i requisiti server per installare Microsoft Office sulla rete.

Test Sensitivo Wan: Il testing di sensitività riguarda **la rottura di links stabili** nell'osservazione di che cosa accade. Quando effettua un test sulla rete, non riscontreremo difficoltà particolari.E' una operazione relativamente semplice. La rete **deve essere disturbata rimuovendo via via le interfacce attive** e **monitorando** come questo cambio ha influito sulla rete. E' possibile inoltre vedere **come il traffico è routato**, la **velocità di convergenza**, e se una o più connettività sono perse, e se si sono sollevati problemi nel testare specifici tipi di traffico. Il livello del traffico sulla

rete, può anche essre cambiato per determinare gli effetti sulla rete in una condizione in cui, lo stesso traffico, sta creando una saturazione del media.

L'utilizzo del modello osi nel Design della Wan: Dopo aver compreso le necessità della rete, è tempo di identificare e **designare l'ambiente di computing**, per andare in contro a queste necessità. Le seguenti sezioni ci aiuteranno con questi task.
Il **modello hierarchico** del design di rete permette di designare una rete **stratificandola in livelli**. Per capire l'importanza del Layering, considerare il modello osi, un modello livellato che ci aiuta, da sempre, a capire la computing comunication.
Utilizzando livello, il modello OSI semplifica i task necessari a 2 computer per comunicare. Anche i **modelli Hierarchici per il design di rete**, usano i livelli per **semplificare** i task necessari per la internetworking. **Ogni livello** può essere focalizzato su **specifiche funzioni**, quindi permettendo ai designer di rete, di scegliere i giusti sistemi e le funzionalità per ogni livello.
Utilizzando **un design Hierarchico**, il design **facilita cambiamenti**. La modularità, sul design di rete, permette la creazione di elementi di design, che possono essere sostituiti in caso in cui la rete cresca. Inoltre, poiché la rete richiederà upgrades, il costo e la complessità dell'esecuzione dell'upgrade sono obbligatorie per almeno una parte dell'intera rete. In grandi reti con architettura di tipo Flat o Meshed, i cambiamenti tendono ad affliggere un ampio numero di sistemi. **L'identificazione sui punti di fallimento** della rete, può essere **facilitata**, strutturando la rete in piccoli elementi facili da comprendere. I Managers i rete, possono facilmente comprendere **il punto di transizione nella rete, che aiuta ad identificare i punti di fallimento**.

Il modello HIERARCHICO del design Wan: I Design di rete tendono a seguire **una delle 2 strategie generali** di design. Esse sono la **Mesh e la Hierarchica**. Nella strtuttura **Mesh**, la tipologia di rete è di tipo **Flat**. **Tutti i routers eseguono essenzialmente le stesse funzioni**, e solitamente ci sono delle definizioni non chiare sul luovo ove specifiche funzioni sono state eseguite.L'espansione della rete tende a procedere in **una casuale ed arbitraria maniera**. In una **struttura hierarchica**, la rete è **organizzata in livelli**, ognuno dei quali ha **una o più specifiche funzioni**.
Il **beneficio nell'utilizzo del modello hierarchico**, è motivato dai seguenti fattori:

- Scalabilità – Le reti che seguono un modello hierarchico, possono **crescere e diventre più vaste** senza sacrificare controllo o maneggevolezza. Il **controllo e la maneggevolezz**a sono mantenuti, poiché la funzionalità è localizzata e potenziali **problemi** possono essere **riconosciuti molto facilmente**. Un esempio di una rete hierarchica di enorme scala è il Public Switched Telephone Network.
- Facilità di Implementazione – Un design hierarchico assegna **una chiara funzionalità di ogni livello** quindi è possibile effettuare **implementazioni** sulla rete molto facilmente.
- Facilità di troubleshooting – Poichè le funzioni di livelli individuali sono ben definite, **l'isolazione dei problemi è meno complicata**. Temporaneamente **segmentando** la rete, dunque l'eliminazione dei problemi può essere più semplice.
- Prevedibilità – Il funzionamento della rete, utilizzando livello funzionali, **è abbastanza prevedibile**, il che genera capacità di progettare crescite

considerevoli della rete abbastanza semplicemente. Questo design permette inoltre modellaggio delle performance di rete per propositi analitici.

- Supporto Protocollo – Il mixing delle correnti e delle future applicazioni e protocolli è molto facile, sulla rete che segue design principalmente hierarchici, poichè **l'evidenza logica dell'infrastruttura è organizzata**.
- Gestionabilità – Tutti i benefici descritti contribuiscono ad **aumentare la gestionabilità** della rete.

Livelli Hierarchici del design Wan: Un design Hierarchico di rete include i 3 seguenti livelli:

- **Il livello Core**, che fornisce trasporto ottimale **fra sites**
- **Il livello Distribuzione**, che fornisce **connettività in base alle policy**
- **Il livello Accesso**, che fornisce **accesso utenti e gruppi** alla rete.

Descrizione dei tre livelli del modello di design wan: Si identifica il punto sulla rete dove esiste un limite per quanto riguarda il livello 3 del modello osi (network). Le **periferiche di livello 3 , separano la rete** in domini di broadcast che comprendono 3 livelli. I modello a tre livello consiste nel **Core, Distribution, E livello di Accesso**. Ognuno di essi ha specifiche funzioni:

- Livello Core: -- Il livello core, fornisce **connessioni veloci Wan fra siti remoti** e geograficamente separati, è possibile inserire **un nuemro di una compus network** insie**me ad una corporate o enterprise WAN. I** links Core sono solitamente point-to-point e raramente ci sono degli host. I servizi Core (per esempio, T1/T3, Frame Relay, SMDS), tipicamente sono forniti **da un service provider**, come Telecom.
- Livello Distribuzione: -- Il livello distribuzione fornisce **servizi di rete per LAN** multiple **all'interno di ambienti WAN**. Questo livello esiste in posozione relativa al backbone, e tipicamente è basato sulla Fast Ethernet. Questo livello è implementato su siti di grandi dimensioni, ed è usato per **interconnettere edifici**.
- Livello Accesso: -- Il livello accesso, è solitamente una **LAN o un gruppo di LANs**, tipicamente ethernet o Token Ring. Il livello Accesso fornisce ad **utenti accesso ai servizi**. Il livello Accesso è in posizione degli host e dei collegamenti fisici al network.

Il modello a tre livelli può incontrare le **necessità di molte reti enterprise**. Tuttavia non tutti gli ambienti richiedono il modello hierarchico a 3 livelli. In molti casi, il design a due livelli o spesso ad un solo livello (FLAT) può essere adeguato. In questi casi, **spesso, una struttura hierarchica,** dev'essere pianificata o mantenuta in modo tale da permettere una **futura espandibilità** di disegn su tre livelli secondo ovviamente le future necessità. Le sottostanti sezioni, discutono più nei dettagli, questi 3 livelli. Quindi saranno discussi i modelli a 1 livello o 2 livelli hierarchici.

La funzione del livello CORE: La funzione del Core è **fornire un percorso rapido ed affidabile fra site remoti**. Questo livello della rete **non esegue** alcuna operazione di **manipolazione pacchetti** o filtraggio. Il livello CORE è solitamente **implementato come una WAN**. La WAN necessita di

percorsi ridondanti affinchè la rete possa sostenere uscite relative a circuiti individualiu e continuare la propria funzione. Il Load Sharing e la rapida convergenza dei protocolli di routing è anch'essa molto importante. **L'uso efficiente della banda nel core è sempre una questione rilevante**.

La funzione del livello DISTRIBUTION: Il livello distribuzione della rete è **il punto di demarcazione fra l'accesso ed il Core**, che aiuta a **definire e differenziare il Core**. L'obiettivo di questo livello è **fornire definizione limitativa**. E' il livello al quale avviene la **manipolazione dei pacchetti**. Nell'ambiente WAN, il livello distribuzione può includere diverse funzioni, fra cui:

- Indirizzo dell'aggregazione Area.
- Dipartimento d'accesso del workgroup al livello Core.
- Definizione del dominio Broadcast\Multicast.
- Routing VLAN.
- Ogni transizione che hanno la necessità di avvenire sul media.
- Sicurezza.

Il livello Distribuzione dovrebbe **includere il Backbone Campus** con tutti i **router** connessi. Poiché **la policy è tipicamente implementata** a questo livello, possiamo dire che il livello di distribuzione fornisce la connettività **basandosi su policy**. La connettività policy-based indica che i routers sono programmati per accettare solo il traffico dal backbone capus. Notare che è buona pratica, per un design di rete, non mettere le stazioni finali sul backbone. Non inserire stazioni finali sui tratti liberi di backbone, poichè esso deve funzionare solo ed esclusivamente come un percorso di transito fra worgroups e capus-wide servers. In un ambiente non-campus, il livello distribuzione può essere il punto in cui sites **remoti hanno accesso alla corporate network**.

La funzione del livello ACCESS: Il livello accesso è il punto in cui u**n utente locale accede alla rete**. Questo livello può anche **contenere una ACCESS control list**, o filtri per futura ottimizzazione, quando necessario, ed espansione per un particolare se ti di utenti. Nell'ambiente campus, le funzioni di livello d'accesso possono includere:

- Banda condivisa
- Banda Switched
- Filtraggio a livello MAC
- Microsegmentazione

Il livello Accesso **connette utenti a lan** ed a loro volta la lan a BACKBone per links Wan. Questo approccio permette agli ingegneri di **distribuire servizi di periferiche operative**, a questo livello. Il livello accesso permette **segmentazione logica della rete** e raggruppamento di utenti **basandosi sulla loro funzione**. Tradizionalmente, questa segmentazione è basata su organizzazioni, tipo marketing, amministrazione o ingeneering. Tuttavia, dal punto di vista del management o del controllo, la funzione principale del livello access è **isolare il traffico broadcast** in un gruppo individuale o in LANs. In ambienti NON-Campus, il livello accesso può dare accesso a siti remoti, o a corporate networks tramite la tecnologia WAN: Possiamo parlare di Frame Relay, ISDN, o linee dedicate. Queste tecnologie verranno spiegate nei capitoli che verranno.

Design di rete ad un unico Livello: **Non tutte le reti** hanno bisogno di una **hierarchia a tre livelli**. Un decisione chiave nel design di una rete è il **posizionamento dei servers**. Essi possono essre **distribuiti su lan multiple** o concentrati in una locazione server centrale.Il design **ad un livello** è tipicamente implementato solo **se ci sono molte locazioni remote** nell'azienda e l'accesso alle applicazioni è mantenuto unicamente dal collegamento Della LAN al server. Ogni site appartiene al proprio Broadcast Domain.

Design di rete a due livelli: In un design di wan a 2 livelli, il wan link è usato per **interconnettere siti separati**. All'interno del sito si possono implementare **LAN multiple**, con ogni segmento della LAN che è il dominio broadcast di se stessa. Il **router** diventa un **punto di concentrazione dei links** WAN.

Il vantaggio del design di WAN hierarchico: Un design Wan **hierarchico**, effettua il **routing di livello 3 per tutta la rete**. I punto di routing forniscono un **metodo per controllare il traffico** dei dati. I routers hanno la possibilità di **determinare il percorso** dalla sorgente alla destinazione basandosi sull'**indirizzamento di livello 3**, perciò il traffico affluisce solo se esiste la necessità di raggiungere un host di destinazione. Esempio: Se l'host A deve stabilire la connessione con l'host B, il traffico deve attraversare solo 1 Router, e sarà subito portato a destinazione. E' necessario che non vi siano interposizioni fra l'host 1 e l'host 2 affinchè venga mantenuta la FULL BAND del link.
In una gerarchia WAN a due livelli, il traffico viaggia sulla gerarchia quanto lontano necessita di andare a destinazione, in questo modo conserva larghezza di banda con gli altri collegamenti della WAN. Notare che la **classificazione dei livelli è determinata dal numero di routers** nel percorso fra l'host e l'accesso WAN.

Posizione dei server sulla Wan: Il **posizionamento dei server** in relazione all'accesso degli host influenza il modello di scorrimento del traffico. Esempio: Se si posiziona un server enterprise nel livello accesso del Site1, tutto il traffico destinato a tale server dal site è forzato al passaggio dal router 1 e 2. Ciò comporta un consumo di banda inutile.
Se l'enterprise server è posizionato ad un livello più alto della gerarchia, il traffico del link fra il router 1 ed il router 2, è ridotto ed è subito disponibile per il Site1. **Un server workgroup** è posozionato al livello accesso del sito con la più **vasta concentrazione di utenti**; il traffico passa attraverso **al link wan accedendo limitatamente**. a questo server.

Alternative da dedicare ai links Wan: **Non è comune** per i siti remoti accedere **alla WAN** usando tecnologie WAN **che non siano links dedicati**. **Frame Relay e ISDN sono 2 alternative**. Se un sito remoto è piccolo e ha poche richieste di accesso ai servizi di rete, l'ISDN è una scelta logica per questa implementazione. Forse un altro sito è **troppo distante** perchè **una linea dedicata** sia affidabile. **Il Frame Relay sarebbe una scelta appropriata** perchè **la distanza non ha importanza** a livello di prezzo

Point To Point Protocol

Che cosa ci serve per il ppp: Nel lontano 1980, i protocolli **su linea seriale (SLIP)** furono limitati dalla crescita di internet. Fu creato **PPP per risolvere i problemi di connettività** remota internet. In aggiunta, PPP ha avuto necessità di assegnare indirizzo ip dinamici e di essere utilizzato per molteplici protocolli. PPP fornisce **connettività router-to-router** e host-to-network su circuiti di tipo **synchronous e asynchronous**.

PPP è il protocollo più largamente usato ed il più popolare sulle WAN, poiché esso offre i seguenti vantaggi:
Controlla il setup data link, Fornisce assegnazione dinamica di indirizzi ip, Network protocol Multiplexing, Configurazione Link e Test di qualità link, rilevazione d'errore, Opzioni di negoziazione per abilità come l'indirizzo network-layer negoziation e la compression negoziation.

Componenti PPP: PPP si indirizza sui **problemi della connettività** internet occupandosi dei seguenti componenti:

- Un metodo per **encapsulare i datagrammi** su linee seriale. PPP utilizza HDLC come base per encapsulare i datagrammi su link point-to-point.
- Un controllo Link **(LCP)** per stabilire, **configurare e testare** la connessione data-link.
- Una famiglia di protocolli per il **controllo di rete (NCPs)** per stabilire e configurare diversi protocolli che appartengono a distinti livelli di rete. PPP è designato per **permettere l'uso simultaneo di multipli protocolli di rete**. Oggi, PPP supporta altri protocolli basati su IP, fra cui IPX e AppleTalk. PPP **usa il proprio componente NCP per encapsulare** multipli protocolli.

Funzionalità livelli PPP: PPP usa l'architettura **a livelli**. Con le sue funzioni di livello inferiore, PPP può usare:

- **Synchronous** physical media, Come ad esempio accade su reti ISDN.
- **Asychronous** physical media, Come quelli che usano i servizi di telefonia base per connessioni modem DIAL-UP.

Con le sue funzioni di livello Superiore, **PPP supporta o encapsula diversi protocolli** di livello network **con NCPs**. Questi protocolli di alto livello sono:

- ***BCP*** -- Bridge Control Protocol
- ***IPCP*** -- Internet Protocol Control Protocol
- ***IPXCP*** -- Internetwork Packet Exchange Control Protocol

Questi protocolli hanno **campi funzionali** contenenti codici standardizzati che indicano il **tipo di protocollo, livello network che PPP encapsula**.

I sei campi del frame PPP: I Campi del PPP Frame sono i seguenti:

- ***Flag*** – Indica l'inizio o la fine del frame e consiste in una sequenza binaria di 01111110
- ***Address*** – Consiste nell'indirizzo di broadcast standard che è la sequenza binaria 11111111. PPP non assegna indirizzi a stazioni individuali.
- ***Control*** – Un byte che consiste nella sequenza binaria 00000011 che chiama per la trasmissione di dati nell'unsequenced frame. E' fornito un servizio connession-less simile a Logical Link Control (LLC) del tipo 1.
- ***Protocol*** – Due Byte che identificano i protocolli encapsulati nel campo data del frame. ***Data*** – Zero o più byte che contengono il datagramma per il protocollo specificato nel campo protocollo. La fine del campo data è trovata localizzando la flag sequence più vicina e permettendono il FCS (frame check sequence) a 2 bit del frame. La lunghezza massima del frame, per default è di 1500 bytes.
- ***FCS*** – Normalmente di 16 bits (due bytes). Si riferisce a caratteri extra aggiunti al frame per il processo di controllo errori.

Le 4 fasi per cui PPP estabilisce una connessione punto punto: PPP fornisce un metodo per **stabilire, configurare, mantenere e terminare** una connessione point-to-point. Per stabilire comunicazioni sul link point-to-point, PPP attraversa 4 fasi:

- Stabilimento Link e negoziazione Configurazione: Un nodo PPP originario, **invia un frame LCP per configurare** e stabilire un Data Link.
- Determinazione della qualità del Link: Il link è testato al fine di determinare se **la sua qualità** è sufficiente per trasportare i protocolli di rete. Questa è una fase Opzionale.
- Configurazione e negoziazione del protocollo di livello network: Il nodo PPP di origine, invia **frames NCP** per scegliere e **configurare protocolli relativo al livello network**.I protocolli scelti di livello network, come ad esempio IP, novell IPX e AppleTalk, sono **configurati e impacchettati**, dal momento in cui ogni protocollo è inviato.
- Terminazione Link: Il link resta configurato per comunicazioni **affinchè i frames LCP e NCP, non chiudono il link** o finchè non avvengono eventi esterni (per esempio, il timer di inactivity espira a causa di interventi da parte di utenti o admins)

Ci sono TRE FASI per gli LCP frames:

- Frames per lo stabilimento del Link: Usati per **stabilire e configurare** un Link
- Frames di terminazione Link: Usati per **terminare** un Link.
- Frames di mantenimento Link: Usati per **configurare e gestire il bebug** di un Link.

I Frames LCP sono usati per completare il lavoro di ognuna delle 4 fasi LCP Elencate Sopra.

Fase 1: Stabilimento del Link: Nella fase di stabilimento link e configurazione della negoziazione, **ogni periferica PPP invia pacchetti LCP** per **configurare e stabilire** il Data Link. I pacchetti LCP contengono un campo relativo ad una **opzione di configurazione** che permette alle periferiche di negoziare ed usare le opzioni. Esempi di queste opzioni includono l'unità massima di **trasmissione (MTU)**, la **compressione di certi campi PPP** ed il protocollo di **autenticazione Link**. Se l'opzione di configurazione non è inclusa in un **pacchetto LCP**, per questo campo opzione si utilizza un valore di DEFAULT. Prima che un datagramma di livello network sia scambiato, LCP deve **prima aprire la connessione e negoziare i parametri** di configurazione. Questa fase è completata quando **un aknownledgement** frame di configurazione è inviato e ricevuto.

Fase 2: Determinazione della qualità del Link: LCP permette una fase opzionale di **determinazione della qualità-link**, a cui seguono le fasi di **stabilimento e di configurazione** della negoziazione. Nella fase di determinazione della **qualità del link, il link è testato** per poter verificare se la qualità del link è abbastanza buona da permette il trasporto di protocolli livello network.
Inoltre, dopo che il link è stabilito, e **il protocollo di autenticazione** è stato scelto, può avvenire l'autenticazione dell'utente. L'autenticazione, se usata, avviene **prima che la fase di configurazione user o client, abbia inizio**. LCP può **ritardare trasmissioni di livello network** finchè questa fase non è completata. PPP Supporta due protocolli di autenticazione: **PAP e CHAP**. Entrambi questi protocolli sono dettagliati in RFC 1334, "PPP Authetincation Protocols". Questi protocolli sono spiegati più tardi in questo capitolo, nella sezione "PPP Authentication".

Fase 3: Configurazione della negoziazione di protocollo livello 3: Quando **LCP completa la fase di determinazione qualità del Link**, il **protocollo di livello network** può separatamente essere **configurato con l'appropriato NCP** e può essere Tirato su, o in stoppato in ogni momento.
In questa fase, le periferiche **PPP inviano pcchetti NCP** per scegliere e configurare uno o più protocolli di livello network, come ad esempio IP. **Quando ognuno** di questi protocolli livello network, scelti, **è stato configurato**, i datagrammi, provenienti da ogni protocollo, possono essere **inviati tramite il Link**. Se **LCP chiude il link**, esso informa i protocolli di livello3 di quanto è avvenuto. Quando **PPP è configurato, è possibile controllare il suo stato LCP e NCP**, usando il comando Show Interfaces.

Fase4: Terminazione del Link: **LCP può determinare il link** in ogni momento. Questo è soitamente effettuato, a seguito di **una richiesta utente**. Tuttavia, ciò può anche accadere a seguito di un **evento Fisico**, come ad esempio perdita del Carrier o TimeOut.

Autenticazione PAP: La fase di **autenticazione** della sessione **PPP è opzionale**. Dopo che il **link è stato stabilito** e che il **protocollo di autenticazione è stato scelto**, è possibile a tutti gli effetti **eseguire l'autenticazione**. Se usata, **l'autenticazione** deve avvenire **prima** che la fase di **configurazione** del protocollo di **livello 3** sia iniziata.
Le opzioni di autenticazione richiedono che **la parte chiamante del link inserisca informazioni di autenticazione.** Questo aiuterà ad essicurarsi che l'utente abbia il permesso dell'amministratore di rete per effettuare la chiamata. I **Peer Routers**, scambiano **messaggi di autenticazione**. Quando si configurara l'autenticazione PPP, è possibile **selezionare PAP o CHAP**. In generale **si preferisce CHAP**.
CHAPnisce un semplice metodo poiché un nodo remoto possa stabilire la propria indentità **utilizzando il Two-Way-Handshake**. Prima si completa la fase di **stabilimento Link**. Quindi una **username e password è inviata dal nodo remoto** tramite il link, finchè la connessione e **l'aknowledgment di autenticazione** non sono terminati.
PAP, **non è un protocollo** di autenticazione molto **forte**. Le password sono inviate tramite il link, **in chiaro testo**. Non esiste protezione dal playback o da ripetuti attacchi trial-and-error (prova e sbaglia e riprova). **Il nodo remoto** è colui che **controlla il frequency**, **Timing ed i tentativi**, della fase di login.

Autenticazione Chap: Chap è usata periodicamente per **verificare l'identità** del nodo **remoto**, utilizzando la **tree-way handshake**. Ciò è effettuato **subito dopo lo stabilimento** del link iniziale,può essere **ripetuto ogni volta** sempre dopo lo stabilimento del link. **CHAP** offre **varie possibilità**, come ad esempio **verifica periodica** per aumentare la sicurezza. Questo rende CHAP **piùefficiente di PAP**. **PAP effettua la verifica solo una volta**, ciò la rende vulnerabile ad hack e modem playback. Oltre a ciò, PAP permette al caller di iniziare il processo di autenticazione, **senza prima ricevere un invito**. Questo rende **PAP vulnerabile** ad attacchi di tipo BRUTE-FORCE; Al contrario **CHAP non permette ciò,** non da la possibilità ad un chiamante di tentare l'autenticazione **senza prima aver ricevuto un invito**. (challenge).
Dopo che la fase di **stabilimento link PPP è completato**, l'host invia **un messaggio d'invito al nodo remoto**. Il nodo remoto **risponde con un valore**. L'host fa un **controllo** ed un **paragono della risposta con i propri valori**. Se i valori coincidono **l'autenticazione è confermata**. Altrimenti la connessione è **terminata**.
CHAP fornisce **protezione contro i playback attach**, tramite l'uso di un valore di invito variabile che è unico e imprevedibile. L'uso di ripetuti inviti è atto a limite il tempo di esposizione ad ogni singolo attacco. Il router Locale (o server di autenticazione third-party, come netscape commerce server) controlla la **frequenza ed il tempo di risposta**.

Comando IOS per autenticazione PPP: Per configurare **l'autenticazione PPP** bisogna inserire i seguenti comandi:

Router (Config-IF) encapsulation ppp
Router (config-IF) ppp authentication (Chap, pap, ecc.ecc)
Router (Config-IF) ppp pap sent-username (nome) password (passw)

Comando IOS per autenticazione CHAP: I seguenti metodi possono essere usati al fine di semplicare i **tasks di cnfigurazione CHAP** sul router:

- Lo stesso host name può essere usato per routers multipli, se si vuole fare in modo che utenti remoti si connettano sullo stesso router durante la fase di autenticazione. Per far ciò, configurare lo stesso host name su ogni router.

```
Router(config-if)# ppp chap hostname
```

- Una password può essere usata per autenticare host sconosciuti. Questa procedura, limite il numero di entries relative ad user e password nel router. Per usare questo, configurare una password che verrà inviata all'host che vuole **l'autenticazione al router**.

  ```
  Router(config-if)#ppp chap password
  ```

  Questa password non è usata quando il router autentica una periferica remota.

ISDN

Che cosa è ISDN: ISDN permette a **segnali digitali** di essere trasmessi **sulle linee telefoniche** esistenti. Questo diventa possibile quando lo **switch** della compagnia telefonica è upgradato e può fare un handle dei segnali digitali. **ISDN** è generalmente vista come **un'alternativa** alle linee dedicate. Le linee dedicate possono essere usate per lavoro a distanza e piccoli e remoti uffici all'interno di LANs.
Le compagnie telefoniche hanno realizzato ISDN, come tentativo per standardizzare i subscriber services. Questo include le User Network Interfaces (UNI), che è la modalità con cui viene visualizzato lo schermo quando l'utente effettua la chiamata. I servizi di standardizzazione subscriber, assicurano compatibilità internazionale. Gli standard ISDN definiscono l'hardware e chiamano schemi di setup per connettività digitale End-To-End.
Gli schemi hardware **e call setup**, aiutano a realizzare gli obiettivi della connettività WorldWide, garantendo che le reti **ISDN forniscano facili comunicazioni** con altre. Di Base, la funzione di **digitizzazione è realizzata sul site utente**. Rarametne ciò avviene all'interno della compagnia telefonica.
L'abilità di ISDN di trasportare connettività digitale a siti locali, comporta molti vantaggi e benefici:

- ISDN può trasportare una varietà di segnali, e traffico utente. ISDN fornisce sccesso a digital video, circuit switched data, e servizi di rete basati sulla telefonia, utilizzando la normale rete telefonica di tipo circuit-switched.
- **ISDN offre il call setup più velocemente** di una connessione modem poiché essa usa una **banda Extra dedicata** (Channel D, delta). Per esempio. Diverse chiamate ISDN possono essere settate in meno di un secondo.
- ISDN fornisce un più veloce rate di trasferimento dati rispetto ai modems, usando i canali B, oguno dei quali ha **64kbit di banda** (b channels, Bearer). Con canali multipli ISDN, è

possibile offrire più banda di quanto, sulla wan, alcune linee dedicate possano offire. Per esempio se si decide di usare due canali B, la banda sarà di 128kps poiché ogni canale B ha 64kbps di banda.

- ISDN può fornire un **chiaro percorso** dati sul quale avviene **la negoziazione dei PPP links**.

Nella fase di design è necessario assicurarsi che le apparecchiature scelte abbiano la capacità di portare vantaggio alla flessibilità di ISDN. In aggiunta bisogna sempre considerare la seguente distribuzione ISDN per il design:

- Distribuzione della Sicurezza: Poichè periferiche di rete possono adesso essere connesse a reti telefoniche pubbliche (PSTN), è cruciale, in fase di design, realizzare un robusto **modello di sicurezza** per proteggere la rete.
- Distribuzione del Costo: Un obiettivo primario per selezionare ISDN per la rete è **evitare il costo del traffico full time** relativo alla connessione (come accade per linee dedicate o frame relay). Perciò è quindi molto importante **valutare** il profilo relativo al **traffico che si terrà su ISDN** per assicurarsi che il costo WAN sarà controllato.

Componenti Base ISDN: I Componenti ISDN includono **terminali**, **terminal adapters** (Tas), **terminazioni di rete** (NT) **line-termination equipment**, ed **exchange-termination equipment**. I terminali ISDN si distinguono in 2 Tipi. Type1 e Type2. Terminali ISDN specializzati sono definiti Terminal Equipment Type1 (**TE1**). Terminali **NON-ISDN come ad esempio il DTE**, che sono antecedenti rispetto agli standards ISDN, sono chiamati Terminal Equipment Type2 (**TE2**). I TE1, connettono le reti ISDN tramite 4 Cavetti, Twisted pair Digital Link. Il TE2 **connette ISDN tramite un TA**. L'ISDN TA può sia una periferica Standalone, o una periferica che include internamente la T2. Se il TE2 è implementata come una periferica standalone, essa connette il TA tramite un'interfaccia standard di livello1 (phisical).
Oltre le periferiche TE1 e TE2, il prossimo **punto di connessione nelle reti ISDN** è il Network Termination Type1 (**NT1**), il Network Termination Type2 (**NT2**). Ci sono periferiche di terminazione di rete, che connettono il Subscriber tramite four-wire, fino ad arrivare al local loop convenzionale (two-wire). In Nord America, NT1 è solitamnete parte del Customer Permises Equipment (CPE). In molte parti del mondo ad eccezione del Nord America, **l'NT1 è una parte della rete fornita dal CARRIER**. L'**NT2** è invece una periferica **molto complicata**, tipicamente **si trova in Digital Private Branch eXchanges** (PBXs) che eseguono servizi di livello 2 e 3. **Esiste anche una periferica NT\2**. Essa è una periferica singola che **combina le funzioni di NT1 e NT2**.

Punti di referenza ISDN: I Customer Permise Equipment (CPE) coprono **un'ampia varietà di servizi e interfacce**. Perciò gli standard si riferiscono alle **interconnessioni tramite punto di referenza**, piuttosto che a necessità hardware. I punti di referenza sono una serie di specifications che definiscono la connessione fra periferiche specifiche, in base alla loro funzione sulla connessione end-to-end. E' importante avere una conoscenza su questi tipi di interfacce, poiché una periferica CPE, come un router, ad esempio, può supportare **differenti tipi di referenza**. Il **punto di referenza supportato, determinerà il tipo di hardware** che ci serve o che dobbiamo acquistare. Un esempio di configurazione ISDN, dove tre periferiche **sono collegte allo switch ISDN al Central Office (CO)**. Due due queste periferiche sono compatibili con ISDN, e quindi possono essere collegate trmite un Punto di referenza S alle periferiche NT2. La terza periferica (Uno standard non-isdn)è collegata tramite il punto di referenza R, al TA.

Switch ISDN e SPIDs: Affinchè ISDN possa operare correttamente, è importante che il **corretto tipo di switch sia configurato sulla periferica ISDN**. Il tipo più comune negli stati uniti è AT&Ts 5ESS e Nortel's DMS-100. Il tipo più comune in giappone è NTT, in UK sono NET3 e NET5. I

service providers ISDN usano una **varietà di Switch** per i propri servizi ISDN. I servizi offerti dai Carrier variano da nazione in nazione, da regione in regione. Come i modems, **ogni tipo di switch opera differentemente, ed ha uno specifico set di requisiti per il Call Setup**.
Come risultato, **prima di connettere un router** ad un servizio ISDN, **bisogna conoscere il tipo di switch usato ed il CO**. Questa informazione è specificata **durante la configurzione del router**, quindi il router può **inizializzare una Chiamata** livello network ISDN ed inviare i dati.
Per sapere maggiori informazioni sul tipo di switch che il provider utilizza, è necessario conoscere quale **profilo di servizio (SPIDs) è assegnato alla connessioni**. L'ISDN Carrier, **fornisce uno SPID** per **identificare la configurazione della linea per un servizio ISDN**. Le **SPIDs sono una serie di caratteri (possono essere visualizzati come numeri di telefono) che identificano l'utente sullo switch e CO**. Dopo che l'utente si è identificato, li switch linka il servizio che si è richiesto alla connessione.

Differenze fra protocolli ISDN E,I e Q: I lavori suglio **standards per ISDN iniziarono nel lontano 1960.** Un comprensivo set di raccomandazioni ISDN è stato pubblicizzato nel 1984. Ci sono continui UPDATES effettuati dalle consultive committee for international telegraph and telephone (CCITT), Internetional Telecommunication Union Telecommunication Standardization Sector (ITU-T). I Gruppi ITU-T verranno descritti in seguito.
Q.921 raccomanda il **processo Data Link sul canale D ISDN**. Il **Q.931** governa la **funzionalità di livello network fra il terminal endpoint e lo switch ISDN locale**. Questo protocollo non impone una raccomandazione End-To-End. I vari ISDN providers e i tipi di switch, possono usare vari tipi di implementazione per quanto riguarda Q.931. Altri switch sono stati realizzati prima che questi gruppi standard finalizzassero questo standard.
Poiché **i tipi di switch, non sono standard**, quando si **configura il router**, è necessario **specificare l'isdn al quale siamo connessi**. In aggiunta, i routers cisco, **hanno un comando DEBUG**, per monitorare **i processi Q.931 e Q.921** quando una chiamata ISDN è iniziata o terminata.

E: Questo protocolli si affidano alle **reti telefoniche standar** per ISDN. Per esempio il protocollo **E.164 descrive l'indirizzamento internazionale per ISDN**.
I: Questi protocolli si occupano di **concetti, terminologie e metodi generali**. La serie **T100** include **concetti generici su ISDN** e strutture di altre serie I-. La serie **T200** parla degli **aspetti legati al servizio ISDN**. La serie **T300** descrive gli **aspetti del network**. La serie **T400** descrive **come è fornita UNI**.
Q: Questi protocolli spiegano **come devono operare lo switching ed il signaling**. Il termine **signaling**, in questo contesto, **è il processo di call setup**, utilizzato. Il **Q 921 descrive il processo data-link ISDN della Link Access Procedure, sul canale D** (LAPD), con funzioni come quelle del livello2, sul modello OSI. Il Q.931 specifica funzioni relative al Livello 3 del modello OSI.

Gli standards ITU-T per i primi 3 livelli ISDN: ISDN utilizza una suite di **standard ITU-T**, attraverso il livello **Fisico, Data Link e Network** del modello OSI:

- Il Livello Fisico: L'ISDN **BRI**, specifica di livello fisico, è definita **ITU-T 1.430**. L'ISDN **PRI**, specifica di livello fisico, è definita **ITU-T 1.431**
- Il livello Data Link: La specifica ISDN di livello **Data Link è basata sul LAPD** ed è formalmente specificata **in ITU-T Q.920, ITU-T Q.921, ITU-T Q.922, e ITU-T Q.923**
- Il Livello Network: Il Livello Network ISDN è **definito in ITU-T Q.930**, conosciuto anche come **1.450**, ed ITU-T Q.931, Conosciuto come 1.451. Questi 2 standard, insieme, **specificano la connessione user-to-user**, **Circuit Switched e Packet Switched**.

Livello Fisico ISDN: Il Livello **fisico ISDN**, **differenzia il formato frame, in relazione all'uscita**. (dal terminale alla network-the TE frame format) **o all'entrata** (dalla network al terminal-the NT froame format). Entrambi i frames hanno una lunghezza **pari a 48Bits**, **di cui 36 rappresentano**

dati. Attualmente un frame è composto da 2 frames di 24 bit che si succedono, consistono in due da 8bit per i canali B e un 2-bit per i canali D e 6bits di informazine frame (2*(2*8b+2d+6f)=32B+4D+12F=48DBF). I Bit del frame ISDN di livello fisico sono usati come segue:

- Framing Bit: Fornisce sincronizzazione
- Load Balancing Bit: Aggiusta il valore medio del bit
- Echo of previous D channel Bits: Usato per conflitto di risoluzione (contention resoluzion) con diversi terminali su un "passive bus" conteso per un canale.
- Activation Bit: Periferiche attivate
- Spare bit: Non assegnato
- B1 channel Bits
- B2 channel bits
- B Channel: Utilizzato per dati

Notare che sono inviati 8000 ISDN Bri frames per secondo. Ci sono 24 Bit in ogni frame (2*8B+2D+6F=24) per un bit rate di 8000*24 = 192 Kbps. L'effettivo rate è 8000*(2*8B+2D)=8000*18 = 144Kps.
Periferiche ISDN multiple possono essere **fisicamente collegate ad un solo circuito**. In questa configurazione, possono **risultare collisioni se due terminali trasmettono simultaneamente**. ISDN fornisce **funzioni che determinano la contesa del Link**. Queste funzioni fanno parte del **canale D ISDN**, che è descritto in maggiori dettagli, più tardi, in questo capitolo.

Livello Data Link ISDN: Il protocollo di signaling **ISDN di livello2 è il Link Acess Procedure**. **Sul canale D (LAPD).** LAPD è simile all'HDLC e Link Access Procedure, Balanced (LAPB). LAPD è **usato sul canale D per garantire che il flusso di informazioni di controllo e di segnaling venga ricevuto correttamente**.
Il LAPD flag ed i campi di controllo sono identici a quelli dell'HDLC. Il campo relativo all'indirizzo **LAPD può essere di lunghezza pari ad uno e due byte**. Se il bit dell'indirizzo esteso del primo byte è settato, l'indirizzo sarà 1 byte. Se non è settato, l'indirizzo sarà 2 Byte. Il primo byte relativo al campo di indirizzo contiene il Service Access Point Identifier (SAPI), che identifica il punto di ingressi in cui LAPD fornisce il servizio di livello 3. Il Bit Command\Response (C\R) indica se il frame contiene un comando o una risposta. Il campo relativo all'identificativo Terminal EndPoint (TEI) identifica sia un terminale singolo che un terminale multiplo. Tutti gli "1" nel TEI field idicano un broadcast.

Livello Network ISDN: Due specifiche di livello 3 sono usate **per il signaling ISDN: ITU-T 1.450** (anche conosciuto come ITU-T Q.930) e **ITU-T 1.451** (anche conosciuto come ITU-T Q.931). Assieme, questi protocolli, **supportano connessioni user-to-user, circuit switched e packet switched**. Vengono specificate numerose varietà di stabilimenti connessione, terminazioni connessione e messaggi misti. Questi includono il **Setup, Connect, Release** ed informazioni relative all'utente. Inoltre **cancel, status, e disconnect**.

Encapsulation per ISDN: Quando vengono realizzate soluzioni di accesso remoto, è possibile scegliere fra **diverse soluzioni per l'encapsulation**. I due tipi di **encapsulation più comuni** sono **PPP e HDLC**. **ISDN per default è settata su HDLC**. Comunque **PPP è molto più robusto** di HDLC, esso fornisce un meccanismo eccellente per **autenticazione e negoziazione e configurazione di un link e protocollo compatibile**. Un'altra **encapsulation per End-To-End ISDN è LAPB** (Link Access Procedure Balanced). Le interfacce **ISDN** permettono **solo una singola encapsulation di livello 2 per la connessione**. Da quando la connessione ISDN è stabilita,

il router può **usare questa connessione per trasportare ogni cosa che è richiesta dal protocollo di livello network**.
La maggior parte dei design di rete **usano l'encapsulation PPP**. PPP è un **meccanismo peer-to-peer potente** e **modulare** usato per **stabilire data link**, fornire **sicurezza** ed **encapsulare** il traffico. Dopo che la connessione PPP è negoziata, fra 2 periferiche, essa può essere **usata dai protocolli di rete, come ad esempio IP ed IPX** al fine di stabilire una connettività di rete.
PPP è un open standard, specificato da RFC 1661. PPP fu realizzato con diverse funzioni che lo rendevano particolarmente utile in applicazioni di accesso remoto. **PPP Utilizza Link Control Protocol (LCP) per inizializzare e stabilire il link e confermare la configurazione**. Esistono funzionalità di sicurezza integrate nel protocollo. **PAP e CHAP**, garantiscono con facilità una struttura robusta, dal punto di vista della sicurezza. **CHAP è il protocollo di autenticazione più popolare per il "call screening".**
PPP consiste in sette componenti:

- PPP Framing: FRC 1662 discute **l'implementazione del PPP in HDLC-like Framing**. Ci sono differenze nel modo in cui **PPP è implementato**, su **asynchronous** e **synchronous** links. Quando uno degli end link usa il **Synchronous PPP** (come ISDN router) e gli altri usa **asynchronous PPP** (come ad ISDN TA connessa ad una porta seriale PC), due tecniche sono disponibili per **fornire la compatibilità nel framing**. Il metodo preferibile è abilitare synchronous-to-asynchronous PPP frame conversion nell'ISDN TA.
- LCP: PPP **LCP** (Link Control Protocol) fornisce un metodo per **stabilire, configurare, mantenere e terminare connessioni point-to-point**.Poichè ogni datagramma di livello 3 (per esempio IP) possa essere scambiato, **LCP, deve prima aprire la connessione e negoziare i parametri di configurazione**. Questa fase è completata quando un frame di aknowledgment è stato inviato e ricevuto.
- Autenticazione PPP: **L'autenticazione PPP** è usata per **fornire sicurezza** primare su ISDN ed altri link di encapsulation PPP. **I protocolli di autenticazione PPP (PAP e CHAP), sono definiti in RFC 1334**. Dopo che **LCP ha stabilito la PPP connection**, è possibile implementare un opzionela protocollo di autenticazione, prima di procedere con la negoziazione e con lo **stabilimento del Network Contro Program** (**NCP**). Se **l'autenticazione** è necessaria, essa deve essere negoziata come **una opzione dello stabilimento dell'LCP**. L'autenticazione può essre **bidirezionale o unidirezionale**. Con l'autenticazione **bidirezionale, ogni lato autentica l'altro (CHAP).** Nell'autenticazione **unidirezionele, un lato, tipicamente il chiamante, si autentica all'altro (PAP).**

L'autenticazione PPP è abilitata con **il comando ppp authentication**. **PAP e CHAP** possono essere usati per **autenticare la connessione remota**. **CHAP** è considerato **un superior authentication protocol** poiché esso **usa il metodo tree-way-handshake** per **evitare l'invio di password in chiaro, sul link PPP**.

Tre Utilizzi per ISDN: ISDN può avere diversi usi nel Networking. Le seguenti sezioni descrivono gli usi dell'ISDN.

- Accesso Remoto
- Nodi Remoti
- Connettività di Piccoli uffici\Casa (SOHO Connectivity)

L'accesso remoto permette la connettività di utenti locati in locazioni remote, tramite **delle connessioni DialUP**. La locazione remota può essere una "telecommuter's home", un utente mobile, una stanza di hotel o un piccolo ufficio. La connessione Dial UP può avvenire **tramite una connessione** analiga **usando il servizio di telefonia base** o via ISDN. La connettività è influenzata dalla **velocità, costo, distanza e disponibilità**.

Il **Link di accesso remoto**, generalmente **rappresenta il link a velocità più bassa nell'enterprise**. Ogni miglioramento in velocità **è comunque benevole**. Il costo dell'accesso remoto tende ad essere relativamente basso, in special modo per i serivizi di telefonia base. I servizi ISDN di tipo FREE possono variare, dipende dall'area geografica, dalla disponibilità del servizio e dal metodo di pubblicizzazione. I servizi di dialup che includono ISDN, possono avere particolari limitazioni per service providers individuali.

Nodi Remoti ISDN: Con il metodo dei nodi remoti, gli utenti si connettono alla LAN sul central site, **tramite il Public Switched Telephone Network (PSTN), per tutta la durata della chiamata**. Nonostante si abbia una connessione a bassa velocità, gli utenti remoti vedono lo stesso ambiente visto dagli utenti locali. La connessione alla LAN **avviene tipicamente tramite un Access Server**. La periferica solitamente **combina le funzioni di un modem e quelle di un Router**.Quando l'utente remoto è loggato, esso può a**ccedere ai server della lan remota, identificandosi come localmente**.
Questo metodo offre **molti vantagi**. E' il più **sicuro e flessibile** ed è anche il più **scalabile**. Solo un pc è indispensabile per l'utente remoto, e molte soluzioni client software sono disponibili. **L'unica aggiunta hardware** necessaria **in locazione remota**, **è un modem**. Lo **svantaggio principale** di questo metodo è **l'addizionale sovraccarico amministrativo** indispensabile per supportare l'utente remoto.Comunque grazie ai suoi numerosi Vantaggi, questa soluzione è usata nel resto degli esami relativi a questo capitolo.
Il **Full-Time telecommutter\teleworker** è **un utente che normalmente lavora fuori da casa**.Questo utente è solitamente un **Power User che necessita di accedere alla rete enterprise per e restare collegato per molto tempo**. Questa connessione deve essere **affidabile e disponibile in ogni momento**. Tale necessità vuole puntare sul metodo di connessione ISDN. Con questa soluzione, la connessione ISDN, può essere usata per un servizio che ogni telefono necessita, e per la connessione di pc workstation.

Connettività SOHO ISDN: Un **piccolo ufficio oppure un ufficio casalingo**, **definito anche SOHO**, consiste in una **connessione rapida per pochi utenti**, più affidabile rispetto alla dialup analogica.
Per esempio, in una configurazione test, tutti gli utenti, nella locazione remota, possono avere uguale accesso al servizio locato presso un corporate office tramite una router ISDN. Questo offre la possibilità a **dei SOHO sites di connettere la rete corporate o internet, ad una velocità molto più alta rispetto al pstn**, sempre percorrendo le normali linee analogiche.
Il design SOHO tipicamente è orientato **SOLO verso il DialUP** (**SOHO-initiated connections**) e può portare vantaggi sulla tecnologia translazione di indirizzi emergenti per cui semplificare il design ed il supporto. Usando queste funzionalità, il **SOHO Site**, **può supportare periferiche multiple, ma appare come un singolo indirizzo IP**.

ISDN Bri e ISDN Pri: Ci sono due servizi ISDN: **Bri e Pri**. Il servizio **ISDN BRI, offre due canali B da 8bit, e un canale D da 2-bit,** il tutto viene spesso riferito al 2B+D. **ISDN BRI fa un delivery della banda totale, di 144Kps** in tre canali separati (8000 frames per secondo*(2*8bit Canale B+2bit Canale D)=8000*18=144Kbps). I servizi **BRI sui canali B, operano a 64Kbps** (8000 frames per secondo*8-bit Canale B), e trasportano **dati e traffico Voce**.
ISDN fornisce grande flessibilità al designer di rete grazie alla sua **abilità di separare ogni canale B per data applications e voce**. Per esempio un lungo documento può essere downloadato da una corporate network attraverso un canale B a 65kbps, mentre l'altro canale B è usato per connettere una web page.
Il terzo canale, il D, è di 16kbps (8000 frames per secondo * 2bit Canale D) usato per **trasportare istruzioni che dicono alla rte telefonica come gestire ognuno dei canali B** (handling). Il canale D BRI service, opera a 16Kbps ed ha il compito di **trasportare e controllare informazioni di**

signaling, oltretutto esso può supportare trasmissione dati utente in certe circostanze. Il protocollo di signaling sul D channel, **avviene al livello 1**, attraverso 3 degli OSI reference model.
I terminali **non possono trasmettere nel canale D** a meno che loro prima non rilevino uno **specifico numero di "ones"** (**indicando no signal**) corrispondenti ad una **priorità** prestabilita. Se il **TE rileva un bit in echo** (E) channel che è **differente dai suoi D bits**, esso deve spettare di **trasmettere immediatamente**. Questa semplice tecnica **fa in modo che solo un terminale alla volta, può trasmettere il proprio D message**. Questa tecnica è **simile** ed ha lo stesso effetto del **"collision detecting"** nelle **ethernet LAN**. **Dopo aver trasmesso** il messaggio con successo, il terminale **riduce la propria priorità** richiedendo di poter rilevare altri "ones" per poter continuare a trasmettere. I **terminali non possono aumentare la loro priorità fino a che tutte le altre periferiche sulla stessa linea non hanno l'opportunità di inviare un D message**. Le connessioni telefoniche hanno una proprità più alta rispetto a tutti gli altri servizi, e le informazioni di singaling, hanno una priorità più alta rispetto alle informazioni di NON-signaling.
Il servizio **ISDN PRI offre 23 canali B ad 8 bit ed un canale D ad 8 bit**, più un bit framing in Nord America e Giappone, si ha in questo caso un bit rate totale di 1.544Megabit (8000 frames per secondo*(23*8bit canale B+8b canale D+1 bit framing) =8000*824.125 = 1.544Mbps) (Il canale D del PRI ISDN funziona a 64kps) la ISDN PRI, in Europa, Australia ed altre parti del mondo, fornisce 30 Canali B da 8-bit, più un canale D da 8 Bit, più un canale framing da 8 bit, per un total rate di 2.048Megabit (8000 Frames per secondo *(30*8-bit canali b + 8-bit canale D + 8-bit canale Framing = 8000*8*32=2.048Megabit).
Con la T1/E1 e con framerate superiori, i canali B sono collegati assieme come i vagoni di un treno.Proprio come i treni in una piazza di smistamento i canali B sono riarrangiati e spostati su altri frames che attraversano la linea classica (PSTN) finchè essi non raggiungono la destinazione. Questo percorso "diretto alla matrice dello switch" (credo) crea un collegamento sincrono tra due endpoints. Ciò permette continuità nella comunicazione voce, senza pause, scarti di data o degradazioni. ISDN porta vantaggi su questa struttura di trasmissione digitale, per il trasferimento di dati digitali.

Come viene stabilita la connessione Bri: In base alle **necessità** dell'applicazione e "traffic engineering", i servizi **BRI e PRI sono scelti x la connettività ISDN** da ciascun sito .Il traffic engineering, può richiedere multipli servizi BRI o multipli PRI per i diversi siti. Dopo che ISDN viene connesso alla struttura tramite interfaccia BRI o PRI, è necessario implementare il design dei servizi end-to-end.
Il BRI local loop è terminato, secondo i permessi del customer, all'NT1. L'**interfaccia** del local loop all'NT1 è chiamata punto di **referenza** U (reference point).
il ciclo locale del BRI è terminato alla (premessa, presupposizione) dell'acquirente ad un NT1. L'interfaccia del loop locale all'NT1 è chiamato "Punto di referenza U". Nel lato della premessa dell'acquirente dell'NT1 è il punto di referenza S/T.
Due tipi comuni di ISDN customer permise equipment (CPE) **sono disponibili** per servizi BRI: **Lan routers e pc TAs.** Molte periferiche BRI, offrono NT1s integrati ed integrate Tas per telefoni analogici.
I **routers ISDN LAN** forniscono routing fra ISDN bri e la LAN usando il **Dial On Domand Routing (DDR)**. DDR **automaticamente stabilisce e rilascia le chiamate circuit switched**, fornendo trasprente connettività a siti remoti basandosi sul traffico di rete. DDR inoltre **controlla lo stabilimento ed il rilascio dei canali B secondari basandosi sulla soglia di carico**.
E' usato il **Multilink PPP** per fornire **aggregazione di banda** quando si usa **multipli canali B**.
Molte applicazioni ISDN **possono aver bisogno di SOHO** user per prendere il diretto controllo sulla chiamata ISDN.
PC TAs si connettono a pc Workstation, sia tramite il bus che esternalmente tramite le porte di comuniazioni (come ad esempio RS-232) e possono essere usate similarmente ai modem analogici interni ed esterni.

PC TAs possono fornire un singolo pc user con controllo diretto sulla sessione ISDN, inizializzazione e rilascio, allo stesso modo in cui si usa un modem analogico. Un meccanismo automatico deve essere fornito per supportare l'aggiunta e la rimozione del canale B secondario. Le PC card Cisco serie 200 possono fornire servizi ISDN a PC.

Parametri Globali e Tasks di configurazione periferica ISDN: E' necessario **specificare parametri globali e relativi all'interfaccia** per preparare il router a lavorare con un ambiente ISDN.

I parametri globali sono i seguenti:

- **Seleziona lo switch che comunicherà con lo switch ISDN** del provider in **posizione del CO**. Questo requisito è indispensabile poiché i diversi standards, **le specifiche di signaling differiscono a seconda della regione** e della nazone.
- Settare i dettagli di destinazione. Questo comporta **l'indicazione di routes statiche dal router ad altre detinazioni ISDN** e stabilire **criteri che interessano i pacchetti nel router**, addetti ad inizializzare la chiamata ISDN verso la destinazione appropriata.

I Parametri d'interfaccia sono i seguenti:

- Selezionare le **specifiche d'interfaccia**. Specificare **il tipo di interfaccia BRI** ed **il numero della porta BRI ISDN**. L'interfaccia utilizza **un indirizzo ip ed un Subnet Mask**.
- Configurare **l'indirizzamento ISDN con il DDR** dialer information, ed **un ID fornito dall'ISDN service provider**. Indicare che l'interfaccia è parte di un dialer group, utilizzando il pacchetto interessato, settato globalmente. Comandi aggiuntivi, permettono all'isdn di giungere alla destinazione appropriata.
- Seguendo la configurazione interfaccia, è possibile **definire delle features opzionali**, fra cui il tempo di attesa per a risposta su ISDN carrier, e i secondi di pausa prima che il router vada in time out e scarti la chiamata.

Scrivere comandi IOS per configurare una BRI ISDN: Per configurare la BRI entrare nella **modalità di configurazione dell'interfaccia**, ed utilizzare il comando interface bri nella global configuration mode. La sintassi completa del comando è la seguente

Interface bri (numero)

Il numero indica la porta, connettore o il numero di carta dell'interfaccia. Il numero è assegnato in fabbrica o nel momento dell'installazione, quando la periferica è aggiunta al sistema. Essa può essere visualizzata utilizzando il comando show interfaces
E' possibile fae un esempio per configurare una BRI 0 affinchè essa possa chiamare e ricevere chiamate da 2 sites. Utilizza PPP encapsulation per chiamate in uscita, con l'autenticazione chap per quelle in entrata.

```
Interface Bri 0
Encapsulation PPP
No keepalive
Dialer map ip 131.108.36.10 name EB1 234
Dialer map ip 131.108.36.9 name EB2 456
Dialer-group 1
Isdn spid1 0146334600
Isdn spid2 0146334610
Isdn T200 1000
PPP authentication chap
```

Scrivere un comando IOS per definire i tipi di Switches ISDN: Prima di usare ISDN BRI, è possibile **definire il comando isdn switch-type per specificare il CO switch a cui il router si deve connettere**. Il comando cisco IOS aiuta ed illustra i tipi di switch BRI supportati (in nord america, i tipi più comuni sono 5ESS, DMS100 e NI-1). Per configurare il tipo di switch sull'interfaccia ISDN si usa il comando **isdn switch-type nella global configuration mode**. La sintassi completa del comando è:

isdn switch-type (switch-type)

Switch Type, **indica il tipo** di switch relativo al service provider. **Il comando switch-type settato di default come (NONE) disabilita lo switch sull'interfaccia ISDN**. Per disabilitare lo switch sull'interfaccia ISDN specificare quindi:

isdn switch-type none

I seguenti esempi configurano tipi di switch AT&T 5ESS:

```
isdn switch-type basic-5ess
```

kdt-3640 (config) # isdn switch-type ?
basic-ltr6 1tr6 switch type for germany
basic-5ess AT%T 5ESS switch type for the US
basic-dms100 Northern DMS-100 switch type
basic-net3 NET3 switch type for the UK and Europe
basic-ni1 National ISDN-1 Switch type
basic-nwnet3 NET3 switch type for Norway
basic-nznet3 NET3 switch tpe New Zeland
basic-ts013 NTT switch type for Australia
ntt NTT switch type for Japan
vn2 VN2 switch type for France
vn3 VN3 and VN4 switch types for France

Scrivere comandi IOS riguardo agli SPIDs: Le **SPIDs permettono a multiple periferiche** ISDN, come voce e data, di **condividere un Local Loop**. In molti casi, come quando si configurare un router per poterlo connettere ad una DMS-100, è necessario **informare le SPIDs**.
Ricordiamoci che **ISDN è tipicamente usato per la connettività DialUP**. **Gli SPIDs sono processati durante ogni operazione di Call SETUP**. E' necessario usare il comando **isdn spid2** nella modalità di configurazione interfaccia al fine di **definire sul router il numero SPID assegnato al service provider ISDN sul canale B2**. La sintassi completa del comando è isdn spid2 spid-(numbero) (ldn). **Il comando opzionale LDN è usato per un local dial directory number**. Per poter usare **entrambi i canali B**, sulla maggior parte degli switch, **il numero deve corrispondere a quello che proviene dallo switch ISDN**.
Si utilizza il comando **no isdn spid2 per disabilitare lo specifico SPID**, perciò si previene l'accesso allo switch. Se si include il comando LDN nel comando che contiene "no", l'accesso allo switch è permesso ma gli altri canali B non hanno la possibilità di ricevere chiamate in entrata, la sintassi completa del comando è: **no isdn spid2 (numero-spid) (ldn)**
Il termine (numero-spid) **indica il numero che identifica il servizio a cui lo switch è stato sottoscritto**. Questo valore è assegnato dal service provider ISDN, ed **è solitamente un numero di 10 cifre che contiene diverse cifre extra. Per default nessun numero SPID è definito**.

Scrivere comandi IOS per completare la configurazione ISDN BRI:

ISDN switch-Type: Select the AT%T switch as the CO ISDN switch type for this router
Dialer-List 1 protocol ip permit: Associates permitted ip traffic with the dialer group 1. The router will not start an ISDN call for any other packet traffico with dialer group 1.
Interface bri 0: Select an interface with TA and other ISDN functions on the router.
Dialer-group 1: Associates the BRI 0 interface with dialing access group 1.
Dialer wait-for-carrier-time: Specifies a 15-second maximum time for the provider for respond after the call initiates.
Dialer idle-timeout: The number of seconds of idle time before the router drops the ISDN call. Note that a long duration is configured to delay termination.

Descrizione della conferma operazioni BRI: Per confermare le operazioni BRI, si usa il comando **show isdn status per visualizzare lo status delle interfacce BRI**. In questo esempio l'output del TEIs è stato negoziato con successo ed il livello 3 ISDN (End-to-end) è pronto per effettuare e ricevere chiamate.

Considerazioni DDR: Quando si realizzano applicazioni di rete, è necessario **determinare come le connessioni ISDN saranno inizializzate, stabilite e mantenute**. DDR crea **connettività fra siti** ISDN **stabilendo e rilasciando connessioni di tipo circuit-switched** a seconda delle necessità di traffico. **DDR può fornire network routing e servizi di directory** in numerosi modi; Una funzionalità simile a
quella del Full time connectivity su connessioni circuit-switched.
Per fornire controllo totale sulle connessioni DDR, è necessario fare attenzione nella considerazione e distribuzione dei seguenti fattori:

- Quali sites possono **iniziare le connessioni in base al traffico**?
- Secondo le **necessità del Dial-out oppure dei SOHO sites**? E' necessaria **la dial up per la rete o per il management delle worktation**? Quali siti possono **terminare le connessioni in base a link** in stato **di IDLE**?
- Come avviene il **supporto dei servizi di directory e delle tavole di routing sulle connessioni Idle?**
- Quale **applicazioni** necessitano di essere **supportate sulla connessione DDR**? **Per quanti utenti deve** essere supportata?
- Quale protocollo inatteso può dare origine ad una **connessione DDR**? Può essere questo **filtrato**?

Comandi usati per verificare le operazioni DDR: Ping\Telnet: Quando si **pinga** o si **telnetta** un **remote site** o quando traffico interessato raggiunge un link, **il router, invia un cambio nel link status** message alla console.
Show Dialer: Usato per ottenere **un'informazione generale di diagnostica sull'interfaccia configurata per il DDR**, come ad esempio il numero di volte che la stringa di dialer è stata raggiunga con successo, il tempo di idle ed il tempo più rapido di Idle raggiunto dal canale B. Vengono inoltre fornite, **le specifiche di chiamata correnti** come ad esempio la lunghezza della chiamata ed il numero o il nome della periferica a cui l'interfaccia è connessa.
Show ISDN active: Si utilizza questo comando **quando si usa ISDN**. Esso mostra che **la chiamata è in progress, e fa una lista numerata delle chiamate**.
Show ISDN status: Utilizzato per **visualizzare le statistiche** della connessione ISDN

Show IP route: Visualizza **le routes conosciute dal router**, includendo le **routes statiche**, e quelle **acquisite dinamicamente**.

Scrivere un comando IOS per il Troubleshooting delle operazioni DDR: I seguenti comandi possono essere usati per fare il **troubleshooting** sulle operazioni DDR.
Debug isdn q921: **Verifica** che si ha effettivamente una **connessione con lo switch ISDN**.
Debug dialer: Mostra diverse **informazioni** relative al **numero dell'interfaccia che sta chiamando**.
Clear interface: Utilizzata per **cancellare una chiamata in progress**. In una situazione di troubleshooting, questo comando può essere spesso **utile** per cancellare statistiche storiche o tracciare un numero corrente di chiamate eseguite con successo in rapporto a quelle fallite. Si deve usare questo comando con attenzione. Esso **richiede spesso** che si **esegua il parametro sia sul router locale che su quello remoto**.
Si eseguono le operazioni di troubleshoot **sugli SPID problems**, usando il comando **debug isdn Q921**.
Debug isdn q921; packet debugging is on; clear interface bri 0
E' possibile verificare lo status di un cisco 700 ISDN con il comando show Status.

Frame Relay

Che cosa è il Frame Relay: Frame relay è uno standard per (CCITT) e (ANSI) he definisce un **processo per l'invio di dati sulla rete di dati pubblica (PDN)**. La **performance** è Alta, la tecnologia è fra le più efficenti usate nel mondo. Frame relay è un modo per inviare informazioni **attraverso una WAN**, dividendo i dati **in pacchetti**. Ogni pacchetto attraversa una serie di **switches facenti parte della rete frame-relay** fino a raggiugnere la destinazione. Esso opera al livello **FISICO e DATA LINK** del modello OSI, ma è dipendente dai protocolli di livello più alto, come ad esempio **TCP**, usato per la **correzione** degli errori. Frame Relay fu originariamente concepito come un protocollo da usarsi per le interfacce ISDN. Oggi frame relay è un protocollo **industriale standard**, definito come switched data link layer protocol, che gestisce molteplici **circuiti virtuali** utilizzando **l'encapsulation HDLC** fra periferiche connesse. Frame Relay utilizza circuiti virtuali per eseguire connessioni attraverso un servizio **connection-oriented**.
La rete fa in modo che l'interfaccia frame relay possa far parte **sia di una rete pubblica** (carrier-provider) **o di una rete privata** formata da apparecchiature private, che generalmente porta servizio **ad un singolo enterprise**. Una rete frame relay consiste in due tipi di periferiche. **User e Network**. Le periferiche utente sono tipicamente **Computers, Servers**, ecc.ecc. Fanno inoltre parte della rete frame relay, **Switches, Routers, CSU\DSUs, o multiplexers**. Come già precedentemente imparato, le periferiche **utente sono spesso riferite a DTE**, mentre gli **equipaggiamenti** di rete che si interfacciano al DTE sono spessso riferiti al **DCE**.

Terminologia Frame Relay: Ecco alcune terminologie usate nell'ambito del Frame Relay:

- Access rate – La velocità di clock (**velocità della porta**) della connessione (local loop) alla nuvola di rete del flame relay. Questo **è il rate** a cui i dati attraversano ed escono dalla rete.
- Data-link connection identifier (DLCI) – Un numero che **identifica l'end point** in una rete Frame Relay. Questo numero ha significato solo sulla rete locale. Il tipo di **switch frame** relay **mappa il DLCIs fra due router** creando un Permanent Virtual Circuit.

- Local management interface (LMI) – Un segnale standard fra la periferica CPE ed il frame relay switch, che è responsabile del **meccanismo Keepalive**, che verifica che i dati stiano passando; Un meccanismo **multicast che può essere fornito dal server di rete con il DLCI** locale; Il multicast addressing, **permette ad alcuni DLCIs di essere usati come indirizzo** (destinazioni multiple) multicast, e fornisce ad alcuni DLCIs significato globale, piuttosto che un significato locale (DLCIs è usato solo su switch locali); Ed un meccanismo di status che fornisce uno **status continuativo sui DLCIs** conosciuti sullo switch. Possono esistere **diversi tipi di LMI** ed i routers hanno la necessità di **conoscere il tipo di LMI** utilizzato. Tre tipi di LMI sono supportati: **Cisco, Ansi e W933A**.
- Committed information rate (CIR) - Il Rate garantito, in **Bit per Secondo**, che il service provider dovrà fornire.
- Committed burst (Bc) – Il **Massimo numero** di bit che lo switch consente di **trasferire** durante un determinato intervallo di tempo.
- Excess burst (Be) – Il numero **massimo di bit indipendenti che il frame relay si appresta a consegnare in accordo con CIR**. Un valore eccessivo è dipendente dall servizio offerto e dalla disponibilità del venditore. Tipicamente un ecceso di risorse è limitato alla velocità della porta definita sul local access loop.
- Forward explicit congestion notification (FECN) – Un bit settato in un frame che notifica un DTE che riconosce la congestione dovrebbe essere inizializzato dal device SORGENTE.Quando uno **switch frame** relay **riconosce la congestione** sulla rete, esso **invia un pacchetto FECN alla periferica di destinazione, indicando che è avvenuta** la congestione.
- Backward explicit congestion notification (BECN) – Un bit settato in un frame che notifica un DTE che riconosce la congestione dovrebbe essere inizializzato dalla periferica INVIATARIA (sorgente). Quando uno **switch frame** relay **riconosce la congestione** sulla rete, esso **invia un pacchetto BECN al router sorgente**, dicendo al router di **ridurre il proprio "rate"** a cui sta inviando i pacchetti, se il router riceve qualche BECNs durante l'intervallo di tempo corrente, esso **diminuisce il rate di trasmissione del 25%.**
- Discard eligibility (DE) indicator – Un set di bit che indica il frame può avere una priorità **di scarto maggiore** rispetto ad altri frame. Ovviamente questo viene fatto **se esiste una congestione**. Quando il **router rileva congestione** di rete, i pacchetti con **il DE bit sono i primi ad essere scartati** dallo switch Frame Relay. Il bit DE è settato sul traffico descritto sopra (che è il traffico che è stato ricevuto dopo l'incontro con il CIR)

Operazioni Frame Relay: Frame relay può essere usata come un un'interfaccia **relativa ad un public-carrier provider o come parte di una rete privata**. Si dispone un servizio pubblico frame relay, inserendo un equipaggiamento di switching frame relay in un central office oppure in un carrier di telecomunicazioni. I servizi frame relay hanno un **basso costo utente**, **sensibile** comunque **al carico del traffico**. Inoltre non è necessario impiegare tempo e fatica per amministrare e mantenere l'equipaggiamento di rete ed il servizio.

Non esistono standard per interconnettere gli equipaggiamenti all'interno **della rete frame relay già esistente**. Perciò, il supporto sulle interfacce frame relay non necesariamente impone che il protocollo frame relay venga utilizzato sulle periferiche di rete. In questo modo, è possibile utilizzare **un mix di tecnologie come circuit-switching, packet-switching, o hybrid**, tutto questo in combinazione.
La linea che connette le periferica di rete all'equipaggiamento di rete, può operare ad una velocità selezionata. Le velocità di **56Kbps e 2MB** sono quelle tipicamente più usate, comunque frame relay **può supportare velocità più alte e più basse di queste**.

Frame Relay DCLIs: Frame relay fornisce un metodo per **multiplexare diverse conversioni** logiche di dati, riferendosi a **Circuiti virtuali** (virtual circuits), attraverso un media fisico condiviso. Ciò è reso possibile tramite **l'associazione di DLCIs** ad ogni **coppia di interfacce DTE\DCE.**
Il Muliplexing frame relay, fornisce **un uso della banda più flessibile ed efficiente**. Perciò frame relay permette ad utenti di condividere la banda ad un costo estremamente ridotto. Per esempio, noi sappiamo che la nostra WAN utilizza frame relay ed il frame relay, poniamo caso, è l'equivalente di un gruppo di strade. LA compagnia telefonica, solitamente, possiede e mantiene le "strade". E' possibile decidere di prendere in affitto le strade (o path) esclusivamente per la nostra azienda (Dedicate) e renderle dedicate; Oppure è possibile scegliere di pagare MENO su determinate strade "condivise". Dunque frame relay è in grado di girare interamente su reti private. Tuttavia, esso è raramente usato in questo modo.
Gli standars **Frame Relay** si indirizzano su **Circuiti Virtuali Permanenti (PVC)** che sono ammistrati, **configurati e mantenuti in una rete frame relay**. I frame relay PVC sono **identificati da DLCI**. I DLCI frame relay hanno **un significato logico**. **I Valori non sono unici**, nell'ambito del frame relay WAN. **Due periferiche DTE connesse tramite un circuito virtuale** possano usare **differenti valori DLCI** in riferimento alla stessa connessione. Frame relay fornisce un metodo per **multiplexare diverse conversioni** di dati logiche. Lo **switching del service provider** costruisce un **tavola di mappung DLCI** con valori relativi a porte in uscita. Quando un frame è ricevuto, la periferica di switching **analizza l'identificativo di connessione** e fa il delivery del frame sulla porta in uscita, associata. Prima che il frame venga inviato, vi è associato un percorso completo per la destinazione.

I campi del Frame Relay: Parleremo ora del formato frame relativo al frame relay. I campi **Flag** indicano **l'inizio e la fine** del frame end-to-end. A seguito del campo flat, ci sono 2 byte di informazioni dati, 10 bit di questi 2 bytes costituiscono il circuit ID. (che è il DLCI).
I campi frame relay sono i seguenti:

- **Flag** – Indica **l'inizio e la fine** del frame di tipo frame relay.
- **Address** – Indica la **lunghezza del campo indirizzo**. Benchè gli indirizzi frame relay siano tutti di lunghezza pari a 2 bytes, l'address bit permette possibili\future esensioni di indirizzo. Gli otto bit di ogni byte del campo address sono usati per indicare l'indirizzo. L'indirizzo contiene le seguente informazioni:
    - **DLCI Value** – Indica **il valore DLCI**. Consiste nei primi 10 bits del campo Address.
    - **Congestion Control** – Gli ultimi tre bit nel campo field, che **controllano la congestione** ed il meccanismo di notifica per essa all'interno del frame relay. **FECN e BECN scartano dei bit con priorità** di scarto maggiore. (DE Bits).

- **Data** – Campi di lunghezza variabile che contengono dati **encapsulati di livello superiore**. **FCS** – E' il Frame Check Sequence, usato per **garantire l'integrità** dei dati trasmessi.

L'Addressing del Frame Relay: Lo spazio di indirizzo riservato al DLCI è limitato a 10 bit. Questo crea **1024 possibili indirizzi DLCI**. La porzione utilizzabile di questi indirizzi è **determinata dal tipo di LMI utilizzato**. La tipologia **CISCO LMI**, supporta un range di indirizzi **DLCI dal DLCI 16-1007** per trasportare i dati utente. La tipologia **ANSI\ITU LMI** supporta il range di indirizzi dal **DLCI 16-992** per il trasporto dei deti utente. Gli indirizzi **DLCI restante** sono riservati per **implementazione** del venditore. Vengono inclusi **messaggi LMI** ed indirizzi MULTICAST.

Le operazioni LMI: C'è stato un grande sviluppo nella storia del frame relay attorno all'anno 1990. Cisco Systems, Northern Telecom e Digital Equipment Corporation, hanno formato un gruppo che si focalizza sullo sviluppo della tecnologia frame relay ed accellera l'introduzione dell'interoperable frame relay product. Questo gruppo, ha creato una specifica **conforme al protocollo frame relay** di base. Hanno inoltre effettuato **un'estensione del frame relay** includendo funzioni addizionali per ambienti di rete complessi. Queste estensioni frame **sono riferite spesso ad LMI** (local management interface).
Ecco le funzioni principali dei processi LMI:

- Determinare lo **stato operazionale dei vari PVC** che riguardano i router conosciuti.
- Far Transitare **pacchetti Keepalive** per garantire che il **PVC resti UP** e non vada giù per inattività.
- Dire al router **quali PVCs sono disponibili**.

Tre tipologia di LMI possono essere utilizzate dal router: **ANSI, CISCO, e Q933A**.
Estensioni **LMI**:
In aggiunta alle funzioni base del frame relay protocol, per trasferire i dati, le specifiche **includono estensioni LMI** che garantiscono un **grande supporto, e facilità di gestione** per complesse internetworks. Molte **esternsioni LMI sono indirizzate ad un riferimento**, che in comune adotta le specifiche di implementazione. **Altre funzioni LMI sono considerate un Optional.** Elenco adesso un sommario delle estensioni LMI:

- Virtual circuit status messages (common) – Fornisce **comunicazione e sincronizzazione** fra **la rete e la periferica utente**, periodicamente riportando **l'esistenza del nuovo PVC**, cancellando l'esistenza del PVC esistente e fornendo informazioni generali sull'integrità del PVC. I messaggi di status relativi ai circuiti virtuali, prevengono l'invio dei dati sul pvc per tempi più lunghi del previsto.
- Multicasting (optional) – Permette ad un inviatario di **trasmettere un singolo frame** ma esso esegue il **delivery sulla rete a multiple destinazioni**. In questo modo, il multicasting sopporta **trasporto efficente di messaggi** relativi a routing protocols e address resoluzion protocol che tipicamente devono essere inviati a diverse destinazioni simultaneamente.
- Global addressing (optional) – Fornisce **identificativi di connessioni** globalmente, piuttosto che localmente, permettendo essi di essere usati **per identificare un'interfaccia specifica sulla rete frame relay**. Il global addressing rende la rete frame relay simile ad una LAN, in termine di addressing. **L'Address Resolution Protocol** esegue la stessa funzione su frame relay **esattamente come sulla LAN**.

- Simple flow control (optional) – Fornisce **un controllo di flusso XON\XOFF** che viene applicato **all'intera interfaccia Frame Relay**. Esso è riservato a periferiche il cui livello alto non utilizza **una notification di congestione** e necessita numerosi **livelli di flow control aggiuntivi**.

I Campi del Formato frame LMI: La specifica frame relay include anche **le procedure LMI**. I **messaggi LMI sono inviati in frames distinti da una specifica LMI DLCI** definita **in associazione con la specifica (DLCI=1023)** Andiamo ad analizzare il Formato **Frame LMI.** Dopo il campo flag e l'LMI DLC, il frame LMI contiene **4 byte obbligatori**. Il **primo** di questi byte (indicatore di informazione non numerato), ha lo stesso formato del "**lapb unnumbered information**", (UI), con il pool\final bit settato a zero. Il byte **successivo** è riferito al **discriminatore di protocollo**, che è settato ad un valore che indica LMI. Il terzo byte, chiamato reference, è sempre composto da degli "zero".
Il byte **finale** è il campo che specifica il **tipo di messaggio**. Due messaggi sono stati definiti, essi sono lo **STATUS** message e lo **STATUS-ENQUIRY** message. Lo status message risponde allo status-equiry message. Esempi di questo messaggi sono **i Keeplalive** (messaggi inviatii tramite una connessione per garantire che entrambi le parti continuino a mantenere attiva la connessione) e i messaggi di status relativi ad **un report individuale su ogni LCDI** definito per il link. Queste funzionalità **comuni LMI** fanno parte di ogni impelementazione conforme alle specifiche frame relay. Assieme, i messaggi **status e status-enquiry**, ci aiutano a verificare **l'integrità del link logico e fisico**. Questa informazione è molto importante nell'ambiente del routing, poiché i protocolli di routing effettuano decisioni in base all'integrità del link.
Il prossimo elemento (information element,IE) o meglio **CAMPO**, è composto da un **numero variabile di bytes**. Il campo successivo è uguale è al precedente. Ognuno di questi IE consiste in un **Byte IE identifier**, un campo IE per la lunghezza e un byte aggiuntivo contenente l'"actual data".

Il Global Addressing: In aggiunta alle comuni **funzionalità dell'LMI**, **molte estensioni opzionali LMI possono rivelarsi estremamente utili**, in un ambiente di internetworking. La **prima opzione** LMI, molto importante è **il Global Addressing**. Con questa estensione, il valore inserito nel campo DLCI del frame significa globalmente **l'indirizzo di una periferica END-USER** (per esempio, routers).
Come abbiamo notato inizialmente la **specifica base** del frame relay **(non estesa**), supporta solo **valori dei capi DLCI** che **identificano i PVCs** con significato locale. In questo caso, non ci sono indirizzi che **identificano le interfacce di rete**, o nodi collegati a queste interface. Poiché questi indirizzi **non esistono**, esso **non possono essere scoperti dai tradizionali sistemi di "address resolution" e tecniche di scoperta varie**. Questo vuol dire che con il normale addressing Frame Relay, è necessario **creare delle mappe statiche**. Queste mappe statiche, dicono ai router quale **DLCI usare per trovare una periferica remota** ed il suo associato indirizzo di internetwork. Notare che **ogni interfaccia ha un proprio identifier**. Supponiamo che Pittsburgh deve inviare un frame a San Jose. Il valode DLCI di San Jose termina con il VC di 22 ed a Pittsburgh il valore è 62. Pittsburg posiziona quindi il valore 62 len DLCI field ed invia il frame sulla rete frame relay in modo da raggiungere sal jose. Ogni interfaccia router è un **valore distinto ed un proprio node identifier,** per cui periferiche individuali possono essre distinge. Questo permette il routing **in un ambiente complesso**. Il Global Addresing fornisce un **beneficio significativo** in una rete complessa e di grandi dimensioni. La rete **frame relay appare come il router nei confronti delle sue periferiche** come una wan.

Il Multicasting e l'inverse ARP: Il **multicasting** è un altro **prezioso dettaglio opzionale**. I Gruppi **multicast** sono designati da una serie di **4 valori DLCI rieservati** (da 1019 a 1022). I Frames inviati da una periferica che sta usando uno di questi DLCI riservati sono **replicati dalla rete** ed

inviati a tutti i punti di uscita esistenti nel set designato. Questa estensione multicasting **definisce i messaggi LMI** che **notificano le periferiche** utente per **l'aggiunta**, la **cancellazione** e la **presenza di gruppi multicast**. All'interno della rete che acquista vantaggi dal **dynamic routing**, le informazioni di routing, devono essere scambiati attraverso diversi routers. **I messaggi di routing possono essere inviati efficentemente usando i frames con un multicast DLCI**. Questo permette ai messaggi di essere inviati ad un gruppo specifico di routers. Il meccanismo di **INVERSE ARP, permette al router di contruire automaticamente una mappa di tavole Frame Relay**. Il router capisce **che i DLCI sono in uso da lo switch durante lo scambio iniziale di LMI**. Il router quindi **invia un inverse arp request ad ogni DLCI per ogni protocollo configurato sulla interfaccia**, se il protocollo è supportato. **L'informazionc he torna indietro dall'inverse ARP, è quindi utilizzata per costruire la mappa Frame Relay**.

Mapping Frame Relay: Il router che secondo l'indirizzo determinato dalla routing table, fa parte del prossimo HOP, dev'essere **scoperto dal frame relay DLCI**. La risoluzione è eseguita tramite una **struttura dati chiamata Frame Relay MAP**. La routing table è quindi usata per **fornire l'indirizzo del prossimo hop** al **protocollo del DLCI** per il traffico in uscita. Questa struttura di dati può essere **configurata staticamente sul router**, e la funzione **inverse ARP** può essere usata per fare un **setup automatico** della Mappa.

Tavole di switching Frame Relay: La tavola di switching frame relay consiste in **4 Entries**. **Due** per la **porta d'ingresso e DLCI** e **due** per la **porta in uscita e DLCI**. **DLCI** può essre **rimappato** a seguito del **passaggio da ogni switch**.
il fatto che il **riferimento di porta possa essere cambiato** è perche' il **DLCI non cambia** anche se **il riferimento di porta puo' cambiare**

SottoInterfacce Frame Relay: Per abilitare l'invio di un **completo update** di **routing** in una rete frame relay, è possibile configurare il router **con interfacce assegnate logicamente**, chiamate **subinterfacce**. Le subinterfacce sono suddivisioni **di logiche o fisiche interfacce**. Nella configurazione delle subinterfacce, **ogni PVC può essere configurato come connessione punto punto**. Questo permette alla **sottointerfaccia** di **funzionare come linea dedicata**.
Una singola interfaccia router, può servire molte locazioni remote, tramite un'unica interfaccia individuale.

Split Horizon Routing: Lo Split Horizon **riduce i routing Loops** facendo in modo che non vi sia un continuo invio dei dati ricevuti da un'interfaccia fisica verso la stessa interfaccia in uscita.Come risultato, se un router remoto invia un aggiornamento ad router principale che sta connettendo multipli PVC su una singola interfaccia fisica, il router principale (headquarters) non puo' comunicare la route attrraverso la stessa interfaccia agli altri routers remoti.

La risoluzione Point To Point e specifiche Multiporta: E' possibile **configurare le SUB interfacce** in modo che esse supportino i seguenti tipi di connessioni:

- Point-to-point – Una subinterfaccia singole è usata per stabilire una connessione PVC verso un'altra interfaccia fisica o verso uin router remoto. In questo caso l'interfaccia dev'essere nella stessa subnet ed ogni interfaccia deve avere un singolo DLCI. Ogni connessione point to point appartiene alla propria SUBNET. In questo ambiente, i broadcast non sono un problema poiché i routers sono point to point e si comportano come linee dedicate..
- Multipoint – Una singola subinterfaccia è usata per stabilire multiple connessioni PVC a multiple interfacce fisiche o subinterfaccia su untenti

remoti. In questo caso, tutte le interfacce partecipanti, devono trovarsi nella stessa subnet, ed ogni interfaccia deve avere il prorpio DLCI locale. La subinterfaccia si comporta come una rete regolare Frame Relay in questo ambiente, perciò i routing updates sono soggetti ad uno split horizon.

Scrivere una sequenza di comandi IOS per la configurazione Frame Relay: Una configurazione base frame relay presuppone che si voglia configurare frame relay su una o più interfacce fisiche e che LMI e Inverse ARP siano supportate dai routers remoti. In questo tipo di ambiente, l'LMI notifica il router sulla disponibilità del DLCIs. Inverse ARP è abilitata per default, essa quindi non appare nella configuration output. Ecco 3 steps per configurre frame relay.

```
Router (config#) interface serial 0
Router (config-if#) ip address 192.168.38.40 255.255.255.0
Router (config-if#) encapsulation frame-relay  (cisco o ietf)
Router (config-if#) frame-relay lmi type (ansi, cisco, q933a)
Router (config-if#) frame-relay inverse-arp  (protocol) (dlci)
```

Comandi per verificare le operazioni Frame-Relay:

show interface serial1: visualizza informazioni sul multicast DLCI, il DLCIs usato sulle interfaccia seriale frame-relay configurata ed il LMI DLCI usato per la LMI.
Show frame-relay pvc: Visualizza lo status di ogni connessione configurata e le statistiche del traffico. Questo comando è anche utile per visualizzare il nmero del BECN e FECN ricevuti dal router.
Show frame-relay map: Visualizza l'indirizzamento di livello 3 e le DLCI associate per ogni destinazione remota a cui il router è connesso.
Show frame-relay lmi: Visualizza le statistiche del traffico LMI. Per esempio, esso mostra il numero dei messaggi di status scambiati fra il router locale e lo switch frame relay.

Comandi Opzionali Frame-Relay: Normalmente l'inverse ARP è usato per richiedere l'indirizzo al protocollo sul prossimo HOP, per una specifica connessione. Le risposte all'inverse ARP sono inserite in un INDIRIZZO-To-DLCI map. (che è la frame relay map) table. La tabella è quindi usata per il traffico in uscita. Ci sono tre istanze in cui è necessario definire l'indirizzo al DCLI table staticamente:

- Quando l'inverse ARP non è supportato dal router remoto
- Quando si configurare OSPF sul Frame Relay
- Quando si vuole controllare il traffico broadcast utilizzando routing.

Le entries statiche sono riferite ad una mappatura statica.

Con il frame relay è possibile incrementare o decrementare l'intervallo di keepalive. E' possibile estendere o ridurre, l'intervallo a cui l'interfaccia router invia i messaggi keepalive allo switch frame relay. Il default è 10 secondi e la sintassi è la seguente:

```
router(config-if)#
keepalive number
```

Dove il numero è il valore, in secondi, solitamente 2 o 3 (che è l'intervallo minore) più veloce rispetto ai settaggi dello switch frame relay, questo serve a garantire una corretta sincronizzazione.

Se un tipo LMI non è usato nella rete, o quando si sta

Se non si usa un 'LMI type' nella rete, o quando stai facendo un test tra i routers, si deve specificare il DLCI per ogni interfaccia locale usando il seguente comando:

```
router(config-if)#
frame-relay
local-dlci number
```

where number is the DLCI on the local interface to be used.

Protocol: Definisce il protocollo supportato, bridging e logical link control.
Protocol-Address: definisce l'indirizzo di livello network sull'interfaccia router di destinazione.
Dlcl: Definisce il DLCI locale usato per connettersi al remote protocol address
Broadcast: (opzionale) Forwarda i broadcasts a questo indirizzo, quando il multicast non è abilitato. Si usa questo comando se si vuole che il router forwardi i routing updates.
Ietf | cisco: (opzionale) Sceglie il tipo di encapsulation frame relay, per l'utilizzo. Si usa ieft solo se ci si connette ad un router non cisco, remoto. Altrimenti si usa cisco.
Payload-compress
Packet-by-packet: (opzionale): payload pacchetto per pacchetto, e compressione usata con lo stacker method.

NETWORK MANAGEMENT

Come dev'essere una rete: La visuale di una rete è importante. Una rete è un insieme di periferiche che interagiscono con altre e forniscono comunicazione. Quando un amministratore di rete vuole **progettare** una rete esso dovrebbe essere iniziare a vedere il progetto **dal punto di vista Generico piuttosto che da quello individuale.** In altre parole, **ogni periferica**, in una rete, può generare **effetti su tutte le altre** periferiche e quindi a tutta la rete, nel suo complesso. Non c'è niente che può essere "isolato", quando si parla di connnessione alla rete.
Un buon paragone può essere fatto con una automobile. L'auto è una serie di parti che forniscono il trasporto, il motore fornisce potenza per spostare la macchina, ma il motore non può lavorare molto bene se non funziona il sistema che permette alla benzine di affluire, o se le gomme dell'auto mancano. I freni sono componenti importanti, ma senza il sistema idraultico essi non funzionano e la macchina non può fermarsi. Tutti i componenti devono lavoare insieme in modo da eseguire l'operazione per cui essi sono stati designati.
La stessa cosa è applicabile su un sistema di rete. Se il server di rete è settato per lavorare con il protocollo IPX\SPX e gli host non lo sono, non ci sarà comunicazione. Dunque, se il sistema sta lavorando bene e l'amministratore cambia i protocolli su una macchina senza fare questa variazione sulle altre, l'intero sistema smette di funzionare. Una periferica influisce sulle altre. La comunicazione fallisce anche quando un host è configurato per cercare un server DNS su un indirizzo ip non corretto. Un server DNS deve essere locato, ad esempio, sull'ip address 192.150.11.23 e tutti gli hosts sono configurati per trovare il DNS a questo indirizzo. Se un tecnico di rete cambia l'indirizzo ip del server senza cambiare la configurazione sugli hosts, questi non avranno più la disponibilità del servizio DNS.
La cosa importante da ricordare **quando ci si dedica alla rete, è vedere essa come una singola unità, comparandola ad un gruppo individuale di periferiche connesse**. Quando è applicabile

anche ad una WAN, che è usata, per collegarsi ad internet, ad esempio. I cambiamenti che sono stati fatti al router, hanno un effetto diretto sull'efficienza e sull'affidabilità della comunicazione all'interno di tutto il sistema.

I requisiti di una rete: In una rete di tipi Enterprise, è importante che lo staff **conosca le proprie responsabilità**.. Il network staff diagnostica problemi dell'utente desktop o più semplicemente determina che il problema,utente, non è relativo alla comunicazione.Spesso ci chiediamo: La responsabilità del network staff si estende solo dalla stesura del cablaggio orizzontale fino al muro, o arriva fino alle schede di rete degli apparati?
Queste definizioni sono molto importanti per il reparto di rete. Esse **influiscono sul carico di lavoro** di ogni persone e sul costo del servizio di rete, dell'intera enterprise. Quanto **più grande è responsabilità, di uno staff di rete, tanto più alto è il costo relativo alle risorse**. Immaginiamo un ristorante che appartiene ad un singolo individuo. Questa persona è responsabile di tutti i tasks, fra cui, cucinare, servire, lavare..ecc.ecc. Il costo per le risorse relative a questo ristorante è relativamente basso. Le possibilità di crescita e le espansioni sono limitate finchè la gestione funzionerà in questo modo. Quando le responsabilità saranno divise, il ristorante potrà servire più persone in molti modi. Nel complesso, i costi relativi alle risorse si sollevano relativamnete a quella che è l'espansione e la crescita complessiva.
L'esempio del ristorante, mostra che il **lavoro del network support**, **può estendersi per tutta la rete, nel proprio complesso o può essere limitato a certi componenti**. Queste responsabilità devono essere definite e rispettate in un determinato reparto per ordine dei responsabili. La chiave è comprendere questa relazione, in cui le **responsabilità eccessive relative ad un'area possono sovraccaricare le risorse dell'azienda**. Se si considera l'area troppo piccola, si può avere delle difficoltà nel risolvere effettivamente i problemi della rete.

Costo di una Rete: L'amministrazione della rete **sviluppa numerose responsabilità**, inclusi i **costi** di analisi. Può essere determinato il **costo del design, e dell'impelementazione. Inoltre il costo per mantenere, upgradare e monitorare la rete**. Determinare il costo di un'installazione di rete, non è un task particolarmente difficile per la maggior parte degli amministratori di reti. La lista degli equipments ed i costo può essere prontamente stabilito. I costi di laboratorio possono essere calcolati usando tassi fissi. Sfortunatamente il **costo di fabbricazione** della rete è un aspetto da considerare **SOLO quando si calcola il final cost**.
Ci sono diversi altri fattori che determinano il **costo**, che devono essere considerati. Questi possono essere, **la crescita della rete, nel tempo. Il training, la produzione software, le riparazioni**. Questi costi sono **difficili da determinare**, più di quanto possa esserlo quello dell'intera rete. L'amministratore di rete dev'essere in grado di vedere **gli storici della crescita, la tendenza, i progetti e quindi i costi della cresciuta relativi alla rete**. Un manager deve considerare il nuovo software ed hardware per determinare se l'azienda dev'essere implementata e quando dev'esser fatto questo. Il training staff ha necessità di supportare queste nuove tecnologie.
Il costo dell'equipment ridondante **per le operazioni di tipo "mission critical",** dev'essere aggiunto al costo di mantenimento relativo alla rete. Si pensa ad un lavoro basato su internet in cui si usa un singolo router collegato ad internet. Se il router va giù, l'azienda non lavora finchè il router non è rimesso su. Questo comporta costi molto alti, quantificabili in migliaian di Dollari\Euro. Un amministratore di rete esperto deve posizionare il **router chiave** in modo tale da minimizzare il tempo in cui l'azienda resterà offline.

Errore nel report della Documentazione: Come già menzionato nei precedenti semestri, un management di rete **richiede documentazione**. Quando i problemi vengono fuori, **è necessario documentarli**. Questi **documenti**, che vengono prodotti, saranno usati per garantire in futuro **informazioni basilari utili ad identificare ed assegnare i problemi di rete**. Ciò fornirà un metodo per tracciare il progresso ed una eventuale soluzione al problema. I **reports** del protocola forniscono

giustificazioni al gestore del team network per poter assumere nuovo staff, acquistare nuove apparecchiature o fornire training addizionale. Questa **documentazione** fornisce **soluzione** per **identificare problemi che sono stati già risolti in passato**.
Tutto il materiale presentato fin qui, in questo capitolo ha a che fare con questioni non tecniche del network management. Il resto del capitolo mostrerà gli strumenti che sono disponibili per monitorare e diagnosticare i problemi sulla WAN.

Perchè è necessario monitorare una rete: Ci sono **molte ragioni** per **monitorare** la rete. Due primarie ragioni sono **prevedere eventuali cambiamenti, relativi ad una futura crescita e rilevare cambiamenti attuali sullo status del network**. I cambi inaspettati possono essere quelli relativi ad **un Fallimento di un router o di uno switch**, o può trattarsi di un **tentantico di hacking** da parte di un hacker con lo scopo di fornire accesso illegale alla rete o far fallire di proposito link di comunicazione. **Senza** la possibilità di **monitorare** la rete, un amministratore non può anticipare e prevedere i problemi; Solo cercare di risolverli **dal momento in cui essi sono già accaduti**. Senza questa abilità, l'amministratore può solo **reagire quando già il problema è nato**.
Nei semestri precedenti, i testi in cui ci si focalizza sul "fuoco" primario su una lan, si spiega che, il monitoring di una WAN, dev'esser fatto **con diverse tecniche di management**, simili a quelle relative alle Lan. Una delle maggiori differenze fra Wan e Lan, è la **posizione fisica** degli elementi che le compongono. La **posizione degli sturmenti di rete**, può a sua volta, **diventare tanto critica** da **interrompere tutte le operazioni sulla WAN**.

Monitoring di connettività: Una delle forme basilari di monitor sulla connessione è effettuato ogni giorno sulla rete; Le connessioni **operano propriamente** quando gli **utenti sono abilitati a fare il logon sulla rete**. Se gli utenti non possono loggarsi, il team di supporto network sarà contattato al più presto. Ovviamente questo sistema non è tra i migliori. **Semplici programmi** offrono all'amministratore la possibilità di avere una **lista di indirizzi ip**.
Questi indirizzi sono **pingati periodicamente**. Se esiste un problema di connessione, il programma **metterà in alert l'amministratore** secondo i **risultati di una ping request**. Questo sistema di monitoring sulla rete è tuttavia **primitivo ed inefficiente**. Difatti esso può solo determinare se c'è una **comunicazione che "cade"** fra la stazione monitor e la periferica "target". Il **fallimento**, può riguardare **un router, uno switch, un segmento** di rete. Il **ping** request riesce a capire che la connessione è Down, ma **non può determinare la locazione del problema**.
Controllando tutti gli hosts sulla WAN tramite questo sistema può portar via molte risorse. Se la rete ha 3000 hosts, pingare tutti i sistemi può **portar via molte risorse di sistema**. Un buon modo è **pingare solo gli hosts importanti**, ad esempio **SERVER**, **Router, e sewitch**, al fine di verificare la loro connettività.
Il test del ping non ti daranno dati reali, a meno che le workstation non sono sempre lasciate attive. Di nuovo, questo metodo di monitorare dati dovrebbe essere usato solo se non ci sono altri metodi disponibili.

Monitoring del Traffico: Il **monitoring del traffico** è il metodo più **sofisticato** di network monitoring. Esso **considera il traffico attuale** dei pacchetti sulla rete e **genera dei reports** basandosi su di esso. Programmi come ad esempio Windows NT Network Monitor, e Fluke's Network Analyzer, sono esempi di questo tipo di software. Questi programmi non solo **rilevano fallimenti** su equipaggiamenti di rete, **ma determinano, SE un componente è sovraccaricato o mal configurato**.Lo **svantaggio** di questo tipo di programma è che esso normalmente **lavora su un singolo segmento alla volta**. Se si ha la **necessità** di **filtrare dati di altri segmenti**, il software di monitoring **dev'essere "spostato"** su questi altri segmenti. Qiesta operazione può essere facilmente effettuata **con l'uso degli agents per i segmenti** remoti di rete. Apparecchiature come switches e routers, hanno l'abilità di **generare e trasmettere statistiche del traffico** in quanto questa funzionalità, fa parte del loro sistema operativo.

Quindi, **in che modo** i dati sono **raccolti e organizzati** in una maniera che possa essere utile all'amministratore della rete centralizzata? la risposta è: il protocollo di gestione semplice della rete,**SNMP**.

SNMP: SNMP è un protocollo che permette la **trasmissine di dati statistici sulla rete verso una console centrale di Management.**
SNMP è un **componente dell'architettura di management della rete**. Questa architettura consiste in 4 maggiori componenti:

1. Stazione di Management: La stazione di management è **l'interfaccia manager di rete**, all'interno del siste.a Ha il compito di **manipolare e controllare i dati** che provengono dalla rte. La stazione di management, inoltre, **mantiene un database di informazioni di management (MIB)** estratte dalle periferiche che gestisce.

2. Management Agent: L'agent di management è il **componente che è contenuto nella periferica che dev'essere controllata.** Bridges, hubs, routers, e switch, possono **contenere agenti SNMP** che permettere il **controllo da parte della stazione di Management**. Il management **Agent risponde** alla stazione di management in due modi. In primo luogo **tramite un POLLING**, la stazione di management **richiede i dati dall'agent** e l'agent risponde con i dati richiesti. **Il TRAPPING**, invece è un metodo di **prelievo ed analisi dati**, designato per **ridurre il traffico sulla rete ed effettuare processi sulle periferiche già monitorate**. La stazione di management fa il **polling all'agent a specifici intervalli**, continuativi, il cui **limite è settato sulla periferica** controllata. Se la soglia, sulla periferica, è ecceduta, verrà inviato **un messaggio di alert alla stazione di management**. Questo elimina la necessità di fare il pool continuamente. Il **trapping** è una tecnica **molto efficace** e porta **vantaggi su reti con un grande numero di periferiche** che hanno bisogno di essere gestite. Esso **riduce** l'ammontare del **traffico SNMP** sulla rete e fornisce più banda per il trasfer dei dati.

3. Informazioni base di management (MIB): Il "management information base" ha un **database strutturato** ed è **residente su ogni periferica** gestita. Il database contiene **una serie di oggetti,** che sono **risorse dati filtrati sulla stessa periferica** gestita. Molte categorie all'interno del MIB includono interfacce dati,dati TCP e dati ICMP.

4. Il Network Management Protcol: Il network management protocol **usato è SNMP**. SNMP è un protocollo di **livello Applicazione**, designato per comunicazioni dati **fra la console management e management agent**. Esso ha 3 possibilità "chiave": **GET, PUT, e TRAP**. **GET** permette alla management console di fare un **retrieving** dall'agent. **PUT**, permette alla **management console di settare valori su oggetti** sull'agent. **TRAP**, operazione per cui il management agent **invia dati alla stazione di management**.

La parola chiave che dobbiamo ricordare è dunque Simple Network Management Protocol. Quando **SNMP** fu creato, esso fu designato per essere uno sistema **a rapida terminazione**, destinato ad essere sostituito poco dopo. Ma TCP\IP, è diventato uno dei maggiori standars nel management delle configurazioni internet-internet. **Con il trascorrere degli anni, si è visto aumentare l'utilizzo dell'SNMP** che ha permesso a sua volta l'espansione del management e del monitoring sulle periferiche. **Uno dei risultati è stato il remote monitoring (RMON).** Si tratta di una **estensione di SNMP** che offre la possibilità di **considerare la rete per intero piuttosto che considerarne, una ad una, le periferiche** che ne fanno parte.

Monitoring Remoto (RMON): La **proble raccoglie** i dati remoti **in un RMON**. Una **probe** a la **stessa funzione di un Agent SNMP**. Una proble ha delle specifiche di Remote monitoring, un agent no. Quando si lavora con **RMON o SNMP** una **console** di management **centrale** rappresenta il **punto di raccolta dati**. Una **probe RMON** è locata **su ogni segmento** della rete monitorata. Queste probes possono essere **hosts dedicati**, residenti **su un server** o **inclusi in una periferica** di rete standard che può essere un router o uno switch. Queste probes **raccolgono dati specifici** da ogni segmento e li **rilasciano sulla console di management**.
Il **redundant management console**, fornisce **2** maggiori **benefici ai processi di management** della rete. Il primo è **abilitare più di un amministratore di re**te in **differenti locazioni fisiche**, a gestire e monitorare **la stessa rete**. Per esempio, un amministratore di rete può essere a new york ed un altro a san jose. Nel caso di **redundanza**, si hanno due o più console di management. Se una delle 2 consoles fallisce, l'altra console può essere usata per monitorare e controllare la rete finchè la prima rete non è riparata.
L'estensione RMON dell'SNMP procol **crea nuove categorie di dati**. Queste categorie aggiungono **molti rami al MIB database**. Ona delle maggiori categorie saranno spiegate nella lista seguente:

1. Il gruppo di statistiche su ethernet
   Contiene **statistiche filtrate** per ogni sottorete monitorata. Queste statistiche includono **contatori** (partono da zero e sono incrementali) per **byte, pacchetti, errori e dimensioni frames**. L'altro tipo di riferimento data è la index table. La tabella **identifica ogni periferica ethernet** monitorata permettendo ai contatori di **tenere il conteggio per ogni periferica ethernet** individuale. Il gruppo di statistiche ethernet fornisce una **visuale del carico complessivo e della vita della sottorete**. Esso effettua ciò **misurando diversi tipi di errori** , fra cui quelli comunemente legati al **CRC, collisioni e pacchetti oltre e sotto la dimensione standard**.

2. Gruppo di controllo storico
   Contiene una tabella di dati che registrerà **campioni dei conteggi** di gruppi di **statistiche** che si registrano **durante un periodo di tempo prestabilito**. Il **tempo di default** settato, per esempio, può essere di trenta minuti (1800 secondi). La dimensione di default della tabella è **relativa a 50 entries**. Il totale è dunque 25ore di monitoraggio continuo. Dopo che l'history è stata creata per specifici contatori, viene creata una nuova entry nella tabella, dopo ogni intervallo di tempo, finchè il **limite di 50 entries** non è raggiunto. **Quindi viene creata una successiva new entry e quella più vecchia viene eliminata**. Questi dati **forniscono una baseline** per la rete. Possono essere usati per pragonare ancora la baseline originale e quindi risolvere problemi o ancora,updatare la baseline a seguito di cmbiamenti che si effettuano sulla rete.

3. Il gruppo Alarm
   Vengono usati **specifici limiti chiamati "thresholds"** (soglie). Se il contatore monitorato, supera
   Questa soglia, viene inviato un **messggio specifico di allarme** ad un utente. Questo processo, conosciuto come **Error Trap**, può automatizzare molte funzioni relative al network monitoring. **Senza l'error Trap**, una persona deve **continuamente monitorare**, in **maniera diretta** la rete, o aspettare che un utente identifichi il problema (quando si è già verificato). Con la **funzionalità Error Trap, il processo di rete automaticamente invia un messaggio all'utente o al personale addetto al management della rete**, segnalando che è avvenuto un problema sulla rete. E' dunque ritenuto, **l'error trap**, un componente molto importante di **troubleshooting preventivo**.

4. Il Gruppo Host

Contiene **contatori che segnalano la scoperta di ogni host sul segmento** della sottorete. Alcune delle categorie, relative a questi contatori, possono basarsi su **Pacchetti, Ottetti, Errori e**

Broadcasts. I tipi di contatori associati con essi possono essere per esempio, **Pacchetti totali, Pacchetti ricevuti, ecc.ecc**

5. Il gruppo Host TOPN

E' usato per **preparare i report su un gruppo di hosts** che mostrano **una lista statistica basata su parametri di misura**. Il miglior modo per descrivere questo gruppo è fornito da un esempio; Un report può essere generato dalla top ten di host che hanno effettuato **maggior broadcast** durante il giorno. Un altro report più essere generato dai **pacchetti più trasmessi** durante il giorno. Questa categoria fornisce un modo facile per determinare **chi e quale tipo di dato solitamente fa parte del traffico che passa da quel determinato segmento**.

6. Il Gruppo matrix

Registra la **comunicazione data fra hosts su una subnetwork**. Questo dati è memorizzato in modalità Matrix (matrix form= a multi-dimensional table). Uno dei reports che può essere generato da questa categoria è quello relativo ad un host che fa utilizzo di un server, Ad esempio. Riconoscendo il "matrix order", è possibile **creare altri reports**. Per esempio, un report può mostrare **tutti gli utenti di un particolare server, mentre un altro report postra tutti i servers utilizzati da un host particolare.**

7. Il gruppo di filtraggio (filter group)

Fornisce un metodo che **consente ad una console di management di istruire un Probe Rmon**, affinchè esso **filtri pacchetti, selezionati da una specifica interfaccia ad una subnetwork**. Questa selezione è basata sull'uso di due filtri, **il Data e lo STATUS filter**. Il Data filter è designato per fare o non fare **un match su particolari gruppi di dati**, permettendo o meno il loro passaggio. Lo status filter è basato sul **tipo di pacchetti individuati**. In questo modo, per esempio è possibile **identificare CrC packet o Valid Packet**. Questi filtri possono essere combinati utilizzando "and" "and" per creare condizioni molti complicate. Il gruppo di filtraggio da la possibilità, all'amministratore di rete, di **selezionare, selettivamente, differenti tipi di pacchetti al fine di un'analisi della rete e del troubleshooting**.

8. Il Gruppo packet capture

Permette all'amministratore di **specificare un metodo da usare per catturare i pacchett**i che sono stati **inclusi all'interno del gruppo di filtraggio**. Catturando specifici pacchetti, l'amministratore di rete può **individuare dettagli esatti riguardanti i pacchetti interessati**. Questo gruppo di paccketti inoltre, **specifica la quantità del pacchetto individualmente catturato**, ed il numero totale.

9. Il gruppo Eventi

Contiene eventi **generati da altri gruppi nel MIB database**. Un esempio può essere quello di un contatoore che **eccede la soglia indicata nell'alarm group**. Questa azione deve **generare un evento, all'interno dell'event group**. Basandosi su questo evento, dev'essere quindi **generata un'azione**, come ad esempio, l'esposizione di un messaggio di warning, che viene inviato alle persone inserite
All'interno dell'alarm group, o pure **avviene una creazione di entry nell'event table**. Un evento è generato **per tutte le operazioni di comparazione all'interno dell'RMON MIB extensions**.

10. Il Gruppo Token Ring

Contiene **contatori specifici** per reti token ring. Mentre **molti dei contatori** compresi **nell'RMON** Extensions **non specificano il tipo di protocollo data link**, **le statistice e l'history group lo fanno**. Esse sono particolarmente selettive per quanto riguarda il **protocollo ethernet**. Il token ring group crea **contatori necessari a monitorare e gestire la rete token ring utilizzando RMON**.

E’ importante ricordare che **RMON** è **una estensione del protocollo SNMP**. Specificatametne questo vuol dire che **ROMN aumenta le operazioni e le capacità di monitoring di SNMP**, quest’ultimo invece, è **necessario per RMON**, affinchè esso possa operare su una rete. Come ultimo punto è importante mensionare che ci sono state delle revisioni recenti di SNMP e RMON. Esse sono chiamate SNMPv2 e RMONv2.

Soluzioni ai problemi: I problemi sono cose di tutti i giorni. Anche quando la rte è monitorata, l’apparecchiatura è affidabile, e gli utenti sono attenti, qualcosa può andare storto. **Lo skill** di un buon amministratore di rete, è concentrato sull’abilità di **analizzare, di diagnositcare e correggere problemi**, sotto la pressione di cadute sulla rete che causano mancanza di disponibilità, nelle risorse di lavoro aziendali. Le tecniche di un buon amministratore di rete sono state descritte nel semestre 3. Vedremo alcuni suggerimento relative a queste tecniche nelle quali vengono inclusi alcuni strumenti di troubleshooting per la rete. Queste tecniche rappresentano degli efficenti strumenti per risolvere i problemi di rete.
La prima cosa, fra l’altro anche la più importante, è usare **l’engineering journal** per prendere note. Ciò può definire un chiaro percorso per la diagnosi dei problemi. E possibile scoprire che cosa è già stato fatto e quindi riuscire a capire qual è la causa effettiva del problema. Una copia di queste note, deve essere inclusa alla risoluzione del problema, quando il troble ticket per il lavoro, è completo. I Futuri troubleshooting per problemi simili, possono giovare positivamente da questo lavoro, così è possibile risparmiare tempo nel cercare tecniche risolutive già precedentemente applicate.
Un altro elemento essenziale di troubleshooting preventivo è il labeling (etichettamento). E’ necessario etichettare ogni cosa, incluse le 2 fini del cablaggio orizzontale. Questa etichettatura deve includere **il numero del cavo, la locazione in cui, eventuali altri cavi sono locati** (nelle vicinanze) e **l’utilizzo del cavo**. Per esempio, si può pensare che il cavo venga utilizzato per Voce, data o video.
Questo tipo di eticchetta può essere anche più preziosa di un foglio di tagliatura cavi (o cablaggio tagliato, non capisco) quando c'è da risolvere dei problemi, perchè questa è posizionata proprio dov'è l'unità e non buttata in qualche cassetto da qualche parte.
E’ necessario **etichettare ogni porta sull’hub, switch, router, evidenziare la locazione, lo scopo ed il punto di connessione**; Sono cose, queste che aiuteranno a risolvere i problemi con più facilità. In fine, tutti gli altri componenti collegati alla rete, devono essere, anch’essi, etichettati per Locazione ed Utilizzo. Con questo tipo di etichettatura, tutti i componenti possono essere locati ed il loro scopo sulla rete potrà essere definito senza grossi problemi.
Il giusto labeling, usato con la documentazione di rete, creata quando la rete è stata costruita o updatata, darà una completa immagine della rete e relazionship di dati. Una reminder importante che proviene dal semestre procedente è che la documentazione **è utile solo se è “corrente”.** Tutti i **cambiamenti effettuati** alla rte, **devono essere documentati** sia sulla periferica sostituita\aggiunta che sul foglio di documentazione usato per definire la rete completa.
Il **primo step** nel troubleshooting di rete, **è definire il problema**. La definizione può essere consolidazione di differenti sorgenti. Una delle sorgenti può essere un trouble ticket o un report che proviene dall’helpdesk, che inizialmente identifica un problema. Gli strumenti di monitoring per il network possono **fornire una completa idea sullo specifico problema** e sulla eventuale **soluzione legata ad esso**. Altri utenti ed osservazioni possono fornire **informazioni aggiuntive**. La valutazione di tutte queste informazioni può fornire al troubleshooter una posizione più chiara per poter risolvere il problema, spesso, migliore rispetto a quella che si avrebbe riciclando informazioni relative ad altre sorgenti.

Metodi per il Troubleshooting: La tecnica del **processo di eliminazione, e la tecnica di divisione** e **acquisizione,** sono i **metodi di maggior successo** per il **troubleshooting** sul networking.

La tecnica relativa al processo di esclusione (the process of elimination technique) è applicabile ai seguenti problemi:

Un utente su una rete chiama l'help desk per segnalare che il suo computer non può più collegarsi ad internet. L'help desk effettua un report e lo passa al supporto network.
L'utente informa il supporto , telefonicamente, che esso non ha fatto niente di diverso nel connettersi ad internet; Il problema si è verificato da solo. La persona di supporto, controlla i logs dell'hardware, via rete, e vede che il pc è stato upgradato la scorsa notte. Si suppone che i driver di rete possono non essere correttamente configurati. Dunque si procede con il controllo sulla configurazione di rete. Essa appare corretta, il ping al server fallisce.
La prossima idea che ci viene in mente è quella di controllare i collegamenti fisici della workstation con il cavo di rete. Entrambi le cime del cavo sono controllate, dunque riproviamo ancora a pingare il server. Dopo di che si prova a pingare 127.0.0.1. Il pung ha successo per cui si elimina possibili problemi relativi al computer, alla configurazione dei driver relativa alla scheda di rete.
Il supporto tecnico, quindi, decide che potrebbe trattarsi di un problema con il server per il segmento di rete. Esiste un altro computer collegato in rete, accanto a questo, ma esso riesce a pingare bene il server. Ciò esclude che si possa trattare di un problema di server, di backbone o di connessione al server. Dunque si va sull'IDF e si cambia la porta relativa alla workstation che da problemi. Il ping è ripetuto di nuovo, dalla workstation al server. Questa soluzione sembra non funziionare. Dunque si effettua una ricerca lungo la cablatura orizzontale fino al patch cable. Dunque si posizione il cavo sulla porta dell'IDF originale, quindi si fa passare un NUOVO patch cable. Dopo aver sostituito il cavo, il ping è ripetuto e questa volta ha SUCCESSO.
Il problema è dunque risolto. L'ultimo step è documentare la soluzione del problema su un report degli errori, ed inviarlo di nuovo all'help desk in maniera tale che questo caso sia registrato e che risulti Risolto.

La tecnica di Divisione e Conquista si applica ai seguenti problemi: Due reti lavorano bene, se non sono connesse, ma quando si effettua una connesione, l'intera struttura smette di funzionare. Il primo step può essere, quello di Dividere la rete in due separati reti e verificare che esse operino correttamente, in questa nuova situazione. Se ciò genera dei dati positivi, si deve rimuovere tutte le connessioni subnet per uno dei router connessi, e riconnetterli ad altre reti che lavorano correttamente. Verificare che effettivamente essi funzionino correttamente.

Se la rete sta funzionando, si aggiunge ogni sottoretete step by step al collegamento sul router finchè non si verifica il problema. Rimuovere quindi l'ultima periferica che è stata connegata e vedere se la rete,in questo modo, funziiona.

Se la rete funziona normalmente, rimuovere questo host dal segmento di rete e sostituirlo con un altro. Dunque controllare ancora il funzionamento della rete. Quando si trova la perifeica "bacata", è necessario rimuoverla e verificare la rete torni al funzionamento normale.

Se la rete funziona normalmente, è necessario Isolare il componente che genera il problema. E' possibile effettuare il troubleshooting ad un host individuale, per trovare la causa per cui, a causa di esso, l'intera rete, crasha. SE non si trova un problema su questa periferica, si può pensare che questa periferica, possa subire un problema relativo alla comunicazione con un'altra,

sulla rete opposta. Dunque trovare l'altra periferica che si connetteva a questa .

Riconnettere l'host che ha causato il fallimento della rete, quindi disconnettere tutte le subnetworks dal router. Controllare se in questo modo la rete torna allo stato operativo originale. Se la rete funziona ancora, aggiunge le sbunetworks al router, finchè non si verifica il problema. Romuovere l'ultima subnet che è stata aggiunta prima che si verificasse il problema, e vedere sle arete torna allo stato normale. Se la rete funziona normalmente rmuovere l'host del segmento e sostituirlo con uno senza problemi. Guardare di nuovo se la rete ha problemi.

Se la rete a questo punto continua di nuovo a funzionare bene, è possibile di nuovo isolare le periferiche per poter effettuare un troubleshooting. Se non si trova niente si analizzano ambedue ed alla fine..Si scopre che eiste un conflitto. Risolvendo questo conflitto entrambi le stazioni possono essere riconnesse sulla rete che automaticamente tornerà a funzionare normalmente.

Strumenti Software: Per il processo descritto in precedenza **esistono del tools** che sono disponibili all'uso, da parte dell'amministratore di rete, per soluzioni di problemi relativi soprattutto alla connettività. Questi tool possono **aiutare il troubleshooting sulla LAN**, ma sono particolarmente utili in situazioni di troubleshooting su una WAN.
Adesso andremo a vedere i comandi **disponibili per un amministratore di rete**, nella maggior parte **dei package software**. Questi comandi solitamnete sono **Ping, Tracert (traceroute), Telnet, Netstat, Arp, IpConfig, e WinIPcfg**

Ping:
Si invia un ICMP echo packets per verificare le connessioni con l'host remoto.

Ping [**-t**] [**-a**] [**-n** ***count***] [**-l** ***length***] [**-f**] [**-i** ***ttl***] [**-r** ***count***] ***destination***

-t	ping until interrupted
-a	resolves host name and ping address
-n	***count*** limits number of echo packets sent
-l	***length*** specifies size of echo packets sent
-f	DO NOT FRAGMENT command sent to gateways
-i	***ttl*** sets the TTL field
-r	***count*** records the route of the outgoing and returning packets
destination	specifies the remote host to ping, by domain name or by IP address

Tracert:

Questa utility mostra la route del pacchetto, dalla sorgente alla destinazione..

Tracert [**-d**] [**-h** ***maximum_hops***] [**-j** ***host-list***] [**-w** ***timeout***] ***target_name***

-d	specifies IP addresses shouldn't be resolved to host names
-h	***maximum_hops*** limits the number of hops searched
-j	***host-list*** specifies the loose source route

-w	***timeout*** waits the number of milliseconds specified for each reply
target_name	***target_name*** specifies remote host tracing too, by domain name or by IP address

Telnet:

Si tratta di un programma di emulazione terminale che consente comandi interattivi sul server telnet. Fino a che la connessione non è statibila, nessun dato passerà. Se la connessione subisce un brak, il telnet ci informerà. Il Telnet è buono per il testing, esiste la possibilità di inserire parametri di configurazione login sull'host remoto.

	destination specifies remote host telnetting to, by domain name or IP address
Telnet *destination*	**Netstat** **Netstat** displays protocol statistics and current TCP/IP network connections. [5]

Netstat [**-a**] [**-e**] [**-n**] [**-s**] [**-p** ***proto***] [**-r**] [***interval***]

-a	Displays all connections and listening ports. (Server-side connections are normally not shown).
-e	Displays Ethernet statistics. This may be combined with the -s option.
-n	Displays addresses and port numbers in numerical form.
-p	Shows connections for the protocol specified by ***proto***; ***proto*** may be tcp or udp. If used with the -s option to display per-protocol statistics, ***proto*** may be tcp, udp, or ip.
-r	Displays the contents of the routing table.
-s	Displays per-protocol statistics. By default, statistics are shown for TCP, UDP and IP; the -p option may be used to specify a subset of the default.
interval	Redisplays selected statistics, pausing interval seconds between each display. Press CTRL+C to stop redisplaying statistics. If omitted, Netstat will print the current configuration information once.

Arp:

Arp è usata per filtrare indirizzi hardware di hosts locali e default gateway. L'arp cache può essere visualizzata e controllata per entries invalide o duplicate.

arp -a [***inet_addr***] [**-N** [***if_addr***]]
arp -d ***inet_addr*** [***if_addr***]
arp -s ***inet_addr ether_addr*** [***if_addr***]

-a or **-g**	displays the current contents of the arp cache
-d	deletes the entry specified by inet_addr
-s	adds a static entry to the cache
-N	displays the arp entries for the specified physical address
inet_addr	IP address, in dotted decimal format
if_addr	IP address whose cache should be modified
ether_addr	the MAC address in hex separated by hyphens

Ip Config o WinIPcfg:

Queste utility di windows visualizzano le informazioni relative all'addressing IP per la periferica di rete locale. (NIC)

IPconfig [**/all** | **/renew** [***adapter***] | **/release** [***adapter***]]

/all	all information about adapter(s)
/renew	renew DHCP lease information for all local adapters if none is named
/release	release DHCP lease information disabling TCP/IP on this ***adapter***

Spero ke questa guida ti sia piaciuta!! E non perderti la mia guida CCNP!! :-)

ESAME NETWORK IN INGLESE....APPUNTI!

Topologie di rete : Tipologia a Stella: In una tipologia a stella, tutte le periferiche sono connesse ad un punto centrale comune, tipiacmente esso è un hub o uno switch. Quando un nodo invia i dati alla locazione centrale, questa retrasmette l'informazione alla destinazione. Poiché tutti i cavi sono connessi ad una periferica centrale, se uno dei link fallisce, solo la sua porzione di rete va già. Il resto della rete non è affetto dal problema. Se il punto centrale fallisce, l'intera rete va bià. Una tipologia stella ha unmassimo di 1024 nodi, su lan. E si usa 10base-T (ieee 802.3) e 100base-tx (ieee 802.13) ethernet.
Un vantaggio della tipologia stella è l'affidabilità, la semplicità d'installazione ed il mantenimento. Il monitoring ed il troubleshooting, può essere affettuato in posizione centrale, con fcilità. Star topology permette grande affidibilità poiché ogni nodo è connesso alla periferica centrale da un segmento, se questo segmento fallisce, la connessione è persa solo ad un solo nodo. Il resto della rete è ok. Ogni nodo è connesso al punto centrale per cui anche il layout diventa facile. Lo svantaggio di questa tipologia è il costo. Per ogni periferica è richiesto molto cavo, più di quanto ne serva per ogni altra tipologia di rete. Bisogna poi considerare il costo relativo all'unità centrale.

Bus Topology:

A bus topology **connects multiple devices** onto one main cable and is sometimes referred to as a backbone, trunk, or segment. Terminators must be connected at each end of the topology to **absorb any reflected signals**. If coaxial cable is **used without terminators**, reflected signals will echo across the network, causing the entire network to be **unusable.**

One advantage of a bus topology is **ease of installation**. Because this topology uses a simple cable layout it can be **easier to implement** than other topologies. In the past it could also cost significantly less to install a bus topology. In the present day, these cost factors have been eliminated and it is often more expensive to purchase the required components.

A disadvantage is that **if a cable segment or the backbone breaks or fails, the network will fail**. Another disadvantage is **only one node can transmit data onto the network at a time**. If **two or more nodes attempt to send data at the same time, a collision will occur.** This **will require a recovery procedure** that will **slow down the network**. Once the **collision** has occurred, all the data must be **re-sent**. A process called

Carrier Sense Multiple Access/Collision Detection **(CSMA/CD) prevents the occurrence of another collision**. CSMA/CD is a process where each node waits its "turn" to retransmit data.

Mesh Topology [2]

Normally used for WANs, **a mesh topology connects all devices on the network** and provides a path to and from each device. Because all the devices are connected, the network **has a higher fault tolerance and greater reliability. If a cable segment breaks along the network, the devices will find the quickest way to reroute the packet to its destination**. Therefore, the data will almost always reach its destination.

Disadvantages of this topology are the cost and **the difficulty in management**. Because there are numerous connections to and from each device, there are a **large number of cabling runs**. This causes a mesh topology **to be somewhat expensive**. If a segment breaks on the network, the complex design can make finding the location quite difficult. In summary, maintaining the network can be time consuming and often outweighs the advantages of redundancy.

Ring Topology [3]

Ring topologies consist of **each device on the network being connected with two other devices**. There is **no beginning or end to the cable**. Instead this particular topology forms a complete ring. The devices on this network **use a transceiver to communicate with their neighbors**. Transceivers act like repeaters **to regenerate** each signal as it is passed through the device.

Advantages of this topology include **better performance** because each device receives a "turn" to transmit signals and, **each device has equal access to the network**. An additional advantage **is that the signal is regenerated by each device** it passes through, thereby preventing the signal from degrading.

A disadvantage of using this topology **is if one device on the cable fails, the entire network will also fail**. Locating the failure can sometimes be difficult. **Another disadvantage** is that **if any changes are made to the network**, including adding or moving devices, the disruption **will cause the network to fail**. [4]

In a star topology, **all devices are connected to a common central location**, typically a hub or a switch. When a **node sends data to the central location, the central device retransmits the information and sends it to the destination**. Because all cabling is connected to a central device, **if one link fails, only that portion of the network will fail**. The rest of the network will not be affected. However, if the central device fails, the entire network will also fail.

A **star topology can have a maximum of 1,024 nodes** on a LAN and is commonly used for 10BASE-T (IEEE 802.3) and 100BASE-TX (IEEE 802.12) Ethernet.

Advantages of star topologies include their **reliability**, along with simpler installation and maintenance. Monitoring and troubleshooting can be maintained at the central device providing **easier maintenance**. Star topologies allow for **greater reliability** because each node is connected to the central device by a segment. **If one segment breaks**, **only that node loses access to the network**, and the rest of the network is not affected. Because each node is connected to the central device, star topologies also allow for an **easy network layout**. This provides the network administrator with a simpler installation when compared to the other topologies.

A disadvantage of this topology is cost. With each device being connected to the central location, **more cabling is required** than with other topologies. In addition**, there is the cost of the central device to consider**.

Segmenti e Backbones:

Segments

In networking, the term "segment" has several meanings. First, in a narrow sense, **it can refer to a trunk** (main line) of cabling, which **connects devices to a concentration device**, such as a hub, MAU, or switch. Second, "segment" can also **refer to a logical grouping of devices**, which communicate within a given subnet separated ("segmented") by bridges, switches, or routers. The term "segment" may **also be synonymous with a collision and/or broadcast domain**. [1]

Backbones

The term "backbone" has several meanings within networking. First, a backbone is most often the main cable (or trunk) to which all nodes and devices connect. Second, **backbones are the foundations of both LANs and WANs where servers, routers, and concentrating devices** (such as switches and hubs) are connected by a **high bandwidth** connection. **Optical** fiber is now **more commonly chosen** for **backbone** cabling over **coaxial** cable and UTP. This is due to the fact that it is immune to most interference and grounding problems. [2]

Sistemi operativi di rete:

Microsoft Windows NT Server

An extremely popular local area network operating system is Microsoft Windows NT Server. This network operating system uses a **graphical user interface (GUI)** that looks very **similar** to that of the **other Windows desktops**. However, NT is designed with **different utilities to manage servers**. NT uses the **User Manager for Domains to administer domain users and group administration programs**, and allows administrators the option to choose from two file systems: New Technology File System (**NTFS**) or File Allocation Table (**FAT**).

Novell NetWare

Novell NetWare, also an **extremely popular** local area network operating system, is designed to support **LANs such as Ethernet and Token Ring networks**. To manage the resources available on the network, NetWare uses the **NetWare Directory Services (NDS)**, where both a physical and a logical file system are used to arrange files and data. NetWare's primary file system is a combination of **FAT** (File Allocation Table) and **DET** (Directory Entry Table). **Layer 3 protocols used by Netware are Internetwork** Package Exchange (**IPX**) and Internet Protocol (**IP**).

UNIX

Developed at the University of California, Berkeley, **UNIX was designed for database management**. UNIX is an important network operating system because its key features include **multitasking, multi-users, and networking capabilities**. UNIX has the **ability to operate multiple processes while users are working with applications on the same machine**. Multiple versions of UNIX exist. These include Sun Microsystems' Solaris, IBM's AIX, Silicon Graphics' IRIX, Linux, or Hewlett-Packard's HP-UX. The operation of all versions is similar.

Sistemi clients:

Windows NT

Windows NT has the ability to support and **effectively function with various network client and operating systems**, including MS-DOS, Windows 9x, Windows 3.11 for Workgroups, Windows NT workstation 4.0, OS/2, LAN Manager, Macintosh, NetWare, Intel, and UNIX. Windows NT Workstation is **best served by a Windows NT server** because of their common **NTFS file system and system management architecture**.

Windows 9x clients must have ***Client for Microsoft Networks*** **installed to connect to an NT server**. To connect to a NetWare server, Windows 9x clients must **use either the a*Microsoft Client for NetWare Networks*** **or *Novell Client*** *32*. There are two **disadvantages** when **a Windows client connects to a Novell** server using *Microsoft Client for Netware Networks*. First, the **TCP/IP protocol cannot be used to connect to a NetWare server causing slower access**, and, second, the *Microsoft* ***Client for NetWare Networks*** **cannot understand the directory service and security system for NetWare v4.0 and v5.0**. Novell Client 32 is called Client v3.3 for Windows 95/98. **Client 32** software provides the **Windows 9x clients connectivity to a NetWare server using either IPX/SPX or TCP/IP and provides full support for the NDS**.

Novell NetWare

Novell NetWare **works** well with **many operating systems** including DOS, Windows 3.11, Windows 9x, and the Windows NT workstation. Novell NetWare, prior to release 5.0, was mainly a text-based network operating system. The network administrator executed most functions from a client workstation that was logged onto the server although **several functions were administered directly from the server console**. NetWare 3.x primarily **used IPX/SPX** as its protocol, while the newer versions NetWare 4.x and 5.x **use TCP/IP or IPX/SPX as their protocols**. Similar to the Windows platforms, NetWare also uses GUI for its applications.

UNIX

UNIX is **a command line driven platform**, which is accessed by terminal sessions from other operating systems or on the same machine. **Windows 95 clients can access UNIX using terminal emulation programs**. UNIX clients, such as Sparc (Solaris) workstations from Sun Microsystems, work best with their manufacturer's proprietary NOS.

A recent relative of UNIX is LINUX, which was developed as **an open source operating system**. Developers who wish to modify the platform can purchase or download a copy of the source code and modify it based on their own needs.

Servizi directory di sistemi operativi:

Windows NT

In the past, with multiple servers Windows **NT required separate domains**. Users were **assigned a password to each domain**. To maintain all the passwords, the domain controller was created to **allow users to have one password and access** all the resources on all the servers.

The domain controller manages user access to the network and stores the security account information into **a common security database, called the Security Access Manager (SAM).** SAM **verifies passwords, enables users to store and secure information, and searches for information on the network**. When a user has successfully logged into the database, the domain controller issues the user an access token. Access tokens allow users to access any service without having to type in each password.

Novell NetWare

Novell NetWare 3.x relies **on a security database**, called the **Bindery,** which uses only **IPX/SPX**. NetWare 4.x and 5.x rely on **Novell Directory Services (NDS),** a built in **directory service** that uses **TCP/IP or IPX/SPX**. NDS is based on the Internet Directory Standard X.500, which uses a resource called the **NDS tree to organize all user and resource information**. The **NDS tree** allows users to **log into the network** and have the **ability to access any of the resources available.**

UNIX

The UNIX directory services use a file system called the **Network File System (NFS),** which is **similar to a DOS** file system. This NFS grants **users permission to certain parts of the file system and controls the security of the UNIX** systems. Because the shared files are transparent, NFS users are able to **view and edit files on other UNIX hosts**.

UNIX systems running **SAMBA have the ability to communicate using Server Message Block (SMB).** When UNIX **connects to the Windows Network with SMB**, Microsoft clients and servers view the UNIX system as if it were another Windows device. UNIX also uses DNS to resolve Application Layer names into logical network addresses.

Ip,IPX, Netbeui e le loro funzioni:

Internet Protocol (IP)

Internet Protocol (IP) is a **routable protocol** that works at the Network Layer of the OSI Model and the Internet layer of the TCP/IP Model. IP provides **packet delivery** and **addressing for source and destination**. Connectionless IP, working together with the connection-oriented TCP, are the de facto protocol standards of the Internet.

Because IP is a connectionless service, it is unreliable and does **not guarantee the delivery** of data or the order in which it was sent. TCP, the connection-oriented Layer 4 protocol, works with IP to provide **reliable and orderly delivery of packets**.

Internetwork Packet Exchange (IPX)

Internetwork Packet Exchange (IPX) is a **connectionless routable protocol**, which also works on the Network layer of the OSI Model. IPX is the network layer protocol **used by Novell Netware**.

IPX is very **efficient and scalable** with acceptable performance and a simple address scheme. It is capable of being used with Ethernet (1500 byte packet size) and Token Ring (4000 byte packet size) networks using the proper Network Interface Card (NIC) drivers. However, **IPX is largely being replaced by the IP protocol**.

NetBIOS Extended User Interface (NetBEUI)

NetBEUI, commonly used for **smaller LANs**, is a **non-routable protocol**. It operates on the **Network and Transport Layers of the OSI** model. Because NetBEUI is non-routable, it is **quick and easy to configure**. Configuration is minimal once NetBEUI is installed and bound to a network adapter. Because it is nonroutable, it **cannot participate in Internet communications and is limited in its usefulness and scalability**.

Mirroring, duplexing, striping:

RAID Overview

A technology called Redundant Array of Inexpensive Disks (RAID) was created to **minimize data loss when disk problems occur**. Each RAID level is defined by differences in **performance, reliability, and cost**.

Mirroring

RAID 1: **Disk Mirroring is a common way to back up data**. All information written to the **first drive** is also written to the **mirror drive**, making the two disk **drives identical**. A disk controller card **connects to both the drives** and writes the data **in parallel to each of them**. This single controller card creates a **single point of failure for disk mirroring.** An **advantage** of RAID 1 is **redundancy**. **Disadvantages** are cost and the amount of **disk space required**.

Duplexing

RAID 1: **Duplexing** provides **fault tolerance** for both data and disk controller. **Duplexing is disk mirroring with a separate controller for each drive**. With its second controller, duplexing has improved **fault tolerance over mirroring**, and it is much **faster than mirroring** since the data can be written to both drivers **at the same time**. The main **disadvantage** of duplexing is the **cost** of the second controller card.

Striping

RAID 2: Striping data is a process where the data is **spread out onto a number of disks**. A minimum of **three** hard disks are needed, with three or more different drives **sharing the data**. With more than one disk sharing the data, the process **makes the input/output (I/O) faster**. **Parity** is also an **option** with data striping. **Striping with parity works on RAID 5**, which provides **redundancy** by interweaving data onto several drives and has a distributed checksum for parity.

Volumes

Volumes are **logical drives** created on servers. Volumes can **span** one or **multiple physical hard drives**. Normally two volumes, a **system** volume and a **data** volume, are **used on servers**. The system volume holds all the operating system files that **allow the network to run**. The data volume holds all of the varieties of user data. Because of volumes more physical disks can be added without administrative work being done to reorganize the logical structure of the storage.

Tape Back Ups

One of the oldest and cheapest ways to store data is by using a **magnetic tape**. There are three types of magnetic tapes that can be used to store data, Quarter Inch Tape (**QIC**), Digital Audio Tape (**DAT**), and Digital Linear Tapes (**DLT**).

Quarter Inch Tape (**QIC**), is rarely used in **networks today**. It is used primarily in **smaller networks** and was one of the **first standards used for PC backups**. The earliest QIC had the ability to **hold up to 40 megabytes** of data. The most recent QIC has a capacity of up to **2 gigabytes**.

Digital Audio Tape **(DAT**), was originally used for audio and video. DAT provides digital recording for tape backups. **DAT uses a SCSI connection** and is used in **most medium sized networks and has a maximum capacity of 24** gigabytes.

Digital Linear Tapes (**DLT**), a more **popular form of tape backup**, has the **capacity of up to 80 gigabytes**. Although this **method is expensive**, it is very fast and reliable. **Like DAT, DLT uses a SCSI connection**.

Il modello OSI e le funzioni dei protocolli:

Application Layer 7

The application layer (the seventh layer) of the OSI Model provides **network services and is closest to the user**. Internet Explorer, Netscape Communicator, Eudora Pro, and other end-user application software are serviced by the application layer. This layer establishes communication between intended partners and synchronizes agreement on procedures for error recovery and control of data integrity.

The protocols, which function on this layer, are Server Message Block (**SMB**) and Network Control Program (**NCP**).

Services, which provide network access, include:

- Telnet and File Transfer Protocol (FTP)
- Trivial File Transfer Protocol (TFTP)
- Network File System (NFS)
- Simple Network Management Protocol (SNMP)
- Simple Mail Transfer Protocol (SMTP)
- Hyper Text Transfer Protocol (HTTP)

Devices that function up to this layer include hosts and gateways.

Presentation Layer 6

The presentation layer ensures that the **information that the application layer** of one system sends out is readable by the application layer of another system. If necessary, the presentation layer translates between multiple data formats by using a common format.

The presentation layer also provides **data encryption to ensure protection** as data journeys through the network. When the encrypted data is received, it is deencrypted and the **formatted message** is then passed to the Application Layer.

Protocols at the Presentation Layer include NCP. Data formats include the following:

- ASCII
- EBCDIC
- encrypted
- jpeg
- gif
- mpeg
- quicktime
- flash
- wav
- avi
- mp3

Devices functioning up to this layer include hosts and gateways.

Session Layer 5

The session layer **establishes, manages, terminates sessions between two communicating hosts**, and provides its services to the presentation layer. It **also synchronizes dialogue** between the two hosts and manages their data exchange. The session layer also offers provisions for **efficient data transfer, class of service, security authorization, and exception reporting of session layer, presentation layer, and application layer problems**.

Three types of dialogs used in the session layer are **simplex, half-duplex, and full-duplex**. A simplex dialog allows information to flow from one device to another without requiring a reply transmission.

Half-duplex, which is also known as a two-way alternate (**TWA) transmission**, allows data to flow in two directions from one device to another. In two-way alternate transmission each device cannot send a transmission until the previous signal has been completely received. When one device sends a transmission and requires the destination device to respond, the destination device must wait until the initial transmission is complete before it can send its response.

Full-duplex, which is also known as a two-way simultaneous (**TWS) transmission**, allows devices to send data to another device without having to wait until the wire is clear. When a device transmits a signal, the destination device does not have to wait until the signal is complete to send a reply to the source device. **Full-duplex enables two-way traffic to occur simultaneously during one communication session**. A telephone is an example of full-duplex.

Protocols include the following:

- Structured Query Language (SQL)
- Remote Procedure Call (RPC)
- X-Window System
- AppleTalk Session Protocol (ASP)
- Digital Network Architecture Session Control Protocol (DNA SCP)

Devices functioning up to this layer include hosts and gateways.

Transport Layer 4

The transport layer **segments data** on the sending host system **and reassembles the data into a data stream on the receiving host system**. The boundary between the session layer and the transport layer can be thought of as the boundary between media-layer protocols and host-layer protocols. Whereas the **application, presentation, and session layers are concerned with application issues**, **the lower three layers are concerned with data transport issues**.

The transport layer attempts to **provide a data transport service** that shields the upper layers from transport implementation details. Specifically, the main concern of the transport layer includes issues such as how reliable transport between two hosts is accomplished. In providing **communication service, the transport layer establishes, maintains, and properly terminates virtual circuits**. To provide reliable service, transport error detection and recovery as well as information flow controls are used.

When **the transport layer receives data from the upper layers, it breaks up the information into segments** (smaller pieces) to be sent through the lower levels of the OSI Model and then to the destination device.

Protocols used in this layer are:

- Package Exchange (SPX)
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- NetBIOS Extended User Interface (NetBEUI)

Services used at this layer use TCP to provide **connection-oriented communication** with error free delivery and **UDP to provide connectionless communications without guaranteed packet delivery** (unreliable delivery).

Devices functioning up to this layer include hosts and gateways.

Network Layer 3

The network layer is a **complex layer that provides connectivity and path selection between two host systems** that may be **geographically separated**. Layer 3 can be **remembered as addressing, path selection, routing, and switching**.

Protocols functioning on this layer include:

Routed Protocols

- IPX
- IP

Layer 3 Protocols

- Internet Control Message Protocol (ICMP)
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Routing Protocols Routing Information Protocol (RIP)
- Internet Gateway Routing Protocol (IGRP)
- Enhanced IGRP (EIGRP)
- Open Shortest Path First (OSPF)
- Exterior Gateway Protocol (EGP)
- Internet Group Management Protocol (IGMP)

Group with Routed Protocols but label as a Non-routable Protocols are:

- NetBEUI Group with Routed Protocols
- DecNET

Services include software and hardware addressing, packet **routing between hosts and networks**, resolution of hardware and software addresses, and reports of packet delivery.

Devices functioning up to this layer **include routers and brouters**.

Data Link Layer 2

The data link layer provides **reliable transit of data across a physical link**. In so doing, the data link layer is **concerned with physical** (as opposed to logical) addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. **Layer 2 can be remembered by frames and media access control**.

Ethernet CSMA/CD also operates on this layer to **determine which devices should transmit at a given time in order to avoid collisions**.

The NIC is also **responsible for CSMA/CD on Ethernet**. In the case where two or more devices attempt to transmit signals at the same time, **a collision will occur**. **CSMA/CD instructs the device to wait a given amount of time before transmitting** another signal to avoid another collision.

The data link layer is broken down into two sublayers by the 802 standards: **Logical Link Control (LLC**) and Media Access Control (MAC). The LLC sublayer (IEEE 802.2) establishes and **maintains communication with other devices and provides connectivity with servers** when data is being transferred. **LLC manages link control and defines service access points (SAPs).**

The MAC sublayer maintains **a table of physical addresses** of devices. Each device is assigned and **must have a unique MAC address** if the device is to participate on the network. For example, the MAC address is similar to the individual's physical residence address, which the post office uses to deliver snail mail.

Protocols used at this layer include **High Level Data Link Control (HDLC) for WAN connections**, including **synchronous and asynchronous** transmissions. The **LLC protocol (IEEE 802.2) provides flow control at this layer**.

Technologies which operate on this layer include more than 18 varieties of Ethernet (specified in the IEEE 802.3 and other standards), Token Ring (IEEE 802.5), and other LAN technologies which rely on frames. Communications with the NIC are also provided.

Devices functioning up to this layer include NICs, bridges, and switches. While routers and **brouters are classified as layer 3 devices, in order to perform their functions, they must operate on layer 1 and 2 as well**.

Physical Layer 1

The physical layer (Layer 1) defines **the electrical, mechanical, procedural, and functional specifications** for activating, maintaining, and deactivating the **physical link between end systems**. Characteristics such as **voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors**, and other, similar, attributes are defined by physical layer specifications.

The physical layer is responsible for **moving bits of data through physical media**. Data, in the form of **ones and zeros**, are turned into electrical signals, pulses of light, or wireless signals. These signals are placed on the copper cables, optical fibers, or emitted as wireless, using a NIC. When receiving data from the network, **the NIC turns the electrical signals, pulses of light or wireless signals back into ones and zeros** to be sent up the hierarchy of the OSI Model.

Protocols are the **cabling, signaling, and connection standards**. Services include **Ethernet, Token Ring, FDDI, and other LAN technologies**. Devices, which function at this layer are repeaters, multiport repeaters (also called hubs), media access units (MAUs), and transceivers (transmitter/receivers, for converting one signal type into another).

Cablaggi di categoria 3,5,fibra ottica,UTP e STP:

Coaxial Cable 1

Coaxial cable is braided-grounded strands of wire that provides some **shielding and noise immunity**. The installation and the termination of the cable itself **can be costly**. Coaxial cabling is known as **thicknet or thinnet** when used as media for Ethernet, in the older **LAN technology, ARCnet, and cable TV. It uses connectors called BNC** (Bayonet Nut Connector).

Cat 3 UTP and STP

Category 3 UTP and STP (Cat 3) are used for voice **(telephony) or data (up to 10 Mbps).** More commonly, **Cat 3 is used on networks for cable segments to workstations or printers**. Cat 3 is not recommended for data installations since its maximum bandwidth of 10Mbps is rapidly being exceeded by many LAN technologies.

Category 5 UTP and STP

Applications for Category 5 UTP and STP include **voice (telephony) or data (100 Mbps to 1000 Mbps).** Cat 5e is sometimes used as backbone cable where the **maximum distance is restricted to 100 meters in length**. It is currently **the most popular cabling for connecting workstations and horizontal cable runs** due to its low cost, high bandwidth, relative ease of installation, and ease of termination with RJ-45 connectors.

Fiber Optic 2

Fiber-optic cabling carries signals that have been converted from electrical to optical (pulses of light) form. It consists of the core, an extremely thin cylinder of glass or **optical quality plastic**, which is **surrounded** by a **second glass or plastic** layer called the **cladding**. The interface between the core and **cladding can trap light signals by a process called Total Internal Reflection (TIR**), resulting in the optical fiber acting as a light pipe. **Protective buffer and jackets materials are used to cover the cladding layer**. This type of cabling is **less frequently used** because it is somewhat **more expensiv**e; however, it is rapidly decreasing in both raw cost and installed cost.

Fiber optic cables are **not susceptible to interference, such as radio waves, fluorescent lighting, or any other source of electrical noise**. It is the common cable used for network **backbones** and can support up to 1000 stations, carrying signals **up to 2 km**. Fiber terminations include SC, ST, and a variety of proprietary connectors. Maximum data transfer rate is virtually limitless**: tens and hundreds of gigabits per second, limited only by the electronics on each end of the fiber**.

Unshielded Twisted Pair (UTP) 3

Unshielded Twisted Pair (**UTP) has four pairs of wires**. Each wire in a pair is **twisted around the other to prevent electromagnetic interference**. UTP cabling **uses RJ-45, RJ-11, RS-232, and RS-449 connectors**. Because it is less expensive and easier to install, **UTP is more popular than Shielded Twisted Pair (STP) or Coaxial Cabling**. Examplex of **UTP applications are telephone network**s, which use **RJ-11** connectors, and **10BASE-T** networks, which use **RJ-45 connectors**. UTP comes in the form of Cat 2, 3, 4, and 5 grades however, only Cat 5e is now recommended for any data applications. The **maximum length for UTP is 100 meters**, without using any kind of signal regeneration device. The **maximum data transfer rate is 1000 Mbps for Gigabit Ethernet**.

Shielded Twisted Pair (STP) 4

Shielded Twisted Pair (**STP**), **like UTP, also has four pairs of wires** with each wire in each pair twisted together. STP **is surrounded with a foil shield and copper braided around the wires**. This **shielding allows more protection** from external electromagnetic interference. Because of the shielding, the cable is physically **larger, more difficult to install and terminate**, and more **expensive than UTP**. Intended for electrically noisy environments, **STP uses RJ-45, RJ-11, RS-232, and RS-449 connectors**. Like UTP, STP also **comes in Cat 2, 3, 4, or 5 grades**. However, only Cat 5e is recommended for data applications. The maximum cable length with no signal regenerating device is **100 meters**. The maximum data transfer rate is **100 Mbps**.

Web Links

CompTIA Home/Net + Certification
Cisco Connection Online
Cisco Documentation
Search Cisco

Tipologie di Ethernet:

10BASE2

10BASE2 cabling systems, which is also referred to as **thinnet, thin wire, or coaxial, use coaxial cables**. The specifications for 10BASE2 require a **maximum of 30 nodes per segment spaced at least one half meter apart**. 10BASE2 cabling is commonly used for small networks because it is **inexpensive and easy to install**.

The **"10"**, in 10BASE2, represents rate of data transfer, in this case **10 Megabits** per second. "**Base**" refers to **the type of signaling**. This type of cabling system uses a baseband signal. The "**2**" indicates the **maximum distance of the cable**. In 10BASE2 the **"2" should refer to 200 however, the maximum unrepeated distance is actually 185 meters**. Therefore, this type of cabling system can transmit 10 Mbps, using baseband signaling, with a maximum distance of 185 meters.

10BASE5

10BASE5 cabling systems also **use coaxial cables**. These systems are often referred to has thicknet, "Yellow Cable" (because of the outer yellow coating), or "Frozen Yellow Garden Hose". 10BASE5 cabling can connect **up to 100 nodes, spaced at 2.5 meters apart**.

10BASE5 cabling systems can transmit at **10 Mbps**, using a **baseband signal**, and have a **maximum unrepeated distance of 500 meters per cable**. This type of cabling is also **expensive and is usually used in circumstances which require heavy cabling**. 10BASE2 and 10BASE5 cabling systems are normally used in **bus topologies**. However, this type of cabling is beginning to be used less often in structured cabling installations.

10BASE-T

10BASE-T cabling systems have become extremely **popular in LANs**. 10BASET is normally found in Ethernet star or extended star topologies where nodes are **connected to central hubs or switches using UTP cable**. This type of cabling system can carry **10 Mbps**, using a baseband signal, with a maximum unrepeated **distance of 100 meters**.

100BASE-T

100BASE-T is the generic name for Fast Ethernet which operates at **100 Mbps** using baseband signaling with a maximum **unrepeated distance of 100 meters**.

100BASE-TX and 100BASE-T4

100BASE-TX and 100BASE-T4 are two variations of 100BASE-T, which are specified by the IEEE. Both cabling types operate at 100 Mbps, use baseband signaling, and have a maximum unrepeated distance of 100 meters per cable. 100BASE-TX uses **Cat 5e UTP**, specifically two pairs of twisted wires, **with the ability to transmit 100 Mbps**. 100BASE-T4 uses **CAT 3** and all four pairs of twisted wires to transmit 100 Mbps. 100BASE-TX is by far the most popular copper version of fast Ethernet.

100BASEVG-AnyLAN

100BASEVG-AnyLAN was developed by Hewlett-Packard and is similar to 100BASEVG. 100BASEVG-AnyLAN has a transmission speed of **100 Mbps using baseband signaling, CAT 3, CAT 4, or Cat 5e UTP** cable for either Ethernet or Token Ring LANs. **The maximum unrepeated length is 250 meters**. The primary benefit of this technology is its **versatility**, including the cabling it uses and the type of LAN technology with which it can be used.

Duplexing, e Server:

Full and Half-Duplexing

The three terms used to describe how transmitters and receivers interact during communications are **simplex, half-duplex, and full-duplex**. In simplex communications, the **data travels only one way and no response** is needed or possible. An example of simplex is a school Public Address (PA) system. In **half-duplex communications, data travels from a transmitter to a receiver then from the receiver to the transmitter**. The transmission is never simultaneous. **Simultaneous** transmission and reception of data is **not possible in half-duplex**. Examples of half-duplex are **walkie-talkies and 10BASE-T Ethernet**. In **full-duplex** communications, both transmitter and receiver may **send and receive simultaneously**. Clearly this is the fastest way to communicate, but requires more sophisticated electronics. Examples of **full duplex are the telephone and switched 100BASE-TX** (Fast Ethernet).

WAN and LAN

A wide-area network (WAN) is **geographically unlimited**, while a **local-area network (LAN) is limited to a smaller region**. **WANs can span cities, countries, and multiple locations**. LANs are limited to a single building or school campuses.

LANs operate within a **limited** geographic area, such as a **single building**, connecting workstations, peripherals, and other devices on a single network. LANs provide a business with complete computer technology to share devices on a network.

WANs are geographically unlimited and vary in size, between **cities, states, or even globally**. WANs provide an efficient way to move information **from one network (a LAN) to another network**. [1][2]

Server, Workstation, and Host

Servers are typically powerful **computers that provide resources and services to other computers on a network**. Workstations (clients) are devices, which are capable of local processing of data. Workstations use resources and services provided by the server. Host is the special name given to any addressable computer system on a network running TCP/IP. Examples of hosts include **workstations, servers, minicomputers, mainframes, and even routers**.

Server-Based Networking and Peer-To-Peer Networking

Two types of networks are **Server-Based and Peer-to-Peer**. A **server-based** network, also **known as client/server,** connects **numerous hosts to a centralized computer**. This computer serves as a server, providing security functions and access to the network and resources, allowing for a central security system. As the network **grows** and the number of nodes increase, this type of network can **add specific servers** to address specific needs and resources. Examples include file and print servers, application server, domain controllers, and directory servers.

Client-Server networks require typically a powerful server computer running a network operating system, and administration by highly trained personnel. Advantages **of client-server networks include the variety of services that can be provided** and the central administration of those services. **Disadvantages include cost and complexity**.

In a **peer-to-peer network**, there is **no centralized server** or security system. Each node on the network **works as its own server,** granting permission to the other nodes on the network to access its resources. This type of **network is limited to approximately 10 nodes** connected to each other. Advantages include **simplicity, low cost, and ease of administration**, while disadvantages include **slow speed and a severely limited range of services** that can be provided.

Cable, NIC, and Router

In order to create a properly functioning network, the **main necessities required include cables, NICs, and routers**. A **cable is the physical media** used to wire networks. The cables that can be used to wire a network include unshielded and shielded twisted pair (UTP and STP), coaxial, fiber optic, or wireless (if no cables are required). These physical media are used in combination **with the network interface card (NIC**), which allows the computer to communicate with the network. Another way to look at the **NIC** is that **it allows the workstation Operating System (OS) to communicate with the local area network operating system (NOS**). A **router is a layer 3 device** which **performs best path selection and packet switching**, and is used to connect one or more Local Area Networks (LAN) together to create a Wide Area Network (WAN).

Broadband and Baseband

Two types of signaling are **Broadband and Baseband**. **Broadband** is an **analog signaling technique normally used in cable television**. This type of signaling can **carry video, voice, and data across a wire**. It **shares the medium's bandwidth over different channels**, often using different carrier frequencies. **One sharing technique is called frequency division multiplexing (FDM).**

Baseband is a digital signaling technique, which uses **the entire medium's bandwidth for a single channel at a time and allows very high throughputs** (the actual measured bandwidths are possible due to this single-channel-at-a-time technique). Signals **are in the form of voltage pulses on copper, light pulses on optical fiber, or electromagnetic waves in the atmosphere**. A form of multiplexor (**MUX**) device **is usually required so that multiple devices can take their turns using the medium**.

Gateway

A **gateway,** which **works as a translator**, provides **communication between different operating systems and frequently services the Internet**. A gateway must exist if two different types of operating systems, such as Windows and UNIX, are to communicate. In order to communicate with node on a different network over the Internet, the device must be connected to a LAN or a dial up connection.

Gateway also **refers to default gateway**, an IP address is used to **forward packets from one subnet to another subnet, if there is no other routing information available**.

Troubleshooting a livello fisico su un'interfaccia di rete:

After installing or replacing a NIC and experiencing problems accessing the network, it is important to troubleshoot the NIC and follow a logical troubleshooting methodology.

1. Determine which areas are affected. Identify what caused the problem: A protocol or a device.
2. Identify the differences of the affected areas and the unaffected areas.
3. Restart the affected hardware. Often the problem can be resolved if the hardware of the affected area is restarted.
4. Divide the network in half and segment the area.
5. Finally, if the problem can not be identified by any of these methods, specialized tools, diagnostic equipment, or information from technical databases may be necessary.

A form of technical diagnostics includes **testing called loopback testing**. Either an external loopback adapter or an internal device is attached to the NIC. Data is **sent from the NIC out and looped back in to verify if the data received is the same as the data**, which was sent out. Vendor supplied diagnostics programs are usually available through a vendor's webpage or technical support service.

The following questions are information that a network installer must understand to properly diagnose NIC card problems.

Question 1: What does the EPROM on a NIC do?

In the Erasable Programmable Read Only Memory (EPROM) on a network adapter allows the NIC to perform basic functions.

In a diskless workstation, commonly in larger networks, the **EPROM is often replaced by a PROM**. The code in the **PROM is unalterable and boots a workstation that has no hard disk or diskette**. This feature can be added to the NIC in order that the system can be enabled to boot using files stored on the network.

Question 2: What do jumpers on a NIC do?

Jumpers are **pieces of plastic and metal that connect two metal posts on a NIC** and are most commonly **used to change a NIC's configuration, mainly the IRQ and the I/O addresses**. Because NICs have multiple connection options, jumpers determine which transceiver needs to be used on the NIC, which transceiver to hook the cable to, and the data rate transfer setting.

Question 3: What does plug and play software (usually packaged with NICs) do?

Plug and Play works with the plug and play BIOS to configure expansion components on a system, such as a NIC and other devices. Plug and Play allows the user to have minimal, if any, configuration issues when installing a device.

Question 4: What are network card diagnostics, such as the loopback test and vendor-supplied diagnostics?

When troubleshooting a network, there are two **diagnostics** that can be used. First, there is the **loopback test**, which tests the **in-bound and out-bound communications of a NIC**. In an external loopback test, a signal is sent from the NIC, out through an adapter, then sent back into the NIC. The information is then verified to **determine if the information received is the same as what was sent out**. Internal loopback tests use the same idea; however, no external adapter is used.

The second method in troubleshooting a NIC is using vendor-supplied diagnostic programs. Normally, the manufacturers of a NIC will provide specific tests that can troubleshoot a NIC. There are generic diagnostics available. Usually, the vendor-supplied diagnostics tests are more reliable. These programs can be retrieved from either the vendor's technical support lines or webpages.

Question 5: What does it mean to resolve hardware resource conflicts, including IRQ, DMA, and I/O Base Address?

Because there are many devices in a personal computer, hardware conflicts may arise when one device tries to communicate to another within a computer. To avoid such conflicts, there are three main ways for devices to communicate to another within a computer.

Interrupt Request (IRQ) is a method, where a device can interrupt the processor and request a service. **In a PC there are 16 IRQ lines available and dedicated to devices**, such as disk controllers, serial, and parallel ports. **Some of the more common IRQs are IRQ 3 (for serial port COM port 2) and IRQ 5 or 10 (dedicated to NICs)**. In general, IRQs can not be assigned to more than one device at a time, or a conflict will occur.

Direct Memory Access (DMA) is a method used by devices to access computer memory without involving the CPU. **DMA is managed by the DMA controller chip**, which is generally **faster than the CPU**, and works as if the CPU had managed the transfer of memory itself.

I/O (input/output) Base Addresses allow the CPU access to each device in the computer. Each device is **assigned a unique I/O address that can not be shared**. If there is more than one device containing the same I/O address, neither device will be able to function properly. The **CPU will attempt to send information to the specified I/O address**; however, because two devices are assigned the same address, both will respond and the data will be corrupted.

Periferiche di livello 1:

Hubs

Hubs, which operate at **the physical layer** of the OSI Model, are central connection points for cabling in star topologies. Three types of hubs include passive, active, and intelligent.

A passive hub receives information through one of its ports, then transmits the data out **through another port to a destination location**. It has no electrical power and does not possess any signaling processing capability. **Passive hubs** only allow communication from one location to another to flow across the network, and they **absorb some signal energy, causing a signal to weaken**.

An **active hub** receives incoming signals through one of its ports**, regenerates and retimes the signals**, and sends them out the other ports to the destination. Active hubs are also known **as multi-port repeaters**. Most hubs **"share" bandwidth among users**. More users connected to the hub results in **less bandwidth per user**.

Intelligent hubs have even **more electronics than active hubs**. They can be **programmed to manage network traffic** ("managed" hubs) or perform switching ("switching hubs" or more commonly "switches").

MAUs

A Multistation Access Unit (MAU) allows **multiple workstations, which are connected on a Token Ring network, the ability to communicate with each other**. Although, MAUs are **not a UTP hub**, they are commonly referred to as a **token ring hub**. Often, this device has eight ports and uses Universal Data Connectors (UDC) or RJ-45 connections. MAUs are not powered devices; however, occasional lights will flash when connected to the network. **MAUs also add fault tolerance to ring networks.**

Switching Hubs

A switching hub, also called a **multi-port bridge**, is a device that automatically **verifies the MAC addresses of each device** connected to its ports. When a packet is sent to its network, the switching hub **checks the MAC address before sending the data to the specified location**. Unlike standard passive or active hubs, switching hubs **do not broadcast signals to each segment** on the network, but transmit data **only to a specific destination**. Switching Hubs (and switches) result in dedicated bandwidth per port; where as other hubs share the total bandwidth with the number of users.

Repeaters

When a repeater receives data from an Ethernet segment, **it decodes/codes the binary information**, and then **retransmits the signal to the destination**. **Advantages** of a repeater include; the ability to **extend the network a greater distance, increase the number of devices connected to the network**, added fault tolerance by isolating breaks on a network to only that cable segment, and the ability to link different cable types together. A **disadvantage** is that repeaters **enlarge collision domains**: If **two computers send packets at the same time**, **a collision** will occur and CSMA/CD is applied to the entire network, thereby slowing down the network.

A repeater **does not manage the flow of traffic**, it only repeats signals. A **maximum of four repeaters** can be installed on a single-segment Ethernet network.

Transceivers

A transceiver (transmitter-receiver) is a device which **transmits and receives data to and from the network**. This device **attaches to the network interface card (NIC) in two different ways: On-Board and External.**

An On-Board Transceiver is usually "on-board" or **attached to the adapter car**d, such **as RJ-45** receptacles and **BNC** connectors.

An External Transceiver makes a physical **connection to the NIC using a small device**, called an **adapter unit interface (AUI) or a Digital-Intel-Xerox (DIX)** connector, which is **attached by an extension cable**. A common external transceiver can also connect one side to an AUI interface and the other to an RJ-45 interface.

Bridges:

Bridges

Bridges are devices which **connect two different networks**, or network segments together and **filter traffic from each network**. The bridge **builds a table of physical (hardware) addresses**, learning the hosts, which exists on each of its ports. The bridge **examines the destination MAC address of each frame**; if the destination address is local (on the same bridge port, based on the bridging table), the frame is not sent. However, if the destination **MAC address is of a different bridge port from the source address**, the frame is forwarded to the non-local destinations. Bridges provide **connectivity with Layer 2 filtering**. Some bridges will connect networks **of differing LAN technologies** (like Ethernet to Token Ring). Since the bridge operates at layer 2, it forwards all upper level protocols.

Specifiche 802:

802.2 Logical Link Control (LLC)

802.2 is the IEEE standard, which defines the **LAN-technology-independent Logical Link Control (LLC).** LLC manages link control and **provides Service Access Points (SAPs)** through software. **LLC adds headers to encapsulated upper layer data to identify which protocols a given frame will carry**. It also provides communication **between the hardware Media Access Control sublayer** and the software implementations of Layer 3.

802.3 Ethernet

802.3 defines **Ethernet based** on a **modification of the original Digital-Intel-Xerox (DIX)** Ethernet standard. Specifically, this standard **defines the frame format to be used by a variety of specific media and topological** implementations of Ethernet. The 802.3 standard also defines the **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**, which is an algorithm for dealing with a situation where two signals collide on a network. CSMA/CD sets the amount of time **each device must wait to send a new frame.**

802.5 Token Ring

802.5 defines the **"passing" of the token around a network** in order to **allow each device to transmit** data **across physical star or logical ring networks**. A token is **created by the first node**, then passed along the network until another device **wants to transmit data and grabs the token**. The data will **flow along the network**, past each node, until the destination node sees it and grabs the information. **Once the data has been received, the destination device transmits a reply to the source device to indicate that the information was received**.

Funzioni e caratteristiche dell'indirizzo MAC:

A **MAC address is a unique address burned onto the memory of a network interface card (NIC**). Ethernet requires each computer to **have a MAC address**, and any computer **with a MAC address is called a node**. MAC addresses **use a 48-bit address**, which is a **unique identifier** for each device and is used for **delivering data to a specific location**. **MAC addresses** (layer 2 addresses, hardware addresses, physical addresses) are **crucial to the functioning of LANs**, allowing local delivery of frames and packets. A MAC address is similar to a social security number or personal identification number.

Il routing a livello Network:

If the **MAC address matches the address burned into the NIC card** the data link layer passes the data to the network layer. If the **MAC address is all 1s** (ones) the data is **also passed to the network layer**. When the network layer receives the packet, it uses the packet's network address to route beyond the local network. Routing allows the network layer **to transfer data packets across the internetwork, from a source to a destination**, and to **choose the most efficient best path to deliver the packet**. [1][2]

La differenza fra Router e Brouter:

Router

A router is a **Layer 3 device** that provides best path **selection and switching of data packets**. In order to **connect two different networks**, a router must be used. Routers **can be used to segment LANs**, creating smaller collision and broadcast domains. The most

important use **of routers is as the backbone devices of WANs**. Networks consisting of **routers, all of which can communicate using routing protocols**, can be built to allow very reliable and flexible delivery of data. **They make the Internet possible**.

Brouter

A **brouter** (Bridging Router) is a **combination of both a router and a bridge**: Acting as **a router for routable protocols and a bridge for non-routable protocols**. It allows the network to be able **to resolve almost all of its connection problems by using one device**; therefore, it **is very cost effective**. However, brouters are decreasing in prevalence. Their functions are being incorporated into separate categories of devices, **which are Layer 3 routers and Layer 2 switches**.

La differenza fra potocollo Routabili e non-routabili:

A **routable (routed) protocol can be delivered beyond a single LAN or WAN segment**; its packets can be routed. For routed protocols, a best path can be selected and the packet switched to the appropriate interface for that best path. **Non-routable protocols cannot leave the LAN on which they originate**. Routable (routed) protocols **include IP, IPX, and AppleTalk**. **NetBEUI** is an example of a **non-routable** protocol.

I concetti di default gateway e subnetworks:

The connection of a LAN to a WAN is **achieved through a router**; therefore, **LANs can be segmented by routers**. **The interface of a router, which resides on a LAN, is called the default gateway**. The default gateway **is the location where all non-local network traffic that has no specific route to a destination is sent**. The default gateway acts as an **entry and exit point of a subnetwork**.

When sending data to a remote subnetwork, the host sends the packet to the initial router specified as its default gateway. The router, receiving the packet, must determine whether the destination location is on one of its local networks or to send the data to another router for delivery.

La ragione per la costituzione di un unico ID di rete:

Each device, which participates on a network, must have a **unique id: A MAC address** (also known as layer 2 address, hardware address, **or physical address**). **MAC** addresses **can be easily identified** and maintained **for LANs up to a certain size**. However, the **addresses become unmanageable for large unsegmented LANs or WANs**. The **Layer 3** or network addressing scheme, which is hierarchical, was created because a **new addressing scheme was needed**. By requiring that **all networks connected to the router have their own network id number**, the router can refer to a group of hosts with one network layer (often IP) address. The router builds **tables of device hardware and network addresses** (typically MAC and IP addresses) and by which interface these **networks can be reached**. The router uses the **network id address to make efficient best path selection and switching decisions**.

La differenza fra routing Statico e Dinamico:

There are two **major types of routing processes, static and dynamic**. **Static** routing is programmed **by the network administrator to determine which path a packet must take to reach its destination**. The administrator must maintain (including any kind of changes, additions or deletions) the routes of each network routing device. Static paths are **not flexible** with changing network environments. Once the static routes are programmed, the determined paths for packets **do not change**, regardless of changing network conditions. Static routes are most often used for security reasons. [1]

Dynamic routing **allows the router to select which path a packet must take in order to reach its destination**. A router uses dynamic routing protocols such as Routing Information Protocol (**RIP**), Interior Gateway Routing Protocol (**IGRP**), Enhanced Interior Gateway Routing Protocol (**EIGRP**), or Open Shortest Path First (**OSPF**) to communicate with other routers. The router then determines **which path is the fastest way to transport data across an internetwork** (a network of networks). Using the **routing protocols, routers "talk"** to each other to update what paths are best to send data through, especially while network conditions are constantly changing. Without routing or its protocols, large networks, such as the Internet, would be impossible to maintain. [2]

La differenza di trasporto fra Connection-LESS e Connection-Oriented:

Connectionless communication is **a fast way to send information to a destination**; however, it **is not reliable** because there is no notification of receipt to the source location. Connectionless protocols include **IP and IPX** (Layer 3) and **UDP** (Layer 4). [1]

Connection-oriented protocols include TCP (Layer 4) **and SPX**. Connection-oriented protocols, such as TCP, typically **use an acknowledgement (ACK)** process between **source and destination**. If a source does **not receive an ACK from the destination, TCP will retransmit the segment until an ACK is received**. The processes of segmentation, handshaking/acknowledgement, **flow control, and error checking** are used to provide reliable transport. [2][3]

Risoluzione indirizzo:

Address resolution is important for **both local and remote delivery of data packets**. Typically, **Layer 2 hardware and Layer 3 network addresses must be resolved**. IP uses **ARP and IPX use SAP to resolve host Layer 3** ("abbreviations" of network addresses) to **MAC addresses**.

Default Gateways IP:

IP Datagrams (packets) use **default gateways as entry and exit points between subnets**. The subnet mask for the default gateway and the network on which it resides must be the same. A **default gateway is usually the computer or router that is connected to the local subnet and/or other networks**, which can determine **the best path for delivery to the destination network id**. Packets that are too large for the gateway are fragmented with three additional pieces of information: a **flag to indicate fragmentation** has occurred, a fragment ID number; and a fragment offset number for reassembling the fragments into the original packet.

DHCP, Wins e Files Host:

DHCP

The Dynamic Host Configuration Protocol (**DHCP**) automatically **distributes IP addresses** to devices which are connected to the network. When a client tries to connect to the network, a request is sent to the DHCP server for configuration settings. **Once the server receives the message, the DHCP server sends a reply to the client, which includes the configuration information, then keeps a record of the addresses that have been assigned**. DHCP uses the **BOOTP protocol** to communicate with clients. Clients must **renew their IP addresses after 50% of the address lease life, and again at 87.5% of the lease life, by sending a DHCPREQUEST message**. Client hosts keep their IP address until their lease expires or they send a DHCPRELEASE command. IPCONFIG and WINIPCFG are utilities run from the command line that allow verification of the IP Address information that has been assigned to the client host.

DNS

Domain Name Services (**DNS**) is a **name resolution service** that resolves (associates) **host names to IP addresses**. **DNS keeps a record of IP addresses and hosts names in a process called a domain**. DNS provides services along a hierarchical chain, with a database design similar to a **file tree structure (root-level/top-level/second-level/host name).** DNS also services **requests for host names that can not be resolved locally**. Large internetworks have **several levels of DNS servers** to provide efficient name resolution.

WINS

Windows Internet Naming Service (**WINS**) functions **like DNS to resolve IP addresses to host names**. However, there is a **difference between WINS and DNS**. **WINS uses a flat namespace using NETBIOS**, and **DNS uses a hierarchical namespace**. To resolve an IP address, a **WINS client host registers its NetBIOS and IP addresses** with the **WINS server**. Then the WINS client host **sends a name query request to the WINS server**, indicating that it desires to transmit to another host. If the desired IP address and host name are found in the server's WINS registry, then they will be sent to original WINS client host. **Requests made by WINS are routable**. **The WINS proxy agent is used for non-WINS clients such as UNIX hosts**; however, WINS does not provide support for Macintosh OS.

HOSTS Files

HOSTS file is a **statically configured host name to IP address translation**. This file is usable in all hosts' IP protocol stacks. If present it **will be referenced for name resolution** before an **external DNS search**. **LMHOST**S provides the **same services in a WINS environment** and is statically configured on Windows networking clients.

Tcp,Udp,Pop3, Sntp,Snmp, Ftp,Http e IP:

TCP

Transmission Control Protocol (**TCP**) is a **connection-oriented protocol**, which operates **on the transport layer** of the TCP/IP and OSI Models. TCP is the de facto standard of the Internet and provides **full-duplex data transmission**. When TCP receives data from the upper layers of the OSI Model, **it guarantees reliable delivery** to remote networks. TCP is **useful** for transmitting **large amounts of data reliably, but with the penalty of large ACK overhead consuming bandwidth**. [1]

UDP

User Datagram Protocol (**UDP**) is a **connectionless** protocol, which operates on the transport layer of the TCP/IP and OSI Models. Because UDP is an **unreliable delivery service**, it does **not require receiving protocols to acknowledge** the receipt of a packet. **An advantage UDP has over TCP is speed**. Because UDP does not concentrate on establishing a connection, it can transmit more information in a less time than TCP. Useful for transmitting **small amounts of data where reliability is less crucial**, UDP lacks the overhead caused by ACKs. [1]

POP3

Post Office Protocol Version 3 (**POP3**), which uses **TCP port 110**, is a mail protocol that is responsible for **holding email until delivery**. When an **SMTP server sends an email message to a POP3 server**, POP3 **holds onto to the message until a request is made** by the user to have the data delivered. Thus POP3 transfers mail files from a mail server to a mail client. [1]

SMTP

The Simple Mail Transfer Protocol (**SMTP**), which uses **TCP port 25**, allows users to be able to **send and receive email over the Internet**. It is the SMTP's **responsibility to make sure that the email is sent to the POP3 server**. [1]

SNMP

Simple Network Management Protocol (SNMP), which **uses TCP port 161**, allows **simple maintenance and remote monitoring of any device on a network**. Administrators are able to address issues, such as problems with a network card in a server, a program or service on the server, or a **device such as a hub or a router by using SNMP**.

Two approaches an administrator **can take when managing a network device using SNMP** are a **central management system and the management information base (MIB)**. The management system allows the administrator to **view performance and operation statistics** of the network devices, enabling remote network diagnostics. [2]

FTP

File Transfer Protocol (**FTP**) is a **fast, connection-oriented, error-free protocol and uses TCP ports 20 and 21**. FTP allows data to **be transferred between servers and clients**. In order for FTP to **connect to a remote server**, the IP address or host name must be provided. FTP must be able **to resolve host names to IP addresses in order to establish a connection.** [1]

HTTP

Hypertext Transfer Protocol (**HTTP**), which uses **TCP port 80**, allows clients to transfer documents written in Hypertext Markup Language (**HTML**) over the World Wide Web for display by a browser. It is the **universal display language of the Internet**. [1]

IP

Internet Protocol (**IP**) is a **routable (routed) connectionless protocol**, which **operates on the network layer** of the OSI and TCP/IP Models. IP is the de facto standard for the Internet and provides **packet delivery and addressing for source and destination**.

Because IP is a **connectionless delivery service**, it is **unreliable** and does not guarantee that the packets received will be in the order sent, if received at all. [1]

L'importanza di Tcp\IP:

TCP/IP is **the most used protocol suite to date**. Millions of hosts worldwide and most operating systems utilize this protocol. **TCP/IP is popular because it is flexible, compatible, and capable of performing well in both small and large network implementations**. Because of **historical reasons and the quality and versatility of its protocols**, TCP/IP is the de facto standard set of protocols for the Internet.

Dns:

The Internet Domain Name Server consists of a **root and subdomain**. The root represents the **upper-indexed pointers to other DNS servers**. For example, when a user, user@cisco.com tries to send an email to an international location, a student at the University of Cambridge in England, student@cam.au.uk, the DNS server **first contacts the subdomain server**, which is cisco.com. The DNS server sends the email to the subdomain. Once the subdomain, cisco.com, has been contacted, the email is then sent to the root, .com. The root will pass it along the other roots, to .uk, which stands for United Kingdom. The .uk root passes the email message down its hierarchy to its subdomain .au and then to .cam. Once .cam receives the data, the email message sits on the POP3 server until the mail is requested.

Indirizzi e Subnet Mask:

IP addresses are divided into classes to accommodate different **sizes of networks**. Depending on the type of IP address, the **first octets** (through the first, second, or third octets) are issued by ARIN or other national agencies. **The IP address has 3 parts**: **The network** field (assigned externally), the **subnetwork field** (created by the network administrator locally), and the **host field** (assigned locally). In order to create **more hierarchical networks with subnets**, the extended network prefix, also **known as the subnet mask**, which allows the **decoding of the IP address into its 3 parts** (network, subnetwork, host) is required.

The classes of IP addresses are as follows: **Class A** addresses begin with binary 0xxx xxxx in the first octet; that is, decimal 1 to 126 (0 and 127 are reserved for special test purposes). **Class B** addresses begin with binary 10xx xxxx in the first octet; that is, decimal 128 to 191. **Class C** addresses begin with binary 110x xxxx in the first octet; that is decimal 192 to 223.

Class A IP addresses are reserved for the **larger networks**. This range allows **Class A** IP addresses to have a possibility of **126 networks**, while each network has a capacity of more than **16 million unique hosts** using the default subnet mask. The default subnet mask for this class network is 255.0.0.0.

Class B IP addresses are reserved for **medium sized networks**. The range dedicated for Class B networks includes IP addresses from 128.0.0.0 to 191.255.0.0. The possibility of networks available for this subnet is a little **more than 16 thousand networks**, with each having the capacity of a few more than 65 **thousand unique hosts** using the default subnet mask. The default subnet mask for a Class B address is 255.255.0.0.

Class C IP addresses are dedicated for **small local networks**. Class C networks range from 192.0.1.0 to 223.255.255.0 with a capacity of **more than 2 million networks**, each with a capacity of **254 usable hosts** using the default subnet mask. The default subnet mask for a Class C address is 255.255.255.0.

Other classes, which are not as popular, are Classes D and E. Class D ranges from 224.0.0.0 to 239.255.255.255 and is used mainly for **multicasting to various amounts of hosts**. It has the potential of having more **than 268 million unique multicast groups**. **Class E, which are experimental** addresses blocked for future use, has a range of 240.0.0.0 to 247.255.255.255.

Various solutions to the problem of IP address depletion are being implemented, including:

- NAT (Network Address Translation) and Private Address
- VLSM (variable length subnet masking)
- CIDR (classless interdomain routing)
- IP v 6 (version 6 of IP with longer IP addresses, and hence far more to assign) [1]- [4]

Numeri di porta:

Each TCP/IP protocol has **at least one specifically designated port number** for the flow of network traffic between client and server. Note that the use of the word "ports" here refers to structures in software, not hardware interfaces. Port numbers **correspond to services to be provided for the upper layers**. Well known port numbers are normally assigned by TCP/IP on the server prior to connections; however, **these numbers can be changed.** Because **clients have the ability to dynamically log on to the server from any location, clients do not have assigned port numbers**. Common port numbers include HTTP (port 80), FTP (port 21), and SMTP (port 25). [1]- [4]

Proxy:

A proxy server is a type of **a "go-between" between the Internet** and the **users of a network**. If a client needs information from the Internet, **the proxy server searches for the destination and retrieves the information**. This provides for **higher security and faster service** because the client **does not directly connect to the destination**.

A **proxy** server is used for **a number of different reasons**. Proxy servers **enhance security by hiding the individual host address**. When a server receives the request, the server **will only see one address**, which is the address of the proxy server, and not the individual host. Because all requests are being made on one server, network traffic is less busy if more than one user requests the same location, enhancing performance. The proxy server copies the information that was downloaded from each of the addresses requested. When another host requests information from the same destination, the server sends out the cached version of that location.

Ip Address, DNS, Default Gateway, Wins, DHCP, Hostname e Internet Domain Name:

Normal configuration parameters for a workstation include**: IP address and subnet mask, DNS** setting, default **gateway and subnet mask**, IP Proxy, WINS, DHCP, host name, and Internet domain name.

IP Address and Subnet Mask

When assigning IP addresses, two important factors must be considered: the IP address **needs to be unique** and the IP address must be assigned a subnet mask. When a DHCP server assigns an IP address, it specifically assigns **unique addresses to each device**, not

duplicating any address. If manually assigning IP addresses, it is important no two devices have the same IP address.

Each address must also have a subnet mask to properly communicate with the network. The network and **host ids of an IP address are determined by the subnet mask**. Therefore, it is important that each IP address has a subnet mask.

DNS Setting

Domain Name Services (**DNS**) is a **name resolution service that resolves (associates) host names to IP addresses**. DNS keeps a record of IP addresses and host names in a process called a domain. DNS provides services along a hierarchical chain, with a database design similar to a file tree structure (root-level/top-level/second-level/host name). DNS also services requests for host names that can not be resolved locally. Large internetworks have several levels of DNS servers to provide efficient name resolution.

Default Gateway and Subnet Mask

The interface of a router, which resides on a LAN, is called the default gateway. The default gateway is the location where all non-local network traffic that has **no specific route to a destination is sent** and the default gateway acts as an entry and exit point of a subnetwork.

When sending data to a remote subnet, the host **sends the packet to the initial router** specified as its default gateway. The router receiving the packet must determine whether the destination location is on its local networks or to send the data to another router for delivery.

IP Proxy

A proxy server is a type of a **"go-between" between the Internet and the users of a network**. If a client needs information from the Internet, the proxy server searches for the destination and **retrieves the information**. This provides for **higher security** and **faster service** because the client does **not directly connect to the destination**.

WINS

Windows Internet Naming Service (**WINS**) works as DNS does to resolve IP addresses with host names. **WINS uses a flat namespace by using NetBEUI, instead of using a hierarchical one like DNS**. To resolve an IP address, WINS client **hosts registers its NetBIOS** and IP addresses **with the WINS server**, then the WINS client host sends a name query request to the WINS server, indicating that it desires to transmit to another host. If the desired IP address and host name are found in the server's WINS registry, then they will be sent to original WINS client host. Requests made by WINS are routable. The WINS proxy agent is used for non-WINS clients such as UNIX hosts. However, WINS does not provide support for Macintosh OS.

DHCP

The Dynamic Host Configuration Protocol (**DHCP**) automatically distributes IP address settings to devices, which are connected to the network, when DHCP Server clients log on. When a client tries to connect to network, a request is sent to the DHCP server for configuration settings. Once the server receives the message, the DHCP server sends a reply to the client, which **includes the configuration information, then keeps a record of the addresses that have been assigned**. DHCP uses the BOOTP protocol to communicate with clients. **Clients must renew their IP addresses after 50% of the address lease life, and again at 87.5% of the lease life, by sending a DHCPREQUEST message**. Client hosts keep their IP address until their lease expires or they send a DHCPRELEASE command. IPCONFIG and WINIPCFG are utilities run from the command line that allow verification of the IP Address information that has been assigned to the client host.

Host Name

A host name is **assigned by the network administrator to identify each device** on the network. By default, on Windows-based machines, host names are the names of the computers.

Internet Domain Name

The Internet Domain Name is **assigned by ARIN**, a company that **assigns all the domain names on the Internet**. The domain name consists of two parts, the hostname and the domain. In the address www.cisco.com, the www is the host name and the cisco.com is the domain. Combined together, www.cisco.com becomes a **fully qualified domain name (FQDN)**.

Utilizzare arp per l'ip Connectivity:

In TCP/IP, the **Address Resolution Protocol** (ARP) **is used to BIND** (associate) **the physical** (**MAC**) addresses **with specific logical** (IP) addresses. When a data packet is sent to a particular destination, ARP takes the addressing information and **matches it against the ARP cache for the appropriate MAC address**. If no matches are made, ARP sends out a broadcast message on the network looking for the particular destination. 1 2 A host will respond with the correct address and send a reply to ARP. The following shows some variations on the arp command.

Commands	**Action**
`arp –a`	To view a list of **all IP and MAC addresses.**
`arp –a –n` Example: arp -a -n 146.188.144.223	Filters the **display to show only the interface specified.**
`arp –s`	To **manually add entries**.
`arp –d`	To manually delete dynamically entered ARP cache.

If **duplicate IP addresses** appear in the ARP cache, a **Windows NT 4.0 TCP/IP stack is written and a new ARP broadcast is sent to each computer** affected by the ARP cache error. 3 4

Utilizzare Telnet per l'ip Connectivity:

Telnet, which **uses port 23**, allows **users to log into and execute text-based** commands when working on a remote server.

To use Telnet, the user needs to run Telnet.exe at the command prompt or from the Start Menu (**Start** > **Programs** > **Accessories** > **Telnet**. Then select **Connect** > **Remote System** until a dialog box appears.

In order to connect to a host, the client must be able to resolve the name to an IP address. The user must also specify the port to connect to (Telnet port 23) on the remote server. VT100 is the default terminal emulation used.

If a user is having problems logging onto a server, Telnet may still be functional. In this case, the user can log on using Telnet and administer the problems associated with the server. For example, if a Windows NT server crashes and displays a Blue Screen and the server allows for a remote administration card to be plugged in, the user is able to Telnet to this card and can determine the problem of the server and reboot it.

Utilitzzare NBTSTAT per l'ip connectivity:

NBTSTAT displays information **regarding NetBIOS names** and corresponding IP addresses, which have been **resolved by a host**. It is used to troubleshoot two computers **trying to connect via NetBIOS** over TCP/IP (NetBT) by **displaying the protocol statistics** and current connection with each remote host. Variations on the **`nbstat`** command are summarized in the table.

Utilizzo di TRACERT per L'ip Connectivity:

TRACERT is a command-line utility used **to trace the exact route the data packet** used to reach its destination. Using the Internet Control Message Protocol (**ICMP**), tracert **sends out echo packets to the destination**, which was the packet's original destination, to **determine the exact route**. Variations of the **`tracert`** command are shown in the table.

Command	**Action**
`tracert` or **`tracert`**	Displays the **exact route taken by the packet** to its destination.
`tracert -d`	To specify that **an IP address should not be resolved** to a hostname.
`tracert -d -h` Example: **`tracert -d -h 15 www.cisco.com`**	To list the **maximum number of hops in a search**.
`tracert -j`	Specifies the **loose source routing** to make the outbound datagram pass through the router and back.
`tracert -w`	Instructs the **amount of time to wait in milliseconds** before timing out.

An example of displaying hops from one location to another: **`tracert -d -h 15 www.asu.edu`**.

Utilizzo di NETSTAT per l'ip Connectivity:

NETSTAT is used to display the methods used by virtual circuits and network interfaces. **NETSTAT is available for troubleshooting specific TCP/IP** issues by displaying protocol statistics and current TCP/IP connections. This utility is **used to show the three-step handshake method** when establishing and disconnecting network sessions. [1]

NETSTAT displays a list of **protocol types**, **local addresses and port information, remote access and port information**, and current state.The information displayed also explains what **connections are open and in progress**. Variations of the **`netstat`** command are shown in the following:

Command	**Action**
`netstat -a`	Displays **connections and listening ports.**
`netstat -e`	Includes the number of **bytes received and sent**, discards and errors, and unknown protocols.
`netstat -s -p`	Displays **contents of routing table**. Allows

users to view the current routes and active sessions and addresses.

NETSTAT enables the user to **troubleshoot TCP/IP** based connections by monitoring TCP protocol activity (by using **`netstat -a`**). Error counts and Ethernet interfaces can also be monitored using **`netstat`**. 2

Utilizzo di Ipconfig e WinIpcfg:

IPCONFIG and **WINIPCFG displays the current TCP/IP configurations** on the local workstation and **enable the user to modify the DHCP address assigned for each interface**. IPCONFIG is used in Windows NT and WINIPCFG is **used for Windows 9x platforms**. This utility enables the user to **view the IP related settings, such as DNS and WINS servers**, and the network interface's physical address. Variations on the **`ipconfig`** command are shown in the table.

IPCONFIG/WINIPCFG Commands

Command	**Action**
`ipconfig /all` or **`winipcfg /all`** (for Win 9x)	Displays all IP configuration information
`ipconfig/renew` or **`winipcfg /renew`**	Renews the DHCP lease information, if none is named.
`ipconfig /release` or **`winipcfg /release`**	Releases the DHCP lease information and disables the TCP/IP on the adapter.

Utilizzo dell'ftp per Ip Connectivity:

File Transfer Protocol, which uses **ports 20 and 21, is a protocol designed to transfer data across a network. Variations** of the **`ftp`** command are shown in the table.

Options to Customize FTP for Specific Needs:

Command	**Action**
`ftp -v`	Suppresses any display server response.
`ftp -n`	Prevents automatic login.
`ftp -i`	Turns off interactive prompting during file transfer
`ftp -d`	Displays all ftp commands between the client and server for debugging.
`ftp -g`	Disables the gobbling capacity.
`ftp -s:` example: **`ftp -s:network.doc`**	Runs the text file containing specific ftp commands.
`ftp` example: **`ftp www.cisco.com`**	Connects to the host

Options to Customize FTP for Specific Needs:

In order to use FTP **to connect to an address or target machine**, like **Telnet, FTP must be able to resolve the host name to the IP address** of the destination machine in order to communicate. Once the **connection and login has been**

made, users can transfer files and manage directories.

Once connected with the remote computer, **commands to navigate around the server** include:

Commands	Action
`CD`	Change working directory.
`DELETE`	To delete files.
`LS`	To list current directory contents.
`BYE`	To end connection and log out.
`GET`	To download a file.
`PUT`	To upload a file.
`VERBOSE`	Turns verbose mode on and off.

A common use of **troubleshooting with FTP** is researching and downloading patches or fixes. For example, Microsoft provides an online FTP server, where patches, upgrades, and the like can be downloaded. Most vendors provide some type of FTP server for users to retrieve these utilities from.

Usare Ping per l'ip Connectivity:

Packet Interface **Groper (PING) is a basic TCP/IP troubleshooting tool**. PING is usually **the first step when troubleshooting the network to verify if a specific machine is active**. Using **ICMP, PING verifies connections between two servers** by sending echo packets to remote servers and listening for replies. Variations on the `ping` command are shown in Figures 1- 4.

La distinzione fra PPP e Slip:

Serial Line Internet Protocol (**SLIP) and Point-to-Point Protocol (PPP) allow users to log on remotely to a network using a device such as a modem** (a dial-up connection through an analog telephone line). Although it is available for Windows 95 and NT desktops, **SLIP was originally designed to connect UNIX platforms to a remote network**. SLIP was one of the first remote connectivity protocols. However, with new technology and better security, **SLIP is being replaced by PPP**.

PPP was designed to replace all the older technology SLIP. It **provides asynchronous and bit-oriented synchronous encapsulation, network protocol multiplexing, session negotiating, and data-compression negotiation**, while supporting protocols such as IPX/SPX, DECnet, and TCP/IP. **PPP uses the High-Level Data-Link Control (HDLC) protocol for data encapsulation during transmission and establishes and maintains connections using the Link Control Protocol (LCP).** Using the Network Control Protocol **(NCP**) with PPP, an administrator can run **different protocols simultaneously on the same line**.

Advantages of PPP over SLIP include the fact that **SLIP can only be used with TCP/IP**, while **PPP can use multi-network protocols** and can use these protocols **simultaneously** during one session**. PPP also uses DHCP to resolve IP addresses with the serve**r, and can handle a **faster speed connection than SLIP**. **PPP** supports **data compression and IP address negotiation**, neither of which SLIP does.

La funzione di PPTP:

Point-to-Point **Tunneling** Protocol (**PPTP**) has **functions similar to that of PPP**. However, it **provides a secure transmission of data from the remote server**. In order to use PPTP, the **PPTP enabled client must dial into a PPP server and gain access to the remote server**. When the connection is established between the PPP and PPTP servers, the **PPTP server creates a connection with the client through a process called tunneling**. When a remote client sends a transmission, the transmission goes **through the PPP server, is encrypted** and then sent **through the tunnel to the PPTP server**. The PPTP server **receives the transmission, de-encrypts it**, and **directs it to the appropriate host**. These features of PPTP **make secure connections possible across the Internet**. PPTP **facilitates the transfer of sensitive data**: a user can **log onto an ISP, use the ISP as a gateway**, and then log securely into an office network.

ISDN e PSTN:

The Public Switched Telephone Network (**PSTN**) was originally designed to **carry analog voice signals across telephone lines**. A technology called Integrated Services Digital Network (I**SDN**) was created to **convert analog signals into digital signals to allow data transfer rates faster than PSTN**.

An **advantage of ISDN** over PSTN is **speed**. The **fastest connection** a modem can establish using a PSTN analog line is 56 Kbps. Data is converted by the modem from the PC's digital signals to analog signals, then sent across the wires to a remote network, where the data is again converted from analog signals to digital signals. **ISDN enables digital signals to travel over regular telephone lines in digital form**. Data is **transmitted in half the time of analog modems**. An ISDN **BRI line can carry data at 128 Kbps**, and ISDN BRI lines can be aggregated to create an ISDN **PRI line to carry 1.544 Mbps(T1) or 2.048 Mbps(E1).** Another advantage of ISDN over PSTN **is the ability to be connected to the network "all the time" without tying up the analog telephone line**, which is especially useful for telecommuters.

Porte seriali, IRQ, IO ADDRESS:

In order for dial up modems to work properly with the dial-up network the parameters, such as serial ports, **IRQs, and I/O addresses must be configured properly**. Modems (Modulators/Demodulators) **use a serial port for connection** and attempt to **use COM1 by default**. The **EIA/TIA 232 serial standards determine how to connect a modem to a computer**.

Serial ports, which **are based on DB-**9 (**nine pins**) or **DB-25** (**25 pins**) connectors, **are commonly known as COM1**, **COM2, COM3, and COM4** ports. Data terminal equipment **(DTE) represents the computer** side of the connection, while the data circuit**-terminating equipment (DCE) represent the modem connection**. Modems should be set properly. Depending on the serial port, modem set up can be done through the Start > Settings > Control Panel > Modems.

Interrupt Request Levels (IRQs) **provide a device a way to send interrupt signals to a computer**. Given that in many cases, multiple devices **may attempt to transfer data into a CPU simultaneously**, it is necessary to **assign a different IRQ to each individual device**. An input/output (I/O) address, a four digit hexadecimal number, **enables the flow of data within the computer**. Addresses are used to **select the information to be accessed in memory or peripherals**.

The **maximum port speed is the speed a modem can support in kilobits per second**. An analog line, also known as a **regular telephone line**, can support **speeds up to 56 kilobits** per second using an analog modem.

The requirements for remote connection include:

- The user must have **a valid ID and password** in order to **access the network remotely**. This includes accounts with **PPP, SLIP, or RAS**.
- A remote server must be available to be accessed.
- The **appropriate hardware device, such as a modem or ISDN line must be enabled** in order to communicate with the server.
- Network **protocols must be configured** in order to access the remote server or network

I Requisiti per una connessione Remota:

The requirements for remote connection include:

- The user must have a **valid ID and password** in order to access the network remotely. This includes accounts with PPP, SLIP, or RAS.
- A remote server must **be available to be accessed**.
- The appropriate hardware device, such as a modem or ISDN line **must be enabled in order to communicate with the server**.

- Network protocols **must be configured** in order to access the remote server or network.

Selezione di un modello di sicurezza:

There are **two types of network security** for protecting the **network: share-level security and user-level security**. Said to be weak and **difficult to manage**, **share-level security allows users to access certain information if assigned a password by the network administrator**. In order for an individual to access information on the network, he or she **must provide a password**, which is specifically **assigned by a network administrator**.

User-level security **specifies the rights and privileges of each user**. The network administrator **assigns the user an account to access a specific computer or network**. When an individual attempts to log onto the network, the computer matches **the user account id and password**(s) against the security database before providing the user access.

L'utilizzo di pratiche standard per la gestione Password e Procedure:

In both **share-level** or **user-level security models**, **passwords** are given to the user for **access** to the network or **specific data**. Passwords should always be kept secure and never written down where unauthorized users may be able to stumble upon them.

Passwords should not be:

- The log on, **first, or last name of the user** (or the names reversed).
- A familiar name, a spouse, child, pet, or relative.
- Easily attainable information, **such as personal information**.

- A word found in any **language dictionary**.
- A group of **single digits or letters**. For instance: AAAAA or 11111.

Passwords should be:

- Between six and eight characters in length.
- Include non-alphanumeric characters
- Be set to expire periodically, ideally once every 30 days.

Encryption:

Data encryption **provides the secure delivery of information being** sent over the internetwork. It takes the information, **which is written in plain text**, and **codes it into a text called ciphertext**. Ciphertext **resembles nothing, making the information unreadable**. When the data is received, it is **decrypted from ciphertext and converted back into its original text**.

Utilizzo di un Firewall:

A firewall is used to **protect the internal network** from the public and insecure Internet. **Firewalls** may be implemented using **hardware or software**. A software firewall is a set of programs on the gateway, which **monitors all traffic** flowing in and out of a network and is **often implemented using specifically configured routers**. All information must go through the firewall and be verified against a **specific set of rules**. If the information **does not meet the specified rules**, the data is bounced back and cannot continue until it meets the set standards. An example of hardware firewall is using specially configured routers to control inbound and outbound traffic.

Test Amministrativi di Account:

Before installing a network, a network administrator must consider the following:

- The configurations of the network
- Physical location
- Topologies
- Physical structure of the network
- Administrative duties (including administrative and test accounts)
- Passwords
- IP addressing
- IP configuration
- Connectivity requirements
- Software

Administrative **accounts allow the administrator to have unrestricted access** to all the information and **security** on the network. These accounts should only be created for individuals whose job requires the need for **unrestricted access**, and they should be **restricted to exercise these privileges only for administrative** duties. Because the role of the administrator is to protect all the data on the network, this account should be sensitive and have a strong password, which must be difficult to break.

Once an administrator uses his or her administrative account to make changes on the network, a test account should be used to test and verify the changes. Test accounts are similar to that of a normal user account, resembling other user accounts and privileges.

Both administrative and test accounts need to have passwords. **Passwords are a form of computer security**, which enables **privileged users to access network information**. A strong password, which should be used for administrative accounts, is a password that is difficult to "crack" by hackers. **Some hackers use what is called the "brute force" attack, which uses dictionary files against a user's account**. It is important to use a password that is an uncommon word **not found in any dictionary**, consists of at least eight characters in length, and a combination of numbers and letters.

Administrators must also consider IP configurations and **standard operating procedures (SOPs**) when **building their networks**. IPCONFIG is a Windows utility used **to determine TCP/IP settings**. This utility verifies IP addresses, default gateways, subnet masks, DNS, and other IP related settings. IP configurations are normally determined by the desktop used.

Although most networks have different names, they use similar standard operating procedures, which is a baseline of the resources in day-to-day operation. **SOPs may include backing up data on the network at the end of each day or each evening, having backup information in case the network goes down, or monitoring performanc**e. To monitor performance, a tool called the "sniffer" may be used to monitor the amount of network traffic on the network. A "sniffer" is also used to analyze network traffic and provide solutions to problems effecting the infrastructure of the network.

Fattori di environment:

Environmental factors should be considered when maintaining or creating a network. Computers and networking devices can easily be affected by extreme situations**, such as temperature, moisture, vibrations**, and electrical interference. If exposed to these situations, computers and networking devices may act irregularly and may sometimes **fail.**

Room conditions should be at normal humidity and temperature to prevent electrostatic discharge (ESD) and overheating. Fluorescent lighting, space heaters, televisions, radios, and other electrical devices may contribute to electromagnetic interference (EMI), especially when copper cabling is the primary networking medium. Often cooler and darker places, such as a basement, are an ideal area to store computer equipment.

Porte, connessioni SCSI ed apparati:

Common Peripheral Ports

Common peripheral ports include the serial and parallel ports. Serial ports, often used for the workstation **mouse or keyboard, and referred to as slow ports because data can flow in only one direction**.

Parallel ports are used for devices which are **quicker and connect outside of the workstation**. Data can be **transmitted in both directions**, making the connection **faster.** A printer for example connects to a parallel cable and port to speed up printing processes.

Data Bus connectors **(DB Connectors**) are a "D" shaped connector used to **connect serial and parallel cables to the computer.** DB connectors are usually referred to with as DB-x, **x representing the number of wires**. DB-9, DB-15, and DB-25 are most commonly used.

External SCSI Connections

Small Computer Standard Interface (SCSI) adaptors installed on workstations, **connect to and communicate with peripheral hardware**, such as CD-ROMs, disk drives, or scanners. SCSI **provides faster data transmission** than the parallel port, is used for high-performance systems, and has the capability to chain together up to **7 or 15 devices**.

Print Server

There **are two types** of print servers, **dedicated and non-dedicated**. Both types receive requests from end-users and direct the requests to a printer pool. **A print server is secure because it has no client access into the network**. **The difference between dedicated and non-dedicated print servers is dedicated is only used as a print server, while non-dedicated will also have some other network server functions.**

Hubs

Using either twisted-pair or coaxial cabling, **hubs connect a number of computers and devices together**. Hubs can be used to strengthen signals **in situations where cable distances need to be extended**. Hubs are normally **used for star topologies**, where each cable segment is connected to the hub. [1][2]

Routers

Routers, which operate on the **third layer** of the OSI Model, route data packets to a destination based on the routing address provided by the data packets. Routers are responsible for addressing and translating logical addresses into the physical address of a packet. [3][4]

Routers are either **statically or dynamically configured** devices and are **normally connected in a mesh topology with other routers**. Statically configured routers have determined fixed routers to other networks which are **manually entered by the administrator. Dynamically** configured routers have the **ability to communicate with other routers to determine the best path to route a packet by a variety of protocols, including RIP, IGRP, EIGRP, and OSPF.**

Brouters

A brouter is a device, which functions as a **bridge and a router**. If a brouter **receives a packet, it must determine the IP address**. If the IP address is not connected to any of its ports, it must route the packet to another location. However, **if it receives a packet with an IP address connected to one of its ports, the brouter acts as a bridge** and delivers the packet to its destination.

Bridges

Bridges are devices that **connect two different networks, or network segments**, together and filter traffic from each network. The bridge **builds a table of physical (hardware) addresses**, **learning the hosts**, which exists on each of its ports. The bridge **examines the destination MAC address of each frame**; **if the destination address is local (on the same bridge port, based on the bridging table), the frame is not sent**. However, **if the destination MAC address is of a different bridge port from the source address, the frame is forwarded to the non-local destinations**. Bridges provide connectivity with Layer 2 filtering. Some bridges will connect networks of differing LAN technologies (like Ethernet to Token Ring). Since the bridge operates at layer 2, it forwards all upper level protocols. [5]- [11]

Patch Panels

Patch panels, which are an **integral part of structured cabling installations**, consist of a row **of female connectors** (or ports) where every cable from different work areas connects directly to the back of the patch panel. They provide support for a UTP, STP, fiber ports, and various CAT ratings of UTP cabling. [12]

UPS

Uninterruptible Power Supply (UPS) **provides protection from spikes and sags** that may come over the electrical wires. While the server is plugged in, the **battery charger constantly charges the battery**. In case of a power outage, the fully charged battery will provide operations to continue or provide enough time for the server to shut down properly. [13]

NIC

Network Interface Cards (NICs) **allow the communication between a computer and the network**, providing a physical connection. In order for the computer to interact with the NIC, the computer must have the proper drivers installed. Each NIC is assigned a **unique address called the MAC address**. This address is also the physical address and is burned onto the NIC by its manufacturer. No two MAC addresses are or can be alike. [14]

Token Ring Media Filters

A token ring media filter is a **passive device**, which is used to **convert output signals from a token ring NIC, so that it may be compatible with different media types**, such as STP cable or different terminations, such as a DB-9 connector. Media filters are also designed to **eliminate unwanted high frequency emissions** and adjust inputs when using **UTP cable**.

Installare un modem analogico su jack digitale:

The technologies of an analog and a digital jack are very different and are not compliant. **Analog modems use a standard phone line to gain remote access**. A **digital jack is reserved to be used with an ISDN line** or PBX switch. A NIC or a transceiver can burn out if it is exposed to the voltages of an analog phone line. Likewise**, an analog modem can be damaged if it is plugged into a digital jack**.

Utilizzo di connettori RJ45:

Registered Jack (RJ) connectors were previously **the standard for telephone connectors**. More recently, RJs have been used to connect not only the telephones, but also 10BASE-T, 100BASE-TX, and Token Rings.

Telephone lines use RJ-11 connections consisting of four wires (2 pair). Analong modems connect to the telephone line using RJ-11 connectors. RJ-12, which is rarely used, is a six-wire version of the RJ-11 used for more complex telephone systems.

RJ-45 connectors have eight wires and are used for network technologies, which require **four pairs of wires**, such as Ethernet and Token Ring networks. RJ-45 connectors are specifically **designed for digital signals**. If an analog modem uses a RJ-45 connector, either the connection will not function or the analog modem will stop functioning and burn out. RJ-45 connectors are **primarily used to connect twisted pair cable to network devices**. These devices could connect to another media type, such as 10Base2 using using a BNC connector. [1] [2]

Cablaggi e lunghezza cavi su segmento:

Patch cables are typically **three meters in length** and often used for either connecting two MAUs (in a token ring topology) together or connecting two Ethernet hubs together. Patch cables are also used to "patch" a system with a NIC to the digital jack on either a cube wall or floor mount. The TIA/EIA-568-A standards govern horizontal cable installations**. For Cat 5e UTP, the distance limitation is 100 meters**, of which **3 meters are designated for workstation patch cables, 90 meters for horizontal cable runs (from the outlet to the Horizontal Cross Connect, or HCC), and 6 meters for patch cables/jumper cables** within the HCC.

Documentazione:

Test documentation normally **is included with the software during packaging**. Vendor patches, fixes, and upgrades usually occur after the product has been **purchased**. Vendors provide **patches and updates** of their products when bugs are found in their software or to make their software run more efficiently. In the case where a bug is found in an earlier release, patches are provided to fix the bugs. The most current patch or fix is likely to be found on a vendor's web page. Normally, a search feature or online support guide on the vendor's web page is available to easily navigate the site to locate the specific patch needed.

Software upgrades are designed to improve and make current software more powerful. Normally, upgrades are free (or can be purchased for a fee) and can be downloaded from a vendor's webpage in the same way as a patch would be downloaded. However, a backup should be made before installation to prevent loss of data.

Without anti-virus software installed on the servers and workstations, no modern network will continue working efficiently. Depending on user requirements, a wide variety of anti-viral packages are available. Updating virus signatures needs to be an ongoing network maintenance strategy. New viruses are spawned frequently and anti-virus software can become useless in a few months if updates are not performed.

Standard Backup procedure:

Each administrator, maintaining a network, should have a **standard backup procedure**, which should be implemented **nightly**. Backup procedures **should include tape drives, tape automation, and full, incremental, and differential back ups**.

DAT and DLT are the **two standard** types of tape drives. Digital Audio Tape (**DAT**) provides a **complete digital recording method**, which was originally used to **record audio and video**. DAT has a **capacity of 24 gigabytes**, uses a **SCSI** connection, and is mostly used for medium sized networks.

Digital Linear Tapes (**DLT**) have a capacity of **up to 80 gigabytes** and is becoming the more popular method of the three backup standards. Although this method is expensive, it is very fast and reliable. Like DAT, DLT uses a SCSI connection as well.

Tape automation is a **scheduled routine backup**, where a tape backup is scheduled with an average of **20-25 tape rotations**. The most common tape backup procedure is the **21-day tape rotation**, scheduled four days per week. Some rotations are **scheduled 5 days per**

week. Storing backup tape offsite is also a good idea in case of a major catastrophe, which will ruin the backed up information.

There are three different types of backups: **Full, incremental, and differential. Full back** up is the process where all **the information is backed up**. Most companies perform **full backups** everyday; however, this process requires the most tape out of the three backup processes.

Incremental backups back up files, which have been changed **since the last incremental or full backup was performed**. This process is **less time consuming and uses the least amount of tape**. In case the data needs to be restored, the last full backup and every incremental tape afterwards would be needed.

Differential backup is a process in which **those files are backed up which were changed since that last full backup was performed.** This type of backup process takes less tape than a full backup and when restoring the information, only two tapes are required; the last full and differential backup tapes.

It is important to patch the software running on the client workstation and the server itself. There are always existing software on the client that will not be on the server, and vice versa. If software is upgraded or patched on a server and not on a workstation, problems may occur when users try to access the software with a different version.

Installare software ANTI-Virus:

Because traffic flows from network to network via the Internet, there is a larger chance of a virus coming over the Internet and onto the network. To prevent a virus from destroying a system or a network, it is important to install anti-virus software on the servers and workstations. Anti-virus software scans files entering the network (incoming files) and scans files as they are accessed from the network (outgoing files). Without anti-virus software installed on the servers and workstations, no modern network will continue working efficiently and can be vulnerable to virus attacks and damages.

It is important to frequently **update virus signatures**, which are used by the virus scanning software when eliminating viruses. These signature files are updated by the vendor and either mailed to or available on the vendor's web page for the user. An ongoing **network maintenance strategy** should be to update virus signatures frequently. Because new viruses are developed daily, within a few months, what was effective anti-virus software can become useless.

Approccio di Troubleshooting:

An example of a troubleshooting approach involves the following four steps:

1. Determine **if the problem exists across the network**. Is the problem across the network or in a portion of the network? Identifying the scale of the problem will determine how many users are affected and may provide clues to what caused (or is causing) the problem.
2. Attempt to **isolate the problem**. Is one workstation not functioning; is that client able to connect to the network? Is the entire workgroup not functioning? Are any of the devices able to print? Is the problem affecting the entire LAN? Is the problem affecting

one Ethernet segment? Is it a WAN problem, or a problem with the LAN-WAN connection? Do the clients have Internet access?

3. Determine **if the problem is consistent**. Is the problem continuous and not intermittent? In other words, is the problem constantly present, instead of occurring periodically or randomly? And can the problem be replicated: given the same conditions on the same machine or another, the same errors are present? This information will help determine what may be causing the problems on the network.
4. Finally, **determine if the problems can be resolved by using tools**. A set of standard tools for maintaining networks should be available. These tools include hardware tools (such as cable testers), software tools (such as protocol analyzers), workstation and server commands, software, and utilities,web-based and text-based hardware and software manuals, and diagnostics that come with various network components, such as servers, NICs, hubs, switches, and routers.

Un poblema può essere attribuito all'operatore o al sistema:

In order to troubleshoot the network for operator or system problems, first identify the issue. Is the problem protocol-based or a network issue? Second, identify what parts of the network are affected and determine if problem exists on the cabling or the workstations.

When identifying the exact issue, begin with a broad view (for example, the entire network) and as the research is conducted, the problem should become more isolated. When dealing with network problems, recreating the problem can provide assistance in learning the events that have occurred during the error. If the problem is complex and is possible to occur in the future, recreating the problem may be beneficial to the troubleshooter for future reference. However, if the problem is simply to replace a NIC or a piece of hardware, recreating the problem may not be necessary.

Isolating the cause of the problem has two benefits. (1) If the problem is isolated to a specific area or number of users, then the rest of the network can continue to be functional. (2) By isolating the issue, it is easier to diagnose the problem between three to five workstations than it is on 500 workstations.

After identifying the problem, correcting the problem may be even more complicated. There may also be more than one way to fix the problem. First, determine the various methods to correct the problem; sometimes a problem can be temporarily patched or a software patch can also provide a temporary fix. There is also a possibility that when the problem is fixed, another problem will arise because of the fix.

Proper documentation (journals, equipment logs) and feedback, such as methods used to contain the problem and additional comments, can be helpful should the problem arise in the future.

Un secondo metodo per capire se il problema dipende del sistema operativo:

After correcting or temporarily patching the problem, another method that should be considered is to have another operator recreate the problem and test it on another workstation. This will allow verification that the problem can be recreated on other machines.

Next, have the operator recreate and test the problem against the original machine to verify that the problem can be created and fixed, and to see if any other issues arise with the effected workstation. Having the operator follow the documentation that was originally created for the problem will verify if other operators are following the standard operating procedures as well.

Indicatori fisici e Logici:

When isolating a problem, physical and logical indicators of trouble may exist. These indicators include the link light, power light, error display, error log and display, and performance monitors.

Link lights should be a steady green or amber indicating that a device is connected to a network. The power light should also be a steady light. If this light is out on a machine, it could mean one of two things. (1) There is no power in the device or (2) the power light could have burned out. All aspects of the problem should be scoped before determining if the device has no power.

Error displays often indicate a malfunction or a failure in a device. Errors can be viewed either as a dialog, which pops up, or in the LED error display of the device. Logs and error displays maintain a listing of errors that have occurred. Although error logs and displays do not provide a solution to the problem, some documentation is provided to help lead to a solution.

Performance monitoring is a tool provided by Windows NT called the Network Monitor. This monitor provides information regarding data coming in and out of a workstation. It tracks the resources used by the components and applications. Performance monitoring is useful when trying to identify bottlenecks in the CPU, memory, disk I/O, network I/O, and error trends. This feature monitors real-time system performance and performance history. By using this monitor, an administrator can determine the capacity of the system and system configurations.

Uno scenario che determina il problema:

Use the following techniques to determine the problem:

- Recognize abnormal physical conditions
- Isolate and correct problems where the fault is in the physical media (patch cable or cable run)
- Check the status of servers
- Check for configuration problems with DNS, WINS, and HOST files
- Check for viruses
- Check the validity of the account name and password
- Recheck operator logon procedures
- Select and run appropriate diagnostics

Question: What are some common issues to look for if a network is having problems?

First, abnormal physical conditions should be considered, such as power interruptions, presence of high heat or humidity where a networking device is located, or large amounts of electrical noise.

An extremely common problem, often referred to as a layer 1 problem, is somewhere in the conducting path from a PCs NIC to the nearest networking device (typically a hub or a switch). The patch cable from the PC to the outlet could be faulty: Bad terminations, bent or crushed cable, or improper wiring sequences. The horizontal cable run, from the outlet to the patch panel, could be bent, crushed, cut, improperly mounted, or otherwise damaged. Or the patch and jumper cables from the patch panel to the networking device could be the incorrect type of cable or also have damage.

Servers should be checked to verify that all servers and resources are functioning properly. Servers and resources such as DNS, WINS, and HOST files should be checked for proper

configuration. A virus scan can be done to be sure that a virus has not entered into the network causing problems. Workstations must have all of the proper settings.

Next, verify the validity of the user's account and password. Is the user typing in the correct user id and password? Does the individual have access? Verify the log in procedures. Finally, if the problem can not be resolved, vendor provided diagnostics should be run.

Strumenti di rete:

Crossover Cable

A crossover cable has the appearance of a twisted-pair cable. However, this cable is used to connect two computers together, instead of a computer onto the network. It has a different pin-out than a straight-through patch cable. Crossover cables can also be used to connect two hubs or two switches together.

Loopback

Loopback is a method used to verify if a device, such as a NIC, is working properly. Either an external loopback adapter or an internal device is attached to the NIC. Data is sent from the NIC out and looped back in to verify if the data received is the same as the data transmitted.

Tone Generator and Tone Locator

Tone generators and tone locators are small handheld devices used to identify wire pairs. Tone generators, also called fox and hound, are used to perform tests on phone and network lines by clipping into the wire, terminal panel, or standard modular jack. By using the fox and hound method, wires can be identified and traced.

A tone generator is placed at one end of the twisted pair to identify a cable. An amplifier is placed on the other end, in the vicinity of the wire, to receive and amplify the audible signal. Using this technique you can identify the wire of interest from among the many wires present.

PREPARAZIONE ESAME CCNA

Funzioni dei livelli osi: The overall goal of communication protocols is to allow a computer application on one computer to communicate with a computer application on another computer. This can be accomplished regardless of the hardware platform or operating system of the two computers.

Livello Applicazione: The application layer is responsible for identifying the communication partner and providing functions for particular application services, such as file transfer and virtual terminals.

Typical TCP/IP applications include:

- Telnet
- FTP (File Transfer Protocol)
- TFTP (Trivial File Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol)

- HTTP (HyperText Transfer Protocol)
- BootP (Bootstrap Protocol)
- DHCP (Dynamic Host Configuration Protocol)

Livello Presentazione: The presentation layer provides communication services. It transparently converts the different data, video, sound, and graphic formats to and from a format suitable for transmission. This layer is also responsible for data compression, decompression, encryption and decryption.

Although, these can be specific protocols, they are usually built into existing application layer protocols.

Some of the presentation layer standards involved include:
Text: ASCII, EBCDIC
Graphics: TIFF, JPEG, GIF, PICT
Sound: MIDI, MPEG, Quick Time

Livello Sessione: The session layer is responsible for controlling the dialogue between devices or hosts. It establishes, manages, and terminates sessions between the applications.

Examples of session layer protocols include:

- Structured Query Language (SQL)
- Remote Procedure Call (RPC)
- X Window System
- AppleTalk Session Protocol (ASP)
- DNA Session Control Protocol (SCP)

Livello Trasporto: The transport layer is responsible for end-to-end delivery of information, including error recovery and flow control.

Transport layer protocols can be reliable or unreliable. Unreliable protocols can have little or no responsibility for establishing connections, acknowledgements, sequencing and flow control. It is possible that unreliable transport layer protocols will leave this responsibility to another layer protocol. The reliable transport layer protocols can be held responsible for:

- Establishing connections and closing connections, such as the Three-way Handshake
- Transferring Data
- Acknowledging what has or has not been received
- Making sure packets arriving out of sequence can be sequenced in their proper order
- Maintaining flow control, i.e. window sizes

TCP/IP reliable transport layer protocol: TCP (Transmission Control Protocol)

- Protocols that use TCP may include FTP, Telnet and HTTP.

TCP/IP unreliable transport layer protocol: UDP (User Datagram Protocol)

- Protocols that use UDP may include TFTP, SNMP, Network File System (NFS), Domain Name System (DNS), and the routing protocol RIP.

Transport layer Protocols include:

- TCP/IP: TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)
- Novell: SPX (Sequenced Packet Exchange)

Livello Network: The network layer provides connectivity and path selection between two end systems, the original source and the final destination, that may be located on geographically diverse networks. Network layer addressing provides addressing for the original source address and the final destination address. In TCP/IP these are the IP addresses. These addresses do not change along the path.

Examples of network layer protocols include:

- IP (Internet Protocol)
- Novell's IPX (Internetwork Packet Exchange)

Livello Data Link: The data link layer provides reliable transit of data across a physical link. The data link layer is thus concerned with physical addressing as opposed to network, or logical addressing. It is also involved in network topology, line discipline (how end systems use the network link), error notification, ordered delivery of frames, and flow control.

The data link layer is responsible for delivery of the frame from one node to the next. Examples include delivery from host to host, host to router, router to router, or router to host. The data link addresses will usually change, representing the current data link address and the next hop data link address. In terms of Ethernet, this would be the source MAC address and the destination MAC address.

Data link layer protocols include:

- Ethernet
- IEEE 802.3
- Token Ring
- IEEE 802.5
- HDLC (High-level Data Link Control)
- PPP (Point-to-Point Protocol)

Livello Fisico: The physical layer defines the electrical, mechanical, procedural, and functional specifications. These specifications activate, maintain, and deactivate the physical link between end systems. Characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connections and other similar attributes are defined by physical layer specifications.

Physical layer standards include:

- 10BASE-T
- 100BASE-TX
- V.35
- RS-232

Encapsulation: Be sure to understand how data is encapsulated and decapsulated at different layers.

Come creare una Subnet: The IP address and a subnet mask can be used to determine:

- The subnet address of this subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet
- The maximum number of subnets for this subnet mask
- The number of hosts for this subnet
- The number of subnet bits and the slash number
- The number of this subnet

Knowing what subnet mask to use will depend on how many subnets and host per subnets are needed. The Figures 1and 2illustrate examples of Class B and C subnetting.

Problemi Esempio:

Problem 1:
Network Address: 172.25.0.0
Requirement: Need 600 hosts per subnet

Solution:
Subnet Mask needed: 255.255.252.0
Reason: 252 in the third octet leaves 10 bits for the hosts, or 1022 hosts per subnet. 255.255.248.0 would have been more hosts than we needed and 255.255.254.0 would not have been enough hosts. 1

Problem 2:
Network Address: 172.25.0.0
Requirement: Need 8 subnets with the greatest number of hosts possible per subnet

Solution:
Subnet Mask needed: 255.255.240.0
Reason: 255.255.240.0 will give you 14 subnets. 255.255.224.0 will not be enough subnets and 255.255.248.0 will not provide the maximum number of hosts per subnet. 2

Testing ed altri comandi Base:

The commands listed in the figures 1- 3are to assist in monitoring, backing up and booting routers. **The commands are only examples and do not reflect the configuration of any actual network.**

Shown in the Figure 1are some commands that may help with troubleshooting the routers. Many of the commands might be used while you are speaking with a Tech Support Engineer.

Backing up and restoring the router configuration and IOS. 2

Boot commands are shown in Figure 3.

Configurare l'IPX routing:

Sample Network: Using the five router lab diagram, we will give the 210.93.105.0 network the IPX 105 network address, and give the 204.204.7.0 network the IPX 7

network address.

Encapsulation PPP, Pap e Chap:

The commands shown in the figures to the left are to assist you in setting up your router. **The commands are only examples and do not reflect the configuration of any actual network.** Your actual commands, IP addresses, network addresses, passwords, etc., will depend upon your network design.

PPP Encapsulation between Lab_B and Lab_C routers

PPP encapsulation 1

NOTE:

The default encapsulation on serial interfaces on Cisco Routers is HDLC.

PPP with PAP authentication 2

PPP with CHAP authentication 3

ISDN:

Notes: Although it is not necessary, the routers below are configured with the data link encapsulation of PPP using CHAP authentication. Also, note that the SPID is only required when connecting to certain ISDN switches, such as the Northern Telecom DMS 100. 1

Gateway 2

ISP 3

ISDN Optional Commands 4

ISDN Monitoring and Testing 5

Interface bri 1
Ip add 10.0.0.3 255.0.0.0
Enacapsulation ppp
Dialer-group 1
Dialer map ip 10.0.0.3 name isp 3355565656
Isdn spid1 08443 213
Isdn spid2 08132 344

Show dialer- status link
Show isdn active- call status
Show isdn status- status isdn connections
Show dialer map- display ip map stantements
Debug q921- connection estabilished and disconnected
Debug isdn active- status of isdn while is in calling
Debug dialer- configuration and operation of dialer

Frame Relay: configuration:

Ip add (ip) (subnet)
Enacapsulation frame-relay
Bandwith 56
Frame-relay map ip 10.16.0.1 100 broadcast ietf
Frame-relay lmi type ansi
\router rip, network..ecc.ecc

Frame relay multiporta:

No ip address
Encapsulation frame-relay
Exit
\interface s2.2 multiport
ip add (ip) (subnet)
bandwith 64
frame relay map ip 10.17.7.20 300 bradcast ietf
\router rip,network..ecc.ecc

Frame relay con subinterfacce:

\interface s2
encapsulation frame-relay
no ip address
exit
\interface s2.2 point-to-point
ip address xxx xxxxx
bandwith 64
frame-relay interface-dlci 300 broadcast cisco
exit
\interface s2.3 point-to-point
ip address xxxx
badwith 64
frame-relay interface-dlci 400 broadcast cisco..
ecc.ecc

Operazioni di switching full duplex e half duplex: In this review of LAN switching, note that one way to help reduce network congestion is to use switches instead of hubs whenever possible. In addition, the efficiency of the switch can be increased with these switching features:

- Fast Ethernet (100 Mbps) switch ports and host NIC cards
- Full-duplex communications
- Cut-through switching

There are two types of Ethernet communications:

- Half-duplex
- Full-duplex

Half-duplex communications allows for two or more devices to communicate with each other, but only one device at a time. [1] If multiple devices attempt to communicate at the same time, a collision will occur. Those devices will then back-off, and a random algorithm within each NIC determines which device will send first.

Hosts that are connected to a hub must operate in half-duplex. This is because the host must be able to detect when a collision occurs in order to stop transmitting.

Full-duplex communications allow two devices to communicate with each other simultaneously. One of the limitations of full-duplex Ethernet is that there must only be one device connected to the switch-port. That device may be a computer, a printer, a router, or another switch. When single devices are attached to switch ports (no hubs) it is a good idea to have them operate in full-duplex.

Operating at full-duplex doubles the amount of throughput on a link. For example, on a standard Ethernet 10 Mbps link, the throughput would be 20 Mbps, 10 Mbps transmitted plus 10 Mbps received. There are virtually no collisions on a full-duplex connection, because there are only two devices in the collision domain. [2]

Configure both ends

It is important that both the switch port and the device connected to the switch are using the same mode of communications, either half-duplex or full-duplex. Both the NIC card in the host, (or in the case of a router, the Ethernet interface) and the switch port must both be using the same mode.

Question: How does the computer NIC get configured for full-duplex or half-duplex operation?

Answer: In older NICs it was done manually, either by software that came with the NIC or with hardware on the NIC itself. Today, most NICs are auto-sensing, and will adapt to the mode in the switch is operating.

Switches can be auto-sensing or software configurable, depending upon the vendor and the model of the switch. If both devices, the host and the switch, are auto sensing and there is only a single device on that switch port, the link will most likely be configured to be full-duplex.

Configuring a Router

If a router is connected to a switch, you may need to configure the router Ethernet interface to be either half or full-duplex. This is a good item to check if you have to troubleshoot a problem with an Ethernet interface on a router.

Mismatch between two switches

Another problem is when two switches are interconnected, and the link seems to be slower than it should be. The problem might be that there is a mismatch between the modes on the ports that link the two switches together. One switch is operating in half-duplex and the other switch is in full-duplex. You may notice the collision light flashing frequently on the device running in half-duplex. The full-duplex device is sending at-will. It is not attempting to sense whether the other device is sending frames or not. This will cause a large number of collisions to occur because as the switch operating in half-duplex senses no traffic on the link, it could forward the frame at the same time the switch operating in full-duplex sends a frame.

Frame Ethernet:

This section covers the parts of the Ethernet frame, as shown in Figure. You will see how internetworking devices such as routers and switches filter and forward these frames.

There are several different types of Ethernet or IEEE 802.3 frames. The terms "Ethernet" and "IEEE 802.3" are similar, but not identical. Ethernet is a product name and a competing standard with IEEE 802.3. There are some differences and similarities, but for the purposes of this section they are not important. To keep things simple, the term "Ethernet" is used throughout this section. However, the information applies to both Ethernet and IEEE 802.3 protocols.

MAC address:

The MAC (Media Access Control) address is a Layer 2 address. It is burned into the ROM chip on an Ethernet network interface card (NIC). This is a unique 48 bit number, written as eight hexadecimal numbers.

The first 24 bits represents the vendor or maker of the of the NIC card. Some vendors may have more than one 24 bit vendor code assigned to them. Each vendor code is a number unique to that vendor. As shown in the Figure, the 24 bit vendor code, together with the 24 bit vendor controlled and assigned serial number, make up a unique 48 bit MAC address.

Funzioni del MAC- L'hub:

In Figure 1, there are four PCs connected to a hub. When a hub receives an Ethernet frame on one port, it forwards (or repeats) it out all other ports.

For example, Host A is sending an Ethernet frame to Host D. Host A encapsulates the data and upper layer headers into the Layer 2 frame field known as the "Data". Normally, when data is being sent from one computer to another, several frames may be needed to transmit it all. In the Ethernet frame header, as shown in Figure 2, Host A is the source MAC address and Host D is the destination MAC address.

Question: After Host A sends out the frame, which hosts will see this frame? More specifically, where does the frame go?

Answer: All of the hosts on this network, every host connected to Hub 1, will see at least part of this frame.

Explanation: Once the frame is sent out from Host A to the hub, the hub forwards (or repeats) the frame out all ports, except the port the frame came in on. Therefore, each host connected to the hub begins to receive the frame. Each host copies the beginning of the frame, the MAC destination Address, into the NIC. If this destination MAC address matches the MAC address of the NIC, then the host copies in the rest of the frame. If the destination MAC address does not match the NIC address, then the host ignores the rest of the frame.

If any other Host on the hub sends an Ethernet frame at the same time Host A is sending its frame as shown in Figure 3, a collision will occur. This is because all four hosts are on the same collision domain.

Funzioni del MAC- Lo switch:

In Figure 1, four hosts are all connected to a switch. Switches forward frames based on Layer 2 addresses (i.e. Ethernet MAC addresses). The switch learns these addresses by examining the Layer 2 source address of the Ethernet frame as it is received. 2

NOTE:

For more information on how switches learn addresses, review Semester 3 information.

Assume that the switch has just been powered on. This means that the switch Source Address Table (SAT), also known as the switch table, is empty as shown in Figure 3. The switch table enables the switch to associate what devices are connected to which switch port. A switch associates which hosts are on which port by "learning". This is why they are sometimes called "learning switches".

When a switch is first turned on, it will not have any entries in its switching table. Each time it sees a frame it will examine the MAC source address. If the MAC source address is not in its table, the switch will enter the address into the switch table that is associated with the port that it was heard on.

In the example in Figure 4, Host A sends a Ethernet frame to Host D. When the switch receives the Ethernet frame from Host A that is destined for Host D, it stores the frame in its memory buffer. The switch examines the MAC source address to see if that particular MAC address is in its SAT table. In this case, it is not, so it adds it to the table, for switch port 1. It has now "learned" that Host A, MAC address 0000.0c11.1111, can be reached via switch port 1.

Next, the switch examines the Ethernet frame destination MAC address and searches for this address in its SAT table. Because this address does not exist in the SAT table, the switch floods it out all ports except for the incoming port. A switch will either filter or flood frames based on its SAT table. As you just learned, a frame gets **flooded** (sent out all ports except for the incoming port) when the switch does not have an entry for the destination MAC address in its SAT table.

A switch filters a frame when it has the Ethernet frame destination MAC address in its SAT table. This means that the switch knows through which port the destination MAC address can be reached. It will only forward the frame out that port.

NOTE:

If the SAT table shows that the destination MAC address is on the same port as the incoming frame, then the switch does not send the frame out any port, including the incoming port. Sending an Ethernet frame out an incoming port would cause duplicate frames on the network.

You will now see what happens when Host D sends information back to Host A. Host D sends a frame with the destination MAC address of Host A, 0000.0c11.1111. 5

The switch examines the MAC Source Address to see if the MAC address of Host D is in its SAT table. In this case it is not, so it adds it to the table for switch port 4. It has now "learned" that Host D, MAC address 0000.0c44.444, can be reached via switch port 4. 6Next, the switch examines the destination MAC address of the Ethernet frame, which is 0000.0c11.1111. The switch looks up this address in its SAT table and acknowledges that it is in its table. The switch forwards this frame out switch port 1 to reach Host A. 7This is an example of a switch filtering a frame.

Question: What would happen if Host A needed to send an Ethernet frame to Host D?

Answer: Because Host D's MAC address (0000.0c44.4444) is in the switch's SAT table, the switch would know to forward this frame only out switch port 4. As shown in

Figure 8, this is another example of the switch filtering the frame.

Segmentazione della lan con lo Switching:

A switch does have an advantage over a hub. A switch allows for a dedicated path between two devices on the switch as shown in Figure 1. This means that pairs of devices on the same switch can communicate in parallel with a minimum number of collisions. When two or more devices attempt to send to the same device on a switch port, a collision does not occur. Instead, one frame will be sent out the switch port to the destination, while the other one will be held in the switch memory or buffer. This is very common when multiple clients are sending information to the same server.

NOTE:

On a switch, each switch port creates a separate collision domain.

In Figure 2, Host A is sending a frame to Host D, and at the same time Host B is sending a frame to Host C. Within the switch, Hosts A and D are communicating in parallel with Hosts B and C, giving two different dedicated paths between senders and receivers. There are no collisions occurring in this example.

However, as shown in Figure 3, a collision may occur if the switch is forwarding a frame at the same time the host on that port is sending a frame towards the switch. This is assuming that the switch and host are operating in half-duplex.

Switch e Buffering:

Another advantage to a switch is that it has a buffer, or memory. If two hosts are sending a frame (or frames) to the same destination, instead of causing a collision, those frames get buffered by the switch. The switch will then send frames out the port to the destination, one frame at a time.

The advantage of the switch buffering these frames is that the source hosts do not need to resend the frame. They are completely unaware that there is contention with another host for that destination. If, for example, Host A and Host B were both sending frames to Host D, as shown in the Figure, the switch would send one of the frames to Host D, and then the next one.

Una rete FLAT:

In many LANs, hubs and switches are interconnected in series. This means the switches must maintain MAC address not only for hosts that are directly connected to one of its switch ports, but also the MAC addresses of hosts connected to other switches and hubs.

In Figure 1, Switch 1 and Switch 2 are interconnected. If Hosts A, B, C, and D send information to Server H, Switch 2 will "learn" that these Hosts' MAC addresses can all be reached via Switch 2's port 1. Figure 2, shows what the Switch 2 SAT table would look like. Remember that if the switch does not have the destination MAC address in its SAT table, then it must flood the frame out all ports.

A completely switched network with all switches and hubs is known as a "flat network." A flat network is a LAN made up entirely of hubs and switches with no routers. All hosts on this LAN are on the same network or subnetwork. Since there are no routers these networks are easy to maintain, and adding a new host or other

device is a relatively simple operation.

However, a flat network has several disadvantages, including a single broadcast domain. As we will see later, a Layer 2 broadcast like an ARP Request will travel to every host and device on the LAN. These and other Layer 2 broadcasts can use up a great deal of the available bandwidth on a LAN.

There are other disadvantages as well, including less manageability of network traffic and security. In a flat network, once the switches have learned which MAC addresses are on which ports, the network traffic will flow accordingly. Except for the placement of the switches, the network administrator has little or no control over the path of the frames.

Segmentazione LAN utilizzando Routers:
Remember that the LAN interfaces on routers, such as an Ethernet interface, perform both the Layer 2 function of a switch and the Layer 3 function of a router. Like switches, routers segment each LAN interface into a separate collision domain as shown in Figure 1. However, routers separate LAN and WAN segments into different networks or subnetworks (Layer 3). This means that routers not only separate interfaces into their own segments, but they also do not propagate or forward Layer 2 broadcast requests, such as ARP Requests, out other interfaces.

Routers interconnect different networks or subnetworks. In Figure 2, the router is connecting two different subnetworks, 172.30.1.0/24 and 172.30.2.0/24. The router has an Ethernet interface on each subnetwork, Ethernet 0 with the IP address 172.30.1.1/24 and Ethernet 1 with the IP address 172.30.2.1/24. The router will only forward packets from one subnetwork to the other if the destination IP address is on the other subnetwork. Because, the destination IP address is a Layer 3 address, as opposed to the Layer 2 addresses, the router will ***not*** forward Layer 2 broadcast addresses like ARP Requests. Therefore, the router separates or segments, the network into separate broadcast domains.

ARP, Richiesta\Risposta: As shown in Figure 1, ARP is a Layer 3 Internet protocol, one of many protocols within the TCP/IP suite of protocols. An ARP Request is used when a sending device knows the IP address for the destination host, but does not know its MAC address. Before the IP packet can be encapsulated into the Ethernet frame, the sending device needs to know the destination MAC address. This relationship of IP to MAC address is normally kept in an ARP table or cache, as shown in Figure 2. This table is dynamically updated based on local network activity. If the IP and MAC address of the destination is not in the ARP table, the device will need to send out an ARP Request in order to get the MAC address.

Question: Why do devices need to map a MAC Address to an IP Address?

Answer: The simple answer is to deliver the IP packet inside an Ethernet frame to the next device along the way in order to reach its final destination. The next device may very well be the final destination or it may be a router. An example is shown in Figure 3.

In this example, host Stevens has an IP packet it wants to send to host Cerf. Host Stevens needs to send this packet to either:

a. the final destination, host Cerf.
   or
b. the default gateway, the router, so it can forward it to its final destination.

Question: How does host Stevens know where it needs to send this packet?

The answer depends on your client software.

Answer 1: Host Stevens will look for host Cerf's IP address of 172.16.10.25 in its ARP table. If it is not found, host Stevens ARPs for the MAC address that is paired to Cerf's IP address. In this example, host Cerf responds with an ARP reply containing its MAC address and the packet is sent.

But what if host Cerf was not on the same local network? If the router has proxy-ARP enabled, it first calculates that the destination IP address was not on the same subnetwork as the source device. It then sends a response of its own MAC address back to host Stevens. Host Stevens then creates a relationship between the destination IP address, host Cerf, and the router MAC address in its ARP table. Next, host Stevens, based on the destination IP address, sends packets to the router for the first hop of the trip to the destination, host Cerf. The router then forwards the packet, based on its IP address, to the destination host or the next hop router.

Answer 2: In this answer, Host Stevens has a default gateway and subnet mask entry stored in its TCP/IP configuration. This is the case with Microsoft Windows™ clients. In this situation, host Stevens does an AND operation on both the source and destination IP addresses using the stored subnet mask, as shown in Figure 4. If the AND operation results in the same subnetwork address, the two hosts are on the same network segment. Host Stevens then looks in its ARP table for the destination IP and MAC address pair. If it cannot find the pair, it issues an ARP request. The destination host responds and the packet is sent. If after ANDing, the resulting subnetwork addresses will be different. If that is the case, then host Stevens will use the default gateway MAC address along with the destination IP address to get the packet to the router for the first hop of the trip to the destination host. The router forwards the packet, based on its IP address, to the destination host or the next hop router.

Esempio 1: La richiesta ARP e la risposta:

In the example in Figure 1, host Cerf's IP address does not appear in host Stevens' ARP table. Host Stevens must send out an ARP request for the IP address 172.16.10.25, host Cerf's IP address. Once again, host Stevens knows it can do an ARP request directly for host Cerf, because it had determined that they are both on the same subnetwork.

As also shown in Figure 1, the ARP request is encapsulated within an Ethernet frame.

ARP request from host Stevens at 172.16.10.10

The ARP Request is a Layer 2 broadcast, which means there are all binary 1s (ones) in the destination MAC address. This is normally written in hexadecimal as all Fs (FF-FF-FF-FF-FF-FF). 2
The IP address Host Stevens is looking for is in the field Target IP Address. All hosts on the LAN receive and process this ARP Request because it is a Layer 2 broadcast. The hosts examine the Target IP Address to see if their IP address matches.

ARP reply from host Cerf at 172.16.10.25

The host with the IP address that matched 172.16.10.25 will reply. This reply is unicast, meaning that only the host that matches the MAC address will process it. Notice that in the ARP reply, the information in the "Sender" and "Target" fields is reversed from the ARP request. This is because the source is now host Cerf instead of host Stevens. 3

Data Transmission from host Stevens

Host Stevens receives the ARP reply and enters host Cerf's IP address and MAC address into its ARP Table. Host Stevens now encapsulates the IP packet into the Ethernet frame and sends the packet directly to host Cerf. 4

Switching Simmetrico ed Asimmetrico:

Symmetric switching is a switch with ports of the same bandwidth as shown in Figure 1. Switching may be optimized through even distribution of network traffic.

Asymmetric switching is a switch with ports of different bandwidth as shown in Figure 2. Asymmetric switching is appropriate when certain switch ports have devices that need more bandwidth, such as servers. Another use for switch ports that need higher bandwidth occurs when that port is connected to another switch.

Whether that switch port needs higher bandwidth or not depends on the amount of network traffic that is received and transmitted through that port. Proper LAN design, network analysis and network traffic monitoring will help network administrators determine which switch ports need the additional bandwidth.

Switching, Cut-Throught e Store-and-Forward: The two main types of switching methods are store-and-forward and cut-through as shown in Figure 1. Depending on the switch, this may be a configurable parameter on each individual port.

Store-and-forward

Store-and-forward is typically the default method on most switches. The switch copies the entire frame into its buffers and checks the FCS (Frame Check Sequence) against its own calculations. If the FCS matches its own calculations, the frame is forwarded out the proper port. If the FCS does not match its own calculations, then the frame is dropped. Checking the FCS takes time, and causes additional latency in the switch, but all errors are filtered. All of this is completed before a switch forwards an Ethernet frame out another interface by looking up the destination MAC address in the switch Source Address Table. 2

Cut-through

There are two types of cut-through switching available on most Cisco switches:

1. Fast-forward
2. Fragment-free

Fast-forward switching begins to forward a frame out the proper switch port immediately after reading the Layer 2 destination address and looking that address up in the switch Source Address Table. The frame will begin to be forwarded out that interface before the rest of the frame is copied into the switch. The FCS is not checked with fast-forward switching therefore there is no error checking.

Fragment-free switching performs like fast-forward switching. However, it waits until the first 64 bytes of the frame have been received before forwarding the first bytes of the frame out of the outgoing switch port. According to Ethernet and 802.3 specifications, collisions should be detected during the first 64 bytes of a frame. Just like fast-forward switching, there is no error checking in fragment-free switching because the FCS is not checked. Fragment-free switching is faster (less latency) than store-and-forward but slower (more latency) than fast-forward.

Controllo Broadcast Livello2:

Virtual LANs or VLANs are used for several reasons, including the creation of separate broadcast domains within a switched network. Routers are necessary to pass information between different VLANs.

A VLAN can be thought of as a subnetwork. There are several ways to implement VLANs. One of the most common methods is to separate subnetworks into separate

VLANs. It is important to note that VLANs are ***not*** necessary to have separate subnetworks on a switched network. However, you will see they provide more advantages when it comes to things like data link (Layer 2) broadcasts

Without VLANs, a Layer 2 broadcast such as an ARP Request would be seen by all hosts on the switched network. On a large switched network, these ARP Requests can consume unnecessary network bandwidth and host processing cycles. Normally, only routers would stop the propagation of Layer 2 broadcast such as these ARP Requests.

Notice in the Figure that although the hosts are on different subnetworks, the ARP Request is being received by all of the computers. This can especially become an issue in a network with Windows 95/98 computers. Windows 95/98 computers keep entries in their ARP tables for only 120 seconds. If the ARP table has not communicated with a device for 120 seconds, it will erase its IP address (MAC address mapping from the ARP table). The next time the host needs to communicate with this same device, it will need to do another ARP Request. UNIX computers normally keep entries in their ARP tables for about 20 minutes.

Perchè usare le V-LAN Port-Centric: The network in Figure 1, has a network address of 172.30.0.0. The network has been divided into subnetworks using the subnet mask 255.255.255.0. Therefore, two subnetworks exist on the network, 172.30.1.0/24 and 172.30.2.0/24.

Question: Suppose VLANs are not in use. What would happen with a Layer 2 broadcast, such as an ARP Request?

Answer: All hosts, regardless of what subnetwork they belong to, will receive the ARP request. The request will be received as long as they are on the same switched network and there is no router between them and the ARP Request.

With port-centric VLANs, the network administrator assigns each switch port to a specific VLAN as shown in Figure 2. It is important that the VLAN assignment on the switch matches the subnetwork assignment on the host that is connected to that switch port.

What would happen with ARP Requests on the network with the use of VLANs? Remember, the VLAN assignment is actually done at the switch. There is no VLAN assignment done on the individual hosts. Figure 3shows the VLAN numbers on the hosts for clarity purposes only.

For hosts on the 172.30.1.0 subnetwork, the switch port will be configured as VLAN 1.

For host on the 172.30.2.0 subnetwork, the switch port will be configured as VLAN 2.

Notice that this time, only hosts on the same VLAN (VLAN 2) that are also on the same subnetwork, will receive the Layer 2 broadcast, the ARP Request. The Layer 2 broadcasts are only meant for hosts within the same subnetwork. Therefore, the VLAN mapping on the switch keeps the unwanted, unnecessary Layer 2 broadcast from being forwarded on links that do not need to receive those frames.

It is important to note that it is the switch that does this filtering. This happened because the network administrator assigned the proper VLAN assignment to the proper switch port. The switch is configured as follows:

Switch Port	VLAN
1	1

2	**2**
3	**1**
4	**2**

Routing e Vlans: Just like subnetworks, a router is needed to route information between different VLANs. There are several different methods available to do this with the router.

One way is to have a router with a separate Ethernet interface for every VLAN (i.e. subnetwork). Figure 1 shows the router with two Ethernet interfaces. The Ethernet 0 interface is configured with an IP address of 172.30.1.1/24. It will be a member of VLAN 1 on the switch. The Ethernet 1 interface is configured with an IP address of 172.30.2.1/24 and will be a member of VLAN 2 on the switch.

Figure 2 shows how the switch and router interconnect.

If information is to be sent from a host on one VLAN (subnetwork) to a host on another VLAN (subnetwork), these packets will need to be sent to and routed through the router. 3

Example:

```
Router(config)# router rip
Router(config-router)#
network 172.30.0.0>
```

One of the disadvantages to this type of router configuration is that the router must have a separate Ethernet interface for every VLAN (subnetwork). This may not scale well for networks with a lot of different VLANs. One solution to this problem is to use "Router-on-stick" or "One-Armed-Router" (OAR).

With the Router-on-stick method, only one physical Ethernet interface is used. The physical interface is divided into sub-interfaces, one for each VLANs (subnetworks). 4

NOTE:

Secondary addresses can be used instead of subinterfaces to accomplish this, but secondary addresses will eventually be no longer supported in future versions of the Cisco IOS.

One disadvantage of Router-on-a-stick is that the single link between the router and the switch is also used for all VLAN traffic to and from the switch. If the link is not of high enough bandwidth, a traffic bottleneck (congestion) may occur. The port on the switch that is connected to the router Ethernet interface will also need to be capable of doing "trunking," either with Cisco's proprietary ISL (InterSwitch Link) or IEEE 802.1Q.

Here is the router configuration (also shown in Figure 4):

```
Router# config t
Router(config)# interface ethernet 0.1
Router(config-subif)# ip address 172.30.1.1 255.255.255.0
Router(config-subif)# encapsulation isl 1 {1 = VLAN 1}
Router(config-subif)# no ip redirects {recommended}
Router(config)# interface ethernet 0.2
Router(config-subif)# ip address 172.30.2.1 255.255.255.0
Router(config-subif)# encapsulation isl 2 {2 = VLAN 2}
Router(config-subif)# no ip redirects {recommended}
```

Tagging Vlan: A standard Ethernet cable can be used to pass traffic between multiple VLANs or subnetworks. In order for the connection to carry multiple VLAN traffic, the switch or router ports must be able to support trunking. In Figure 1, it is the switch ports making the connection that must be capable of trunking.

VLAN terminology:

- **Trunk** - a single link that carries multiple VLAN traffic
- **Tagging** - identifies which VLAN a frame belongs to while being transported across a trunk

Different tagging protocols include:

- IEEE 802.1q
- ISL (Inter-Switch Link) - Cisco proprietary
- 802.10 - FDDI
- ATM LANE

Tagging in relationship to Trunking

Frame tagging and trunking are often confused when describing VLANs. A tag is a header that is added to a data link header, this indentifying the VLAN membership of the frame. The term trunking is used to describe a single connection that carries multiplexed network traffic. Multiplexing is a term that describes the sending of several sources of traffic over a single physical line.

Tagging

Cisco Catalyst switches support two types of tagging on Ethernet interfaces:

1. IEEE 802.1Q
2. Cisco proprietary Inter-Switch Link (ISL)

These two standards define the information carries in the frame tag, including VLAN identifier information. ISL is used for Fast Ethernet and Gigabit Ethernet. IEEE 802.1Q can be used with all layer two protocols including Fast Ethernet, Gigabit Ethernet, Token Ring, and FDI. The tag is added to the frame by the switch or router that is sending the frame over VLAN trunk. It is not added by a host computer. The switch or router at the other end of the VLAN trunk removes the frame tag.

Trunking

Trunking allows you to multiply the traffic of several VLANs over a single link. Without a trunk line, separate links would be required for each VLAN. Many switches will have at least one or two ports that are also for trunking. In this case, the port can carry traffic for multiple VLANs. Trunking is used where there is a need to transmit traffic for multiple VLANs by connecting two switches, or a switch and a router.

In Figure 2, you will notice that there are two links where trunking is taking place.

1. Between Switch 1 (Port A) and Switch 2 (Port A)
2. Between Switch 2 (Port B) and Router (Ethernet 0)

The router uses subinterfaces to allow trunking into the router. Each VLAN is attached to its own logical subnetwork interface. Each subinterface has its own IP subnet address, which is how the router can route data between the VLANs.

Question: What would you do if your equipment was not capable of trunking, but you still wanted to do VLANs?

Answer: You would require a separate link for every VLAN between switches, and between a switch and a router. Be sure to configure the switch ports for the proper VLANs.

Funzione Spanning Tree:

The main function of the **Spanning Tree Protocol (STP)** is to allow redundant switched/bridged paths without suffering the effects of loops in the network. Spanning Tree allows for multiple links between switches. However, only one link is active (Forwarding mode), while all other redundant links are in standby (Blocking mode) in case the primary link fails.

Question: What would happen if there were multiple links between two switches, and you did not have Spanning Tree?

Answer: This could cause frames to be forwarded out the wrong switch ports, or even worse, cause Layer 2 broadcast storms. Remember that a broadcast storm is when frames keep getting duplicated on a switched network, until it finally overwhelms the network, and brings it down.

Spanning Tree is important even in networks where there are no redundant links between switches. It is not uncommon for someone to accidentally connect a link between two switches when a connection already exists. Spanning Tree is an excellent safeguard from keeping a mistake like this from bringing down a network.

For more information on Spanning Tree Protocol and how it works, review the Power Point presentation on Spanning Tree in Semester 3.

Comandi Vari:

What follows are two similar practical exams to help you prepare for the Semester 3/4 Skills-Based Final Exam and for your CCNA Certification Exam.

Duration: 1 hour
Setup: Serial Cables will be connected.
Router status: Routers will not have a startup-config.
Resources: Cisco documentation provided by instructor. No other books or notes.

Primary Skills

Subnetting

Basic Configuration Commands

- Hostnames
- Passwords
- Interface addressing, descriptions, clock rates

Routing

- Dynamic: RIP, IGRP

- IPX (secondary skill)
- Static routes
- Default routes

Access Lists

- *Standard ACL*
- *Extended ACL*

WAN Encapsulations

- *PPP*
    - *CHAP authentication*
    - *PAP authentication*
- *HDLC*

SecondarySkills

ISDN

- *switch-type*
- *dialer map*
- *spids*
- *DDR (non-critical)*
    - *dialer-list*
    - *dialer-group*
    - *access-list*

Frame Relay

- *Simple configuration*
    - *encapsulation*
    - *frame-relay ip map*
    - *frame-relay interface-dlci*
    - *frame-relay lmi-type*
