Laboratorio di configurazione e gestione di reti locali

20th March 2012

Stefano Pilla

Cisco Academy Instructor (CCAI)

stefano.pilla@clorofillaroma.it

Cisco | Networking Academy®
Mind Wide Open™

Argomenti

Networking e i suoi benefici

Modello ISO/OSI

Tipologie di rete e protocolli di comunicazione

Broadcast domain/Collision Domain

Differenze tra Hubs and Switches

Access/Distribution/Core Layer

Reti Ethernet

Cisco IOS

VLANs

InterVLAN Routing

Laboratorio

Networking: Client e Server

Tutti i computer connessi ad una rete e capaci di comunicare attraverso la rete stessa vengono definiti **host**. Il software installato sugli host definisce il loro **ruolo**, nel senso che un host può agire da **client, da server o da entrambi.**

I **server** sono host con software installato che permette loro di fornire servizi (ad esempio servizi web o di posta) agli altri host della rete; **ogni servizio richiede che sia installato un server software separato.**

I **client** sono host il cui software consente loro di richiedere informazioni ai server e di visualizzare le informazioni ottenute (ad esempio un browser è un software client)

Networking: Le reti P2P

Le reti **peer-to-peer (P2P)** sono quelle reti in cui gli host hanno **simultaneamente il ruolo di client e server**, situazione tipica di una rete di due soli computer. Reti peer-to-peer più grandi si possono realizzare connettendo i computer mediante un **hub** o uno **switch**. Al crescere del numero di host, le performance degradano a causa del fatto che ogni host agisce sia da server sia da client.

Protocolli di comunicazione

Tutte le comunicazioni iniziano con un messaggio che deve essere inviato da un individuo (o dispositivo) ad un altro. I metodi con cui i messaggi vengono inviati cambiano nel tempo al progredire della tecnologia

Tutti i metodi di comunicazione hanno in comune tre elementi: **la sorgente, il ricevente ed il canale** (il percorso dei messaggi dalla sorgente al ricevente)

Protocolli di comunicazione

In qualsiasi comunicazione (tra umani o computer) devono esserci delle **regole** perchè il messaggio sia ricevuto e compreso con successo

I **protocolli** definiscono in dettaglio le regole con cui il messaggio deve essere trasmesso e consegnato. I protocolli per la comunicazione tra dispositivi si basano su molti concetti che rendono affidabile e comprensibile la comunicazione tra esseri umani

Protocolli di comunicazione: Encoding

Nella comunicazione umana la **codifica** delle informazioni avviene tutte le volte che qualcuno esprime ad un altro i propri pensieri attraverso **parole** e **gesti**. Il ricevente deve poi **decodificare** per interpretare e comprendere il pensiero dell'altro.

Nella comunicazione tra computer ogni messaggio viene prima **convertito in bit** e poi **codificato con impulsi elettrici**, **luminosi**, **onde e.m**. a seconda del mezzo trasmissivo. Il messaggio codificato viene inviato all'host ricevente, che dovrà **decodificarlo** per poterlo "interpretare" e "comprendere".

Protocolli di comunicazione - Encapsulation

Ogni messaggio spedito da sorgente a destinazione viene costruito **secondo uno specifico formato** che dipende dal tipo di messaggio e dal canale usato

Quando si scrive una lettera, il messaggio ha una certa struttura (intestazione, saluto, corpo del messaggio). Inoltre viene **“incapsulato”** in una busta che contiene altre informazioni (indirizzo del mittente e del destinatario)

Allo stesso modo ogni messaggio tra computer viene **incapsulato** in uno specifico formato, detto **frame, pacchetto,** prima di essere spedito sulla rete. Il frame “avvolge” il messaggio e contiene gli indirizzi dell’host sorgente e di quello di destinazione.

Protocolli di comunicazione - Timing

Un altro fattore importante, di cui i protocolli tengono conto, è il **timing** (la temporizzazione, la gestione del tempo) che si divide in:

Metodo di accesso: perché un messaggio sia ricevuto e compreso si può parlare **quando nessun altro parla.** Se due persone parlano contemporaneamente si ha una **collisione** tra messaggi. Allo stesso modo, gli host sulla rete necessitano di un metodo di accesso per sapere quando trasmettere.

Controllo di flusso: se una persona parla troppo velocemente, l'altra potrebbe non capire. Gli host negoziano la velocità adeguata attraverso il controllo di flusso.

Timeout della risposta: se non si ottiene risposta ad una domanda in un tempo ragionevole, la domanda viene ripetuta. Gli host hanno regole che stabiliscono quale azione intraprendere alla scadenza del timeout.

Protocolli di comunicazione

Così come accade per gli esseri umani, anche nel caso degli host esistono delle circostanze in cui la comunicazione è “da uno a uno”, altre in cui è “da uno a molti”. Pertanto i vari tipi di messaggi vengono classificati come:

Unicast: un solo destinatario

Multicast: più di un destinatario, all’interno di un gruppo (ma non tutti)

Broadcast: tutti gli appartenenti ad un gruppo

Protocolli di comunicazione

Se all'interno di una stessa stanza, delle persone usassero ognuna una lingua differente questi potrebbero non capirsi

Gli host in una rete locale devono condividere uno stesso protocollo perchè la comunicazione abbia successo

Il protocollo maggiormente utilizzato nelle reti locali è **Ethernet**. Il protocollo Ethernet definisce molti aspetti della comunicazione su rete locale, tra cui: **formato e dimensioni del messaggio, timing e codifica.**

Modello a strati (o a livelli)

Perchè la comunicazione tra due host possa avere successo **diversi protocolli devono interagire**. Questi protocolli sono implementati nel **software e/o nell'hardware degli host** e **dei dispositivi di rete**. L'interazione tra i protocolli può essere rappresentata mediante una **pila (o stack)**, **una struttura gerarchica in cui i protocolli dei livelli superiori dipendono dai servizi offerti dai protocolli dei livelli inferiori.** A questa pila ci si riferisce con il nome di **suite (o pila) TCP/IP**. I protocolli dei livelli più bassi gestiscono lo spostamento dei dati sulla rete e forniscono servizi ai livelli superiori. I livelli più alti si riferiscono al contenuto informativo dei messaggi inviati e all'interfaccia verso l'utente.

Modello a strati (o a livelli) - Funzionamento

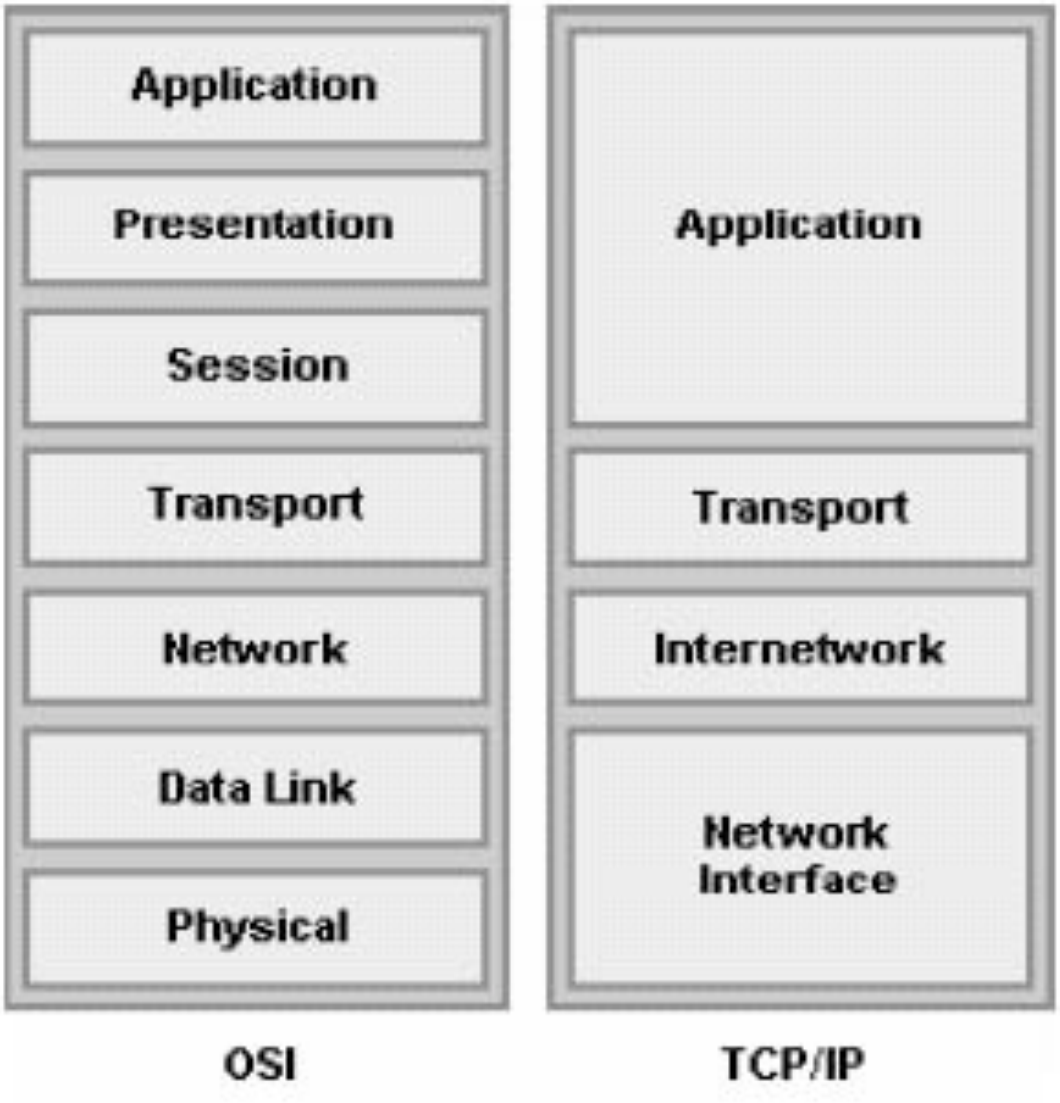
Quando un host invia messaggi, lo stack dei protocolli opera dall'alto verso il basso. Ciò corrisponde ad un processo di **incapsulamento**.
Consideriamo un web server che invia una pagina web ad un client. Il codice HTML ed il protocollo HTTP vengono suddivisi in segmenti dal protocollo TCP, che successivamente aggiunge un'intestazione con le porte sorgente e destinazione. I segmenti TCP vengono passati al livello inferiore che li incapsula in pacchetti IP, con un'intestazione che contiene indirizzi IP sorgente e destinazione. I pacchetti IP vengono inviati al livello sottostante che li incapsula in un frame Ethernet, con un header che contiene MAC sorgente e destinazione, ed un trailer che contiene codice di controllo per eventuali errori. Infine i bit sono codificati dalla NIC in segnali la cui natura dipende dal mezzo fisico e dalla tecnologia.
Quando i messaggi sono ricevuti, lo stack opera dal **basso verso l'alto. Ciò corrisponde ad un meccanismo di de-incapsulamento**. La NIC decodifica i bit e se riconosce il MAC di destinazione coincidente con il proprio, passa il frame al livello Ethernet che rimuove header e trailer. Il livello internet rimuove l'header IP. Il livello trasporto rimuove l'header TCP e riassembla i segmenti. Infine i dati sono passati al livello applicazione, dove il browser mostra la pagina web ricevuta.

Pila ISO/OSI

Il modello **OSI (Open Systems Interconnection)** fu creato nel 1984 dall'ente di standardizzazione **ISO.** È stato creato come un'architettura che gli sviluppatori dovrebbero seguire nel progettare i protocolli di rete. Il modello OSI contiene tutte le **funzioni (o task) associate alla comunicazione tra reti,** non solo quelle relative al **TCP/IP**.

Avendo sette livelli, i task sono organizzati in **maniera più specifica, nel senso che con questo modello si è cercato di individuare le funzioni veramente essenziali e di separarle in livelli diversi (cosa che non sempre succede con il TCP/IP)**

Pila ISO/OSI



Comunicazione in una rete locale Ethernet

Quando le reti iniziarono a svilupparsi, c'erano molti protocolli proprietari, cosa che impediva a prodotti di marche diverse di interoperare. Ci si accorse ben presto che la standardizzazione portava ad una più facile progettazione dei dispostivi e ad una effettiva interoperabilità tra dispositivi di produttori diversi. Negli anni **Ethernet si è imposto come lo standard de facto per le reti locali.** Fin dalla nascita nel 1973 ed attraverso le successive standardizzazioni **(1980 DIX, 1983 IEEE 802.3…)** la tecnologia si è evoluta verso forme più veloci e flessibili. I primi standard **(10BASE-T)** operavano a 10Mbps. Oggi Ethernet opera a **10Gbps (GigaEthernet)**

Reti Ethernet - Il MAC Address

Ogni scheda di rete **Ethernet** ha un **indirizzo fisico (MAC Address)** che le viene assegnato quando viene prodotta

L'indirizzo fisico serve ad individuare un host nella rete

Quando un host comunica su una rete Ethernet, invia frame che contengono il suo MAC address **(che identifica la sorgente)** ed il MAC address dell'host di destinazione. Ogni host che riceve il frame lo decodifica e ne legge il MAC destinazione: se coincide con il proprio MAC address processa il messaggio; se non coincide lo ignora.

Reti Ethernet - Protocol Data Unit (PDU)

Il protocollo Ethernet definisce molti aspetti della comunicazione: formato e dimensioni del frame, timing e codifica. Quando dei messaggi vengono inviati su una rete Ethernet, gli host li formattano in una struttura di frame che è definita dagli standard. I frame vengono anche chiamati **PDU (Protocol Data Unit).**

Il protocollo definisce inoltre: **le dimensioni massime (1518 byte) e minime (64 byte) del frame**; la codifica dei bit come segnali fisici sul canale (cavi in rame, fibra…)

Reti Ethernet - Livelli Gerarchici

Le reti Ethernet di grandi dimensioni sono **inefficienti a causa dei broadcast** generati dalla tecnologia **Ethernet** stessa e dalla difficoltà a localizzare un host in base al **solo MAC Address** (l'indirizzo fisico identifica una NIC, ma non permette di localizzare né l'host che la possiede all'interno di une rete, né la rete stessa)

In base a queste difficoltà sarebbe impensabile realizzare **Internet come una gigantesca rete Ethernet.** L'**approccio gerarchico** raggruppa gli host in più reti locali, organizzate a livelli. Il traffico passa in un altro livello solo quando deve raggiungere una rete locale diversa da quella di origine

Il design gerarchico ha tre livelli base:

Access layer: connette dispositivi in rete locale
Distribution layer: connette più reti locali (Access Layer)
Core layer: connette I dispositivi del distribution layer

Reti Ethernet - Indirizzi IP

Il MAC Address è fisicamente assegnato alla NIC degli host e non cambia, dovunque l'host si trovi nella rete. **L'indirizzo IP** viene detto **indirizzo logico** perchè è **assegnato logicamente in base a dove un host si trova (rete di appartenenza).**

Viene assegnato da un amministratore di rete ed è costituito da due parti. Una prima parte dell'indirizzo identifica **la rete locale di appartenenza**, la seconda parte **individua uno specifico host.**

Gli indirizzi MAC ed IP possono essere paragonati rispettivamente al nome ed all'indirizzo di una persona.

E' chiaro che entrambi sono necessari perché i computer possano comunicare su una rete gerarchica.

L’avvio di un router Cisco - Stage 1

La fase di avvio di un Router Cisco è composta principalmente da 3 Stages:

1) Fare un Power-on Self Test e avviare il programma di bootstrap

Il Post è quel processo che avviene su tutti i Pc quando si avviano. Il POST viene utilizzato per testare l’hardware. **Dopo il POST il programma di bootstrap viene avviato.**

2) Localizzare e avviare il Cisco IOS Software

Dove cercarli?

In una Flash memory, un TFTP Server o quasiasi altra posto indicato nel file di configurazione d’avvio. Di default l’avvio avviene dalla memoria flash.

L’avvio di un router Cisco - Stage 3

3) Localizzare e eseguire la “startup-config” o entrare in “Setup Mode”

Dopo aver avviato e caricato l’IOS il bootstrap software cerca la startup-config nella **NVRAM**. Questo file contiene la configurazione salvata, inclusi gli indirizzi delle interfacce, le informazioni di routing, password, etc... Se il file di configurazione non viene trovato, il router entra in una modalità in cui è possibile riconfigurarlo da zero. Se la startup-config viene trovata, viene **copiata nella RAM** e il prompt con l’hostname viene visualizzato. **Il prompt indica che è tutto andato a buon fine!**

Running/Startup Config

Per evitare la perdita di dati è importantissimo conoscere la differenza tra **Running-Config e Startup-Config.**

La **Startup Config** è quel file di configurazione che configura il router ogni volta che si avvia. Questo file è memorizzato in una **NVRAM (Non-Volatile RAM)**, questo significa che resta in memoria anche quando il Router viene spento. Quando un Router viene avviato, **l'IOS viene caricato in RAM**. Lo step successivo è quello di copiare la **startup-config dalla NVRAM nella RAM.** Quando il file viene copiato diventa la **"Running-config"**

Running/Startup Config

La running-config fa riferimento all'attuale configurazione presente in RAM. Il file contiene tutti i comandi utilizzati per determinare come il dispositivo deve funzionare sulla rete.

La running-config è memorizzata nella RAM. I cambiamenti a questa possono essere solo fatti quando il file si trova nella RAM. Quando il device viene spento, la running config viene persa. Per non perdere anche i cambiamenti effettuati e per renderli "permanenti" bisogna memorizzarli nella "startup-config" con il comando

copy running-config startup-config (copy run start)

ATTENZIONE! La running config NON viene automaticamente salvata dopo un tot di secondi!

Quando viene utilizzata l'SDM, c'è un opzione per salvare la running-config nella startup-config.

Out-of-band Management

Richiede che un computer (dotato di emulatore di terminale) sia connesso alla porta **console** o alla porta **AUX** del dispositivo.

Questo tipo di connessione è adatta nei casi in cui **le interfacce di rete non sono ancora attive**, come nella prima configurazione, o quando la connettività di rete mostra problemi e non vi sono altri modi di raggiungere il dispositivo.

Sfrutta collegamenti di rete (sia LAN sia WAN) e necessita che almeno una interfaccia di rete sia attiva e propriamente configurata. Due protocolli TCP/IP possono essere usati allo scopo: **HTTP (con uso del browser) e Telnet (con un telnet client)**

Configurazione tramite CLI

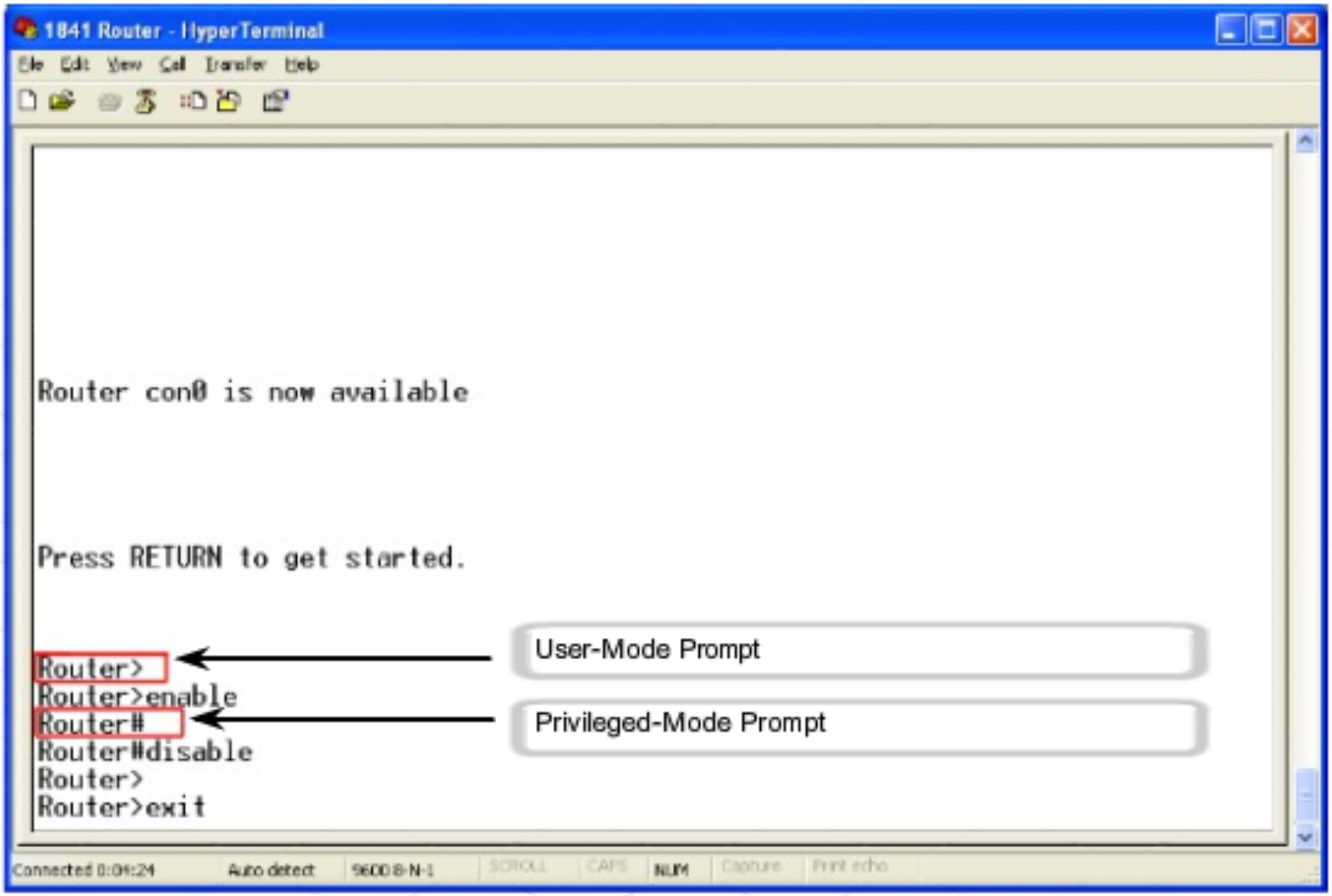
La **Cisco IOS CLI** offre due livelli di accesso all'interfaccia di configurazione: **user EXEC (Router>) e privileged EXEC (Router#).**

Il primo è quello in cui si trova per default un dispositivo appena viene acceso. In questa modalità si accede ad informazioni base ed a strumenti di troubleshooting come il ping.

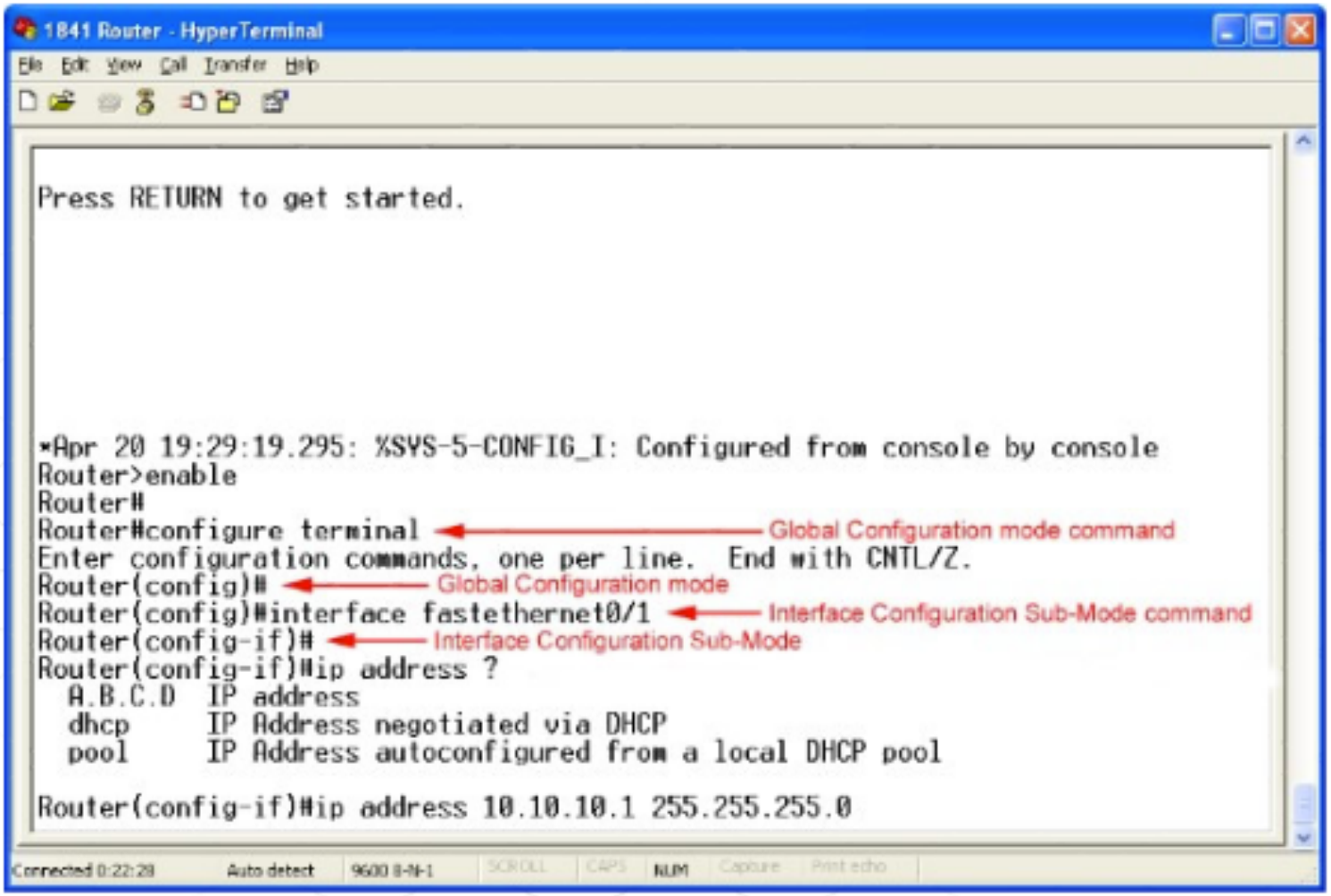
Alla modalità privilegiata si passa con il comando **enable**. In questa modalità è possibile impartire i comandi che possono modificare l'operatività del dispositivo. Entrambi i livelli di accesso possono essere protetti con una password.

Per impartire comandi di configurazione è necessario entrare in **modalità di configurazione**, tramite il comando **configure terminal.** Comandi successivi possono far passare a modalità di configurazione più specifiche, ad esempio quella di configurazione delle interfacce o quella di configurazione dei protocolli di routing.

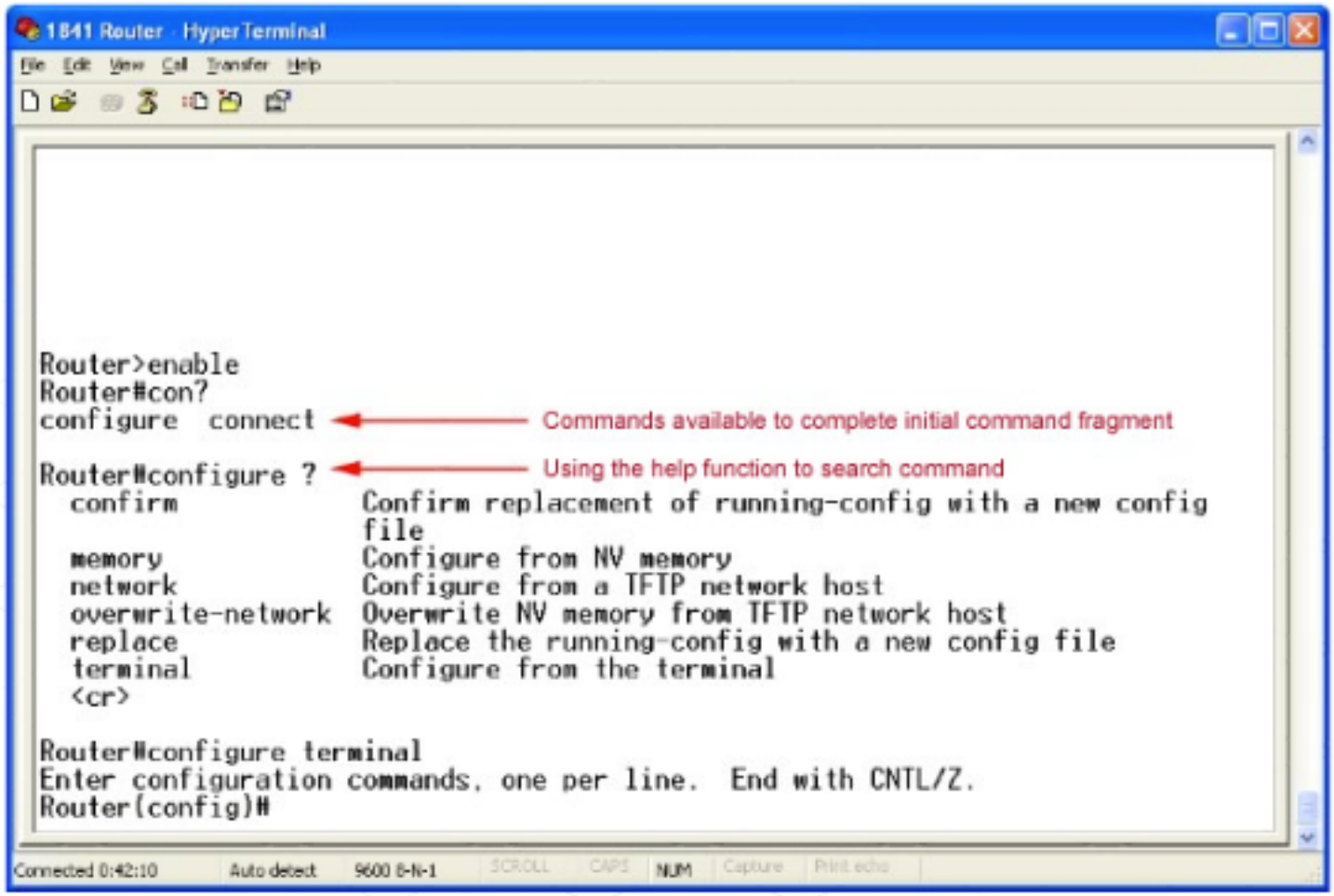
Configurazione tramite CLI



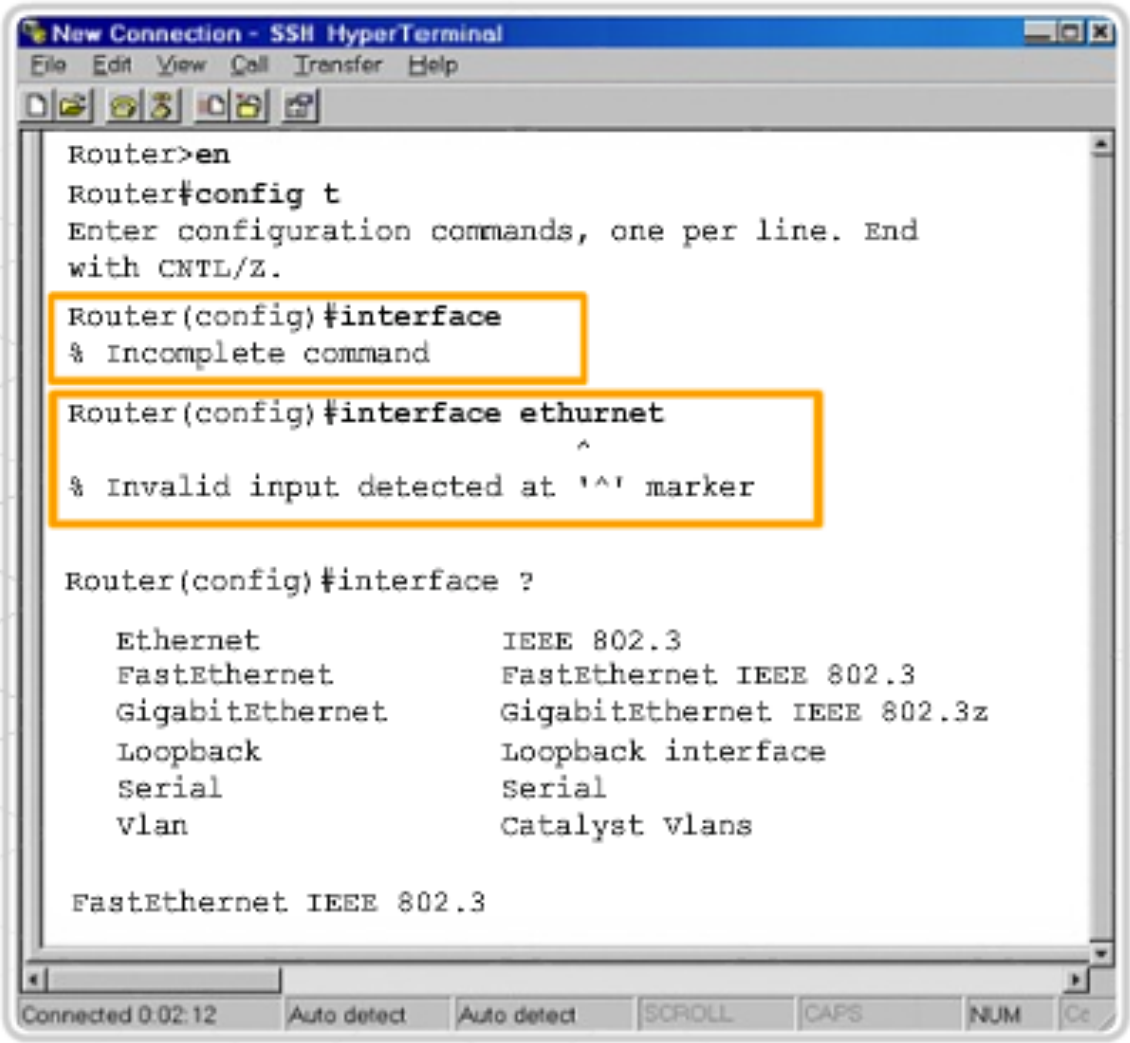
Livelli di configurazione



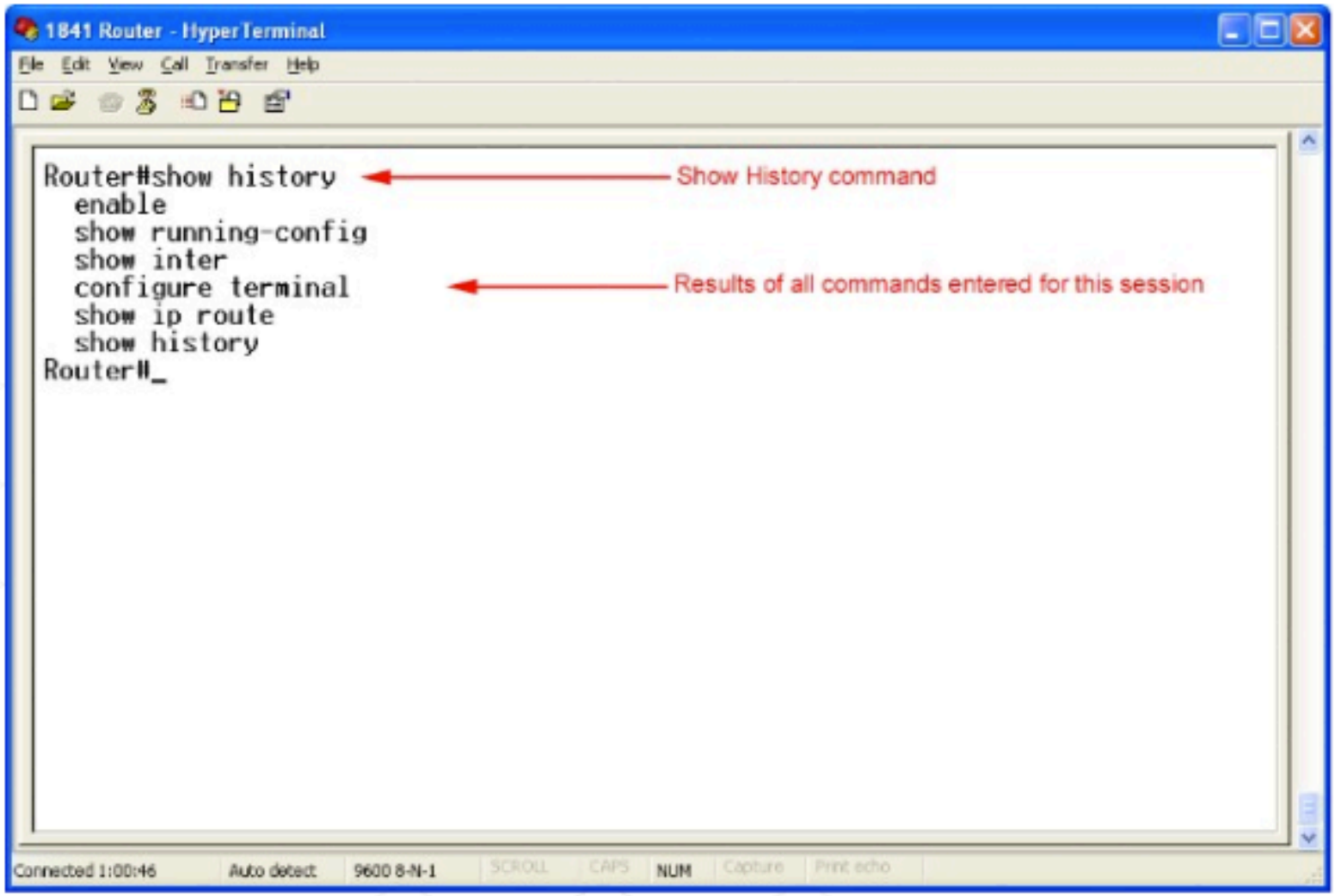
Question Mark (?) ..help!



Invalid Input (^) - Incomplete Command



History command



Access Layer - Hub e Switch

L'Access layer fornisce un punto di connessione alla rete per i dispositivi dell'utente finale. È la porzione della rete in cui si ottiene l'accesso ad altri host ed a file e stampanti condivise. **Questo livello è costituito dagli host e dai dispositivi di rete (hub e switch)** ai quali gli host sono connessi.

Diversamente da una semplice rete costituita da due computer, nell'access layer si deve usare un dispositivo per interconnettere gli host.

Ogni host può essere collegato ad un dispositivo di rete tramite un cavo, che soddisfa i requisiti degli standard Ethernet.

Ogni cavo è una connessione **point-to-point inserito in una NIC da un lato e in una porta di uno dei dispositivi dall'altro.**

Access Layer - Hub

Ha più porte per connettere gli host alla rete. Non avendo l'elettronica necessaria a decodificare il messaggio, si limita **a ripetere e rigenerare il segnale ricevuto da una porta su tutte le altre porte.**

È un dispositivo a **banda condivisa** perchè tutte le sue porte costituiscono un unico canale. Se due o più host tentano di spedire messaggi contemporaneamente, si verifica una **collisione** e i **messaggi vengono corrotti**. La zona della rete dove un host può essere raggiunto **da un messaggio corrotto viene detta dominio di collisione.**

Quando gli host rilevano una collisione, aspettano per un breve intervallo di tempo, poi provano a ritrasmettere **(CSMA/CD).** All'aumentare del numero di host, aumentano le probabilità di collisione, quindi è necessario limitare le dimensioni dei domini di collisione.

Access Layer - Switch

Come un hub, collega più host alla rete. Diversamente da un hub, spedisce un messaggio **allo specifico host di destinazione, potendo leggere il MAC di destinazione all'interno dei frame.**

La **tabella dei MAC Address (MAC o CAM Table)** associa le porte attive dello switch ai MAC address degli host collegati. Quando un frame arriva su una porta dello switch, esso **controlla se il MAC address di destinazione è associato ad una porta.** Se sì, lo switch crea un **circuito temporaneo** tra la porta sorgente e la porta di destinazione. Ogni circuito è un canale separato, **che ha tutta la banda disponibile a disposizione ed è libero da collisioni.** Ciò permette a più host di spedire messaggi contemporaneamente, senza che avvengano collisioni.

E se il MAC address di destinazione non è presente nella MAC Table?

Lo switch fa **flooding**, ossia invia il frame ricevuto su tutte le altre porte. Tutti gli host confrontano il MAC destinazione con il proprio indirizzo fisico, ma solo la corretta destinazione processa il messaggio (ed eventualmente risponde alla sorgente)

Access Layer - Hub collegato allo Switch

Lo switch costruisce un'entry nella MAC Table leggendo il MAC address sorgente in un frame ed associandolo alla porta su cui il frame è stato ricevuto.

Quando un hub è connesso alla porta di uno switch, **questo associa alla porta tutti i MAC degli host collegati all'hub.** Se un host connesso all'hub invia un messaggio ad un altro host connesso all'hub, il messaggio arriva anche alla porta dello switch, che però scarta. Tra gli host connessi all'hub sono possibili collisioni. Anche i risultati delle collisioni che giungono sulla porta dello switch non vengono da questo inoltrati

Access Layer - Comunicazioni Broadcast

Sulle reti locali può essere spesso necessario che un host possa inviare messaggi a tutti gli altri host contemporaneamente (es. flooding). Siccome un frame può contenere un solo MAC di destinazione, si è posta la convenzione che il MAC di destinazione di un frame spedito in broadcast è costituito da **48 bit posti ad 1**. In esadecimale corrisponde a **FFFF.FFFF.FFFF**.

Hub e switch spediscono i messaggi in broadcast a tutti gli host in una rete locale. Per questa ragione, una rete locale viene detta **dominio di broadcast.** Se molti host sono collegati ad una rete locale, **può verificarsi un eccessivo traffico broadcast che decrementa le prestazioni della rete.** Pertanto può essere necessario dividere una rete locale in più reti locali, aumentando il numero dei domini di broadcast, ma diminuendo le dimensioni di ciascun dominio.

Distribution Layer - I router

Quando le dimensioni di una rete locale aumentano, è bene dividerla in più reti di tipo **Access layer**. Il **Distribution layer** connette queste reti indipendenti e controlla il traffico che passa da una all'altra. I dispositivi del DL sono (principalmente) **router. I router interconnettono reti, non singoli host.**

I router del Distribution layer possono:

Contenere i broadcast nelle reti locali dove è necessario che tali broadcast vengano ricevuti

Proteggere specifici gruppi di computer e nascondere al mondo esterno i loro indirizzi interni per prevenire attacchi

Collegare location separate geograficamente di una stessa organizzazione

Raggruppare host su base logica, ad esempio l'appartenenza ad uno stesso dipartimento e la necessità di accedere a risorse comuni

Distribution Layer - Encapsulation (MAC+IP)

I router sono dispositivi di rete che connettono tra loro **reti locali e remote**. Diversamente dagli switch che decodificano i **frame** per poterne leggere i MAC Address, i router decodificano il **pacchetto incapsulato nel frame.** Il pacchetto contiene gli indirizzi IP degli host sorgente e destinazione, oltre ai dati tra essi scambiati. **Ogni NIC del router è connessa ad una differente rete locale**. Ogni router conserva una tabella (**detta "di routing"**) delle reti locali connesse e delle rotte per raggiungere reti remote. Quando un frame giunge al router, esso estrae il pacchetto contenuto e ne legge le informazioni IP. Se la rete di destinazione coincide con una delle reti presenti nella tabella di routing, il router **costruisce un nuovo frame incapsulando il pacchetto**, poi instrada il nuovo frame sull'interfaccia corrispondente nella tabella di routing alla rete di destinazione. Questa operazione prende il nome di **routing. Il router non instrada messaggi indirizzati con il broadcast fisico FFFF.FFFF.FFFF, pertanto tali broadcast non si propagano da una rete locale all'altra (Segmentazione della rete).**

Distribution Layer - Default Gateway

Il metodo usato da un host per inviare messaggi su una rete locale differisce da quello usato per inviarli su un'altra rete.

Quando un host invia un messaggio ad un altro host in una rete diversa dalla propria, deve usare un router. L'indirizzo IP di destinazione sarà quello dell'host remoto, mentre il MAC address di destinazione sarà quello del router, in modo che il frame possa essere consegnato al router che provvederà ad instradare il pacchetto in esso contenuto. **Il default gateway** di un host è l'IP **dell'interfaccia del router connessa alla stessa rete locale dell'host.** Gli host conoscono l'IP del default gateway dalle impostazioni TCP/IP. Il MAC address del default gateway può essere ricavato tramite una richiesta **ARP (Address Resolution Protocol).**

Distribution Layer - Tabelle di routing e ARP

I router muovono dati tra reti locali e remote. Per svolgere questo compito usano sia la **tabella di routing sia la tabella ARP**

Le **tabelle di routing** non contengono indirizzi di host specifici, bensì gli indirizzi **di reti (locali o remote) ed i percorsi per raggiungerle, ossia le interfacce da usare per instradare i pacchetti ad esse destinati.**

Per evitare che pacchetti destinati a reti ignote vengano eliminati, gli amministratori di rete configurano una **default route**, ossia un'interfaccia sulla **quale instradare tutti i pacchetti diretti a reti non note.** Generalmente la default route connette ad un altro router che può instradare i pacchetti verso la rete di destinazione

I router mantengono **tabelle ARP per ogni rete alla quale sono connessi**. In questo modo, dopo aver determinato l'interfaccia di uscita, costruiscono il frame che ha come MAC di destinazione o quello dell'host di destinazione (nel caso la rete da raggiungere sia direttamente connessa) o quello di una altro router posto sul cammino per raggiungere la rete (non direttamente connessa)

Distribution Layer - Local Area Network?

Agli inizi del networking il termine **LAN (Local Area Network)** indicava una piccola rete che si estendeva su **una singola locazione fisica**. Oggi il termine si è evoluto e comprende anche reti costituite da centinaia o migliaia di host.

Il concetto chiave è che con il temine LAN ci si riferisce o ad **una singola rete locale** o a più reti locali interconnesse **poste sotto un unico controllo amministrativo.**

Le LAN utilizzano soprattutto protocolli Ethernet e wireless, caratterizzati da alti bit rate.

Virtual LAN (VLAN)

In una Switched Network, le **Virtual LAN (VLAN)**, vengono create per contenere i domini di broadcast e gruppi di host.

Una **VLAN è un dominio di broadcast** che separa logicamente un unico dominio di broadcast in più sottodomini di broadcast. Questo permette agli amministratori di rete di raggruppare gli utenti non solo in base alla locazione fisica!

Virtual LAN (VLAN)

Ogni VLAN deve essere considerata come una LAN separata. Le principali funzioni di una VLAN sono:

Contenere i domini di broadcast
Raggruppare i dispositivi in base alla loro locazione logica.

Per il passaggio da una VLAN ad un altra è necessario quindi un **dispositivo di Layer 3** (come avviene per le normali LAN che abbiamo conosciuto fino ad ora)

Per il raggruppamento logico vengono spesso utilizzati: *MAC Address, IP Address o le varie applicazioni applicazioni.*

Esistono due metodi di assegnazione ad una VLAN:

Metodo Statico (Port-based VLAN)
Metodo Dinamico (VLAN Membership Policy Server - VMPS)

Management VLAN

Il massimo numero di VLAN è limitato dal tipo di switch e dall'IOS (da 1000 a più di 4000). **Di Default però la VLAN 1 è la Management VLAN**.
Un amministrator può utilizzare l'indirizzo della vlan di management per poter configurare gli apparati (vi ricorda qualcosa l'ip sulla vlan 1?)

Inoltre la Management VLAN può essere utilizzata per scambiare informazioni di controllo (Duplex Mismatch, Speed Mismatch)

Quando una VLAN viene creata, bisogna assegnarli un numero e un nome.
Il nome non è obbligatorio ma è una Best Practices.

VLAN Commands

Per **creare una VLAN** basta utilizzare i seguenti comandi:

Switch(config)#vlan vlan_number
Switch(config-vlan)#name vlan_name
Switch(config-vlan)#exit

Per **assegnare una porta** ad una VLAN si utilizzano i seguenti comandi (di default tutte le porte appartengono alla VLAN 1)

Switch(config)#interface fa<slot_number>/<port_number>
Switch(config-if)#switchport access vlan vlan_number

Per **assegnare un range di porte** ad una VLAN si utilizza il seguente comando:

Switch(config)#interface range fa<slot_number>/start_of_range - end_of_range
Switch(config-if)#switchport access vlan vlan_number

Per **eliminare una VLAN** o per disassociare una porta utilizzare gli stessi comandi preceduti dalla keyword: **“no”**

VLAN Ports

Le porte devono possono essere configurate principalmente in 2 modalità:

Access Port: Una porta di Access può appartenere ad una sola VLAN. *Tipicamente a queste porte sono collegati gli host.* Se è collegato un Hub ad una porta di Access tutti i PC collegati all'Hub apparterranno alla stessa VLAN.

Trunk Port: Una porta in Trunk è una connessione *punto-punto tra due switch e/o un altro apparato di networking (es. Router)*. **I Trunk possono "far passare" più VLAN su un singolo link e permettono alle VLAN di essere raggiunte attraverso l'intera rete.**

L'**IEEE 802.1Q** è lo standard approvato per il **frame tagging**. Cisco ha sviluppato un protocollo proprietario chiamato **ISL (Inter-Switch Link)**. La maggior parte degli switch di fascia bassa non supportano l'ISL ma solo il dot1q.

Trunk Encapsulation

Tutte le porte degli switch di default sono in Access mode. Per configurare una porta in Trunk mode bisogna utilizzare i seguenti comandi:

Switch(config)#interface fa<slot_number>/port_number
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk encapsulation {dot1q | isl | negotiate}

La keyword "**negotiate**" è valida solo per gli switch di fascia alta e permette di negoziare il **protocollo** da utilizzare. Se un Trunk deve essere creato, questo può essere anche "negoziato" in modo automatico utilizzando il comando:

Switch(config-if)#switchport mode dynamic {desirable | auto}

Desiderable: il trunk viene stabilito solo se l'altro switch è configurato con auto, desiderable o trunk.

Auto: il trunk viene stabilito solo se l'altro switch è configurato con desiderable o trunk

VLAN Nativa

I trunk abilitano il traffico tra gli switches utilizzando una singola porta. Un Trunk configurato con **dot1q** da entrambi i lati, aggiunge ai frames un **tag aggiuntivo di 4bytes.**

Un determinato tipo di traffico che passa su un link 802.1Q senza VLAN IDè chiamato "untagged". Un esempio di traffico "untagged" è ad esempio il *Cisco Discovery Protocol (CDP), VTP (VLAN Trunking Protocol), etc...*

Per permettere questo "passaggio" c'è la necessità di stabilire una VLAN Nativa (in cui in traffico non viene taggato). Questo è possibile attraverso il comando:

Switch(config-if)#dot1q native vlan vlan-id

Inter-VLAN Routing

Come detto in precedenza, due dispositivi possono comunicare *solo se appartengono alla stessa VLAN*. Due dispositivi su VLAN differenti hanno bisogno di un *dispositivo a Layer 3 per potersi scambiare informazioni.* Quindi un Router dovrebbe avere un'interfaccia dedicata per ogni VLAN!!!!

Un altro metodo per poter far comunicare dispositivi su VLAN differenti è quello delle "**SubInterfaces**" con l'**Inter-VLAN Routing**

Questa feature divide logicamente una interfaccia fisica in più interfacce logiche, una per ogni VLAN. Per supportare le comunicazioni **Inter-VLAN** le sottointerfacce richiedono una particolare configurazione:

1) Devono appartenere alla stessa VLAN dei dispositivi che devono comunicare.
2) Il Link deve essere un Trunk

Una sottointerfaccia permette quindi ad ogni VLAN di avere un proprio **"Default Gateway" (raggiungibile a Layer 2).**

Questa configurazione è in genere chiamata **"Router-on-a-stick"**

Configurare le SubInterfaces

Dopo aver configurato la porta dello switch in Trunk dot1q basta procedere alla seguente configurazione:

Router(config)#interface fa0/0
Router(config-if)#no ip address
Router(config-if)#no shutdown
Router(config)#interface fa0/0.10
Router(config-subif)#encapsulation dot1q 10
Router(config-subif)#ip address 192.168.10.1 255.255.255.0

Per ogni interfaccia, prima di inserire l'indirizzo ip, va inserito il comando

encapsulation dot1q <vlan_id>

per indicare a quale VLAN quella sottointerfaccia appartiene.

Thank you.

clorofillaroma

www.clorofillaroma.it