Appunti di preparazione al Corso CISCO CCNA Routing & Switching

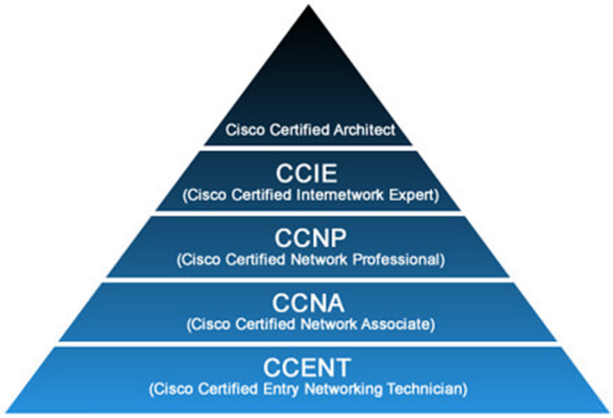
Dedico questo lavoro alla persona che ha reso/rende e spero continuerà a rendere la mia vita privata e professionale ricca e piacevole.
Grazie GRA di essere entrata nella mia vita e di s"u/o"pportarmi continuamente.
Grazie GRA di aver realizzato assieme una famigli bellissima.
Grazie anche ad Alex & Sara che sono ormai da anni il mio principale scopo nella vita.
Un grazie fondamentale a Papà e Mamma per il loro incoraggiarmi e supportarmi ancora nonostante il mio ego e la mia età non più quindicenne (grazie davvero).
Grazie mille anche a Mirco che con il suo "ma sa' t'in frega, lascia perdere" mi riporta sulla retta via di pensiero (mitico BRO.)
Grazie alle nonne (anche se ormai non ci sono più), perché con i loro detti hanno sempre mantenuto acceso il mio lumicino della continua voglia d'imparare.

Infine grazie ai BOSS Paolo ed EMA che continuano ad incentivarmi e spronarmi nel lavoro offrendomi sempre nuove e più complesse sfide.

Modulo 1

Info:

Le certificazioni Cisco si riassumono con un diagramma piramidale (come da figura accanto). Ogni certificazione richiede come propedeuticità quella sottostante



I siti di riferimento per il corso sono:

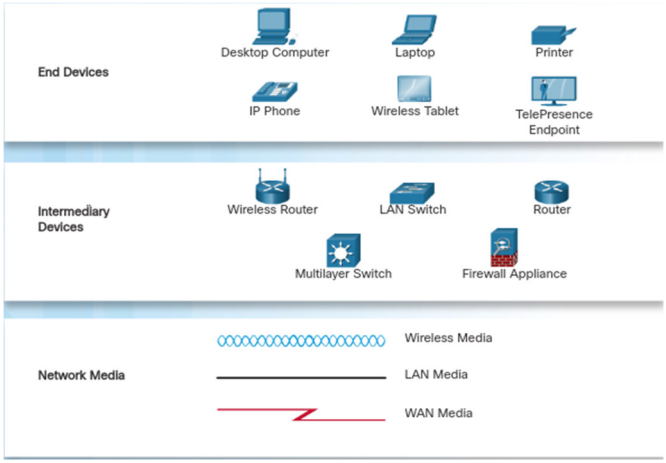
http://www.netacad.com	→	Contiene Slide e la ClassRoom creata quando inizia il corso (la ClassRoom dura 6 mesi, poi si chiude automaticamente)
http://www.cisco.com	→	Sito istituzionale CISCO e contiene tutte le info sulle certificazioni
http://www.pearsonvue.com/cisco	→	Sito sul quale bisogna registrarsi per poter sostenere l'esame

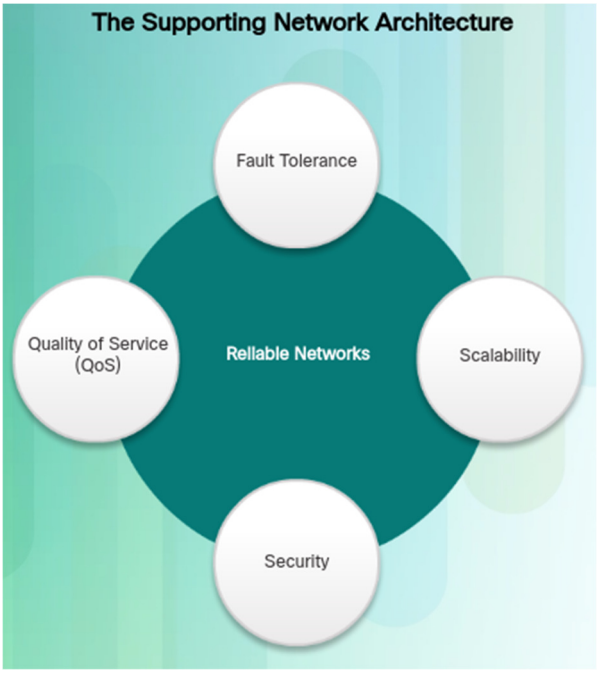
a) Il corso che seguiremo sarà diviso in 4 moduli, 2 riguarderanno il CCENT, e 2 il CCNA
b) Ogni modulo ha un test finale da svolgere in aula, che risulta fondamentale da passare con almeno il 70% di risposte corrette per poter accedere al modulo successivo. Se si passano tutti i test con più del 75% si avrà uno sconto finale sul costo dell'esame di certificazione, **con più si è bravi, meno si paga**.

Comunicazioni di rete:

Client → Server	Comunicazione tra 2 apparati che comunicano a livello differente, uno offre un servizio, l'altro lo utilizza. Es. le comunicazioni HTTP
Peer2Peer	Comunicazione tra apparati allo stesso livello, dove uno offre un servizio A e richiede un servizio B e l'altro viceversa Es. mio: la condivisione torrent Es. CISCO le stamapnti condivise tra pc

Indicazione su come leggere gli schemi del corso





Per creare una rete ad alta affidabilità devono essere 4 punti ben bilanciati
Fault Tolerance = Ridondanza

Il **QoS** funziona con il **tagging** del pacchetto, e poi viene gestito dal **queuing** dopo aver verificato la fiducia del tag stesso.

Tutta la gestione delle applicazioni nel cloud hanno iniziato a predisporre anche un minimo di sicurezza di utilizzo anche in locale, utilizzando l'**EDGE Computing**, ossia mantenere una base di funzionamento anche in locale nel caso in cui la connessione alla rete venga a mancare

1.3.1.3 Lab - Researching Converged Network Services.pdf

1.4.4.3 Lab - Researching IT and Networking Job Opportunities.pdf

1.5.1.1 Class Activity - Draw Your Concept of the Internet Now.pdf

2.0.1.2 Class Activity - It is Just an Operating System.pdf

Switch: è un'hardware semplice e veloce con tecnologia ASIC che interconnette lo stesso tipo di porte (Es. tutte porte LAN)
Router: è un'hardware più complesso, lavora a livello software perché gestisce più tipo di porte (LAN, doppino, ecc…)

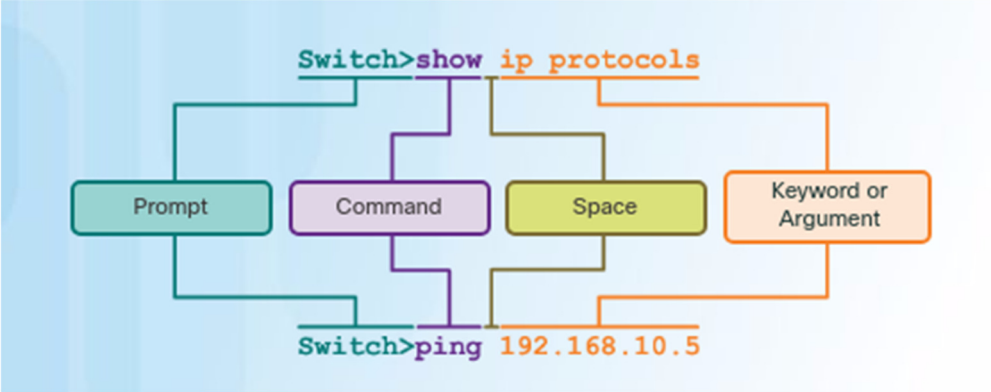
Per uniformare e semplificare la programmazione degli apparati, CISCO è stata la prima ad introdurre un sistema operativo (IOS) comune tra l'hardware e l'interfaccia utente, che risulterà quella che impareremo a gestire.

Come accedere agli apparati:
Consolle: è una porta fisica, che non viene usata per il traffico, è dedicata solo alle configurazioni e si gestisce tramite un appostio cavo RS232 → RJ45
AUX: è una porta fisica simile in tutto e per tutto alla porta Consolle (non sempre è presente), e generalmente viene usata per avere la possibilità di effettuare configurazioni da remoto
Telnet: connessione di rete non cifrata
SSH: connessione di rete cifrata

Tutti i metodi di accesso agli apparati, convergono alla shell base che si chiama "User Exec" ed è indicata con > (come il $ nel mondo linux per intenderci)
Per aumentare i miei privilegi devo digiatare il comando **enable** ed al posto del > comparirà il #, ora ci troveremo nella shell denominata "Privileged Exec"
Ora per poter iniziare la configurazione dell'apparato dovrò dare il comando **configure terminal** e mi troverò nel terminale di "Global Configuraion".
La parte di configurazione si organizza ad albero (tree) a scendere da qui in poi, per cui per effettuare la configurazione delle varie voci bisogna spostarsi dentro alla voce da configurare e poi risalire (**exit**) e rientrare a sua volta nella voce successiva. (**NB: non è obbligatorio, ma è la best practice per evitare errori**).
ATTENZIONE: i vari comandi che lanciamo sono subito operativi e vengono subito eseguiti sull'apparato.

Negli apparati CISCO, vi sono 2 tipi di configurazioni:
startup-config: memorizzata in NVRAM, è quella che parte all'avvio dell'apparato ed appena avviato l'apparato è quella che coincide con l'altra configurazione
running-config: memorizzata in RAM, è la configurazione che sta girando sull'apparato in questo momento.

Struttura dei comandi:



Comodità nel CLI (command line interface)

- ➢ Se il comando che viene dato è univoco, anche se non completo, il sistema lo riconosce ugualmente. Es: # **conf t** viene processato come # **configure terminal**
- ➢ Il tab completa il comando
- ➢ Il ? Nella digitazione del comando o all'inizio della digitazione mi elenca le opzioni di digitazione (come il doppio tab in linux)
- ➢ Le frecce in su ed in giù richiamano i vecchi comandi
- ➢ Se per caso digito un comando che non esiste il sistema prova a risolverlo tramite la rete, e fino a quando non và in timeout non mi sblocca la CLI, per cui se lancio un comando sbagliato e non voglio attendere il timeout, basta premere i tasti [CTRL]+[ALT]+[6]
- ➢ Anteporre il no all'ultimo comando dato ne elimina l'esecuzione (sempre che sia fattibile)

Es.: il comando **no write**, dopo aver dato **write** è inutile

Impostare ora e data. Da "Privileged Exec" lanciare il comando: **clock set 20:50:00 19 Sep 2017**

2.1.4.6 Packet Tracer - Navigating the IOS.pdf

Configurazione base consigliata da fare su ogni apparato, a partire dalla "Global Configuraion":

A) Cambiare hostname

hostname nome_da_assegnare

B) Impostare la password

- ✓ console:

Entrare nel ramo di configurazione della console: **line console 0**
Impostare la password: **password mia_pwd**
Impostarne l'avvio: **login**
Tornare al ramo superiore: **exit**

- ✓ AUX:

Entrare nel ramo di configurazione della console: **line console 1**
Impostare la password: **password mia_pwd**
Impostarne l'avvio: **login**
Tornare al ramo superiore: **exit**

- ✓ Telnet: essendo predisposte fino a 16 connessioni telnet, si può decidere di configurarne una alla volta o tutte assieme. Per configurarle tutte procedere come segue:

Entrare nel ramo di configurazione apposito: **line vty 0 15**
Impostare la password: **password mia_pwd**
Impostarne l'avvio: **login**
Tornare al ramo superiore: **exit**

- ✓ Per abilitare il login per entrare in "Privileged Exec", abbiamo 2 modalità:
  - I. **enable password mia_pwd** questo comando mi abilita la password, ma quando vado ad esportare il file di running_config o di startup-config la password è in chiaro
  - II. **enable secret mia_pwd** questo comando mi abilita la password e me la cifra. Nel running-config o nello startup-config nella riga relativa alla password c'è un 5 (o un'altro numero) e server a segnalare al sistema che la password è cifrata.

  Se per caso mi sbaglio e le imposto entrambe, il sistema dà la precedenza al secret

NB: per disabilitare la password basta mettere no davanti al comando senza la password, nell'apposito ramo del tree

IMPORTANTE: per abilitare la funzione che imposta tutte le password cifrate dentro ai file di configurazione, dare il comando: **service password-encryption**

C) Impostare il BANNER di pre-LOGIN (è il disclaimer che compare prima del login dell'apparato):

Avviare la modalità per scrivere il messaggio: **banner motd #**
Terminare il messaggio: **#**
NB: il carattere # infica l'inizio e la fine del messaggio
NNB: non è obbligatorio utilizzare il carattere #, ma lo si consiglia in quanto è uno dei caratteri meno utilizzati, l'importante è ricordarsi che il carattere che viene utilizzato dopo la parola motd è anche quello che terminerà l'inserimento del messaggio di banner

Per visualizzare le configurazioni esistenti sull'apparato dare i comandi:
show running-config→ per visualizzare la configurazione attuale
show startup-config → per visualizzare la configurazione di avvio

Per copiare le configurazioni in IOS, considerando di avere:
A) Server TFTP B) running-config C) startup-config
il comando da dare nella "Privileged Exec" risulta essere: copy X Y
dove X ed Y sono A, B o C.
NB: se Y è running-config non tutti i comandi verranno processati, come ad esempio la password di enable in cui secret vince su password, infatti in questo caso aggiunge la riga, ma risulta inutile

Sempre nel "Privileged Exec" il comando **erase startup-config** ripristina l'apparato alle impostazioni di fabbrica

2.1.4.7 Lab - Establishing a Console Session with Tera Term.pdf
2.1.4.6 Packet Tracer - Navigating the IOS.pka
2.2.3.4 Packet Tracer - Configuring Initial Switch Settings.pdf
2.2.3.4 Packet Tracer - Configuring Initial Switch Settings.pka

Configurazione ip di:
Router:

configure terminal	
interface g0/0	oppure un'altra interfaccia, ma nei router l'ip bisogna assegnarlo ad una specifica porta
ip address 192.168.1.1 255.255.255.0	
no shutdown	serve per attivare l'interfaccia, poiché le interfacce sono sempre spente per sicurezza
exit	per tornare nel "Privileged Exec"
copy run start	**per salvare la configurazione appena effettuata**

Switch:

configure terminal	
interface vlan 1	oppure un'altra interfaccia virtuale
ip address 192.168.1.2 255.255.255.0	
no shutdown	serve per attivare l'interfaccia, poiché le interfacce sono sempre spente per sicurezza
exit	**NB:** Negli switch il gateway si configura nel "Global Config"
ip default-gatweay 192.168.1.1	
exit	per tornare nel "Privileged Exec"
copy run start	per salvare la configurazione appena effettuata

Importante, negli switch con porte Poe, se voglio disattivare la funzione PoE, prima devo andare nella configurazione della porta, poi devo dare il comando:
power inline never
mentre per rimetterla
no power inline never

2.3.2.5 Packet Tracer - Implementing Basic Connectivity.pdf
2.3.2.5 Packet Tracer - Implementing Basic Connectivity.pka
2.3.3.3 Lab - Building a Simple Network.pdf
2.3.3.4 Lab - Configuring a Switch Management Address.pdf
2.4.1.2 Packet Tracer - Skills Integration Challenge.pdf
2.4.1.2 Packet Tracer - Skills Integration Challenge.pka

PROTOCOLLI

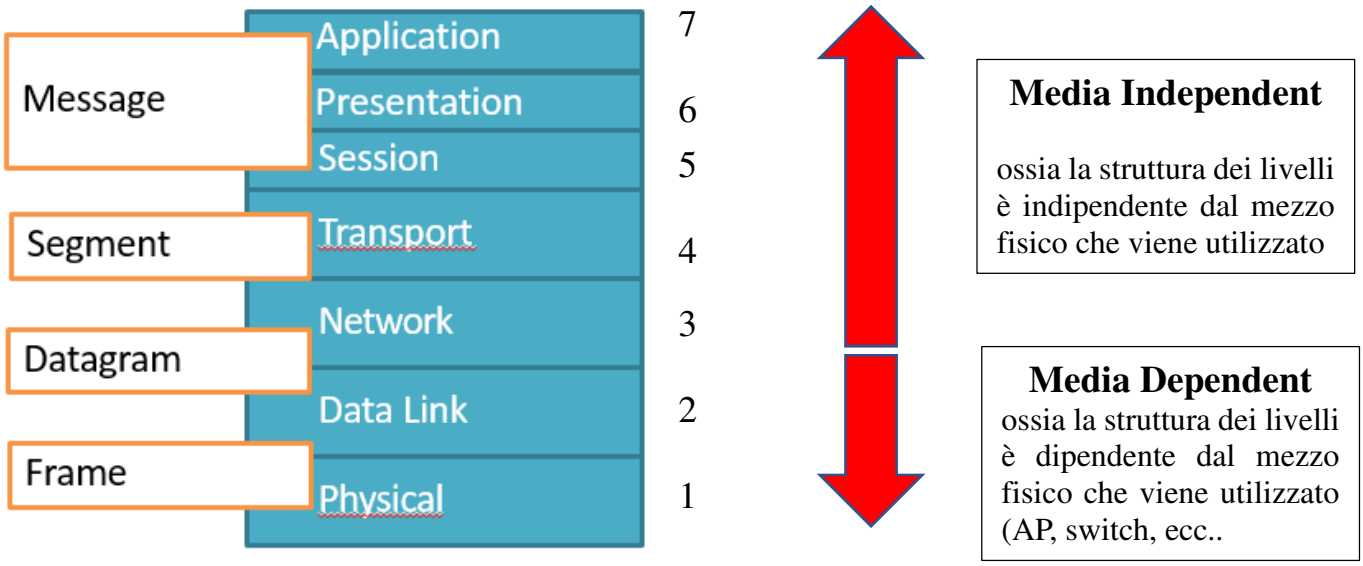
Ogni livello fornisce il proprio servizio effettuando determinate azioni all'interno del livello
Ogni livello fornisce il proprio servizio in modo trasparente agli strati superiori
Ogni livello utilizza i servizi dello strato immediatamente inferiore
Ogni variazione dell'implementazione di un livello non implica una modifica degli strati superiori/inferiori (*modularità*)

PRO:

- permettere a differenti *vendor* di inter-operare
- dividere il processo di comunicazione in componenti piccoli e più semplici
- favorire la standardizzazione dei componenti di rete
- definire le funzioni di ogni livello →incoraggia la standardizzazione industriale
- permettere la comunicazione tra diversi tipi di hw/sw
- impedire che i cambiamenti apportati ad un livello modifichino anche gli altri

CONTRO:

- possibilità di duplicazione di alcune funzionalità in livelli differenti



7) Application Layer:

- Agisce come interfaccia tra i programmi applicativi
- Stabilisce se ci sono sufficienti risorse disponibili
- Esegue la codifica delle applicazioni (http, ftp, ecc…)

6) Presentation Layer:

- Presenta i dati all'Application Layer
- Traduzione dei dati, ovvero codifica del formato (ascii, cifratura, ebcdic..)
- Funzioni di conversione

5) Session Layer:

- Discrimina sessioni (mantenendo separati i dati di applicazioni diverse). Instaura, gestisce e chiude sessioni tra le entità del presentation layer (Per intenderci è quello che decide quanto fare grandi i pacchetti)
- Fornisce uno scambio di info di controllo tra device/nodi di rete
- Offre tre modalità di comunicazione tra sistemi e server: simplex, half duplex e full
- duplex

4) Transport Layer:
- ➢ Fornisce trasporto end-to-end (connessione logica tra host Mitt e host Dest), Reordering dei pacchetti
- ➢ Segmentation (divisione dei pacchetti)
- ➢ Multiplexing, separa il traffico dei livelli superiori
- ➢ Error Correction, se un qualche pacchetto è corrotto ne richiede il trasferimento

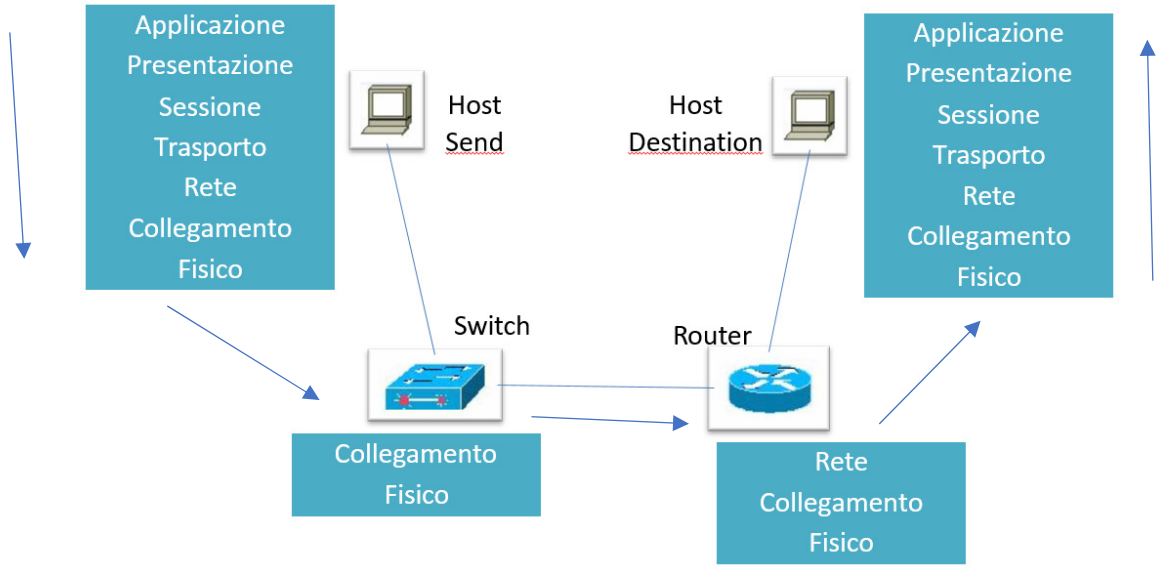
3) Network Layer:
- ➢ Forwarding: quando un router riceve un pacchetto, lo deve trasferire sull'appropriato *link* d'uscita
- ➢ Routing: il livello di rete deve determinare il percorso, attraverso algoritmi specifici, che i pacchetti devono seguire
- ➢ Per inoltrare i pkt i router si avvalgono della **forwarding table** (database), che contiene network *address, interface, metric* (metric = distanza verso una rete remota)

2) Data Link Layer:
- ➢ Fornisce la trasmissione fisica dei dati e gestisce gli errori di notifica, la topologia di rete ed il controllo di flusso (formato frame: ethernet, frame relay, ppp..)

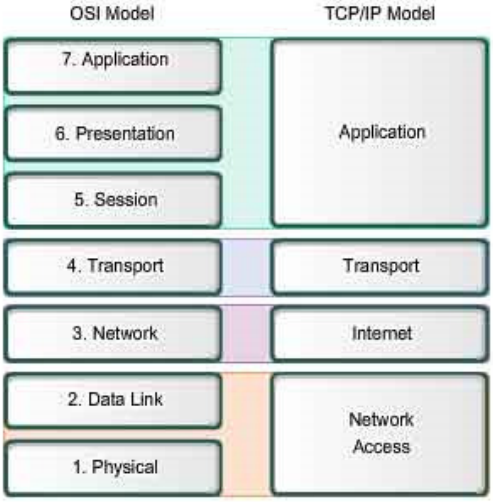
1) Physical Layer:
- ➢ Specifiche elettriche, meccaniche, procedurali e funzionali x attivare, mantenere, disattivare un link fisico
- ➢ Connector, Frequency, Channel, ecc…

Come avviene la comunicazione?

La comunicazione avviene grazie a protocolli, ossia insiemi di regole e convenzioni seguite dai computer che intendono comunicare tra loro (protocolli formati da una sintassi, una semantica e dalle conseguenze della temporizzazione). I protocolli sono raggruppati in blocchi (protocol stack), e ogni livello è caratterizzato da una service interface (interfaccia col livello superiore) e da una p2p interface (interfaccia col pari livello nel calcolatore di destinazione). Mentre la comunicazione concettuale avviene quindi tra peer entity (tra sorgente e destinazione), la comunicazione effettiva è indiretta: il messaggio proveniente dal livello superiore della sorgente deve passare tutti i livelli sottostanti, incapsulato con i rispettivi header, passare il mezzo fisico, per poi essere disassemblato seguendo il procedimento inverso nella destinazione. A ciascun livello, il messaggio si compone di un PCI (Protocol Control Information, ossia un header) e da un SDU (Service Data Unit, ossia l'informazione), per formare il PDU (Protocol Data Unit).

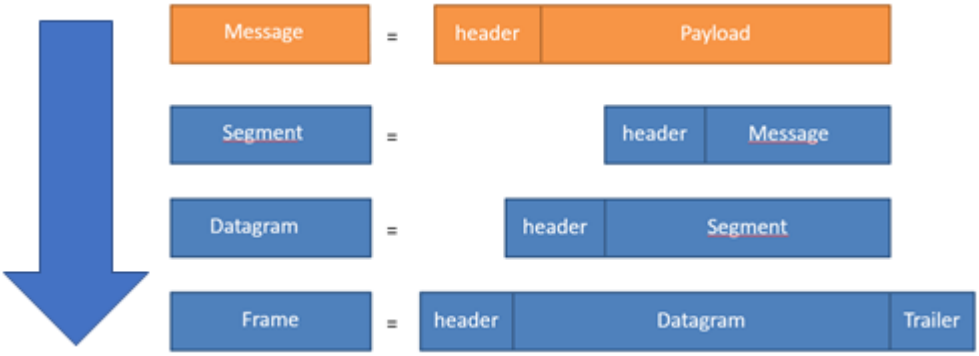


Nell'Host Send l'informazione viene convertita in fisica ed inviata, nell'Host Destination l'informazione arriva fisica e viene decapsulata fino ad essere l'etta ed interpretata.
Il protocollo realmente utilizzato dalle reti, è il TCP/IP che prevede l'accorpamento di alcuni livelli dell'ISO/OSI come se fossero un unico livello.



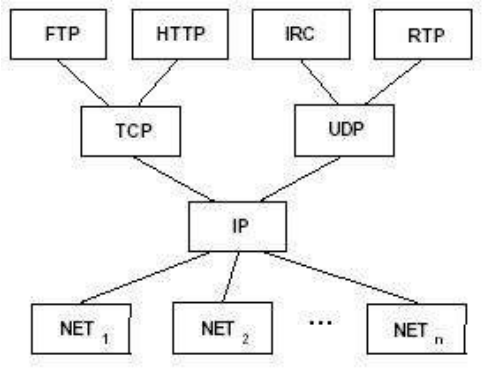
The key parallels are in the Transport and Network layers.

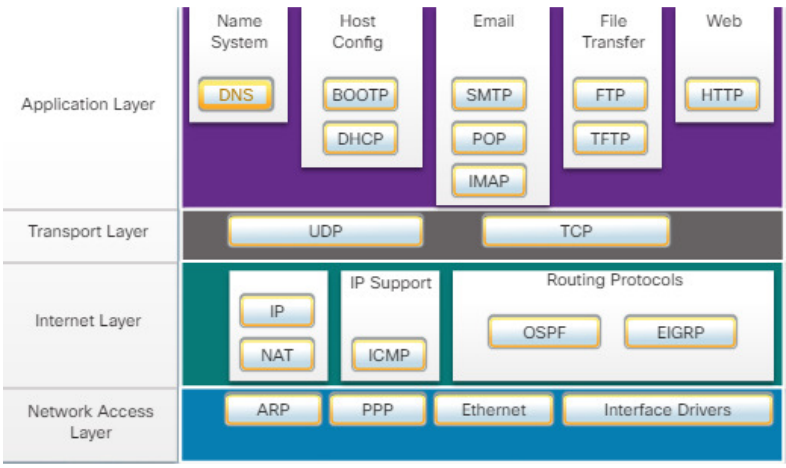
Gli Incapsulamenti tra un livello e quello sottostante funzionano come nel seguente grafico

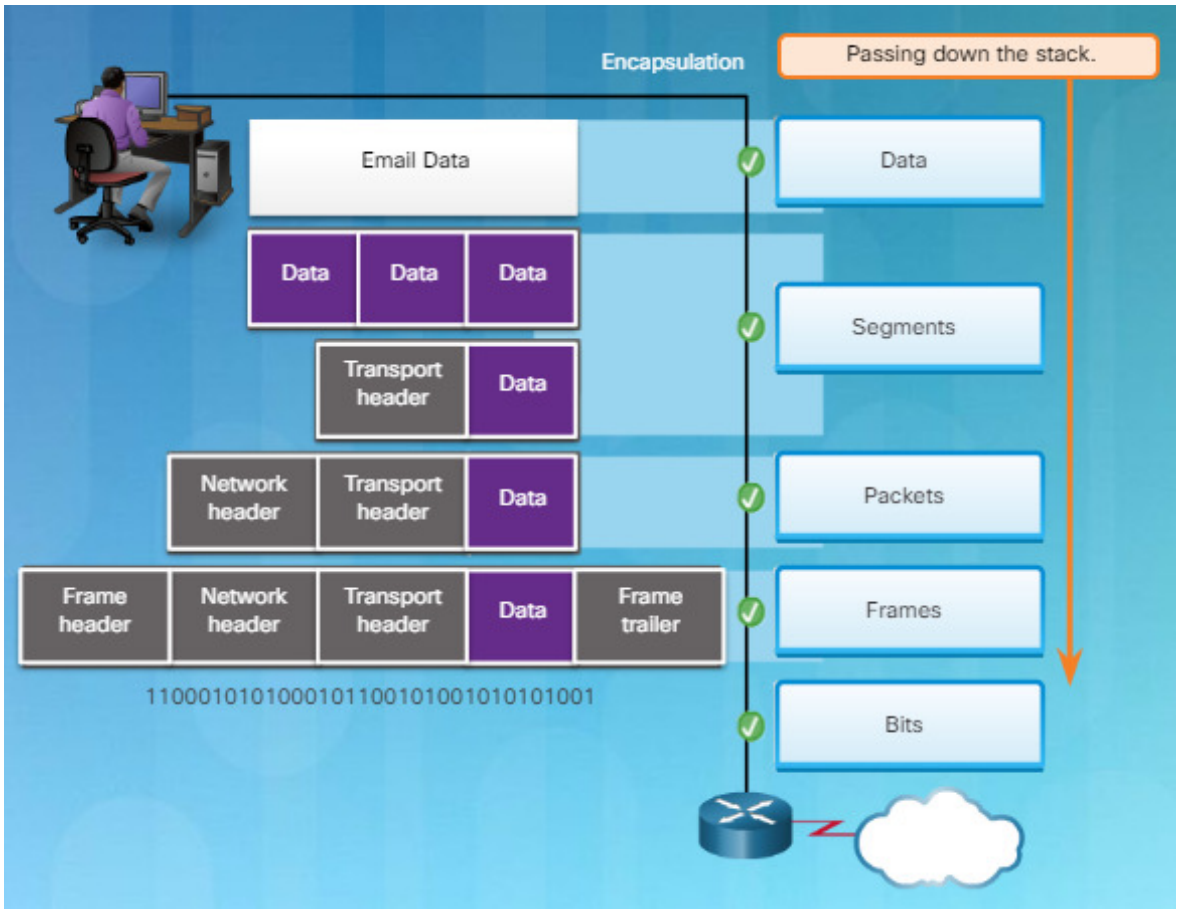


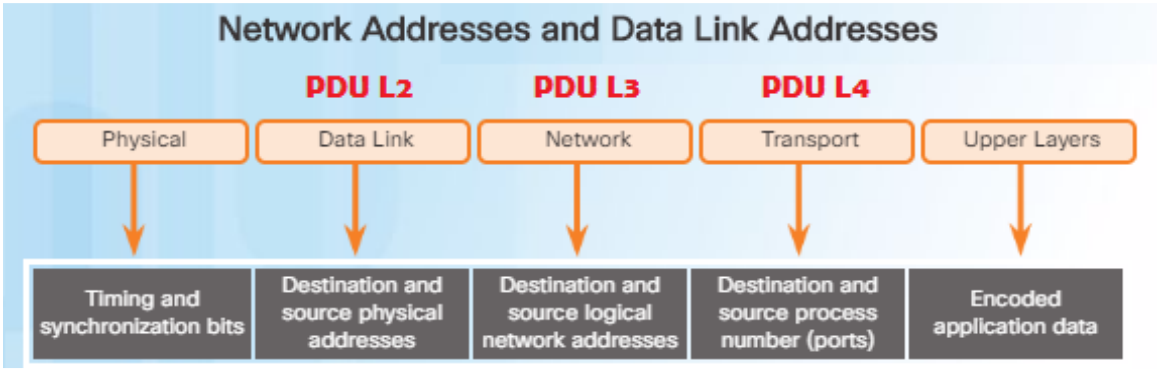
Il **Message**, viene incapsulato aggiungendo un header e passa agl livello sottostante, che aggiunge un header, prende il nome di **Segment** e lo passa al livello sottostante, che a sua volta aggiunge un header, diventa **Datagram** e lo passa al livello sottostante che aggiunge un header ed un trailer, cambia nome diventando **Frame** e lo passa al mezzo fisico che lo invia.

Il passaggio dei livelli nelle reti risulta essere riassumibile dal seguente schema:

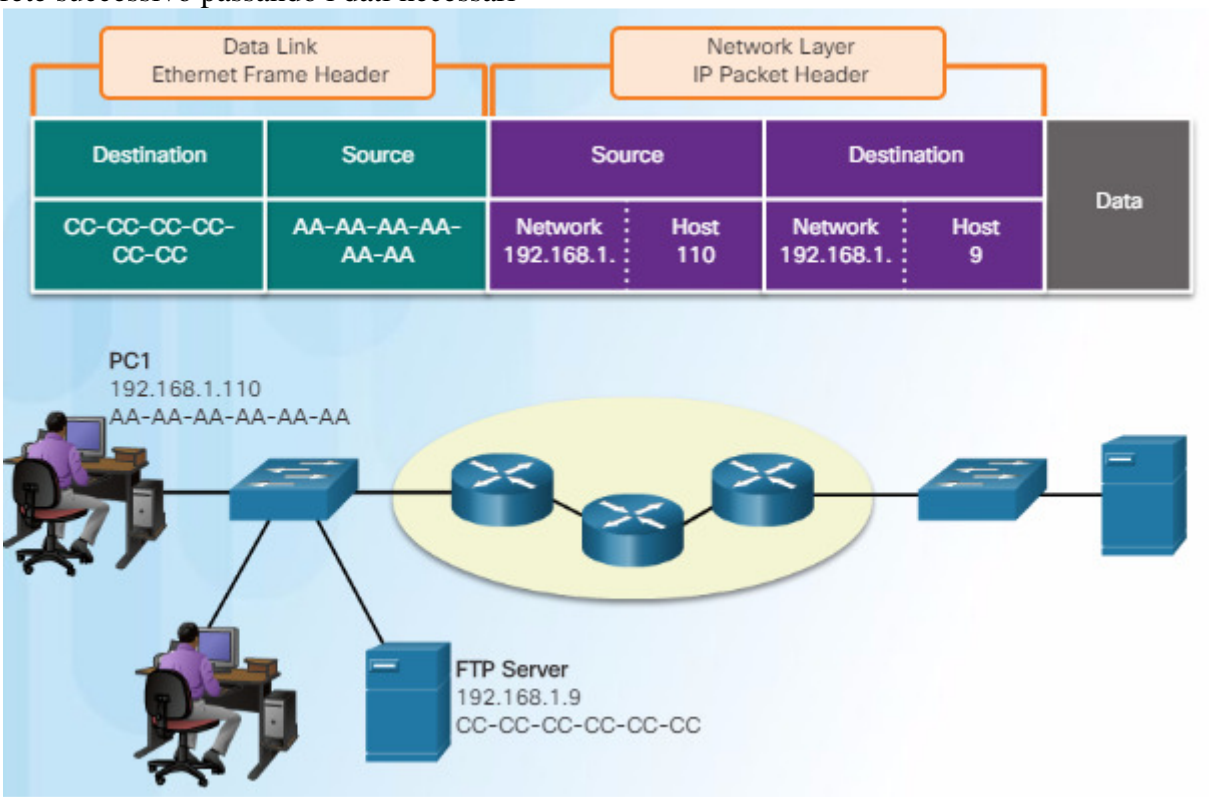








Andando più in dettaglio, ogni header aggiunge i suoi parametri per poter attraversare il dispositivo di rete successivo passando i dati necessari



NB: nell'header del Layer2 sarà contenuto in un apposito campo la descrizione del tipo di protocollo IP da utilizzare (v4 o v6).
Il FRAME, lavora tra nodi, ossia lavora all'interno del **broadcast domain**, mentre tra un nodo e quello successivo viene ri-creato (Next Layer3 Hop)
Il Broadcast Domain ha un riscontro nel livello IP Network, più precisamente nella netmask
L'unico altro caso in cui il FRAME viene distrutto e ri-creato è se abbiamo un media change (es. da cavo a wi-fi).
Il BROADCAST agisce a Layer2

FINE CAPITOLO 3

A livello Network Access, ossia quando metto il dato sul MEDIA, ho bisogno di 3 funzioni fondamentali:

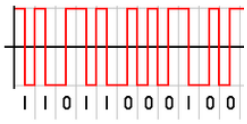
Nome	4B	5B	Descrizione
0	0000	11110	hex data 0
1	0001	01001	hex data 1
2	0010	10100	hex data 2
3	0011	10101	hex data 3
4	0100	01010	hex data 4
5	0101	01011	hex data 5
6	0110	01110	hex data 6
7	0111	01111	hex data 7
8	1000	10010	hex data 8
9	1001	10011	hex data 9
A	1010	10110	hex data A
B	1011	10111	hex data B
C	1100	11010	hex data C
D	1101	11011	hex data D
E	1110	11100	hex data E
F	1111	11101	hex data F
I	-NONE-	11111	Idle
J	-NONE-	11000	SSD #1
K	-NONE-	10001	SSD #2
T	-NONE-	01101	ESD #1
R	-NONE-	00111	ESD #2
H	-NONE-	00100	Halt

Physical components: il componente fisico che è l'hadrware vero e proprio, quello che posso toccare

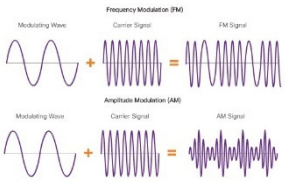
Encoding: che è il metodo per convertire il mio stream di dati in bit da inviare

Esempi possono essere

4b5b: lavora mappando gruppi di 4 bit in gruppi di 5. Siccome ci sono 32 possibili combinazioni usando 5 bit e solo 16 usandone 4, i 16 gruppi di 5 bit col maggior numero di transizioni sono usati per fornire più transizioni possibili. 4B5B garantisce almeno una transizione per blocco (ingresso di 4 bit / uscita di 5) il quale permette al segnale di essere scoperto. Sfortunatamente l'uso di 5 bit per rappresentarne 4 implica che per trasmettere i dati abbiamo bisogno di una larghezza di banda più grande del 25%



Manchester: Ogni bit viene trasmesso in un intervallo di tempo di bit predefinito (es. se devo fare la nota DO per 100 secondi, posso farla in continuo oppure posso fare 100 DO da 1 secondo. Nel secondo caso anche per me che non ho il cronometro risulterà più facile tener controllato i 100 secondi, mi basta controllare che vengano fatti 100 DO)



- Signaling: è il modo di rappresentazione dei bit sul mezzo, infatti vi sono vari modi di trasmissione, come la strasmissione AM ed FM (vedi figura)

Caratteristiche del Layer2

- Bandwidth: è la capacità di un'interfaccia di gestire i bit/secondo ed è caraterrizzata dalle proprietà del mezzo e dalla tecnologia del segnale
- Throughput: è la reale velocità del traffico tra HOST ed è fortemente dipendente dalla situazione attuale della rete
- Overhead: è il tempo all'interno della trasmissione dei dati che si impiega per "establishing session, acknowledgments and encapsulation"
- Goodput: è l'informazione (dato) che ti ho mandato, diviso il tempo che ho impiegato a mandarti.

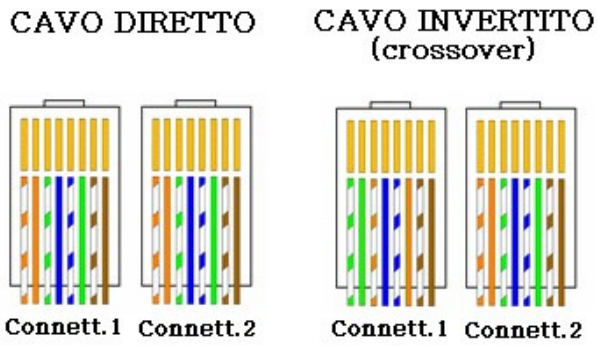
  Goodput = Throughput - Overhead

Tipi di cavi (descrizione):

- UTP - Unshield Twisted-Pair: sono i cavi più utilizzati e terminano con un connettore RJ45. Sonsistono di 4 coppie di cavi tra loro più o meno intrecciati (twisted). I differenti livelli di intreccio tra le coppie servono per ridurre al massimo le eventuali interferenze.
- STP - Shield Twisted-Pair: simili ai cavi UTP dai quali ereditano le caratteristiche migliorando però la schermatura. Di contro sono cavi più spessi e di più difficile installazione.
- Coaxial: in Italia viene utilizzato principalmente per le trasmissioni televisive

Cablaggio RJ45

- ✓ Straight (dritto): esistono 2 standard (T568B e T568A) ed entrambi i plug hanno lo stesso orientamento
- ✓ Crossover: è il cavo che si utilizza (utilizzava) per connettere device simili (es: pc con pc, router con router, switch con switch, ma attenzione anche per connettere pc con router…)
- ✓ Rollover: vecchio cavo cisco con tutti i cavi incrociati

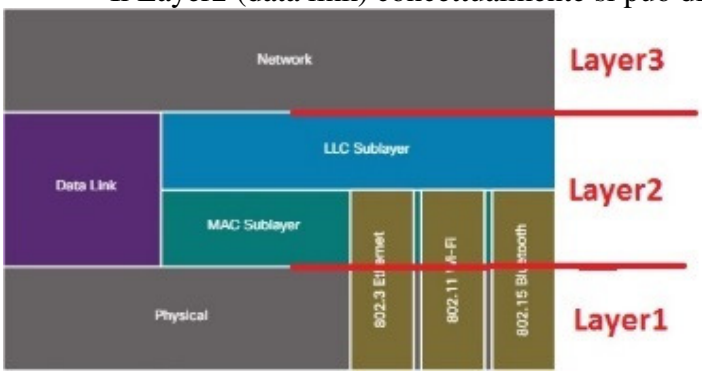


Per specifica, l'Ethernet Legacy (lo standard) sui pin 1 e 2 trasmette e sui pin 3 e 4 riceve per cui basandomi su questo concetto posso realizzare i cavi Crossover e Strainght.
Per ridurre al minimo i problemi di rete ed per evitare che ci si possa sbagliare a collegare in rete gli apparati dello stesso tipo con un cavo straight, hanno creato le interfacce MDIX che rilevano il tipo di apparato che trasmette e loro si mettono nella modalità di ascolto migliore

Scrivi appunti sui cavi di fibra (non necessari, ma potrebbe essere interessante)
Slide 4.2.3.3 ecc..

Appunti sul wifi
Lab e slide 4.2.4.4

Il Layer2 (data link) concettualmente si può dividere in 2 sottolivelli



- Liv. MAC (ieee 802.2): può cambiare a seconda del mezzo fisico, è la parte del livello 2 inferiore, cioè quella che va a mascherare la parte fisica
- Liv. LLC (ieee 802.3): è la parte del livello 2 che offre servizi al livello 3. La sua funzione quindi è quella di definire il tipo di protocollo trasportato (es. IPv4 o IPv6)

La topologia della rete è necessaria per capire come strutturare la rete al meglio e la si può "visualizzare" in 2 modi:
Physical topology: si riferisce alle connessioni fisiche ed identifica i device e l'infrastruttura. Tale topologia è punto-punto o a stella
Logical topology: si siferisce alla via di trasmissione e consiste in una connessione virtuale tra i nodi

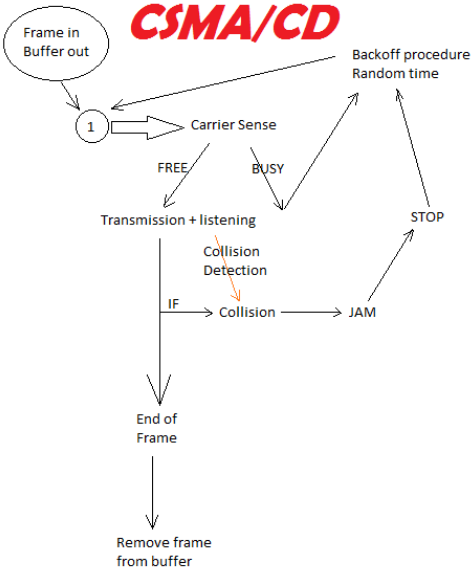
La trasmissione nella LAN avviene in due modalità:

- ✓ Half-Duplex: o trasmetto o ricevo
- ✓ Full-Duplex posso sia trasmettere che ricevere in contemporanea

Con la condivisione del mezzo di trasmissione (shared media), vi sono 2 metodi di controllo del mezzo:

- Contention based: tutti i nodi trasmettono in half-duplex e competono per l'uso del mezzo
- Controlled: ogni nodo ha un proprio tempo per utilizzare il mezzo

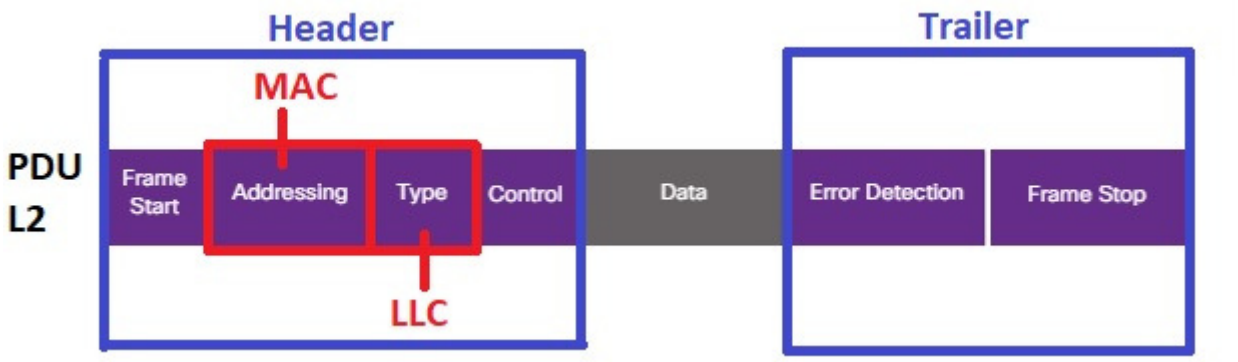
Il processo che governa il sistema di dati che girano all'interno della LAN si riassume in CSMA/CD (Carrier sense multiple access with collision detection)



- CSMA/CD: Il dispositivo che vuole iniziare una trasmissione controlla il mezzo per la presenza di un segnale dati. Se un segnale di dati è assente e quindi il mezzo è libero, il dispositivo trasmette i dati. Se vengono rilevati i segnali che mostrano un altro dispositivo che stava trasmettendo contemporaneamente, tutti i dispositivi smettono di inviare e riprovano in seguito dopo un tempo random.

- CSMA/CA: Carrier sense multiple access with collision avoidance è la metodologia di controllo del mezzo nel wifi. Il dispositivo che vuole trasmettere esamina il mezzo per la presenza di un segnale di dati. Se il mezzoè libero, il dispositivo invia una notifica attraverso il mezzo della sua intenzione di utilizzarlo (inviando un segnaleRTS). Una volta che riceve uno spazio su cui trasmettere (riceve un segnale CTS), il dispositivo invia i dati. Come contro riceve un incremento di overhead (establishing session, acknowledgments and encapsulation)

NB: l'access-point è un media half-duplex poiché l'onda radio è un mezzo condiviso
Quindi nel CDMA, il tempo frame deve essere < di 2 volte il tempo che il frame impiega ad andare da A a B.
$T_{frame} < 2T_{A-B}$
Per convenzione si impone che 64byte $< 2T_{A-B}$
Max MTU 1518Byte, Min MTU 64Byte. Se la collisione avviene prima del 64°Byte ho una **collision**, se avviene dopo ho una **late collision**.



Frame start/stop: usati per indicare l'inizio ed il limite del frame
Il Frame stop
Addressing: indica il sorgente e la destinazione all'interno del mezzo
Type: identifica il protocollo di layer3 che stò trasportando
Control: identifica un carattere di controllo che viene utilizzato nel QoS (quality of service)
Data: contiene il packet header, il segment header ed il dato)
Error Detection: questa parte è utilizzata per capire se il frame trasmesso è corrotto oppure no
FCS (frame check sequence) è un valore di un'operazione di controllo che viene effettuata tenendo in considerazione anche l'header. La dimensione dell'FCS è 4Bytes, per cui 2 combinazioni di frame differenti avranno lo stesso valore di FCS.
(NB: non è a questo livello che in caso di frame corrotto si richiede la ri-trasmissione)

Class activity 4.5.1.1

FINE CAPITOLO 4

Class activity 5.0.1.2
Esercizi 5.1.1.7 pdf

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

L'Ethernet MAC Address è formato da 48 bit, divisi in sei coppie a loro volta divise da 4 bit a valore, in modo da poter creare una corrispondenza biunivoca tra la rappresentazione binaria e quella esadecimale come in tabella accanto.
In modo tale da poter rappresentare correttamente in valore MAC con 12 cifre esadecimali

Il MAC Address a sua volta segue una standardizzazione che prevede di assegnare i primi 24 bit univoci al produttore, infatti sono detti OUI (Organizationally Unique Identifier). Gli ultimi 24 bit invece sono assegnati dal produttore (Vendor Assignement) ai prodotti realizzati in modo tale che (in linea teorica) ogni prodotto abbia un MAC Address univoco.
Degli ultimi 24bit, in realtà i produttori assegnano gli ultimi 23, in quanto il primo dei 24 a disposizione da assegnare agli apparati per convenzione viene impostato a 0 per consentire agli utilizzatori di poter fare prove e configurazioni sugli apparati.
I MAC Address sono solitamente rappresentati nel seguente modo
AA:AA:AA:AA:AA:AA oppure AA-AA-AA-AA-AA-AA

Vi sono 3 tipi di traffico MAC, ed al Layer2 per identificare il tipo di traffico si visualizza il destination MAC Address.
Broadcast: dove il traffico arriva a tutti gli apparecchi collegati. Tutti i bit sono a 1.
Destination MAC Address = FF:FF:FF:FF:FF:FF
Unicast: MAC Address è l'esatto MAC Address del destinatario
Destination MAC Address = 01:5D:2E:0F:A3:09
Multicast: per la creazione del MAC Address di destinazione si compone di una prima parte fissa, ossia 01:00:5E (per l'IPv4) oppure 33:33 (per l'IPv6), mentre per la seconda parte, si và a leggere dei dati dal layer superiore, e più precisamente si vanno a leggere gli ultimi 24bit dell'indirizzo ip di destinazione e li si vanno a scrivere negli ultimi 23 bit del MAC Address
Destination MAC Address = 01:00:5E:XX:XX:XX dove XX:XX:XX dipende dall'ip di destinazione

Esercizio 5.1.2.8 pdf

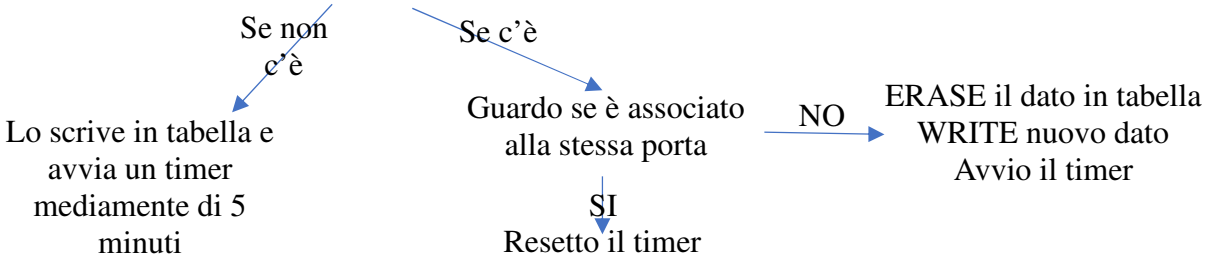
Se l'apparato in cui transita il mio frame non termina il broadcast domain non è il destinatario del Layer2 MAC Address Destination.
Il MAC Address di destinazione se è quello del router vuol dire che il destinatario finale è il router stesso oppure che il destinatario finale non è nel mio broadcast domain.

Ok, abbiamo idea di cosa sia un MAC Address, ma come funziona uno switch?

Lo switch utilizza i MAC Address per prendere le "forwarding decisions".
Lo switch ha un collision domain su ogni interfaccia ed è caratterizzato da **Selective Forwarding** e **Buffer**.
Lo switch si basa du MAC destination e MAC source per creare una TABLE MAC, ossia una tabella dove ha registrato i MAC che la attraversano e da che interfaccia escono.

Ma come funziona?

Inizia con una funzione di Learning (dynamic or everytime), analizza il sorgente del frame che gli arriva ed in una tabella registra il MAC Source e la porta dal quale ha ricevuto il frame.
Quando arriva un nuovo frame guarda la tabella



NB: posso avere più MAC Address sulla stessa porta, ma non più MAC su porte diverse, in questo secondo caso vuol dire che si sono venuti a creare dei loop sulla rete che la rallentano e non la mantengono in condizioni ottimali. Per tutelarsi si utilizza un metodo detto Spanning Tree (STP)

Attività slide 5.2.1.6
Esercizio 5.2.1.7 pdf

Il traffico sullo switch in base alla sua MAC Table si divide in:
Unicast switch:
- In table (known unicast): SELECTIVE - out over 1 interface
- Not in table (unknown unicast): FLOODING – out over all interface, but not in sending interface

Broadcast: FLOODING
Multicast:
- Se gestisce traffico IGMP, fa un selecting forward (creando un'apporita tabella)
- Se non gestisce traffico IGMP → FLOODING

NB: tutte le tabelle sono in RAM, tranne nel caso in cui si specifichi il salvataggio

I metodi che ha lo switch per far girare i frame sono principalmente 2:
Storage Forward: dove lo switch riceve tutto il frame, poi analizza l'FCS e poi decide, se non è corrotto lo manda fuori, quindi è un apparato molto affidabile sulla rete, ma di contro risulta essere molto lento e necessita di risorse.
Cut Through: ha 2 modalità:

- **Fast Forward**: non aspetta tutto il frame prima di ritrasmetterlo, ma lo gira subito, questo risulta essere molto veloce.
- **Fragment Free**: dove prima di trasmettere aspetto i primi 64bytes. Se riceve i primi 64bytes vuol dire che non è avvenuta nessuna collisione, per cui il frame è integro, magari potrebbe però essere corrotto

Il Buffer sugli switch è fondamentale poiché mi consente di avere il collision detect. In ogni switch il buffer è gestito o in modo selettivo su ogni porta oppure in maniera generale/condiviso tra tutte le interfacce.

All'interno della rete locale (LAN), vi sono 2 indirizzi primari assegnati ai device, ossia il MAC Address (utilizzato per le comunicazioni fisiche) e l'indirizzo IP

Esercizio 5.3.1.3 pdf
Esercizio 5.3.1.3 packet tracert

Per poter ricavare il MAC Address Destination, si sfrutta la risoluzione dell'indirizzo il tramite il protocollo ARP dal quale si realizza una tabella detta ARP Table.

Mando una ARP request in broadcast → Qualcuno mi risponde ARP response → UNICAST → OK, scrivo tutto in ARP Table

Tutti gli apparati Layer3 hanno una ARP Table. Importante sapere che l'ARP Table si crea solo su ARP Response. Il timing dei valori di un'ARP Table sono indicativamente di 2 minuti

Dimostrazione ARP 5.3.2.3 pdf

Comandi per visualizzare la tabella ARP
PC: **arp –a**
CISCO: **show ip arp** in "Privileged Exec"

Esercizio 5.3.2.8 packet tracert

FINE CAPITOLO 5
LAYER ETHERNET

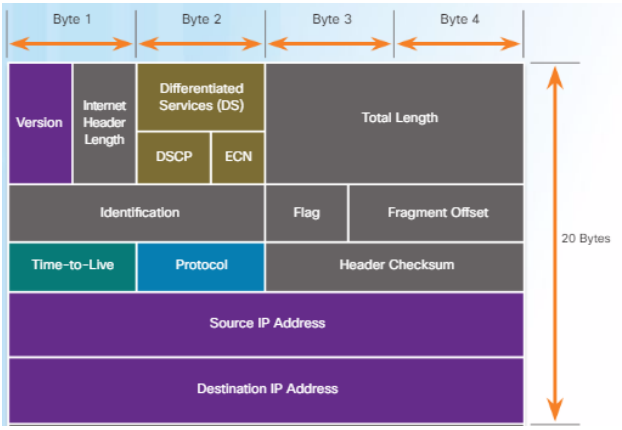
CAPITOLO 6 – Network Layer

Il livello network (Layer3) ha le seguenti caratteristiche:

- Si disinteressa del mezzo
- Si occupa di problematiche END-to-END. Ossia di routing, il suo compito è di consegnare il pacchetto al destinatario
- Non è richiesta la garanzia di consegna, quindi non effettua la ritrasmissione dei pacchetti corrotti (Best Effort)
- Connectionless: ossi non viene effettuata nessuna connessione con l'host di destinazione prima dell'invio dei pacchetti
- Una sua parte importante (che lo caratteristica maggiormente) è l'Addressing
- Gestisce la frammentazione, ossia se arriva un pacchetto con un determinato MTU che però risulta essere > del massimo MTU del link sul quale lo devo ri-trasmettere, gestisto il pacchetto frammentandolo

Il Packet è la PDU di Layer3
I 2 principali protocollo del Layer3 sono IPv4 e IPv6

Header L3 IPv4:



Version: contiene 4 bit settati a 0100 identifica che si tratta di IPv4
Differentiade Services: sono 8bit che identificano la priorità dei pacchetti trasportati
TTL: è il valore che l'host di trasmissione dà ai pacchetti che trasmette, e ad ogni passaggio di apparato L3 viene decrementato, e nel caso in cui il valore arriva a 0 ed il pacchetto si trova in un'apparato non di distinazione, viene cancellato.
Protocol: indica il protocollo di livello superiore che viene trasportato
Source/Destination: contengono IPv4 di partenza e destinazione

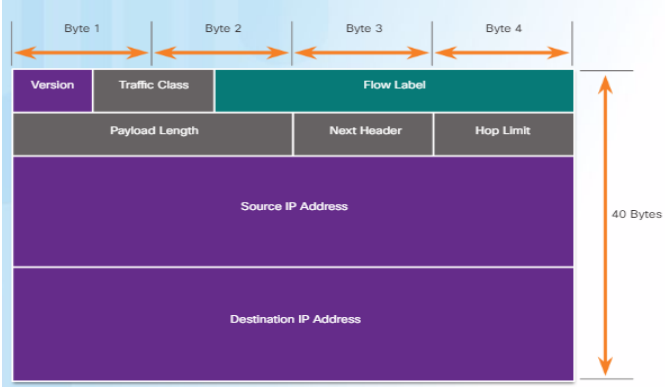
I problemi principali dell'IPv4 principalmente sono:

- ✓ Numero di indirizzi limitati (massimo 4 miliardi [2^{32}])
- ✓ Routing table expansion: l'aggiornamento delle tabelle di routing è nolto dispendioso in termini prestazionali
- ✓ Integrazione del NAT per poter aumentare il numero di dispositivi interconnessi

Per ovviare a questi limiti, è stato introdotto l'IPv6

1. Il numero di indirizzi è considerato infinito → 2^{128} = 340 millioni di decilioni (340 miliardi di miliardi di miliardi di miliardi) di indirizzi IPv6
2. Improved packet handling: l'header è stato semplificato
3. Eliminata la necessità di avere i NAT

Header L3 IPv6



Version: contiene 4 bit settati a 0110 identifica che si tratta di IPv6
Traffic Class: sono 8bit e si possono paragonare alla Differentiade Services dell'IPv4
Payload Length: è composto da 16 bit ed indica la lunghezza del dato trasportato
Next Header: è l'equivalente del Protocon nell'IPv4
Hop Limit = TTL
Source/Destination: contengono IPv6 di partenza e destinazione

Per poter uscire dal mio broadcast domain devo impostare un gateway che mi consente di dirottare il mio traffico verso altri broadcast domain ed ha almeno un'interfaccia sul mio broadcast domain.
Il Router farà poi un frowarding, ossia deciderà su quale interfaccia girare il pacchetto che è entrato, tramite un'apposita tabella di routing

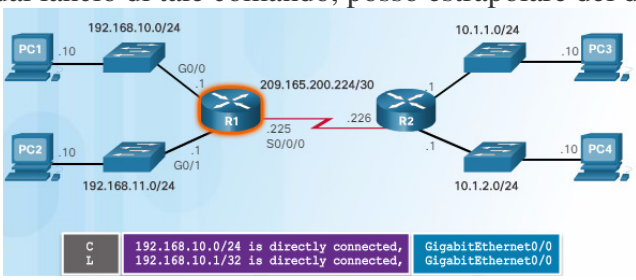
Table Routing	
Destinazione	**Interfaccia di uscita o Next Hop**
Network1	fe0/0
Network2	fe0/1
Network3	fe0/2
Network4	fe0/3
Network5	fe0/4
Network6	fe0/5

DESTINAZIONE → AZIONE

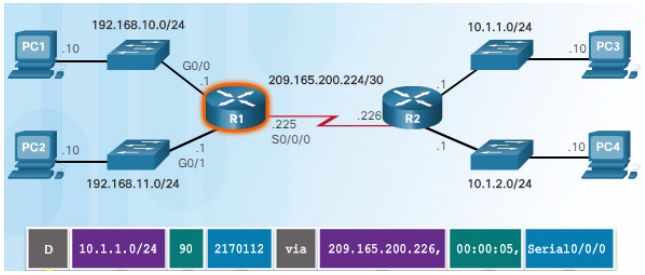
Per visualizzare la propria tabella di routing basta lanciare il comando **netstat -r** oppure **route print**
Le decisioni di Router Forwarding vengono prese nei seguenti modi:

- **Directly-connected routes**: il router conosce già la destinazione in base alla sua tabella di routing
- **Remote routes**: il router conosce già il router che gestisce tale rete e "forwarda" il pacchetto direttamente a lui, o per meglio dire il nostro router è già stato programmato con apposite tabelle di routing
- **Default route**: il nostro router non conosce la destinazione, ma conosce solo il router successico (NEXT HOP)

Per vedere la tabella di routing dare il comando **show ip route** nel "Privilege Exec".
Nel risultato che compare dal lancio di tale comando, posso estrapolare dei dati:



- C indica che la rotta è direttamente connessa al router, e viene creata automaticamente quando ad un'interfaccia viene assegnato un IP ed attivata
- L indica che si tratta dell'interfaccia locale, indica che l'IP assegnato è quello dell'interfaccia specifica



- D identifica che la rete 10.1.1.0/24 è raggiungibile tramite l'IP 209.165.200.226 (NEXT HOP) tramite l'interfaccia Serial0/0/0

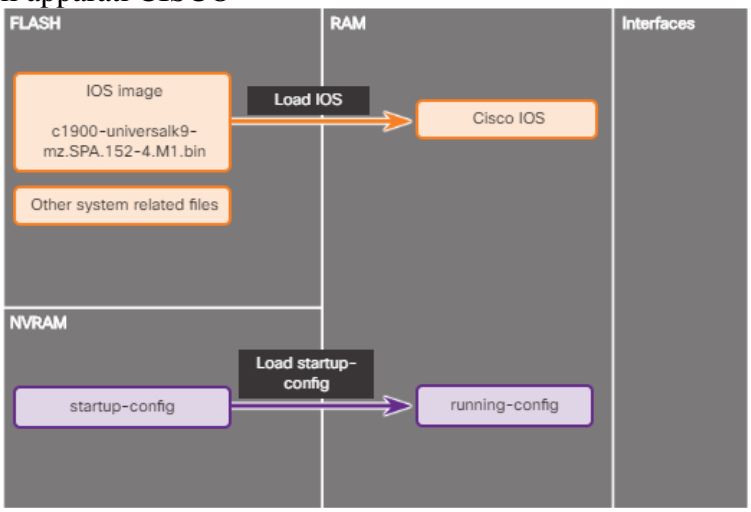
6.3.1.8 Packet Tracer - Exploring Internetworking Devices.pdf
6.3.1.8 Packet Tracer - Exploring Internetworking Devices.pka

Regole d'oro del router:

1. Every router is autonomous
2. If router A known router X → non è detto che → router B known router X
3. If router A known router B → non è detto che → router B known router B
4. In ogni router è fondamentale che sia configurato il NEXT HOP

I router valutano la "**metric**", cioè valutano la strada migliore per consegnare il pacchetto e la valutano tramite AD (Administrative Distance)

Sistema di avvio degli apparati CISCO



Per avere informazioni sullo IOS installato sul nostro dispositivo, basta avviare la "Privileged Exec" e dare il comandi: **show version**

6.3.2.7 Lab - Exploring Router Physical Characteristics.pdf

Switch Configuration Task:

```
enable
configure terminal
hostname S1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd # Configurazione Switch di Giordy#
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
exit
copy running-config startup-config
```

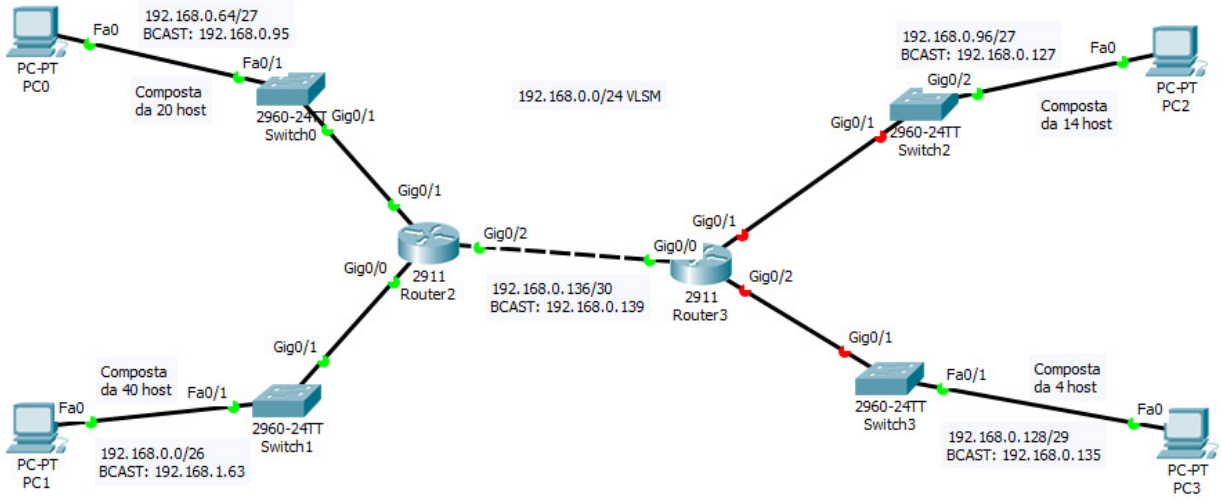
Router Configuration Task:

```
enable
configure terminal
hostname R1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #Configurazione Router di Giordy#
exit
copy running-config startup-config
```

6.4.1.3 Packet Tracer - Configure Initial Router Settings.pdf
6.4.1.3 Packet Tracer - Configure Initial Router Settings.pka

Nel **configure terminal:**
interface f0/0 → indicare l'interfaccia da configurare
description Metti la descrizione di cosa fa interfaccia
ipaddress 192.168.1.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
Nel Privileged Exec:
show ip interface brief: indica la tabella di routing delle interfacce fisiche dell'apparato
show ip route: mostra le tabelle di routing in RAM
show interfaces: mostra le statistiche per ogni interfaccia del dispositivo
show ip interface: mostra le statistiche dell'IPv4 di tutte le interfacce del dispositivo

Vediamo ora come configurare le tabelle di routing in modo statico, basandoci sull'esempio in figura



Iniziamo configurando il Router2, impostando le password, hostname ecc, come abbiamo già visto, poi iniziamo a configurare le interface di accesso, nello specific:
G0/0 → 192.168.0.1
G0/1 → 192.168.0.65
G0/2 → 192.168.0.137
Poi configureremo Router3
G0/0 → 192.168.0.138
G0/1 → 192.168.0.97
G0/2 → 192.168.0.129

--- ROUTER2---

```
enable
enable
configure terminal
interface g0/0
ip address 192.168.0.1 255.255.255.192
no shutdown
exit
interface g0/1
ip address 192.168.0.65 255.255.255.224
no shutdown
exit
interface g0/2
ip address 192.168.0.137 255.255.255.252
no shutdown
exit
```

--- ROUTER3---

```
enable
configure terminal
interface g0/0
ip address 192.168.0.138 255.255.255.252
no shutdown
exit
interface g0/1
ip address 192.168.0.97 255.255.255.224
no shutdown
exit
interface g0/2
ip address 192.168.0.129 255.255.255.248
no shutdown
exit
```

Ora se assegnamo in ip ai pc PC0 e PC1, questi si riescono a pingare l'un l'altro, così come PC2 con PC3. Il nostro problema ora è il riuscire a mettere in contatto PC1 con PC3, e per fare ciò dovremo configurare le tabelle di routing all'interno dei router Router2 e Router3

--- ROUTER2---

```
enable
configure terminal
ip route 192.168.0.96 255.255.255.224 192.168.0.138
ip route 192.168.0.128 255.255.255.248 192.168.0.138
exit
```

le righe "ip router …" indicano al router che i pacchetti che devono andare verso la rete 192.168.0.96/27 devono essere passati al ROUTER3, che risulta già conosciuto in quanto l'IP 192.168.0.138 è nella stessa subnet dell'IP 192.168.0.137 detenuto dal ROUTER2 sulla porta G0/2.
ATTENZIONE però che i pacchetti che arrivano agli host collegati al ROUTER3, arriveranno senza problem, ma i pacchetti di risposta non potranno tornare indietro fino a quando non configureremo anche la tabella di routing anche su ROUTER3 poichè i pacchetti di risposta contengono come IP di destinazione, IP che sono collegati al ROUTER2

--- ROUTER3---

```
enable
configure terminal
ip route 192.168.0.0 255.255.255.192 192.168.0.137
ip route 192.168.0.64 255.255.255.224 192.168.0.137
exit
```

Ora su un router possiamo dare il commando "execute privilege"

show ip route

ed analizzarne l'output:

ROUTER2

```
192.168.0.0/24 is variably subnetted, 8 subnets, 5 masks
C 192.168.0.0/26 is directly connected, GigabitEthernet0/0
L 192.168.0.1/32 is directly connected, GigabitEthernet0/0
C 192.168.0.64/27 is directly connected, GigabitEthernet0/1
L 192.168.0.65/32 is directly connected, GigabitEthernet0/1
S 192.168.0.96/27 [1/0] via 192.168.0.138
S 192.168.0.128/29 [1/0] via 192.168.0.138
C 192.168.0.136/30 is directly connected, GigabitEthernet0/2
L 192.168.0.137/32 is directly connected, GigabitEthernet0/2
```

Lettura dell'OUTPUT

Inizia dicendo che ha identificato 8 subnet con 5 netmask (essendo 3 il numero delle schede di rete configurate)
C 192.168.0.0/26 indica la rete connessa all'interfaccia g0/0, mentre L indica l'IP assegnato all'interfaccia g0/0 (infatti è un /32)
Così come per g0/1 e g0/2
S 192.168.0.96/27 indica che si tratta di una rotta statica (impostata appunto da me) e che per contattarla bisogna contattare in NextHop raggiungibile all'IP 192.168.0.138

6.4.3.3 Packet Tracer - Connect a Router to a LAN.pdf
6.4.3.3 Packet Tracer - Connect a Router to a LAN.pka
6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues.pdf
6.4.3.4 Packet Tracer - Troubleshooting Default Gateway Issues.pka
6.5.1.1 Class Activity - Can You Read This Map.pdf
6.5.1.2 Lab - Building a Switch and Router Network.pdf
6.5.1.3 Packet Tracer Skills Integration Challenge.pdf
6.5.1.3 Packet Tracer Skills Integration Challenge.pka

L'IPv4 è formato da 4 Bytes → 32 bit, 4 blocchi da 1 byte l'uno. Dove ogni blocco è separato da quello successivo con un .
XXXXXXXX.xxxxxxxx.XXXXXXX.xxxxxxxx

Da binario a decimale:

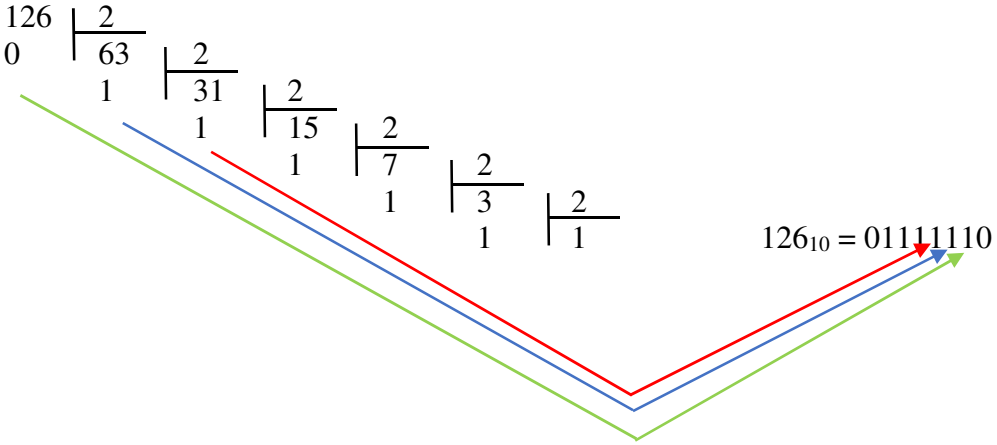
A quanto corrisponde il numero binario 110111012 in decimale?

Posizione bit	8	7	6	5	4	3	2	1
Valore bit	1	1	0	1	1	1	0	1
Elevamento a Potenza	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Operazione da svolgere	1×2^7	1×2^6	0×2^5	1×2^4	1×2^3	1×2^2	0×2^1	1×2^0
Valori da sommare	128	64	0	16	8	4	0	1
Somma o valore decimale	128+64+0+16+8+4+0+1=221							

Da decimale a binario:

A quanto corrisponde 126_{10}?

Bisogna dividere il numero per 2 e il resto della divisione ci fornisce il codice binario a partire dalla cifra meno significativa.



L'IP nella rete locale deve essere univoco
L'IP nella LAN deve essere gerarchico, ossia diviso in gruppi, assegnando valori diversi a porzioni di indirizzi diversi, gestiti tramite le subnet (netmask).
L'IP è diviso in 2 parti, la prima parte che ne identifica la rete (NET) e la seconda parte che ne identifica il dispositivo (HOST)
IP → 

Il confine tra NET e HOST è gestito dalla subnet mask che in IPv4 potrà essere gestita in 2 modi:

1) Indicando i BIT (max 32) che possono variare nell'ip. Ha valore 1 in corrispondenza dei bit che non possono variare (es. 255.255.255.0)
2) /X dove X indica il numero dei bit a 1 (cioè che non possono variare) e si parte a contarli da sinistra

Per semplificare, le netmask /8, /16, /24 indicano che il primo o il secondo o il terzo byte non è modificabile, cioè è a $255_{10} = 11111111_2$. Quindi mi conviene utilizzare la notazione /X solo se la subnet netmask è più restrittiva di una di queste 3
Per velocizzare il calcolo degli ip a mia disposizione da assegnare alla rete, eseguo questo calcolo:
n=net h=host ip=n+h=32 /24→ n=24 ip-n=h → 32-24=8
quindi il numero degli ip a mia disposizione sarà: 2^h-2=254

Esempio:
192.168.10.143/25 mi dice che:

- ✓ i primi 25 bit della mia subnet mask sono a 1
- ✓ io posso impostare nella mia rete tutti i valori esprimibili dagli ultimi 7 bit
- ✓ tranne il primo che è il valore della mia rete (NET)
- ✓ tranne l'ultimo che è l'indirizzo di broadcast

Per cui avrò che:
convertendo 143_{10} → 10010011_2 per cui potendo modicicare solo gli ultimi 7 bit avrò

- ✓ Indirizzo di rete (NET Address): **10000000**$_2$ = 128_{10}
- ✓ Indirizzo di Broadcast: **11111111**$_{2=}$ 255_{10}
- ✓ Quindi il range degli ip (ossia il mio Broadcast Domain) andrà:
  - Da 192.168.10.128
  - A 192.168.10.255

Un HOST quindi per poter accedere ad una rete dovrà avere impostato IP e NETMASK. Se vogliamo che l'host parli anche con altre reti, ossia con altri broadcast domain dovrà aver impostato anche il DEFAULT GATEWAY. Infine se voglio utilizzare anche i nomi degli Host devo specificare almeno un DNS.

Trasmissione IPv4:
Unicast: trasmetto direttamente all'ip dell'Host di destinazione
Direct Broadcast: è tendenzialmente il broadcast della mia rete (/24), ed i router tendenzialmente lo bloccano, ma se sono appositamente configurato possono anche lasciar passare questo traffico.
Limited Broadcast: 255.255.255.255 (/32) rimane SEMPRE dentro al broadcast domain.
ATTENZIONE: Broadcast ≠ Rete
Multicast: tutti gli ip di classe D

Classi IPv4: le classi degli ip vengono divise in base ai bit con cui iniziano

CLASSE	Bit d'inizio	1° Btye	IP
A	**0**	00000000	0.0.0.0
		01111111	127.255.255.255
B	**10**	10000000	128.0.0.0
		11111111	191.255.255.255
C	**110**	11000000	192.0.0.0
		11011111	223.255.255.255
D	**1110**	11100000	224.0.0.0
		11101111	239.255.255.255
E	**11110**	11110000	240.0.0.0
		11110111	247.255.255.255

La classe E è definita come experimentale.
A livello legacy ad ogni classe è assegnata una Default Netmask, che risulta essere:
A/8 B/16 C/24
Attenzione: NETMASK ≠ CLASSE

Nell'IPv4 vi sono indirizzi riservati speciali ed indirizzi riservati per uso privato.

IP Riservati:
127.0.0.0/8 → Indirizzi di Loopback
169.254.0.0/16 → Indirizzi di Link Local: gli host se li auto assegnano in mancanza di DHCP per tentare di stabilire lo stesso una comunicazione di rete, generalmente gli ultimi 2 numeri si auto-completano con il MAC Address
192.0.0.2/24 → rete per effettuare dei test

IP Privati:
Classe A: 10.0.0.0/8
Classe B: da 172.16.0.0/16 a 172.31.0.0/16
Classe C: da 192.168.0.0/24 a 192.168.255.0/24

Ormai tutti gli apparati iniziano ad essere Dual Stack, ossia gestiscono sia IPv4 sia IPv6

Nel calcolo degli ip della rete, ricordarsi la tabellina dell'AND logico

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0

Host Address	172	25	119	84
Subnet Mask	255	255	252	0
Host Address in binary	10101100	00011001	01110111	01010100
Subnet Mask in binary	11111111	11111111	11111100	00000000
Network Address in binary	10101100	00011001	01110100	00000000
Network Address in decimal	172	25	116	0

7.1.2.8 Lab - Using the Windows Calculator with Network Addresses.pdf
7.1.2.9 Lab - Converting IPv4 Addresses to Binary.pdf
7.1.3.8 Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic.pdf
7.1.3.8 Packet Tracer - Investigate Unicast, Broadcast, and Multicast Traffic.pka
7.1.4.9 Lab - Identifying IPv4 Addresses.pdf

Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

L'IPv6 è formato da 16 Bytes (128bit) e si rappresenta in 8 gruppi di 4 cifre esadecimali separate da:
La conversione bit → Hex viene effettuata tramite la solita tabella biunivoca in cui 4 bit sono sempre rappresentabili da un numero esadecimale.

La scrittura di tutto l'indirizzo IPv6 (ossia indicando ognuna delle 4 cifre degli 8 gruppi) è detta **PREFERED FORMAT**.
Una delle caratteristiche dell'IPv6 è che si può scrivere anche in modo compatto seguendo 2 regole:

1) Di ogni gruppo di 4 cifre posso eliminare gli 0 iniziali (se ce ne sono)
2) Una sola sequenza di ":0:" può essere tolta e sostituita con "::"

Per convenzione il loopback address (127.0.01) si indica con **::1**

Tipi di trasmissione nell'IPv6
Non c'è più il concetto di Broadcast, ma è stato introdotto il concetto di:
ANYCAST: cioè l'ip di anycast viene assegnato o acquisito a/da più dispositivi e il pacchetto viene consegnato a quello più vicino
La parte MULTICAST è andata a sostituire la parte broadcast in modo tale che il traffico sia più selettivo.

La rappresentazione della netmask dell'IPv6 è solo /X che di default è/64, starà poi a noi decidere come frazionarla.

Classificazione tipi di IPv6

- Global Unicast: come gli IPv4 sono quelli pubblici. Li assegna l'ISP. Ma a differenza dell'IPv4, qui ogni dispositivo che vuole navigare, deve avere uno di questi
- Link Local: è l'evoluzione del Link Local dell'IPv4. In IPv6 è quello che viene assegnato per lo scambio di dati in LAN
- LoopBack → ::1
- Unspecified Address: quando identifico tutta la mia rete
- Unique Local: sono IP assegnati, ma non vengono nattati, ossia non vengono usati per fare traffico fuori dalla mia rete. Quindi se non lo configuro sull'interfaccia, non ce l'ho. Posso usarlo per far parlare tra loro reti da me create con apposite configurazioni di routing

NB: Per ogni interfaccia posso avere più tipi di IPv6 su essa configurati

Gli indirizzi di Link Local sono:

FE80::/10			
F	E	8	0
1111	1110	1000	0
1111	1110	10	non cambiano

Per cui gli indirizzi a disposizione variano
da: FE80:0000:0000:0000:0000:0000:0000:0000
a: FEBF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Dove B = **1011**

Gli indirizzi di Global Unicast sono:

2000::/3			
2	0	0	0
0010	0000	0000	0000
001			non cambiano

Per cui gli indirizzi a disposizione variano
da: 2000:0000:0000:0000:0000:0000:0000:0000
a: 3000:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
Dove 3 = **0011**

Gli indirizzi di Multicast sono:
FFFF::/8
FF02::/1 → su tutti i nodi
FF02::/2 → per tutti i router ed esclude i nodi

StateLess: significa che nonostante io apporti dei cambiamenti alla rete, nulla viene aggiornato
StateFull: è il contrario di StateLess, cioè se io esegui qualcosa sulla rete o su un'apparato, avvengono dei cambiamenti che anche altri apparati registrano (es. più lampante è il FW in quanto il traffico in uscita è consentito per principio ed conseguenza il FW si adatta/adopera affinchè le mie richieste di navigazione possano anche tornarmi indietro)

Assegnazione dell'IPv6:
a) Static: l'IP lo inseriamo noi staticamente
b) SLAAC (stateless)
c) DHCPv6 (statefull)
d) SLAAC + DHCPv6 (stateless)

In questi 3 casi, appena collego un dispositivo alla rete, esso parla con il router che gli manda dei dati (RA), tra cui: Gateway, RangeNet di partenza, ecc…

Vediamo più in dettaglio:

b) La parte di NET me la comunica il router, mentre per quanto riguarda la parte di HOST vi sono 2 metodologie:
- RANDOM: dove i valori vengono compilati in maniera RANDOM appunto
- EUI64: viene creato attraverso l'utilizzo del MAC Address

c) Funziona come il DHCP per l'IPv4
d) Ho un'assegnazione dell'ip con SLAAC e il DHCP mi dà informazioni aggiuntive (es. servizi NTP, …)
L'ICMP è una suite di protocolli di supporto all'IP, nei quali c'è da specificare almeno l'IP di destinazione. Ogni protocollo utilizzato ci fornisce delle risposte che vanno interpretate, quindi fare ATTENZIONE

Attenzione, nei router per configurare l'IPv6 bisogna specificarlo

```
interface g0/0
ipv6 address 2001:db8:acad:2::1/64
no shutdown
```

nella configurazione dell'IPv6 l'indirizzo di link-local è da abilitare
interface g0/0
ipv6 address fe80::1 link-local
no shutdown

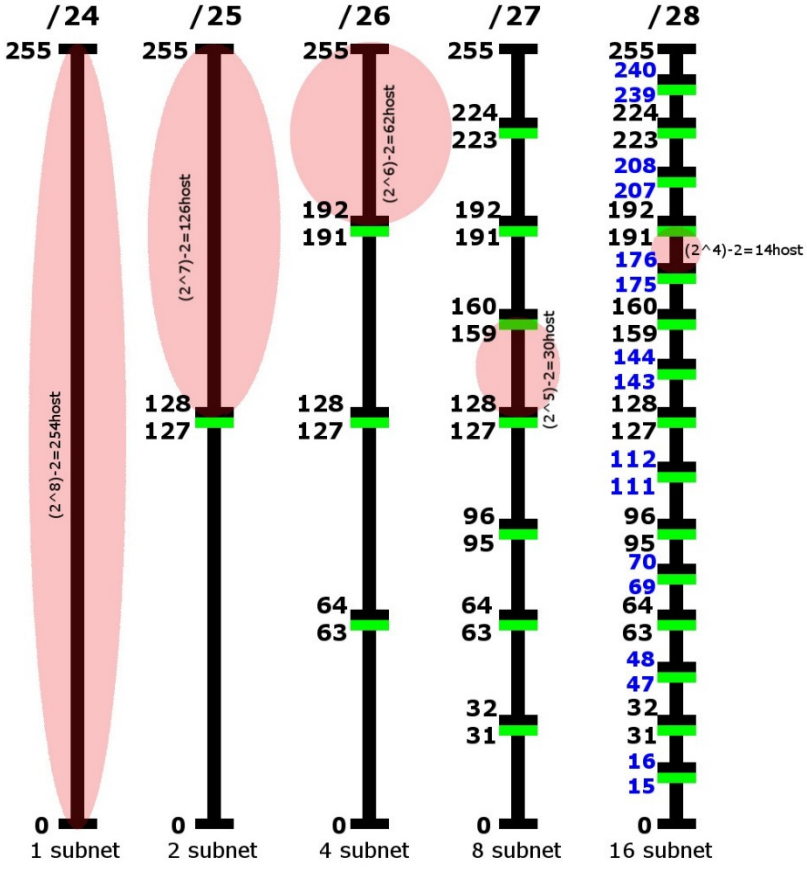
NNB: un'interfaccia può avere più IPv6 a seconda del traffico che deve eseguire

Per verificare una configurazione IPv6, basta dare il comando:
show ipv6 interface brief
che ci darà come output:
il nome dell'iterfaccia e tra parentesi se è up o down e sotto l'elenco degli indirizzi ad essa attribuiti

7.2.4.9 Packet Tracer - Configuring IPv6 Addressing.pdf
7.2.4.9 Packet Tracer - Configuring IPv6 Addressing.pka
7.2.5.3 Lab - Identifying IPv6 Addresses.pdf
7.2.5.4 Lab - Configuring IPv6 Addresses on Network Devices.pdf
7.3.2.5 Packet Tracer - Verifying IPv4 and IPv6 Addressing.pdf
7.3.2.5 Packet Tracer - Verifying IPv4 and IPv6 Addressing.pka
7.3.2.6 Packet Tracer - Pinging and Tracing to Test the Path.pdf
7.3.2.6 Packet Tracer - Pinging and Tracing to Test the Path.pdf
7.3.2.7 Lab - Testing Network Connectivity with Ping and Traceroute.pdf
7.3.2.8 Lab - Mapping the Internet.pdf
7.3.2.9 Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing.pdf
7.3.2.9 Packet Tracer - Troubleshooting IPv4 and IPv6 Addressing.pka
7.4.1.2 Packet Tracer - Skills Integration Challenge.pdf
7.4.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 7

SUBNETTING è il meccanismo in cui dividiamo una rete in tante **sub-net**.
Ad esempio: 192.168.1.0/24 è la nostra classfull, cioè la nostra classe di partenza essendo di default una classe C e quindi avendo una netmask /24. Nello schema sotto, vediamo come restringere una netmask, creando quindi differenti subnet a partire dalla /24 (/25, /26, /27, ….. /30)
Ricapitolando quindi il /X mi dice quanti bit dell'IPv4 non posso cambiare sui 32 di cui è composto.



IP=X bit di NET + Y bit di HOST
IP = N + H
Indicando con S i bit di host presi in prestito (borrow), avremo
Magic Number (MN) = 2^{H-S}

Con il quale potremo semplificarci e velocizzare i calcoli per sapere IP a nostra disposizione per gli host, subnet a nostra disposizione ecc…

2^S = al numero delle subnet che vi possono essere nella mia rete

Ad esempio:
192.168.1.0/26
S=26-24=2 → posso creare $2^2 = 4$ subnet

Attenzione, il subnetting è un processo ricorsivo e se viene suddivisa, i valori che limitano una subnet, sono compresi anche all'interno della subnet più restrittiva, cioè i valori che delimitano la sbubnet /25 sono compresi anche all'interno della subnet /27 o /28 (come si vede anche in figura.
Il numero di host a mia disposizione si calcola con il Magic Number (MN):
Host a mia disposizione = MN-2
Per il calcolo della netmask nella seconda modalità, basta ricordarsi che il /X indica il numero dei bit che devo impostare a 1, per cui:
/24→11111111.11111111.11111111.**00000000**→255.255.255.**0**
/27→11111111.11111111.11111111.**11100000**→11100000_2=128+64+32=224 → 255.255.255.**224**
/30→11111111.11111111.11111111.**11111100**→11111100_2=128+64+32+16+8+4=252→255.255.255.**252**
Oppure sfruttando il MN
/30 → MN = 4 = 2^{H-S} → 255-2^{H-S}+1 → 255.255.255.**252**
/26 → MN = 64 = 2^{H-S} → 255-2^{H-S}+1 → 255.255.255.**192**
Per i valori da assegnare ad ogni subnet, o per sapere se in una determinata netmask i valori che si vorrebbe assegnare sono di Netword e Broadcast, bisogna farsi una tabellina mentale (con l'esperienza) o con carta e penna all'inizio, come quelle allegate
Nella progettazione, per evitare di consumare gli indirizzi, si parte prima ad assegnare le subnet più esose di indirizzi e via via quelle più piccole.

Facciamo anche un esempio di subnetting su una netmask di classe B
172.16.115.30/19
/19 → XXXXXXXX.XXXXXXXX.**XXX**XXXXX.XXXXXXXX
Bit di host = 8
Bit di host presi in prestito (S) = 3
N° di subnet a mia disposizione = 2^3=8
MN = 2^{H-S} = $2^{8-3=5}$ = 32
Quindi potrò fare massimo 8 subnet /19 ed ognuna di loro avrà a disposizione
N° Host = (MN * n°host totali dell'ultimo byte) = 32 * 256
Quindi i valori che potranno avere le subnet /19 nel penultimo byte saranno:
0, 32, 64, 96, 128, 160, ….
Infine possiamo ricavare da qui che il nostro IP 172.16.**115**.30/19 preso in esempio avrà
Indirizzo di NET: 172.16.96.0
Indirizzo di BROADCAST: 172.16.127.255

8.1.4.6 Lab - Calculating IPv4 Subnets.pdf
8.1.4.7 Packet Tracer - Subnetting Scenario.pdf
8.1.4.7 Packet Tracer - Subnetting Scenario.pka
8.1.4.8 Lab - Designing and Implementing a Subnetted IPv4 Addressing Scheme.pdf

ATTANZIONE: subnetting ≠ range ip → se a me servono gli indirizzi da 192.168.0.100 a 192.168.0.200, posso scegliere il range, ma non la subnet, poiché tali indirizzi sono nella stessa subnet solo se questa è /24, altrimenti saranno in 2 subnet differenti

Importante ricordarsi che (esempi):
192.168.1.0/24 → NETWORK
192.168.1.0/27 → SUBNET
192.168.0.0/16
192.168.4.0/22 → SUPERNET

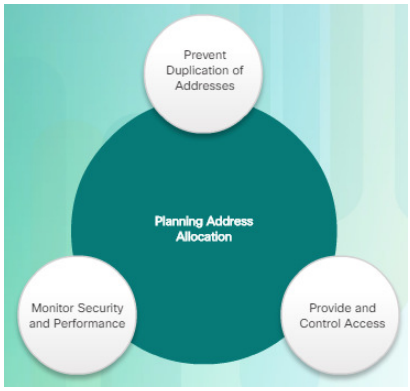
CLASS-FULL

allargo SUPERNET ← → restringo SUBNET

La suddivisione di una class-full può essere fatta in 2 modalità:

1) Uniform subnetting: in cui trasformo la mia subnet in altre subnet tutte uniformi /24 → in 2 /25 oppure in 4 /26 oppure in 8/27, ecc…fino alla /30 di cui ho a disposizione solo 2 ip
2) VLSM (Variable Length Subnet Masks): in cui trasformo la network (es. /24) in subnet non uniformi. In questo caso come già anticipato sopra spiegato sopra si inizia assegnando le subnet più grandi e via via a scendere verso le più piccole.

Per la pianificazione degli indirizzi da assegnare alle varie reti è bene utilizzare questo schema:



8.2.1.4 Packet Tracer - Designing and Implementing a VLSM Addressing Scheme.pdf
8.2.1.4 Packet Tracer - Designing and Implementing a VLSM Addressing Scheme.pka
8.2.1.5 Lab - Designing and Implementing a VLSM Addressing Scheme.pdf
8.3.1.4 Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme.pdf
8.3.1.4 Packet Tracer - Implementing a Subnetted IPv6 Addressing Scheme.pka
8.4.1.2 Packet Tracer - Skills Integration Challenge.pdf
8.4.1.2 Packet Tracer - Skills Integration Challenge.pka

Tabella di calcolo di alcune subnet

	/24, quindi 32-24=8bit che possono variare									n°subnet
da	0	0	0	0	0	0	0	0	0	1
a	1	1	1	1	1	1	1	1	255	

	/25, quindi 32-25=7bit che possono variare									n°subnet
da	0	0	0	0	0	0	0	0	0	1
a	0	1	1	1	1	1	1	1	127	
da	1	0	0	0	0	0	0	0	128	2
a	1	1	1	1	1	1	1	1	255	

	/26, quindi 32-26=6bit che possono variare									n°subnet
da	0	0	0	0	0	0	0	0	0	1
a	0	0	1	1	1	1	1	1	63	
da	0	1	0	0	0	0	0	0	64	2
a	0	1	1	1	1	1	1	1	127	
da	1	0	0	0	0	0	0	0	128	3
a	1	0	1	1	1	1	1	1	191	
da	1	1	0	0	0	0	0	0	192	4
a	1	1	1	1	1	1	1	1	255	

	/27, quindi 32-27=5bit che possono variare									n°subnet
da	0	0	0	0	0	0	0	0	0	1
a	0	0	0	1	1	1	1	1	31	
da	0	0	1	0	0	0	0	0	32	2
a	0	0	1	1	1	1	1	1	63	
da	0	1	0	0	0	0	0	0	64	3
a	0	1	0	1	1	1	1	1	91	
da	0	1	1	0	0	0	0	0	92	4
a	0	1	1	1	1	1	1	1	127	
da	1	0	0	0	0	0	0	0	128	5
a	1	0	0	1	1	1	1	1	159	
da	1	0	1	0	0	0	0	0	160	6
a	1	0	1	1	1	1	1	1	191	
da	1	1	0	0	0	0	0	0	192	7
a	1	1	0	1	1	1	1	1	223	
da	1	1	1	0	0	0	0	0	224	8
a	1	1	1	1	1	1	1	1	255	

FINE CAPITOLO 8

Iniziamo a parlare di Layer4 ossia di Transport Layer. Il PDU di L4 è il segment.
Il L4 ha alcune funzioni che risultano essere:

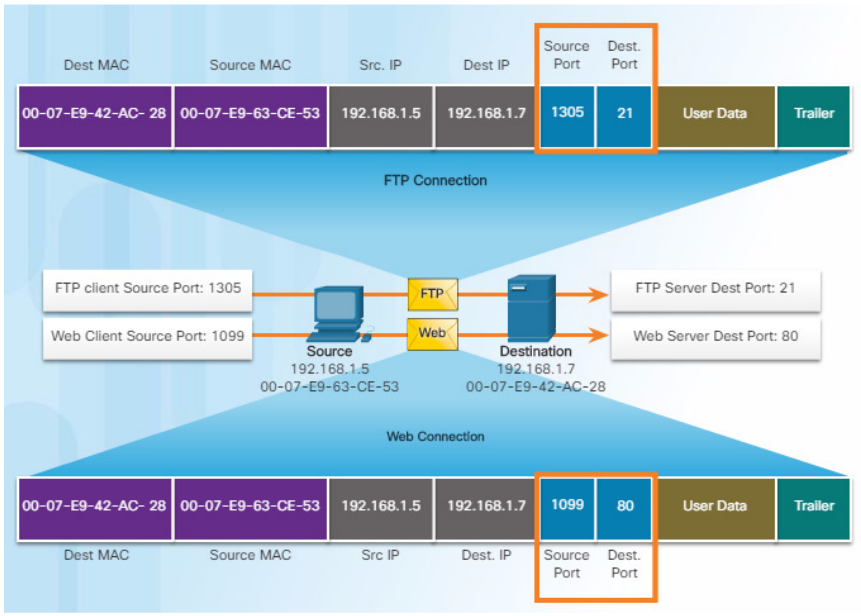
TCP UDP
4. Segmentation/Reassembling: dove divide i dati in partenza, ossia quelli da spedire al destinatario (segmentation) oppure riassembla quelli che gli arrivano dal mittente (reassembling)
5. Multiplexing: posso usarlo per collegare applicazioni differenti

TCP
6. Error Correction: il L4 è reliability (è affidabile)
7. Reordering: i pacchetti che vengono scambiati dagli host possono essere riordinati
8. FlowControl: vi è un controllo del flusso in base al canale che si usa per trasmettere

I principali protocolli che si usano a L4 sono: TCP ed UDP

Il TCP offre più servizi rispetto all'UDP. Cioè ordina i segmenti (Reordering), introducendo il concetto di Sequence Number, l'Acknowledged (controllo di ricezione) e di Windowing (FlowControl). Naturalmente il TCP offrendo più servizi rispetto all'UDP risulterà più lento nelle comunicazioni e più esoso in termini di prestazioni richieste agli apparati poiché appunto risulta essere più complesso.
UDP → Connection Less
TCP → Connection Oriented (3way hand shake)

Segment TCP



Destination port: è la porta del servizio che devo contattare (es. 80 per un sito web)
Source port: è la porta LOGICA che il sistema mi assegna (random), in quanto potrei anche utilizzare la stessa porta 80 per la prima richiesta, ma per richieste conccorrenti, dovrei utilizzarne un'altra, altrimenti i pacchetti non sarebbero consegnati alla stessa applicazione.

Le porte logiche vengono suddivise nei seguenti gruppo:

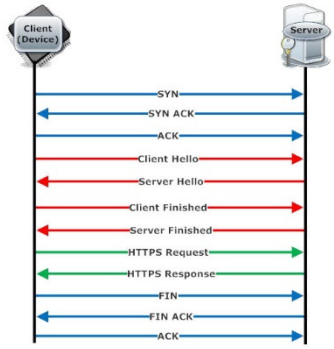
0-1023	Well known: tali porte sono di default assegnate a determinati servizi (es. 80 web, 21 FTP, 443 https, 22 ssh, 995 pop3s, ecc…)
1024-49151	Registered: porte che gli enti e le aziende possono richiedere all'IANA di poter riservare per eventuali loro applicazioni (es. 1194 OpenVPN, 1234 VLC default port stream, ecc…)
49152-65535	Dynamio o Private: assegnate dinamicamente dal client durante le trasmissioni di L4

Nei device per poter vedere le assegnazioni della porte logiche Source → Destination, basta dare il comando:

netstat

l'opzione -n sostituisce gli hostname dell'output con i loro IP

In realtà i pacchetti non vengono numerati, ma si contano i bytes trasmessi.

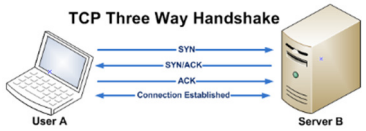


Il processo di una connessione TCP viene vista in modo molto schematico nella figura accanto, dove abbiamo

1. Un processo di creazione del canale di trasmissione (frecce BLU)
2. Un processo di presentazione tra il client ed il server sui servizi proposti dal serve al client
3. Un processo di scambio dei dati vero e proprio
4. Un processo finale di chiusura del canale di trasmissione

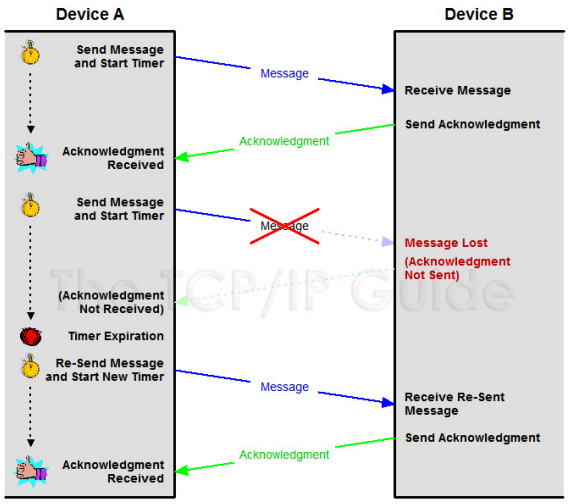
NB: i punti 2 e 3 li considereremo assieme

Vediamo ora di analizzare più in dettaglio la situazione

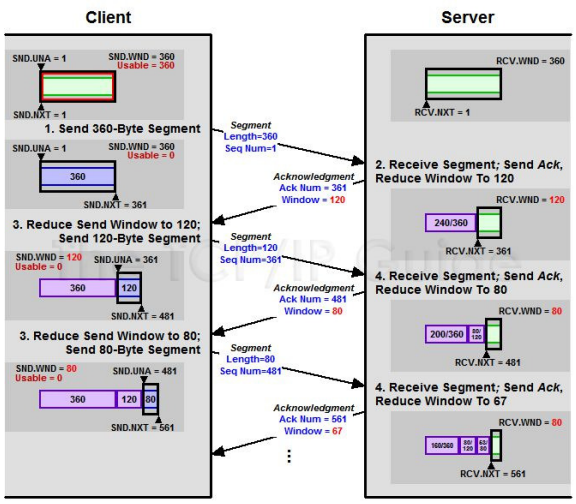


Il primo processo viene detto "e Way Hand Shake", dove gli Host creano un canale di trasmissione sicuro

Poi abbiamo una parte centrale dove vengono trasmessi i dati tra gli Host facendo attenzione al timing di validità del pacchetto, anche per sapere se il pacchetto è arrivato oppure no, all'acknowledging ed al windowing

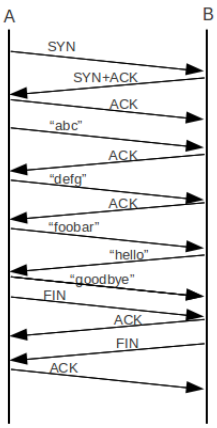


Timing



Windowing

Il window size: indica quanti bytes può lasciare esposti la trasmissione senza ricevere un Acknoledgment, ossia quanti ne mando prima di ricevere un ACK. Se la connessione è buona e stabile senza perdita di dati (quindi ricevo sempre in un tempo utile gli ACK), la window size si allarga, mentre se la qualità della connessione peggiora la W.S. si riduce



Infine abbiamo l'ultimo passaggio in cui viene chiuso il canale di trasmissione (parte finale della figura accanto, ultime 4 frecce).

Tutti i passaggi che vengono effettuati in una connessione TCP si vedono nell'immagine accanto

L'UDP da questo punto di vista è molto più fluido, in quanto non richiede la ritrasmissione, come non ha il riordino dei pacchetti.

Per vedere tutti i processi descritti nel capitolo si consiglia di fare dei test con Wireshark

9.2.4.3 Lab - Using Wireshark to Examine TCP and UDP Captures.pdf
9.3.1.2 Packet Tracer Simulation - Exploration of TCP and UDP Communication.pdf
9.3.1.2 Packet Tracer Simulation - Exploration of TCP and UDP Communications.pka

Socket: è la combinazione di un indirizzo IP di origine e di un numero di porta o di un indirizzo IP di destinazione e di un numero di porta

FINE CAPITOLO 9

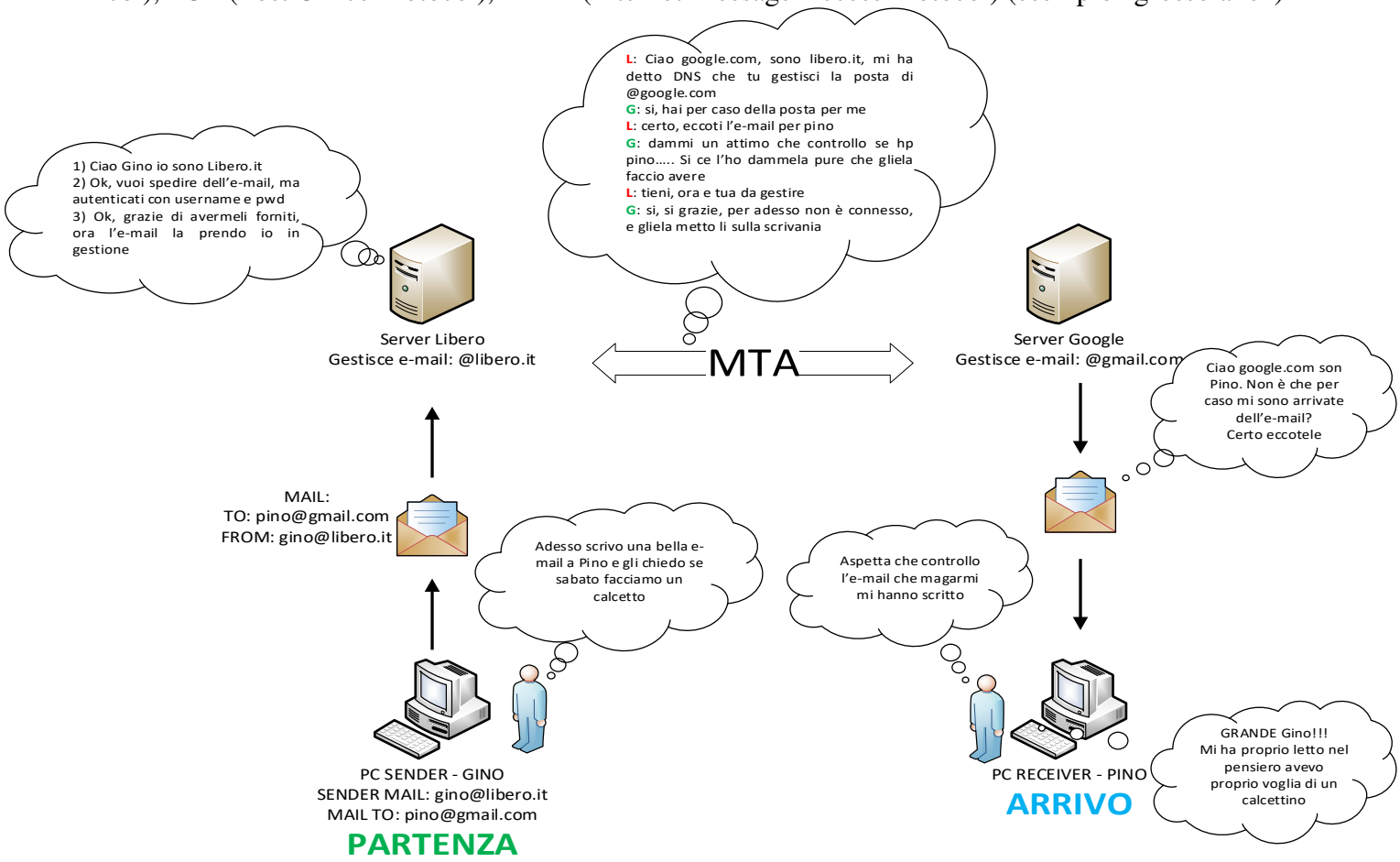
Nel TCP/IP, l'Application Layer, condensa i livelli 5, 6, 7 dell'stack ISO/OSI. Questo è il livello di interfaccia con l'end user. In questo livello vi sono molti protocolli conosciuti e altri che potranno esservi applicati in futuro. Questo livello comprende come detto sopra L7 (Application Layer) http (80 tcp), https (443 tcp), ssh (22 tcp), pop3 (110 tcp), imap (tcp 143), smtp (tcp 25), DNS (udp 53), TFTP (udp 69), FTP,DHCP/BOOTP (67 udp server, 68 udp client), ecc…
L6 (Presentation Layer) es. per le foto abbiamo JPEG, TIFF, PNG

Vi sono 2 tipo di comunicazione:
Client-Server: dove uno fornisce un servizio e l'altro ne usubruisce
P2P: dove ogni host richiede e fornisce servizi. Vi sono anche servizi che utilizzano un sistema ibrido in cui forniscono e richiedono servizi, ma poi l'indicizzazione del sistema rimane su un server centralizzato. Varie applicazioni P2P possono essere i programmi di file sharing.

10.1.2.5 Lab - Researching Peer-to-Peer File Sharing.pdf

Nell'utilizzo di siti web (protocollo http/https) si utilizza una comunicazione Client-Server, in cui il nostro browser con una chiamata GET richiede dei dati. Quando compiliamo un form utilizziamo un una funzione di invio dati POST. Infine quando carichiamo dati su un sito (es. upload di foto o altro) utilizziamo la funzione PUT.

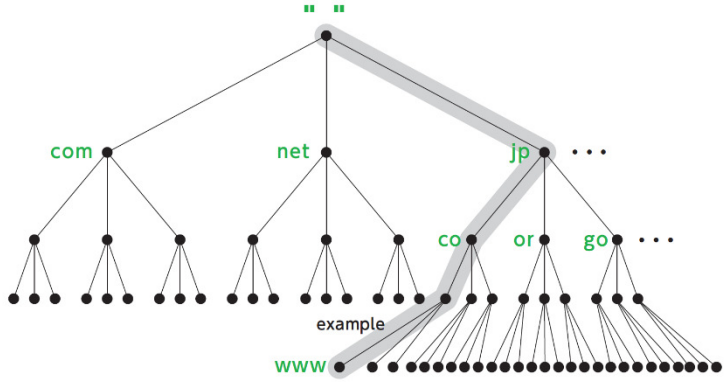
Nella gestione dell'e-mail utilizziamo 2 protocolli per ogni invio, e tra questi 2 utilizzati abbiamo la scelta ulteriore di quale utilizzare per l'archiviazione dell'e-mail.
I protocolli (L6 – Application Layer) in gioco risultano essere: SMTP (Simple Mail Transfert Protocol), POP (Post Office Protocol), IMAP (Internet Message Access Protocol) (esempio "grossolano")



Il POP scarica le mail e si tiene una copia dell'e-mail in locale
L'IMAP esegue una sincronia delle cartelle (selezionate e decise dall'utente) con il server

10.2.1.7 Packet Tracer - Web and Email.pdf
10.2.1.7 Packet Tracer - Web and Email.pka

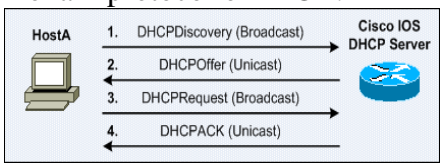
Internet è gestito totalmente in modo matematico, per cui i nomi come possono essere quelli del sito http://www.pincopallino.it non sono direttamente raggiungibili. Ha il vantaggio di essere facilmente ricordabile, rispetto ad esempio ad un http://194.87.43.98 .Si è avuto quindi la necessita di realizzare un sistema che desse la possibilità all'utente di ricordarsi il nome ma non il numero ed è stato ideato il DNS (Domain Name Service) che svolge proprio questa conversione.
Il DNS è composto da vari campi che ne identificano le funzioni ed i servizi che a me interessa contattare, come ad esempio l'elenco dei campi sotto:
A – un IPv4 generico da contattare per un determinato servizio, ad esempio
www.pincopallino.it → 194.87.43.98
webmail.pincopallino.it → 74.54.33.56
NS – il DNS autoritativo per il dominio, ossia nel caso in cui io voglia contattare un indirizzo di terzo livello di un determinato dominio ed i DNS che ho interrogato non hanno l'abbinamento hostname-IP, posso contattare questo DNS che può darmi le informazioni che cerco, compreso anche l'informazione che il terzo livello non esiste
AAAA – un IPv6 generico da contattare per un determinato servizio
MX – identifica i server mail da contattare per le caselle e-mail di quel determinato dominio. In questo campo vi è anche un valore che identifica la priorità del server (più il valore è basso più il server è importante per la gestione del servizio)



Le richieste ai DNS è detta hierarchical system (a piramide), in quanto ogni server DNS ha una cache con la risposta alle richieste più frequenti che gli vengono fatte. Nel caso in cui non abbia una risposta contatta il DNS sopra a lui, che funziona con la stessa modalità. In caso anche l'ultimo DNS contattato non abbia la risposta, questi contatterà uno dei 13 root DNS che conterrà sicuramente la risposta.

Il comando /nei pc) per avere maggiori informazioni su un determinato dominio con i relativi indirizzi IP che ne contraddistinguono i servizi è: **nslookup**

Il protocollo DHCP consente ad un host che viene collegato su una determinata rete (NET) di poter acquisire gli indirizzi IPv4 o IPv6 per poter "parlare" con gli altri host della rete stessa. Come funziona il protocollo DHCP?



Quando un host viene collegato alla rete, cerca subito un Server DHCP. Il server quando contattato gli offre il servizio, l'host gli manda la richiesta ed il server risponde con i parametri da impostare

10.2.2.7 Packet Tracer - DNS and DHCP.pdf
10.2.2.7 Packet Tracer - DNS and DHCP.pka
10.2.2.8 Lab - Observing DNS Resolution.pdf

Il protocollo FTP (File Transfer Protocol) è un protocollo nato per trasferire grandi quantità di dati sulla rete. Le porte de di default sono la 21 per l'attivazione del canale di trasmissione e la sua gestione e la 20 che viene utilizzata per il passaggio dei dati.

Un altro protocollo molto utilizzato nella LAN è il protocollo di condivisione directory SMB (Server Message Block), nel mondo linux è chiamato samba.

10.2.3.3 Packet Tracer - FTP.pdf
10.2.3.3 Packet Tracer - FTP.pka
10.2.3.4 Lab - Exploring FTP.pdf
10.3.1.1 Class Activity - Make it happen!.pdf
10.3.1.2 Packet Tracer - Explore a Network.pdf
10.3.1.2 Packet Tracer - Explore a Network.pka
10.3.1.3 Packet Tracer Multiuser - Tutorial.pdf
10.3.1.3 Packet Tracer Multiuser - Tutorial - Client Side.pka
10.3.1.3 Packet Tracer Multiuser - Tutorial - Server Side.pka
10.3.1.4 Packet Tracer Multiuser - Implement Services.pdf
10.3.1.4 Packet Tracer Multiuser - Implement Services - Client Side.pka
10.3.1.4 Packet Tracer Multiuser - Implement Services - Server Side.pka

FINE CAPITOLO 10

11.0.1.2 Class Activity - Did You Notice.pdf

NETWORK DESIGN

La maggior parte delle aziende hanno "Small Network Topology" che per essere realizzate, hanno la necessità di essere analizzate per valutare vari parametri necessari a realizzare la miglior soluzione possibile. Tali parametri sono:

Cost: inteso come costo degli apparati in base alle features che ci interessa avere, al numero di host che dobbiamo collegare, al tipo di collegamento che dobbiamo effettuare. La Secure Tecnology che dobbiamo avere sulla rete, ecc…

Speed & Type Port Interface: se le porte sono FastEthernet, Gigabit, 10 Gigabit ecc…

Expandibility: se dobbiamo o meno prevedere una rapida espansione, mantenendo un certo grado di scalabilità del sistema.

OS Features & Service: servizi che voglio integrare sulla mia rete, come il QoS, VoIP, Layer3, NAT, DHCP, ecc… Tra queste quelle che ultimamente viene più richiesta è la "Traffic Prioritizing/Management" (QoS) poiché un pacchetto VoIP se mi arriva in ritardo perdo dei pezzi di chiamata, mentre se un pacchetto di un'immagine jpg che stò visualizzando su un sito arriva in ritardo, semplicemente visualizzerò la foto con qualche secondo di ritardo.

Inoltre nello studio di una nuova "Small Network Topology" è bene decidere (anche in base ai punti sopra), come suddividere gli ip dei device, se suddividerli ad esempio in range di stampanti, server, pc, laptop, telefoni, tablet, smartphone, oppure in range o subnet per dipartimenti, o in altre metodologie a nostra scelta.

Gli switch, da scegliere nella realizzazione di un Network possono essere:

Semplici: ogni switch è un device a se stante;

Modulari: in cui c'è un case esterno ed io aggiungo switch man mano che mi servono;

Espandibili: dove i vari switch che vado ad aggiungere sono collegati tra loro con appositi cavi e vengono visti dal sistema come un unico device;

Un altro aspetto fondamentale di cui bisogna tener conto è la ridondancy (ridondanza) del sistema, per prevenire eventuali guasti o interruzione di link. Questo implica però maggior complessità del sistema (infatti bisogna fare molta attenzione a non creare dei loop nel sistema). E la complessità a sua volta genera una gestione più esosa di risorse fisiche ed economiche.

NNB: i loop a L3 sono relativamente arginati dal TTL (Time To Live), mentre a L2 sono arginati dallo Spanning Tree.

Se abbiamo già una Small Network e vogliamo implementarla, per poterne studiare l'implementazione, abbiamo bisogno d'avere:

Network documentation: cioè sapere com'è realizzata la struttura attualmente

Device inventory: sapere che device ho a disposizione e cosa possono offrire in più rispetto a quello che già fanno

Budget: sapere quanto posso spendere per implementare

Traffic analysis: protocolli e traffico di cui avranno bisogno i servizi futuri, servizi e traffico attuale sulla rete.

NETWORK SECURITY

Nella progettazione di una rete bisogna tener conto anche delle minacce che agiscono sulla rete e ne possono danneggiare o deteriorare il funzionamento. Queste minacce possono essere:

1) Furto d'informazioni
2) Dati persi o appositamente manipolati
3) Furto d'identità
4) Distruzione di servizi

Per una maggiore sicurezza della rete è buona norma adottare anche una Physical Security, mettendo gli apparati in appositi spazi sotto chiave più o meno sorvegliati.
NB: indicando in apposita documentazione chi ha le chiavi, come reperirle, come accedere ai locali, ecc…

I principali tipi di vulnerabilità sono:

- ✓ Sui protocolli TCP/IP, come possono essere le falle su thhp, ftp, ecc…
- ✓ Sugli OS, come possono essere dei bug sul kernel linux, ecc…
- ✓ Sulle policy di sicurezza della rete, come può essere un AP lasciato con la password di default, ecc…

Tipi di Malware:

- ✓ Virus: tipi di malware che si auto replicano (con l'interazione umana) e diventano parte di altri programmi fino ad arrivare a causare Denied Of Service (DoS), per essere passati richiedono di essere attivi su file che vengono poi passati
- ✓ Worms: simili ai virus nella replica di se stessi, ma si auto replicano in autonomia
- ✓ Trojan Horses: consentono ad altri l'accesso al nostro host e possono gestirlo a loro piacimento

Oltre ai malware vi sono anche attacchi che possono essere effettuati sulla rete stessa e si dividono in:

- ✓ Reconnaissance (ricognizione): in cui l'attacco è atto alla raccolta di informazioni sul sistema, quali, porte aperte, servizi forniti, vulnerabilità
- ✓ Access (accesso): dove vengono tentati approcci di accesso agli apparati per cercare di predere il controllo della rete:
  - o password attack: bruteforce, dictionary, ecc…
  - o trusted exploitation: per arrivare all'hostA, che è protetto riesco a bucare l'hostB che non è adeguatamente protetto, ma che è ritenuto sicuro dall'hostA
  - o port redirection
  - o man in the middle
- ✓ Denied Of Service (DoS): la disabilitazione di servizi e la non raggiungibilità di server

Per effettuare questi attacchi si utilizzano strumenti molto utili per l'analisi della rete come **whois** e **nslookup**.

11.2.2.6 Lab - Researching Network Security Threats.pdf

Per ovviare ad alcuni di questi attacchi è bene:

- ✓ Mantenere i sistemi aggiornati, patchati, e svolgere un abituale processo di controllo dei backup
- ✓ Sfruttare il concetto di AAA (Authentication, Authorization, Accounting) ossia di autenticazione, autorizzazione, contabilità. E' un modo per controllare chi è autorizzato ad accedere a una rete (Authentication), cosa possono fare mentre sono lì (Authorization) e quali azioni eseguono durante l'accesso alla rete (Accounting).

Inserendo inoltre un firewall nella rete è possibile effettuare controlli di:

- **Packet filtering** – autorizzando o meno gli ip o i MAC address
- **Application filtering** – autorizza o meno determinate applicazioni in base alla porta utilizzata
- **URL filtering** – impedisce o meno l'accesso a determinati url o parole chiave
- **Stateful packet inspection (SPI)** - i pacchetti in entrata devono essere risposte legittime alle richieste degli host interni. I pacchetti non richiesti sono bloccati a meno che non sia consentito specificamente. SPI può anche includere la capacità di riconoscere e filtrare tipi specifici di attacchi, come il diniego di servizio (DoS)

Infine cercare di limitare il più possibile tutti i dispositivi di end-point, nello specifico limitare il più possibile le attività che gli utenti possono realmente fare sugli host a loro assegnati

Un comando molto utile al termine della configurazione di base è **auto secure** da dare in "Privilege Execute" per impostare in sicurezza tutti i parametri da me assegnati.

Altro punto fondamentale per una maggior sicurezza è la creazione delle password che devono essere il più "STRONG" possibili.

Altre "best practices" sugli apparati CISCO:
a partire dal configure terminal

```
service password-encryption
security password min-length 8
login block-for 120 attempts 3 with 60
line vty 0 15
exec-timeout 10
exit
```

Riassumendo: cifra le password, indica che le password dovranno essere di minimo 8 caratteri, che il sistema si bloccherà 120 secondi se vi saranno 3 tentativi di accesso sbagliati nell'arco di 60 secondi e come ultimo punto se dopo 10 minuti in cui la sessione telnet non riceve input, disconnette l'utente
Per abilitare la connessione agli apparati tramite ssh dalla configuration terminal dare i seguenti comandi.

```
ip domain-name mydomain.local
crypto key generate rsa general-keys modulos 1024
username mio_username secret mia_password
line vty 0 15
login local
transport input ssh
exit
```

11.2.4.5 Packet Tracer - Configuring Secure Passwords and SSH.pdf
11.2.4.5 Packet Tracer - Configuring Secure Passwords and SSH.pka
11.2.4.8 Lab - Securing Network Devices.pdf

NETWORK PERFORMANCE

Interpretare i risultati del ping in IOS:
! – indica la ricezione di un messaggio ICMP
. – indica che un tempo è scaduto durante la richiesta di attesa di un TTL. Può indicare che un problema di connettività si è verificato da qualche parte lungo il percorso. Può anche indicare che un router lungo il percorso non ha avuto un percorso verso la destinazione e non ha inviato un messaggio non raggiungibile destinazione ICMP. Può anche indicare che il ping è stato bloccato dalla protezione del dispositivo
U – indica che un router lungo il percorso ha mandato un pacchetto ICMP indicando che la destinazione è irraggiungibile
ATTENZIONE: il ping può anche essere lanciato senza mettere l'host da raggiungere come parametri, in questo caso l'IOS mi porrà alcune domande per poter espletare la sua funzionalità. E tra le opzioni vi è anche quella di poter mettere un differente indirizzo sorgente. Questa funzionalità è molto utile nel Trubleshouting.

Nella manutenzione della rete è buona norma tenere monitorati i link facendo dei ping e segnandomi i risultati nel tempo in modo tale da sapere se la rete inizia ad avere anomalie o se devo valutare un'implementazione.

Interpretare anche i risultati del **traceroute** (tracert in Windows)

11.3.2.3 Packet Tracer - Test Connectivity with Traceroute.pdf
11.3.2.3 Packet Tracer - Test Connectivity with Traceroute.pka
11.3.2.4 Lab - Testing Network Latency with Ping and Traceroute.pdf

Comandi per visualizzare le configurazioni esistenti o apportate
show running-config - mostra la configurazione che stà girando sull'apparato
show interfaces - mostra le interfaccie dell'appareto, lo stato in cui sono e tutti i dati a disposizione
show arp - mostra la tabella di arp
show ip route - mostra la tabella di routing
show protocols - mostra le interfacce se sono up o down e gli eventuali ip assegnati
show version - mostra la versione dello IOS la ram e la nvram a disposizione sul dispositivo

11.3.3.3 Packet Tracer - Using Show Commands.pdf
11.3.3.3 Packet Tracer - Using Show Commands.pka

Comandi ed utility comode possono essere ipconfig/ifconfig, tracert, arp

Un comando molto utile che vi è su IOS è **show cdp neighbors**
Tale comando funziona e produce risultato solamente tra apparati CISCO ed il risultato mi dice tutti gli apparati direttamente collegati all'apparato sul quale ho dato il comando, con relative informazioni aggiuntive.

show ip interface brief - mostra tutte le interfacce sul router, l'indirizzo IP assegnato ad ogni interfaccia, se presente, e lo stato operativo dell'interfaccia.

11.3.4.6 Lab - Using the CLI to Gather Network Device Information.pdf

La funzione di debug può risultare molto utile, e come tale, gli apparati le danno molta importanza/priorità, per cui prima di avviarla, è bene lanciare il comando **undebug all** che non apporterà nessun cambiamento al dispositivo, ma essendo che la funzione di debug potrebbe essere molto esosa di risorse hardware, così facendo sappiamo che premendo 2 volte la freccia in su e dando invio potremmo fermare l'attività.
Una delle informazioni che mi può dare il debug è se le interfacce ad esempio di rete non sono configurate entrambe nello stesso modo (es. HalfDuplex o Auto, ecc…) in questo caso otterrò molti errori di collision o lite collision.
Ora possiamo lanciare la funzione, come ad esempio:
debug ip icmp
NB: la funzione di debug è attivabile in locale, cioè quando sono collegato con il cavo console. Per attivarla (e vedere l'output) anche in telnet o ssh bisogna dare il comando **terminal monitor**

NETWORK TROUBLESHOOTING

Per risolvere il problema nel minor tempo possibile è bene adottare una tipologia d'intervento ed applicarla sempre senza saltare nessun passaggio. O applicando la Top-Down o la Bottom-UP dei seguenti punti:

1) Identificare il problema
2) Stabilire una teoria dell'eventuali cause
3) Test della teoria per determinare le eventuali cause
4) Stabilire un piano ed un'azione per risolvere il problema ed implementare la soluzione
5) Verificare di aver definitivamente risolto il problema
6) Creare un'apposita documentazione della casistica

IMPORTANTE: se non so o non riesco a risolvere il problema devo avere uno strumento od una persona a cui posso demandare il problema, conscio del fatto che il problema debba essere risolto

11.4.3.5 Lab - Troubleshooting Connectivity Issues.pdf
11.4.3.6 Packet Tracer - Troubleshooting Connectivity Issues.pdf
11.4.3.6 Packet Tracer - Troubleshooting Connectivity Issues.pka
11.5.1.1 Class Activity - Design and Build a Small Network.pdf
11.5.1.2 Packet Tracer - Skills Integration Challenge.pdf
11.5.1.2 Packet Tracer - Skills Integration Challenge.pka
11.5.1.3 Packet Tracer - Troubleshooting Challenge.pdf
11.5.1.3 Packet Tracer - Troubleshooting Challenge.pka

Modulo 2

1.0.1.2 Do We Really Need a Map Final Instructions.pdf

Caratteristiche di una rete:

- Topology (topologia): può essere:
  - Fisica: è l'insieme dei cavi e dei device ed indica come sono tra loro interconnessi;
  - Logica: è il percorso su cui i dati vengono trasferiti in una rete, descrive come i dispositivi di rete appaiono connessi agli utenti della rete.
- Speed: è la misura della velocità con cui i dati si muovono sui link. Generalmente viene riportato come dato il bandwidth, anche se non è un dato molto accurato per questo parametro
- Cost: è il costo di installazione e manutenzione della rete per mantenerla allo stato attuale o implementarla
- Security: indica quanto la rete è protetta
- Availability (disponibilità): è la probabilità che la rete sia disponibile all'uso quando richiesta
- Scalability: indica quanto facilmente la rete può ospitare più utenti e requisiti di trasmissione dati. Se un progetto di rete è ottimizzato per soddisfare solo le esigenze correnti, può essere molto difficile e costoso soddisfare nuove esigenze quando la rete cresce
- Reliability (affidabilità): indica l'affidabilità della componentistica della rete. L'affidabilità è spesso misurata come probabilità di guasto o come tempo medio tra guasti (MTBF).

I router sono essenzialmente dei computer, composti da CPU, RAM, e Storage e tutto questo hardware è gestito dal Sistema Operativo (IOS).

Le memorie dei router si dividono in:

- ✓ RAM: è la memoria volatile che salta quando tolgo corrente, e contiene: running config, running IOS, IP routing e ARP table, packet buffer
- ✓ ROM: memoria non volatile in sola lettura e contiene: bootup istruction, basic diagnostic software, IOS base per avviare il router in caso di malfunzionamenti
- ✓ NVRAM: è la ram non volatile che contiene la start-up config
- ✓ Flash: è lo storage vero e proprio e contiene l'IOS (compresso) e gli altri file (data file) necessari al sistema

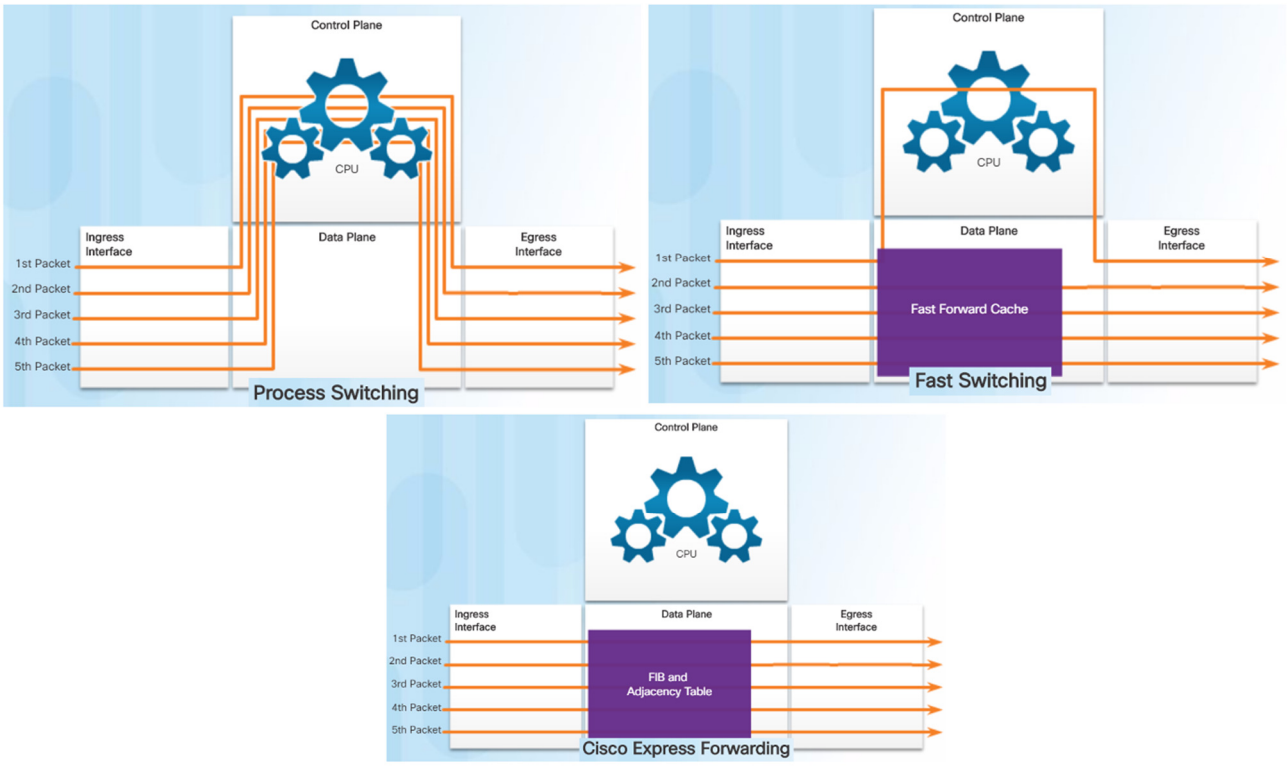
Le funzioni principali dei router sono:

- ✓ Individuare la miglior strada per consegnare un pacchetto
- ✓ Effettuare il forward del pacchetto su quella strada

I meccanismi di forward dei pacchetti sono 3:

- Process Switching: il pacchetto arriva su un'interfaccia, viene inoltrato al "Control Plane" in cui la CPU analizza il pacchetto ed in base alla sua tabella di routing determina l'interfaccia di uscita, ed inoltra il pacchetto. È un meccanismo molto dispendioso di risorse e nelle reti moderne è raramente implementato
- Fast Switching: è un sistema che utilizza una cache di commutazione rapida. Il pacchetto arriva su un'interfaccia, viene inoltrato al "Control Plane" in cui la CPU cerca una corrispondenza nella cache di commutazione rapida. Se non è presente, viene commutato al processo e inoltrato all'interfaccia di uscita. Le informazioni di flusso per il pacchetto sono memorizzate anche nella cache di commutazione rapida. Se un altro pacchetto che va alla stessa destinazione arriva su un'interfaccia, le informazioni di hop successive nella cache vengono riutilizzate senza l'intervento della CPU.

- Cisco Express Forwarding (CEF): Come per il Fast Switching, costruisce una "Forward Information Base" (FIB) ed una tabella di adiacenza. Le voci di tabella non vengono attivate da pacchetti come la commutazione veloce, ma vengono commutati, ad esempio quando qualcosa cambia nella topologia di rete. Pertanto, quando una rete è convergente, le tabelle FIB e adiacenza contengono tutte le informazioni che un router dovrebbe prendere in considerazione quando si inoltra un pacchetto. La FIB contiene ricerche inverse pre-calcolate, informazioni successive di hop per percorsi tra cui l'interfaccia e le informazioni Layer 2. Cisco Express Forwarding è il meccanismo di inoltro più rapido e la scelta preferita sui router Cisco.

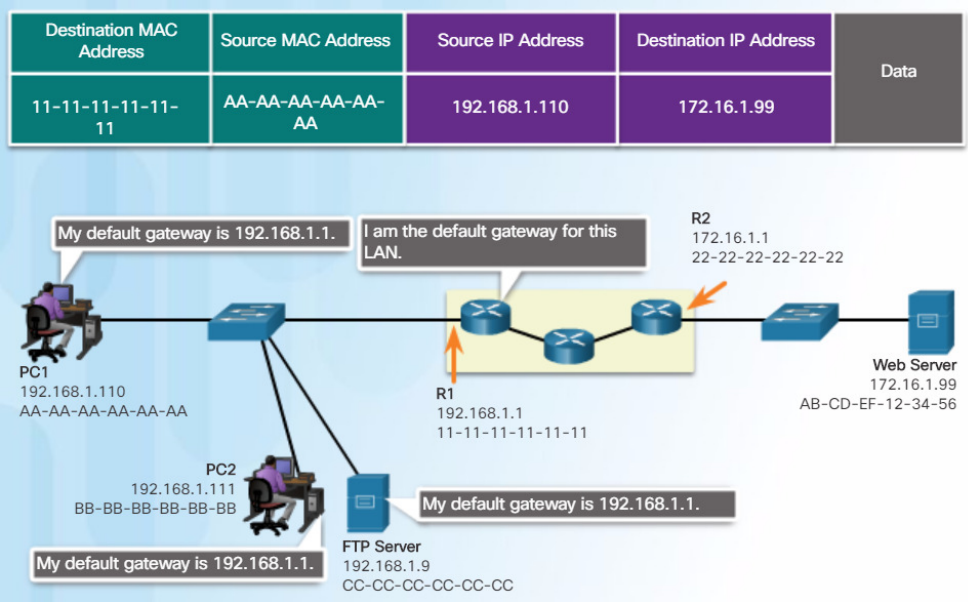


L'esasperazione tra il Control Plane (Learing what we will do) e il Data Plane (Moving the packets based on what we learned) è l'SDN (Software Defined Networking)

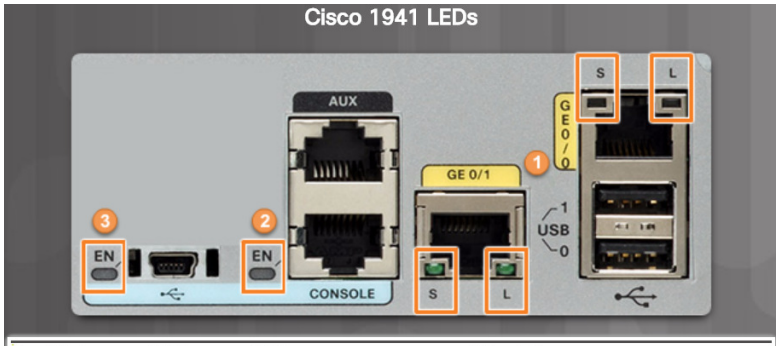
Semplificando/parafrasando con un esempio, abbiamo:

- Process Switching: come risolvere un problema di matematica scrivendo tutte le operazioni e senza saltare nemmeno un passaggio, per ogni problema che mi viene presentato
- Fast Switching: risolvo un problema di matematica scrivendo tutti i passaggio e mi faccio di conseguenza uno schema risolutivo, così facendo per le prossime casistiche simili farò prima
- CEF: risolvo il problema tramite una tabella excel che mi vado ad implementare con casistiche differenti man mano che mi capitano, ma poi basta cambiare i dati e in quattro e quattr'otto avrò le soluzioni future

1.1.1.8 Packet Tracer - Using Traceroute to Discover the Network instructions.pdf
1.1.1.8 Packet Tracer - Using Traceroute to Discover the Network.pka
1.1.1.9 Lab - Mapping the Internet.pdf



NOTE:
Quando un host invia un pacchetto a un dispositivo che si trova sulla stessa rete IP, il pacchetto viene semplicemente inoltrato dall'interfaccia host al dispositivo di destinazione.
Quando un host invia un pacchetto a un dispositivo su una rete IP diversa, il pacchetto viene inoltrato al gateway predefinito, in quanto un dispositivo host non può comunicare direttamente con i dispositivi esterni alla rete locale.



#	Port	LED	Color	Description
1	GE0/0 and GE0/1	S (Speed)	1 blink + pause	Port operating at 10 Mb/s
			2 blink + pause	Port operating at 100 Mb/s
			3 blink + pause	Port operating at 1000 Mb/s
		L (Link)	Green	Link is active
			Off	Link is inactive
2	Console	EN	Green	Port is active
			Off	Port is inactive
3	USB	EN	Green	Port is active
			Off	Port is inactive

Port on Computer	Cable Required	Port on ISR	Terminal Emulation
Serial Port	RJ-45-to-DB-9 Console Cable	RJ-45 Console Port	Tera Term
USB Type-A Port	• USB-to-RS-232 compatible serial port adapter • Adapter may require a software driver • RJ-45-to-DB-9 console cable		
	• USB Type-A to USB Type-B (Mini-B USB) • A device driver is required and available from cisco.com.	USB Type-B (Mini-B USB)	PuTTY

Abilitare l'IPv4 su uno switch:
A partire dalla configuration terminale:
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
ip default gateway 192.168.1.1

1.1.2.9 Packet Tracer - Documenting the Network Instructions.pdf

Abilitare l'IPv6 su un router (a partire dalla configuration terminal)
interface gigabitethernet 0/0
description LINK to LAN 1
ipv6 address 2001:db8:acad:1::1/64
no shutdown
exit

L'interfaccia di loopback è un'interfaccia sempre "UP" di default che non è assegnata e nessuna porta fisica e che può essere molto utile in fase di test e di trubleshooting. Vediamo anche come impostarla, sempre a partire dalla configuration terminal

interface loopback 0
ip address 10.0.0.1 255.255.255.0
exit

1.1.3.5 Packet Tracer - Configuring IPv4 and IPv6 Interfaces Instructions.pdf
1.1.3.5 Packet Tracer - Configuring IPv4 and IPv6 Interfaces.pka

Comandi di verifica delle interfacce, da lanciare nella privileged exec:

show ip brief interface: visualizza un riepilogo per tutte le interfacce
show ip route: visualizza il contenuto della tabella di routing IPv4 memorizzata in RAM. In Cisco IOS 15, le interfacce attive dovrebbero apparire nella tabella di routing con due voci correlate identificate dal codice 'C' (collegato) o 'L' (locale). L è l'IP dell'interfaccia del router
show running-config interface gigabitethernet 0/0: visualizza i comandi configurati sull'interfaccia g0/0
show interfaces gigabitethernet 0/0: visualizza tutti i dati dell'interfaccia g0/0 compresi errori ecc… molto utili in fase di trubleshooting
show ip interface gigabitethernet 0/0: visualizza tutte le informazioni dell'interfaccia riguardanti l'IPv4

NB: per quanto riguarda l'ipv6 basta aggiungere v6 accanto ad ip ai comandi sopra

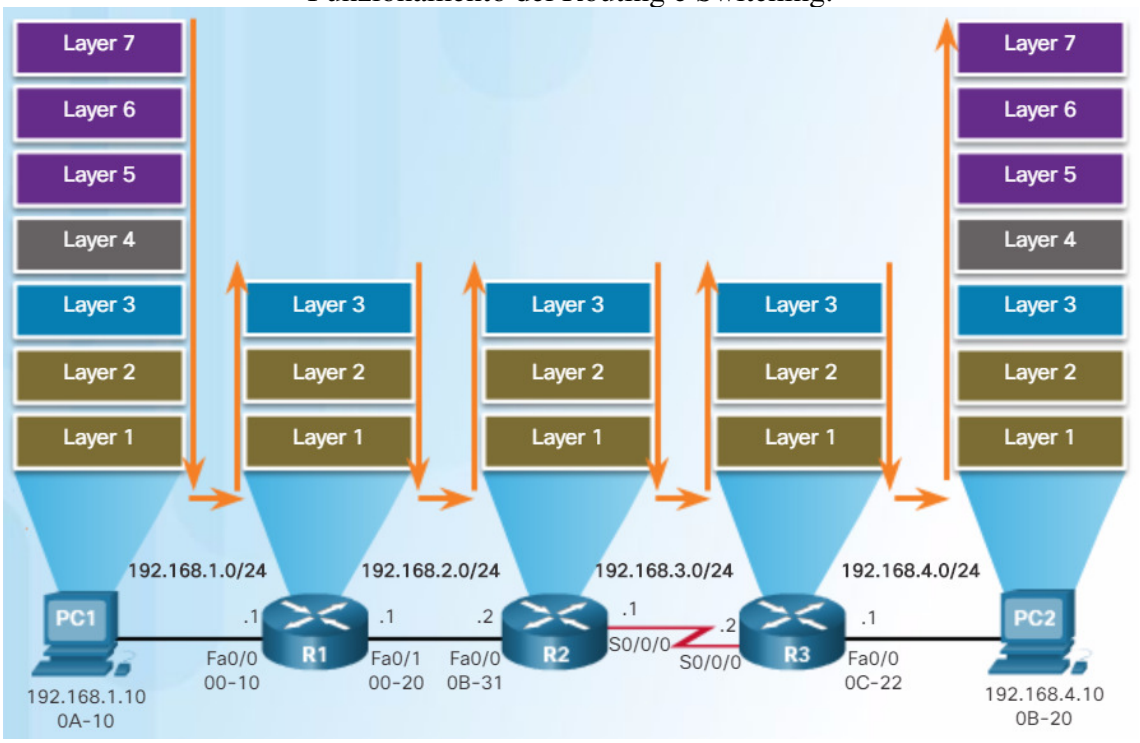
Nel terminale di configurazione degli apparati, vi sono alcune scorciatoie e soluzioni che possono tornare utili per leggere meglio l'output da console, come i seguenti comandi:

section: mostra tutta la sezione che inizia con l'espressione di filtraggio
include: include tutte le linee di output che corrispondono all'espressione filtrante
exclude: esclude tutte le linee di output che corrispondono all'espressione di filtraggio
begin: mostra tutte le linee di uscita da un certo punto, partendo dalla riga che corrisponde all'espressione filtrante
Esempio:
show running-config | section line vty (viene mostrata la sezione di configurazione di telnet)

Di default la history dei comandi è impostata agli ultimi 10, se la si vuole incrementare basta dare il comando: **terminal history size 200** (così la si porta agli ultimi 200 comandi, che sono memorizzati in RAM e vengono cancellati al riavvio o se effettuo un logout).

1.1.4.5 Packet Tracer - Configuring and Verifying a Small Network Instructions.pdf
1.1.4.5 Packet Tracer - Configuring and Verifying a Small Network.pka
1.1.4.6 Lab - Configuring Basic Router Settings with IOS CLI.pdf

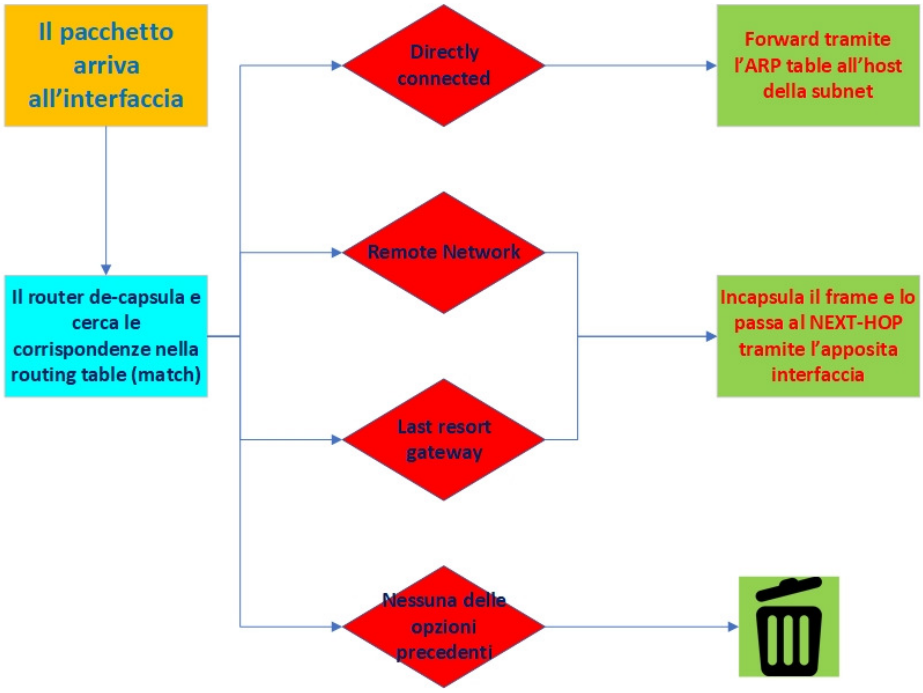
Funzionamento del Routing e Switching.



In ogni router (o switch di layer3) abbiamo le seguenti 3 fasi:

a) Decapsulamento dell'intestazione e del trailer del frame L2 leggere il pacchetto L3
b) Viene esaminato l'indirizzo IP di destinazione del pacchetto IP per trovare il percorso migliore nella tabella di routing.
c) Se il router trova un percorso alla destinazione, re-incapsula il pacchetto L3 in un nuovo frame di L2 e lo inoltra all'interfaccia di uscita.

Packet Forwarding Decision Process



Una delle funzioni primarie di un router è decidere dove instradare i pacchetti che riceve. E per fare ciò controlla la sua Routing Table che verifica se:
Directly connected: l'IP di destinazione del pacchetto appartiene a un dispositivo su una rete direttamente connessa a una delle interfacce del router. Ciò significa che l'IP di destinazione del pacchetto è un indirizzo host sulla stessa rete dell'interfaccia del router.
Remote network: l'IP di destinazione del pacchetto appartiene a una rete remota, il pacchetto viene inoltrato a un altro router.
Last resort gateway: un gateway di ultima risorsa viene impostato quando una route predefinita viene configurata o appresa su un router.
Nessuna delle opzioni precedenti: nel caso nessuna delle precedenti opzioni risulti vera, il pacchetto viene "droppato"

Ad ogni collegamento tra router o switch L3, nella routing table, viene assegnato un valore di metrica ed uno di "Administrative Distance". Questi valori servono per consentire ad ogni "nodo" di poter decidere su quale link è meglio instradare i pacchetto per l'apposita rete di destinazione.
Poiché i pacchetti possono raggiungere la stessa destinazione uscendo da differenti porte del router.
La metrica è il valore quantitativo utilizzato per misurare la distanza di una determinata rete (è in pratica il conto degli HOP). Il percorso migliore per una rete è il percorso con la metrica più bassa. Nell'impostazione di route statica, il valore di default della metrica è 1. Per impostare un valore differente ad una rotta statica, basta impostare il valore in fondo alla riga.
Es: **ip route 192.168.2.0 255.255.255.0 172.16.1.6 10**
I protocolli di routing dinamico utilizzano in genere le proprie regole e metriche per creare e aggiornare la routing table. L'algoritmo di routing che viene utilizzato, genera un valore (Administrative Distance) o una metrica per ogni percorso attraverso la rete. Le metriche possono essere basate su una singola caratteristica o su diverse caratteristiche di un percorso. Alcuni protocolli di routing possono basare la selezione del percorso su più metriche, combinandole in un'unica metrica.

Di seguito un elenco di alcuni protocolli dinamici:

- RIP (Routing Information Protocol): è un protocollo in cui vengono conteggiati gli hop
- OSPF (Open Shortest Path First): è un protocollo di routing link state, dove viene valutato il costo della larghezza di banda cumulativa dall'origine alla destinazione
- EIGRP (Enhanced Interior Gateway Routing Protocol): è un protocollo proprietario CISCO, di tipo distance-vector ed è basato su bandwidth, delay, load e reliability (larghezza di banda, ritardo, carico, affidabilità)

NB: se in routing table vi sono più rotte per raggiungere la stessa rete, con egual metrica, i router inviano i pacchetti in load balancing (ossia uno da una parte ed uno dall'altra). Solamente il protocollo EIGRP supporta anche un load balancing non proporzionale (es. 30% dei pacchetti su un'interfaccia e il restante su un'altra interfaccia)

È possibile configurare un router con più protocolli di routing e percorsi statici. In questo caso, la tabella di routing potrebbe avere più di una sorgente di percorso per la stessa rete di destinazione. Tuttavia, ciascun protocollo di routing può decidere su un percorso diverso per raggiungere la destinazione in base alle metriche del protocollo di routing.
Solamente che ci troveremmo a confrontare ad esempio del Litri con dei Kilogrammi… QUINDI????

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

Cisco IOS utilizza la cosiddetta "Administrative Distance" (AD) per determinare la route da installare nella tabella di routing IP. L'AD rappresenta "l'affidabilità" del percorso, più basso è l'AD, più affidabile è la fonte del percorso (vedi figura accanto).

La Routing Table memorizza informazioni su:

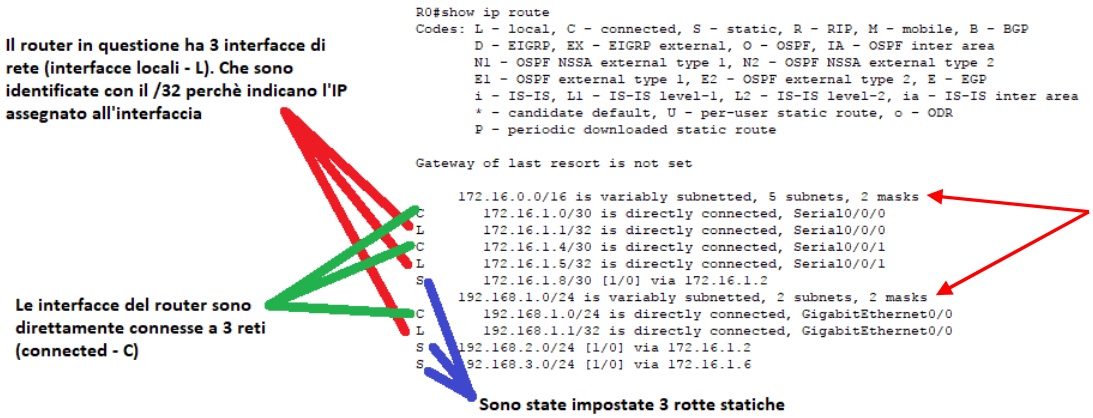
- ✓ Directly connected routes: questi percorsi provengono dalle interfacce router attive alle quali è stato assegnato un IP
- ✓ Remote routes: sono reti remote collegate ad altri router. I percorsi verso queste reti possono essere configurati staticamente o appresi in modo dinamico tramite i protocolli di routing dinamico.

La tabella di routing contiene le associazioni di rete o di next-hop.
L'associazione next-hop può essere l'IP del next-hop oppure interfaccia di uscita verso il next-hop.
ES.: **ip route 192.168.2.0 255.255.255.0 172.16.1.6**
ip route 192.168.2.0 255.255.255.0 gigabitethernet 0/0
NB: si possono anche mettere entrambe:
ip route 192.168.2.0 255.255.255.0 172.16.1.6 gigabitethernet 0/0
Le voci nella routing table possono essere aggiunte come:

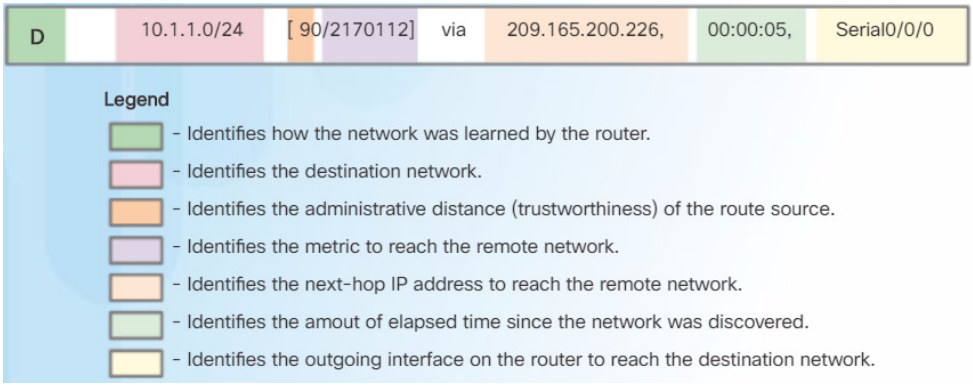
- ➢ Local route interface: aggiunte quando un'interfaccia è configurata e attiva
- ➢ Directly connected interface: aggiunte quando un'interfaccia è configurata e attiva
- ➢ Static routes: aggiunta quando un percorso viene configurato manualmente e l'interfaccia di uscita è attiva
- ➢ Dynamic routing protocol: aggiunto quando i protocolli di routing che apprendono in modo dinamico sulla rete

Ogni riga in routing table viene presentata con un codice che ne indica la modalità di apprendimento L, C, S, D, O, …
Analizziamo la tabella di routing di un router CISCO, dando il comando:
show route ip

Leggendone l'output:



Rimane da notare che per ogni subnet direttamente connessa al dispositivo, compare una riga riassuntiva della ClassFul di appartenenza



Esempio di riga di dati raccolti da un routing dynamic di tipo EIGRP

1.3.2.5 Packet Tracer - Investigating Directly Connected Routes Instructions.pdf
1.3.2.5 Packet Tracer - Investigating Directly Connected Routes.pka

Se si vuole indicare la default route, il comando da dare è:
ip route 0.0.0.0 0.0.0.0 Next-Hop-IP Interface-EXIT

Per determinare quali protocolli di routing dinamico sono supportati dal router che stiamo utilizzando, in configuration terminal basta dare il comando:
router ?
ed otterremo l'elenco dei protocolli utilizzabili ed abilitabili.

Prima di procedere oltre, con i protocolli di routing dinamico, spieghiamo le tipologie:

- Link state: richiede che tutti i router siano a conoscenza di tutti i percorsi raggiungibili dagli altri router della rete.
- Distance Vector: utilizzano Administrative Distance e metrica, un router sa da quale vicino è stata appresa una rotta, ma non sa dove quel vicino ha imparato il percorso, quindi un router non può vedere oltre i propri vicini. (attenzione ai loop)

1.4.1.1 We Really Could Use A Map Instructions.pdf

FINE CAPITOLO 1

1.4.1.1 We Really Could Use A Map Instructions.pdf

Vantaggi e svantaggi delle rotte statiche e di quelle dinamiche

	Dynamic Routing	Static Routing
Configuration Complexity	indipendente dalle dimensioni del Network	aumenta con il crescere del Network
Topology Change	si auto-adatta al cambiamento	Richiede l'intervento dell'amministratore
Scaling	utilizzabile in semplici e complesse topologie	utilizzabile in semplici topologie
Security	poco sicura	sicura
Resorce Usage	CPU, RAM, Link Bandwith	nessuna risorsa extra
Predictability	le rotte dipendono dalla topologia	le rotte sono sempre le stesse

Nella configurazione delle Static Route è bene prevedere anche delle Floating Route, ossia delle rotte che vengono utilizzate di backup nel caso la rotta principale non funzioni.
Per impostare una floating route basta aggiungere un parametro alla fine della configurazione di una rotta. Essendo le rotte statiche con valore di metrica 1, per far si che la rotta sia di floating basta mettere questo valore >1
ES. (in configuration terminal): OPZIONALE

ip route rete_remota netmask_remota ip_next-hop interfaccia_uscita administrative_distance
ip route 192.168.2.0 255.255.255.0 172.16.1.6 gigabitethernet 0/0 10
NB: se vi è sia il next-hop sia l'interfaccia di uscita, la rotta viene detta **Fully Specified Static Route**

Vediamo ora anche come configurare le Static Route IPv6
ipv6 route 2001:db8:acad:2::/64 s0/0/0 fe80::2 (Fully Specified Static Route)
Il comando di configurazione globale:
ipv6 unicast-routing
deve essere configurato per consentire al router di inoltrare i pacchetti IPv6
Visualizzare la routing table IPv6
show ipv6 route
NB: l'output si legge nello stesso modo della routing table IPv4 e vale lo stesso discorso anche per le floading route

Possiamo anche visualizzare rotte nello specifico dando i comandi:
show ipv6 route static
show ipv6 route 2001:db8:acad:2::/64
show running-config | section ipv6 route

Impostare la default route ipv6
ipv6 route ::/0 fe80::2 s0/0/0

2.2.2.4 Packet Tracer - Configuring IPv4 Static and Default Routes Instructions.pdf
2.2.2.4 Packet Tracer - Configuring IPv4 Static and Default Routes.pka
2.2.2.5 Lab - Configuring IPv4 Static and Default Routes.pdf
2.2.4.4 Packet Tracer - Configuring IPv6 Static and Default Routes Instructions.pdf
2.2.4.4 Packet Tracer - Configuring IPv6 Static and Default Routes.pka
2.2.4.5 Lab - Configuring IPv6 Static and Default Routes.pdf
2.2.5.5 Packet Tracer - Configuring Floating Static Routes Instructions.pdf

Per fare trubleshooting utilizzare i seguenti comandi:
ping
traceroute
show ip route
show ip interface brief
show cdp neighbors detail

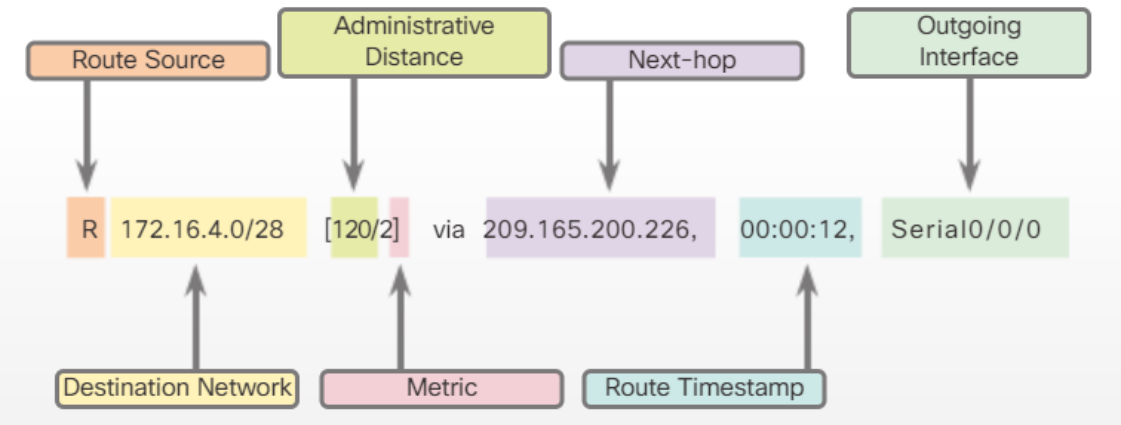
2.3.2.3 Packet Tracer - Troubleshooting Static Routes Instructions.pdf
2.3.2.3 Packet Tracer - Troubleshooting Static Routes.pka
2.3.2.4 Lab - Troubleshooting IPv4 and IPv6 Static Routes.pdf
2.4.1.1 Class Activity - Make It Static Instructions.pdf

NB: se una porta è configurata una rotta statica và in down, la rotta statica viene tolta dalla tavella di routing

FINE CAPITOLO 2

3.0.1.2 How Much Does This Cost Instructions.pdf

Vediamo ora come abilitare i sistemi di Dynamic Route che ci possono servire:
Abilitiamo il RIP a partire sempre dalla configuration terminal:
router rip
version 2
ora indichiamo quali informazioni delle reti a bordo del router vogliamo propagare (inserendo la classful)
network 192.168.1.0
network 172.16.0.0
NB: ogni informazione viene propagata a tutti i router connessi su tutte le interfacce attive (broadcast), se vogliamo negare l'invio su una determinata interfaccia (es. perché sappiamo che non vi sono apparati L3 collegati a quell'interfaccia) diamo il comando:
passive-interface g0/0
Naturalmente se non propago una rete questa non si attiva nella ricezione del rip
Per verificare il settagio del RIP, da privileged exec:
show ip protocols
show ip route
Summarization (sommarizzazione), è il contrario del subnetting. Ossia è il modo di accorpare più reti (subnet o classful che siano). Per capirle meglia facciamo un esempio:
192.168.0.0/24 → 11000000.10101000.00000000.00000000
192.168.1.0/24 → 11000000.10101000.00000001.00000000
192.168.2.0/24 → 11000000.10101000.00000010.00000000
192.168.3.0/24 → 11000000.10101000.00000011.00000000
Come si vede dalla linea rossa nelle 4 reti indicate possono variare solo gli ultimi 10bit, per cui la rete può essere sommarizzata in 192.168.0.0/22
ATTNZIONE:
Di default nel protocollo RIP è prevista la summarization delle reti solo a livello di classful, quindi l'esempio sopra non mi viene fatto automaticamente. Comunque è meglio inibirla e basta dare il comando:
no auto-summary
Per propagare anche le default route agli altri router, basta dare il comando (dopo essere entrato in router rip)
default-information originate
3.2.1.8 Packet Tracer - Configuring RIPv2 Instructions.pdf
3.2.1.8 Packet Tracer - Configuring RIPv2.pka
3.2.1.9 Lab - Configuring Basic RIPv2.pdf
Riassumendo con uno schema abbiamo come leggere le righe della routing table



Le route si dividono in:

- Ultimate route: identifica una rotta che contiene un indirizzo ipv4 nel next-hop o un'interfaccia d'uscita
- Level 1 route: è una rotta con una netmask uguale o inferiore alla classful dell'indirizzo di rete, e si può dividere in:
  - Network route: è un indirizzo di rete con una subnet mask uguale a quella della maschera classful
  - Supernet route: è un indirizzo di rete con una netmask inferiore alla classful
  - Default route: è una rotta con l'indirizzo 0.0.0.0/0
- Level 1 parent route: è una level 1 route con una subnet, ossia è identificata da un NET ip e non può mai essere un'ultimate route
- Level 2 child route: è una route identificata da una subnet di una classful ed in ordine di visualizzazione è sotto alla Level 1 parent route che la ingloba. Anche queste rotte sono Ultimate route

Vediamo ora come funziona il processo di ricerca del percorso:
Quando un pacchetto arriva su un'interfaccia, il router esamina l'intestazione IPv4, identifica l'indirizzo IPv4 di destinazione e procede attraverso il processo di ricerca nella routing table.

1) Il router esamina i percorsi di rete di livello 1 per la migliore corrispondenza con l'indirizzo di destinazione del pacchetto IPv4:
   a. se la migliore corrispondenza è una "level 1 route", questa rotta viene utilizzata per inoltrare il pacchetto.
   b. se la migliore corrispondenza è una "level 1 parent route", procede al passaggio successivo
2) Il router esamina le "level 2 child" (le sottoreti della "level 1 parent route") per una corrispondenza migliore:
   a. se esiste una corrispondenza con un "level 2 child", tale sottorete viene utilizzata per inoltrare il pacchetto
   b. se non c'è una corrispondenza con nessuno dei "level 2 child", procedere al passaggio successivo
3) Il router riparte a cercare le "level 1 route" nella tabella di routing per una corrispondenza, inclusa la route predefinita:
   a. se ora c'è una corrispondenza minore con una "level 1 route" o un percorso predefinito, il router utilizza quella rotta per inoltrare il pacchetto
   b. se la tabella di instradamento non corrisponde a nessun percorso, il router "droppa" il pacchetto

NB: la ricerca all'interno della routing table deve fornire il BEST MATCH (miglior corrispondenza). Tale risultato è garantito mandando il pacchetto sulla rotta più restrittiva a lui corrispondente. (come in figura sotto).

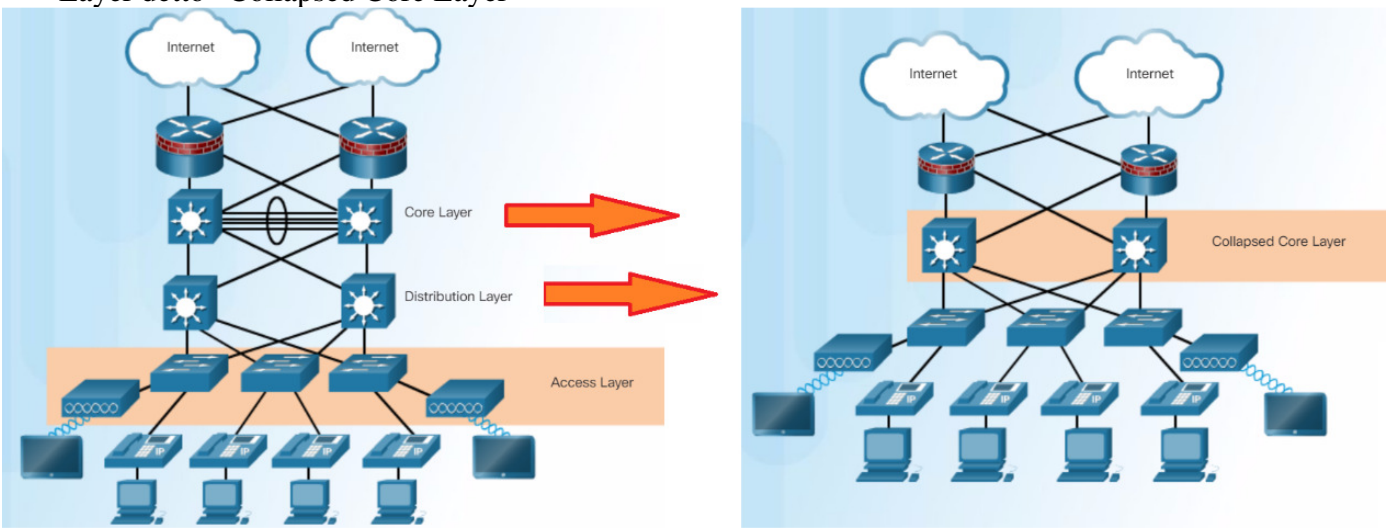
3.4.1.1 Class Activity - IPv6 - Details, Details... Instructions.pdf

FINE CAPITOLO 3

Gli elementi che convergono (che utilizzano) la rete possono essere svariati (telefonia, navigazione, e-mail, streaming audio-video, ecc…) per cui uno studio della gestione futura ed implementazione della rete **è fondamentale** in fase di progettazione.
Per semplificare la progettazione della rete, dobbiamo far riferimento principalmente alla configurazione di apparati su 3 livelli:

- Access Layer: sono i dispositivi ai quali collego fisicamente i miei terminali di utilizzo della rete (es. i PC e le periferiche)
- Distribution layer: è la parte degli apparati di rete che si interfaccia con gli access layer e scambia i dati con il livello superiore
- Core Layer: è il cuore pulsante dell'azienda, quello che contiene tutti i dati elaborati e da elaborare

Molto spesso per una questione di costi il Core Layer e il Distribution Layer vengono fusi in un unico Layer detto "Collapsed Core Layer"



Per quanto riguarda tutta le funzionalità, suddivisione e scelta degli switch ripassare il Modulo 1
Tipi d iswitch → Capitolo 11 (pag. 40)
Metodologie di inoltro dei frame → Capitolo 4 (pag. 17)

4.3.1.1 It's Network Access Time Instructions.pdf

Comandi per configurazione base dello switch

```
hostname R1
enable secret password
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
service password-encryption
interface vlan 1
ip address 192.168.1.2 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.1.1
```

FINE CAPITOLO 4

5.0.1.2 Stand By Me Instructions.pdf

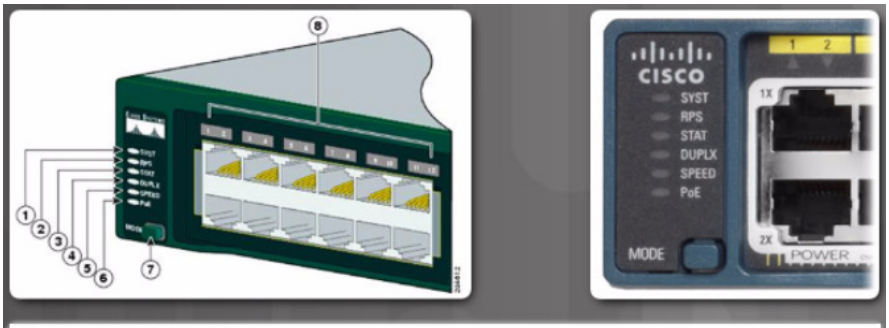
Metodologia di avvio dello switch:

1) Lo switch carica il POST (Power-On Self-Test) e testa l'hardware al suo interno
2) Lo switch carica il boot loader (che si trova in ROM). Il boot loader inizializza la CPU a basso livello, ed il file system della flash sull'apparato. Infine il boot loader individua e carica l'immagine del sistema operativo (IOS)
3) Se l'immagine del sistema operativo sulla flash non viene trovato, lo switch inizia una ricerca ricorsiva nelle cartelle della flash per ricercare un'immagine del Sistema Operativo avviabile.
4) Quando il sistema operativo è caricato, lo switch utilizza i comandi forniti dallo IOS per caricare le configurazioni (che si trovano in NVRAM) e per inizializzare le porte con le relative configurazioni

Lo switch potrebbe anche non essere più raggiungibile (per errori di configurazione, per cui potrebbe essere necessario accedervi in modalità recovery nel seguente modo:

- ✓ collegare un PC tramite un cavo console alla porta della console dello switch e configurare il software di emulazione terminale per connettersi allo switch
- ✓ scollegare il cavo di alimentazione dell'interruttore
- ✓ ricollegare il cavo di alimentazione all'interruttore ed entro 15 secondi, premere e tenere premuto il pulsante MODE mentre il led di sistema continua a lampeggiare in verde
- ✓ continuare a premere il pulsante MODE fino a quando il led System diventa brevemente giallo e poi verde fisso, quindi rilasciare il pulsante MODE
- ✓ a questo punto viene visualizzato il prompt dei comandi all'interno del software di emulazione del terminale sul PC

NOTA: la riga di comando del boot loader supporta i comandi per formattare il file system flash, reinstallare il software del sistema operativo e recuperare una password persa o dimenticata



Catalyst 2960 Switch LEDs

1	The system LED
2	The RPS LED (if RPS is supported on the switch)
3	The port status LED (This is the default mode.)
4	The port duplex mode LED
5	The port speed LED
6	The PoE status LED (if PoE is supported on the switch)
7	The Mode button
8	The port LEDs

Tabella riassuntiva su come leggere le indicazioni fornite dai led dello switch

Uno switch per poter essere amministrato e gestito ha necessità di aver configurato un indirizzo IP. Tale IP negli switch non può essere assegnato a nessuna interfaccia, ma semplicemente essere assegnato ad una VLAN (configurazione vista in precedenza).
È possibile anche creare altre VLAN (oltre alla VLAN 1 creata di default dal sistema).
La VLAN 1 è assegnata di default a tutte le porte, mentre per assegnare ad una determinata porta (interfaccia) altre vlan create secondariamente bisogna dare l'apposito comando switchport

```
vlan 99
name vlan99_management
exit
interface g0/0
switchport access vlan 99
```

5.1.1.6 Lab - Configuring Basic Switch Settings.pdf

Cambiare impostazioni di scambio dati alle interfacce

```
interface fa0/0
duplex full
speed 100
```

oppure:

```
interface fa0/0
duplex auto
speed auto
```

se vogliamo impostare l'auto assegnazione della porta in base al cavo usato (se dritto o rovescio) do il comando all'interno della porta

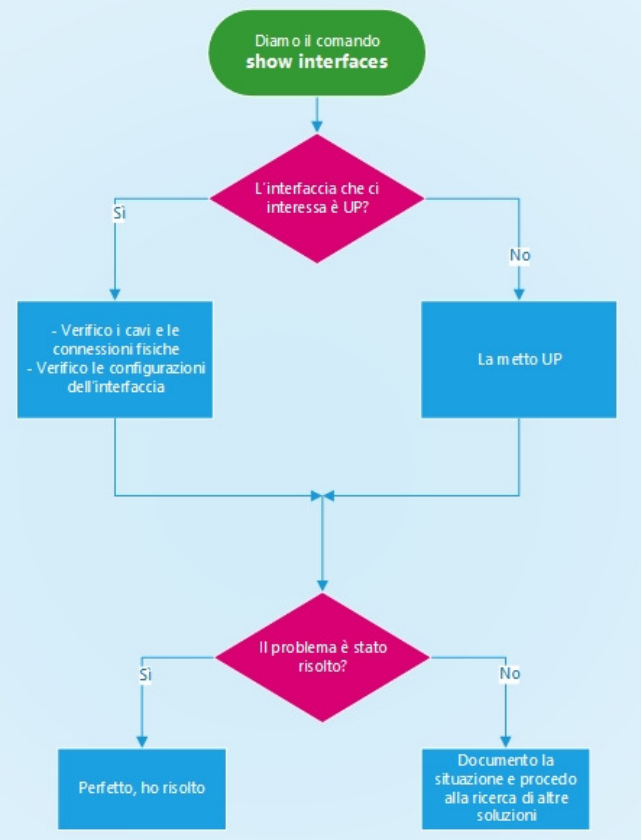
```
mdix auto
```

Per verificare l'auto mdix per una specifica interfaccia

```
show controllers ethernet-controller fa 0/1 phy
```

Per vedere la mac table

```
show mac-address-table
```



Per configurare l'accesso allo switch in ssh:

```
ip domain-name mydomain.local
crypto key generate rsa
1024
username mio_username secret mia_password
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
exit
```

5.2.1.4 Packet Tracer - Configuring SSH Instruction.pdf
5.2.1.4 Packet Tracer - Configuring SSH.pka

Durante la configurazione di uno switch dobbiamo ricordarci che lo switch in quanto tale funziona anche senza configurazione, per cui per una best practice di sicurezza è bene "spegnere" le porte che non vengono utilizzate.
Se vogliamo modificare un parametro su più porte, ci basta indicare il range delle porte che vogliamo prendere in considerazione
interface range fa0/0-10
Altre impostazioni per implementare la sicurezza del sistema switch è il secure MAC address types, in cui configuro il numero dei MAC address validi consentiti su una determinata porta. Ossia i MAC address legittimi sono autorizzati ad accedere alla morta, mentre gli altri no.
Se tale valore è configurato a 1 solamente il dispositivo con il MAC address indicato potrà accedere a quella porta.
Se su una porta configurata in un determinato modo si tenta di accedere con un dispositivo con MAC address non consentito, si genererà una violazione.
Tipi di MAC secure:

- Static secure MAC address: è un elenco di MAC address consentiti su una porta, questa è una configurazione statica
  switchport port-security mac-address 0A:BE:04:6D:53:FF
  Tali MAC address sono memorizzati nell'address table
- Dynamic secure MAC address: vengono appresi dinamicamente e scritti nell'address table, ma al riavvio dello switch saranno azzerati. È soggetta a timeout
- Sticky secure MAC address: è un mix dei precedenti. Per abilitare lo sticky secure basta dare il comando:
  switchport port-security mac-address sticky
  Per aggiungere staticamente un indirizzo MAC
  switchport port-security mac-address sticky 0A:BE:04:6D:53:FF
  La tabella è aggiornata dinamicamente, e non è soggetta a timeout perché è in running-config. E quando riavvio lo switch se non salvo la running in startup la perdo.

Per definire il numero di MAC address consentiti su un'interfaccia
switchport port-security maximum 10
Nel caso in cui vi sia una violazione sulla mia configurazione di MAC security potrò agire in uno dei seguenti modi:

- Protect: quando il numero di indirizzi MAC sicuri raggiunge il limite consentito sulla porta, i pacchetti con indirizzi di origine sconosciuti vengono eliminati fino a quando viene rimosso un numero sufficiente di indirizzi MAC sicuri o viene aumentato il numero di indirizzi consentiti massimi. Non vi è alcuna notifica che si sia verificata una violazione della sicurezza.
- Restrict: quando il numero di indirizzi MAC sicuri raggiunge il limite consentito sulla porta, i pacchetti con indirizzi di origine sconosciuti vengono eliminati fino a quando non viene rimosso un numero sufficiente di indirizzi MAC sicuri o viene aumentato il numero di indirizzi consentiti massimi. In questa modalità, c'è una notifica che si è verificata una violazione della sicurezza.
- Shutdown: in questa modalità (che è quella predefinita), una violazione della sicurezza della porta fa sì che l'interfaccia diventi immediatamente disabilitata per errore e spenga il LED della porta. Aumenta il contatore delle violazioni. Quando una porta protetta si trova nello stato disabilitato per errore, può essere riattivata con il comando **no shutdown**.

ATTENZIONE: il port-security non sarà abilitato sull'interfaccia fino a quando non darò il semplice comando (senza parametri):
switchport port-security

Per cambiare il tipo di violazione che si vuole applicare, il comando da dare all'interno della configurazione dell'interfaccia è:
switchport port-security protect
switchport port-security restrict
switchport port-security shutdown

Riassumendo abbiamo quello descritto in tabella:

Security Violation Modes

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Di default uno switch spacchettato e messo in produzione avrà:
Port security → disattivato su tutte le porte
Numero massimo di MAC address consentiti su ogni porta → 1
Violation mode → shutdown
Sticky address learning → disattivato

Per verificare le Port Security di un'interfaccia:
show port-security interface fa0/10
Per verificare tutti gli indirizzi della Port Security
show port-security address
Quando andiamo a verificare la configurazione di un'interfaccia tramite il comando
show interface fa0/18 status
l'output che compare in colonna sotto status ci indica se la porta è up, down oppure in err-disabled, ossia se è in down per una violation di cui sopra.

5.2.2.7 Packet Tracer - Configuring Switch Port Security Instructions.pdf
5.2.2.7 Packet Tracer - Configuring Switch Port Security.pka
5.2.2.8 Packet Tracer - Troubleshooting Switch Port Security Instructions.pdf
5.2.2.8 Packet Tracer - Troubleshooting Switch Port Security.pka
5.2.2.9 Lab - Configuring Switch Security Features.pdf
5.3.1.1 Switch Trio Instructions.pdf
5.3.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
5.3.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 5

6.0.1.2 Vacation Station Instructions.pdf

Le VLAN forniscono segmentazione e flessibilità della rete, e consentono di raggruppare dispositivi all'interno di gruppo (VLAN). Le VLAN sono connessioni logiche e non fisiche.
Ogni dispositivo all'interno della propria VLAN agiscono come se si trovassero all'interno di una lan indipendente. Qualsiasi porta di uno switch può appartenere ad una qualsiasi VLAN. Tutti i pacchetti unicast, multicast e broadcast vendono inoltrati solo alla VLAN nella quale sono stati generati. I pacchetti destinati a dispositivi che non appartengono alla VLAN devono essere inoltrati attraverso un apposito dispositivo che supporti il routing.
Più subnet possono esistere su un'unica LAN senza l'utilizzo di VLAN, tuttavia, i dispositivi si troveranno nello stesso dominio di trasmissione Layer 2. Ciò significa che tutte le trasmissioni di L2, come una richiesta ARP, saranno ricevute da tutti i dispositivi sulla LAN.
Le VLAN migliorano le prestazioni di rete dividendo i broadcast domain.

I principali vantaggi nell'utilizzo delle VLAN sono i seguenti:

- Security: dividendo la rete in gruppi, ho che i dati sensibili di ogni gruppo sono isolati dagli altri gruppi
- Cost reduction: i risparmi sui costi derivano dalla riduzione della necessità di costosi aggiornamenti della rete e di un uso più efficiente del bandwidth
- Better performance: la suddivisione di reti piane di livello 2 in più gruppi di lavoro logici (broadcast domain) riduce il traffico non necessario sulla rete e aumenta le prestazioni
- Reduce size of BD: dividere un unico grande broadcast domain in altri più piccoli ne riduce appunto le dimensioni
- Efficiency of IT staff: le VLAN semplificano la gestione della rete perché gli utenti con requisiti di rete simili condividono la stessa VLAN. Quando viene eseguito il provisioning di un nuovo switch, tutte le politiche e le procedure già configurate per la particolare VLAN vengono implementate quando vengono assegnate le porte. È anche facile per il personale IT identificare la funzione di una VLAN dandogli un nome appropriato
- Simply project & management: le VLAN aggregano utenti e dispositivi di rete per supportare esigenze aziendali o geografiche. Avere funzioni separate rende più semplice la gestione di un progetto o il lavoro con un'applicazione specializzata

Nella maggior parte dei casi le VLAN vengono utilizzare per separare il flusso dei dati, ad esempio una VLAN per il VoIP ed uno per lo scambio dei dati.
Alcune informazioni riguardanti le VLAN per quanto riguarda gli switch sono:

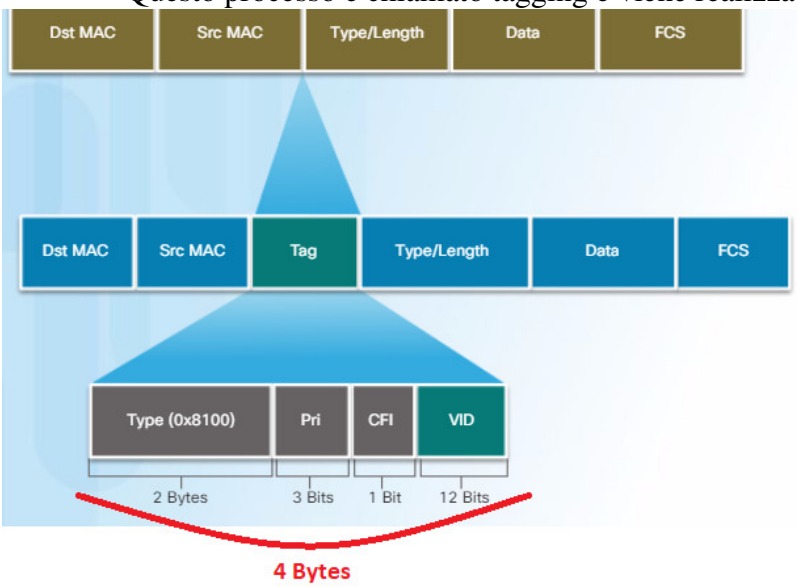
- La VLAN di default è la VLAN1
- A tutte le porte dello switch di default è assegnata la VLAN1
- La VLAN1 non può essere eliminata
- Il management della VLAN (ossia un ip assegnato alla switch virtual interface (SVI) di gestione dello switch) di default è assegnato alla VLAN1
  NB: l'interfaccia d imanagement non andrà up fino a quando non andrà up una porta ad essa associata, ossia fino a quando non collegherò un cavo ad una delle interfacce abilitare al management
- Le VLAN native sono le VLAN non taggate all'interno del dei trunk

Separare il VoIP in un'apposita VLAN è fondamentale poiché il VoIP richiede:

- Larghezza di banda garantita per garantire la qualità della voce
- Priorità di trasmissione rispetto ad altri tipi di traffico di rete
- Possibilità di essere instradati nelle aree congestionate della rete
- Ritardo inferiore a 150 ms attraverso la rete

6.1.1.5 Packet Tracer - Who Hears the Broadcast Instructions.pdf
6.1.1.5 Packet Tracer - Who Hears the Broadcast.pka
Un trunk è un collegamento point-to-point tra due dispositivi di rete che trasportano più di una VLAN. Un trunk VLAN estende le VLAN su un'intera rete. Cisco supporta IEEE 802.1Q per il coordinamento di trunk su interfacce Fast Ethernet, Gigabit Ethernet e 10 Gigabit Ethernet.
Le VLAN non sarebbero molto utili senza i trunk VLAN. I trunk VLAN consentono a tutto il traffico VLAN di propagarsi tra gli switch, in modo che i dispositivi che si trovano nella stessa VLAN, ma connessi a diversi switch, possano comunicare senza l'intervento di un router.
Un trunk VLAN non appartiene a una VLAN specifica.

Vediamo ora come funziona il TAG del frame Ethernet per l'identificazione delle VLAN
Gli switch sono dispositivi di livello 2. Usano le informazioni di intestazione del frame Ethernet per inoltrare i pacchetti. Non hanno tabelle di routing. L'intestazione del frame Ethernet standard non contiene informazioni sulla VLAN a cui appartiene il frame, quindi, quando i frame Ethernet sono posizionati su un trunk, è necessario aggiungere le informazioni sulle VLAN a cui appartengono. Questo processo è chiamato tagging e viene realizzato utilizzando l'intestazione IEEE 802.1Q.



L'intestazione 802.1Q include un tag a 4 Byte inserito nell'intestazione del frame Ethernet originale, che specifica la VLAN a cui appartiene il frame.

Quando lo switch riceve un frame su una porta configurata in modalità **access** e viene assegnata una VLAN, lo switch inserisce una tag VLAN nell'intestazione del frame, ricalcola il Frame Check Sequence (FCS) e invia il frame con TAG fuori da una porta trunk.

Il campo del tag VLAN è composto da:

- ✓ Type: un valore a 2 Byte chiamato valore ID protocollo tag (TPID). Per Ethernet, è impostato su 0x8100 esadecimale
- ✓ User priority: un valore a 3 bit che supporta l'implementazione di livelli o servizi (3bit = 7 valori disponibili)
- ✓ Canonical Format Identifier (CFI): è un identificativo a 1 bit che consente il trasporto di frame Token Ring su collegamenti Ethernet
- ✓ ID VLAN (VID): numero di identificazione VLAN a 12 bit che supporta fino a 4096 ID VLAN

Al termine lo switch inserisce il type e e il tag control information, ricalcola l'FCS, aggiunge l'FCS al frame e inoltra.

6.1.2.7 Packet Tracer - Investigating a VLAN Implementation Instructions.pdf
6.1.2.7 Packet Tracer - Investigating a VLAN Implementation.pka

CISCO identifica le VLAN da 1 a 1002 come VLAN normal range, mentre quelle dal 1006 al 4096 come VLAN extended range. Per quanto riguarda le VLAN 1002, 1003, 1004, 1005 queste sono riservate. Le VLAN configurate sono salvate all'interno del file vlan.dat all'interno della flash memory dello switch.

Per configurare una VLAN
vlan 99
name VLAN99
Per visualizzare le impostazioni delle VLAN (a quali interfacce sono abbinate, quali sono, ecc)
show vlan brief
Come assegnare una porta ad una VLAN:
interface fa0/11
switchport mode access → non necessario, ma è una best practice per la sicurezza
switchport access vlan 10
end
Per abilitare il QoS del traffico VoIP su un'interfaccia dare il comando seguente (a seconda dei casi) all'interno della configurazione dell'interfaccia:
mls qos trust cos → il più usato
oppure
mls qos trust device cisco-phone
oppure
mls qos trust dscp
oppure
mls qos trust ip-precedence
Rimuovere tutte le VLAN assegnate ad una porta:
no switchport access vlan
Rimuovere una determinata VLAN da una porta
no switchport access vlan 20
Le VLAN possono anche essere cancellate (ad eccezione dalla VLAN 1 ossia quella di default)
Prima di eliminarla verificare sempre con il comando
show vlan brief
se è rimasta assegnata a qualche porta, poi quando si è certi di poterla eliminare, dare il comando
no vlan 10
Per eliminare tutte le VLAN create (ad eccezione dalla VLAN 1 ossia quella di default) si potrebbe dare il comando sotto
delete flash:vlan.dat → abbreviabile in: **delete vlan.dat**
NB: anche dopo il comando **erase startup-config** se non si elimina il file sopra le vlan non sono state eliminate
Quando si gestiscono le VLAN, queste hanno 2 modalità di utilizzo

- Access: se alla porta è assegnata una sola VLAN, significa che questa interfaccia è utilizzata direttamente per interfacciare i dispositivi e vi è solo una VLAN untagged
- Trunk: se alla porta sono assegnate più VLAN, significa che l'interfaccia viene utilizzata per spostare dati e vi sono più vlan. È utilizzata tra apparati di rete

Piccola precisazione: la VLAN nativa si configura sui trunk e risulta essere quella non taggata.
Per assegnare una delle 2 modalità alla porta, da configuration terminal
interface g0/0
switchport mode access
switchport access vlan 10
exit
oppure
interface g0/0
switchport mode trunk
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30
exit

ATTENZIONE: nell'interfaccia trunk se dobbiamo aggiungere una VLAN in un secondo momento, ricordiamoci di dare il comando
switchport trunk allowed vlan add 33
ne non aggiungiamo il comando **add**, il comando toglie l'assegnazione alle altre vlan e imposta solo la VLAN 33.

Naturalmente per togliere le assegnazioni delle VLAN alle interfacce
no switchport trunk alloewd vlan 10
no switchport trunk native vlan 10

6.2.1.7 Packet Tracer - Configuring VLANs Instructions.pdf
6.2.1.7 Packet Tracer - Configuring VLANs.pka
6.2.2.4 Packet Tracer - Configuring Trunks Instructions.pdf
6.2.2.4 Packet Tracer - Configuring Trunks.pka
6.2.2.5 Lab - Configuring VLANs and Trunking.pdf

Vediamo ora alcuni comandi che possono tornare utili in fase di trubleshooting:
show vlan brief
show vlan id 10
show vlan name vlan1
show vlan summary
show interface vlan 1
show interface swithport
show interface trunk
show interface g0/0

Comandi utili nella console:
CTRL + a per andare all'inizio della riga
CTRL + e per andare alla fine della riga

Premettendo che i principali problemi che si incontrano sui trunk sono errori di configurazione, vediamo i principali che generalmente si incontrano:

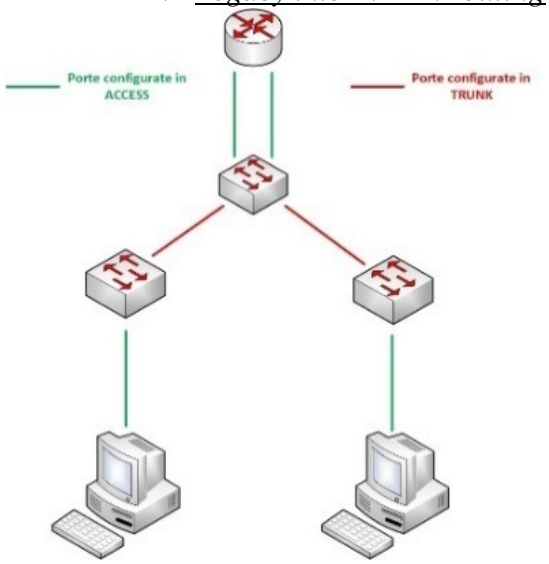
- ✓ Native VLAN mismatches: ossia le VLAN native di 2 apparati che si scambiano dati tramite porte configurate in trunk, hanno vlan nativa differente
- ✓ Trunk mode mismatches: ossia sulla porta di 2 apparati che dovrebbero scambiarsi dei dati in trunk, una è configurata in trunk e l'altra in access
- ✓ Allowed VLANs on trunks: ossia l'elenco delle vlan consentite sul truk non è stato aggiornato

6.2.3.7 Packet Tracer - Troubleshooting a VLAN Implementation - Scenario 1 Instructions.pdf
6.2.3.7 Packet Tracer - Troubleshooting a VLAN Implementation - Scenario 1.pka
6.2.3.8 Packet Tracer - Troubleshooting a VLAN Implementation - Scenario 2 Instructions.pdf
6.2.3.8 Packet Tracer - Troubleshooting a VLAN Implementation - Scenario 2.pka
6.2.3.9 Lab - Troubleshooting VLAN Configurations.pdf

Sugli switch di L2 per definizione di vlan (le vlan limitano i broadcast domain), le varie VLAN non possono parlare tra di loro se non attraverso apparati di L3.

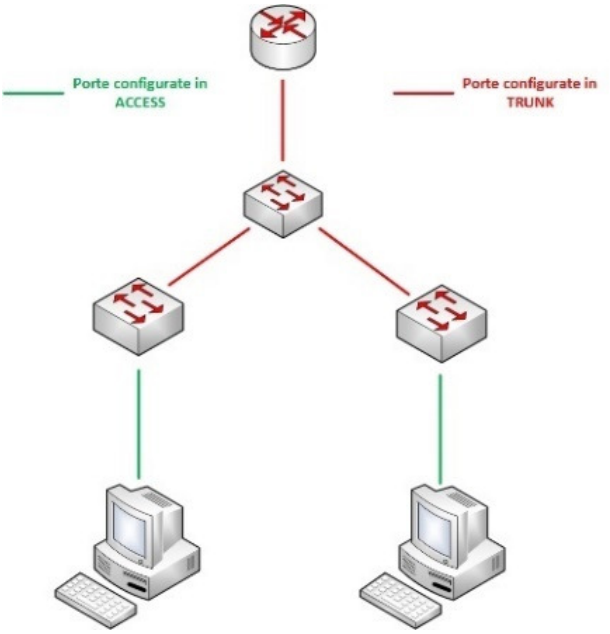
Per poter parlare tra di loro le VLAN (inter-VLAN routing), devono agire in uno dei seguenti 3 modi:

1. *Legacy inter-VLAN routing*



Dove abbiamo che gli switch si passano tra loro le informazioni e poi lo switch collegato al router, configurerà una porta in access collegata al router per ogni vlan che deve interagire con le altre

2. *Router-on-a-Stick*



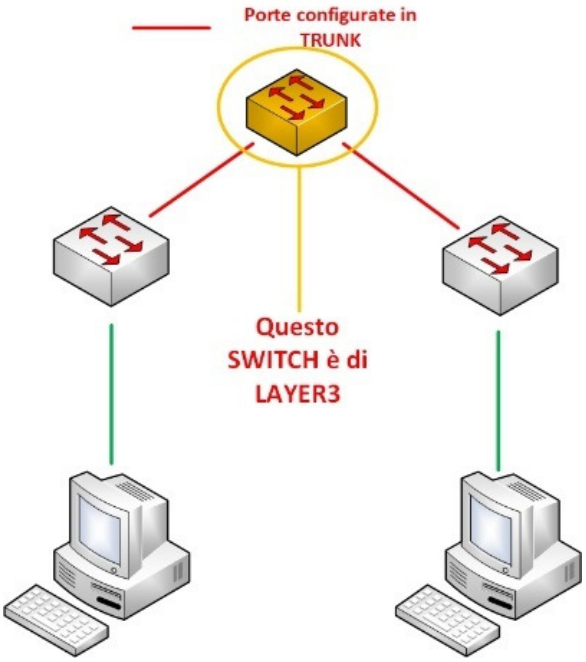
A differenza della modalità precedente, lo switch passa al router tutte le vlan che devono tra loro interagire, con un unico cavo, quindi la porta dello switch deve essere in trunk.
Il router però non ha il concetto di VLAN, per cui lato router dobbiamo introdurre il concetto di sub-interface e dirgli di utilizzare il protocollo 802.1Q
Le sub-interface sono interfacce virtuali basate su un'unica interfaccia fisica.
Ogni sub interface è configurata in modo indipendente con un indirizzo IP ed una vlan ad essa associata.
Il router-on-a-stick è limitato a 50 VLAN

Comandi base:

```
interface g0/0
no shutdown
interface g0/0.10
encapsulation dot1q 10 native
ip address 192.168.1.62 255.255.255.192
no shutdown
exit
interface g0/0.20
encapsulation dot1q 20
ip address 192.168.1.94 255.255.255.224
no shutdown
exit
interface g0/0.30
encapsulation dot1q 30
ip address 192.168.1.110 255.255.255.240
no shutdown
exit
```

← questo è importantissimo poiché è quello che mi mette up l'interfaccia

3. *Layer3 switching using SVIs* (trattazione non svolta in questo corso, giusto un accenno)

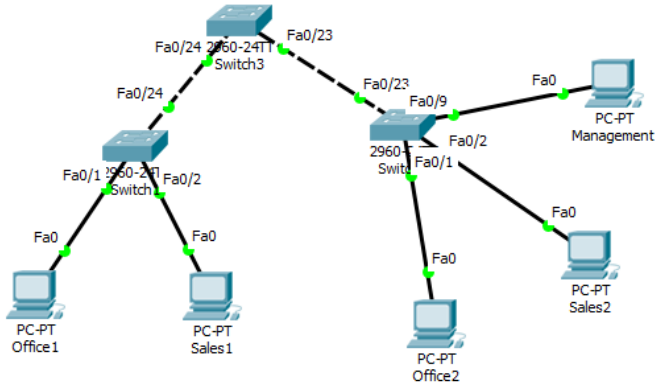


Viene sostituito lo switch centrale con uno switch di Layer3, ed al suo interno dando il comando
Ip unicast routing
Abilitò la possibilità di poter assegnare un IP ad ogni VLAN
NB: tale abilitazione mi consente anche di avere il managing su più vlan, per cui è bene ricordarsi anche il lato sicurezza

6.3.2.4 Lab - Configuring Per-Interface Inter-VLAN Routing.pdf
6.3.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing Instructions.pdf
6.3.3.6 Packet Tracer - Configuring Router-on-a-Stick Inter-VLAN Routing.pka
6.3.3.7 Lab - Configuring 802.1Q Trunk-Based Inter-VLAN Routing.pdf
6.3.3.8 Packet Tracer - Inter-VLAN Routing Challenge Instructions.pdf
6.3.3.8 Packet Tracer - Inter-VLAN Routing Challenge.pka
6.4.1.1 The Inside Track Instructions.pdf
6.4.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
6.4.1.2 Packet Tracer - Skills Integration Challenge.pka

Scenario dell'esercizio e svolgimento

STEP1: Dobbiamo realizzare una rete (subnetting della classful 192.168.1.0/24) divisa nel seguente modo:
VLAN 10 – 50 host – Rete Office
VLAN 20 – 24 host – Rete Sales
VLAN 30 – 10 host – Management
Gli switch dovranno far parte della VLAN di Management
Default Gateway per ogni VLAN è l'ultimo ip disponibile della subnet
L'assegnazione degli IP ai pc parte dal primo IP disponibile della subnet



VLAN10 – 50 host → /26 che ha 62 host a disposizione
NetIP: 192.168.1.0
BroadcastIP: 192.168.1.64
Netmask: 255.255.255.192
Range ip: 192.168.1.1 – 192.168.1.62
Gateway: 192.168.1.62
Office1: 192.168.1.1 Office2: 192.168.1.2

VLAN20 – 24 host → /27 che ha 30 host a disposizione
NetIP: 192.168.1.64
BroadcastIP: 192.168.1.95
Netmask: 255.255.255.224
Range ip: 192.168.1.65 – 192.168.1.94
Gateway: 192.168.1.94
Sales1: 192.168.1.65 Sales2: 192.168.1.66

VLAN30 – 10 host → /28 che ha 14host a disposizione
NetIP: 192.168.1.96
BroadcastIP: 192.168.1.111
Netmask: 255.255.255.240
Range ip: 192.168.1.97 – 192.168.1.110
Gateway: 192.168.1.110
Management: 192.168.1.97 Switch1: 192.168.1.98
Switch2: 192.168.1.99 Switch3: 192.168.1.100

A partire dalla configuration terminal:

SWITCH 1

```
vlan 10
name Office
no shutdown
exit
vlan 20
name Sales
no shutdown
exit
vlan 30
name Management
no shutdown
exit
interface fa0/24
switchport mode trunk
switchport trunk allowed vlan 10,20,30
no shutdown
exit
interface vlan30
ip address 192.168.1.98 255.255.255.240
no shutdown
exit
interface fa0/1
switchport mode access
switch access vlan 10
no shutdown
exit
interface fa0/2
switchport mode access
switch access vlan 20
no shutdown
exit
exit
copy running-config startup-config
```

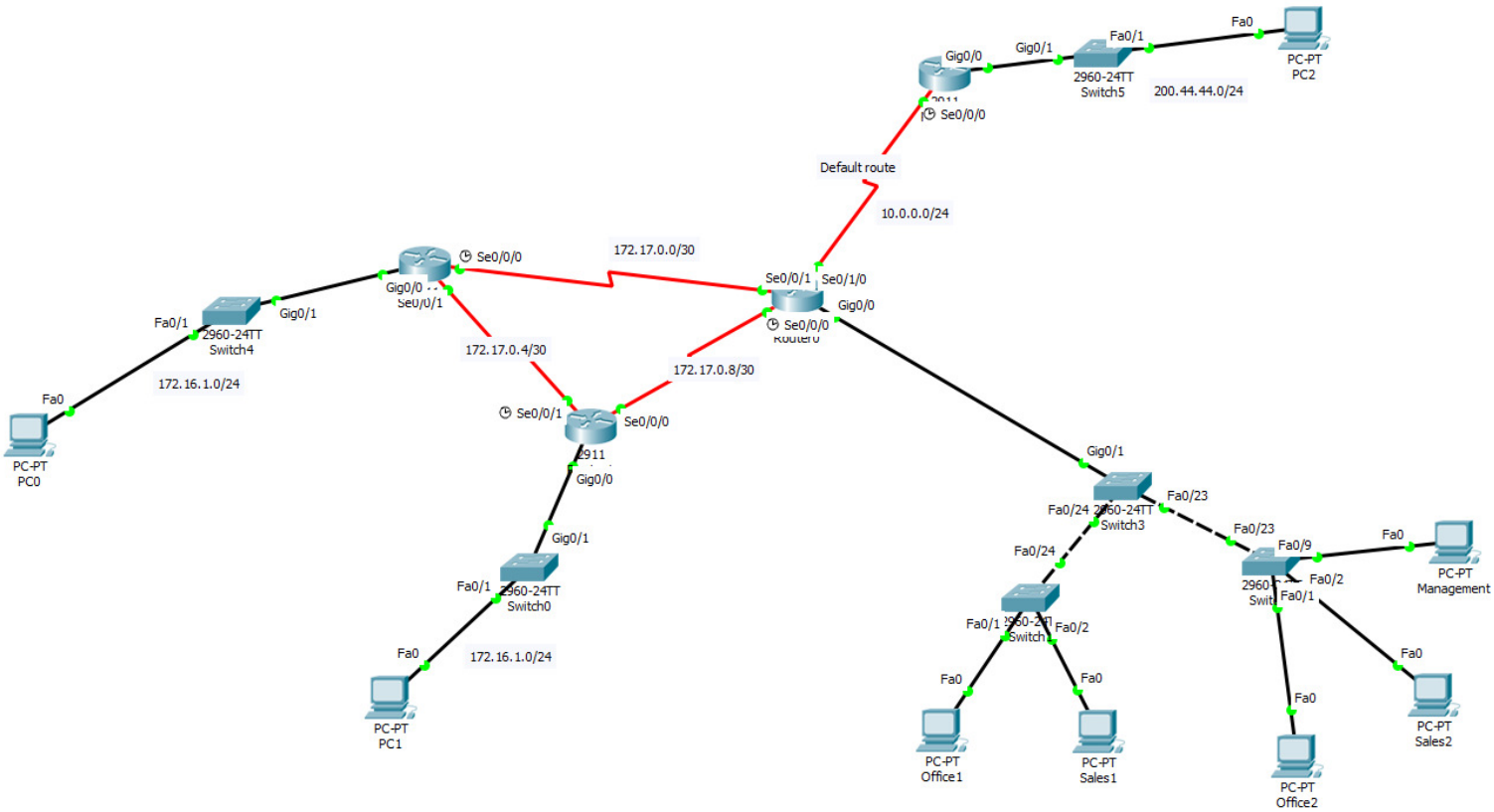
SWITCH 2

```
vlan 10
name Office
no shutdown
exit
vlan 20
name Sales
no shutdown
exit
vlan 30
name Management
no shutdown
exit
interface fa0/23
switchport mode trunk
switchport trunk allowed vlan 10,20,30
no shutdown
exit
interface vlan30
ip address 192.168.1.99 255.255.255.240
no shutdown
exit
interface fa0/1
switchport mode access
switch access vlan 10
no shutdown
exit
interface fa0/2
switchport mode access
switch access vlan 20
no shutdown
exit
interface fa0/9
switchport mode access
switch access vlan 30
no shutdown
exit
exit
copy running-config startup-config
```

SWITCH 3

```
vlan 10
name Office
no shutdown
exit
vlan 20
name Sales
no shutdown
exit
vlan 30
name Management
no shutdown
exit
interface fa0/23
switchport mode trunk
switchport trunk allowed vlan 10,20,30
no shutdown
exit
interface fa0/24
switchport mode trunk
switchport trunk allowed 10,20,30
no shutdown
exit
interface vlan30
ip address 192.168.1.100 255.255.255.240
no shutdown
exit
exit
copy running-config startup-config
```

STEP2: implementiamo ora la rete affinché vi sia un router che funga da gateway per le varie VLAN considerando però che solo il pc di management possa amministrare gli switch. Inoltre creiamo una rete di router con altre loro sotto-reti (no VLAN), che si scambino informazioni tramite il RIPv2. Configuriamo anche una default route, il tutto come figura sotto



La possibilità di gestire il management solo dall'apposito PC è garantita dal fatto che sugli switch non è stato impostato l'IP del gateway tramite il comando

ip default gateway 192.168.1.110

Da aggiungere nello ***SWITCH3***

```
interface g0/1
switchport mode trunk
switchport trunk allowed vlan 10,20,30
no shutdown
exit
```

Router0

```
hostname R0
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.1.62 255.255.255.192
no shutdown
exit
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.1.94 255.255.255.224
no shutdown
exit
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.1.110 255.255.255.240
no shutdown
exit
interface g0/0
no shutdown
exit
interface Serial0/0/0
ip address 172.17.0.9 255.255.255.252
clock rate 2000000
no shutdown
exit
interface Serial0/0/1
ip address 172.17.0.2 255.255.255.252
no shutdown
exit
interface Serial0/1/0
ip address 10.0.0.2 255.255.255.0
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
router rip
version 2
no auto-summary
passive-interface g0/0
default-information originate
network 192.168.1.0
network 172.17.0.0
exit
```

Router1

```
hostname R1
interface GigabitEthernet0/0
ip address 172.16.1.254 255.255.255.0
no shutdown
exit
interface Serial0/0/0
ip address 172.17.0.10 255.255.255.252
no shutdown
exit
interface Serial0/0/1
ip address 172.17.0.5 255.255.255.252
clock rate 2000000
no shutdown
exit
router rip
version 2
no auto-summary
passive-interface g0/1
network 172.16.1.0
network 172.17.0.0
exit
```

Router2

```
hostname R2
interface GigabitEthernet0/0
ip address 172.16.2.254 255.255.255.0
no shutdown
exit
interface Serial0/0/0
ip address 172.17.0.1 255.255.255.252
clock rate 2000000
no shutdown
exit
interface Serial0/0/1
ip address 172.17.0.6 255.255.255.252
no shutdown
exit
router rip
version 2
no auto-summary
passive-interface g0/0
network 172.16.2.0
network 172.17.0.0
exit
```

Router3

```
hostname R3
interface Serial0/0/0
ip address 10.0.0.1 255.255.255.0
clock rate 2000000
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
interface g0/0
ip address 200.44.44.254 255.255.255.0
exit
```

Così come scritto sopra, abbiamo la "pingabilità" totale di tutti i PC tra loro

NB: per velocizzare la configurazione sono state omesse le configurazioni base standard, ossia attivazione telnet, ed impostazione password (con cifratura)

Router o Switch

```
hostname nome_device
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R1 - Accesso consentito solo al personale autorizzato#
ip domain-name mydomain.local
crypto key generate rsa
1024
username mio_username secret mia_password
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
exit
```

FINE CAPITOLO 6

7.0.1.2 Permit Me to Assist You Instructions.pdf

Le ACL (Access Control List) servono per filtrare il traffico, più precisamente è quello strumento che serve per identificare il traffico sui parametri di Layer3 e di Layer4.
Attenzione a non creare confusione, l'ACL è un insieme di regole ACE comunemente definite istruzioni ACL, quindi non da una sola regola
Le ACL agiscono in ingresso o in uscita su una determinata interfaccia per varie ragioni, come limitare il traffico, fornire un livello di sicurezza a basso livello, fornire controllo sul flusso di traffico.
L'IPv4 d'origine è il criterio standard impostato nelle ACL. Un router configurato con un ACL IPv4 standard estrae l'indirizzo IPv4 di origine dall'intestazione del pacchetto. Il router inizia nella parte superiore dell'ACL e confronta l'indirizzo in ogni ACE in modo sequenziale. Quando viene effettuata una corrispondenza, il router esegue l'istruzione, consentendo o negando il pacchetto. Dopo aver effettuato una corrispondenza, gli ACE rimanenti nell'ACL, se presenti, non vengono analizzati. Se l'indirizzo IPv4 di origine non corrisponde a nessun ACE nell'ACL, il pacchetto viene "droppato".
L'ultima affermazione di un'ACL è sempre un rifiuto implicito. Questa istruzione viene inserita automaticamente alla fine di ogni ACL anche se non è presente fisicamente. L'istruzione implicita nega/blocca tutto il traffico. A causa di questo rifiuto implicito, un ACL che non ha almeno un'istruzione di autorizzazione bloccherà tutto il traffico (riassumendo: tutto ciò che non è espressamente dichiarato, viene negato)

7.1.1.4 Packet Tracer - ACL Demonstration Instructions.pdf
7.1.1.4 Packet Tracer - ACL Demonstration.pka

Introduciamo alcuni concetti che ci serviranno poi per elencare le "regole d'oro delle ACL"

Wild Card Mask: mi dice quali sono i bit da considerare nel momento in cui vado a fare un match, sembra il contrario della netmask, ma è un concetto slegato dalla rete, cioè è un filtro logico. Cioè devo tenere fermi tutti i bit a 0
Net Mask e Wild Card Mask devono sempre essere associate ad un indirizzo IPv4 di riferimento
Partiamo indicando una differenza fondamentale, ossia la netmask in ognuno dei suoi 4 blocchi da 8 bit può assumere solo i valori: 0 – 128 – 192 – 224 – 240 – 248 – 252 – 254 – 255, le wild card mask invece possono assumere tutti i valori compresi nel range 0-255, quindi in alcuni casi **POSSONO** coincidere con la netmask, ma in molti altri no.

Esempi IPv4 di riferimento 192.168.1.0

Con Net Mask: 255.255.255.128	→ rete da 192.168.1.0 a 192.168.1.127	oppure
	→ rete da 192.168.1.128 a 192.168.1.255	
Con Wild Card Mask: 0.0.0.127	→ rete da 192.168.1.0 a 192.168.1.127	oppure
	→ rete da 192.168.1.128 a 192.168.1.255	

Avendo IPv4 di riferimento 192.168.1.19 posso variare la Net Mask (subnetting) e diminuendo il range di ip a mia disposizione, secondo i valori sopra elencati, mentre posso ridurre il range degli ip a mia disposizione anche con la Wild Card Mask, ma posso inibire gli ip anche a salti

Con Net Mask 255.255.255.192	→ rete da 192.168.1.0 a 192.168.1.63
Con Wild Card 0.0.0.92	→ rete da 192.168.1.0 a 192.168.1.255 Ma i valori che mi saranno consentiti saranno tutti quelli con i bit a uno nella Wild Card Mask, mentre i bit a 0 non potranno essere variati (in questo caso il bit che non possono essere variati saranno identificati dai valori 128, 32, 2 e 1)

Valore ultimo Byte in binario								Valore in decimale	NOTE
0	0	0	1	0	0	1	1	19	IPv4 di riferimento
0	1	0	1	1	1	0	0	92	Wild Card Mask
0		0				1	1		Tengo fissi tutti i valori dell'IPv4 di riferimento dove ho degli zeri nella wild card mask
0	0	0	0	0	0	1	1	3	Calcolo tutti i valori consentiti, variando i bit che possono cambiare (ossia quelli a 1 della wild card mask)
0	0	0	0	0	1	1	1	7	
0	0	0	0	1	0	1	1	11	
0	0	0	0	1	1	1	1	15	
0	0	0	1	0	0	1	1	19	
0	0	0	1	0	1	1	1	23	
0	0	0	1	1	0	1	1	27	
0	0	0	1	1	1	1	1	31	
0	1	0	0	0	0	1	1	67	
0	1	0	0	0	1	1	1	71	
0	1	0	0	1	0	1	1	75	
0	1	0	0	1	1	1	1	79	
0	1	0	1	0	0	1	1	83	
0	1	0	1	0	1	1	1	87	
0	1	0	1	1	0	1	1	91	
0	1	0	1	1	1	1	1	95	

Quindi tutti i valori consentiti da questa Wild Card Mask in base all'ip di riferimento 192.168.1.19 saranno:
3, 7, 11, 15, 19, 23, 27, 31, 67, 71, 75, 79, 83, 87, 91, 95
Questa annotazione può essere molto utile in varie situazione, come ad esempio
Wild Card Mask: 0.0.0.254 → se abbinata all'IPv4 192.168.1.0 esclusione di tutti gli ip dispari
→ se abbinata all'IPv4 192.168.1.1 esclusione di tutti gli ip pari
Comunque nella maggior parte dei casi, le Wild Card Mask risultano essere il completamento delle Net Mask.

Per creare un'ACL che permetta il traffico di qualsiasi IPv4, dalla "Configuration Terminal"
access-list 1 permit 0.0.0.0 255.255.255.255
oppure
access-list 1 permit any
Per cerare un'ACL che permetta il traffico d'un determinato IPv4 specifico
access-list 1 permit 192.168.1.33 0.0.0.0
oppure
access-list 1 permit host 192.168.1.33
Esistono 2 tipi di ACL

- Standard (valori da 1 a 99 e da 1300 a 1999): il match è sul source IP address (ossia controllo l'IP in ingresso)
- Extended (valori da 100 a 199 e da 2000 a 2699): il match deve essere basato più su dati: protocol (L3 o L4), source ip (L3), source port (L4), destination ip (L3), destination port (L4)

I 2 tipi di ACL (Standard ed Extended) possono essere configurate in 2 modi:

- Numbered
- Named

Nel Modulo2 vedremo come configurare solo le ACL Standard
ACL (esempio)
access-list number (deny|permit|remark) ip wild_card (remark serve per descrivere un'ACL)
access-list 1 remark Permetti tutti gli ip pari --> es. descrive cosa fa l'ACL
access-list 1 permit 192.168.1.0 0.0.0.254 --> es. tutti gli ip pari
Le ACL create vanno poi assegnate in ingresso o in uscita alle varie interfacce (esempio)
Numbered
access-list 1 permit 192.168.1.0 0.0.0.254
interface Serial0/0/0
ip access-group 1 out
Per eliminare un'ACL da un'interfaccia, da dentro la config terminal dell'intrfaccia
no access-group 1
Dopo aver tolto le assegnazioni di una determinata ACL a tutte le porte a cui era assegnata, posso eliminare l'ACL
no access-list 10
Named
A differenza di quelle numbered, quelle Named, quando vengono create mi mettono all'interno della sua interfaccia di configurazione per cui prima di assegnarle ad un'interfaccia bisogna uscire
ip access-list (standard|extended) NOME
(deny|permit|remark) ip wild_card
exit
interface g0/0
ip access-group NOME out
7.2.1.6 Packet Tracer Configuring Numbered Standard IPv4 ACLs Instructions.pdf
7.2.1.6 Packet Tracer Configuring Numbered Standard IPv4 ACLs.pka
7.2.1.7 Packet Tracer - Configuring Named Standard IPv4 ACLs Instructions.pdf
7.2.1.7 Packet Tracer - Configuring Named Standard IPv4 ACLs.pka

Per vedere le priorità e l'ordine delle regole applicata ad un'ACL
show access-lists 10
show access-lists NOME
Per modificarla (numbered o named)
e o per aggiungercene o cancellarne una riga:
ip access-list standard 10
no 20
20 deny host 192.168.10.10
exit
oppure
ip access-list standard NOME
no 20
20 deny host 192.168.10.10
exit
Per verificare quali ACL sono presenti su una determinata porta:
show ip interface g0/0
Per vedere tutte la ACL configurate sull'apparato (mi dice anche quante volte si è verificato un determinato match)
show access-lists
Per azzerare il contatore di una determinata ACL:
clear access-list counter 10

7.2.2.6 Lab - Configuring and Modifying Standard IPv4 ACLs.pdf

Il comando **access-class** serve per limitare con ACL le connessioni telnet ed ssh (vty). Sempre a partire da config term

```
line vty 0 4
login local
transport input ssh
access-class 21 in
exit
access-list 21 permit 192.168.1.10 0.0.0.255
access-list 21 deny any
```

7.2.3.3 Packet Tracer - Configuring an IPv4 ACL on VTY Lines Instructions.pdf
7.2.3.3 Packet Tracer - Configuring an ACL on VTY Lines.pka
7.2.3.4 Lab - Configuring and Verifying VTY Restrictions.pdf
7.3.2.4 Packet Tracer - Troubleshooting Standard IPv4 ACLs Instructions.pdf
7.3.2.4 Packet Tracer - Troubleshooting Standard IPv4 ACLs.pka
7.4.1.1 FTP Denied Instructions.pdf
7.4.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
7.4.1.2 Packet Tracer - Skills Integration Challenge.pka
Da 7.3.1.4 a 7.3.2.3 → Trubleshooting

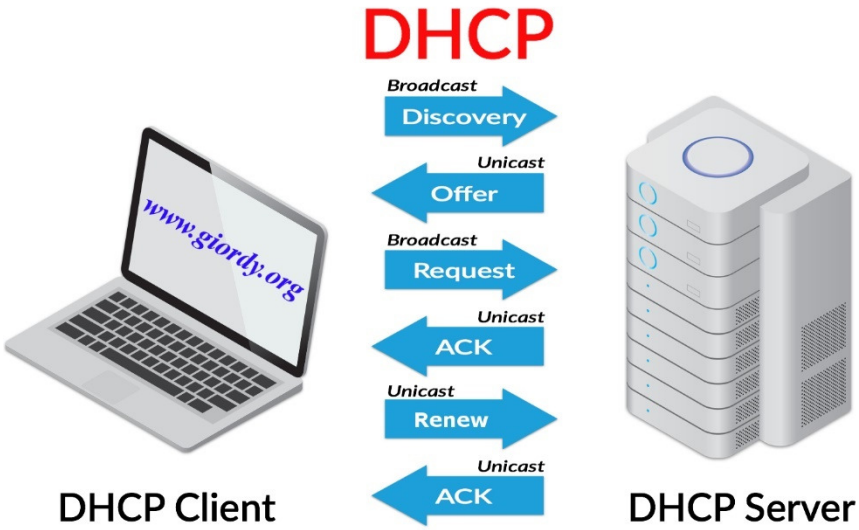
Le regole d'oro delle ACL

- Regola1: su ogni interfaccia non posso applicare più di una sola ACL per IPv4 per senso, ossia massimo un'ACL in ingresso e massimo un'ACL in uscita
- Regola2: first match. Un'ACL è una lista di regole, di cui è molto importante l'ordine, perché si ferma al primo match positivo che incontra (list of statement) → Orders Matter (l'ordine è importante) → More specific first (ossia le regole più specifiche o più importanti vanno messe all'inizio). Sintetizzando e traslando con un esempio fisico, possiamo pensare ad un setaccio
- Regola3: Best practice:
  - Quando facciamo le ACL facciamo riferimento a della documentazione e scriviamole
  - Prepariamo una descrizione e mettiamola nelle note
  - Metterla giù con un text editor prima per averne una copia
  - Testare l'ACL su una rete di test
- Regola4: dove vado ad inserire la mia ACL? In base al tipo di ACL avrò:
  - La standard và vicino alla destinazione
  - Extended mi permette di bloccare il traffico il prima possibile, quindi il più vicino possibile all'origine del traffico da filtrare
- Regola5: deny any è implicito, ossia per l'IPv4 tutto quello che non è dichiarato, è impostato come negato, ossia se non trova nessun match lui blocca (se non me lo dici io blocco)

FINE CAPITOLO 7

Un server DHCPv4 dedicato è scalabile e relativamente facile da gestire. Tuttavia, in una piccola filiale o in una posizione SOHO, è possibile configurare un router Cisco per fornire servizi DHCPv4 senza la necessità di un server dedicato. Il software Cisco IOS supporta un server DHCPv4 opzionale completo di funzionalità.

Il funzionamento del DHCPv4 è ben sintetizzato nella figura sottostante.



Le ultime 2 frecce indicano il re-new del lease.
Tale parametro viene impostato dall'amministratore della rete e server per riprendere possesso degli IPv4 non più utilizzati in rete dagli apparati

Il protocollo DHCP lavora su 2 porte assegnate, ossia la 67 per le richieste e la 68 per le risposte.

8	16	24	32
OP Code (1)	Hardware Type (1)	Hardware Address Length (1)	Hops (1)
Transaction Identifier			
Seconds - 2 bytes		Flags - 2 bytes	
Client IP Address (CIADDR) - 4 bytes			
Your IP Address (YIADDR) - 4 bytes			
Server IP Address (SIADDR) - 4 bytes			
Gateway IP Address (GIADDR) - 4 bytes			
Client Hardware Address (CHADDR) - 16 bytes			
Server Name (SNAME) - 64 bytes			
Boot Filename - 128 bytes			
DHCP Options - variable			

Per analizzare il formato del massaggio DHCPv4 di rimanda alla slide 8.1.1.3 (la figura/tabella accanto indica lo schema del formato)

DHCP Server:

1) Metto prima gli ip che non voglio assegnare
2) Stabilisco il pool d'IP che voglio rilasciare, che dev'essere assegnato ad una rete già configurata sul dispositivo
3) Nel Router, essendo che una rete può essere associata ad una sola porta, nel momento in cui la porta è attiva il DHCP si aggancia ad essa

Partiamo sempre dalla configuration terminal
Prima devo mettere gli l'elenco degli ip che voglio escludere (se metto 2 ip è un range che escludo, come in esempio sotto)

```
ip dhcp excluded-address 192.168.1.10 192.168.1.20
ip dhcp pool NOME_POOL
network 192.168.1.0 255.255.255.0
default-router 192.168.1.254
domain-name ESEMPIO.local
dns-server 8.8.8.8
exit
```

Verificare i parametri
show ip dhcp binding → **ipconfig /all** (in windows)

Il tempo di lease standard se non viene specificato nulla è di 24 ore, altrimenti ecco alcuni esempi
lease 2 ← lease di 2 giorni
lease 0 6 ← lease di 6 ore
lease 0 0 30 ← lease di 30 minuti
lease infinite ← lease senza scadenza

All'interno della rete per evitare di avere troppi servizi decentralizzati (quindi evitando di perdere risorse ed aumentare la complessità) è possibile impostare gli apparati affinché utilizzino servizi di altri apparati, come ad esempio configurare il DHCP Realy.
DHCP realy (entrando nella configure terminal di una determinata interfaccia)
interface g0/0
ip helper-address 192.168.11.6

NB: di default il comando sopra propaga anche le seguenti informazioni:
- ✓ Port 37: Time
- ✓ Port 49: TACACS
- ✓ Port 53: DNS
- ✓ Port 67: DHCP/BOOTP client
- ✓ Port 68: DHCP/BOOTP server
- ✓ Port 69: TFTP
- ✓ Port 137: NetBIOS name service
- ✓ Port 138: NetBIOS datagram service

8.1.2.4 Lab - Configuring Basic DHCPv4 on a Router.pdf
8.1.2.5 Lab - Configuring Basic DHCPv4 on a Switch.pdf

Per quanto riguarda invece gli apparati client, basta assegnare ad ogni interfaccia la modalità DHCP per l'assegnazione dell'IPv4
interface g0/1
ip address dhcp
no shutdown
exit

8.1.3.3 Packet Tracer - Configuring DHCPv4 Using Cisco IOS Instructions.pdf
8.1.3.3 Packet Tracer - Configuring DHCPv4 Using Cisco IOS.pka

Trubleshooting del DHCPv4
1) Risoluzione dei conflitti degli indirizzi IPv4: se viene rilevato un conflitto di indirizzi, l'indirizzo viene rimosso dal pool e non viene assegnato fino a quando un amministratore non risolve il conflitto
   show ip dhcp conflict
2) Verificare che l'interfaccia: se funziona ed che sia UP
   show interface g0/1
3) Verificare la connettività: provare a verificare le funzionalità con un indirizzo IPv4 statico, se non funziona allora il problema non è il DHCPv4
4) Attenzione alle VLAN sugli switch

Per effettuare debugging sui router nei quali sembra non funzionare il DHCPv4 server (ossia non riceve richieste DHCP), bisogna utilizzare le ACL estese (argomento ancora non trattato, ma di cui mettiamo un esempio sotto)

access-list 100 permit udp any any eq 67
access-list 100 permit udp any any eq 68
exit
debug ip packet 100
debug ip dhcp server events

8.1.4.4 Lab - Troubleshooting DHCPv4.pdf

Come visto nel Modulo precedente (Appunti Modulo1 pag. 30), gli IPv6 possono essere assegnati nei seguenti modi:

e) Static: l'IP lo inseriamo noi staticamente
f) SLAAC (stateless)
g) DHCPv6 (stateful)
h) SLAAC + DHCPv6 (stateless)

In questi 3 casi, appena collego un dispositivo alla rete, esso parla con il router che gli manda dei dati (RA), tra cui: Gateway, RangeNet di partenza, ecc…

NB: parliamo di indirizzi **GLOBAL UNICAST**

Vediamo più in dettaglio SLAAC: La parte di NET me la comunica il router tramite una comunicazione ICMPv6. Il dispositivo invia una comunicazione Multicast all'IPv6 FF02 :: 2 (comunicazione Router Solicitation RS). Il router quando riceve la comunicazione risponde con una comunicazione Router Advertisement (RA) in cui comunica all'dispositivo la parte di NET dell'IPv6 che il client dovrà configurarsi Global Unicast.
Mentre per quanto riguarda la parte di HOST vi sono 2 metodologie:

- RANDOM: dove i valori vengono compilati in maniera RANDOM appunto
- EUI64: viene creato attraverso l'utilizzo del MAC Address

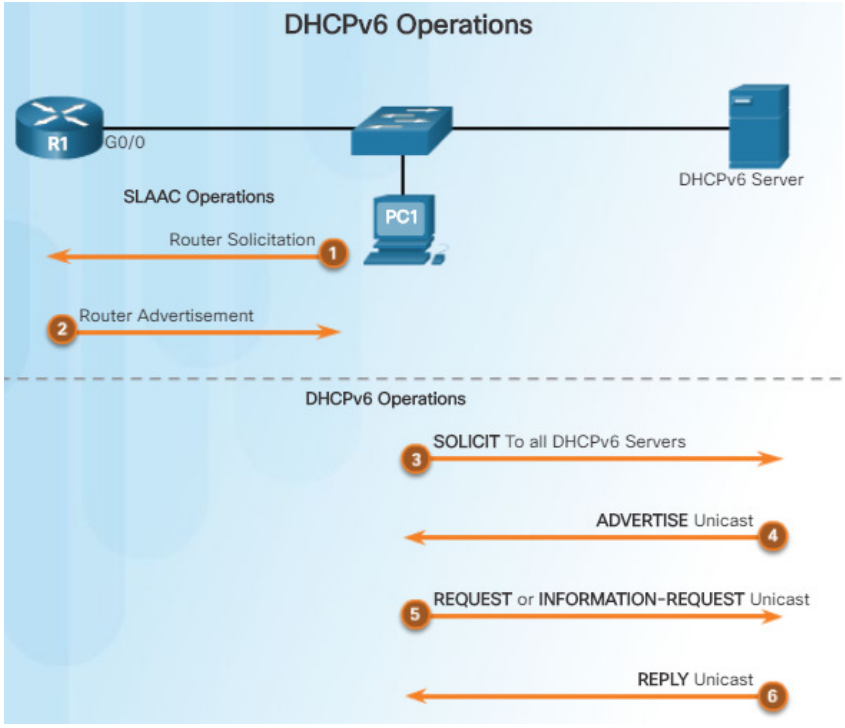
I router CISCO inviano periodicamente o per risposta, comunicazioni RA ogni 200 secondi.
I messaggi RA possono contenere anche altre informazioni, come Gateway, DNS, RangeNet, ecc…
I messaggi RA inviati ogni 200 secondi vengono inviati all'indirizzo Multicast FF02::1
Essendo appunto SLAAC stateless, non vi è nessun apparato che gestisca le informazioni sull'indirizzo di rete, ossia non vi è nessun apparato che sappia se in IPv6 è già stato utilizzato oppure no, per cui il dispositivo dopo essersi creato l'IPv6 manda una comunicazione ICMPv6 Neighbor Solicitation per verificare che l'IPv6 non sia duplicato. Questo processo è noto come DAD (Duplicate Address Detection)

NB: si consiglia sempre di utilizzare DAD per sicurezza anche in caso di IPv6 static o DHCPv6. DAD è implementato in ICMPv6 con specifiche RFC4443

Ricordiamoci che per poter utilizzare IPv6 sugli apparati CISCO, dobbiamo abilitarlo
ipv6 unicast-routing

La decisione su quale sistema utilizzare per la configurazione dell'IPv6 è racchiusa all'interno del messaggio RA e sono indicati dai sefuenti flag:
- Managed Address Configuration flag (M)
- Other Configuration flag (O)

È importante sapere che un client può anche decidere d'ignorare i messaggi RA ed utilizzare esclusivamente i servizi di un server DHCPv6.



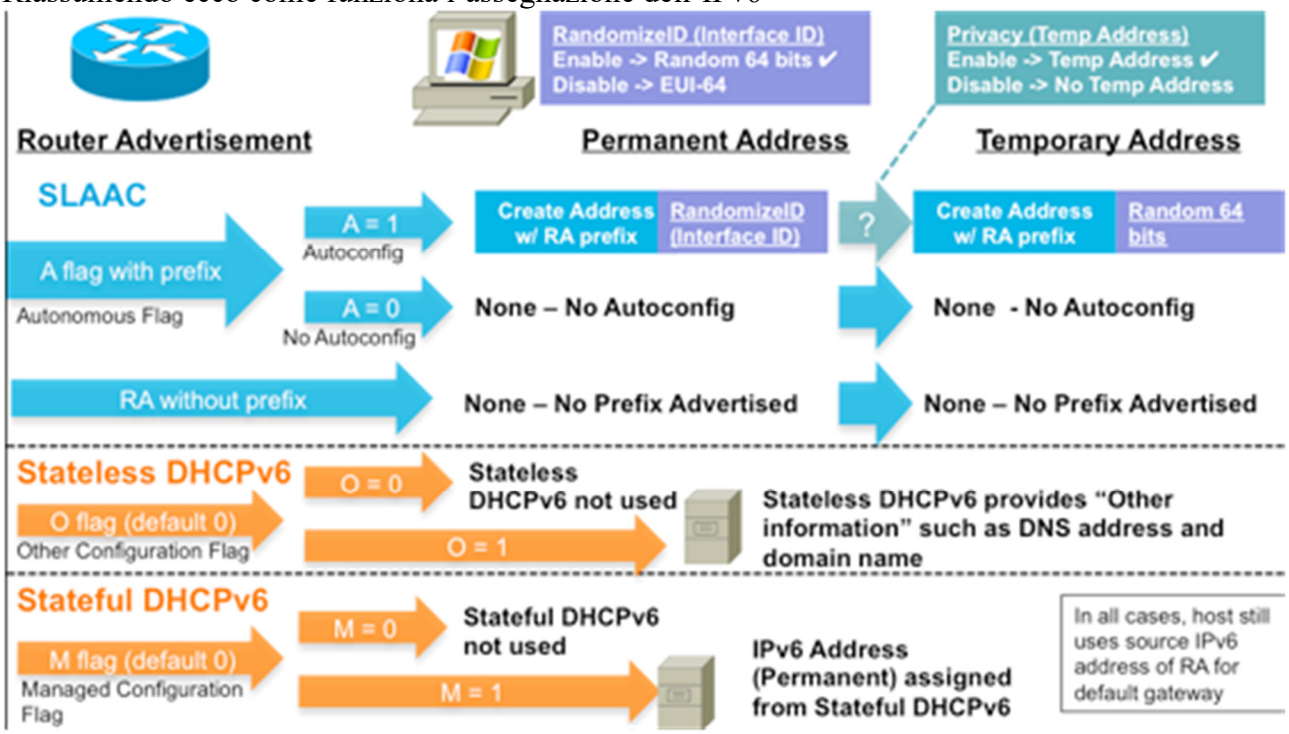
FLAG dell'IPv6

- ✓ Slaac → M=0 O=0
- ✓ Slaac + DHCPv6 → M=0 O=1
- ✓ DHCPv6 → M=1

Nei router CISCO SLAAC è l'impostazione di default ed indica al client di utilizzare esclusivamente le informazioni che gli vengono fornite, quali PrefissoNET, DNS, MTU, Gateway predefinito.
Per modificare il valore di un flag (che ricordiamo di default è 0), basta andare all'interno dell'interfaccia nella configuration terminale

interface g0/0
no ipv6 nd managed-config-flag ← rimetto il flag a 0
no ipv6 nd other-config-flag ← rimetto il flag a 0

Riassumendo ecco come funziona l'assegnazione dell'IPv6



Vediamo ora come configurare la funziona server DHCPv6 (Slaac + DHCPv6)
ipv6 unicast-routing
ipv6 dhcp pool NOME_POOL
dns-server 2001:4860:4860::8888 ← metto i DNS di Google
domain-name retelocale.local
exit
interface g0/0
ipv6 dhcp server NOME_POOL
ipv6 nd other-config-flag ← metto il flag a 1

Abilitiano l'IPv6 su un'interfaccia in modalità Stateless DHCPv6 client:
interface g0/1
ipv6 enable
ipv6 address autoconfig
exit

Comandi di debugging
Verificare pool e parametri IPv6
show ipv6 dhcp pool
Per vedere quali IPv6 (Global Unicast, Link Local, ecc…)sono configurati su una determinata interfaccia
show ipv6 interface g0/0
Per vedere i messaggi scambiati tra il client ed il server IPv6
debug ipv6 dhcp detail

Vediamo ora come configurare la funziona server DHCPv6 (DHCPv6)
ipv6 unicast-routing
ipv6 dhcp pool NOME_POOL
address prefix 2001:DA3:CAFE:1::/64 lifetime infinite
dns-server 2001:4860:4860::8888 ← metto i DNS di Google
domain-name retelocale.local
exit
interface g0/0
ipv6 address prefix 2001:DA3:CAFE:1::1/64
ipv6 dhcp server NOME_POOL
ipv6 nd managed-config-flag ← metto il flag a 1

NB: nell'IPv6 configuro anche dei parametri sull'interfaccia, cosa che non accade nell'IPv4, come ad esempio i flag

Abilitiano l'IPv6 su un'interfaccia in modalità Stateful DHCPv6 client:
interface g0/1
ipv6 enable
ipv6 address dhcp
exit

Il comando
show ipv6 dhcp binding
visualizza come output l'associazione automatica tra Link Local e quello associato dal server

Per impostare un DHCPv6 Relay
ipv6 unicast-routing
interface g0/1
ipv6 dhcp relay destination 2001:DA3:CAFE:1::6
exit
Per visualizzare in questo caso se l'impostazione di relay è corretta
show ipv6 dhcp interface g0/1

8.2.3.5 Lab - Configuring Stateless and Stateful DHCPv6.pdf

Trubleshooting del DHCPv6

1) Risoluzione dei conflitti degli indirizzi IPv4: se viene rilevato un conflitto di indirizzi, l'indirizzo viene rimosso dal pool e non viene assegnato fino a quando un amministratore non risolve il conflitto
   show ipv6 dhcp conflict
2) Verificare che l'interfaccia: se funziona ed che sia UP ed anche i flag
   show ipv6 interface g0/1
3) Verificare la connettività: provare a verificare le funzionalità con un indirizzo IPv6 statico, se non funziona allora il problema non è SLAAC o DHCPv6
4) Attenzione alle VLAN sugli switch

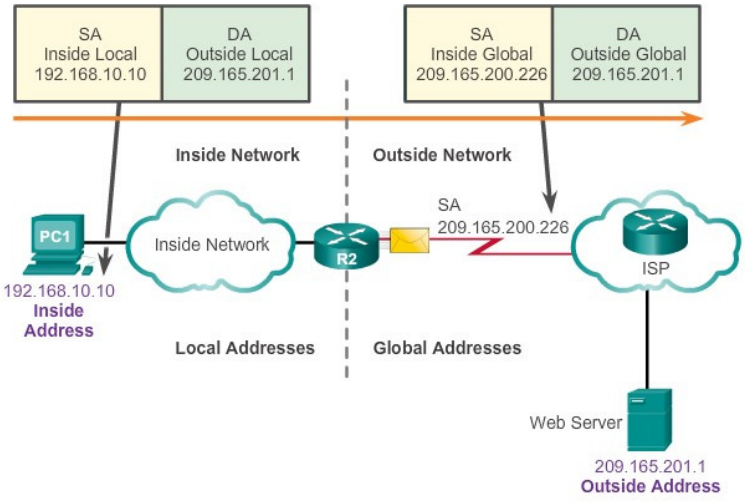
Per effettuare debugging sui router nei quali sembra non funzionare il DHCPv6 server basta lanciare il comando
debug ipv6 dhcp detail
per avere l'output dei messaggi che vengono scambiati tra il server ed i client

8.2.4.4 Lab - Troubleshooting DHCPv6.pdf
8.3.1.1 IoE and DHCP Instructions.pdf
8.3.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
8.3.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 8

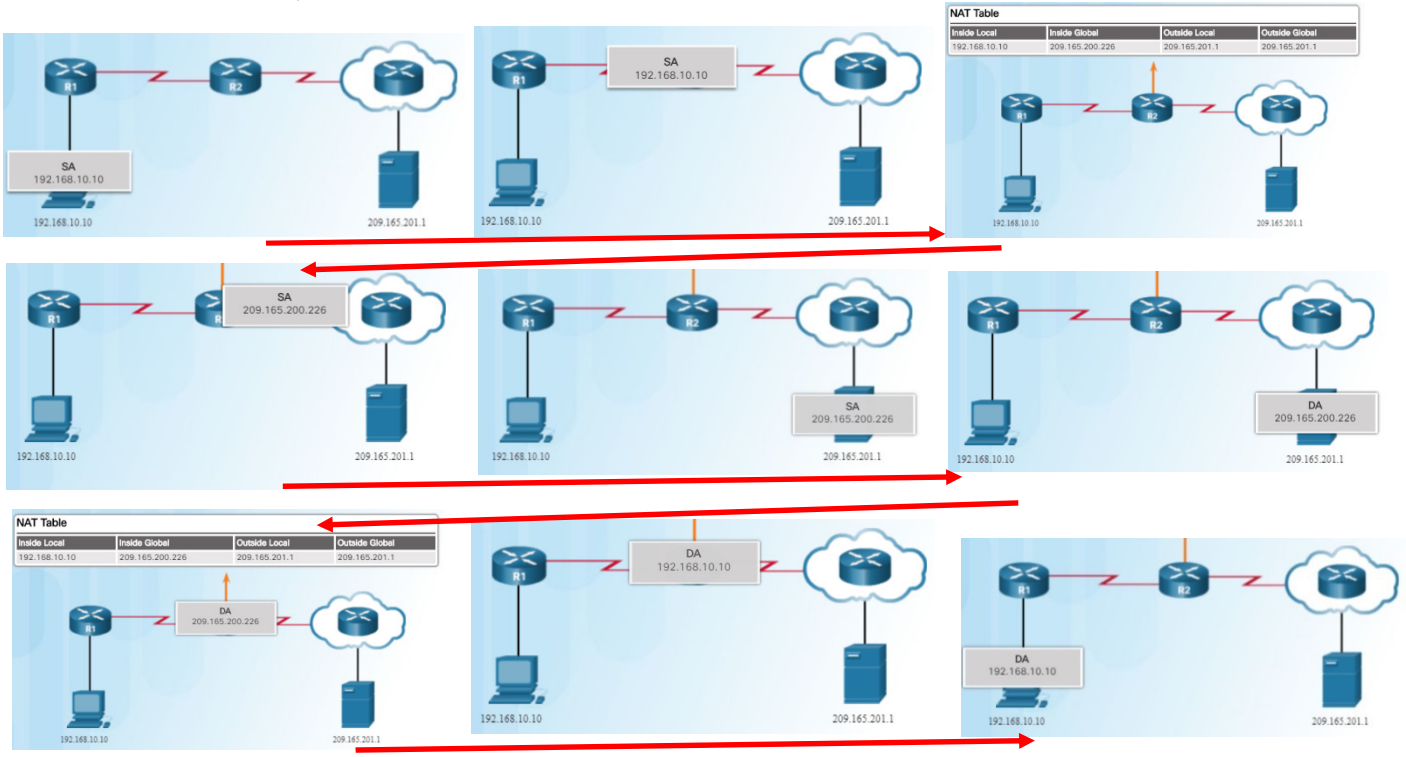
9.0.1.2 Conceptual NAT Instructions.pdf

Essendo gli IPv4 limitati, per scongiurare il collasso della rete internet, si è studiato un sistema in cui le reti locali utilizzano indirizzi privati e per interfacciarsi con internet utilizzano l'IPv4 pubblico fornito dall'ISP tramite il "protocollo" di NAT. Vediamo ora la terminologia per definire gli IPv4 che entrano in gioco a seconda della posizione in cui operano.



Inside Local: IPv4 del dispositivo che viene tradotto da NAT
Outside Local: IPv4 del dispositivo di destinazione
Local Address: qualsiasi IPv4 che compare nella parte locale della rete
Global Address: qualsiasi IPv4 che compare nella parte globale della rete (pubblico)
Inside Global: detto in modo semplice è l'IPv4 con il quale esco
Outside Global: l'IPv4 che devo contattare

Nella sequenza sotto si vede come vengono scambiati gli indirizzi dal router per consentire la funzione di NAT, in vi è un'associazione 1 a 1 tra IPV4 e viene svolta dal router



Esistono 3 tipi di NAT (Network Address Translation):

1) NAT Static: mappatura 1 a 1 tra Inside Local ed Inside Global
2) NAT Dynamic: mappatura molti a molti in maniera dinamica, ossia a turno vi è una mappatura tra Inside Local ed Inside Global
3) PAT (Port Address Translation): vi è una mappatura molti Inside Local ad un Inside Global. Questo processo è detto di NAT Overload. Per capire meglio questo è il processo standard che troviamo sicuramente in tutte le reti domestiche, dove il router si registra IPv4 di partenza, IPv4 di destinazione, porta virtuale di avvio dell'applicazione che utilizzo e porta reale della destinazione. Nel caso in cui due dispositivi vogliano contattare il medesimo server sulla medesima porta ed abbiano deciso di utilizzare (in maniera random) la stessa porta virtuale, sarà il router arbitrariamente ad assegnare nella sua tabella un'assegnazione "porta virtuale +1" ad una delle due connessioni da un dispositivo (slide 9.1.2.4)

Comparazione NAT/PAT

NAT

Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

I pacchetti IPv4 che trasportano dati diversi da un segmento TCP o UDP, ossia che non contengono un numero di porta Layer 4, vengono gestiti da PAT traducendoli in protocolli del livello di trasporto. Il più comune di questi è ICMPv4. Ciascuno di questi tipi di protocolli è gestito in modo diverso da PAT. Ad esempio, i messaggi di query ICMPv4, le richieste di eco e le risposte di eco includono un ID query. ICMPv4 utilizza l'ID query per identificare una richiesta echo con la sua risposta echo corrispondente. L'ID query viene incrementato con ogni richiesta echo inviata.

Semplificando al massimo abbiamo che:

- Il PAT è un Port Forwarding dinamico
- Port Forwarding è un PAT stativo

9.1.2.6 Packet Tracer - Investigating NAT Operation Instructions.pdf
9.1.2.6 Packet Tracer - Investigating NAT Operation.pka

Vantaggi del NAT:

a) Conserva lo schema di indirizzamento interno tramite il multiplexing a livello di porta e applicazione;
b) Aumenta la flessibilità delle connessioni alla rete pubblica;
c) Coerenza per gli schemi di indirizzamento di rete interna. Ossia Se cambio ISP, il cambio di indirizzo pubblico non intacca la gestione della mia rete interna
d) Nasconde gl'IPv4 della rete interna (NB: attenzione a non confondere NAT IPv4 con sicurezza)

Svantaggio del NAT:

a) Degrado delle performance: come ad esempio nelle comunicazioni VoIP perché il NAT deve tradurre i vari IP interni in esterni e viceversa;
b) Degrado delle applicazioni end-to-end: come ad esempio applicazioni di sicurezza, come le firme digitali, falliscono perché l'indirizzo IPv4 di origine cambia prima di raggiungere la destinazione;
c) La tracciabilità end-to-end di IPv4 viene persa. Diventa molto più difficile rintracciare i pacchetti che subiscono numerose modifiche agli indirizzi dei pacchetti su più hopcon NAT, rendendo difficile la risoluzione dei problemi;
d) L'utilizzo del NAT complica anche l'uso di protocolli di tunneling, come IPsec, perché NAT modifica i valori nelle intestazioni, causando il fallimento dei controlli di integrità;
e) I servizi che richiedono l'avvio di connessioni TCP dalla rete esterna o protocolli senza stato, come quelli che utilizzano UDP, possono essere interrotti. A meno che il router NAT sia stato configurato per supportare tali protocolli, i pacchetti in entrata non possono raggiungere la loro destinazione. Alcuni protocolli possono ospitare un'istanza di NAT tra gli host partecipanti (ad esempio, l'FTP in modalità passiva), ma falliscono quando entrambi i sistemi sono separati da Internet tramite NAT;

Vediamo ora come configurare una rotta di NAT statica.
Innanzitutto bisogna creare una mappatura tra gli indirizzi "inside locale" e "inside global", successivamente a questa mappatura, quindi, si avrà che le interfacce che partecipano alla mappatura sono configurate come interne (internal) o esterne (global) rispetto al NAT. Quindi i pacchetti che arrivano sull'interfaccia interna vengono girati a quella esterna e viceversa.

```
ip nat inside source static 192.168.5.3 201.32.34.5
interface g0/0
ip nat inside
exit
interface s0/0/0
ip nat outside
exit
```

Verifica impostazioni di NAT:
show ip nat translations
Nell'output sono sempre presenti le rotte statiche
show ip nat statistics
Fornisce il numero di transazioni eseguite, ed altre info
clear ip nat statistics
Svuota la cache delle statistiche viste sopra, questa funzione è utile per verificare che le NAT route funzionino correttamente durante il trubleshooting.

9.2.1.4 Packet Tracer - Configuring Static NAT Instructions.pdf
9.2.1.4 Packet Tracer - Configuring Static NAT.pka

SOHO → Small Office Home Office

Il NAT dinamico consente appunto una mappatura dinamica tra indirizzo "inside local" e un indirizzo "inside global". Utilizza un pool di IPv4 pubblici che "NATta" dinamicamente a seconda dell'esigenza. Anche il NAT dinamico richiede la mappatura delle interfacce inside ed outside che partecipano alla "mappatura".
Vediamo ora come configurare un NAT dinamico

```
ip nat pool NOME_POOL 155.185.3.1 155.185.3.5 255.255.255.248
access-list 11 permit 192.168.5.0 0.0.0.255
ip nat inside source list 11 pool NOME_POOL
interface g0/0
ip nat inside
exit
interface s0/0/0
ip nat outside
```

Per quanto riguarda il trubleshooting i comandi aggiuntivi rispetto a quelli visti sopra sono:
show ip nat translations verbose
Nell'output sono sempre le rotte con dati aggiuntivi, come il timeout delle rotte di NAT dinamico, che generalmente vengono create di 24
show ip nat translation timeout 3600
modifica il timeout delle rotte di NAT dinamico in 1 ora (si esprime in secondi)
clear ip nat translation *
Pulisce tutte le rotte di NAT dinamico esistenti prima dello scadere del timeout
clear ip nat translation inside 155.185.3.1 192.168.5.3 outside 192.168.5.3 155.185.3.1
Pulisce solamente la rotta dinamica indicata prima dello scadere del timeout

9.2.2.5 Packet Tracer - Configuring Dynamic NAT Instructions.pdf
9.2.2.5 Packet Tracer - Configuring Dynamic NAT.pka
9.2.2.6 Lab - Configuring Dynamic and Static NAT.pdf

Il PAT è un anche detto sovraccarico di NAT, ed è il meccanismo che consente di tradurre molti indirizzi “inside local” in un unico o in alcuni “inside global”. Per capire è quello che fa il nostro modem/router di casa, Che traduce il nostro IPv4 pubblico per i vari device che devono accedere alla rete.

- PAT POOL address

```
ip nat pool PAT-POOL 209.165.200.226 209.165.200.240 255.255.255.224
access-list 32 permit 192.168.1.0 0.0.255.255
ip nat inside source list 32 pool PAT-POOL overload
interface g0/0
ip nat inside
exit
interface s0/0/0
ip nat outside
exit
```

- PAT single address

```
access-list 18 permit 192.168.1.0 0.0.255.255
ip nat inside source list 18 interfce Serial0/0/0 overload
interface g0/0
ip nat inside
exit
interface s0/0/0
ip nat outside
exit
```

Il trubleshooting del PAT si esegue con i comandi di trubleshooting del NAT poiché il PAT è uno specifico caso di NAT.

9.2.3.6 Packet Tracer - Implementing Static and Dynamic NAT Instructions.pdf
9.2.3.6 Packet Tracer - Implementing Static and Dynamic NAT.pka
9.2.3.7 Lab - Configuring Port Address Translation (PAT).pdf

Il port forwarding è l'atto di inoltrare il traffico indirizzato a una specifica porta di rete da un nodo di rete a un altro. Il port forwarding è un NAT statico solamente di servizi che sono forniti dai device della rete.
Vediamo come realizzare uno specifico port forward

```
ip nat inside source static tcp 192.168.5.3 80 201.32.34.5 80
interface g0/0
ip nat inside
exit
interface s0/0/0
ip nat outside
exit
```

9.2.4.4 Packet Tracer - Configuring Port Forwarding on a Wireless Router.pdf
9.2.4.4 Packet Tracer - Configuring Port Forwarding on a Wireless Router.pka

Il NAT su protocollo IPv6 diretto non è utilizzato per progettazione stessa dell'IPv6, in quanto è stato pensato che ad ogni device corrisponda un IPv6, ma per poter effettuare una comunicazione tra IPv4 ed IPv6 il NAT è uno strumento molto utili e versatile. Infatti in questo periodo di transazione, ci imbattiamo nel
NAT64 → è il NAT tra IPv6 to IPv4

Utilizzare il comando **debug nat ip** per verificare l'operazione della funzione NAT visualizzando le informazioni su ogni pacchetto che viene "NATtato" dal router

9.3.1.4 Packet Tracer - Verifying and Troubleshooting NAT Configurations Instructions.pdf
9.3.1.4 Packet Tracer - Verifying and Troubleshooting NAT Configurations.pka
9.3.1.5 Lab - Troubleshooting NAT Configurations.pdf
9.4.1.1 NAT Check Instructions.pdf
9.4.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
9.4.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 9

Cisco Discovery Protocol (CDP) è un protocollo Layer 2 proprietario di Cisco che viene utilizzato per raccogliere informazioni sui dispositivi Cisco che condividono lo stesso collegamento dati. CDP è indipendente dal protocollo e funziona su tutti i dispositivi Cisco, come router, switch e server di accesso. CDP può anche essere usato come strumento di scoperta della rete per determinare le informazioni sui dispositivi vicini. Queste informazioni raccolte da CDP possono aiutare a costruire una topologia logica di una rete quando manca la documentazione o manca in dettaglio.
Per i dispositivi Cisco, CDP è abilitato per impostazione predefinita.

Per verificare lo stato di CDP e visualizzare le informazioni su CDP
show cdp
Per disabilitare CDP globalmente per tutte le interfacce
no cdp run
Per disabilitarlo in una specifica interfaccia
interface g0/1
no cdp enable
Per verificare lo stato di CDP e visualizzare un elenco di vicini
show cdp neighbors
Per verificare lo stato di CDP e visualizzare un elenco di vicini con maggiori dettagli
show cdp neighbors detail
Per visualizzare le interfacce abilitate per CDP su un dispositivo
show cdp interface

10.1.1.4 Packet Tracer - Map a Network Using CDP.pdf
10.1.1.4 Packet Tracer - Map a Network Using CDP.pka

I dispositivi Cisco supportano anche il protocollo LLDP (Link Layer Discovery Protocol), che è un protocollo di individuazione dei vicini di prossimità simile a CDP.
A seconda del dispositivo, LLDP può essere abilitato per impostazione predefinita

Per abilitare LLDP globalmente su un dispositivo
lldp run
Per disabilitare LLDP
no lldp run
Simile a CDP, LLDP può essere configurato su interfacce specifiche, Tuttavia, LLDP deve essere configurato separatamente per trasmettere e ricevere pacchetti LLDP
Per verificare che LLDP sia stato abilitato sul dispositivo
show lldp
Per disattivare LLDP su una specifica interfaccia
interface s0/0/0
no lldp transmit
end
Per vedere i vicini e le loro caratteristiche
show lldp neighbors
Per vedere i vicini e le loro caratteristiche con maggiori dettagli
show lldp neighbors detail

10.1.2.5 Lab - Configure CDP and LLDP.pdf

Impostare l'orario di sistema degli apparati:

- modalità statica:
  clock set 17:08:00 gen 7 2018
- Server ntp (protocollo UDP su porta 123):
  I server NTP sono suddivisi in livelli detti strati, dallo 0 a salire, quindi con il numero più piccolo si identifica la minor distanza dalla fonte più autorevole.
  ntp server 193.204.114.232 ← Server NTP INRIM (orologio Atomico di Torino)

Verifica dell'orario di sistema
show clock
Verifica dell'orario di sistema dettagliato
show clock detail
Mostra a quale server NTP tentiamo di collegarci per aggiornare l'orario
show ntp associations
Mostra lo stato di aggiornamento orario con il server ntp
show ntp status

10.2.1.4 Packet Tracer - Configure and Verify NTP.pdf
10.2.1.4 Packet Tracer - Configure and Verify NTP.pka

Quando determinati eventi si verificano su una rete, i dispositivi di rete dispongono di meccanismi affidabili per notificare all'amministratore messaggi di sistema dettagliati. Questi messaggi possono essere archiviati secondo un protocollo detto "Syslog".
Il protocollo SYSLOG utilizza la porta UDP 514 per inviare messaggi di notifica degli eventi su reti IP agli appositi server di archiviazione.

Il servizio di registrazione dei log tramite syslog offre 3 principali funzioni

1) La capacità di raccogliere informazioni di registrazione per il monitoraggio e la risoluzione dei problemi
2) La possibilità di selezionare il tipo di informazioni di registrazione acquisite
3) La possibilità di specificare le destinazioni dei messaggi syslog catturati

Negli apparati CISCO il protocollo SYSLOG si avvia con il debug, ma si può inviare l'output ad un server SYSLOG oppure mandare l'output in CLI oppure decidere quale output far visualizzare in CLI.
Riassumendo quindi in un dispositivo CISCO le destinazioni popolari per i messaggi SYSLOG includono:

- ✓ Buffer di registrazione (RAM all'interno di un router o switch)
- ✓ Linea di console (CLI)
- ✓ Linea terminale (Telnet, SSH)
- ✓ Server SYSLOG

I dispositivi Cisco producono messaggi SYSLOG come risultato di eventi di rete. Ogni messaggio SYSLOG contiene un livello di gravità e una funzionalità.

Severity Name	Severity Level	Explanation
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

I livelli numerici più piccoli sono gli allarmi SYSLOG più critici. Accanto una tabella riassuntiva dei livelli

Oltre a specificare la gravità, i messaggi di SYSLOG contengono anche informazioni sulla struttura. Le strutture di SYSLOG sono identificatori di servizio che identificano e categorizzano i dati di stato del sistema per la segnalazione di messaggi di errore e di eventi. Le opzioni della funzione di registrazione disponibili sono specifiche per il dispositivo di rete.
Alcune delle comuni funzioni di messaggio syslog riportate sui router Cisco IOS includono:

- IP
- Protocollo OSPF
- Sistema operativo SYS
- Sicurezza IP (IPsec)
- IP interfaccia (IF)

Per impostazione predefinita, il formato dei messaggi SYSLOG sul software Cisco IOS è il seguente:

```
seq no: timestamp: %facility-severity-MNEMONIC: description
```

seq no - registra il messaggio di registro con un numero di sequenza solo se il comando di configurazione globale del numero di sequenza del servizio del server è configurato
timestamp - data e ora del messaggio o dell'evento, che appare solo se è configurato il comando di configurazione globale del timestamp del servizio
facility – la struttura a cui si riferisce il messaggio
severity - codice a una cifra da 0 a 7 che indica la gravità del messaggio
MNEMONIC - stringa di testo che descrive in modo univoco il messaggio
description - stringa di testo contenente informazioni dettagliate sull'evento segnalato

Vediamo sotto un esempio di output:

```
00:00:46: %LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

I messaggi più comuni sono i messaggi di collegamento delle interface UP o DOWN ed i messaggi che un dispositivo produce quando esce dalla modalità di “Configuration Terminal”. Se la registrazione ACL è configurata, il dispositivo genera messaggi SYSLOG quando i pacchetti corrispondono a una condizione di parametro.

Per impostazione predefinita, i messaggi di registro non sono Timestamp, ossia non viene loggata la data e l’ora dei cambiamenti di stato. Ma per avere una migliore e più completa lettura nell’eventuale SYSLOG è bene attivare il TIMESTAMP

```
interface g0/0
shutdown
exit
service timestamps log datetime
interface g0/0
shutdown
exit
```

NB: quando si utilizza la parola **datatime**, l’orologio del device dev’essere già stata configurata o manualmente o con server NTP come precedentemente descritto

Per visualizzare i messaggi SYSLOG, è necessario installare un server SYSLOG sulla rete (Win: KIWI, Linux: Zabbix, Nagios). Il server SYSLOG fornisce un'interfaccia relativamente user-friendly per la visualizzazione dell'output di SYSLOG. Il server analizza l'output e posiziona i messaggi in colonne predefinite per una facile interpretazione. Se i timestamp sono configurati sul dispositivo di rete che genera i messaggi SYSLOG, la data e l'ora di ciascun messaggio vengono visualizzate nell'output del server SYSLOG.

Per impostazione predefinita, i router e gli switch Cisco inviano messaggi di log per tutti i livelli di gravità alla console. Su alcune versioni IOS, il dispositivo memorizza anche i messaggi di registro per impostazione predefinita. Per abilitare queste 2 impostazioni dalla "Configuration Terminal":
logging console
logging buffered

```
R1# show logging
Syslog logging: enabled (0 messages dropped, 2 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)

No Active Message Discriminator.

No Inactive Message Discriminator.

        Console logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Monitor logging: level debugging, 0 messages logged, xml disabled,
                         filtering disabled
        Buffer logging: level debugging, 32 messages logged, xml disabled,
                         filtering disabled
        Exception Logging: size (4096 bytes)
        Count and timestamp logging messages: disabled
        Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 34 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (8192 bytes):

*Jan 2 00:00:02.527: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License
Agreement is accepted
*Jan 2 00:00:02.631: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
```

Il comando **show logging**, mostra le impostazioni del servizio di registrazione predefinito su un router Cisco.

La prima riga evidenziata indica che questo router accede alla console e include i messaggi di debug. Ciò significa che tutti i messaggi di livello di debug e tutti i messaggi di livello inferiore (come i messaggi a livello di notifica) vengono registrati nella console.

La seconda riga evidenziata indica che questo router accede a un buffer interno. Poiché questo router ha abilitato la registrazione su un buffer interno, il comando di registrazione elenca anche i messaggi in quel buffer.
È possibile visualizzare alcuni dei messaggi di sistema che sono stati registrati alla fine dell'output.

Ci sono tre passaggi per configurare il router per inviare messaggi di sistema a un server SYSLOG:
logging 192.168.1.200
logging trap 4 ← invia tutti i log di livello 4 o inferiori
logging source-interface g0/0 ← indica da che interfaccia provengono i log **OPZIONALE**.
Quest'ultimo comando che indica l'interfaccia di origine specifica in realtà quale indirizzo IP di interfaccia verrà utilizzato come indirizzo IP di origine dei pacchetti SYSLOG inviati al server, ma l'effettiva interfaccia in uscita sarà determinata dalla tabella di routing.
Ossi se nel mio router ho impostato l'ip 10.0.0.44/8 alla porta g0/0 ed il server SYSLOG è il 192.168.1.200, nel server SYSLOG come mittente avrò 10.0.0.44

10.2.3.5 Packet Tracer - Configuring Syslog and NTP Instructions.pdf
10.2.3.5 Packet Tracer - Configuring Syslog and NTP.pka
10.2.3.6 Lab - Configuring Syslog and NTP.pdf

Per la gestione degli apparati vi sono vari comandi (in stile Linux) che ci possono tornare utili:
show file systems
che indica tutti i file system presenti sul device, ma a noi interesseranno principalmente tftp, flash, nvram.
Con l'output del comando sopra, si ottengono anche informazioni extra, come il file system flash ha un asterisco che lo precede, ciò indica che il flash è il file system predefinito. L'IOS avviabile si trova in flash, pertanto, il simbolo cancelletto (#) viene aggiunto all'elenco Flash, e sta ad indicare che si tratta di un disco di avvio.

Comandi CLI
dir – elenca il contenuto di una directory
cd – mi sposto tra le directory
pwd – mi dà il percorso assoluto della directory in cui mi trovo
more – per vedere il contenuto di un file (es. una configurazione salvata)

Per effettuare il salvataggio delle configurazioni di un device, vi sono vari modi:

1) Copia in Notepad
2) Copia tramite server tftp
   copy running-config tftp
   e mi verrà chiesto: ip del server TFTP, nome del file di configurazione e la conferma
3) Copia su dispositivo USB (de il device lo supporta)
   copy running-config usbflash0:
   e mi verrà chiesto il nome del file di configurazione
   NB: nel caso un file con lo stesso nome esiste, mi chiederà conferma per la sovrascrittura

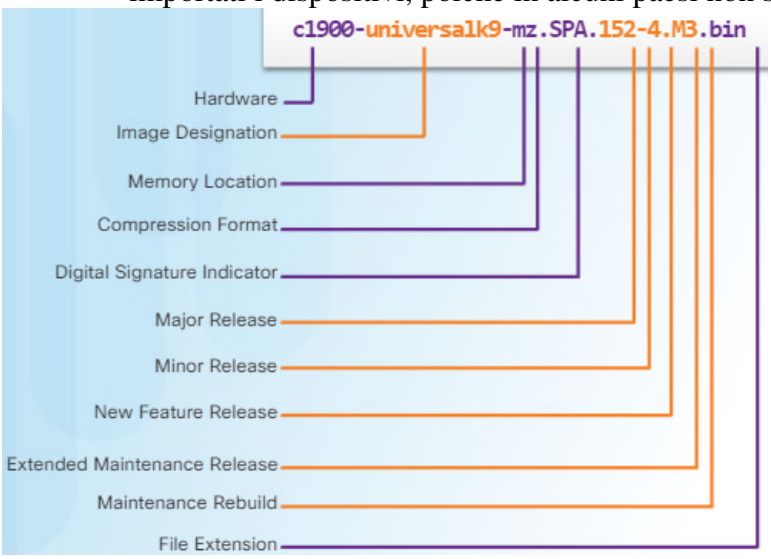
Vediamo ora come effettuare il reset di una password

1) Innanzitutto bisogna avere accesso fisico al device
2) Spegnere e ri-accendere il device
3) Durante la fase di boot, andare in modalità ROMMON
   a. su tastiera inglese: Ctrl-Break
   b. su tastiera italiana: Ctrl-Interr (Pausa) oppure CTRL+C oppure Ctrl+P
4) **confreg 0x2142**
5) **reset**
6) Attendere il riavvio del device
7) **enable** (ed entro senza password)
8) **copy startup-config running-config**
9) **configure terminal**
10) **enable secret cisco**
11) **config-register 0x2102**
12) **exit**
13) **copy running-config startup-config**
14) **reload**

10.3.1.8 Packet Tracer - Backing Up Configuration Files Instructions.pdf
10.3.1.8 Packet Tracer - Backing Up Configuration Files.pka
10.3.1.9 Lab - Managing Router Configuration Files with Terminal Emulation Software.pdf
10.3.1.10 Lab - Managing Device Configuration Files Using TFTP, Flash, and USB.pdf
10.3.1.11 Lab - Configure and Verify Password Recovery.pdf

La gestione dell'OS Cisco IOS, viene gestita tramite licenza.
Sui dispositivi è installata un'immagine base standard con "teoricamente" tutto il software a disposizione, che viene sbloccato in base alle licenze che vi vengono attivate sopra.
Ciascuna chiave di licenza è unica per un particolare dispositivo ed è ottenuta da Cisco fornendo l'ID del prodotto e il numero di serie del router e una chiave di attivazione del prodotto (PAK). Il PAK è fornito da Cisco al momento dell'acquisto del software.
Per vedere la versione dello IOS installato, dare il comando **show version**
L'immagine del sistema viene identificata con la nomenclatura ***univarsalk9***.

Una nomenclatura ***univarsalk9_npe*** identifica un'immagine con una forte applicazione alla crittografia, e quindi alla sicurezza, questa immagine però varia a seconda del paese in cui vengono importati i dispositivi, poichè in alcuni paesi non sono consentite alcune tecnologie di crittazione.



Per avere maggiori informazioni sull'OS installato sul nostro router per poi poter cercare l'apposita immagine per aggiornarlo, possiamo dare il comando:

show flash0:

e leggere l'output come la figura accanto

Vediamo come effettuare il backup dell'OS tramite server TFTP:
show flash0:
copy flash0: tftp:
c1900-iniversalk9-mz.SPA.152-4.M3.bin
192.168.1.200

Vediamo come aggiornare l'immagine dell'OS tramite server TFTP:

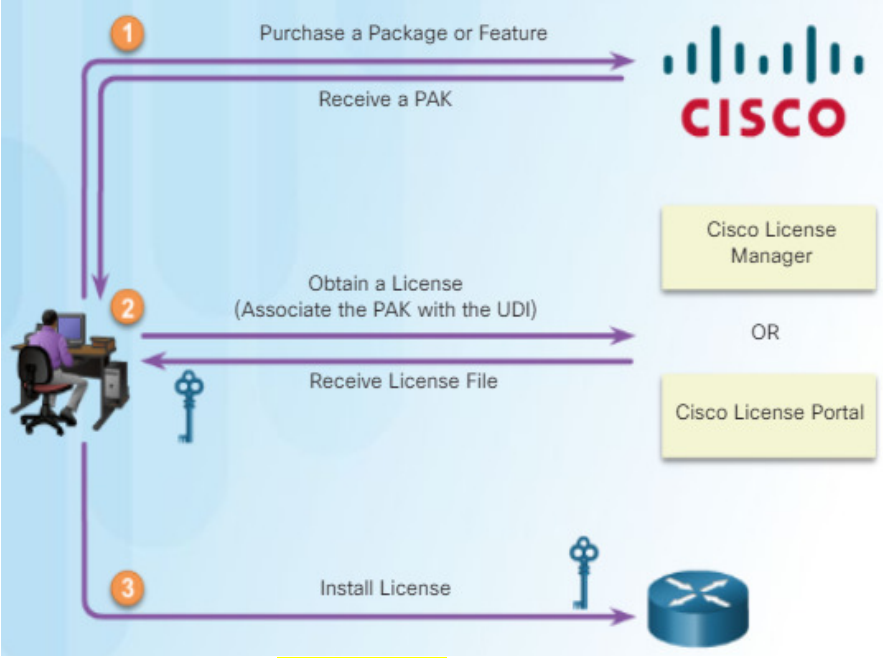
prima la si deve copiare dal server TFTP alla flash
copy tftp: flash0:
192.168.1.200
c1900-iniversalk9-mz.SPA.152-4.M3.bin

poi bisogna "flashare" il device
configure terminal
boot system flash0:// c1900-iniversalk9-mz.SPA.152-4.M3.bin
exit

10.3.3.5 Packet Tracer - Using a TFTP Server to Upgrade a Cisco IOS Image Instructions.pdf
10.3.3.5 Packet Tracer - Using a TFTP Server to Upgrade a Cisco IOS Image.pka

Lanciando il comando **show license feature**, posso sapere quali funzionalità sono attivate sul mio device.

Per attivare una determinata funzionalità (licenza) su un device, dovvrò procedere nel seguente modo:



1) Acquisto del software fornendo a CISCO o al partener CISCO, UDI, Seriale e PAK. Tranne il PAK gli altri 2 codici possono essere lettei dall'apparato con il comando **show license udi**

2) Si riceve il seriale da uno dei 2 canali CISCO

3) Lo si installa sul device

```
copy tftp: flash0:
192.168.1.200
securityk9:-CISCO1941-FHH12250057.lic
license install flash0: securityk9:-
CISCO1941-FHH12250057.lic
reload
```

Il comando **show license** mi mostra l'elenco delle licenze attivabili sul device e il relativo stato di attivazione.
È anche possibile attivare le licenze per una valutazione (circa 60 giorni) con il comando:

```
license accept end user agreement
license boot module YYYY technology-package XXX
```

YYYY module name, identifica il device es. c19000
dove XXX è uno dei moduli attivabili:

- ipbasek9 - Pacchetto della tecnologia IP Base
- securityk9 - Pacchetto sulla tecnologia di sicurezza
- datak9 - Pacchetto di tecnologia dati
- uck9 - Pacchetto Unified Communications (non disponibile su serie 1900)

Salvare la licenza:

```
license save flash0:all_licenses.lic
```

Considerando XXXX → moduli e YYYY → id device avremo che:
Disattivare una licenza

```
configure terminal
license boot module YYYY technology-package XXXX disable
exit
reload
```

Togliere la licenza

```
license clear XXXX
configure terminal
no license boot module YYYY technology-package XXXX disable
exit
reload
```

NB: si possono rimuovere o disabilitare solo le licenze che si sono installate
10.4.1.1 Packet Tracer - Skills Integration Challenge.pdf
10.4.1.1 Packet Tracer - Skills Integration Challenge.pka

Modulo 3

CAPITOLO 1

1.0.1.2 Class Activity - Network by Design

La creazione di una rete dev'essere fatta in modo intelligente sia per l'utilizzo intrinseco, sia con una previsione di crescita aziendale senza stravolgimento della struttura nella scalabilità, considerando anche che tutte le reti aziendali devono:

- Supportare applicazioni critiche
- Supportare traffico di rete convergente
- Sostenere diverse esigenze aziendali
- Fornire un controllo amministrativo centralizzato

Le LAN aziendali utilizzano un modello di progettazione gerarchico per suddividere i reparti in livelli (creando più broadcast domain), che rimanendo più piccoli sono più comodi da gestire, ossia il progetto in livelli consente a ciascun livello di implementare funzioni specifiche, semplificando la progettazione della rete e quindi l'implementazione e la gestione della rete.
Un design LAN gerarchico include i seguenti tre livelli:

- Livello di accesso
- Strato di distribuzione
- Strato centrale

Il livello di accesso fornisce agli endpoint e agli utenti l'accesso diretto alla rete. Il livello di distribuzione aggrega i livelli di accesso e fornisce connettività ai servizi. Infine, il livello principale fornisce connettività tra i livelli di distribuzione per ambienti LAN di grandi dimensioni. Il traffico dell'utente viene avviato al livello di accesso e passa attraverso gli altri livelli se è richiesta la funzionalità di tali livelli.
Nelle architetture di rete piatte o mesh (collapsed core), le modifiche tendono a influire su un numero elevato di sistemi. Il design gerarchico aiuta a limitare le modifiche operative a un sottoinsieme della rete, il che semplifica la gestione e migliora la resilienza. La strutturazione modulare della rete in elementi piccoli e di facile comprensione facilita anche la resilienza tramite un migliore isolamento dei guasti.

Nel design di una LAN per progettare la futura scalabilità della rete, bisogna:

- Utilizzare dispositivi espandibili e modulari o dispositivi cluster che possono essere facilmente aggiornati per aumentare le capacità
- Progettare una rete gerarchica per includere moduli che possono essere aggiunti, aggiornati e modificati, se necessario, senza influire sul design delle altre aree funzionali della rete
- Creare una strategia di indirizzo IPv4 o IPv6 gerarchica. Un'attenta pianificazione degli indirizzi elimina la necessità di reindirizzare la rete per supportare utenti e servizi aggiuntivi
- Scegli router o switch multistrato per limitare le trasmissioni e filtrare altro traffico indesiderato dalla rete
- Implementazione di collegamenti ridondanti nella rete tra dispositivi critici e tra livello di accesso e dispositivi di livello base
- Implementazione di più collegamenti tra apparecchiature, con link aggregation (EtherChannel) o bilanciamento del costo, per aumentare la larghezza di banda
- Utilizzo di un protocollo di routing scalabile e implementazione delle funzionalità all'interno di tale protocollo di routing per isolare gli aggiornamenti di routing e ridurre al minimo le dimensioni della tabella di routing

Per molte aziende la parte più critica della rete è la ridondanza dei collegamenti, ed è una delle parti più importanti nella progettazione delle reti. Un metodo per implementare la ridondanza è installare apparecchiature duplicate e fornire servizi di failover per dispositivi critici. Un altro metodo per implementare la ridondanza è rappresentato dai percorsi ridondanti (link ridondati).
Tuttavia, a causa del funzionamento degli switch, i percorsi ridondanti in una rete Ethernet commutata possono causare loop logici di livello 2. Per questo motivo, è richiesto lo Spanning Tree Protocol (**STP**).
STP elimina i loop Layer 2 quando vengono utilizzati collegamenti ridondanti tra gli switch. Lo fa fornendo un meccanismo per disabilitare i percorsi ridondanti in una rete commutata finché il percorso non è necessario. **STP** è un protocollo standard aperto, utilizzato in un ambiente commutato per creare una topologia logica senza loop.

Nella progettazione gerarchica della rete, alcuni collegamenti tra gli switch di accesso e di distribuzione potrebbero dover elaborare una quantità di traffico maggiore rispetto ad altri collegamenti. Poiché il traffico proveniente da più collegamenti converge su un singolo link in uscita, è possibile che quel collegamento diventi un collo di bottiglia. L'aggregazione dei collegamenti consente a un amministratore di aumentare la larghezza di banda tra i dispositivi creando un collegamento logico costituito da diversi collegamenti fisici. EtherChannel è una forma di aggregazione di link utilizzata nelle reti commutate.
EtherChannel utilizza le porte dello switch esistenti ed è visto come un collegamento logico. La maggior parte delle attività di configurazione viene eseguita sull'interfaccia EtherChannel, anziché su ogni singola porta, garantendo la coerenza della configurazione attraverso i collegamenti. Infine, la configurazione EtherChannel sfrutta il bilanciamento del carico tra i collegamenti che fanno parte dello stesso EtherChannel e, a seconda della piattaforma hardware, è possibile implementare uno o più metodi di bilanciamento del carico.

Protocolli di routing avanzati, come OSPF e EIGRP, vengono utilizzati nelle reti di grandi dimensioni. I protocolli di routing link-state come Open Shortest Path First (OSPF), funzionano bene per reti gerarchiche più grandi in cui la convergenza veloce è importante. I router OSPF stabiliscono e mantengono l'adiacenza o le adiacenze dei vicini, con altri router OSPF collegati. Quando i router iniziano un'adiacenza con i vicini, inizia uno scambio di aggiornamenti sullo stato dei collegamenti. Con OSPF, gli aggiornamenti dello stato dei collegamenti vengono inviati quando si verificano cambiamenti di rete.

- **Cost** - The cost of a switch will depend on the number and speed of the interfaces, supported features, and expansion capability.
- **Port Density** - Network switches must support the appropriate number of devices on the network.
- **Power** - It is now common to power access points, IP phones, and even compact switches using Power over Ethernet (PoE). In addition to PoE considerations, some chassis-based switches support redundant power supplies.
- **Reliability** - The switch should provide continuous access to the network.
- **Port Speed** - The speed of the network connection is of primary concern to end users.
- **Frame Buffers** - The ability of the switch to store frames is important in a network where there may be congested ports to servers or other areas of the network.
- **Scalability** - The number of users on a network typically grows over time; therefore, the switch should provide the opportunity for growth.

Nella scelta degli switch di rete (“nella scelta del ferro”) bisogna prendere in considerazione i parametri qui accanto per l’utilizzo che ne dobbiamo fare nella rete in progettazione.
Poi al termine delle valutazioni ci riconduciamo alle macro categorie per scegliere l’apparato:

- Campus LAN
- Data Center
- Cloud-Managed
- Service Provider
- Virtual Networking

Un altro aspetto da prendere in considerazione è il Port Density, a seconda del numero di device che dobbiamo collegare alla rete.
Nelle PMI di solito bastano i dispositivi fissi, ossia switch che hanno 16/24 o 48 porte, che eventualmente possono avere 4 porte aggiuntive SFP (small-form factor pluggable) per collegare gli switch ad altri (magari con fibra).
Per le grandi aziende che necessitano di collegare migliaia di dispositivi, si utilizzeranno degli switch modulari che sono in grado di supportare densità di porte molto elevate grazie all'aggiunta di più schede di linea per le porte degli switch.

Un punto importante per la scelta di uno switch è il Forwarding Rate, ossia la gestione di banda che può supportare. Ad esempio, un tipico switch gigabit a 48 porte che funziona a piena velocità, genera 48 Gb/s di traffico. Se lo switch supporta solo una velocità di inoltro di 32 Gb/s, non può funzionare a piena velocità su tutte le porte contemporaneamente. Ciò significa che gli switch meno costosi e dalle prestazioni più basse possono essere utilizzati a livello di accesso (perché difficilmente tutti i device collegati dovranno andare al massimo della velocità di rete consentita), mentre gli switch più costosi e dalle prestazioni più elevate possono essere utilizzati nei livelli di distribuzione e core, dove la velocità di inoltro ha un impatto maggiore sulle prestazioni della rete.

Infine bisogna valutare se si necessita di switch PoE (Power over Ethernet) oppure no.
PoE consente allo switch di fornire alimentazione a un dispositivo tramite il cablaggio Ethernet esistente. Questa funzione può essere utilizzata dai telefoni IP e da alcuni punti di accesso wireless. PoE consente una maggiore flessibilità durante l'installazione di punti di accesso wireless e telefoni IP, permettendo di installarli ovunque ci sia un cavo Ethernet.
Il PoE è uno standard ma a differenti livelli per cui è necessario valutare sia l'energia fornita dallo switch sia quella richiesta dal dispositivo prima di acquistare uno switch, come mostrato nelle tabelle.

Property	802.3af (802.3at Type 1) "PoE"	802.3at Type 2 "PoE+"	802.3bt Type 3 "4PPoE"	802.3bt Type 4
Power available at PD	12.95 W	25.50 W	51 W	71 W
Maximum power delivered	15.40 W	30.0 W	60 W	100 W
Voltage range	44.0–57.0 V	50.0–57.0 V	50.0–57.0 V	52.0–57.0 V
Voltage range	37.0–57.0 V	42.5–57.0 V	42.5–57.0 V	41.1–57.0 V
Maximum current	350 mA	600 mA[27]	600 mA per pair	960 mA per pair
Maximum cable resistance per pairset	20 Ω	12.5 Ω	12.5 Ω	12.5 Ω
Supported cabling	Category 3 and Category 5	Category 5	Category 5	Category 5

Classi 802.3af

Classe	Corrente misurata (mA)	Range potenza utilizzatore (W)	Note
0	da 0 a 4	da 0,44 a 12,95	standard
1	da 9 a 12	da 0,44 a 3,84	opzione1
2	da 17 a 20	da 3,84 a 6,49	opzione2
3	da 26 a 30	da 6,49 a 12,95	opzione3
4	da 36 a 44	riservato	uso futuro

Per esempio un apparato che richieda come standard di utilizzo da data-sheet un "PoE IEEE 802.3af Class 3", nella scelta dello switch dovrò cercare i parametri composit e segnalati dalle 2 tabelle

1.2.1.7 Packet Tracer - Compare 2960 and 3560 Switches.pdf
1.2.1.7 Packet Tracer - Compare 2960 and 3560 Switches.pka

Nel livello di distribuzione di una rete aziendale, è richiesto il routing. Senza il processo di routing, i pacchetti non possono lasciare la rete locale. I router possono anche fungere da traduttore tra diversi tipi di media e protocolli. I router utilizzano la parte di rete dell'indirizzo IP di destinazione per instradare i pacchetti alla destinazione corretta. Selezionano un percorso alternativo se un collegamento o percorso scende. Tutti gli host su una rete locale specificano l'indirizzo IP dell'interfaccia del router locale nella loro configurazione IP. Questa interfaccia del router è il gateway predefinito.
I router servono anche per :

- Limitare i broadcast domain
- Connettere postazioni remote
- Raggruppare gli utenti logicamente per applicazione o per reparto
- Fornire maggiore sicurezza

Man mano che la rete cresce, è importante selezionare i router appropriati per soddisfare i propri requisiti. CISCO suddivide i router in 3 categorie:

Branch Routers: ottimizzano i servizi di filiale su una singola piattaforma offrendo al tempo stesso un'esperienza applicativa ottimale tra infrastrutture Branch e WAN.
Network Edge Routers: i router di bordo (Edge) della rete consentono alla rete di offrire servizi ad alte prestazioni, altamente sicuri e affidabili che uniscono campus, data center e reti di filiali.
Service Provider Routers: sono i router dei service provider differenziano il portafoglio di servizi e aumentano i ricavi offrendo soluzioni scalabili end-to-end e servizi consapevoli dell'abbonato.

Anche i router come gli switch possono essere classificati in fissi e modulari con le medesime spiegazioni di fissi e modulari.

Gli apparati di rete (switch e router) possono essere amministrati in 2 modalità:

- Out-of-band: ossia collegandomi direttamente al dispositivo su porta Console o AUX (anche tramite dispositivi remoti)
- In-band: ossia collegandomi sul dispositivo tramite la rete ed un protocollo di rete abilitato per il management sul dispositivo (Ssh, Telnet, http, Https)

1.3.1.1 Class Activity - Layered Network Design Simulation.pdf
1.3.1.3 Packet Tracer - Skills Integration Challenge.pdf
1.3.1.3 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 1

Con l'espansione della rete aziendale, anche la gestione delle VLAN da parte dell'amministratore diventa più complessa, ecco che CISCO in aiuto dei SysAdmin ha introdotto il VTP (VLAN trunking protocol), ossia consente a un amministratore di rete di gestire le VLAN su uno switch configurato come server VTP. Il server VTP distribuisce e sincronizza le informazioni VLAN sui collegamenti trunk verso gli switch abilitati VTP in tutta la rete. Ciò minimizza i problemi causati da configurazioni errate e incongruenze di configurazione.
NB: VTP apprende solo sulle VLAN a intervallo normale (ID VLAN da 1 a 1005). VLAN a lungo raggio (ID superiori a 1005) non sono supportate da VTP versione 1 o versione 2.

VTP Components	Definition
VTP Domain	• Consists of one or more interconnected switches. • All switches in a domain share VLAN configuration details using VTP advertisements. • Switches that are in different VTP domains do not exchange VTP messages. • A router or Layer 3 switch defines the boundary of each domain.
VTP Advertisements	• Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. • Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.
VTP Modes	A switch can be configured in one of three VTP modes: server, client, or transparent.
VTP Password	Switches in the VTP domain can be also be configured with a password.

Nella tabella accanto i principali parametri da settare sugli switch per ottimizzare il VTP

Analizziamoli ora più nel dettaglio:
VTP Modes – Vi sono 3 modalità di configurazione:

Server:
- Pubblicizza le informazioni VLAN del dominio VTP ad altri switch VTP abilitati nello stesso dominio VTP
- Memorizza le informazioni VLAN per l'intero dominio in NVRAM (vlan.dat)
- Crea, elimina o rinomina le VLAN per il dominio
- È la modalità VTP predefinita

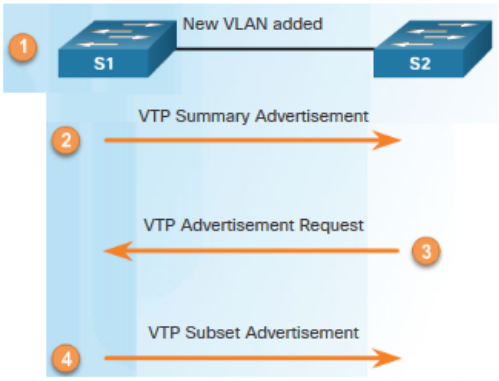
Client:
- Non consente di creare, modificare o eliminare VLAN
- Memorizza le informazioni VLAN per l'intero dominio nella RAM (se spendo l'apparato teoricamente dovrebbe perdere le VLAN, ma dai test che ho effettuato su packet-tracer 7 non è così, mi riservo di provare su switch veri).
- Deve essere configurato come client VTP (ossia non è un'impostazione di default)

Transparent.
- Non partecipa a VTP tranne che per inoltrare annunci VTP a client VTP e server VTP
- Le VLAN create, rinominate o eliminate su switch trasparenti sono locali solo per tale switch
- Deve essere configurato come VTP trasparente (ossia non è un'impostazione di default)

VTP Question	VTP Server	VTP Client	VTP Transparent
What are the differences?	• Manages domain and VLAN configuration. • Multiple VTP servers can be configured.	• Updates local VTP configurations. • VTP client switches cannot change VLAN configurations.	• Manages local VLAN configurations. • VLAN configurations are not shared with VTP network.
Does it respond to VTP advertisements?	Participates fully	Participates fully	Only forwards VTP advertisements
Is the global VLAN configuration preserved on restart?	Yes, global configurations are stored in NVRAM	No, global configurations are stored in RAM only	No, local VLAN configuration is only stored in NVRAM
Does it update other VTP-enabled switches?	Yes	Yes	No

La tabella accanto riassume i punti sopra descritti

VTP Advertisements – Vi sono 3 tipi di advertisements (invio di segnali di comunicazione):



- Summary advertisements: informano gli switch adiacenti del nome del dominio VTP e del numero di revisione della configurazione;
- Advertisement request: risposta a un messaggio summary advertisement, quando il summary advertisement contiene un numero di revisione della configurazione più alto del valore corrente;
- Subset advertisements: contengono informazioni sulla VLAN incluse l'eventuali modifiche;

Per impostazione predefinita, CISCO scambia i summary advertisements ogni cinque minuti.
I summary advertisements, informano gli switch VTP adiacenti del nome di dominio VTP corrente e il numero di revisione della configurazione.
Il numero di revisione della configurazione è un numero a 32 bit che indica il livello di revisione per un pacchetto VTP. Ogni dispositivo VTP tiene traccia del numero di revisione della configurazione VTP che gli viene assegnato.
Questa informazione viene utilizzata per determinare se le informazioni ricevute sono più recenti rispetto alla versione corrente. Ogni volta che si modifica una VLAN in un dispositivo VTP server, la revisione della configurazione viene incrementata di uno.
COME FUNZIONA:
Quando lo switch riceve un pacchetto di summary advertisements, lo switch confronta il nome del dominio VTP con il proprio nome di dominio VTP. Se il nome è diverso, lo switch semplicemente ignora il pacchetto. Se il nome è lo stesso, ed eventualmente la password VTP è la stessa (nel caso sia configurata) lo switch confronta la revisione della configurazione con la sua revisione. Se il proprio numero di revisione della configurazione è superiore o uguale al numero di revisione della configurazione del pacchetto, il pacchetto viene ignorato. Se il proprio numero di revisione della configurazione è inferiore, viene inviata una richiesta di annuncio (advertisement request) che richiede il messaggio di annuncio secondario (subset advertisements).
Del VTP esistono 3 versioni riassunte in tabella (VTP v3 esula da questo corso)

VTP Version	Definition
VTP Version 1	• Default VTP mode on all switches. • Supports normal range VLANs only.
VTP Version 2	• Supports normal range VLANs only. • Supports legacy Token Ring networks. • Supports advanced features including unrecognized Type-Length-Value (TLV), version-dependent transparent mode, and consistency checks.

In uno switch appena montato senza alcuna configurazione effettuata, dando il comando (da privilege exec)
show vtp status
possiamo vedere i parametri VTP di configurazione base standard, ossia:
VTP Version Running: **1**
VTP Domain Name: ← il valore è NULL e quindi lo switch si aggancia al primo dominio che rileverà senza password
VTP Pruning Mode: Disabled ← Pruning (potatura), non propaga le VLAN se non servono (quindi limita i broadcast domain)
VTP Trap Generation: Disabled ← Trap, se abilitato invia un messaggio snmp sulla rete ad ogni evento VTP generato
Device ID ← Device MAC Address
Configuration last modified by 0.0.0.0 at 20-12-2017 00:03:00
VTP Operation mode: **Server**
Maximum VLANs Supported Locally: 255
Number of Existing VLANs: **5** ← la VLAN default e le VLAN (da 1002 a 1005)
Configuration Revision: **0**

NNB: best practice, per evitare di rischiare di avere problemi nell'aggiunta di uno switch alla rete esistente, prima di collegarlo alla rete assicurarsi che abbia una configurazione di default magari effettuando un reset del device con relativa cancellazione delle VLAN
delete flash:vlan

Procedura di configurazione VTP (da configuration terminal):

- Configurare il server VTP
  vtp mode server
- Configurare il nome dominio e la password VTP
  vtp domain CCNA
  vtp password passwordMIA123
  Per visualizzare la password VTP: **show vtp password** (in privileged exec)
- Configurare i client VTP
  vtp mode client
  vtp domain CCNA
  vtp password passwordMIA123
- Configurare le VLAN sul server VTP
  vlan 10
  name SISTEMISTI
  vlan 20
  name SVILUPPATORI
  vlan 30
  name AMMINISTRAZIONE
  NB: ho apportato 6 modifiche alle VLAN per cui la revision avrà valore 6
- Verificare che i client VTP abbiano ricevuto le nuove informazioni VLAN
  show vlan brief
- Abilitare vtp pruning → set vtp pruning 1-20 (i numeri in fondo indicano le vlan che partecipano)
  vtp pruning
- Abilitare vtp trap
  snmp-server enable traps vtp

Per quanto riguarda le extended VLAN abbiamo che:

1) Hanno un identificativo dal 1006 al 4094
2) Le configurazioni non sono scritte nel file vlan.dat
3) Non sono propagabili con il VTP
4) Supportano un numero minore di funzionalità rispetto alle VLAN a intervallo normale
5) Sono, per impostazione predefinita, salvati nel file di configurazione in esecuzione

NB: 4096 è il limite superiore per il numero di VLAN disponibili sugli switch Catalyst, perché ci sono 12 bit nel campo ID VLAN dell'intestazione IEEE 802.1Q
Ripassiamo la creazione delle VLAN sempre a partire dalla configuration terminal:
vlan 10
name SISTEMISTI
Creiamone per intervalli vari
vlan 10,20,30 ← creiamo le vlan 10, 20, 30
vlan 100-105 ← creiamo le vlan 100, 101, 102, 103, 104, 105
Assegnazione delle VLAN alle porte dello switch:
interface g0/0
switchport mode access
switchport access vlan 10
Per avere informazioni su una determinata VLAN
show vlan name SISTEMISTI

Configurare le extended VLAN
vtp mode transparent
vlan 2000

Il DTP (Dynamic Trunking Protocol) è un protocollo di proprietà di CISCO che opera solo punto-punto sugli switch per decidere dinamicamente (default) come attivare le porte tra gli switch se non diversamente configurato.
DTP gestisce la negoziazione del trunk solo se la porta sullo switch vicino è configurata in una modalità trunk che supporta DTP.
Per abilitare il trunking da uno switch Cisco a un dispositivo che non supporta DTP, utilizzare i comandi della modalità di configurazione dell'interfaccia
switchport mode trunk e **switchport nonegotiate**

Le interfacce Ethernet sugli switch Catalyst supportano diverse modalità di trunk con l'aiuto di DTP:

- switchport mode access: imposta l'interfaccia in modalità permanente non di negoziazione e negozia per convertire il collegamento in un collegamento non-trunk
- switchport mode dynamic auto: rende l'interfaccia in grado di convertire il collegamento in un collegamento trunk. L'interfaccia diventa un'interfaccia trunk se l'interfaccia adiacente è impostata su trunk o su mode dynamic desirable
- switchport mode dynamic desirable: Fa in modo che l'interfaccia tenti attivamente a convertire il collegamento in un collegamento trunk. L'interfaccia diventa un'interfaccia trunk se l'interfaccia adiacente è impostata su trunk, o su mode dynamic desirable, o mode dynamic auto
- switchport mode trunk: Mette l'interfaccia in modalità trunking permanente e negozia per convertire il collegamento adiacente in un collegamento trunk. L'interfaccia diventa un'interfaccia trunk anche se l'interfaccia adiacente non è un'interfaccia trunk
- switchport nonegotiate: Impedisce all'interfaccia di generare frame DTP. È possibile utilizzare questo comando solo quando la modalità di switchport dell'interfaccia è access o trunk. È necessario configurare manualmente l'interfaccia adiacente come interfaccia trunk per stabilire un collegamento trunk

La tabella riassume quanto appena descritto:

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	
Access	Access	Access		Access

NB: quando possibile è sempre meglio impostare manualmente l'interfaccia trunk tra gli switch manualmente impostando la modalità nonegotiate

2.1.4.4 Packet Tracer - Configure VLANs, VTP, and DTP.pdf
2.1.4.4 Packet Tracer - Configure VLANs, VTP, and DTP.pka
2.1.4.5 Lab - Configure Extended VLANs, VTP, and DTP.pdf

Per sapere la modalità in cui si trova una determinata interfaccia
show interface fa0/16 switchport

2.2.2.4 Packet Tracer - Troubleshooting Inter-VLAN Routing.pdf
2.2.2.4 Packet Tracer - Troubleshooting Inter-VLAN Routing.pka
2.2.2.5 Lab - Troubleshooting Inter-VLAN Routing.pdf

Attenzione ai problemi che potrebbero verificarsi nella configurazione del VTP tra gli switch:

a) Incompatibilità delle versioni;
b) VTP password sbagliata
c) Dominio VTP sbagliato o differente
d) Tutti gli switch impostati in Client Mode
e) Revision Number sbagliato

Problemi sul DPS:

A. Differenza di configurazione sulle porte collegate (una in trunk e una in access)
B. VLAN con configurata sul trunk
C. VLAN native differenti configurate sulla porta trunk di collegamento

2.2.3.3 Packet Tracer - Troubleshoot VTP and DTP.pdf
2.2.3.3 Packet Tracer - Troubleshoot VTP and DTP.pka

Tutti gli switch multistrato Catalyst supportano i seguenti tipi di interfacce Layer 3:

- Router port: è una pura interfaccia L3 simile a un'interfaccia fisica su un router Cisco IOS
- Switch virtual interface (SVI): una per ogni VLAN configurata, e viene utilizzata per l'inter-vlan routing. Ossia sono le interfacce VLAN con routing virtuale

2.3.1.5 Packet Tracer - Configure Layer 3 Switching and inter-VLAN Routing.pdf
2.3.1.5 Packet Tracer - Configure Layer 3 Switching and inter-VLAN Routing.pka

Per risolvere I problemi dell'inter-vlan routing bisogna fare attenzione ai seguenti punti:

- Le VLAN devono essere definite su tutti gli switch. Le VLAN devono essere abilitate sulle porte trunk. Le porte devono essere nelle VLAN corrette
- Gli SVI devono avere l'indirizzo IP o la subnet mask corretti. Gli SVI devono essere attivi. Ogni SVI deve corrispondere al numero VLAN appropriato
- I l routing deve essere abilitato. Ogni interfaccia o rete deve essere aggiunta al protocollo di routing o alle route statiche immesse, se necessario
- Gli host devono avere l'indirizzo IP o la subnet mask corretti. Gli host devono avere un gateway predefinito associato a una SVI o una porta indirizzata

Negli switch L3 per abilitare la funzione di routing devo dare il comando
ip routing

FINE CAPITOLO 2

3.0.1.2 Class Activity - Stormy Traffic.pdf

La ridondanza in una LAN anche a livello di accesso è bene realizzarla, ma la ridondanza genera LOOP che bisogna gestire.
I Loop possono essere su 2 livelli:

- Layer3: hanno un elevato consumo di banda, ma hanno la fortuna di avere un TTL, quindi dopo “un po' di loop” all’interno della rete i pacchetti vengono “droppati”
- Layer2: ossia loop all’interno del Broadcast Domain, dove il loop è generato dai frame in un loop infinito generando:
  - Broadcast storm: si verifica quando ci sono così tanti frame di trasmissione catturati in un loop Layer 2 che tutta la larghezza di banda disponibile viene consumata. Di conseguenza, non è disponibile larghezza di banda per il traffico legittimo e la rete non è più disponibile per la comunicazione dei dati. Questo è un efficace DoS. Ciò può causare il malfunzionamento del dispositivo finale a causa dei requisiti di elaborazione necessari per sostenere un carico di traffico così elevato sulla scheda NIC;
  - Duplicated frame: i frame di trasmissione non sono l'unico tipo di frame interessati dai loop. I frame unicast sconosciuti inviati su una rete in loop possono generare frame duplicati in arrivo sul dispositivo di destinazione. Un frame unicast sconosciuto è quando lo switch non ha l'indirizzo MAC di destinazione nella sua tabella degli indirizzi MAC e deve inoltrare il frame a tutte le porte, ad eccezione della porta di ingresso;
  - MAC table flapping: I frame Ethernet non hanno un attributo time to live (TTL). Di conseguenza, se non è abilitato alcun meccanismo per bloccare la propagazione continua di questi frame su una rete, continuano a propagarsi tra gli switch all'infinito, o fino a quando un collegamento non viene interrotto e interrompe il ciclo; I frame di trasmissione vengono inoltrati a tutte le porte dello switch, ad eccezione della porta di ingresso originale. Ciò garantisce che tutti i dispositivi di un dominio di broadcast possano ricevere il frame. Se è presente più di un percorso per il frame da inoltrare, può verificarsi un loop infinito. Quando si verifica un loop, è possibile che la tabella degli indirizzi MAC su uno switch cambi costantemente con gli aggiornamenti dai frame di trasmissione, il che risulta nell'instabilità del database MAC

3.1.1.5 Packet Tracer - Examining a Redundant Design Instructions.pdf
3.1.1.5 Packet Tracer - Examining a Redundant Design.pka

Per ovviare al problema dei loop sul Layer2 è stato introdotto lo Spanning Tree Protocol (STP), protocollo IEEE 802.1D. (Attenzione che la documentazione ufficiale 802-1D-2004 si riferisce con il termine STP al Rapid Spanning Tree Protocol, quello che noi in questi appunti definiremo RSTP)
STP garantisce che vi sia un solo percorso logico tra tutte le destinazioni sulla rete bloccando intenzionalmente percorsi ridondanti che potrebbero causare un loop. Una porta viene considerata bloccata quando viene impedito l'ingresso o l'uscita di tale porta da parte dei dati utente.
Ossia tutte le volte che lui rileva un loop lo blocca in base a calcoli deterministici.
Gli switch che eseguono STP sono in grado di compensare i guasti sbloccando dinamicamente le porte precedentemente bloccate e consentendo al traffico di attraversare i percorsi alternativi.

STP e RSTP utilizzano lo Spanning Tree Algorithm (STA), per determinare quali porte degli switch su una rete devono essere messe in stato di blocco per impedire il verificarsi di loop.

Introduciamo quindi BPDU, che è il frame di servizio dello STA

Step dello Spanning Tree Algorithm

1) Viene identificato il Route bridge: è lo switch con tutte le interfacce attive (cioè non disabilitate) e l'elezione di tale switch è definito dal bridge ID [BID] (contenuto nel BPDU) definito da un parametro detto Bridge Priority e dal MAC e l'elezione la vince chi ha il bridge ID più basso. Ogni switch appena avviato invia agli apparati limitrofi un BPDU ogni 2 secondi, nel quale indica secondo lui qual è il route bridge. Naturalmente appena acceso non avendo nessun BPDU di altro apparato, si auto proclama route bridge. Alla fine, gli switch a forza di scambiare BPDU, concordano su un bridge root. L'elezione non è mai finita, perché nel momento in cui aggiungo un altro switch riparte l'identificazione del route bridge.
   Il BID è costituito da un numero di priorità del bridge configurabile e un indirizzo MAC. La priorità del bridge è un valore compreso tra 0 e 65.535. Il valore predefinito è 32.768, al quale bisogna aggiungere il valore della VLAN di riferimento. Se due o più switch hanno la stessa priorità, lo switch con l'indirizzo MAC più basso diventerà il root bridge.
2) Quando il root bridge è stato scelto per l'istanza dello spanning tree, lo STA avvia il processo di determinazione dei migliori percorsi per il bridge root da tutte le destinazioni nel dominio broadcast. L'informazione sul percorso, nota come costo del percorso root interno, è determinata sommando i costi delle singole porte lungo il percorso dal passaggio al bridge root. Questo è il costo del percorso dallo switch d'invio al root bridge. Tale informazione è sempre contenuta nel BPDU.

Link Speed	Cost
10 Gb/s	2
1 Gb/s	4
100 Mb/s	19
10 Mb/s	100

Sebbene le porte dello switch abbiano un costo di porta predefinito associato, il costo della porta è configurabile. La possibilità di configurare i singoli costi delle porte offre all'amministratore la possibilità di controllare manualmente i percorsi STP verso il route bridge.

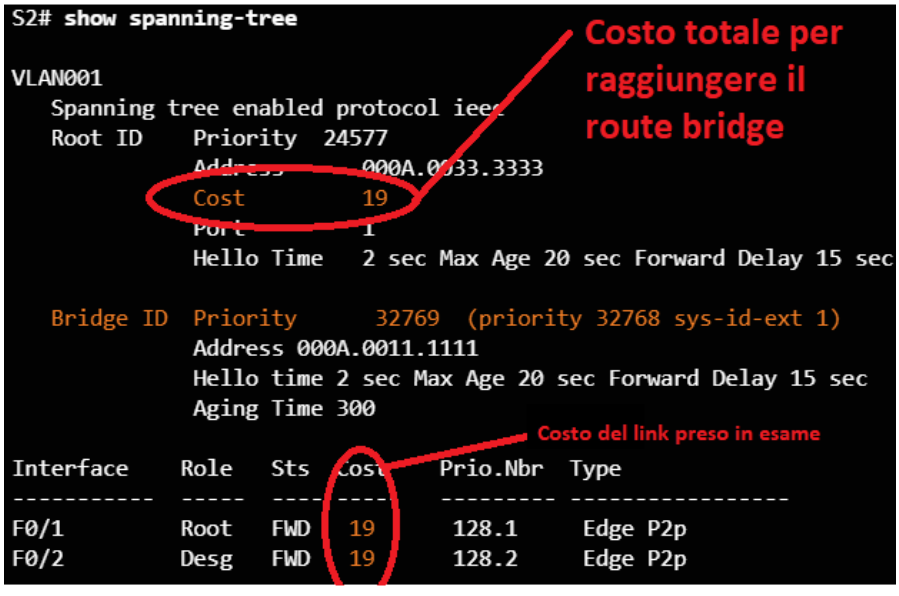
interface f0/1
spanning-tree cost 25
end

Oppure per resettare un path cost precedentemente aggiunto

interface f0/1
no spanning-tree cost
end

Per avere info sullo STP

show spanning-tree



3) Port status (protocollo PVST+): negli switch le porte possono essere messe in:
    a. Forwarding: inviano e ricevono tutti i frame (tutte le interfacce del route bridge lo sono)
    b. Learning: processa solo i frame di data in ingresso mentre processa i BPDU in ingresso e uscita
    c. Listening: non processa il frame di data (né in ingresso, né in uscita) e processa i BPDU in ingresso e uscita
    d. Blocking: non processa il frame di data (né in ingresso, né in uscita) e accetta solo BPDU in ingresso

    Il funzionamento è il seguente, se ho un loop, da Forwarding passo in Blocking, poi se necessario passo in Listening e se c'è un loop ripasso in Blocking se non c'è passo in Learning, ed anche qui rimango un po' in ascolto per creare una MAC table e non tempestare la rete di MAC unknown, poi passo in Forwarding, nel momento in cui il link principale torna up io torno in Blocking.
    Il tempo tra Blocking e Listening ed il tempo tra Listening e Learning è di 15 secondi. Se la nostra rete è composta da una distanza massima di circa 7 hop (ossia deve attraversare 7 switch come distanza massima) non tocchiamo il timer, altrimenti se è molto inferiore o superiore possiamo modificare il timer.

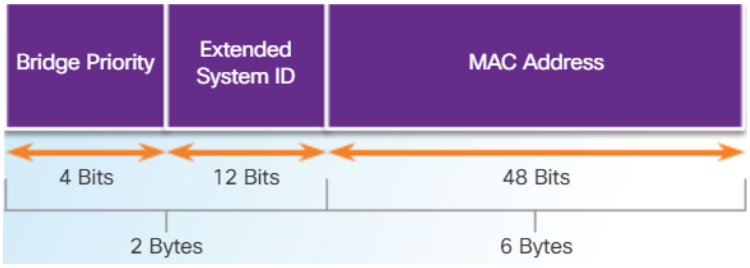
3a) Ogni switch è tenuto ad identificare le sue porte più vicine al route bridge e metterle in Forwarding (minimo 1 porta) e la identifica attraverso il path cost che è il valore numerico cumulativo di tutti i costi relativi ai link che la BPDU ha percorso per arrivare a me. Vince il costo più basso.

4) Nelle porte che non sono route port all'interno del loop identificato, si ha, che ogni porta che interessa il loop invia il proprio BPDU e confrontano il path cost con quello del vicino. Quello che ha il path cost più basso metterà la propria porta Designed in Forwarding e l'altro switch metterà la sua porta Assigned in Blocking. A parità di path cost si guarda il BID e quello con il bridge ID più basso va in frowarding e l'altra in Blocking
    La porta Designed è la porta che invia e riceve il traffico da e verso quel link al route bridge. Questa è la porta migliore su quel segmento verso il root bridge. La porta alternativa non invierà o riceverà traffico su quel segmento.

Un frame BPDU contiene 12 campi distinti che trasmettono il percorso e le informazioni prioritarie utilizzate per determinare il root bridge e i percorsi del root bridge.
I primi quattro campi identificano il protocollo, la versione, il tipo di messaggio e gli indicatori di stato. I successivi quattro campi vengono utilizzati per identificare il root bridge e il costo del percorso root per il root bridge. Gli ultimi quattro campi sono tutti campi timer che determinano la frequenza con cui vengono inviati i messaggi BPDU e la durata di conservazione delle informazioni ricevute tramite il processo BPDU.

Ogni VLAN ha il suo Spanning Tree.

Il Bridge ID (BID) contiene:



- ✓ Priority Bridge (4bit): è un valore personalizzabile che può essere utilizzato per influenzare quale switch diventa il root bridge. Lo switch con la priorità più bassa, che implica il BID più basso, diventa il root bridge perché un valore di priorità inferiore ha la precedenza.
- ✓ Extended ID (12 bit): Le informazioni sulla VLAN sono incluse in questo ID. Riserva i 12 bit per la configurazione, questo spiega perché il valore di priorità del bridge può essere configurato solo in multipli di 4096 (2^{12}). Il valore dell'Extended ID è un valore decimale aggiunto al valore di priorità del bridge nel BID per identificare la priorità e la VLAN del frame BPDU di riferimento.
- ✓ MAC Address: quando due switch sono configurati con la stessa Priority Bridge e lo stesso Extended ID, lo switch con l'indirizzo MAC con il valore più basso, espresso in esadecimale, avrà il BID inferiore.

3.1.2.12 Lab - Building a Switched Network with Redundant Links.pdf

Vi sono vari tipi di Spanning Tree Protocol:

- STP: questa è la versione originale IEEE 802.1D. Common Spanning Tree (CST) presuppone un'istanza dello spanning tree per l'intera rete a ponte, indipendentemente dal numero di VLAN.
- PVST+: questo è un miglioramento Cisco di STP che fornisce un'istanza dello spanning tree 802.1D separata per ciascuna VLAN configurata nella rete. CISCO di default utilizza il protocollo PVST+
- 802.1D-2004: questa è una versione aggiornata dello standard STP, che incorpora IEEE 802.1w (RSTP)
- Rapid Spanning Tree Protocol (RSTP): questa è un'evoluzione dell'STP che fornisce una maggiore velocità rispetto all'STP
- Rapid PVST+: questo è un miglioramento Cisco di RSTP che utilizza PVST+. Rapid PVST + fornisce un'istanza separata di 802.1w per VLAN
- MSTP (Multiple Spanning Tree Protocol): si tratta di uno standard IEEE ispirato alla precedente implementazione STP (Multiple Instance STP) proprietaria di Cisco. MSTP mappa più VLAN nella stessa istanza dello Spanning Tree. L'implementazione Cisco di MSTP è MST, che fornisce fino a 16 istanze di RSTP e combina molte VLAN con la stessa topologia fisica e logica in un'istanza RSTP comune.

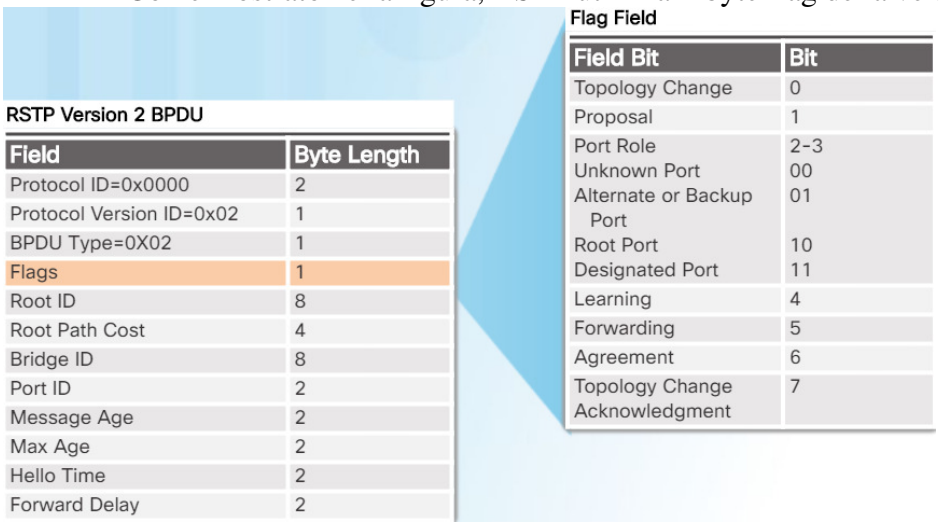
TABELLA RIASSUNTIVA STANDARD/RISORSE

Protocol	Standard	Resources Needed	Convergence	Tree Calculation
STP	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
Rapid PVST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s, Cisco	Medium or high	Fast	Per Instance

Le reti che eseguono PVST + hanno queste caratteristiche:

- ✓ Possono gestire un bilanciamento ottimale del carico;
- ✓ Un'istanza dello Spanning Tree per ciascuna VLAN gestita, può comportare un notevole spreco di cicli della CPU per tutti gli switch della rete. Ciò sarà solo problematico se viene configurato un numero elevato di VLAN.

Come mostrato nella figura, RSTP utilizza il byte flag della versione 2 BPDU:



RSTP Version 2 BPDU

Field	Byte Length
Protocol ID=0x0000	2
Protocol Version ID=0x02	1
BPDU Type=0X02	1
Flags	1
Root ID	8
Root Path Cost	4
Bridge ID	8
Port ID	2
Message Age	2
Max Age	2
Hello Time	2
Forward Delay	2

Flag Field

Field Bit	Bit
Topology Change	0
Proposal	1
Port Role Unknown Port Alternate or Backup Port Root Port Designated Port	2-3 00 01 10 11
Learning	4
Forwarding	5
Agreement	6
Topology Change Acknowledgment	7

- I bit 0 e 7 vengono utilizzati per il cambio e il riconoscimento della topologia. Sono nell'802.1D originale.
- I bit 1 e 6 sono utilizzati per il processo del contratto di proposta (utilizzato per la convergenza rapida).
- I bit da 2 a 5 codificano il ruolo e lo stato della porta.
- I bit 4 e 5 sono usati per codificare il ruolo della porta usando un codice a 2 bit.

Una porta Edge RSTP è una porta switch che non è mai stata progettata per essere collegata a un altro switch. Passa immediatamente allo stato di Forwarding quando abilitato.
Il concetto di Edge Port RSTP corrisponde alla funzione PVST+ PortFast. Una porta Edge è direttamente collegata a una stazione finale e presuppone che nessun dispositivo switch sia collegato ad esso.

```
interface f0/1
spanning-tree portfast
end
```

A seconda di ciò che è collegato a ciascuna porta, è possibile identificare due diversi tipi di collegamento:

- Point-to-Point: una porta che opera in modalità full-duplex generalmente connette uno switch ad un'altro switch ed è un candidato per una transizione rapida verso uno stato di Forwarding.
- Shared: una porta che opera in modalità half-duplex connette uno switch a un hub che collega più dispositivi.

Il tipo di collegamento può determinare se la porta può immediatamente passare a uno stato di Forwarding, presupponendo che vengano soddisfatte determinate condizioni. Queste condizioni sono diverse per le porte Edge e non-Edge. Le porte non Edge sono classificate in due tipi di collegamento: Point-to-Point e Shared. Il tipo di collegamento viene determinato automaticamente, ma può essere sovrascritto con i comandi

```
spanning-tree point-to-point
```

oppure

```
spanning-tree shared
```

Le connessioni della porta Edge e le connessioni Point-to-Point sono candidate per la transizione rapida a uno stato di Forwarding. Tuttavia, prima di considerare il link type, RSTP deve determinare il ruolo della porta. Le porte di root sono in grado di effettuare una transizione rapida allo stato di Forwarding non appena la porta è sincronizzata (riceve una BPDU dal root bridge). Una transizione rapida allo stato di Forwarding per la porta Designed si verifica solo se il link type è impostato su Point-to-Pint.

Configurare e verificare il Route Bridge
Per impostare uno switch come Route Bridge, lo si può fare in 2 modi:

1) **spanning-tree vlan 1 root primary**
   end
   La priorità per lo switch è impostata sul valore predefinito di 24.576 o sul multiplo più alto di 4.096, inferiore alla priorità bridge più bassa rilevata sulla rete.
   Se si desidera un bridge root alternativo, utilizzare il comando:
   spanning-tree vlan 1 root secondary
   end
   Questo comando imposta la priorità per lo switch sul valore predefinito di 28.672. Ciò garantisce che lo switch alternativo diventi il root bridge se fallisce il root bridge primario. Ciò presuppone che il resto degli switch nella rete abbia il valore di priorità predefinito pari a 32.768
2) **spanning-tree vlan 1 priority 24576**
   end
   NB: il valore dopo priority dev'essere un multiplo di 4096

PortFast è una funzionalità Cisco per gli ambienti PVST+. Quando una porta switch è configurata con PortFast, la porta passa immediatamente dallo stato di Blocking a quello di Forwarding, ignorando i consueti stati di transizione STP 802.1D. In una configurazione PortFast valida, i BPDU non dovrebbero mai essere ricevuti, poiché ciò indicherebbe che un altro bridge o switch è connesso alla porta, causando potenzialmente un loop Spanning Tree. Gli switch Cisco supportano una funzionalità chiamata protezione BPDU. Quando è abilitato, la protezione BPDU pone la porta in uno stato errdisabilitato (disabilitato) alla ricezione di una BPDU. Questo spegnerà la porta dello switch e sarà necessario riattivare manualmente l'interfaccia.

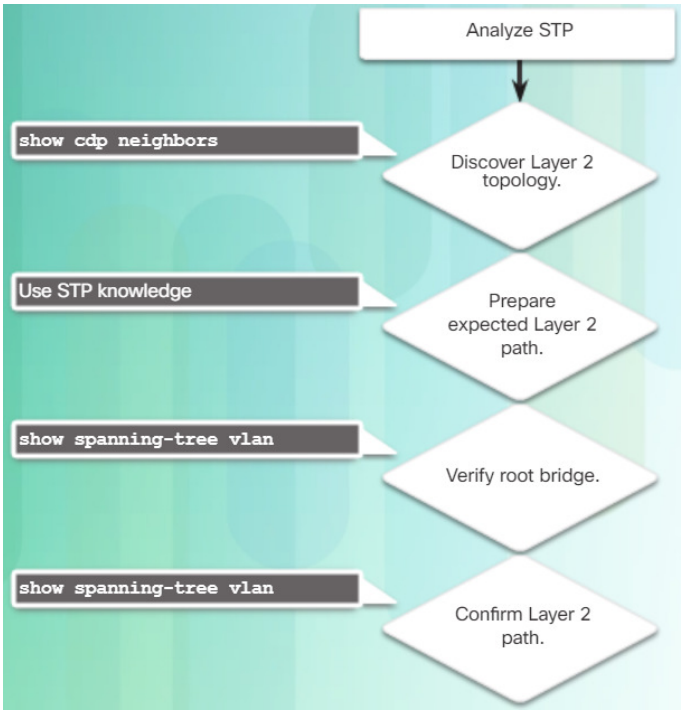
Per attivare il BPDU Guard
interface f0/1
spanning-tree portfast
spanning-tree bpduguard enable
end

3.3.1.5 Packet Tracer - Configuring PVST.pdf
3.3.1.5 Packet Tracer - Configuring PVST.pka

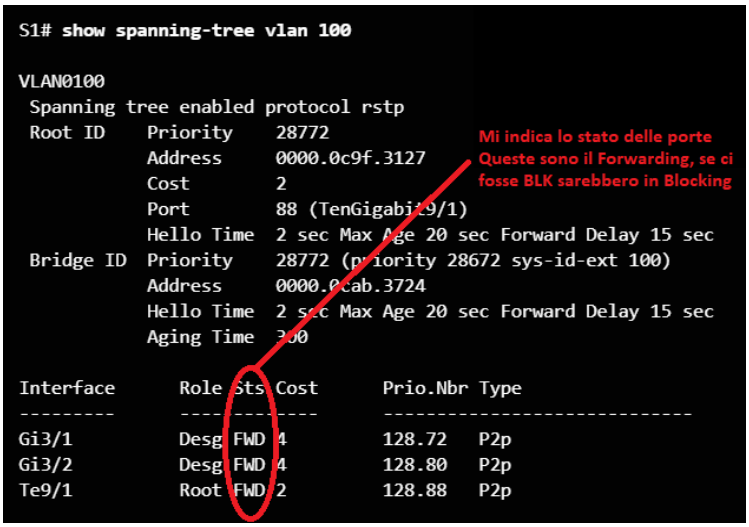
configure terminal
spanning-tree mode rapid-pvst
interface g0/1
spanning-tree link-type point-to-point
end
clear spanning-tree detected-protocol

3.3.2.2 Packet Tracer - Configuring Rapid PVST.pdf
3.3.2.2 Packet Tracer - Configuring Rapid PVST.pka
3.3.2.3 Lab - Configuring Rapid PVST, PortFast, and BPDU Guard.pdf

La figura accanto indica gli step necessari ed i relativi comandi per verificare lo Spanning Tree Protocol all'interno degli switch



Attenzione anche a leggere l'output di
show spanning-tree vlan 1



3.4.1.1 Class Activity - Documentation Tree.pdf

FINE CAPITOLO 3

4.0.1.2 Class Activity - Imagine This.pdf

L'aggregazione di link, server per consentire il passaggio di dati tra più switch attraverso più link, ma per configurazione predefinita, tra gli switch Layer2 è presente ed attivo l'STP (Spanning Tree Protocol) che inibisce più collegamenti. Per questo motivo per poter avere la configurazione precedentemente descritta bisogna implementare una configurazione EtherChannel
L'EtherChannel, quando viene configurata, risulta essere una porta virtuale detta "channel port" e le porte fisiche che ne fanno parte sono raggruppate sotto di essa.

La configurazione dell'EtherChannel ha molti vantaggi, come:

- La maggior parte delle attività di configurazione può essere eseguita direttamente sull'interfaccia EtherChannel (con relativa propagazione automatica alle porte che ne fanno parte).
- EtherChannel si basa su porte switch esistenti. Non è necessario aggiornare il collegamento a una connessione più veloce e più costosa per avere più larghezza di banda.
- Il bilanciamento del carico avviene tra i link che fanno parte dello stesso EtherChannel. Questi metodi includono il MAC di origine al bilanciamento del carico MAC di destinazione o l'IP di origine al bilanciamento del carico IP di destinazione, attraverso i collegamenti fisici.
- EtherChannel crea un'aggregazione che è vista come un collegamento logico. Quando esistono più bundle EtherChannel tra due switch, STP può bloccare uno dei bundle per impedire loop di commutazione. Quando STP blocca uno dei collegamenti ridondanti, blocca l'intero EtherChannel. Questo blocca tutte le porte che appartengono al collegamento EtherChannel. Dove esiste un solo collegamento EtherChannel, tutti i collegamenti fisici nell'EtherChannel sono attivi perché STP vede solo un collegamento logico.
- EtherChannel fornisce ridondanza perché il collegamento generale è visto come una connessione logica. Inoltre, la perdita di un collegamento fisico all'interno del canale non crea un cambiamento nella topologia; pertanto non è richiesto un ricalcolo dello Spanning Tree.

Limitazioni EtherChannel:

- ✓ Le interfacce devono essere omogenee: Fast Ethernet, con Fast Ethernet, Gigabit Ethernet con Gigabit Ethernet, ecc…
- ✓ Ogni EtherChannel può contenere fino a massimo 8 porte Ethernet (attualmente gli switch CISCO massimo 6)

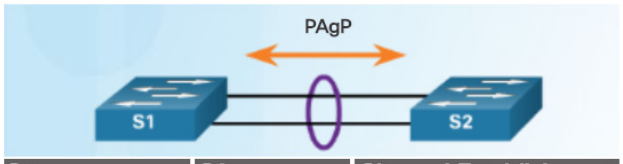
Attenzione che adesso anche i server supportano i protocolli EtherChannel, quindi potrebbe essere utile sfruttare l'opportunità fornita.

IMPORTANTISSIMO: la configurazione della porta del singolo membro del gruppo EtherChannel deve essere coerente su entrambi i dispositivi. Se le porte fisiche di un lato sono configurate come trunk, anche le porte fisiche dell'altro lato devono essere configurate come trunk all'interno della stessa VLAN nativa. Inoltre, tutte le porte in ciascun collegamento EtherChannel devono essere configurate come porte Layer 2.

Un EtherChannel Layer3 ha un singolo indirizzo IP associato all'aggregazione logica delle porte switch nell'EtherChannel, ossia (ogni channel port ha il suo ip).

L'EtherChannel può essere realizzato utilizzando uno dei seguenti protocolli:

- PAgP (pronuncia pag-p): il Port Aggregation Protocol, è un protocollo proprietario CISCO, che aiuta nella creazione automatica di collegamenti EtherChannel. Quando un collegamento EtherChannel viene configurato utilizzando PAgP, i pacchetti PAgP vengono inviati tra le porte che supportano EtherChannel per negoziare la formazione di un canale. Quando PAgP identifica i collegamenti Ethernet corrispondenti, raggruppa i collegamenti in EtherChannel. EtherChannel viene quindi aggiunto allo Spanning Tree come singola porta. I pacchetti PAgP vengono inviati ogni 30 secondi. PAgP verifica la coerenza della configurazione e gestisce le aggiunte e gli errori dei collegamenti tra due switch. Assicura che quando viene creato un EtherChannel, tutte le porte abbiano lo stesso tipo di configurazione.
  Nota: in EtherChannel, è obbligatorio che tutte le porte abbiano la stessa velocità, impostazione duplex e informazioni VLAN. Qualsiasi modifica della porta dopo la creazione del canale cambia anche tutte le altre porte del canale.
  Le porte fisiche degli switch rispetto al protocollo PAgP possono essere impostate in modo:

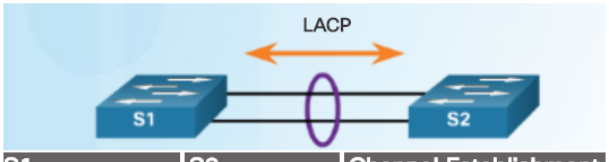


S1	S2	Channel Establishment
On	On	Yes
Auto/Desirable	Desirable	Yes
On/Auto/Desirable	Not Configured	No
On	Desirable	No
Auto/On	Auto	No

  - On: forza l'interfaccia al canale senza PAgP e non scambiano i pacchetti PAgP. Modalità passiva
  - Desirable: pone un'interfaccia in uno stato di negoziazione attivo in cui l'interfaccia avvia le negoziazioni con altre interfacce inviando pacchetti PAgP. Modalità attiva
  - Auto: pone un'interfaccia in uno stato di negoziazione passivo in cui l'interfaccia risponde ai pacchetti PAgP che riceve, ma non avvia la negoziazione PAgP. Modalità passiva

  Le modalità devono essere compatibili su ciascun lato. Se tutte le modalità sono disabilitate usando il comando no, o se nessuna modalità è configurata, EtherChannel è disabilitato.

- LACP: il Link Aggregation Control Protocol, fa parte di una specifica IEEE (802.3ad) che consente di raggruppare più porte fisiche per formare un port channel. Esegue una funzione simile a PAgP con Cisco EtherChannel. Poiché LACP è uno standard IEEE, può essere utilizzato per facilitare EtherChannel in ambienti multivendor.
  Nota: LACP è stato originariamente definito come IEEE 802.3ad. Tuttavia, LACP è ora definito nel nuovo standard IEEE 802.1AX per le reti locali e metropolitane.
  LACP offre gli stessi vantaggi di negoziazione di PAgP.
  Le porte fisiche degli switch rispetto al protocollo LACP possono essere impostate in modo:



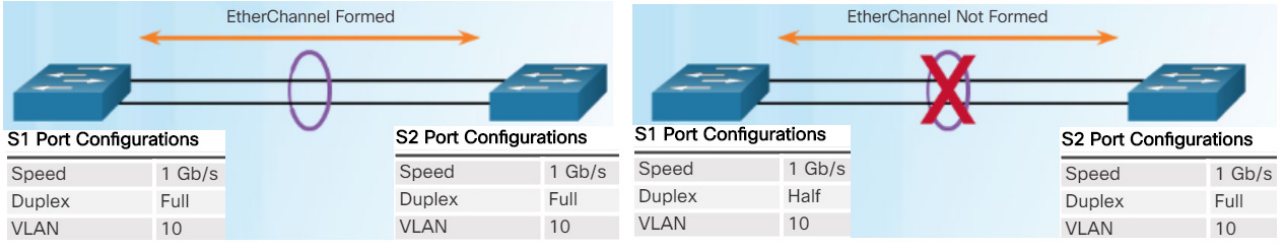
S1	S2	Channel Establishment
On	On	Yes
Active/Passive	Active	Yes
On/Active/Passive	Not Configured	No
On	Active	No
Passive/On	Passive	No

  - On: forza l'interfaccia al canale senza LACP. Le interfacce configurate in modalità on non scambiano i pacchetti LACP.
  - Active: posiziona una porta in uno stato di negoziazione attivo. In questo stato, la porta avvia i negoziati con altre porte inviando pacchetti LACP.
  - Passive: pone una porta in uno stato di negoziazione passiva. In questo stato, la porta risponde ai pacchetti LACP che riceve, ma non avvia la negoziazione dei pacchetti LACP.

  Proprio come con PAgP, le modalità devono essere compatibili su entrambi i lati per consentire la creazione del collegamento EtherChannel.
  LACP consente otto collegamenti attivi e otto collegamenti standby. Un collegamento di standby diventerà attivo in caso di guasto di uno dei collegamenti attivi correnti.

Quindi ricapitolando per una corretta configurazione dell'EtherChannel, si deve avere:

- EtherChannel support: tutte le interfacce in gioco devono supportare il protocollo;
- Speed & Duplex: configurare tutte le interfacce in un EtherChannel per operare alla stessa velocità e nella stessa modalità duplex;
- VLAN match: tutte le interfacce nel pacchetto EtherChannel devono essere assegnate alla stessa VLAN o configurate come trunk ed avere la stessa VLAN nativa



ATTENZIONE ricordarsi che: apportare modifiche alla configurazione a un'interfaccia che fa parte di un collegamento EtherChannel può causare problemi di compatibilità dell'interfaccia.

Vediamo ora come configurare manualmente un EtherChannel:

interface range fa0/1 – 2 → prendo la fast ethernet 1 e 2
channel-group 1 mode active → quindi uso il protocollo LACP
interface port-channel 1 → inizio ad impostare la port-channel 1 che comprende fa0/1-2
switchport mode trunk
swithcport trunk allowed vlan 1,2,20

4.2.1.3 Packet Tracer - Configuring EtherChannel.pdf
4.2.1.3 Packet Tracer - Configuring EtherChannel.pka
4.2.1.4 Lab - Configuring EtherChannel.pdf

Comandi per visualizzare le impostazioni EtherChannel (anche per fare Trubleshooting):

show interface port-channel 1 → verifica lo stato dell'interfaccia
show etherchannel summary → mostra una linea riassuntiva per ogni channel-group attenzione allo stato delle porte tra parentesi
show etherchannel port-channel → mostra le informazioni di ogni channel-group
show interfaces f0/1 etherchannel → mostra le regole di un'interfaccia dell'etherchannel

4.2.2.3 Packet Tracer - Troubleshooting EtherChannel.pdf
4.2.2.3 Packet Tracer - Troubleshooting EtherChannel.pka
4.2.2.4 Lab - Troubleshooting EtherChannel.pdf

Se in una rete la navigazione tramite un gateway fallisce, bisogna studiare una metodologia per cui tutti i dispositivi e gli apparati di rete possano avere un gateway alternativo, ossia creando una ridondanza di routing, tramite la configurazione di un router virtuale. Per implementare questo tipo di ridondanza del router, più router sono configurati per lavorare insieme per presentare l'illusione di un singolo router agli host sulla LAN. L'indirizzo IPv4 del router virtuale è configurato come gateway predefinito per le workstation su un segmento IPv4 specifico. Quando i frame vengono inviati dai dispositivi host al gateway predefinito, gli host utilizzano ARP per risolvere l'indirizzo MAC associato all'indirizzo IPv4 del gateway predefinito. La risoluzione ARP restituisce l'indirizzo MAC del router virtuale. I frame inviati all'indirizzo MAC del router virtuale possono quindi essere elaborati fisicamente dal router attualmente attivo all'interno del gruppo di router virtuale. Il router fisico che inoltra questo traffico è trasparente per i dispositivi host.
La capacità di una rete di ripristinare in modo dinamico dall'errore di un dispositivo che agisce come gateway predefinito è nota come first-hop redundancy.

Ma come funziona il router failover in modo semplice?

1) Vi è un router attivo ed uno in standby (stabilito tra i router tramite appositi protocolli)
2) Il router attivo viene "bindato" al virtual router
3) Il router in standby smette di visualizzare i messaggi Hello dal router attivo
4) Il router di standby assume il ruolo del router attivo e viene "bindato" al router virtuale
5) Poiché il nuovo router attivo presuppone di possedere sia l'indirizzi IPv4 che il MAC del router virtuale, i dispositivi host non vedono alcuna interruzione del servizio

Tutto questo viene detto First Hop Redundancy Protocol (FHRP)

Le principali opzioni disponibili per FHRP sono:

1) Hot Standby Router Protocol (HSRP): proprietario di Cisco progettato per consentire il failover trasparente di un dispositivo IPv4 first-hop. HSRP viene utilizzato in un gruppo di router per la selezione di un dispositivo attivo e di un dispositivo di standby.
2) HSRP per IPv6: proprietario di Cisco che fornisce la stessa funzionalità di HSRP, ma in un ambiente IPv6. Un gruppo IPv6 HSRP ha un indirizzo MAC virtuale derivato dal numero del gruppo HSRP e un indirizzo IPv6 link locale virtuale derivato dall'indirizzo MAC virtuale HSRP. Gli annunci di router periodici (RA) vengono inviati per l'indirizzo locale IPv6 virtuale HSRP quando il gruppo HSRP è attivo. Quando il gruppo diventa inattivo questi RA si fermano dopo l'invio di un RA finale.
3) Virtual Router Redundancy Protocol versione 2 (VRRPv2): assegna dinamicamente la responsabilità di uno o più router virtuali ai router VRRP su una LAN IPv4. Ciò consente a più router su un collegamento multiaccess di utilizzare lo stesso indirizzo IPv4 virtuale. Un router VRRP è configurato per eseguire il protocollo VRRP in combinazione con uno o più router collegati a una LAN. In una configurazione VRRP, viene scelto un router come master del router virtuale, con gli altri router che fungono da backup, nel caso in cui il master del router virtuale non riesca.
4) VRRPv3: fornisce la capacità di supportare indirizzi IPv4 e IPv6. VRRPv3 funziona in ambienti multi-vendor ed è più scalabile di VRRPv2.
5) Gateway Load Balancing Protocol (GLBP): proprietario di Cisco che protegge il traffico dati da un router o circuito guasto, come HSRP e VRRP, consentendo anche il bilanciamento del carico (chiamato anche condivisione del carico) tra un gruppo di router ridondanti.
6) GLBP per IPv6: proprietario di Cisco che fornisce la stessa funzionalità di GLBP, ma in un ambiente IPv6. GLBP per IPv6 fornisce il backup automatico del router per gli host IPv6 configurati con un singolo gateway predefinito su una LAN. Più router first-hop sulla LAN si combinano per offrire un singolo router IPv6 virtuale first-hop condividendo il carico di inoltro dei pacchetti IPv6.
7) ICMP Router Discovery Protocol (IRDP): specificato in RFC 1256, è una soluzione FHRP legacy. IRDP consente agli host IPv4 di individuare router che forniscono connettività IPv4 ad altre reti IP (non locali).

La versione HSRP predefinita per Cisco IOS 15 è la versione 1. HSRP versione 2 fornisce i seguenti miglioramenti:

- HSRPv2 espande il numero di gruppi supportati. HSRP versione 1 supporta numeri di gruppo da 0 a 255. HSRP versione 2 supporta numeri di gruppo da 0 a 4095.
- HSRPv1 utilizza l'indirizzo multicast di 224.0.0.2. La versione 2 di HSRP utilizza l'indirizzo multicast IPv4 224.0.0.102 o l'indirizzo multicast IPv6 FF02 :: 66 per inviare i pacchetti hello.
- HSRPv1 utilizza l'intervallo di indirizzi MAC virtuale da 0000.0C07.AC00 a 0000.0C07.ACFF, dove le ultime due cifre esadecimali indicano il numero del gruppo HSRP. HSRPv2 utilizza l'intervallo di indirizzi MAC da 0000.0C9F.F000 a 0000.0C9F.FFFF per IPv4 e da 0005.73A0.0000 a 0005.73A0.0FFF per indirizzi IPv6. Sia per IPv4 che per IPv6, le ultime tre cifre esadecimali dell'indirizzo MAC indicano il numero del gruppo HSRP.
- HSRPv2 aggiunge il supporto per l'autenticazione MD5

HSRP:

- Il ruolo dei router attivi e in standby è determinato durante il processo elettorale HSRP. Per impostazione predefinita, il router con l'indirizzo IPv4 numericamente più alto viene eletto come router attivo. Tuttavia, è sempre meglio controllare il funzionamento della rete in condizioni normali piuttosto che lasciarlo al caso.
- La priorità HSRP può essere utilizzata per determinare il router attivo. Il router con la massima priorità HSRP diventerà il router attivo. Per impostazione predefinita, la priorità HSRP è 100. Se le priorità sono uguali, il router con l'indirizzo IPv4 numericamente più alto viene eletto come router attivo.
- Per configurare un router come router attivo, utilizzare il comando:
  standby priority
  L'intervallo della priorità HSRP è compreso tra 0 e 255.
- Per impostazione predefinita, dopo che un router è diventato il router attivo, rimarrà il router attivo anche se un altro router è in linea con una priorità HSRP più alta
- Per forzare un nuovo processo di elezione HSRP, è necessario abilitare il preemption utilizzando il comando:
  standby preempt
  La prelazione è la capacità di un router HSRP di attivare il processo di rielezione. Con la preventiva abilitata, un router che arriva online con una priorità HSRP più alta assumerà il ruolo del router attivo.
- Preemption consente solo a un router di diventare il router attivo se ha una priorità più alta. Un router abilitato per la prelazione, con uguale priorità ma un indirizzo IPv4 superiore non preverrà un router attivo.
- Se la Preemption è disattivata, il router che si avvia per primo diventerà il router attivo se non ci sono altri router online durante il processo di elezione.

Quando un'interfaccia è configurata con HSRP o viene prima attivata con una configurazione HSRP esistente, il router invia e riceve pacchetti hello HSRP per iniziare il processo di determinazione dello stato che assumerà nel gruppo HSRP. I router HSRP attivi e in standby inviano i pacchetti hello all'indirizzo multicast del gruppo HSRP ogni 3 secondi, per impostazione predefinita. Il router di standby diventerà attivo se non riceve un messaggio di hello dal router attivo dopo 10 secondi.

State	Definition
Initial	This state is entered through a configuration change or when an interface first becomes available.
Learn	The router has not determined the virtual IP address and has not yet seen a hello message from the active router. In this state, the router waits to hear from the active router.
Listen	The router knows the virtual IP address, but the router is neither the active router nor the standby router. It listens for hello messages from those routers.
Speak	The router sends periodic hello messages and actively participates in the election of the active and/or standby router.
Standby	The router is a candidate to become the next active router and sends periodic hello messages.
Active	The router currently forwards packets that are sent to the group virtual MAC address. The router sends periodic hello messages.

Accanto tabella degli stati del router

Vediamo come configurate HSRP su 2 router:
Router1
interface g0/1
ip address 172.16.10.2 255.255.255.0
standby version 2
standby 1 ip 172.16.10.254
standby 1 priority 150
standby 1 pempt
no shutdown

Router2
interface g0/1
ip address 172.16.10.3 255.255.255.0
standby version 2
standby 1 ip 172.16.10.254
no shutdown

Comandi di verifica:
show standby
show standby brief

4.3.3.4 Lab - Configure HSRP.pdf

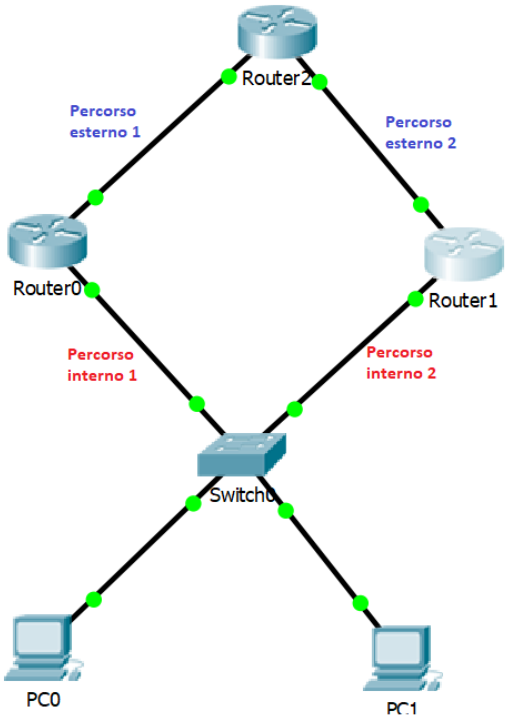
La maggior parte dei problemi in cui HSRP non funziona, si presenta quando:
1) È impossibile eleggere correttamente il router attivo che controlla l'IP virtuale per il gruppo.
2) Mancato funzionamento del router di standby per tenere traccia del router attivo.
3) Non è possibile determinare quando il controllo dell'IP virtuale per il gruppo deve essere trasferito su un altro router.
4) Mancato funzionamento dei dispositivi finali per configurare correttamente l'indirizzo IP virtuale come gateway predefinito.

I comandi di debug HSRP consentono di visualizzare l'operazione di HSRP mentre un router si guasta o viene arrestato dall'amministratore. I comandi di debug HSRP disponibili possono essere visualizzati dando il comando
debug standby ? ← indicando al posto del ? una delle opzioni che compare a seconda di cosa vogliamo controllare:
- packets: per controllare l'invio o la ricezione dei pacchetti
- terse: indica se il router che prima era attivo è stato spento
- ecc…

Problemi comuni durante il debug di HSRP:
- ❖ I router HSRP non sono collegati allo stesso segmento di rete.
- ❖ I router HSRP non sono configurati con indirizzi IPv4 dalla stessa subnet.
- ❖ I router HSRP non sono configurati con lo stesso indirizzo IPv4 virtuale.
- ❖ I router HSRP non sono configurati con lo stesso numero di gruppo HSRP.
- ❖ I dispositivi finali non sono configurati con l'indirizzo gateway predefinito corretto.

4.3.4.4 Packet Tracer - Troubleshoot HSRP.pdf
4.3.4.4 Packet Tracer - Troubleshoot HSRP.pka

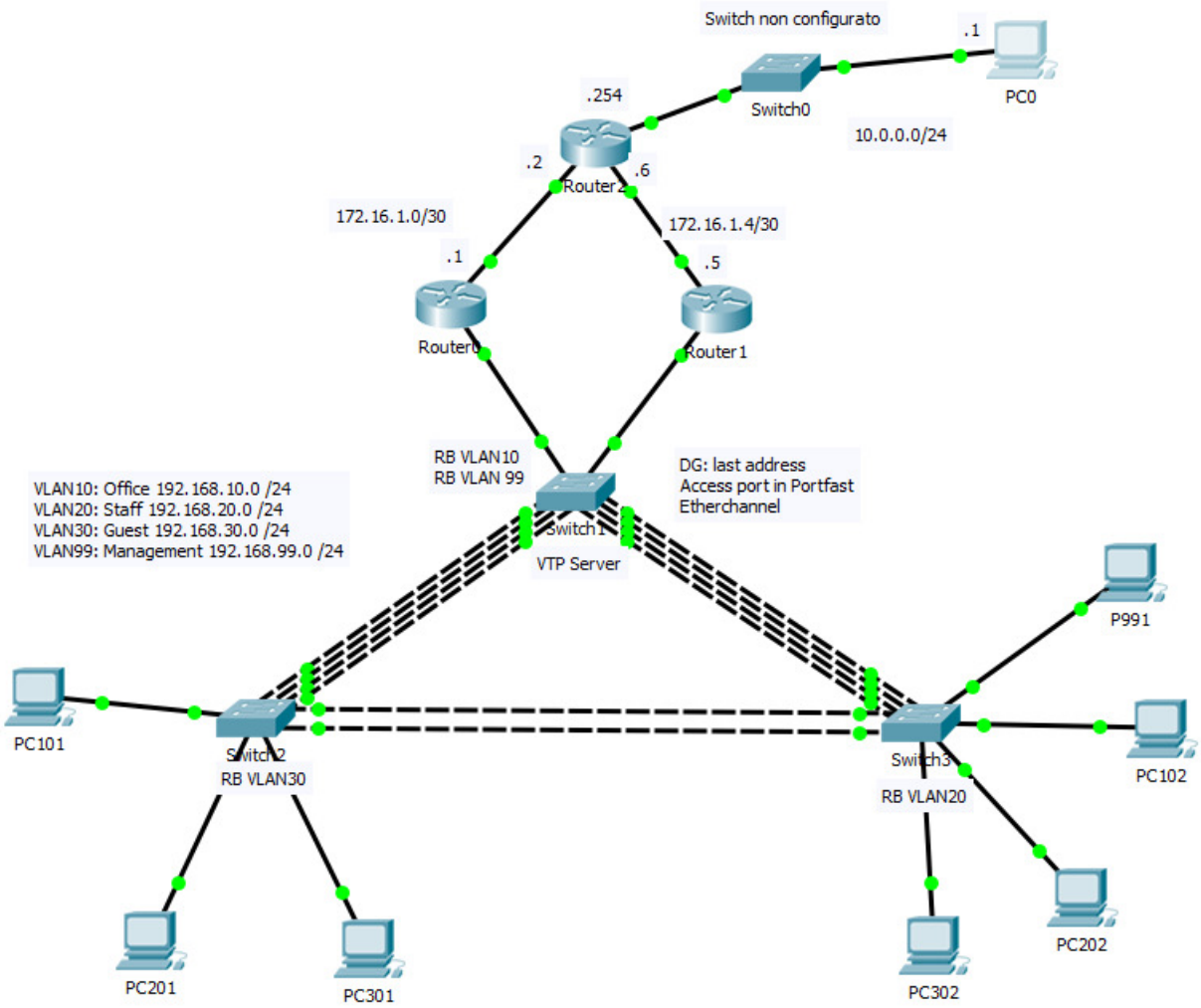
Per quanto riguarda la configurazione dei router e del protocollo HSRP, vi è un'ulteriore funzionalità che può tornare molto utile. Ossia ipotizzando di avere 2 router che utilizzano tra loro il protocollo HSRP, il traffico interno verrà girato su un router o su un altro a seconda che il link principale sia attivo oppure no, mentre se il collegamento tra il router e la rete esterna non viene monitorato.



Per spiegarmi meglio, riferendomi alla figura a lato, abbiamo che i protocolli FHRP monitorano solamente i percorsi interni 1 e 2, ma se da configurazione il PC1 contatta il Router2 tramite il percorso interno1, nel momento che la disponibilità del percorso interno 1 viene a mancare, il protocollo indirizzerà il mio traffico verso il percorso interno 2.
Se però quello che viene a mancare a tutto il routing della mia rete è il percorso esterno 1, PC1 continuerà sempre a contattare il Router2 tramite il percorso interno 1 senza però riuscirci.
Il protocollo HSRP ci consente di agire sulla priority del link di default di 10 punti in caso il router principale abbia il link fuori uso, tramite il comando
standby 30 track

NB: considerando che la priority di default è 100, se io ho impostato
standby 30 priority 150
il rilevare o meno il link attivo non ha nessuna utilità, ma se imposto il link principale con priority 105, nel momento in cui il percorso esterno 1 non sarà più utilizzabile, il mio traffico verrà dirottato sul percorso esterno 2

Vediamo ora un piccolo esercizio per configurare una rete come in figura, con RIP, STP, VTP ed FHRP
Basandoci sulla figura sottostante vediamo i comandi da dare su ogni apparato



Switch 1

enable
configure terminal
hostname Switch1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #S1 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface range fa0/1 - 4
channel-group 1 mode active


```
exit
interface range fa0/5 - 8
channel-group 3 mode active
exit
interface port-channel 1
switchport mode trunk
exit
interface port-channel 3
switchport mode trunk
exit
vtp mode server
vtp domain CISCO
vtp password cisco
vlan 10
name Office
exit
vlan 20
name Staff
exit
vlan 30
name Guest
exit
vlan 99
name Management
exit
interface vlan 99
ip address 192.168.99.250 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.254
interface fa0/7
switchport mode access
switchport access vlan 10
spanning-tree portfast
spanning-tree bpduguard enable
exit
interface fa0/8
switchport mode access
switchport access vlan 20
spanning-tree portfast
spanning-tree bpduguard enable
exit
interface fa0/9
switchport mode access
switchport access vlan 30
spanning-tree portfast
spanning-tree bpduguard enable
exit
spanning-tree vlan 1 priority 24576
spanning-tree vlan 10 priority 24576
spanning-tree vlan 99 priority 24576
spanning-tree vlan 20 priority 28672
interface range g0/1 - 2
switchport mode trunk
exit
exit
copy running-config startup-config
```

Switch 2

```
enable
configure terminal
hostname Switch2
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
```

```
banner motd #S2 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface range fa0/1 - 4
channel-group 1 mode active
exit
interface range fa0/5 - 6
channel-group 2 mode active
exit
interface port-channel 1
switchport mode trunk
exit
interface port-channel 2
switchport mode trunk
exit
interface vlan 99
ip address 192.168.99.249 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.254
vtp mode client
vtp domain CISCO
vtp password cisco
spanning-tree vlan 30 priority 24576
spanning-tree vlan 10 priority 28672
spanning-tree vlan 99 priority 28672
exit
copy running-config startup-config
```

Switch 3

```
enable
configure terminal
hostname Switch3
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #S3 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface range fa0/1 - 4
channel-group 3 mode active
exit
interface range fa0/5 - 6
channel-group 2 mode active
exit
interface port-channel 2
switchport mode trunk
exit
interface port-channel 3
switchport mode trunk
exit
```

```
interface vlan 99
ip address 192.168.99.251 255.255.255.0
no shutdown
exit
ip default-gateway 192.168.99.254
vtp mode client
vtp domain CISCO
vtp password cisco
interface fa0/7
switchport mode access
switchport access vlan 30
spanning-tree portfast
spanning-tree bpduguard enable
exit
interface fa0/8
switchport mode access
switchport access vlan 20
spanning-tree portfast
spanning-tree bpduguard enable
exit
interface fa0/9
switchport mode access
switchport access vlan 10
spanning-tree portfast
spanning-tree bpduguard enable
exit
interface fa0/10
switchport mode access
switchport access vlan 99
spanning-tree portfast
spanning-tree bpduguard enable
exit
spanning-tree vlan 20 priority 24576
spanning-tree vlan 1 priority 28672
spanning-tree vlan 30 priority 28672
exit
copy running-config startup-config
```

Router 0

```
enable
configure terminal
hostname ROUTER0
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R0 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.253 255.255.255.0
standby version 2
standby 10 ip 192.168.10.254
exit
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.253 255.255.255.0
standby version 2
```

```
standby 20 ip 192.168.20.254
standby 20 priority 105
standby 20 priority prempt
standby 20 track
exit
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.253 255.255.255.0
standby version 2
standby 30 ip 192.168.30.254
standby 30 priority 105
standby 30 priority prempt
standby 30 track
exit
interface GigabitEthernet0/0.99
encapsulation dot1Q 99
ip address 192.168.99.253 255.255.255.0
standby version 2
standby 99 ip 192.168.99.254
exit
interface GigabitEthernet0/0
no shutdown
exit
interface GigabitEthernet0/1
ip address 172.16.1.1 255.255.255.252
no shutdown
exit
router rip
version 2
no auto-summary
passive-interface g0/0
default-information originate
network 192.168.99.0
network 192.168.10.0
network 192.168.20.0
network 192.168.30.0
network 172.16.1.4
exit
exit
copy running-config startup-config
```

Router 1

```
enable
configure terminal
hostname ROUTER1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R1 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 192.168.10.252 255.255.255.0
standby version 2
standby 10 ip 192.168.10.254
standby 10 priority 105
standby 10 priority prempt
```

```
standby 10 track
exit
interface GigabitEthernet0/0.20
encapsulation dot1Q 20
ip address 192.168.20.252 255.255.255.0
standby version 2
standby 20 ip 192.168.20.254
exit
interface GigabitEthernet0/0.30
encapsulation dot1Q 30
ip address 192.168.30.252 255.255.255.0
standby version 2
standby 30 ip 192.168.30.254
exit
interface GigabitEthernet0/0.99
encapsulation dot1Q 99
ip address 192.168.99.252 255.255.255.0
standby version 2
standby 99 ip 192.168.99.254
standby 99 priority 105
standby 99 priority prempt
standby 99 track
exit
interface GigabitEthernet0/0
no shutdown
exit
interface GigabitEthernet0/1
ip address 172.16.1.5 255.255.255.252
no shutdown
exit
router rip
version 2
no auto-summary
passive-interface g0/0
default-information originate
no network 192.168.1.0
network 192.168.99.0
network 192.168.10.0
network 192.168.20.0
network 192.168.30.0
network 172.16.1.4
exit
exit
copy running-config startup-config
```

Router 2

```
enable
configure terminal
hostname ROUTER2
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R2 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 172.16.1.2 255.255.255.252
no shutdown
```



```
exit
interface GigabitEthernet0/1
ip address 172.16.1.6 255.255.255.252
no shutdown
exit
interface GigabitEthernet0/2
ip address 10.0.0.254 255.255.255.0
no shutdown
exit
router rip
version 2
no auto-summary
passive-interface g0/2
default-information originate
network 172.16.1.0
network 172.16.1.4
network 10.0.0.4
exit
exit
copy running-config startup-config
```

FINE CAPITOLO 4

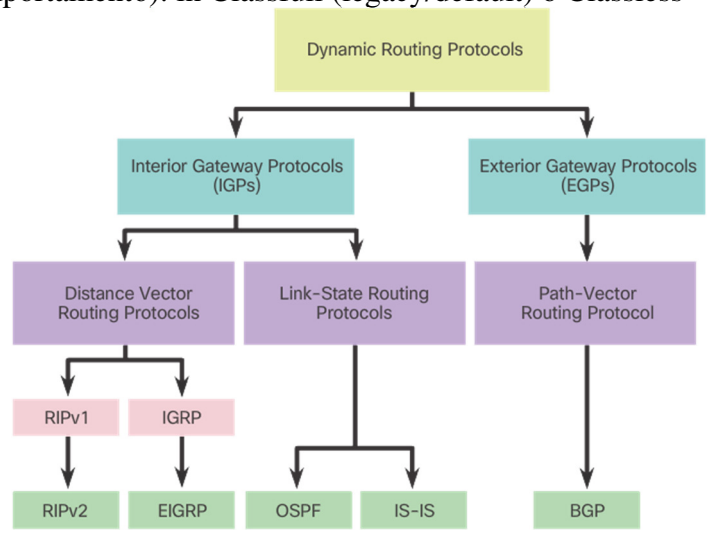
5.0.1.2 How Much Does This Cost Instructions.pdf

Un protocollo di routing è un insieme di processi, algoritmi e messaggi che vengono utilizzati per scambiare informazioni di routing e popolare la tabella di routing con la scelta dei migliori percorsi del protocollo di routing. Lo scopo dei protocolli di routing dinamico include:

- Scoperta di reti remote
- Mantenimento delle informazioni di routing aggiornate
- Scegliere il percorso migliore per le reti di destinazione
- Possibilità di trovare un nuovo percorso migliore se il percorso corrente non è più disponibile

La distinzione principale tra IGP ed EGP è riferita allo scambio d'informazioni all'interno e all'esterno di un Autonomous System (AS), ma ciò non significa che non si possano utilizzare protocolli EGP all'interno di AS, semplicemente sono appositamente stati studiati per connessioni extra AS. Il protocollo BGP (Border Gateway Protocol) è l'unico EGP attualmente valido ed è il protocollo di routing ufficiale utilizzato su Internet.
Possono essere classificati in base a:

- Purpose (scopo): in Interior Gateway Protocol (IGP) o Exterior Gateway Protocol (EGP)
- Operation: in Distance-Vector (DV), Link-State (LS), Path-Vector (PV)
- Behavior (comportamento): in Classfull (legacy/default) o Classless

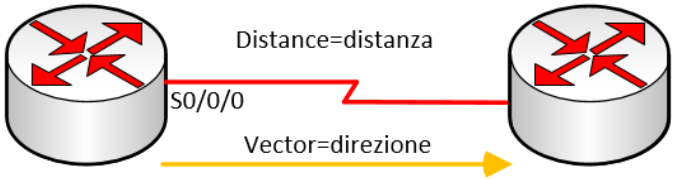


Riassumendoli:

- ✓ RIPv1 (legacy) - IGP, **DV**, Classful
- ✓ IGRP (legacy) - IGP, **DV**, Classful (sviluppato da Cisco)
- ✓ RIPv2 - IGP, **DV**, Classless
- ✓ EIGRP - IGP, **DV**, Classless (sviluppato da Cisco)
- ✓ OSPF - IGP, **LS**, Classless
- ✓ IS-IS - IGP, **LS**, Classless
- ✓ BGP - EGP, **PV**, Classless

I protocolli Distance-Vector: significa che i percorsi sono pubblicizzati fornendo 2 caratteristiche:

- Distance: identifica la distanza dalla rete di destinazione e si basa su una metrica come il conteggio degli hop, il costo, la larghezza di banda, il ritardo e altro
- Specifica la direzione del router next-hop o l'interfaccia di uscita per raggiungere la destinazione



Un router che utilizza un protocollo di routing DV non ha la conoscenza dell'intero percorso verso una rete di destinazione.

Come funziona un protocollo Distance-Vector.
Un router prende la sua tabella di routing, la codifica in un pacchetto, lo manda al router vicino. Il vicino prende il pacchetto, guarda le informazioni contenute, ed all'interno di queste informazioni guarda se gli interessano. Cosa significa, "se gli interessano"? Significa che verifica se sono informazioni che si riferiscono a destinazioni che prima non conosceva, o si riferiscono a destinazioni che conosce già (ma sono migliorative), quindi una distanza più breve per raggiungere la destinazione o è un aggiornamento che arriva dalla stessa sorgente, cioè magari non è migliorativa l'informazione, magari è peggiorativa, ma l'informazione di peggioramento mi è arrivata dalla stessa sorgente che prima mi aveva dato l'informazione, per cui devo aggiornarla peggiorata nel sistema.
NB: Distance-Vector è un approccio più semplice e per questo con determinati limiti.

A differenza di un protocollo DV, un protocollo Link-State (LS) può creare una vista completa o una topologia della rete raccogliendo informazioni da tutti gli altri router.
Quindi, l'utilizzo di un protocollo di routing link-state è come avere una mappa completa della topologia della rete. Un router che utilizza LS utilizza le informazioni sullo stato del collegamento per creare una mappa topologica e per selezionare il percorso migliore per tutte le reti di destinazione nella topologia.
I protocolli LS sono "triggered", ossia quando hanno appreso tutta la topologia della rete, inviano aggiornamenti solo quando vi sono cambiamenti sulla rete, come ad esempio se cade un link. Inoltre vengono inviati solo i dati variati, e non tutti i dati del router.

I protocolli Classful nei loro aggiornamenti non inviano la subnet, perché si riferiscono all'intera classe ip (classe A, B, ecc…) e di conseguenza non supportano il VLSM e Class Interdomain Routing (CIDR)
I protocolli Classful e Classless si applicano solo al protocollo IPv4, poiché IPv6 è solo CLASSLESS, perché includono la lunghezza del prefisso con l'indirizzo IPv6.
I protocolli di routing possono essere confrontati in base alle seguenti caratteristiche:

- Speed of Convergence (velocità di convergenza): definisce la velocità con cui i router nella topologia di rete condividono le informazioni di routing e raggiungono uno stato di conoscenza coerente. Più veloce è la convergenza, più è preferibile il protocollo. I loop di routing possono verificarsi quando le tabelle di routing incoerenti non vengono aggiornate a causa della convergenza lenta in una rete che cambia.
- Scalability: definisce quanto può essere grande una rete, in base al protocollo di routing che viene distribuito. Più grande è la rete, più scalabile deve essere il protocollo di routing.
- Classful or Classless: utilizzo o meno di VLSM e CIDR
- Utilizzo delle risorse: include i requisiti di un protocollo di routing come lo spazio di memoria (RAM), l'utilizzo della CPU e l'utilizzo della larghezza di banda del link. Requisiti di risorse più elevati richiedono hardware più potente per supportare l'operazione del protocollo di routing, oltre ai processi di inoltro dei pacchetti.
- Implementazione e manutenzione: descrivono il livello di conoscenza necessario per un amministratore di rete per implementare e mantenere la rete in base al protocollo di routing implementato.

	Distance Vector				Link State	
	RIPv1	RIPv2	IGRP	EIGRP	OSPF	IS-IS
Speed of Convergence	Slow	Slow	Slow	Fast	Fast	Fast
Scalability - Size of Network	Small	Small	Small	Large	Large	Large
Use of VLSM	No	Yes	No	Yes	Yes	Yes
Resource Usage	Low	Low	Low	Medium	High	High
Implementation and Maintenance	Simple	Simple	Simple	Complex	Complex	Complex

Ci sono casi in cui un protocollo di routing impara più di un percorso verso la stessa destinazione. Per selezionare il percorso migliore, il protocollo di routing deve essere in grado di valutare e decidere tra i percorsi disponibili. Questo è realizzato attraverso l'uso di metriche di routing.
Una metrica è un valore misurabile che viene assegnato dal protocollo di routing a diversi percorsi in base all'utilità di tale percorso. Nelle situazioni in cui esistono più percorsi verso la stessa rete remota, le metriche di routing vengono utilizzate per determinare il "costo" complessivo di un percorso dall'origine alla destinazione. I protocolli di routing determinano il percorso migliore in base alla rotta con il costo più basso.
Protocolli di routing utilizzano metriche diverse. La metrica utilizzata da un protocollo di routing non è paragonabile alla metrica utilizzata da un altro. Di conseguenza, due protocolli di routing diversi potrebbero scegliere percorsi diversi per la stessa destinazione.
Ecco l'elenco delle metriche dei protocolli utilizzati:
RIP: conteggio degli hop
OSPF: costo sulla larghezza di banda cumulativa dall'origine alla destinazione
EIGRP: larghezza di banda, minor conteggio di hop, affidabilità del link

Quando un router si accende, non conosce la topologia della rete. Non sa nemmeno che ci sono dispositivi all'altro capo dei suoi collegamenti. L'unica informazione che ha un router proviene dal proprio file di configurazione salvato memorizzato nella NVRAM. Dopo il corretto avvio di un router, applica la configurazione salvata. Se l'indirizzamento IP è configurato correttamente, il router scopre inizialmente le proprie reti direttamente connesse. Dopo l'avvio iniziale, la tabella di routing viene aggiornata con tutte le reti direttamente connesse e le interfacce su cui risiedono tali reti. Se è configurato un protocollo di routing, il passaggio successivo prevede che il router inizi a scambiare gli aggiornamenti di routing per conoscere eventuali percorsi remoti.
Il router invia un pacchetto di aggiornamento a tutte le interfacce abilitate sul router. L'aggiornamento contiene le informazioni presenti nella tabella di routing.
Allo stesso tempo, il router riceve e elabora anche aggiornamenti simili da altri router connessi. Dopo aver ricevuto un aggiornamento, il router controlla la presenza di nuove informazioni di rete. Vengono aggiunte tutte le reti che non sono attualmente elencate nella tabella di routing.
A questo punto i router hanno conoscenza delle proprie reti direttamente connesse e delle reti connesse dei loro "neighbors". Continuando il viaggio verso la convergenza, i router scambiano il prossimo ciclo di aggiornamenti periodici. Ogni router controlla nuovamente gli aggiornamenti per nuove eventuali informazioni da aggiungere in tabella di routing.
I protocolli di routing DV in genere implementano una tecnica di prevenzione del ciclo di routing nota come split horizon. Split horizon impedisce che le informazioni vengano inviate dalla stessa interfaccia da cui è stata ricevuta.

La rete è convergente quando tutti i router dispongono di informazioni complete e accurate sull'intera rete. Le proprietà di convergenza includono la velocità di propagazione delle informazioni di routing e il calcolo dei percorsi ottimali. La velocità di propagazione si riferisce al tempo impiegato dai router all'interno della rete per inoltrare le informazioni di routing.
I protocolli di routing possono essere classificati in base alla velocità alla convergenza; più veloce è la convergenza, migliore è il protocollo di routing. Generalmente, i protocolli più vecchi, come il RIP, sono lenti a convergere, mentre i protocolli moderni, come EIGRP e OSPF, convergono più rapidamente.

5.2.1.6 Packet Tracer - Investigating Convergence Instructions.pdf
5.2.1.6 Packet Tracer - Investigating Convergence.pka

I protocolli di routing Distance-Vector:

- Inviano aggiornamenti sono ai vicini;
- RIP Invia aggiornamenti periodici ogni 30 secondi anche senza variazioni sulla topologia di rete;
- RIPv1 invia gli aggiornamenti come trasmissioni all'indirizzo IPv4 di tutti gli host 255.255.255.255

La trasmissione di aggiornamenti periodici è inefficiente perché gli aggiornamenti consumano la larghezza di banda e le risorse della CPU del dispositivo di rete. Ogni dispositivo di rete deve elaborare un messaggio broadcast. Invece di utilizzare trasmissioni come RIP, RIPv2 ed EIGRP possono utilizzare indirizzi multicast per raggiungere solo router vicini specifici. EIGRP può anche utilizzare un messaggio unicast per raggiungere uno specifico router adiacente. Inoltre, EIGRP invia gli aggiornamenti solo quando necessario, anziché periodicamente.

Algoritmo Distance-Vector:

- Invia e Riceve aggiornamenti dai router vicini
- Calcola il percorso migliore e lo salva in routing table
- Rileva e reagisce ai cambiamenti della topologia di rete

RIP utilizza l'algoritmo Bellman-Ford, mentre IGRP ed EIGRP utilizzano l'algoritmo di routing Diffusion Update Algorithm (DUAL)

Caratteristiche	RIPv1	RIPv2
metrica	Il conteggio hop viene utilizzato come metrica per la selezione del percorso. Un conteggio hop superiore a 15 hop è considerato infinito	
aggiornamenti agli indirizzi	255.255.255.255	224.0.0.9
supporto VLSM e CIDR		
Supporto alla sommarizzazione		
Suppoto all'autenticazione		

Gli aggiornamenti RIP sono incapsulati in un segmento UDP, con i numeri di porta di origine e di destinazione impostati sulla porta UDP 520 e vengono inviati ogni 30 secondi.
Nel 1997 è stata rilasciata la versione di RIP abilitata per IPv6. RIPng è basato su RIPv2. Ha ancora un limite di 15 hop e la distanza amministrativa è 120.

Caratteristiche	IGRP	EIGRP
metrica	Larghezza di banda, ritardo, carico e affidabilità vengono utilizzati per creare una metrica composita	
aggiornamenti agli indirizzi	255.255.255.255	224.0.0.10
aggiornamenti ogni 90 secondi		
aggiornamenti solo con variazioni		
supporto VLSM e CIDR		
Supporto alla sommarizzazione		
Suppoto all'autenticazione		
Messaggio "Hello keepalive"		
DUAL backup route		
Convergenza rapida		

EIGRP ha il supporto del protocollo a più livelli di rete, ossia utilizza i moduli Protocol Dependent Modules (PDM), che significa che è l'unico protocollo a includere il supporto per protocolli diversi da IPv4 e IPv6, come IPX legacy e AppleTalk.

5.2.3.4 Packet Tracer - Comparing RIP and EIGRP Path Selection Instructions.pdf
5.2.3.4 Packet Tracer - Comparing RIP and EIGRP Path Selection.pka

I protocolli Link-State (LS) sono detti protocollo con il percorso più breve e sono costruiti attorno all'algoritmo SPF (shortest path first di Edsger Dijkstra).
Questo algoritmo utilizza i costi accumulati lungo ciascun percorso, dalla sorgente alla destinazione, per determinare il costo totale di una rotta.
Per raggiungere una determinata posizione, ogni router calcola l'algoritmo SPF e determina il costo dalla sua prospettiva.
NB: il percorso più breve non è necessariamente quello con il numero di HOP più basso (fondamentale da capire)

Protocollo Link-State (in una rete OSPF)

1) Ogni router apprende i propri collegamenti e le proprie reti direttamente connesse. Questo viene fatto rilevando che un'interfaccia è in stato up.
2) Ogni router è responsabile per incontrare i suoi vicini su reti direttamente connesse, scambiando pacchetti "Hello" con altri router direttamente connessi, sia per sapere che ci sono sia per sapere se sono ancora operativi, viene utilizzato come sistema di keepalive.
3) Ogni router crea un pacchetto Link-State Packet (LSP) contenente lo stato di ciascun collegamento direttamente connesso. Questo viene fatto registrando tutte le informazioni pertinenti su ciascun vicino, incluso l'ID del vicino, il tipo di collegamento e la larghezza di banda.
4) Ogni router inoltra l'LSP a tutti i vicini (Flooding=allagamento). I vicini memorizzano tutti gli LSP ricevuti in un database. Quindi inviano i LSP ai loro vicini fino a quando tutti i router nell'area hanno ricevuto gli LSP. Ogni router memorizza una copia di ogni LSP ricevuto dai suoi vicini in un database locale.
5) Ogni router utilizza il database per costruire una mappa completa della topologia e calcola il percorso migliore per ciascuna rete di destinazione. L'algoritmo SPF viene utilizzato per costruire la mappa della topologia e determinare il percorso migliore per ciascuna rete.

Questo processo è lo stesso per OSPF per IPv4 e OSPF per IPv6
Vantaggi e Svantaggi dei protocolli Link-State rispetto ai protocolli Distance-Vector

Vantaggi	Svantaggi
Crea una mappa topologica	Requisiti di memoria aggiuntivi
Convergenza rapida	Requisiti di elaborazione maggiori
Aggiornamenti basati su eventi	Requisiti di larghezza di banda (il fooding occupa più banda)
Progettazione gerarchica	

FINE CAPITOLO 5

6.0.1.2 Classless EIGRP Instructions.pdf

EIGRP è stato introdotto come protocollo di routing Distance-Vector nel 1992.
Nel 2013, EIGRP è diventato un protocollo di routing multi-vendor.
EIGRP include funzionalità sia di Distance-Vector sia di Link-State anche se tuttavia si basa sul protocollo Distance-Vector. ***←ATTANZIONE*** non è hybrid è un protocollo Distance-Vector
In IOS 15.0 CISCO ha introdotto il comando EIGRP.
EIGRP come comando consente la configurazione di EIGRP per IPv4 e IPv6 in un'unica modalità di configurazione. Ciò consente di eliminare la complessità della configurazione che si verifica durante la configurazione di EIGRP per IPv4 e IPv6 (tale comando va oltre lo scopo di questo corso).
Features di EIGRP:

- Diffusing Update ALgorithm (DUAL): risiede al centro del protocollo di routing e garantisce percorsi loop-free e di backup in tutto il dominio di routing. Memorizza tutte le rotte di backup disponibili per le destinazioni in modo che possa adattarsi rapidamente a percorsi alternativi quando necessario.
- Establishing Neighbor Adjacencies: stabilisce relazioni con router direttamente connessi che sono anche abilitati per EIGRP. Le adiacenze del vicinato vengono utilizzate per tenere traccia dello stato di questi vicini.
- Reliable Transport Protocol (RTP): è univoco per EIGRP e fornisce i pacchetti EIGRP ai vicini. L'RTP e il tracciamento delle adiacenze dei vicini impostano il palcoscenico per DUAL.
- Partial and Bounded Updates (parziali e limitati): a differenza di RIP, EIGRP non invia aggiornamenti periodici e le voci di percorso non invecchiano. L'aggiornamento include solo informazioni sulle modifiche al percorso e vengono inviate solamente a quei router che influenzano le modifiche della topologia della rete. Ciò riduce al minimo la larghezza di banda necessaria per inviare gli aggiornamenti EIGRP.
- Equal and Unequal Cost Load Balancing: consente agli amministratori di distribuire meglio il flusso di traffico nelle loro reti.

EIGRP ha la capacità di instradare diversi protocolli, inclusi IPv4 e IPv6. EIGRP lo fa utilizzando i protocol-dependent modules (PDMs).
I PDMs sono responsabili delle attività di routing specifiche per ciascun protocollo del livello di rete, tra cui:

- Manutenzione delle tabelle neighbor e topologia dei router EIGRP
- Costruzione e traduzione di pacchetti specifici del protocollo per DUAL
- Interfacciamento DUAL alla tabella di routing specifica del protocollo
- Calcolo della metrica e trasmissione di queste informazioni a DUAL
- Implementazione di filtri e elenchi di accesso
- Esecuzione di funzioni di ridistribuzione da e verso altri protocolli di routing
- Ridistribuire percorsi che vengono appresi da altri protocolli di routing

Quando un router scopre un nuovo vicino, registra l'indirizzo e l'interfaccia del vicino come una voce nella tabella vicina. Esiste una tabella adiacente per ciascun modulo dipendente dal protocollo, come IPv4. EIGRP mantiene anche una tabella di topologia. La tabella della topologia contiene tutte le destinazioni pubblicizzate dai router adiacenti. Esiste anche una tabella di topologia separata per ciascun PDM.
EIGRP è stato progettato come protocollo di routing indipendente dal livello di rete. A causa di questo design, EIGRP non può utilizzare i servizi di UDP o TCP. Invece, EIGRP utilizza il protocollo RTP (Reliable Transport Protocol) per la consegna e la ricezione di pacchetti EIGRP. Ciò consente a EIGRP di essere flessibile e può essere utilizzato per protocolli diversi da quelli della suite di protocolli TCP/IP, come i protocolli IPX e AppleTalk ormai obsoleti.

RTP include sia la consegna affidabile sia la consegna inaffidabile di pacchetti EIGRP.
Il pacchetti EIGRP Hello (inviato generalmente ogni 5 secondi, mentre su reti T1 o più scarse generalmente ogni 60 secondi) è un pacchetto RTP inaffidabile, mentre un aggiornamento dello stato è un pacchetto RTP affidabile che richiede una conferma.
RTP può inviare pacchetti EIGRP come unicast o multicast:

- I pacchetti EIGRP multicast per IPv4 utilizzano l'indirizzo multicast IPv4 riservato 224.0.0.10
- I pacchetti EIGRP multicast per IPv6 vengono inviati all'indirizzo multicast IPv6 riservato FF02::A

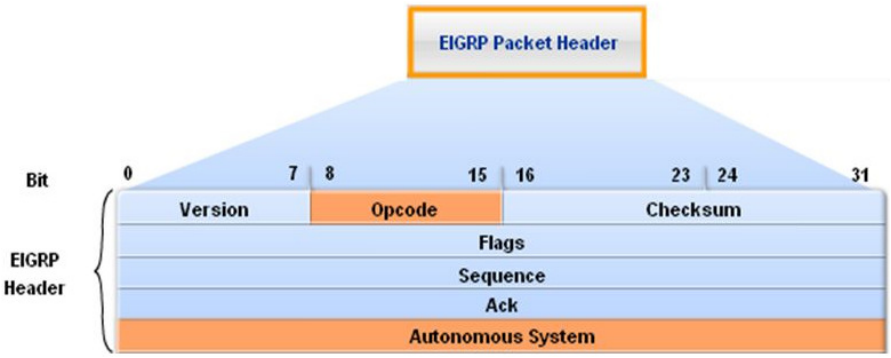
Una buona pratica è autenticare le informazioni di routing trasmesse. Ciò garantisce che i router accetti solo le informazioni di routing da altri router configurati con la stessa password o le stesse informazioni di autenticazione.
NB: l'autenticazione non crittografa gli aggiornamenti di routing EIGRP, ma mette al riparo il router da propagazione d'informazioni esterne non autorizzate.

EIGRP utilizza cinque diversi tipi di pacchetti:

Tipi di pacchetti	Usato per	
Hello	Used for neighbor discovery and to maintain neighbor adjacencies	- Inviato con consegna inaffidabile - Multicast (sulla maggior parte dei tipi di rete)
Update	Propagates routing information to EIGRP neighbors Acknowledgment the recept of any EIGRP packet	- Inviato con consegna affidabile - Multicast o Unicast
Acknowledgment	Used to acknowledge the receipt of an EIGRP message that was sent using RTP	- Inviato con consegna inaffidabile - Unicast
Query	Used to query routes from neighbors	- Inviato con consegna affidabile - Multicast o Unicast
Reply	Sent in response to an EIGRP query	- Inviato con consegna affidabile - Unicast

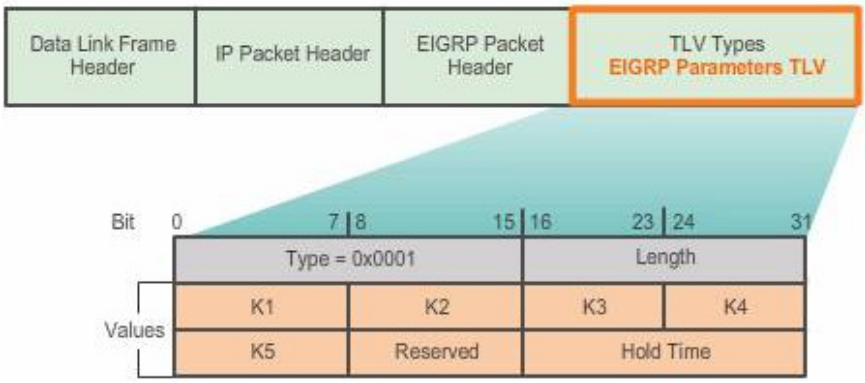
EIGRP utilizza un timer **Hold** per determinare il tempo massimo che il router deve attendere per ricevere il prossimo Hello prima di dichiarare irraggiungibile quel vicino. Per impostazione predefinita, il tempo di attesa è tre volte l'intervallo Hello. Se il tempo di attesa scade, EIGRP dichiara il percorso come inattivo e DUAL cerca un nuovo percorso inviando query.
Durante la fase di Query/Reply tutti i vicini devono inviare una risposta, indipendentemente dal fatto che abbiano o meno un percorso verso la rete abbattuta. Poiché le risposte utilizzano anche la consegna affidabile, devono inviare una conferma.

La porzione di dati di un messaggio EIGRP è incapsulata in un pacchetto. Questo campo dati è chiamato TLV (type, length, value). I tipi di TLV rilevanti per questo corso sono parametri EIGRP, percorsi interni IP e percorsi esterni IP. L'intestazione del pacchetto EIGRP è inclusa in ogni pacchetto EIGRP, indipendentemente dal suo tipo. L'intestazione del pacchetto EIGRP e il TLV vengono quindi incapsulati in un pacchetto IPv4. Nell'intestazione del pacchetto IPv4, il campo del protocollo è impostato su 88 per indicare EIGRP e l'indirizzo di destinazione IPv4 è impostato sul Multicast 224.0.0.10. Se il pacchetto EIGRP è incapsulato in un frame Ethernet, l'indirizzo MAC di destinazione è anche un indirizzo Multicast, 01-00-5E-00-00-0A.
L'indirizzo di destinazione IPv6 sarebbe l'indirizzo multicast FF02::A e il prossimo campo di intestazione sarebbe impostato su 88.



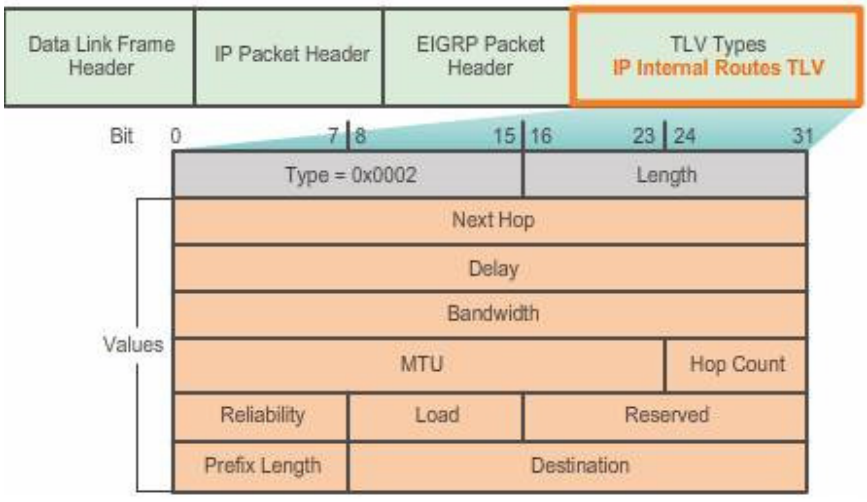
I campi importanti includono il campo Opcode e Autonomous System.
Opcode specifica il tipo di pacchetto EIGRP come segue:
- Update
- Query
- Reply
- Hello

The Autonomous System specifica il processo di routing EIGRP. A differenza di RIP, più istanze di EIGRP possono essere eseguite su una rete. Tale numero viene utilizzato per tracciare ogni processo EIGRP in esecuzione.



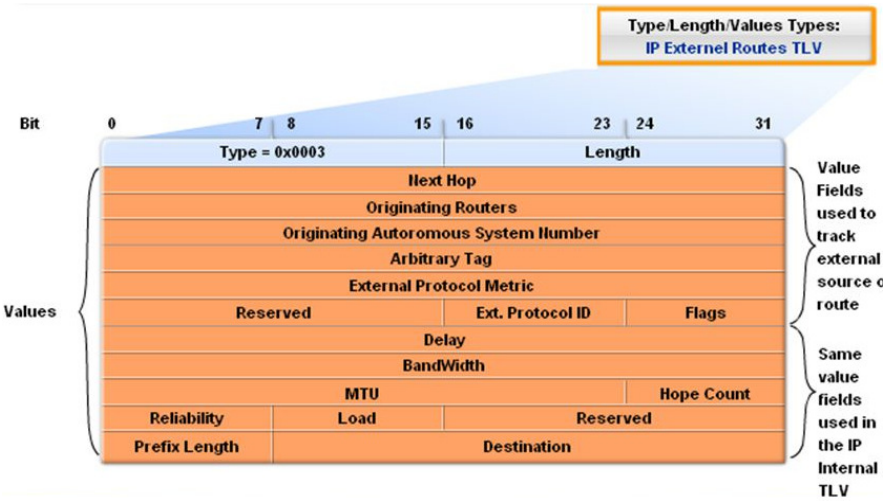
Per impostazione predefinita, solo la larghezza di banda e il ritardo sono ponderati. Entrambi sono ugualmente pesati; pertanto, il campo K1 per la larghezza di banda e il campo K3 per il ritardo sono entrambi impostati su uno (1). Gli altri valori K sono impostati su zero (0).

Il Tempo di attesa (hold) è la quantità di tempo che il vicino EIGRP che riceve questo messaggio dovrebbe attendere prima di considerare che il router pubblicitario sia inattivo



TLV IP Internal Routes. Il messaggio interno IP viene utilizzato per pubblicizzare le rotte EIGRP all'interno dell'Autonomous System. I campi importanti includono i campi di metrica (delay e bandwidth), il campo della subnet mask (lunghezza del prefisso) e il campo di destinazione.

Il ritardo è calcolato come la somma dei ritardi dalla sorgente alla destinazione in unità di 10 microsecondi. La larghezza di banda è la larghezza di banda configurata più bassa di qualsiasi interfaccia lungo il percorso.
La subnet mask viene specificata come lunghezza del prefisso o numero di bit di rete nella subnet mask.
Il campo Destination memorizza l'indirizzo della rete di destinazione.



Il messaggio IP esterno viene utilizzato quando le rotte esterne vengono importate nel processo di routing EIGRP.
Si noti che la metà inferiore del TLV di percorsi esterni IP include tutti i campi utilizzati dal TLV IP interno.

NB: l'MTU nell'EIGRP è incluso negli aggiornamenti di routing, ma non è utilizzato per determinare la metrica di routing.

Per abilitare EIGRP si usa il comando
router eigrp 10 ← NB: 10 è un valore che identifica il mio Autonomous System e non ha nulla a che vedere con il valore degli Autonomous System assegnati dall'IANA. Questo valore è di 16 bit, quindi può avere un qualunque valore tra 1 e 65.535 e tutti i router all'interno del mio dominio di routing devono avere lo stesso valore.
Il comando sopra non avvia il processo EIGRP stesso. Il router non inizia a inviare aggiornamenti. Piuttosto, questo comando fornisce solo l'accesso per configurare le impostazioni EIGRP.
Per rimuovere completamente il processo di routing EIGRP da un dispositivo, utilizzare il comando
no router eigrp 10

L'ID router EIGRP viene utilizzato per identificare in modo univoco ciascun router nel dominio di routing EIGRP.
Tuttavia, il ruolo dell'ID router è più significativo in OSPF.
EIGRP per IPv4 utilizza l'ID router a 32 bit per identificare il router di origine per la ridistribuzione di percorsi esterni. La necessità di un router ID diventa più evidente nella discussione di EIGRP per IPv6.
Per determinare il suo ID router, un router Cisco IOS utilizzerà i seguenti tre criteri nell'ordine:

- Utilizza l'indirizzo configurato con il comando
  eigrp router-id 1.1.1.1
  NB: non è un IPv4 specifico, ma un identificativo
- Se l'ID del router non è configurato, seleziona l'indirizzo IPv4 più alto di qualsiasi delle sue interfacce di loopback
- Se non sono configurate interfacce di loopback, sceglie l'indirizzo IPv4 attivo più elevato di una qualsiasi delle sue interfacce fisiche

Se l'amministratore di rete non configura esplicitamente un ID router, EIGRP genera il proprio ID router utilizzando un indirizzo IP di loopback o fisico.
Tuttavia, l'interfaccia deve essere nello stato up/up.
NOTA: Alcune versioni di IOS accetteranno il comando id-router, senza prima specificare eigrp

Per abilitare un'interfaccia all'invio e alla ricezione dei pacchetti del protocollo EIGRP bisogna dare il comando
network 172.16.1.0

Questo comando ha le seguenti conseguenze:

- Abilita qualsiasi interfaccia su questo router che corrisponda all'indirizzo di rete nel comando della modalità di configurazione del router di rete per inviare e ricevere gli aggiornamenti EIGRP.
- La rete delle interfacce è inclusa negli aggiornamenti di routing EIGRP.
- Il comando imposta la classful

Quando EIGRP viene attivato (appena inserita la prima network), DUAL genera automaticamente il messaggio di notifica perché il comando:
eigrp log-neighbor-changes
è abilitato per impostazione predefinita.
Se però non si vuole includere tutta una classful in una propagazione poiché è stata suddivisa, la si può propagare tramite le wildcard
network 172.16.1.0 0.0.0.255

Si può anche decidere di disattivare EIGRP su una determinata interfaccia, questo semplicemente blocca la ricezione e l'invio dei pacchetti TLV Hello.
NB: la rete (network) può essere propagata, sulle altre interfacce, ma non su quella tramite il comando
passive interface gigabitethernet 0/0
Per configurare tutte le interfacce come passive
passive interface default
Per disabilitare un'interfaccia come passiva
no passive interface gigabitethernet 0/0

```
R3# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
<output omitted>
Routing for Networks:
    192.168.1.0
    192.168.10.4/30
    192.168.10.8/30
 Passive Interface(s):
   GigabitEthernet0/0
 Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.10.5          90      01:37:57
    192.168.10.9          90      01:37:57
  Distance: internal 90 external 170
R3#
```

Per verificare se un'interfacci è in passive mode, dal privileged exec, dare il comando
show ip protocols
e verificare: quello in figura accanto

Con il comando
show ip eigrp neighbors

Trubleshooting

Se con EIGRP attivato un router vicino non viene elencato, dopo aver stabilito le adiacenze, controllare l'interfaccia locale per assicurarsi che venga attivato con il comando

show ip interface brief

Se l'interfaccia è attiva, provare a eseguire il ping dell'indirizzo IPv4 del router adiacente. Se il ping fallisce, significa che l'interfaccia adiacente è inattiva e deve essere attivata. Se il ping ha esito positivo e EIGRP continua a non vedere il router come un vicino, esaminare le seguenti configurazioni:

- Entrambi i router sono configurati con lo stesso numero di System Autonomous?
- La rete direttamente connessa è inclusa nella propagazione con EIGRP?

Con il comando

show ip protocols

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"  (1) Routing protocol and Process ID (AS Number)
  Outgoing update filter clist for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight K1=1, K2=0, K3=1, K4=0, K5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1 (2)                    EIGRP Router ID
    Topology : 0 (base)
      Active Timer: 3 min
  Distance: internal 90 external 170 (3)      EIGRP Administrative Distances
      Maximum path: 4
      Maximum hopcount 100
      Maximum metric variance 1

  Automatic Summarization: disabled (4)       EIGRP Automatic Summarization is disabled.
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources: (5)
    Gateway         Distance      Last Update
    192.168.10.6         90       00:40:20
    172.16.3.2           90       00:40:20
                                   EIGRP Routing Information Sources lists all the EIGRP routing sources the IOS uses to build its IPv4 routing table.
  Distance: internal 90 external 170

R1#
```

Abbiamo a disposizione le seguenti informazioni:

1) Che sul router è attivo un protocollo dinamico EIGRP attivo
2) Il router-ID è: 1.1.1.1
3) L'Administrative Distance è
   i. Internal: 90
   ii. External 170
4) Di default EIGRP non effettua la sommarizzazione delle classi (NB: prima di IOS 15 la sommarizzazione delle classi era attiva di default). Per disattivarlo nelle versioni precedenti:

no auto-summary

5) Elenco dei router vicini con EIGRP attivo

Administrative Distance Table

Routing Protocol	Default Administrative Distance Value
Connected interface	0
Static route out an interface	1
Static route to a next-hop address	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIPv1 and RIP v2	120
Exterior Gateway Protocol (EGP)	140
On-Demand Routing (ODR)	160
External EIGRP	170
Internal BGP	200

6.2.2.4 Packet Tracer - Configuring Basic EIGRP with IPv4 Instructions.pdf
6.2.2.4 Packet Tracer - Configuring Basic EIGRP with IPv4.pka
6.2.2.5 Lab - Configuring Basic EIGRP for IPv4.pdf

Composizione della metrica dell'EIGRP

Nell'interfaccia di configurazione dell'EIGRP
posso impostare il peso della metrica tramite il comando
metric weight tos k1 k2 k3 k4 k5

con i valori che rappresentano:

- K1: bandwidth (banda a disposizione)
- K2: load (carico)
- K3: delay (ritardo)
- K4: reiliability (afifdabilità)
- K5: reiliability (afifdabilità)

Dove K2, K4, K5 di default vengono assunti a 0, mentre K1 e K3 a 1

I valori che eventualmente vogliamo assegnare vengono utilizzati per il calcolo secondo la formula che vediamo sotto

$$[(K_1 * Bandwidth + \frac{K_2 * Bandwidth}{256 - Delay} + K_3 * Delay) * \frac{K_5}{K_4 + Reliability}] * 256$$

By default

$$K_2, K_4, K_5 = 0$$

So the formula simplifies to

$$[(K_1 * Bandwidth) + (K_3 * Delay)] * 256$$

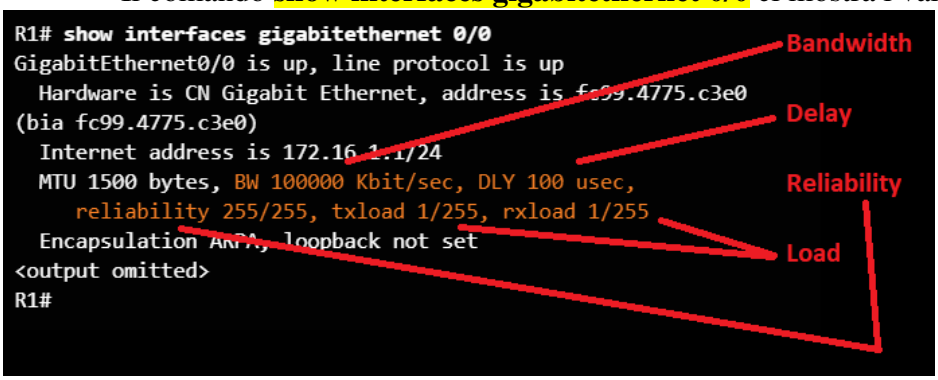
ATTENZIONE: il metodo di calcolo della metrica ed il numero di Autonomous System dell'EIGRP devono corrispondere tra i vicini EIGRP. Se non corrispondono, i router non formano un'adiacenza. Ossia se su un link di un router modifico un valore di Kx, lo devo modificare anche sull'interfaccia del router adiacente sullo stesso link, altrimenti l'adiacenza non si forma.

```
R1# show ip protocols
*** IP Routing is NSF aware ***

Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP-IPv4 Protocol for AS(1)
    Metric weight k1=1, k2=0, k3=1, k4=0, k5=0
    NSF-aware route hold timer is 240
    Router-ID: 1.1.1.1
    <output omitted>
    R1#
```

Il comando **show ip protocols** all'interno di un router mostra i valori di k1, k2, k3, k4, k5 nel calcolo della metrica (come si vede in figura accanto).

Il comando **show interfaces gigabitethernet 0/0** ci mostra i valori mostrati nella figura sottostante



- Larghezza di banda in Kbit/s
- Ritardo: in decimi di millisecondo
- Affidabilità 100%
- Carico del link in invio ed in ricezione

Poiché sia EIGRP che OSPF utilizzano la larghezza di banda nei calcoli di metrica predefiniti, un valore corretto per la larghezza di banda è molto importante per l'accuratezza delle informazioni di routing.
Vediamo come configurare la larghezza di banda:

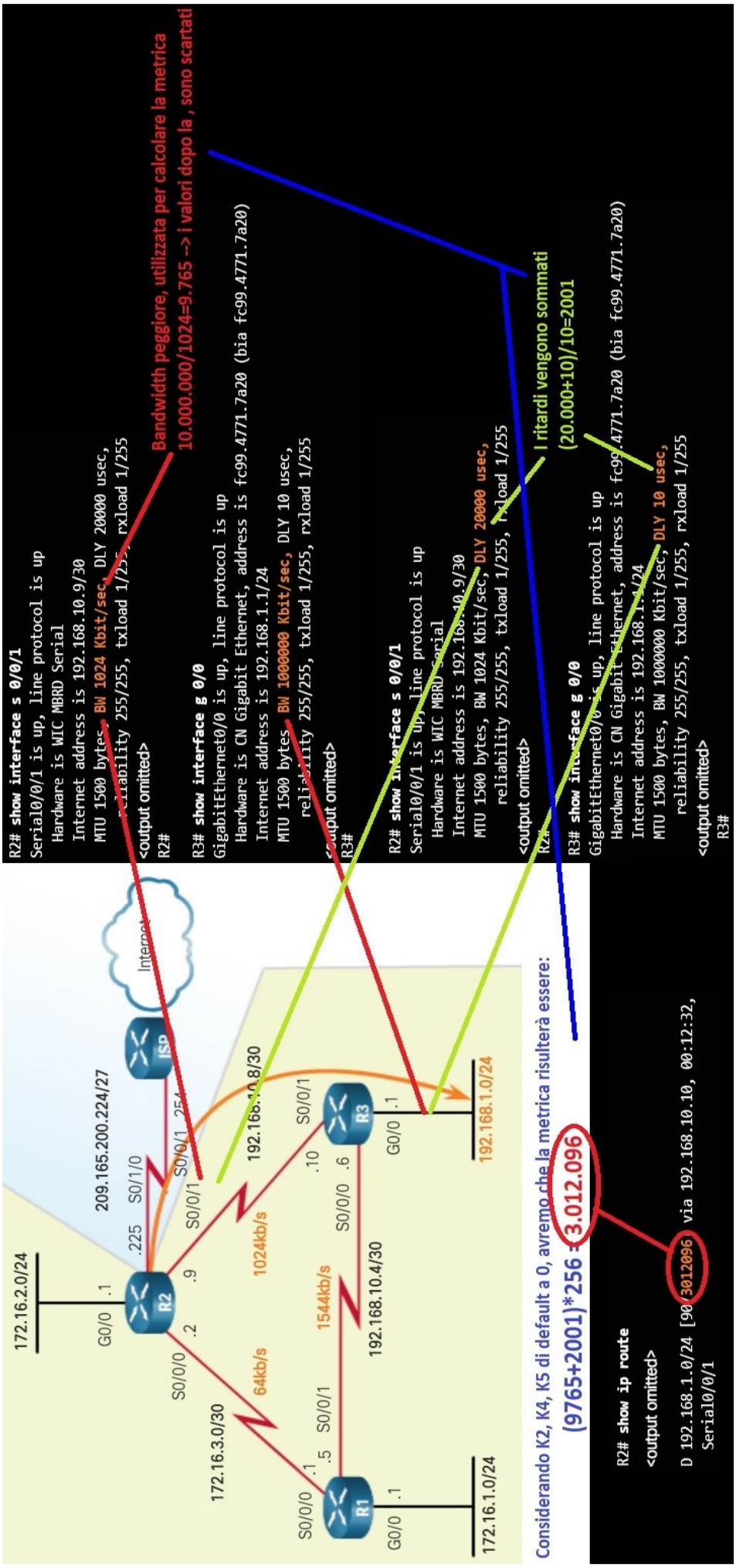
interface gigabitethernet 0/0
bandwidth 1024 ← valore in kb/s

Media	Delay
Ethernet	1,000
Fast Ethernet	100
Gigabit Ethernet	10
16M Token Ring	630
FDDI	100
T1 (Serial Default)	20,000
DS0 (64 kb/s)	20,000
1024 kb/s	20,000
56 kb/s	20,000

Il delay è un valore statico associato al tipo di collegamento a cui l'interfaccia è connessa ed è espressa in microsecondi. È un valore modificabile, ma di default viene assunto in base alla tabella accanto.

Quando viene utilizzato per determinare la metrica EIGRP, il ritardo è la somma cumulativa di tutti i ritardi dell'interfaccia lungo il percorso (misurati in decine di microsecondi).

SUPER SUPER ATTENZIONE: nel calcolo della metrica di una distanza da un router A ad uno Z, si guarda tutto il percorso che si deve attraversare e si utilizza il valore di bandwidth del link più scadente per effettuare il calcolo. Mentre il ritardo (delay) che viene utilizzato nel calcolo è la somma di tutti i ritardi dei vari link. COME ILLUSTRATO NELLA PAGINA SUCCESSIVA


R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 192.168.10.9/30
MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R2#
Bandwidth peggiore, utilizzata per calcolare la metrica
10.000.000/1024=9.765 --> i valori dopo la , sono scartati
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20 (bia fc99.4771.7a20)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R3#
R2# show interface s 0/0/1
Serial0/0/1 is up, line protocol is up
Hardware is WIC MBRD Serial
Internet address is 192.168.10.9/30
MTU 1500 bytes, BW 1024 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R2#
I ritardi vengono sommati
(20.000+10)/10=2001
R3# show interface g 0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is CN Gigabit Ethernet, address is fc99.4771.7a20 (bia fc99.4771.7a20)
Internet address is 192.168.1.1/24
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
<output omitted>
R3#
Internet
ISP
209.165.200.224/27
S0/1/0
.225
S0/0/1
.254
R2
G0/0
.1
.2
S0/0/0
.9
S0/0/1
192.168.10.8/30
1024kb/s
172.16.2.0/24
172.16.3.0/30
64kb/s
S0/0/0
.1
.5
S0/0/1
1544kb/s
192.168.10.4/30
S0/0/1
.10
S0/0/0
.6
R3
G0/0
.1
192.168.1.0/24
R1
G0/0
.1
172.16.1.0/24
Considerando K2, K4, K5 di default a 0, avremo che la metrica risulterà essere:
(9765+2001)*256 = 3.012.096
R2# show ip route
<output omitted>
D 192.168.1.0/24 [90/3012096] via 192.168.10.10, 00:12:32,
Serial0/0/1

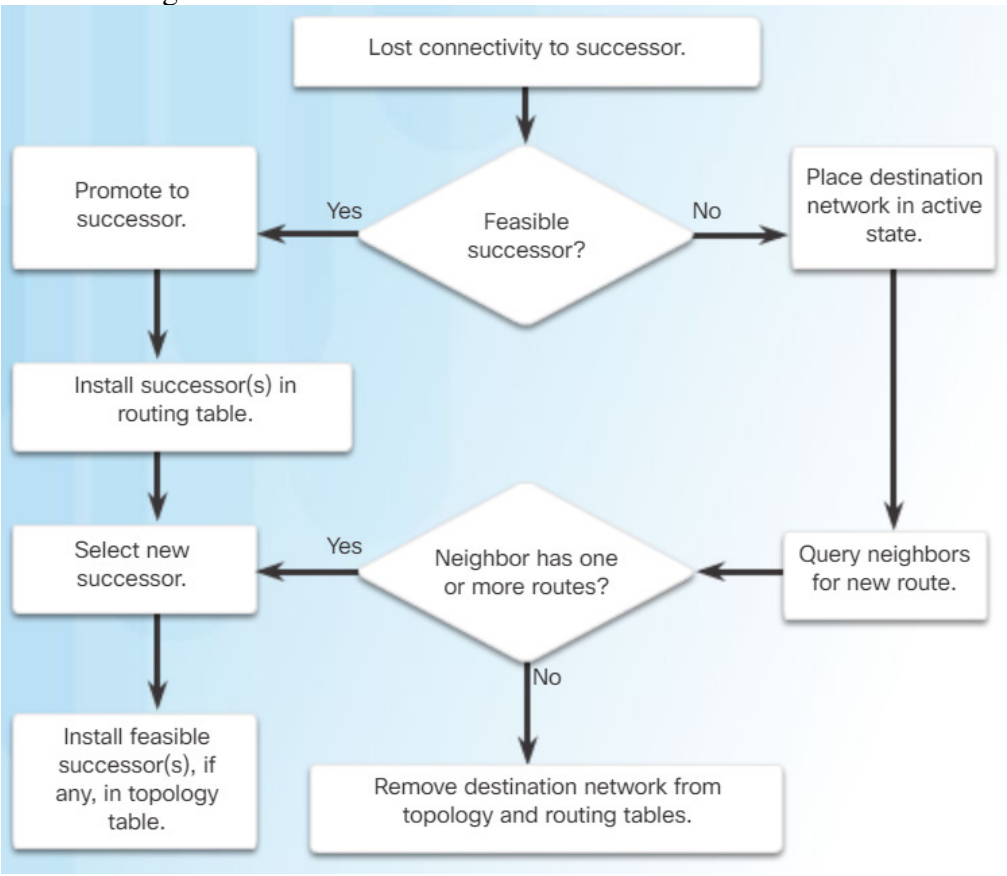
Analizziamo ora il protocollo DUAL utilizzato da EIGRP che ci permette di avere il miglio percorso loop-free e di avere un percorso di routing di backup sempre loop-free.
Il processo decisionale per tutti i calcoli del percorso viene eseguito dal DUAL utilizza FSM (Finite State Machine). DUAL FSM è un modello di flusso di lavoro, simile a un diagramma di flusso.
DUAL FSM tiene traccia di tutte le rotte e utilizza le metriche EIGRP per selezionare percorsi efficienti e senza loop e per identificare i percorsi con il percorso meno costoso da inserire nella tabella di routing.
Il ricalcolo dell'algoritmo DUAL può richiedere un uso intensivo del processore. EIGRP evita la ricompilazione quando possibile mantenendo un elenco di percorsi di backup che DUAL ha già stabilito di essere senza loop. Se la route principale nella tabella di routing non riesce, la migliore route di backup viene immediatamente aggiunta alla tabella di routing.

Tramite il comando
show ip eigrp topology
Potremo visualizzare la tabella della topologia EIGRP che contiene tutti i percorsi noti a ciascun vicino EIGRP. Poiché un router EIGRP apprende i percorsi dai suoi vicini, tali percorsi vengono installati nella sua tabella di topologia EIGRP.

```
R4>show ip eigrp topology
IP-EIGRP Topology Table for AS 100
                    Il router non stà aggiornando o ricalcolando
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.45.0.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/1/1
P 10.43.0.0/24, 1 successors, FD is 40512000
         via Connected, Serial0/0/1
P 10.34.0.0/24, 1 successors, FD is 20512000
         via Connected, Serial0/0/0
P 10.15.0.0/24, 1 successors, FD is 20514560
         via 10.45.0.5 (20514560/258560), Serial0/1/1
P 10.36.0.0/24, 1 successors, FD is 20514560
         via 10.34.0.3 (20514560/28160), Serial0/0/0 <-- Rotta principale
         via 10.43.0.3 (40514560/28160), Serial0/0/1 <-- Rotta di backup
```

Riassumiamo con il diagramma sotto il funzionamento di DUAL FSM



6.3.4.4 Packet Tracer - Investigating DUAL FSM Instructions.pdf
6.3.4.4 Packet Tracer - Investigating DUAL FSM.pka

EIGRP per IPv4 ed IPv6 sono molto simili anche se girano su canali separati e tra loro indipendenti. I pacchetti che vendono scambiati tra i router vicini, utilizzano gli indirizzi Link-Local, poiché l'indirizzo Link-Local IPv6 direttamente collegato, consente a un dispositivo di comunicare con altri dispositivi abilitati IPv6 sullo stesso collegamento e solo su quel collegamento.
EIGRP per i messaggi IPv6 vengono inviati utilizzando:

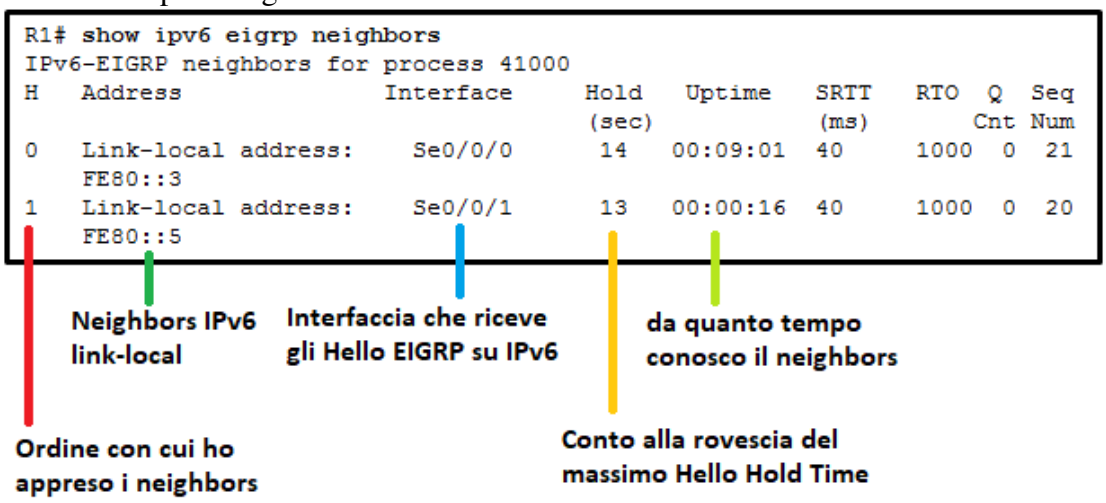
- Indirizzo IPv6 di origine: questo è l'indirizzo Link-Local IPv6 dell'interfaccia di uscita.
- Indirizzo IPv6 di destinazione: quando il pacchetto deve essere inviato a un indirizzo multi-cast, viene inviato all'indirizzo multicast IPv6 FF02::A. Se il pacchetto può essere inviato come indirizzo unicast, viene inviato all'indirizzo di Link-Local del router adiacente.

Nota: gli indirizzi Link-Local IPv6 si trovano nell'intervallo FE80::/10. La /10 indica che i primi 10 bit sono 1111 1110 10xx xxxx, il che risulta nel primo hextet con un intervallo di 1111 1110 1000 0000 (FE80) a 1111 1110 1011 1111 (FEBF).

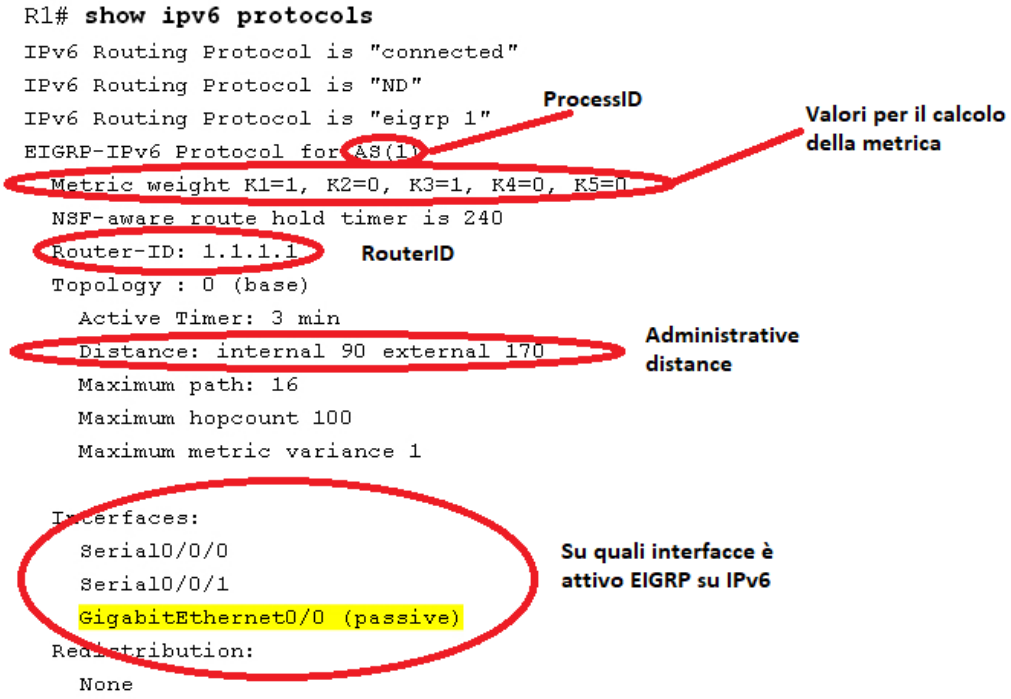
Gli indirizzi link-local sono automaticamente creati quando viene assegnato un indirizzo IPv6 global-unicast ad un'interfaccia.
A meno che non siano configurati manualmente, i router Cisco creano l'indirizzo link-local utilizzando il prefisso FE80::/10 e il processo EUI-64.
Per le interfacce seriali, Cisco utilizza l'indirizzo MAC di un'interfaccia Ethernet.
NNB: un router con diverse interfacce seriali può assegnare lo stesso indirizzo link-local a ciascuna interfaccia IPv6, poiché gli indirizzi link-local devono essere solo locali sul collegamento.
Gli indirizzi ink-local possono essere configurati manualmente utilizzando lo stesso comando della modalità di configurazione dell'interfaccia utilizzato per creare indirizzi unicast globali IPv6, ma con parametri diversi:
ipv6 address FE08::1 link-local

Vediamo ora come configurare EIGRP con IPv6
ipv6 unicast-routing ← **ricordarsi per prima cosa di attivare ipv6**
ipv6 router eigrp 2
eigrp router-id 1.1.1.1
no shutdown
poi bisogna entrare nelle varie interfacce ed assegnare l'EIGRP
interface gigabitethernet0/0
ipv6 eigrp 2
exit
interface gigabitethernet 0/1
ipv6 eigrp 2
exit
interface serial 0/0/0
ipv6 eigrp 2
exit
come per IPv4 si può configurare un'interfaccia in passive, in modo tale che non risponda agli hello e di conseguenza non propaghi EIGRP, tramite il comando
ipv6 eigrp 2
passive-interface gigabitethernet 0/1
exit

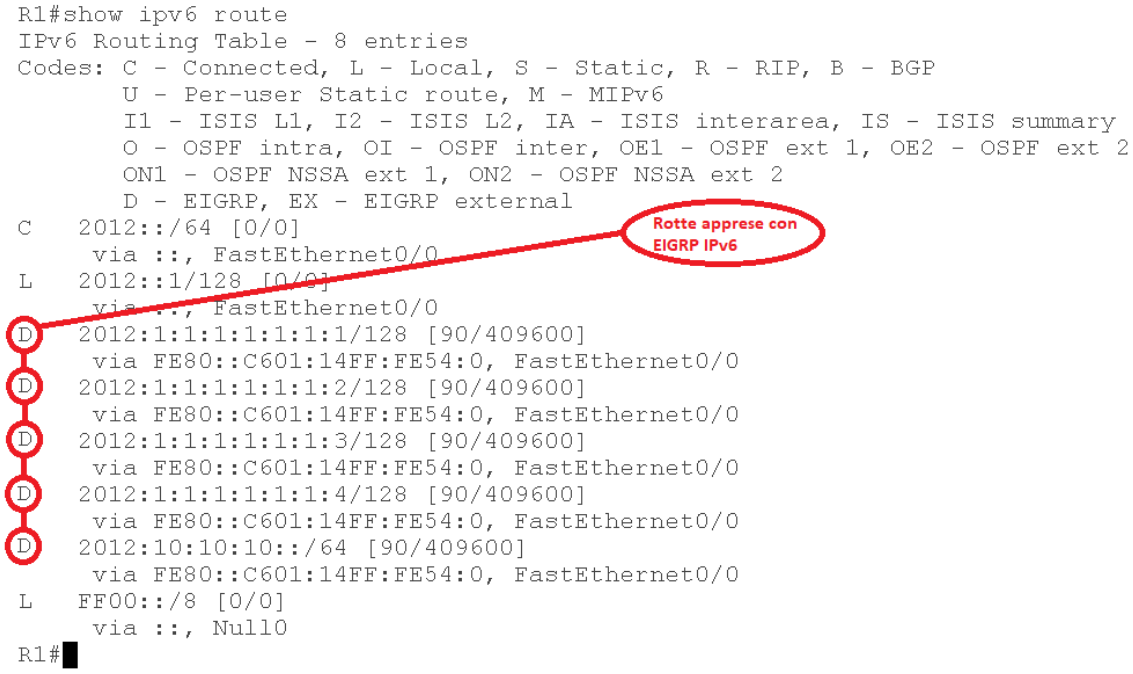
Per verificare che il router stia creando tutte le adiacenze correttamente con i suoi vicini (neighbors), diamo il comando:
show ipv6 eigrp neighbors
e analizziamo l'output in figura



Con il comando
show ipv6 protocols
possiamo controllare le informazioni indicate



Per visualizzare come si sta popolando la tabella di routing sui nostri router diamo il comando
show ipv6 route



6.4.3.4 Packet Tracer - Configuring Basic EIGRP with IPv6 Routing Instructions.pdf
6.4.3.4 Packet Tracer - Configuring Basic EIGRP with IPv6 Routing.pka
6.4.3.5 Lab - Configuring Basic EIGRP for IPv6.pdf
6.5.1.1 Portfolio RIP and EIGRP Instructions.pdf

FINE CAPITOLO 6

7.0.1.2 Class Activity - EIGRP - Back to the Future.pdf
Si noti che i comandi bandwidth saranno utilizzati per variare il valore appunto di bandwidth predefinito sulle interfacce, come ad esempio 1.544 kb/s sull'interfaccia seriale.
L'autosommarizzazione non è abilitata di default sull'EIGRP, quindi per facilitare il compito ai router di frontiera possiamo abilitarla tramite il comando
router eigrp 3
auto-summary
exit

Per propagare una rotta statica predefinita generalmente viene propagata la default route 0.0.0.0/0 dalla quale poi si accede a tutto il resto della rete.
ip route 0.0.0.0 0.0.0.0 serial 0/1/0 ← NB: ricordarsi di mettere UP l'interfaccia prima
router eigrp 3
redistribute static
exit
RICORDARSI: una rotta statica di default propagata accanto al protocollo che mi indica com'è stata appresa, vi è un'*

In IPv6
ipv6 unicast-routing
ipv6 route ::/0 serial 0/1/0
ipv6 router eigrp 3
redistribute static
exit

7.1.3.4 Packet Tracer - Propagating a Default Route in EIGRP for IPv4 and IPv6 Instructions.pdf
7.1.3.4 Packet Tracer - Propagating a Default Route in EIGRP for IPv4 and IPv6.pka

Per impostazione predefinita, EIGRP utilizza solo fino al 50% del bandwidth dell'interfaccia per le informazioni EIGRP. Ciò impedisce al processo EIGRP di sovra-utilizzare un link.
Su ogni link è possibile modificare questo valore tramite:
interface gigabitethernet 0/0
ip bandwidth-percent eigrp 3 40
exit
Per IPv6
interface gigabitethernet 0/0
ipv6 bandwidth-percent eigrp 3 40
exit

Di default su una connessione seriale, gli Hello vengono inviati ogni 60 secondi, mentre l'Hold Time è 3 volte il valore di Hello di default, mentre per le linee T1 ed Ethernet Hello è a 5 secondi e l'Hold Time a 15, per variare questi valori:
interface gigabitethernet 0/0
ip hello-interval eigrp 3 4
ip hold-time eigrp 3 10
exit
Per IPv6
interface gigabitethernet 0/0
ipv6 hello-interval eigrp 3 4
ipv6 hold-time eigrp 3 10
exit

IMPORTANTISSIMO

Se si cambiano i valori su un'interfaccia di un link, bisogna cambiare gli stessi valori anche sull'interfaccia del link dell'altro lato, ossia sull'interfaccia dell'altro router che si affaccia sul medesimo link

Il bilanciamento di carico (in riferimento a EIGRP) è la capacità di un router di distribuire il traffico in uscita utilizzando tutte le interfacce che hanno la stessa metrica dall'indirizzo di destinazione. Il bilanciamento di carico utilizza i link ed il bandwidth in modo efficiente. IOS applica di default il bilanciamento di carico fino a 4 link.
Quest'ultimo valore può essere variato con il comando:
maximum-paths 4
NB: se il valore è 1 il bilanciamento è disattivato

EIGRP per IPv4 e IPv6 può anche bilanciare il traffico su più percorsi con metriche diverse. Questo tipo di bilanciamento è chiamato bilanciamento del carico ineguale. La variazione viene effettuata tramite il comando
variance
Per visualizzare come viene distribuito il carico utilizzare il comando
traffic share balanced

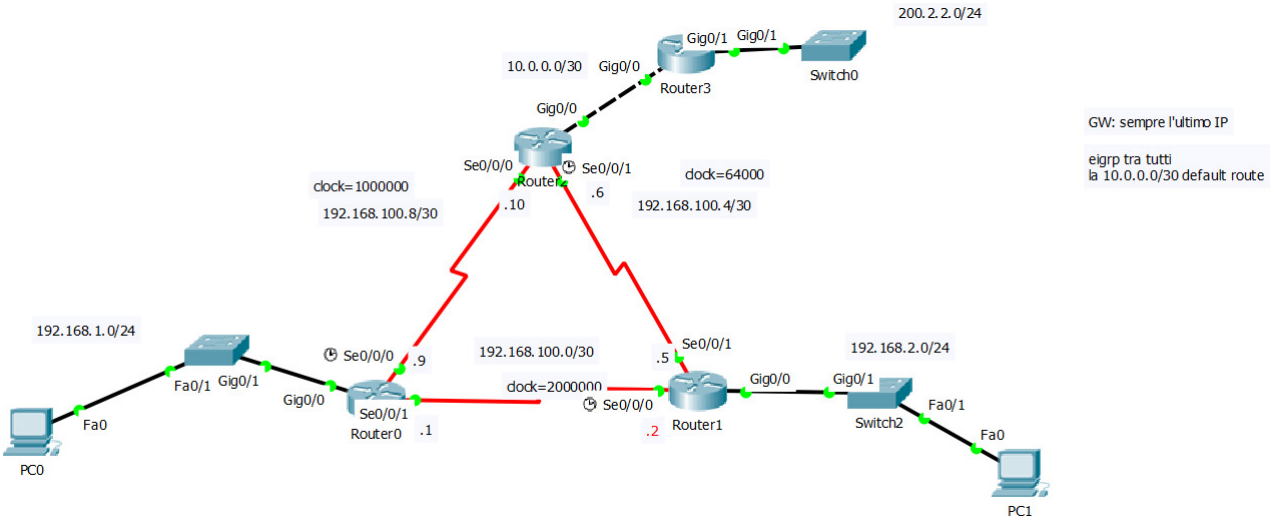
7.1.3.6 Lab - Configuring Advanced EIGRP for IPv4 Features.pdf

Comandi riassuntivi di Troubleshooting
show ip eigrp neighbors
show ip route eigrp
show ip protocols
show ip interface brief

show ipv6 eigrp neighbors
show ipv6 route eigrp
show ipv6 protocols
show ipv6 interface brief

7.2.3.5 Packet Tracer - Troubleshooting EIGRP for IPv4 Instructions.pdf
7.2.3.5 Packet Tracer - Troubleshooting EIGRP for IPv4.pka
7.2.3.6 Lab - Troubleshooting Basic EIGRP for IPv4 and IPv6.pdf
7.2.3.7 Lab - Troubleshooting Advanced EIGRP.pdf
7.3.1.1 Class Activity - Tuning EIGRP.pdf
7.3.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
7.3.1.2 Packet Tracer - Skills Integration Challenge.pka

Esercizio EIGRP



--- ROUTER0 ---

```
hostname ROUTER0
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R0 - Accesso consentito solo al personale autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 192.168.1.254 255.255.255.0
no shutdown
exit
interface Serial0/0/0
ip address 192.168.100.9 255.255.255.252
clock rate 1000000
no shutdown
exit
interface Serial0/0/1
ip address 192.168.100.1 255.255.255.252
no shutdown
exit
router eigrp 1
eigrp router-id 1.1.1.1
network 192.168.1.0
network 192.168.100.0 0.0.0.3
network 192.168.100.8 0.0.0.3
passive-interface g0/0
exit
exit
copy running-config startup-config
```

--- ROUTER1 ---

```
hostname ROUTER1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R1 - Accesso consentito solo al personale autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 192.168.2.254 255.255.255.0
no shutdown
exit
interface Serial0/0/0
ip address 192.168.100.2 255.255.255.252
clock rate 2000000
no shutdown
exit
interface Serial0/0/1
ip address 192.168.100.5 255.255.255.252
no shutdown
exit
router eigrp 1
eigrp router-id 2.2.2.2
network 192.168.2.0
network 192.168.100.0 0.0.0.3
network 192.168.100.4 0.0.0.3
passive-interface g0/0
exit
exit
copy running-config startup-config
```

--- ROUTER2 ---

```
hostname ROUTER2
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R2 - Accesso consentito solo al personale autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.0.0.1 255.255.255.252
no shutdown
exit
interface Serial0/0/1
ip address 192.168.100.6 255.255.255.252
clock rate 64000
no shutdown
exit
interface Serial0/0/0
ip address 192.168.100.10 255.255.255.252
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.2
router eigrp 1
eigrp router-id 3.3.3.3
network 192.168.1.0
network 192.168.100.4 0.0.0.3
network 192.168.100.8 0.0.0.3
passive-interface GigabitEthernet0/0
redistribute static
exit
exit
copy running-config startup-config
```

--- ROUTER3 ---

```
hostname ROUTER3
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R3 - Accesso consentito solo al personale autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.0.0.2 255.255.255.252
no shutdown
exit
interface GigabitEthernet0/1
ip address 200.2.2.254 255.255.255.0
no shutdown
exit
exit
copy running-config startup-config
```

FINE CAPITOLO 7

8.0.1.2 Class Activity - Can Submarines Swim Instructions.pdf

OSFPv2 (anno 1991) è disponibile per IPv4, mentre OSPFv3 (anno 1999) è disponibile per IPv6.
OSPF è l'acronimo di Open Shortest Path First.
Features dell'OSPF:

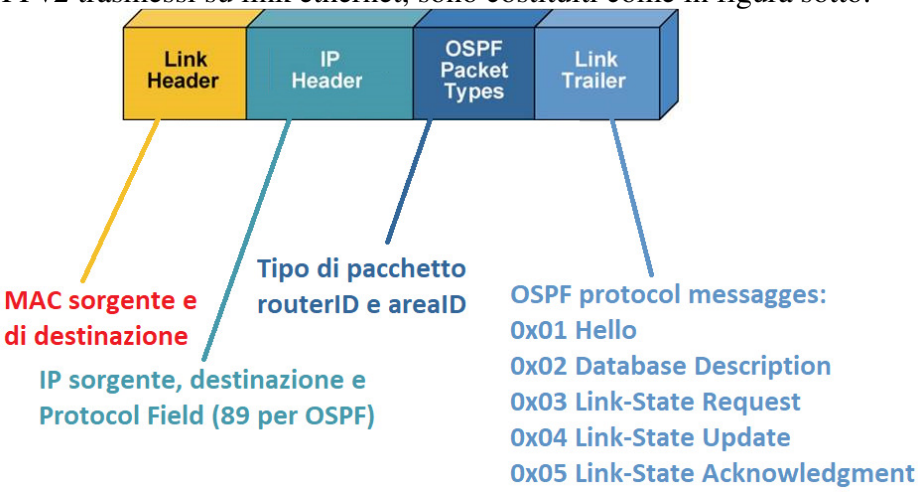
Classless: OSPFv2 supporta VLSM e CIDR
Efficient: invia solamente le modifiche della routing table quando avvengono. Utilizza l'algoritmo SPF per scegliere il percorso migliore
Fast Convergence: propaga rapidamente le modifiche alla rete
Scalable: funziona bene in reti di piccole e grandi dimensioni. I router possono essere raggruppati in aree per supportare un sistema gerarchico
Secure: OSPFv2 supporta l'autenticazione SHA ed MD5. OSPFv3 utilizza IPsec per aggiungere l'autenticazione.

L'Administrative Distance predefinita di OSPF è 110.
I 3 componenti principali del protocollo OSPF sono:

1) Strutture dati: OSPF crea e mantiene:
   - Adjacency database: crea la tabella dei vicini (neighbors)
     show ip ospf neighbors
   - Link-state database: crea la topologia della rete
     show ip ospf database
   - Forwarding database: crea la tabella di routing
     show ip route
2) Routing protocol messagges: i device layer3 che si scambiano informazioni tramite OSPF utilizzano 5 tipi di pacchetto:
   - Hello: utilizzato per stabilire e mantenere le adiacenze con i neighbors. Pubblicizza i parametri su cui due router devono essere d'accordo per diventare vicini. Eleggere il **Designated Router (DR)** e il **Backup Designated Router (BDR)** su reti multiaccess come Ethernet. Di default la priority è 1, ma può variare da 0 a 255 (vince chi ha il valore più alto), nel caso di uguaglianza vince chi ha il RouterID più alto.
   - Database description (DBD): contiene un elenco abbreviato di LSDB (Link-State DataBase) del router di invio e viene utilizzato dal router ricevente per verificare l'LSDB locale. L'LSDB deve essere identico su tutti i router Link-State all'interno di un'area per costruire un albero SPF accurato
   - Link-state request (LSR): i router riceventi possono richiedere ulteriori informazioni su qualsiasi voce nel DBD inviando un LSR
   - Link-state update (LSU): sono usati per rispondere agli LSR e per annunciare nuove informazioni. Gli LSU contengono 11 diversi tipi di LSA
   - Link-state acknowledgment (LSAck): il router ricevente invia un LSAck per confermare la ricezione della LSU. Il campo dati LSAck è vuoto.

3) Algoritmo: il router crea la tabella della topologia utilizzando i risultati dei calcoli basati sull'algoritmo SPF Dijkstra. L'algoritmo SPF si basa sul costo cumulativo per raggiungere una destinazione.
   L'algoritmo SPF crea un albero, posizionando ciascun router nella radice dell'albero e calcolando il percorso più breve per ogni nodo.
   OSPF posiziona i percorsi migliori nel database di inoltro, che viene utilizzato per creare la tabella di routing.

L'OSPF mi consente di creare reti di medie grandi dimensioni in maniera gerarchica.
In OSPF il sistema si divide in aree per controllare meglio la crescita della rete (scalability). Tra 2 aree ci deve essere sempre un router che è in mezzo tra esse. Un link non può passare tra 2 aree, ma le aree devono per forza essere divise da router.
I messaggi OSPFv2 trasmessi su link ethernet, sono costituiti come in figura sotto:

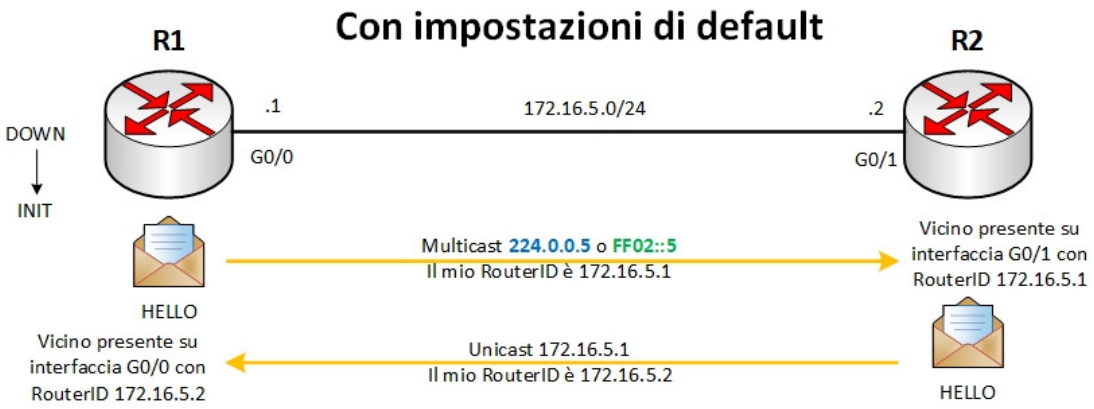


I pacchetti OSPF Hello vengono trasmessi all'indirizzo IPv4 224.0.0.5 e FF02::5 in IPv6.
Con tempistiche di default di 10 secondi nelle reti multiaccess e 30 secondi nelle reti multipl-access non broacast.
L'intervallo Dead è il periodo in cui il router attende di ricevere un pacchetto Hello prima di dichiarare il neighbor down. Se l'intervallo Dead scade prima che i router ricevano un pacchetto Hello, OSPF rimuove quel neighbor dal suo LSDB. Cisco utilizza un valore di Dead predefinito di 4 volte l'intervallo Hello.

Tipi di LSA che possono essere contenuti in LSU

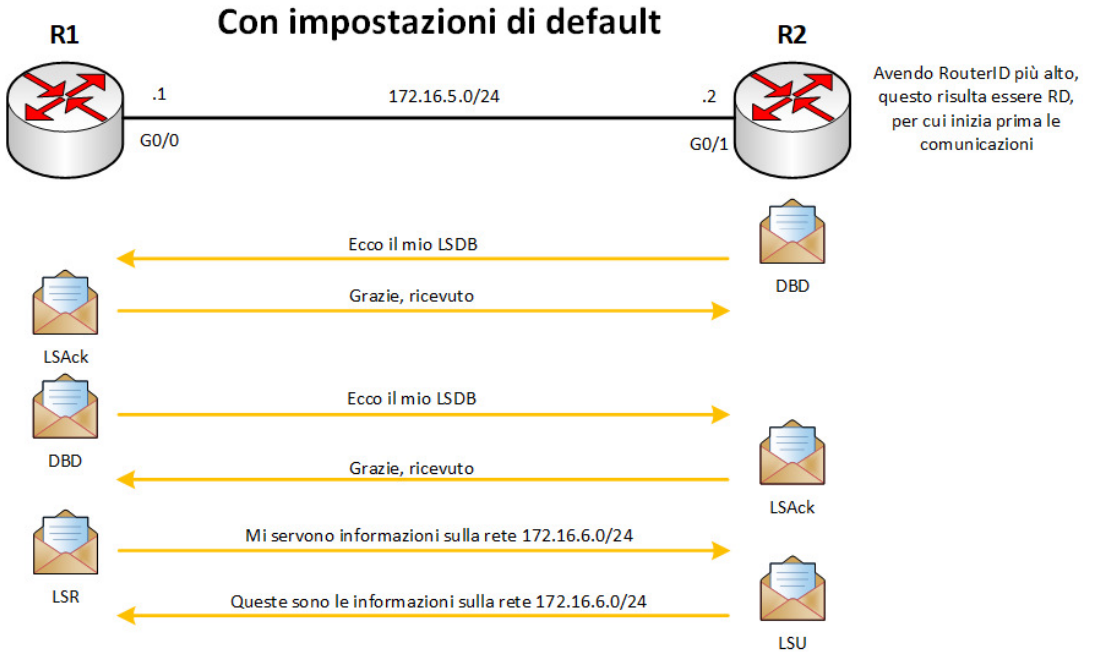
LSA Type	Description
1	Router LSAs
2	Network LSAs
3 or 4	Summary LSAs
5	Autonomous System External LSAs
6	Multicast OSPF LSAs
7	Defined for Not-So-Stubby Areas
8	External Attributes LSA for Border Gateway Protocol (BGP)
9, 10, 11	Opaque LSAs

Quindi riassumendo il percorso che effettua l'OSPF è il seguente:
Crea adiacenze con i vicini → Scambia informazioni di routing → Calcola i migliori percorsi → Raggiungi la convergenza



Essendo i router impostati di default, l'elezione del DR vince R2 in quanto hanno stessa priority, ma RD ha il valore di RouterID più alto

Vediamo ora la formula per calcolare il numero di adiacenze di una rete, ossia il numero delle connessioni neighbors.
Considerando n come il numero di router a nostra disposizione, avremo che il numero di adiacenze sarà: $= \frac{n*(n-1)}{2}$
L'elezione del DR e del BDR si rende necessaria per evitare di avere un flooding di LSAs (parte dell'LSU), in modo tale di avere un unico punto di raccolta e distribuzione per gli LSAs inviati e ricevuti. Anche un BDR viene eletto in caso di fallimento del DR. Tutti gli altri router diventano DROTHERs (ossia ne DR ne BDR).
NB: il DR viene utilizzato solo per la diffusione di LSAs.



Vediamo ora come attivare l'OSPF (sempre partendo dalla configuration terminal)
router ospf 9
dove il valore 9 è identificativo solo sul router in cui viene lanciato, e non è obbligatorio sia lo stesso sugli altri router che eseguono OSPF, ed è un valore che varia da 1 fino a 65.535
Assegniamo un identificativo univoco a 32bit al router in formato IPv4, questo deve essere univoco all'interno del mio dominio OSPF
router-id 3.3.3.3

Se il RouterID non viene configurato in modo esplicito, il router sceglie l'indirizzo IPv4 più alto di qualsiasi interfaccia loopback configurata.
Se non sono configurate interfacce di loopback, il router sceglie l'indirizzo IPv4 attivo più alto di qualsiasi delle sue interfacce fisiche.
Se il router utilizza l'indirizzo IPv4 più alto per il RouterID, non è necessario che l'interfaccia sia abilitata per OSPF. Ciò significa che l'indirizzo dell'interfaccia non deve essere incluso in uno dei comandi OSPF network affinché il router utilizzi tale indirizzo IPv4 come RouterID. L'unico requisito è che l'interfaccia sia attiva e UP.

Vediamo quindi come attivare un'interfaccia di loopback

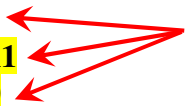
```
interface loopback 0
ip address 10.99.99.1 255.255.255.255
no shutdown
exit
```

A volte è necessario modificare un RouterID, ma tuttavia dopo che un router ha selezionato un RouterID, un router OSPFv2 attivo non consente di modificare RouterID fino a quando il router non viene ricaricato o il processo OSPFv2 viene cancellato.
Per cui l'unico modo per riavviare il processo di analisi della topologia della rete è pulire il processo OSPF tramite il comando (***NB***: in privileged exec e non configuration terminal)

```
clear ip ospf process
```

Vediamo come abilitare OSPF sulle interfacce:

```
router ospf 10
router-id 3.3.3.3
network 10.10.0.2 0.0.0.0 area 0
network 10.99.99.2 0.0.0.0 area 11
network 10.11.0.2 0.0.0.0 area 10
exit
```



mettendo l'IPv4 dell'interfaccia e la netmask a 0.0.0.0 non devo calcolarmi la wild card mask in quando da IOS 15 OSPF non sommarizza più di default per cui il sistema mi prende in automatico la rete e la netmask di propagazione

naturalmente si può decidere di mettere in passive mode un'interfaccia, in modo tale che questa non risponda più agli Hello. In questo modo l'interfaccia non invia più i segnali di Hello per cui risulta non attiva per i neighbros. Per fare ciò si utilizza il comando:

```
router ospf 10
passive-interface gigabitethernet 0/0
exit
```

per mettere tutte le interfacce in passive mode e poi successivamente abilitarle in base alle nostre esigenze con (**no passice-interface**):

```
router ospf 10
passive-interface default
exit
```

8.2.2.7 Packet Tracer - Configuring OSPFv2 in a Single Area Instructions.pdf
8.2.2.7 Packet Tracer - Configuring OSPFv2 in a Single Area.pka

Un protocollo di routing utilizza una metrica per determinare il percorso migliore di un pacchetto attraverso una rete. Una metrica fornisce l'indicazione del sovraccarico necessario per inviare pacchetti attraverso una determinata interfaccia. Un costo inferiore indica un percorso migliore rispetto a un costo più elevato.
Il costo di un'interfaccia è inversamente proporzionale alla larghezza di banda dell'interfaccia.
La larghezza di banda di riferimento predefinita è 10^8

$$Costo = \frac{100.000.000 \text{ bps}}{larghezza\ di\ banda\ dell'interfaccia\ in\ bps}$$

Interface Type	Reference Bandwidth in bps		Default Bandwidth in bps	Cost
10 Gigabit Ethernet 10 Gbps	100,000,000	÷	10,000,000,000	1
Gigabit Ethernet 1 Gbps	100,000,000	÷	1,000,000,000	1
Fast Ethernet 100 Mbps	100,000,000	÷	100,000,000	1
Ethernet 10 Mbps	100,000,000	÷	10,000,000	10
Serial 1.544 Mbps	100,000,000	÷	1,544,000	64
Serial 128 kbps	100,000,000	÷	128,000	781
Serial 64 kbps	100,000,000	÷	64,000	1562

```
R1# show ip route | include 172.16.2.0
O        172.16.2.0/24 [110/65] via 172.16.3.2, 03:39:07,
         Serial0/0/0
```

Per il calcolo della miglior rotta da seguire, per raggiungere un nodo, OSPF utilizza la somma dei costi dei link del miglior percorso.
Se il calcolo del costo risulta qualcosa di meno di un intero, OSPF arrotonda il numero intero più vicino. Per questo motivo, dal punto di vista dell'OSPF, un'interfaccia con una larghezza di banda dell'interfaccia di 100 Mb/s ha lo stesso costo di un'interfaccia con una larghezza di banda di 100 Gb/s.
La modifica della larghezza di banda di riferimento non influisce in realtà sulla capacità di larghezza di banda sul collegamento, ma influenza semplicemente il calcolo utilizzato per determinare la metrica.
Per modificare il valore della banda di riferimento utilizzare il comando

```
router ospf 10
auto-cost reference-bandwidth 10000
exit
```

← valore in Mb/s in questo caso 10Gb/s

Anche il bandwidth può essere variato per comodità o magari si rende necessario quando si notano degradi dei cavi di collegamento, tramite il comando

```
interface serial 0/0/1
bandwidth 64
exit
```

per ripristinare il valore di default utilizzare il comando

```
no bandwidth
```

SUPER ATTENZIONE: questi comandi non modificano il bandwidth del link, ma il bandwidth nel calcolo della metrica
In casi particolari può anche essere utile impostare direttamente il costo dell'link OSPF, ma fare molta attenzione a documentare il tutto, altrimenti si rischia poi di incasinare tutta le rete o meglio di non riuscire ad effettuare un corretto trubleshooting. Il comando per modificare il costo è:

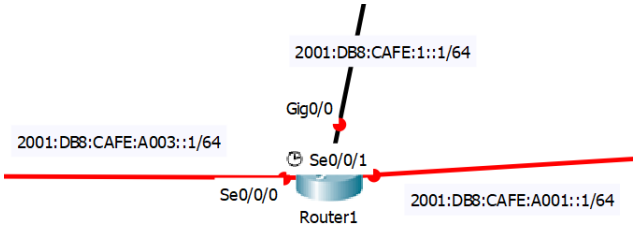
```
interface serial 0/0/1
no bandwidth 64
ip ospf cost 15625
exit
```

Correzione bandwidth	=	Impostazione manuale costo
R1(config)# interface S0/0/1 R1(config-if)# bandwidth 64	=	R1(config)# interface S0/0/1 R1(config-if)# ip ospf cost 15625
R2(config)# interface S0/0/1 R2(config-if)# bandwidth 1024	=	R2(config)# interface S0/0/1 R2(config-if)# ip ospf cost 976

Per vedere la propagazione dei dati dei router OSPF possiamo dare il comando
show ip ospf neighbor
Per vedere i dati informativi dell'OSPF propagato dare il comando
show ip ospf
Per avere informazioni sulle interfacce che vengono propagate in OSPF con relativi costi stato ecc…
show ip ospf interface brief

8.2.4.5 Lab - Configuring Basic Single-Area OSPFv2.pdf

Avendo capito i concetti di OSPFv2 (quindi per IPv4) vediamo di estenderli a OSPFv3 (quindi per IPv6). Per iniziare impostiamo i parametri di rete:




```
ipv6 unicast-routing                                  ← attiviamo IPv6
interface gigabitethernet 0/0
description Router1 GLAN
ipv6 address 2001:DB8:CAFE:1::1/64                    ← global unicast
ipv6 address FE80::1 link-local
no shutdown
exit
interface serial 0/0/1
description Serial2R2
ipv6 address 2001:DB8:CAFE:A001::1/64                 ← global unicast
ipv6 address FE80::1 link-local
clock rate 128000
no shutdown
exit
interface serial 0/0/0
description Serial2R3
ipv6 address 2001:DB8:CAFE:A003::1/64                 ← global unicast
ipv6 address FE80::1 link-local
no shutdown
exit
```

Attenzione, in questo caso io ho ESPRESSAMENTE configurato anche un indirizzo link-local, ma se non l'avessi fatto IOS avrebbe automaticamente configurato un indirizzo link-local per il router assegnandolo a tutte le interfacce attive, basandosi sulla codifica EUI64 a partire da FE80::/10
Vediamo ora come attivare OSPFv3

```
ipv6 router ospf 32
router-id 2.2.2.2
auto-cost reference-bandwidth 1000
exit
```

Per verificare i servizi IPv6 attivi
show ipv6 protocols
Se dobbiamo modificare dei parametri in OSPFv3, prima li modifichiamo, poi usciamo dalla configuration terminal e torniamo nella privileged exec e diamo il comando
clear ipv6 ospf process
Infine vediamo come assegnare OSPFv3 alle varie interfacce

```
interface gigabitethernet 0/0
ipv6 ospf 32 area 0
exit
interface serial 0/0/0
ipv6 ospf 32 area 0
exit
interface serial 0/0/1
ipv6 ospf 32 area 0
exit
```


Per verificare le configurazioni effettuate:
show ipv6 ospf interfaces brief ← NB: da privileged Exec, come tutti i comandi show

Per visionare l'elenco dei neighbors:
show ipv6 ospf neighbor

Ricorda: se OSPF è in single area si tende ad utilizzare Area 0, ma utilizzare anche altri valori non è un errore.

Per verificare la routing table appresa da OSPFv3
show ipv6 route ospf ← Ricorda: se c'è * è la default route

8.3.3.5 Packet Tracer - Configuring Basic OSPFv3 in a Single Area Instructions.pdf
8.3.3.5 Packet Tracer - Configuring Basic OSPFv3 in a Single Area.pka
8.3.3.6 Lab - Configuring Basic Single-Area OSPFv3.pdf
8.4.1.1 Class Activity - Stepping Through OSPFv3 Instructions.pdf
8.4.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
8.4.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 8

9.0.1.2 Leaving on a Jet Plane Instructions.pdf

Nell'OSPF multi-area, possiamo considerare le multi aree come i petali di un fiore, dove tutte le varie aree sono dei petali, che devono essere in contatto tra loro tramite l'AREA 0.
Ogni area deve avere uno o più router di confine che avranno un'interfaccia all'interno dell'area di origine ed un'altra all'interno dell'area 0. Si crea quindi una gerarchia di aree a 2 livelli.
L'AREA 0 è detta Backbone AREA
Le AREE non 0 sono dette Regular AREA

Le regole ottimali per la realizzazione/suddivisione delle aree dovrebbero essere le seguenti:
- Un'area non dovrebbe avere più di 50 router.
- Un router non dovrebbe essere in più di tre aree.
- Ogni singolo router non dovrebbe avere più di 60 vicini

Nella gestione/studio dell'OSPF multi-area si identificano 4 tipi di router:
1) Internal router: i router che rimangono all'interno di una sola AREA (sia esse backbone o regular)
2) Backbone router: sono i router con almeno un'interfaccia all'interno dell'AREA
3) Area Border Routers (ABRs): sono i router che hanno un'interfaccia in AREA 0 ed una in un'altra AREA
4) Autonomous System Border Router (ASBR): sono i router collegati ad un'AREA ma che hanno anche un'interfaccia collegata ad una rete esterna (come internet). La ridistribuzione in OSPF multi-area si verifica quando un ASBR connette diversi domini di routing (ad es. EIGRP e OSPF) e li configura per scambiare e pubblicizzare le informazioni di routing tra tali domini di routing. Una route statica, (come una route predefinita), può anche essere ridistribuita come percorso esterno nel dominio di routing OSPF.

Vediamo come girano i pacchetti LSA all'interno del multi-area
a) LSA di tipo1: rimangono all'interno dell'area, verranno poi convertiti in LSA di tipo 3 dai router ABR e scambiati
b) LSA di tipo 2: esistono solo su reti con un DR per far conoscere anche agli altri router la topologia dell'area, e non viene mai propagato all'esterno dell'area
c) LSA di tipo 3: sono utilizzati dagli ABR per pubblicizzare le reti da altre aree. I percorsi recepiti vengono aggiunti alla tabella di routing senza effettuare nessun calcolo SPF completo.
d) LSA di tipo 4: sono utilizzati collettivamente per identificare un ASBR e pubblicizzare reti esterne. LSA di tipo 4 viene generato da un ABR solo quando esiste un ASBR all'interno di un'area. Un LSA di tipo 4 identifica l'ASBR e fornisce un percorso per raggiungerlo. Tutto il traffico destinato a una rete esterna richiede la conoscenza della tabella di routing dell'ASBR che ha originato i percorsi esterni.
e) LSA di tipo 5: descrivono percorsi verso reti esterne al dominio. Sono generati direttamente dall'ASBR e propagati a tutte le aree.

Dando il comando:
show ip route
show ipv6 route
otteniamo l'elenco della tabella di routing e la prima colonna ci indica come abbiamo appreso le rotte, se con OSPF (O), in modo statico (S), con EIGRP (D), se è la default route (*), se è inter-area (IA) o external-area (E1 o E2).
Ipotizzando solo di avere OSPF per apprendere le rotte e semplificando la lettura dell'output sopra citato, leggendo solo la prima colonna avremo che l'ordine per il calcolo della miglior rotta sarebbe:
C → O → O IA → O*E2

Se si vuole implementare OSPF multi-area, ci sono 4 passaggi da effettuare:

1) Raccogliere i requisiti e i parametri di rete
2) Definizione dei parametri OSPF:
   - Indirizzamento IP: modo in cui è possibile distribuire OSPF e quanto può evolvere la distribuzione OSPF
   - Aree OSPF: la divisione di una rete OSPF in aree riduce la dimensione LSDB e limita la propagazione degli aggiornamenti dello stato dei collegamenti quando la topologia cambia. I router che devono essere ABR e ASBR devono essere identificati, così come quegli ABR o ASBR che devono eseguire qualsiasi riepilogo o ridistribuzione.
   - Topologia di rete: collegamenti che connettono le apparecchiature di rete e appartengono a diverse aree OSPF. È importante per determinare i collegamenti primari e di backup.
3) Configurare l'implementazione OSPF
4) Verificare l'implementazione OSPF

Per vedere com'è organizzato il database di tutte le informazioni recepite dal router con OSPF diamo il comando (in privileged exec):
show ip ospf database
show ipv6 ospf database

9.2.2.6 Packet Tracer - Configuring Multiarea OSPFv2 Instructions.pdf
9.2.2.6 Packet Tracer - Configuring Multiarea OSPFv2.pka
9.2.2.7 Packet Tracer - Configuring Multiarea OSPFv3 Instructions.pdf
9.2.2.7 Packet Tracer - Configuring Multiarea OSPFv3.pka
9.2.2.8 Lab - Configuring Multi-area OSPFv2.pdf
9.2.2.9 Lab - Configuring Multi-area OSPFv3.pdf
9.3.1.1 Digital Trolleys Instructions.pdf

FINE CAPITOLO 9

10.0.1.2 DR and BDR Elections Instructions.pdf

OSPF gestisce 5 tipi di reti:
- Punto-punto: router interconnessi su un collegamento comune 1-a-1
- Broadcast multiaccess: router interconnessi su una rete Ethernet.
- No-broadcast multiaccess
- Punto-multipunto: router interconnessi in una topologia hub-and-spoke
- Virtual link: rete OSPF speciale utilizzata per interconnettere aree OSPF distanti all'area Backbone

Per impostare la priority nell'elezione del DR o del BDR utilizzare il comando
interface gigabitethernet 0/0
ip ospf priority 10
ipv6 ospf priority 10
exit
dove il valore varia da 0 a 255. Di default è impostato a 1, per cui se voglio assegnare sia DR che il BDR, al DR darò un valore ed al BDR un valore inferiore ma comunque superiore a 1.
D'altra parte se voglio che un router rimanga DROHTER posso assegnargli priority 0.
Se tutti i router sono a priority 0 diventerà DR quello con il RouterID più alto

Attenzione che se abbiamo intenzione di cambiare priority e propagarla tramite OSPF, dobbiamo dare sui router il comando (in privileged exec)
clear ipv ospf process
clear ipv6 ospf process
altrimenti come DR e BDR rimarranno impostati quelli precedentemente eletti

10.1.1.12 Packet Tracer - Determining the DR and BDR Instructions.pdf
10.1.1.12 Packet Tracer - Determining the DR and BDR.pka
10.1.1.13 Lab - Configuring OSPFv2 on a Multiaccess Network.pdf

Per propagare una default route, presente in un router ASBR, dare il comando sul router con la rotta:
ip route 0.0.0.0 0.0.0.0 10.88.88.2
ipv6 route ::/0 2001:DB8:FEED:1::2
router ospf 10
default-information originate
exit

10.1.2.5 Packet Tracer - Propagating a Default Route in OSPFv2 Instructions.pdf
10.1.2.5 Packet Tracer - Propagating a Default Route in OSPFv2.pka

Per variare i tempi di Hello e di Dead utilizzare i comandi
interface gigabitethernet 0/0
ip ospf hello-interval 5
ip ospf dead-time 20
ipv6 ospf hello-interval 5
ipv6 ospf dead-time 20
exit

Tenendo a nota che è bene mantenere il rapporto 1 a 4 tra hello e dead time
Per ripristinare i valori di default anteporre il comando **no** e non inserire alcun valore (es. **no ip ospf dead-time** oppure **no ipv6 ospf dead-time**)

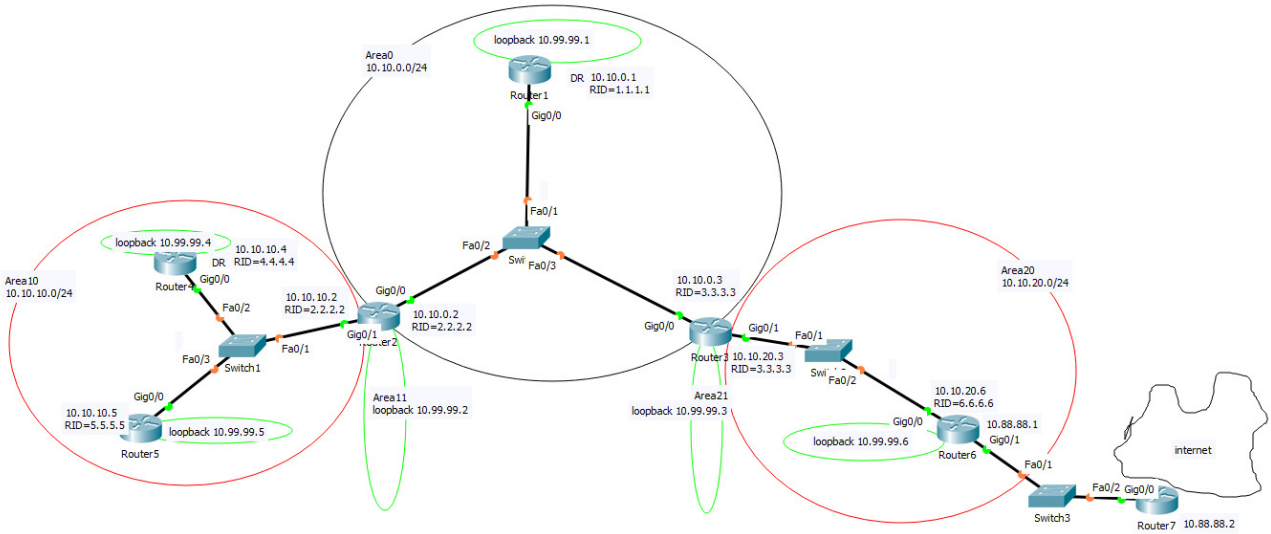
10.1.3.4 Packet Tracer - Configuring OSPF Advanced Features.pdf
10.1.3.4 Packet Tracer - Configuring OSPF Advanced Features.pka
10.1.3.5 Lab - Configuring OSPFv2 Advanced Features.pdf

I comandi più importanti da ricordarsi in fase di Troubleshooting dell'OSPF sono i seguenti:
show ip protocols
show ip ospf neighbors
show ip ospf interface serial 0/0/0
show ip ospf
show ip route ospf
show ipv6 protocols
show ipv6 ospf neighbors
show ipv6 ospf interface serial 0/0/0
show ipv6 ospf
show ipv6 route ospf

10.2.2.3 Packet Tracer - Troubleshooting Single-Area OSPFv2 Instructions.pdf
10.2.2.3 Packet Tracer - Troubleshooting Single-Area OSPFv2.pka
10.2.3.3 Lab - Troubleshooting Basic Single-Area OSPFv2 and OSPFv3.pdf
10.2.3.4 Lab - Troubleshooting Advanced Single-Area OSPFv2.pdf
10.2.4.3 Packet Tracer - Troubleshoot Multiarea OSPFv2.pdf
10.2.4.3 Packet Tracer - Troubleshoot Multiarea OSPFv2.pka
10.2.4.4 Packet Tracer - Troubleshoot Multiarea OSPFv3.pdf
10.2.4.4 Packet Tracer - Troubleshoot Multiarea OSPFv3.pka
10.2.4.5 Lab - Troubleshooting Multiarea OSPFv2 and OSPFv3.pdf
10.3.1.1 OSPF Troubleshooting Mastery Instructions.pdf
10.3.1.2 Packet Tracer - Skills Integration Challenge Instructions.pdf
10.3.1.2 Packet Tracer - Skills Integration Challenge.pka

Esercizio OSPF

SPECIFICHE: configurare i router come in figura e propagare le tabelle di routing tramite OSPFv4



---- ROUTER 1 ----

```
enable
configure terminal
hostname R1
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R1 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.10.0.1 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.1 255.255.255.255
no shutdown
exit
router ospf 10
router-id 1.1.1.1
network 10.10.0.1 0.0.0.0 area 0
network 10.99.99.1 0.0.0.0 area 0
exit
interface GigabitEthernet0/0
ip ospf priority 255
exit
copy running-config startup-config
```

---- ROUTER 2 ----

```
enable
configure terminal
hostname R2
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R2 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.10.0.2 255.255.255.0
no shutdown
exit
interface GigabitEthernet0/1
ip address 10.11.0.2 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.2 255.255.255.255
no shutdown
exit
router ospf 10
router-id 2.2.2.2
network 10.10.0.2 0.0.0.0 area 0
network 10.99.99.2 0.0.0.0 area 11
network 10.11.0.2 0.0.0.0 area 10
exit
exit
copy running-config startup-config
```

---- ROUTER 3 ----

```
enable
configure terminal
hostname R3
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R3 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.10.0.3 255.255.255.0
no shutdown
exit
interface GigabitEthernet0/1
ip address 10.10.20.3 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.3 255.255.255.255
no shutdown
exit
router ospf 10
router-id 3.3.3.3
network 10.10.0.3 0.0.0.0 area 0
network 10.99.99.3 0.0.0.0 area 21
network 10.10.20.3 0.0.0.0 area 20
exit
exit
copy running-config startup-config
```

---- ROUTER 4 ----

```
enable
configure terminal
hostname R4
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R4 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.11.10.4 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.4 255.255.255.255
no shutdown
exit
router ospf 10
router-id 4.4.4.4
network 10.11.10.4 0.0.0.0 area 10
network 10.99.99.4 0.0.0.0 area 10
exit
interface GigabitEthernet0/0
ip ospf priority 255
exit
copy running-config startup-config
```

---- ROUTER 5 ----

```
enable
configure terminal
hostname R5
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R5 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.11.10.5 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.5 255.255.255.255
no shutdown
exit
router ospf 10
router-id 5.5.5.5
network 10.11.10.5 0.0.0.0 area 10
network 10.99.99.5 0.0.0.0 area 10
exit
exit
copy running-config startup-config
```

---- ROUTER 6 ----

```
enable
configure terminal
hostname R6
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R6 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.10.20.6 255.255.255.0
no shutdown
exit
interface loopback 0
ip address 10.99.99.6 255.255.255.255
no shutdown
exit
router ospf 10
router-id 4.4.4.4
network 10.10.20.6 0.0.0.0 area 20
network 10.99.99.6 0.0.0.0 area 20
exit
interface GigabitEthernet0/1
ip address 10.88.88.1 255.255.255.252
no shutdown
exit
ip route 0.0.0.0 0.0.0.0 10.88.88.2
router ospf 10
default-information originate
exit
copy running-config startup-config
```

---- ROUTER 7 ----

```
enable
configure terminal
hostname R7
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R7 - Accesso consentito solo al personale autorizzato#
ip domain-name corso.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 10.88.88.2 255.255.255.252
no shutdown
exit
exit
copy running-config startup-config
```

FINE CAPITOLO 10

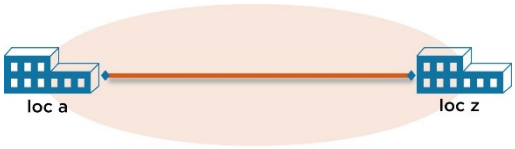
Modulo 4

CAPITOLO 1

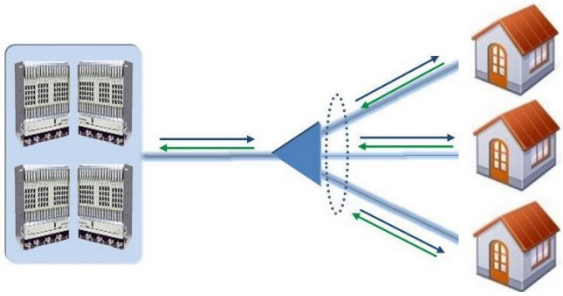
Vedremo come interconnettere tra loro le LAN, attraverso le reti WAN

1.0.1.2 Class Activity - Branching Out.pdf

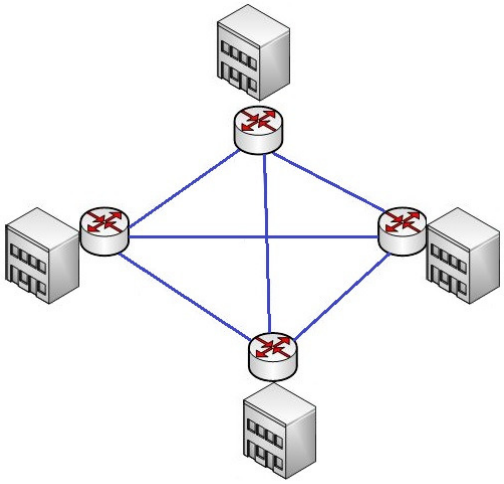
Le WAN sono di proprietà degli ISP.
Esistono 4 tipi di collegamenti WAN:



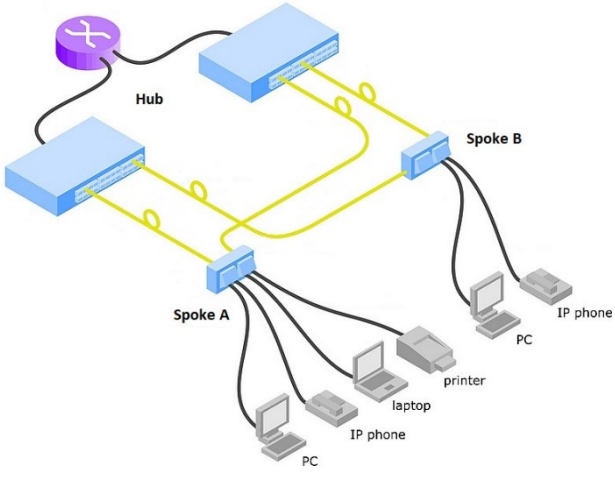
✓ Point-to-Point: coinvolge un servizio di trasporto Layer 2 attraverso la rete del fornitore di servizi. I pacchetti inviati da un sito vengono consegnati all'altro sito e viceversa. Una connessione point-to-point è trasparente per la rete del cliente, come se ci fosse un collegamento fisico diretto tra due endpoint.



✓ Hub-and-Spoke (point-to-multipoint): una singola interfaccia per l'hub può essere condivisa da tutti i circuiti dei raggi. (Uno degli svantaggi delle topologie hub-and-spoke è che tutta la comunicazione deve passare attraverso l'hub)



✓ Full Mesh: utilizza circuiti virtuali, qualsiasi sito può comunicare direttamente con qualsiasi altro sito. Lo svantaggio qui è il gran numero di circuiti virtuali che devono essere configurati e mantenuti.



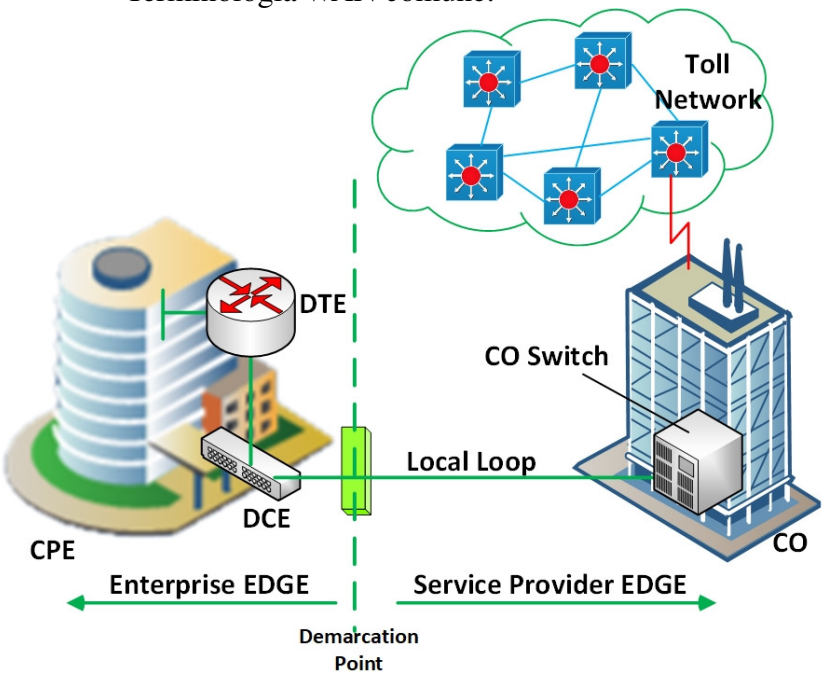
✓ Dual-Homed: due router hub sono dual-homed e collegati in modo ridondante a tre router spoke su una nuvola WAN. Lo svantaggio delle topologie dual-homed è che sono più costose da implementare rispetto alle topologie single-homed. Questo perché richiedono hardware di rete aggiuntivo, come router e switch aggiuntivi. Le topologie dual-homed sono anche più difficili da implementare perché richiedono configurazioni aggiuntive e più complesse. Tuttavia, il vantaggio delle topologie dual-homed è che offrono ridondanza di rete, bilanciamento del carico, elaborazione o elaborazione distribuita e possibilità di implementare connessioni di provider di servizi di backup.

Le operazioni WAN si concentrano principalmente sul livello fisico e sul livello di collegamento dati. Gli standard di accesso WAN descrivono in genere sia i metodi di consegna dello strato fisico che i requisiti del livello di collegamento dati. I requisiti del livello di collegamento dati includono indirizzamento fisico, controllo di flusso e incapsulamento.
Gli standard di accesso WAN sono definiti e gestiti da un certo numero di autorità riconosciute:

- Telecommunications Industry Association e Electronic Industries Alliance (TIA / EIA)
- Organizzazione internazionale per la standardizzazione (ISO)
- Istituto di ingegneri elettrici ed elettronici (IEEE)

I protocolli di Layer1 descrivono come fornire collegamenti elettrici, meccanici, operativi e funzionali ai servizi di un ISP.
I protocolli di Layer2 definiscono il modo in cui i dati vengono incapsulati per la trasmissione verso una posizione remota e i meccanismi per il trasferimento dei frame risultanti. Viene utilizzata una varietà di tecnologie diverse, come il protocollo PPP (Point-to-Point Protocol), Frame Relay e ATM. Alcuni di questi protocolli utilizzano lo stesso schema di base o un sottoinsieme del meccanismo HDLC (High-Level Data Link Control).
La maggior parte dei collegamenti WAN sono punto-punto. Per questo motivo, il campo indirizzo nel frame Layer2 non viene in genere utilizzato.

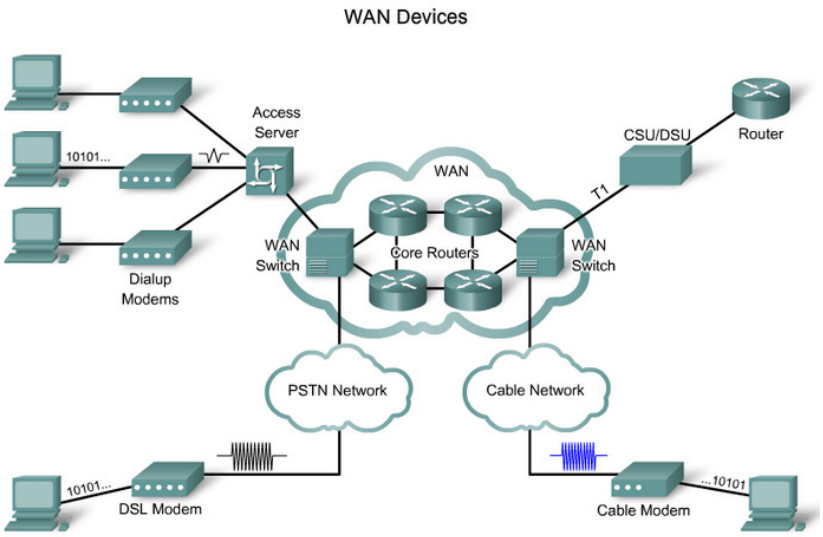
Terminologia WAN comune:



💻CPE (Customer Premises Equipment): è costituito dai dispositivi e dai cablaggi interni situati sul bordo aziendale che si collega a un collegamento carrier. Il sottoscrittore è proprietario del CPE o affitta il CPE dal fornitore di servizi.
💻DCE (Data Communications Equipment): chiamate anche apparecchiature di terminazione del circuito di dati, il DCE è costituito da dispositivi che inseriscono dati sul loop locale. Il DCE fornisce principalmente un'interfaccia per connettere gli abbonati a un collegamento di comunicazione WAN cloud.
💻DTE (Data Terminal Equipment): sono i dispositivi del cliente che trasmettono i dati da una LAN o da un computer host per la trasmissione sulla WAN. Il DTE si collega al loop locale attraverso il DCE.

- 💻 Demarcation Point: è un punto stabilito in un edificio o complesso per separare le attrezzature del cliente dalle apparecchiature del fornitore di servizi. Fisicamente, il punto di demarcazione è la scatola di giunzione dei cavi, situata nei locali del cliente, che collega il cablaggio CPE al loop locale. Di solito è posizionato per un facile accesso da parte di un tecnico. Il punto di demarcazione è il luogo in cui la responsabilità della connessione cambia da utente a fornitore di servizi.
  Es. per semplificare, e far comprendere il concetto, in casa ho l'FTTC se il modem è in affitto dall'ISP ed ho un problema di navigazione dovuto al modem rotto, il problema è dell'ISP, mentre se ho lo stesso problema ma il modem l'ho acquistato io, il problemaè mio. Ossia il demarcation point nel primo caso è il modemo, nel secondo caso è la presa telefonica.
- 💻 CO: (Central Office) è la struttura o l'edificio del fornitore di servizi locale che collega il CPE alla rete del fornitore
- 💻 Local Loop: cavo in rame o in fibra che collega il CPE al CO del fornitore di servizi. Il loop locale è talvolta chiamato anche "ultimo miglio".
- 💻 Toll network: le linee di comunicazione a lungo raggio, interamente digitali, in fibra ottica, switch, router e altre apparecchiature all'interno della rete di provider WAN.

WAN Devices:



✓ Modem dialup: sono considerati una tecnologia WAN legacy. Un modem voiceband converte (cioè, modula) i segnali digitali prodotti da un computer in frequenze vocali. Queste frequenze vengono poi trasmesse sulle linee analogiche della rete telefonica pubblica. Dall'altro lato della connessione, un altro modem converte i suoni in un segnale digitale (ad esempio, demodula) per l'input su un computer o una connessione di rete.

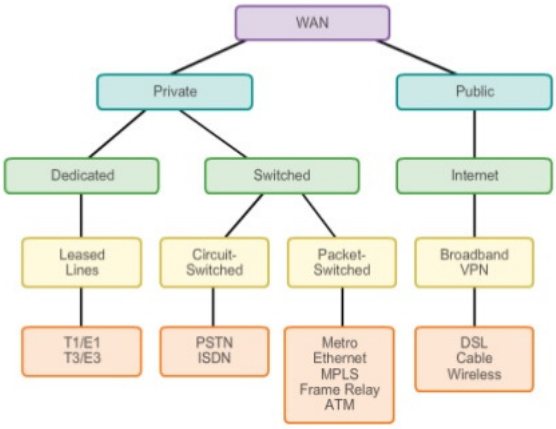
✓ Access server: controlla e coordina le comunicazioni dialup modem, dial-in e dial-out dell'utente. Considerata una tecnologia legacy, un server di accesso può avere una combinazione di interfacce analogiche e digitali e supportare centinaia di utenti simultanei.

- ✓ Modem a banda larga: un tipo di modem digitale utilizzato con DSL ad alta velocità o servizio Internet via cavo. Entrambi funzionano in modo simile al modem voiceband, ma utilizzano frequenze a banda larga e velocità di trasmissione più elevate.
- ✓ CSU/DSU: le linee affittate digitali richiedono una CSU e una DSU. Una CSU/DSU può essere un dispositivo separato come un modem o può essere un'interfaccia su un router. La CSU fornisce la terminazione per il segnale digitale e garantisce l'integrità della connessione attraverso la correzione degli errori e il monitoraggio della linea. La DSU converte i frame della linea in frame che la LAN può interpretare e viceversa.
- ✓ Switch WAN: dispositivo di rete multiporta utilizzato nelle reti dei provider di servizi. Questi dispositivi in genere commutano il traffico, come Frame Relay o ATM, e operano sul Layer2.
- ✓ Router: fornisce porte di interfaccia di accesso in rete e WAN utilizzate per connettersi alla rete del fornitore di servizi. Queste interfacce possono essere connessioni seriali, Ethernet o altre interfacce WAN. Con alcuni tipi di interfacce WAN, è necessario un dispositivo esterno, come una DSU/CSU o un modem (analogico, via cavo o DSL) per connettere il router al fornitore di servizi locale.
- ✓ Router core/Switch Multilayer: apparati che risiedono nella parte centrale o backbone della WAN, piuttosto che nella sua periferia. Per adempiere a questo ruolo, un router o uno switch multistrato deve essere in grado di supportare più interfacce di telecomunicazione della massima velocità utilizzata nel core WAN. Deve inoltre essere in grado di inoltrare i pacchetti IP alla massima velocità su tutte queste interfacce. Il router o lo switch multilayer devono supportare anche i protocolli di routing utilizzati nel core.
- ✓

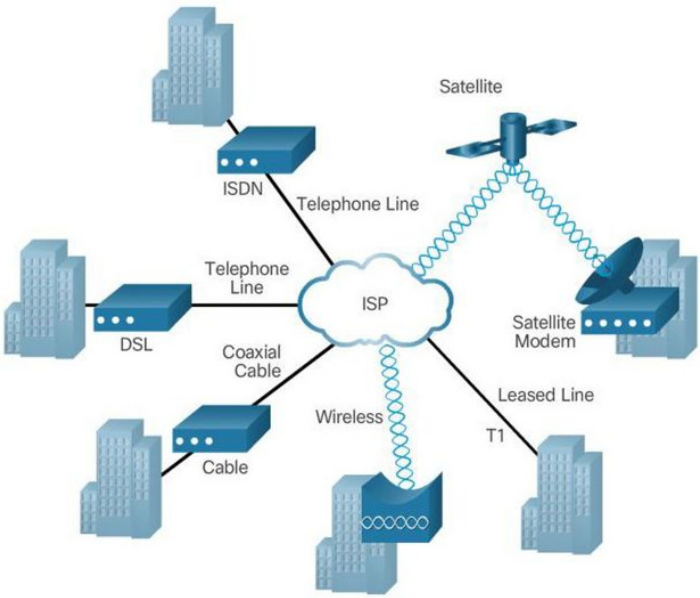
Nota: l'elenco precedente non è esaustivo e potrebbero essere necessari altri dispositivi, a seconda della tecnologia di accesso WAN scelta.

All'interno delle WAN vi sono reti:

- Circuit Switching: è quella rete che stabilisce un circuito (o canale) dedicato tra nodi e terminali prima che gli utenti possano comunicare. Lo switching stabilisce dinamicamente una connessione virtuale dedicata per voce o dati tra un mittente e un ricevitore. Prima che la comunicazione possa iniziare, è necessario stabilire la connessione attraverso la rete dell'ISP. I due tipi più comuni di circuit-switched WAN sono le reti PSTN ed ISDN.
- Packet Switching: divide i dati di traffico in pacchetti che vengono instradati su una rete condivisa. Le reti packet switching non richiedono la creazione di un circuito e consentono a molte coppie di nodi di comunicare sullo stesso canale.
  Gli switch in una rete packet switched determinano i collegamenti a cui i pacchetti devono essere inviati in base alle informazioni di indirizzamento in ciascun pacchetto. In questo tipo di collegamento abbiamo 2 varianti:
  - Connectionless: le informazioni complete sull'indirizzamento devono essere contenute in ciascun pacchetto. Ogni switch deve valutare l'indirizzo per determinare dove inviare il pacchetto.
  - Connection-oriented: la rete predetermina il percorso per un pacchetto e ogni pacchetto deve solo portare un identificatore. Lo switch determina la rotta in avanti, osservando l'identificatore nelle tabelle mantenute in memoria. L'insieme di voci nelle tabelle identifica una particolare rotta o circuito attraverso il sistema. Quando il circuito viene stabilito temporaneamente mentre un pacchetto lo attraversa, e poi si interrompe nuovamente, viene chiamato circuito virtuale (VC).

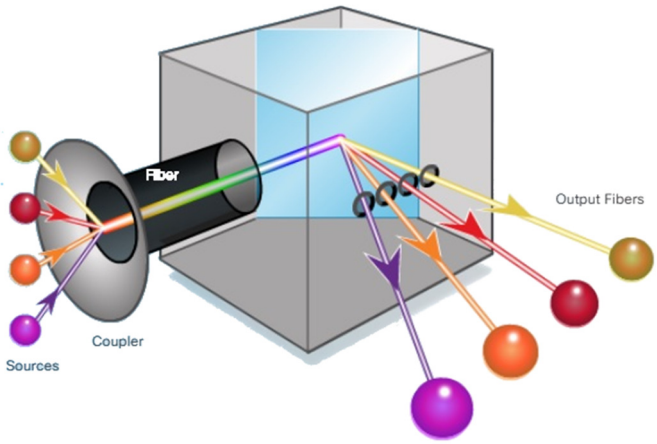


Come si vede dallo schema accanto, abbiamo vari tipi di accesso alle WAN e varie tecnologie (immagine sotto). La scelta di uno di questi influenzerà (anche di molto) il costo del nostro accesso alla rete ed è una parte importante della sua progettazione.



Le comunicazioni a lungo raggio sono di solito quelle connessioni tra gli ISP o tra filiali in aziende molto grandi.
Sono costituiti principalmente da supporti in fibra ottica a banda larga, che utilizzano lo standard Synchronous Optical Networking (SONET [standard americano]) o Synchronous Digital Hierarchy (SDH [standard europeo]), ma sono tendenzialmente simili.

Un nuovo sviluppo di fibre ottiche per comunicazioni a lungo raggio è chiamato dense wavelength division multiplexing (DWDM). DWDM moltiplica la quantità di larghezza di banda che un singolo filamento di fibra può supportare, come mostrato nella figura accanto.



Esistono molti modi in cui DWDM consente la comunicazione a lungo raggio:

- Abilita le comunicazioni bidirezionali su un filamento di fibra.
- Può multiplexare più di 80 diversi canali di dati (cioè lunghezze d'onda) su una singola fibra.
- Ogni canale è in grado di trasportare un segnale multiplexato da 10 Gb/s.
- Assegna i segnali ottici in ingresso a specifiche lunghezze d'onda della luce (cioè, frequenze).
- Può amplificare queste lunghezze d'onda per aumentare la potenza del segnale.
- Supporta gli standard SONET e SDH.

I circuiti DWDM sono utilizzati in tutti i moderni sistemi di cavi sottomarini per le comunicazioni e altri circuiti a lungo raggio.

WAN PRIVATE

Quando sono richieste connessioni dedicate permanenti, viene utilizzato un collegamento point-to-point per fornire un percorso di comunicazione WAN prestabilito dalla sede del cliente alla rete del provider. Le linee point-to-point sono solitamente noleggiate da un fornitore di servizi e sono chiamate linee dedicate.
Queste linee offrono vari
Vantaggi:

- Semplicità: i collegamenti di comunicazione point-to-point richiedono competenze minime per l'installazione e la manutenzione.
- Qualità: i collegamenti di comunicazione point-to-point offrono solitamente un'alta qualità del servizio, se dispongono di una larghezza di banda adeguata. La capacità dedicata rimuove la latenza o il jitter tra gli endpoint.
- Disponibilità - La disponibilità costante è essenziale per alcune applicazioni, come l'e-commerce. I collegamenti di comunicazione point-to-point forniscono una capacità dedicata permanente, necessaria per VoIP o Video over IP.

Svantaggi:

- Costo: i collegamenti punto a punto sono generalmente il tipo più costoso di accesso WAN. Il costo delle soluzioni di linee dedicate può diventare significativo quando vengono utilizzati per collegare molti siti a distanze crescenti. Inoltre, ogni endpoint richiede un'interfaccia sul router, che aumenta i costi delle apparecchiature.
- Flessibilità limitata: il traffico WAN è spesso variabile e le linee affittate hanno una capacità fissa, pertanto la larghezza di banda della linea corrisponde raramente alla necessità. Qualsiasi modifica alla linea dedicata richiede generalmente una visita in loco da parte del personale ISP per adeguare la capacità.

Quando non sono disponibili altre tecnologie WAN, potrebbe essere richiesta una tecnologia Dialup. L'accesso dialup è adatto quando sono necessari trasferimenti di dati intermittenti a basso volume.
La telefonia tradizionale utilizza un cavo in rame, chiamato loop local, per collegare il telefono nella sede dell'abbonato al CO (Central Office) dell'ISP.
Il segnale sul loop local durante una chiamata è un segnale elettronico che varia in modo continuo che è una traduzione della voce dell'abbonato in un segnale analogico.
I loop local tradizionali possono trasportare dati di computer binari attraverso la rete telefonica tramite un modem. Il modem modula i dati binari in un segnale analogico alla sorgente e demodula il segnale analogico in dati binari nella destinazione. Le caratteristiche fisiche del loop local e la sua connessione al PSTN limitano la velocità del segnale a meno di 56 kb/s.
Vantaggi:

1) Semplicità
2) Disponibilità
3) Bassi costi

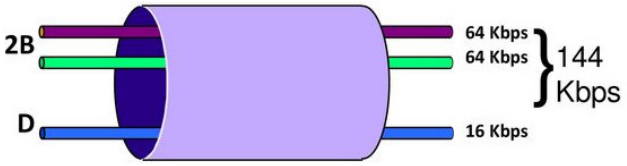
Svantaggi:

1) Basse velocità di trasmissione dati
2) Tempo di connessione relativamente lungo

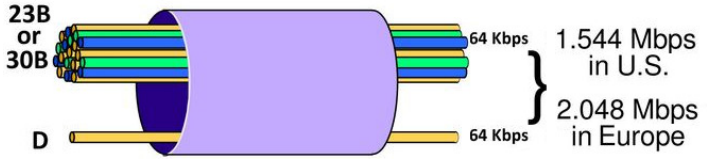
La rete ISDN (Integrated Services Digital Network) è una tecnologia circuit-switching che consente al loop local di una rete PSTN di trasportare segnali digitali, con conseguente maggiore capacità di connessione. ISDN modifica le connessioni interne della PSTN dal trasferimento di segnali analogici a segnali digitali time-division-multiplexed (TDM). TDM consente a due o più segnali, o flussi di bit, di essere trasferiti come sottocanali in un canale di comunicazione. I segnali sembrano trasferirsi simultaneamente; ma fisicamente, i segnali stanno prendendo il turno sul canale.

Vi sono 2 tipo di interfacce ISDN:

- Basic Rate Interface (BRI): è destinato alla casa e alle piccole imprese e offre due canali di portanti a 64 kb/s (B) per il trasporto di voce e dati e un canale delta a 16 kb/s (D) per segnalazione, configurazione chiamata e altri scopi.



  Ha un tempo di impostazione della chiamata inferiore a un secondo e il canale B da 64 kb/s offre una capacità maggiore rispetto a un collegamento modem analogico. Se è richiesta una maggiore capacità, è possibile attivare un secondo canale B per fornire un totale di 128 kb/s.
- Primary Rate Interface (PRI): è un'ISDN disponibile anche ad installazioni più grandi. In America offre 23 canali B con 64 kb/s e un canale D con 64 kb/s per un bitrate totale fino a 1,544 Mb/s. In Europa, Australia e altre parti del mondo fornisce 30 canali B e un canale D, per un bitrate totale fino a 2.048 Mb/s, compreso il sovraccarico di sincronizzazione. È possibile collegare più canali B tra due endpoint. Ciò consente connessioni di videoconferenza e connessioni a larghezza di banda elevata senza latenza.



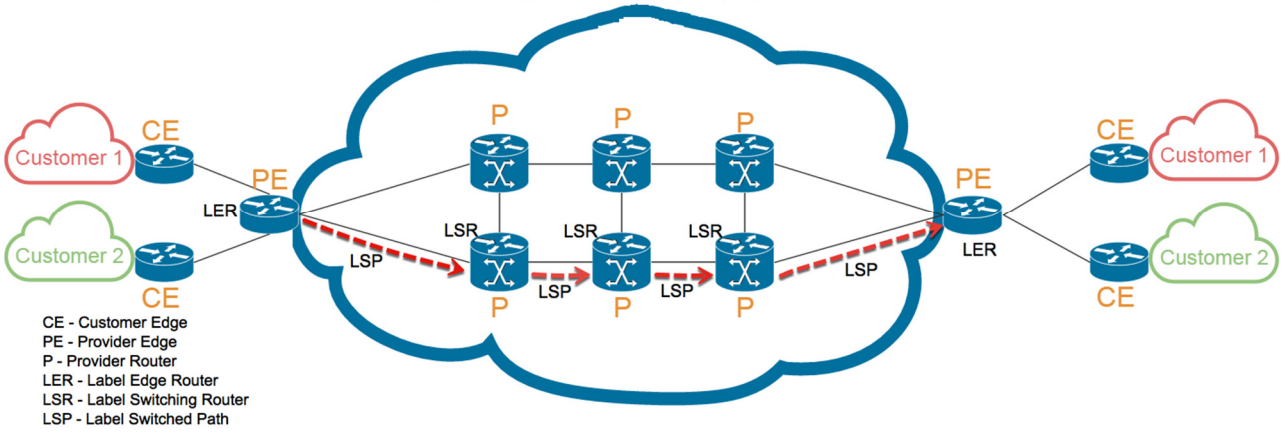
Frame Relay è una semplice tecnologia WAN Layer 2 non-broadcast multi-access (NBMA) utilizzata per interconnettere LAN aziendali. È possibile utilizzare un'unica interfaccia router per connettersi a più siti tramite PVC (private virtual circle). I PVC sono utilizzati per trasportare traffico voce e dati tra una fonte e una destinazione e supportano velocità di trasmissione dati fino a 4 Mb/s.
Frame Relay crea PVC che sono identificati in modo univoco da un data-link connection identifier (DLCI). I PVC e DLCI assicurano la comunicazione bidirezionale da un dispositivo DTE a un altro.

La tecnologia ATM (Asynchronous Transfer Mode) è costruito su un'architettura basata su celle piuttosto che su un'architettura basata su frame. Le celle ATM hanno sempre una lunghezza fissa di 53 byte. La cella ATM contiene un'intestazione ATM a 5 byte seguita da 48 byte di payload ATM. Piccole celle a lunghezza fissa sono adatte per trasportare traffico voce e video perché questo traffico è intollerante ai ritardi.
Una linea ATM tipica ha bisogno di una larghezza di banda quasi del 20% maggiore rispetto a Frame Relay per trasportare lo stesso volume di dati di livello di rete.
ATM è stato progettato per essere estremamente scalabile e per supportare velocità di collegamento tra T1/E1 e OC-12 (622 Mb/s) e più veloce.

I nuovi standard Ethernet che utilizzano cavi in fibra ottica hanno reso Ethernet un'opzione di accesso WAN ragionevole. Ad esempio, lo standard IEEE 1000BASE-LX supporta lunghezze del cavo in fibra ottica di 5 km, mentre lo standard IEEE 1000BASE-ZX supporta cavi lunghi fino a 70 km.
Il servizio Ethernet WAN può assumere molti nomi, tra cui Metropolitan Ethernet (MetroE), Ethernet su MPLS (EoMPLS) e Virtual Private LAN Service (VPLS).
Vantaggi:

- Costi e amministrazione ridotti
- Facile integrazione con le reti esistenti
- Maggiore produttività aziendale

Multiprotocol Label Switching (MPLS) è una tecnologia WAN multiprotocollo ad alte prestazioni che indirizza i dati da un router all'altro. MPLS si basa su etichette a percorso breve anziché su indirizzi di rete IP.
È multiprotocollo, cioè ha la capacità di trasportare qualsiasi carico utile incluso il traffico IPv4, IPv6, Ethernet, ATM, DSL e Frame Relay. Usa etichette che dicono al router cosa fare con un pacchetto. Le etichette identificano i percorsi tra router distanti piuttosto che endpoint e mentre MPLS instrada effettivamente i pacchetti IPv4 e IPv6, tutto il resto può essere instradato diversamente.
MPLS è principalmente una tecnologia WAN fornita dagli ISP



Very small aperture terminal (VSAT): è una soluzione che crea una WAN privata utilizzando le comunicazioni satellitari, tendenzialmente nelle postazioni in cui non è possibile reggiungere la struttura con i cavi di rame o con la fibra ottica. Un VSAT è una piccola parabola simile a quella usata per Internet e TV domestici.
Nello specifico, un router si connette a una parabola satellitare puntata sul satellite di un fornitore di servizi. Questo satellite è in orbita geosincrona nello spazio. I segnali devono percorrere circa 35.786 chilometri verso il satellite e ritorno, e questo implica un importante delay nella creazione del canale di trasmissione.

WAN Pubbliche

DSL: è una tecnologia di connessione sempre attiva che utilizza linee telefoniche a doppino telefonico esistenti per trasportare dati a elevata larghezza di banda e fornisce servizi IP agli abbonati. Un modem DSL converte un segnale Ethernet dal dispositivo dell'utente a un segnale DSL, che viene trasmesso al CO.
Più linee di sottoscrizione DSL sono multiplexate in un unico collegamento ad alta capacità utilizzando un DSL access multiplexer (DSLAM) [che si trova in sede all'ISP]. I DSLAM incorporano la tecnologia TDM per aggregare molte linee di abbonati in un singolo supporto, generalmente una connessione T3 (DS3).

Coaxial cable: negli stati uniti è molto utilizzato per distribuire segnali televisivi. I modem via cavo forniscono una connessione sempre attiva e una semplice installazione. Un abbonato collega un computer o un router LAN al modem via cavo, che converte i segnali digitali nelle frequenze a banda larga utilizzate per la trasmissione su una rete televisiva via cavo.

Wireless: utilizza lo spettro radio senza licenza per inviare e ricevere dati. Lo spettro senza licenza è accessibile a chiunque abbia un router wireless e una tecnologia wireless nel dispositivo che sta utilizzando.
Attualmente vi sono vari accessi alla rete wireless:

- Wi-Fi municipale:
- WiMAX (Worldwide Interoperability for Microwave Access): è descritta nello standard IEEE 802.16. Offre un servizio a banda larga ad alta velocità con accesso wireless e offre un'ampia copertura come una rete di telefoni cellulari piuttosto che attraverso piccoli hotspot Wi-Fi. Funziona in modo simile al Wi-Fi, ma a velocità più elevate, a distanze maggiori e per un numero maggiore di utenti.
- VSAT: utilizzato tipicamente dagli utenti rurali in cui non sono disponibili cavi e DSL.

3G/4G Cellular: molti utenti con smartphone e tablet possono utilizzare i dati della rete cellulare per inviare email, navigare sul Web, scaricare app e guardare video. È un'abbreviazione per accesso cellulare di 3a generazione e 4a generazione. Queste tecnologie supportano l'accesso a Internet senza fili. Evoluzione a lungo termine (LTE): si riferisce a una tecnologia più recente e più veloce ed è considerata parte della tecnologia di quarta generazione (4G).

Per risolvere i problemi di sicurezza, i servizi a banda larga forniscono funzionalità per l'utilizzo delle connessioni VPN (Virtual Private Network) a un dispositivo di rete che accetta connessioni VPN, che di solito si trova nel sito aziendale.
Una VPN è una connessione crittografata tra reti private su una rete pubblica.
Vantaggi:

- Risparmio sui costi
- Sicurezza
- Scalabilità
- Compatibilità con la tecnologia a banda larga

Esistono 2 tipi di accessi VPN:

- Site-to-Site: connettono tra loro intere reti.
- Remote-Access (in OpenVPN vengono chiamati roadwarrior): consentono a singoli host, quali telelavoratori, utenti mobili ed utenti extranet, di accedere in modo sicuro a una rete aziendale su Internet.

1.2.4.3 Lab - Researching WAN Technologies.pdf
1.3.1.1 Class Activity - WAN Device Modules.pdf

FINE CAPITOLO 1

2.0.1.2 Class Activity - PPP Persuasion.pdf

Un tipo comune di connessioni WAN è la connessione point-to-point.
Una connessione point-to-point LAN-to-WAN viene anche definita connessione seriale o connessione a linee dedicate. Questo perché le linee sono noleggiate da un ISP e sono dedicate all'uso da parte dell'azienda che affitta le linee. Le aziende pagano per una connessione continua tra due siti remoti e la linea è continuamente attiva e disponibile.
Per una linea point-to-point, l'ISP dedica risorse specifiche per una linea che viene affittata dal cliente.

Tipo di linea	Bit Rate Capacity
56	56 kb/s
64	64 kb/s
T1	1,544 Mb/s
E1	2,048 Mb/s
J1	1,544 Mb/s
E3	34,368 Mb/s
T3	44,736 Mb/s
OC-1	51,84 Mb/s
OC-3	155,52 Mb/s
OC-9	466,56 Mb/s
OC-12	622,08 Mb/s
OC-18	933,12 Mb/s
OC-24	1,244 Gb/s
OC-36	1,866 Gb/s
OC-48	2,488 Gb/s
OC-96	4,976 Gb/s
OC-192	9,954 Gb/s
OC-768	39,813 Gb/s

Bandwidth (larghezza di banda): si riferisce alla velocità con cui i dati vengono trasferiti sul collegamento di comunicazione. La tecnologia portante sottostante determinerà la larghezza di banda disponibile (vedi tabella accanto).
Le velocità di trasmissione OC sono un insieme di specifiche standardizzate per la trasmissione di segnali digitali trasportati su reti in fibra ottica SONET. La designazione utilizza OC, seguito da un valore intero che rappresenta la velocità di trasmissione di base di 51,84 Mb/s
Nota: E1 (2,048 Mb/s) ed E3 (34,368 Mb/s) sono standard europei come T1 e T3, ma con diverse larghezze di banda e strutture di frame.

Su ciascuna connessione WAN, i dati vengono incapsulati in frame prima di attraversare il collegamento WAN. Per garantire che venga utilizzato il protocollo corretto, è necessario configurare il tipo di incapsulamento Layer 2 appropriato. La scelta del protocollo dipende dalla tecnologia WAN e dall'apparecchiatura di comunicazione.
Questi protocolli possono essere:

- ✓ HDLC: è il tipo di incapsulamento predefinito sulle connessioni punto-punto CISCO. HDLC è ora la base per il PPP sincrono utilizzato da molti server per connettersi a una WAN, più comunemente Internet.
- ✓ PPP: fornisce connessioni da router a router e da host a rete su connessioni synchronous e asynchronous. PPP funziona con diversi protocolli di livello di rete, come IPv4 e IPv6. PPP si basa sul protocollo di incapsulamento HDLC, ma ha anche meccanismi di sicurezza integrati come PAP e CHAP.
- ✓ SLIP (Serial Line Internet Protocol): è un protocollo standard per le connessioni seriali punto-punto tramite TCP / IP.
- ✓ X.25/LAPB (Link Access Procedure Balanced): è uno standard ITU-T che definisce come vengono mantenute le connessioni tra un DTE e DCE per l'accesso al terminale remoto e le comunicazioni informatiche nelle reti di dati pubbliche. X.25 specifica LAPB, un protocollo del livello di collegamento dati. X.25 è un predecessore di Frame Relay.
- ✓ Frame Relay: eun protocollo standard, switched, a livello di collegamento dati che gestisce più circuiti virtuali. Frame Relay elimina alcuni dei lunghi processi (come la correzione degli errori e il controllo del flusso) impiegati in X.25.
- ✓ ATM: è lo standard internazionale per di connessione per i dispositivi che inviano più tipi di servizi. Le celle a lunghezza fissa consentono l'elaborazione nell'hardware; in tal modo, riducendo i ritardi di transito. ATM sfrutta i mezzi di trasmissione ad alta velocità come E3, SONET e T3.

A noi interesseranno HDLC e PPP

HDLC

È un protocollo a livello di collegamento dati sincrono bit-oriented sviluppato dall'ISO.
Lo standard attuale per HDLC è ISO 13239. HDLC è stato sviluppato dallo standard SDLC (Synchronous Data Link Control).
Offre sia un servizio orientato alla connessione che un servizio senza connessione.
Utilizza la trasmissione seriale sincrona per fornire comunicazioni prive di errori tra due punti. HDLC definisce una struttura di frame Layer 2 che consente il controllo del flusso e il controllo degli errori attraverso l'uso di riconoscimenti. Ogni frame ha lo stesso formato, sia che si tratti di un frame di dati o di un frame di controllo.
Quando i frame vengono trasmessi su collegamenti sincroni o asincroni, questi collegamenti non hanno alcun meccanismo per contrassegnare l'inizio o la fine dei frame. Per questo motivo, HDLC utilizza un delimitatore di frame, o flag, per contrassegnare l'inizio e la fine di ciascun frame.

HDLC

Cisco ha sviluppato un'estensione del protocollo HLDC per risolvere l'impossibilità di fornire supporto multiprotocollo. Sebbene Cisco HLDC (noto anche come cHDLC) sia proprietario, Cisco ha consentito a molti altri produttori di apparecchiature di rete di implementarlo. I frame Cisco HDLC contengono un campo per identificare il protocollo di rete che viene incapsulato. La figura confronta HLDC standard con Cisco HLDC.

Cisco HDLC

Vediamo come configurarle HDLC:

interface s0/0/0
encapsulation hdlc

```
Router#show interfaces s0/0
Serial 0 is up, line protocol is up
  Hardware is MCI Serial
  Internet address is 131.108.156.98, subnet mask is
255.255.255.240
  MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely
255/255, load 1/255
  Encapsulation HDLC, loopback not set, keepalive set
(10 sec)
```

È possibile verificarne la configurazione come si vede qui accanto.

Il comando restituisce uno dei sei possibili stati seguenti:

1. La seriale è attiva, il protocollo di linea è attivo (OK)
2. Seriale è giù, il protocollo di linea è inattivo (KO)
3. La seriale è attiva, il protocollo di linea è inattivo (KO)
4. La seriale è attiva, il protocollo di linea è attivo (in loop) (KO)
5. La seriale è attiva, il protocollo di linea è inattivo (disabilitato) (KO)
6. La seriale è amministrativamente inattivo, il protocollo di linea è inattivo (KO)

Come si può notare, gli ultimi 5 stati sono definiti problematici. Di seguito una tabella che indica i problemi che ne derivano e come risolverli

Status Line	Possible Condition	Problem / Solution
Serial x is up, line protocol is up	This is the proper status line condition.	No action is required.
Serial x is down, line protocol is down (DTE mode)	The router is not sensing a carrier detect (CD) signal, which means the CD is not active. A WAN carrier service provider problem has occurred, which means the line is down or is not connected to CSU/DSU. Cabling is faulty or incorrect. Hardware failure has occurred (CSU/DSU).	1. Check the LEDs on the CSU/DSU to see whether the CD is active, or insert a breakout box on the line to check for the CD signal. 2. Verify that the proper cable and interface are being used by looking at the hardware installation documentation. 3. Insert a breakout box and check all control leads. 4. Contact the leased-line or other carrier service to see whether there is a problem. 5. Swap faulty parts. 6. If faulty router hardware is suspected, change the serial line to another port. If the connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DTE mode)	A local or remote router is misconfigured. Keepalives are not being sent by the remote router. A leased-line or other carrier service problem has occurred, which means a noisy line or misconfigured or failed switch. A timing problem has occurred on the cable, which means serial clock transmit external (SCTE) is not set on CSU/DSU. SCTE is designed to compensate for clock phase shift on long cables. When the DCE device uses SCTE instead of its internal clock to sample data from the DTE, it is better able to sample the data without error even if there is a phase shift in the cable. A local or remote CSU/DSU has failed. Router hardware, which could be either local or remote, has failed.	1. Put the modem, CSU, or DSU in local loopback mode and use the **show interfaces serial** command to determine whether the line protocol comes up. If the line protocol comes up, a WAN carrier service provider problem or a failed remote router is the likely problem. 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify all cabling. Make certain that the cable is attached to the correct interface, the correct CSU/DSU, and the correct WAN carrier service provider network termination point. Use the **show controllers** exec command to determine which cable is attached to which interface. 4. Enable the **debug serial interface** exec command. 5. If the line protocol does not come up in local loopback mode, and if the output of the **debug serial interface** exec command shows that the keepalive counter is not incrementing, a router hardware problem is likely. Swap the router interface hardware. 6. If the line protocol comes up and the keepalive counter increments, the problem is not in the local router. 7. If faulty router hardware is suspected, change the serial line to an unused port. If the connection comes up, the previously connected interface has a problem.
Serial x is up, line protocol is down (DCE mode)	The **clockrate** interface configuration command is missing. The DTE device does not support or is not set up for SCTE mode (terminal timing). The remote CSU or DSU has failed.	1. Add the **clockrate** interface configuration command on the serial interface. Syntax: **clockrate** *bps* Syntax Description: *bps* - Desired clock rate in bits per second: 1200, 2400, 4800, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 250000, 500000, 800000, 1000000, 1300000, 2000000, 4000000, or 8000000 2. If the problem appears to be on the remote end, repeat Step 1 on the remote modem, CSU, or DSU. 3. Verify that the correct cable is being used. 4. If the line protocol is still down, there is a possible hardware failure or cabling problem. Insert a breakout box and observe leads. 5. Replace faulty parts as necessary.
Serial x is up, line protocol is up (looped)	A loop exists in the circuit. The sequence number in the keepalive packet changes to a random number when a loop is initially detected. If the same random number is returned over the link, a loop exists.	1. Use the **show running-config** privileged exec command to look for any **loopback** interface configuration command entries. 2. If there is a **loopback** interface configuration command entry, use the **no loopback** interface configuration command to remove the loop. 3. If there is no **loopback** interface configuration command, examine the CSU/DSU to determine whether they are configured in manual loopback mode. If they are, disable manual loopback. 4. After disabling loopback mode on the CSU/DSU, reset the CSU/DSU, and inspect the line status. If the line protocol comes up, no other action is needed. 5. If upon inspection, the CSU or DSU cannot be manually set, then contact the leased-line or other carrier service for line troubleshooting assistance.
Serial x is up, line protocol is down (disabled)	A high error rate has occurred due to a WAN service provider problem. A CSU or DSU hardware problem has occurred. Router hardware (interface) is bad.	1. Troubleshoot the line with a serial analyzer and breakout box. Look for toggling CTS and DSR signals. 2. Loop CSU/DSU (DTE loop). If the problem continues, it is likely that there is a hardware problem. If the problem does not continue, it is likely that there is a WAN service provider problem. 3. Swap out bad hardware as required (CSU, DSU, switch, local, or remote router).
Serial x is administratively down, line protocol is down	The router configuration includes the **shutdown** interface configuration command. A duplicate IP address exists.	1. Check the router configuration for the **shutdown** command. 2. Use the **no shutdown** interface configuration command to remove the **shutdown** command. 3. Verify that there are no identical IP addresses using the **show running-config** privileged exec command or the **show interfaces** exec command. 4. If there are duplicate addresses, resolve the conflict by changing one of the IP addresses.

Il comando
show controllers serial 0/0/0
è un altro strumento diagnostico importante.

```
Router#show controllers serial 0/0
Interface Serial0/0
Hardware is PowerQUICC MPC860
DTE V.35 TX and RX clocks detected.
idb at 0x81414E2C, driver data structure at 0x8141753C
```

L'output indica lo stato dei canali di interfaccia e se un cavo è collegato all'interfaccia. Nella figura, l'interfaccia seriale 0/0/0 ha un cavo V.35 DCE collegato.
Se l'uscita dell'interfaccia viene visualizzata come "UNKNOWN", il problema probabile è un cavo collegato in modo non corretto.

2.1.2.5 Packet Tracer - Troubleshooting Serial Interfaces.pdf
2.1.2.5 Packet Tracer - Troubleshooting Serial Interfaces.pka

PPP

HDLC è il metodo di incapsulamento seriale predefinito quando si collegano due router Cisco. Tuttavia, quando è necessario connettersi a un router non Cisco, è necessario utilizzare l'incapsulamento PPP. L'incapsulamento PPP è stato accuratamente progettato per mantenere la compatibilità con l'hardware di supporto più comunemente utilizzato. PPP incapsula i frame di dati per la trasmissione su collegamenti fisici di Layer 2. Stabilisce una connessione diretta utilizzando cavi seriali, linee telefoniche, linee principali, telefoni cellulari, collegamenti radio specializzati o collegamenti in fibra ottica.

PPP contiene tre componenti principali:

- Framing HDLC: per il trasporto di pacchetti multiprotocollo su collegamenti point-to-point.
- Extensible Link Control Protocol (LCP): per stabilire, configurare e testare la connessione del collegamento dati.
- Family of Network Control Protocols (NCPs): per stabilire e configurare diversi protocolli di livello di rete. PPP consente l'uso simultaneo di più protocolli di livello di rete. Gli NCPs più comuni sono IPv4 Control Protocol e IPv6 Control Protocol.

Ci sono molti vantaggi nell'usare il PPP, incluso il fatto che non è proprietario.
PPP include molte funzionalità non disponibili in HDLC:

- LQM (link quality management feature): può essere configurato con la percentuale di qualità di comando ppp dell'interfaccia. Se la percentuale di errore scende al di sotto della soglia configurata, il collegamento viene rimosso e i pacchetti vengono reindirizzati o eliminati.
- Supporta l'autenticazione PAP e CHAP.

L'architettura do PPP è layered (a livelli).
A livello fisico, è possibile configurare PPP su un intervallo di interfacce. L'unico requisito assoluto imposto da PPP è un full-duplex circuit, che può funzionare in modalità bit-seriale sincrona o asincrona.
Gli standard del livello fisico sono trasparenti ai frame del livello di collegamento PPP. PPP non impone alcuna restrizione sulla velocità di trasmissione.
La maggior parte del lavoro svolto da PPP avviene sul collegamento dati e sui livelli di rete, da LCP e NCP.

LCP funziona all'interno del livello di collegamento dati e ha un ruolo nello stabilire, configurare e testare la connessione del collegamento dati. Stabilisce il collegamento point-to-point, negozia inoltre e imposta le opzioni di controllo sul collegamento dati WAN, che sono gestite dagli NCP.

LCP fornisce la configurazione automatica delle interfacce a ciascuna estremità:

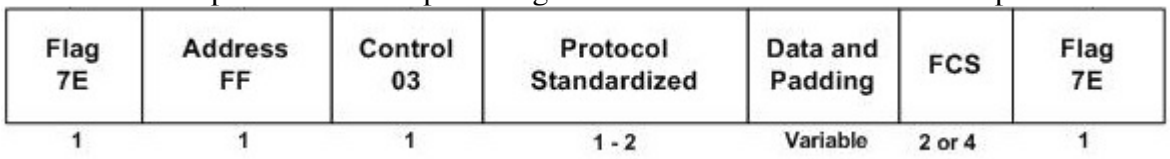
- Gestire i vari limiti sulla dimensione del pacchetto.
- Rilevazione di errori di errate configurazioni comuni.
- Terminare il collegamento.
- Determinare quando un collegamento funziona correttamente o quando non funziona.
- Dopo aver stabilito il collegamento, PPP usa anche LCP per concordare automaticamente i formati di incapsulamento come l'autenticazione, la compressione e il rilevamento degli errori.

PPP consente a più protocolli di livello di rete di operare sullo stesso collegamento di comunicazione. Per ogni protocollo di livello di rete utilizzato, PPP utilizza un NCP separato.

Valore (hex)	Cosa fa il protocollo
8021	Internet Protocol (IPv4) Protocollo di controllo
8057	Internet Protocol (IPv6) Protocollo di controllo
8023	OSI Protocollo di controllo livello rete
8029	AppleTalk Protocollo di controllo
802b	Novell IPX Protocollo di controllo
c021	Protocollo di controllo del collegamento
c023	Protocollo di autenticazione Password
c223	test del protocollo di autenticazione handshake

Gli NCP includono campi funzionali contenenti codici standardizzati per indicare il protocollo del livello di rete incapsulato da PPP (vedi tabella accanto).
Ogni NCP gestisce le esigenze specifiche richieste dai rispettivi protocolli del livello di rete. I vari componenti NCP incapsulano e negoziano opzioni per più protocolli di livello di rete.

Un frame PPP è composto da sei campi. Le seguenti descrizioni riassumono i campi del frame PPP:



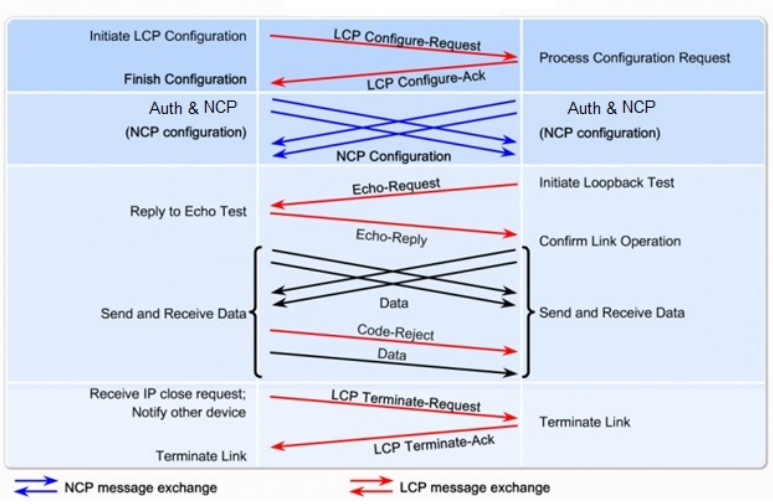
- Flag - 1 singolo byte che indica l'inizio o la fine di un frame. Il campo Flag è costituito dalla sequenza binaria 01111110.
- Indirizzo - 1 singolo byte che contiene la sequenza binaria 11111111, l'indirizzo di trasmissione standard. PPP non assegna indirizzi di stazione individuali.
- Controllo: 1 singolo byte che contiene la sequenza binaria 00000011, che richiede la trasmissione di dati utente in una cornice non sincronizzata.
- Protocollo: 2 byte che identificano il protocollo incapsulato nel campo di informazioni del frame. Il campo Protocollo a 2 byte identifica il protocollo del payload PPP.
- Dati: 0 o più byte che contengono il datagramma per il protocollo specificato nel campo del protocollo.
- Frame Check Sequence (FCS) - Normalmente 16 bit (2 byte). Se il calcolo del ricevitore dell'FCS non corrisponde all'FCS nel frame PPP, il frame PPP viene scartato in modo silenzioso.

Gli LCP possono negoziare modifiche alla struttura del frame PPP standard. I frame modificati, tuttavia, sono sempre distinguibili dai frame standard.

Per stabilire una sessione PPP vi sono 3 fasi:

1) Stabilimento e negoziazione della configurazione del link: LCP deve prima aprire la connessione e negoziare le opzioni di configurazione. Questa fase è completa quando il router ricevente invia un frame di conferma della configurazione al router che avvia la connessione.
2) LQM (opzionale): LCP verifica il collegamento per determinare se la qualità del collegamento è sufficiente per richiamare i protocolli del livello di rete. L'LCP può ritardare la trasmissione delle informazioni sul protocollo di livello di rete fino al completamento di questa fase.
3) Network layer protocol configuration negotiation: dopo che l'LCP ha terminato la fase di determinazione della qualità del collegamento, il dispositivo NCP appropriato, può configurare separatamente i protocolli del livello di rete e portarli verso l'alto e rimuoverli in qualsiasi momento. Se l'LCP chiude il collegamento, informa i protocolli del livello di rete in modo che possano intraprendere le azioni appropriate. Il collegamento rimane configurato per le comunicazioni fino a quando i frame LCP o NCP espliciti chiudono il collegamento o fino a quando si verifica qualche evento esterno

L'operazione LCP include le disposizioni per la creazione del collegamento, la manutenzione del collegamento e la terminazione del collegamento. L'operazione LCP utilizza tre classi di frame LCP per eseguire il lavoro di ciascuna fase LCP:



- Link-establishment frames: stabiliscono e configurano un link. Questa fase deve essere completata correttamente, prima che sia possibile scambiare qualsiasi pacchetto di livello di rete. Qui vi è anche la NCP configuration.
- Link-maintenance frames: gestiscono e eseguono il debug di un link. LCP può utilizzare i messaggi per fornire feedback e testare il collegamento.

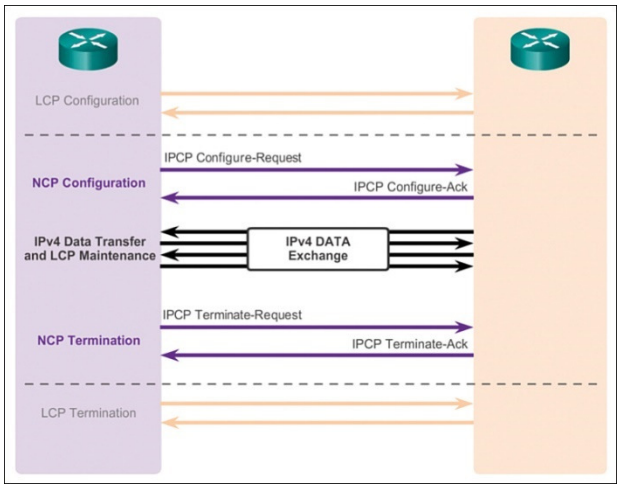
1. Link Termination: LCP termina il collegamento, NCP termina solo il livello di rete e il collegamento NCP. Il collegamento rimane aperto finché l'LCP non lo termina. Se l'LCP termina il collegamento prima del NCP, anche la sessione NCP viene chiusa.

PPP può essere configurato per supportare varie funzioni opzionali:

- ✓ Autenticazione usando PAP o CHAP.
- ✓ Compressione utilizzando Stacker o Predictor.
- ✓ Multilink che combina due o più canali per aumentare il bandwidth della WAN.

Dopo che l'LCP ha configurato e autenticato il collegamento di base, viene richiamato l'NCP appropriato per completare la configurazione specifica del protocollo del livello di rete utilizzato. Quando l'NCP ha configurato correttamente il protocollo del livello di rete, il protocollo di rete si trova nello stato aperto sul collegamento LCP stabilito. A questo punto, PPP può trasportare i corrispondenti pacchetti di protocollo di livello di rete.

Vediamo di seguito un esempio:



Dopo che LCP ha stabilito il collegamento, i router scambiano messaggi IPCP, negoziando le opzioni specifiche per IPv4. IPCP è responsabile della configurazione, abilitazione e disabilitazione dei moduli IPv4 su entrambe le estremità del collegamento.

IPCP negozia due opzioni:

1) Compressione: consente ai dispositivi di negoziare un algoritmo per comprimere le intestazioni TCP e IP e risparmiare larghezza di banda.
2) Indirizzo IPv4: consente al dispositivo di avvio di specificare un indirizzo IPv4 da utilizzare per l'instradamento IP tramite il collegamento PPP o per richiedere un indirizzo IPv4 per il risponditore.

Una volta completato il processo NCP, il collegamento passa allo stato aperto e LCP riprende in una fase di mantenimento del collegamento. Al termine del trasferimento dei dati, NCP termina il collegamento del protocollo e LCP termina la connessione PPP.

Opzioni LCP di configurazione PPP:

- Autenticazione: i router peer scambiano messaggi di autenticazione.
  - Password Authentication Protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP)
- Compressione: aumenta il throughput effettivo sulle connessioni PPP riducendo la quantità di bit che devono attraversare il collegamento
  - Stacker
  - Predictor
- Rilevamento degli errori: identifica le condizioni di errore.
- Richiamata PPP: la callback PPP viene utilizzata per migliorare la sicurezza. Con questa opzione LCP, un router Cisco può fungere da client di callback o server di richiamata. Il client effettua la chiamata iniziale, richiede che il server lo richiami e termina la chiamata iniziale. Il router di callback risponde alla chiamata iniziale e effettua la chiamata di ritorno al client in base alle sue istruzioni di configurazione.
- Multilink: questa alternativa fornisce il bilanciamento del carico sulle interfacce del router utilizzate da PPP. Multilink PPP, indicato anche come MP, MPPP, MLP o Multilink, fornisce un metodo per diffondere il traffico tra più link fisici WAN fornendo frammentazione e rimontaggio dei pacchetti, sequenziamento appropriato, interoperabilità di più fornitori e bilanciamento del carico sul traffico in entrata e in uscita.

Quando le opzioni sono configurate, nel campo dell'opzione LCP viene inserito un valore di campo corrispondente.

Vediamo ora come impostare i parametri precedentemente visti
Configurazione base PPP

```
interface s0/0/0
ip adderss 10.0.0.1 255.255.255.252
ipv6 address 2001:bd8:cafe:1::1/64
encapsulation ppp
compression predictor          oppure    compression stac    ← Compression
ppp quality 80                                               ← LQM (valore in %)
```

Creare un multilink tra 2 router:

ROUTER3

```
interface Multilink 1
ip adderss 10.0.1.1 255.255.255.252
ipv6 address 2001:bd8:cafe:1::1/64
ppp multilink
ppp multilink group 1

interface s0/1/0
no ip adderss
no ipv6 address
encapsulation ppp
ppp multilink
ppp multilink group 1

interface s0/1/1
no ip adderss
no ipv6 address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

ROUTER2

```
interface Multilink 1
ip adderss 10.0.1.2 255.255.255.252
ipv6 address 2001:bd8:cafe:1::2/64
ppp multilink
ppp multilink group 1

interface s0/0/0
no ip adderss
no ipv6 address
encapsulation ppp
ppp multilink
ppp multilink group 1

interface s0/0/1
no ip adderss
no ipv6 address
encapsulation ppp
ppp multilink
ppp multilink group 1
```

NB: Attenziane le caso in qui si vada a disattivare il ppp multilink (**no ppp multilink**) poiché la connessione cade immediatamente

I comandi IMPORTANTI da ricordarsi per effettuare la verifica della configurazione sono i seguenti:

```
R2# show interfaces serial 0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.0.1.2/30
  MTU 1500 bytes, BW 1544 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: IPCP, IPV6CP, CCP, CDPCP, loopback not set
```

show interfaces serial 0/0/0

```
R3# show ppp multilink

Multilink1
  Bundle name: R4
  Remote Endpoint Discriminator: [1] R4
  Local Endpoint Discriminator: [1] R3
  Bundle up for 00:01:20, total bandwidth 3088, load 1/255
  Receive buffer limit 24000 bytes, frag timeout 1000 ms
    0/0 fragments/bytes in reassembly list
    0 lost fragments, 0 reordered
    0/0 discarded fragments/bytes, 0 lost received
    0x2 received sequence, 0x2 sent sequence
  Member links: 2 active, 0 inactive (max 255, min not set)
    Se0/1/1, since 00:01:20
    Se0/1/0, since 00:01:06
No inactive multilink interfaces
R3#
```

show ppp multilink

L'autenticazione dl protocollo PPP è facoltativa è può essere effettuate con modalità:

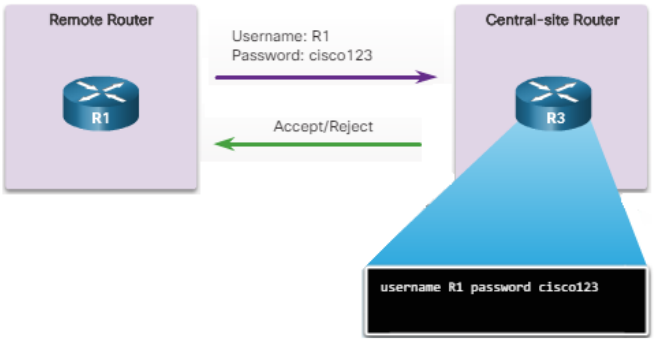
- ❖ PAP: è un processo bidirezionale molto basilare. Non c'è crittografia. Il nome utente e la password sono inviati in chiaro. Se è accettato, la connessione è consentita.
- ❖ CHAP: è più sicuro di PAP. Implica uno scambio a tre vie di una chiave condivisa.

NB: nelle WAN è sempre il router dell'ISP che verifica se utente e password coincidono in relazione al suo DB interno

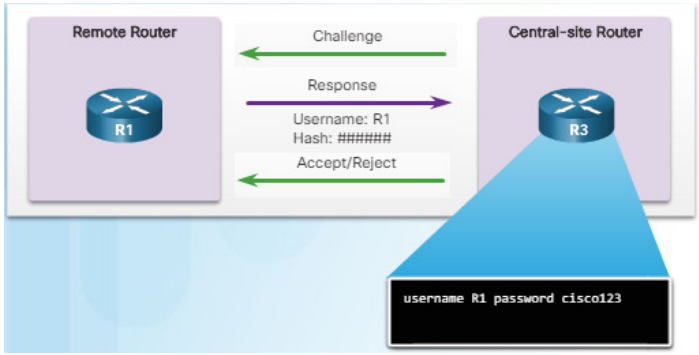
Se utilizzato, il peer viene autenticato dopo che LCP stabilisce il collegamento e sceglie il protocollo di autenticazione. L'autenticazione ha luogo prima che inizi la fase di configurazione del protocollo del livello di rete.

Le opzioni di autenticazione richiedono che il lato chiamante del collegamento inserisca le informazioni di autenticazione. Questo aiuta a garantire che l'utente abbia il permesso dell'amministratore di rete di effettuare la chiamata.

PAP



CHAP



AUTENTICAZIONE PAP:

ROUTER1

hostname R1
username R2 password indovinami
interface s0/0/0
ip adderss 10.0.1.1 255.255.255.252
ipv6 address 2001:bd8:cafe:1::1/64
encapsulation ppp
ppp authentication pap
ppp pap sent-username R1 password indovinami

ROUTER2

hostname R2
username R1 password indovinami
interface s0/0/0
ip adderss 10.0.1.2 255.255.255.252
ipv6 address 2001:bd8:cafe:2::1/64
encapsulation ppp
ppp authentication pap
ppp pap sent-username R2 password indovinami

AUTENTICAZIONE CHAP:

ROUTER1

hostname R1
username R2 password indovinami
interface s0/0/0
ip adderss 10.0.1.1 255.255.255.252
ipv6 address 2001:bd8:cafe:1::1/64
encapsulation ppp
ppp authentication chap

ROUTER2

hostname R2
username R1 password indovinami
interface s0/0/0
ip adderss 10.0.1.2 255.255.255.252
ipv6 address 2001:bd8:cafe:2::1/64
encapsulation ppp
ppp authentication chap

2.3.2.6 Packet Tracer - Configuring PAP and CHAP Authentication.pdf
2.3.2.6 Packet Tracer - Configuring PAP and CHAP Authentication.pka
2.3.2.7 Lab - Configuring Basic PPP with Authentication.pdf

Per effettuare il Troubleshooting sull'incapsulamento PPP su porta seriale si utilizza il comando
debug ppp packet
debug ppp negotiation
debug ppp error
debug ppp authentication
debug ppp compression
debug ppp cdcp
Per cercare di capire dove risiede il nostro problema:

- ✓ NCP supportati su entrambe le estremità di una connessione PPP
- ✓ Qualsiasi loop che potrebbe esistere in una rete interna PPP
- ✓ Nodi che stanno (o non stanno) negoziando correttamente le connessioni PPP
- ✓ Errori che si sono verificati sulla connessione PPP
- ✓ Cause per errori di sessione CHAP
- ✓ Cause per errori di sessione PAP
- ✓ Informazioni specifiche per lo scambio di connessioni PPP utilizzando il Callback Control Protocol (CBCP), utilizzato dai client Microsoft
- ✓ Informazioni sul numero di sequenza del pacchetto errato in cui è abilitata la compressione MPPC

IMPORTANTISSIMO: non dare mai per scontata l'autenticazione, verificarla sempre, sempre sempre.

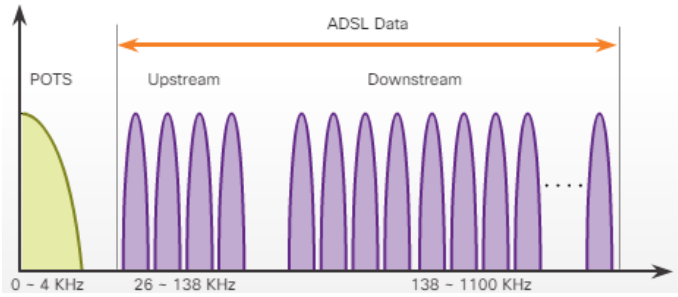
2.4.1.4 Packet Tracer - Troubleshooting PPP with Authentication.pdf
2.4.1.4 Packet Tracer - Troubleshooting PPP with Authentication.pka
2.4.1.5 Lab - Troubleshooting Basic PPP with Authentication.pdf
2.5.1.1 Class Activity - PPP Validation.pdf
2.5.1.2 Packet Tracer - Skills Integration Challenge.pdf
2.5.1.2 Packet Tracer - Skills Integration Challenge.pka

FINE CAPITOLO 2

3.0.1.2 Class Activity - Broadband Varieties.pdf

Connessioni Broadband:

- Cable: è un'opzione popolare (negli Stati Uniti) utilizzata dai telelavoratori per accedere alla rete aziendale. Il sistema via cavo utilizza un cavo coassiale che trasporta segnali in radiofrequenza (RF) attraverso la rete. Il cavo coassiale è il mezzo principale utilizzato per costruire sistemi TV via cavo. Gli operatori via cavo utilizzano in genere reti ibride fibra-coassiali (HFC) per consentire la trasmissione ad alta velocità di dati a modem via cavo situati in un SOHO (Small Office Home Office). Il DOCSIS (Data over Cable Service Interface Specification) è lo standard internazionale per l'aggiunta di dati a larghezza di banda elevata a un sistema via cavo esistente. Per utilizzare questo tipo di connessione, sono nevessari 2 tipi di apparato:
  - CMTS (Cable Modem Termination System): presso l'ISP
  - CM (Cable Modem): presso il cliente
- DSL (Digital Subscriber Line): è un mezzo per fornire connessioni ad alta velocità su fili di rame installati.
  La figura accanto mostra una rappresentazione dell'allocazione dello spazio della larghezza di banda su un filo di rame per Asymmetric DSL (ADSL). L'area etichettata POTS (Plain Old Telephone System) identifica l'intervallo di frequenza utilizzato dal servizio telefonico per voce. L'area etichettata ADSL rappresenta lo spazio di frequenza utilizzato dai segnali DSL upstream e downstream. L'area che comprende sia l'area POTS che l'area ADSL rappresenta l'intera gamma di frequenze supportata dalla coppia di fili in rame.



  Per utilizzare questo tipo di connessione, sono nevessari 2 tipi di apparato:
  - Transceiver, ossia il Modem DSL presso il cliente
  - DSLAM (DSL access multiplexer) presso il CO dell'ISP

  Attenzione: un micro filtro (noto anche come filtro DSL) consente di collegare dispositivi analogici come telefoni o fax e che devono essere installati quando si utilizza DSL.
- Reti Wireless: indicando semplicemente con il termine wireless, comprendono al suo interno varie tipologie, cognuna cone punti di accesso separati tra loro interconnessi e risultano essere:
  - Municipal Wi-Fi
  - Cellular 2G/3G/4G/LTE
  - Satellitare
  - WiMAX

3.1.2.2 Lab - Researching Broadband Internet Access Technologies.pdf

Vi sono vari motivi per cui gli ISP preferiscono utilizzare PPP:

1. PPP può essere utilizzato su tutti i collegamenti seriali compresi quelli creati con modem analogici dial-up e ISDN.
2. Con PPP abilitato, gli ISP possono utilizzare PPP per assegnare a ciascun cliente un indirizzo IPv4 pubblico.
3. PPP supporta l'autenticazione CHAP. Gli ISP spesso desiderano utilizzare CHAP per autenticare i clienti perché durante l'autenticazione, gli ISP possono controllare i record contabili per determinare se la fattura del cliente viene pagata, prima di consentire al cliente di connettersi a Internet.

Per i punti elencati sopra gli ISP preferiscono PPP mentre gli utenti sarebbero più propensi ad utilizzare Ethernet che non supporta nativamente PPP. Per cui si è passati ad utilizzare PPPoE dove il router del cliente è solitamente collegato a un modem DSL tramite un cavo Ethernet. PPPoE crea un tunnel PPP su una connessione Ethernet. Ciò consente ai frame PPP di essere inviati attraverso il cavo Ethernet all'ISP dal router del cliente. Il modem converte i frame Ethernet in frame PPP eliminando le intestazioni Ethernet. Il modem trasmette quindi questi frame PPP sulla rete DSL dell'ISP.

Vediamo ora come configurare una connessione PPPoE:

```
interface dialer 5                          ← Creo un'interfaccia virtuale
encapsulation ppp
ip address negotiation
ip mtu 1492                                 ← rispetto al valore predefinito di 1500, per adattarsi alle intestazioni PPPoE
dialer pool 5
ppp chap hostname giordy_router
ppp chap password Indovinami2018
no shutdown
exit
interface GigabitEthernet 0/0
no ip address
pppoe enable
pppoe-client dial-pool-number 5
no shutdown
exit
```

il risultato sarà essere il seguente:

```
R1# show ip interface brief
Interface              IP-Address      OK? Method  Status    Protocol
GigabitEthernet0/0     unassigned      YES NVRAM   up        up
GigabitEthernet0/1     172.16.1.1      YES manual  up        up
Dialer5                64.100.10.1     YES manual  up        up
Virtual-Access1        unassigned      YES unset   up        up
```

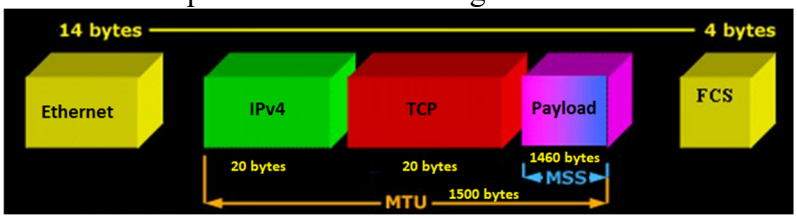
I comandi per verificare se la connessione è "salita" o stà dando dei problemi e per identificare dove potrebbero essere, sono:

show ip interface brief
show interface dialer 5
show ip route
show pppoe session
debug ppp negotiation
show running-config | section interface Dialer5

I principali problemi in una connessione PPPoE potrebbero essere insiti in:

- Fallimento del processo di negoziazione
- Autenticazione PPP
- Dimensionamento dell'MTU

L'accesso ad alcune pagine Web potrebbe essere un problema con il PPPoE. Quando il client richiede una pagina Web, si verifica un 3 way handshake TCP. Durante la negoziazione, il client specifica il valore della sua dimensione massima del segmento TCP (MSS). Il TCP MSS è la dimensione massima della porzione di dati nel segmento TCP.



Un host determina il valore del relativo campo MSS sottraendo le intestazioni IP e TCP dall'unità di trasmissione massima Ethernet (MTU). Su un'interfaccia Ethernet, il valore MTU predefinito è 1500 byte.

Sottraendo l'intestazione IPv4 di 20 byte e l'intestazione TCP di 20 byte, la dimensione MSS predefinita sarà 1460 byte (come mostrato nella figura)

La dimensione MSS predefinita è 1460 byte, quando il MTU predefinito è 1500 byte. Tuttavia, PPPoE supporta un MTU di soli 1492 byte per accogliere l'ulteriore intestazione PPPoE a 8 .
Questa disparità tra la dimensione MTU host e PPPoE può causare la caduta dei pacchetti da 1500 byte del router e la chiusura delle sessioni TCP sulla rete PPPoE.
Il comando:
interface gigabitEthernet 0/0
ip tcp adjust-mss 1452
consente di evitare che le sessioni TCP vengano eliminate regolando il valore MSS durante il 3 way handshake. Nella maggior parte dei casi, il valore ottimale per l'argomento della dimensione massima del segmento è 1452 byte.

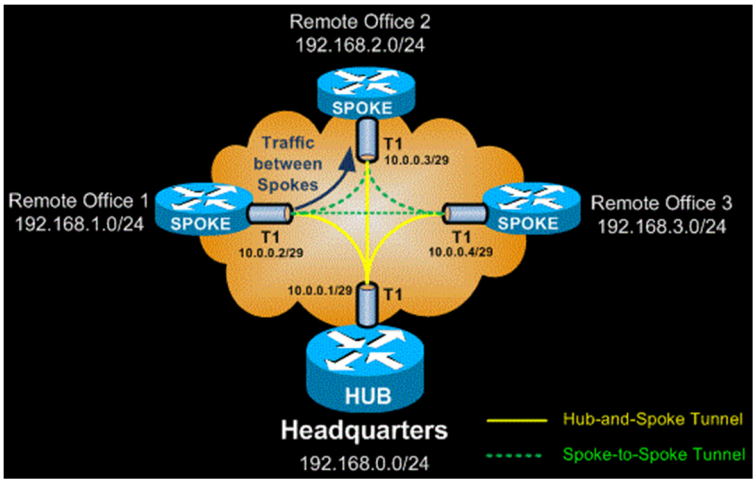
3.2.2.7 Lab - Configuring a Router as a PPPoE Client for DSL Connectivity.pdf
3.2.2.8 Lab - Troubleshoot PPPoE.pdf

Le organizzazioni utilizzano le VPN per creare una connessione di rete privata end-to-end su reti di terze parti, come Internet. Il tunnel elimina la barriera di distanza e consente agli utenti remoti di accedere alle risorse della rete del sito centrale. Una VPN è una rete privata creata tramite tunneling su una rete pubblica, solitamente Internet. Una VPN è un ambiente di comunicazione in cui l'accesso è strettamente controllato per consentire connessioni peer all'interno di una determinata comunità di interesse.
Per implementare le VPN, è necessario un gateway VPN. Il gateway VPN potrebbe essere un router o un firewall.
Vantaggi delle VPN:

- Risparmio sui costi: non bisogna più affittare banda dagli ISP, basta già la connessione che si ha a disposizione
- Scalabilità: l'aumento di sedi/utenti collegati in VPN comporta un piccolo lavoro e non l'intero cambio dell'infrastruttura
- Compatibilità con le tecnologie di connessione a disposizione
- Sicurezza: possono includere meccanismi di sicurezza che garantiscono il massimo livello di sicurezza utilizzando protocolli avanzati di crittografia e autenticazione che proteggono i dati da accessi non autorizzati

Le VPN possono essere:

- Site-2-Site: tra 2 sedi dell'azienda
- Remote Access: ogni dispositivo che si collega al centro-stella



Cisco ha creato un sistema dinamico per creare VPN multiple in maniera semplice, crando il Dynamic Multipoint VPN (DMVPN).
L'obiettivo è semplificare la configurazione, collegando in modo semplice e flessibile i siti di uffici centrali ai siti di filiali. Questo è chiamato hub-to-spoke.
Con DMVPN, i siti di succursale possono anche comunicare direttamente con altri siti di filiali (hub-to-spoke & spoke-to-spoke)

DMVPN è costruito utilizzando le seguenti tecnologie:

- ✓ Next Hop Resolution Protocol (NHRP): è un protobollo simile ad ARP che crea un DataBase di IP pubblici per tutti gli spoke. NHRP è un protocollo server client costituito dall'hub NHRP noto come Next Hop Server (NHS) e dagli spoke NHRP noti come Next Hop Clients (NHC).
- ✓ Multipoint Generic Routing Encapsulation (mGRE) tunnels: è un protocollo di tunneling sviluppato da Cisco che può incapsulare un'ampia varietà di tipi di pacchetti di protocollo all'interno dei tunnel IP. Un'interfaccia tunnel mGRE consente a un'unica interfaccia GRE di supportare più tunnel IPsec.
- ✓ IP Security (IPsec) encryption: è un protocollo di crittografica molto usato da CISCO

Generic Routing Encapsulation (GRE) è un esempio di un protocollo di tunneling VPN di base, non sicuro e sito-sito. GRE è un protocollo di tunneling sviluppato da Cisco che può incapsulare un'ampia varietà di tipi di pacchetti di protocollo all'interno dei tunnel IP. GRE crea un collegamento punto-punto virtuale ai router Cisco in punti remoti, su una rete IP.
GRE è progettato per gestire il trasporto di traffico multiprotocollo e IP multicast tra due o più siti, che può avere solo la connettività IP

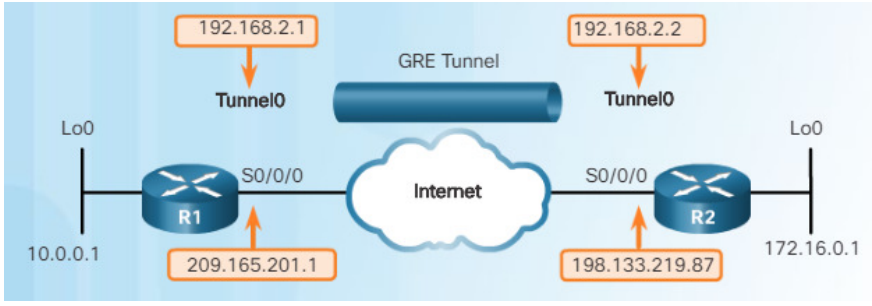
Il tunneling IP tramite GRE consente l'espansione della rete su un ambiente backbone a protocollo singolo.
GRE ha queste caratteristiche:

- è definito come standard IETF (RFC 2784)
- Nell'intestazione IP esterna, 47 viene utilizzato nel campo del protocollo per indicare che seguirà un'intestazione GRE
- L'incapsulamento GRE utilizza un campo di tipo protocollo nell'intestazione GRE per supportare l'incapsulamento di qualsiasi protocollo OSI Layer 3. I tipi di protocollo sono definiti in RFC 1700 come "EtherTypes".
- Per impostazione predefinita, non include alcun meccanismo di controllo del flusso
- GRE non include alcun meccanismo di sicurezza forte
- L'intestazione GRE, insieme all'intestazione IP tunneling, crea almeno 24 byte di overhead aggiuntivo per i pacchetti tunnel

Vediamo ora come configurare una VPN GRE

R1

```
interface Tunnel0
tunnel mode gre ip
ip address 192.168.2.1 255.255.255.0
tunnel source 209.165.201.1
tunnel destination 198.133.219.87
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
```



R2

```
interface Tunnel0
tunnel mode gre ip
ip address 192.168.2.2 255.255.255.0
tunnel source 198.133.219.87
tunnel destination 209.165.201.1
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
```

Per verificare che tutto sia stato configurato correttamente possiamo dare i comandi in figura sotto e visionare se i dati si sono propagati tramite la VPN

```
R1# show ip interface brief
<output omitted>
Interface              IP-Address      OK? Method Status    Protocol
Serial0/0/0            209.165.201.1   YES manual up        up
Loopback0              10.0.0.1        YES manual up        up
Tunnel0                192.168.2.1     YES manual up        up
R1#

R2# show ip interface brief
<output omitted>
Interface              IP-Address      OK? Method Status    Protocol
Serial0/0/0            198.133.219.87  YES manual up        up
Loopback0              172.16.0.1      YES manual up        up
Tunnel0                192.168.2.2     YES manual up        up
R2#
```

3.4.2.4 Packet Tracer - Configuring GRE.pdf
3.4.2.4 Packet Tracer - Configuring GRE.pka
3.4.2.5 Packet Tracer - Troubleshooting GRE.pdf
3.4.2.5 Packet Tracer - Troubleshooting GRE.pka
3.4.2.6 Lab - Configuring a Point-to-Point GRE VPN Tunnel.pdf

Border Gateway Protocol (BGP) è un EGP (Exterior Gateway Protocol) utilizzato per lo scambio di informazioni di routing tra autonomous systems.
In BGP, ad ogni AS viene assegnato un numero AS univoco a 16 o 32 bit che lo identifica in modo univoco su Internet.
WiMoRe – AS34526
Vodafone Italia spa – AS30722
TIM S.p.A. – AS16232

I router BGP scambiano diversi attributi di percorso, incluso un elenco di numeri AS (hop-hop) necessari per raggiungere una rete di destinazione.
Gli aggiornamenti BGP sono incapsulati su TCP sulla porta 179. Pertanto, BGP eredita le proprietà di TCP orientate alla connessione, assicurando che gli aggiornamenti BGP siano trasmessi in modo affidabile. BGP è utilizzato da un AS per pubblicizzare le sue reti e, in alcuni casi, le reti che ha appreso da altri sistemi autonomi, al resto di Internet.
IL BGP si divide in:

- BGP esterno (eBGP) - BGP esterno è il protocollo di routing utilizzato tra router in diversi sistemi autonomi.
- BGP interno (iBGP) - BGP interno è il protocollo di routing utilizzato tra router nello stesso AS.

L'uso di BGP è più appropriato quando un AS ha connessioni a più sistemi autonomi. Questo è noto come multi-homed.
ATTENZIONE: prima di eseguire BGP, è importante che l'amministratore di rete abbia una buona conoscenza di BGP. Un'errata configurazione di un router BGP potrebbe avere effetti negativi su tutta la rete.

BGP non dovrebbe essere usato quando esiste almeno una delle seguenti condizioni:

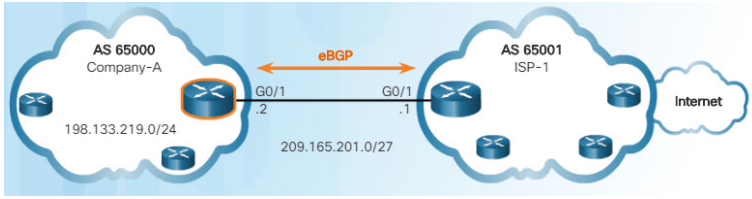
1) C'è una singola connessione a Internet
2) Quando c'è una comprensione limitata del BGP. Un'errata configurazione di un router BGP può avere effetti di vasta portata al di là dell'AS locale

Esistono tre modi in cui un'organizzazione può scegliere di implementare BGP in un ambiente multi-homed:

a) Default Route Only: questo è il metodo più semplice per implementare BGP verso Company-A
b) Default Route and ISP Routes: gli ISP pubblicizzano il loro percorso predefinito e la loro rete verso Company-A
c) All Internet Routes: Gli ISP pubblicizzano tutte le rotte Internet verso Company-A

Vediamo una semplice configurazione:

Router Company-A
router bgp 65000
neighbor 209.165.201.1 remote-as 65001
network 198.133.219.0 mask 255.255.255.0

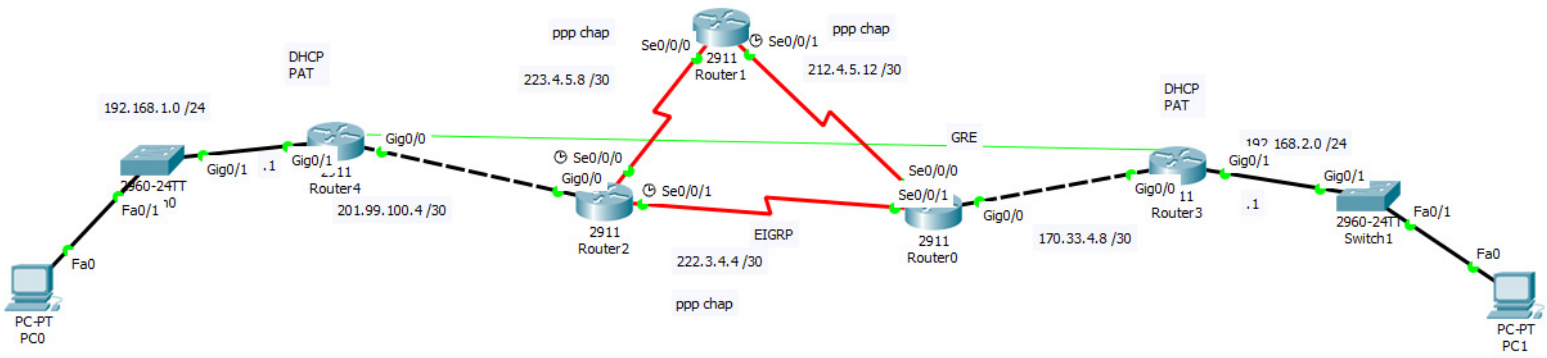


Router ISP
router bgp 65001
neighbor 209.165.201.1 remote-as 65001
network 0.0.0.0

Comandi per verificare le configurazioni BGP:
show ip route
show ip bgp
show ip bgp summary

3.5.3.4 Packet Tracer - Configure and Verify eBGP.pdf
3.5.3.4 Packet Tracer - Configure and Verify eBGP.pka
3.5.3.5 Lab - Configure and Verify eBGP.pdf
3.6.1.1 Class Activity - VPN Planning Design.pdf
3.6.1.2 Packet Tracer - Skills Integration Challenge.pdf
3.6.1.2 Packet Tracer - Skills Integration Challenge.pka
3.6.1.3 Lab - Configure a Branch Connection.pdf

FINE CAPITOLO 3



ROUTER0

```
hostname ROUTER0
username R2 password indovinami
username R1 password indovinami
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R0 - Accesso consentito solo al personale
autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 170.33.4.9 255.255.255.252
no shutdown
exit
interface Serial0/0/0
ip address 212.4.5.14 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username R0 password indovinami
no shutdown
exit
interface Serial0/0/1
ip address 222.3.4.6 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username R0 password indovinami
no shutdown
exit
router eigrp 1
eigrp router-id 1.1.1.1
network 170.33.4.8 0.0.0.3
network 212.4.5.12 0.0.0.3
network 222.3.4.4 0.0.0.3
passive-interface g0/0
exit
exit
copy running-config startup-config
```

ROUTER1

```
hostname ROUTER1
username R0 password indovinami
username R2 password indovinami
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R1 - Accesso consentito solo al personale
autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface Serial0/0/0
ip address 223.4.5.10 255.255.255.252
encapsulation ppp
ppp authentication pap
ppp pap sent-username R1 password indovinami
no shutdown
exit
interface Serial0/0/1
ip address 212.4.5.13 255.255.255.252
clock rate 1000000
encapsulation ppp
ppp authentication pap
ppp pap sent-username R1 password indovinami
no shutdown
exit
router eigrp 1
eigrp router-id 2.2.2.2
network 212.4.5.12 0.0.0.3
network 223.4.5.8 0.0.0.3
exit
exit
copy running-config startup-config
```

ROUTER2

```
hostname ROUTER2
username R0 password indovinami
username R1 password indovinami
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R2 - Accesso consentito solo al personale
autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 201.99.100.5 255.255.255.252
no shutdown
exit
interface Serial0/0/0
ip address 223.4.5.9 255.255.255.252
clock rate 1000000
encapsulation ppp
ppp authentication pap
ppp pap sent-username R2 password indovinami
no shutdown
exit
interface Serial0/0/1
ip address 222.3.4.5 255.255.255.252
clock rate 1000000
encapsulation ppp
ppp authentication pap
ppp pap sent-username R2 password indovinami
no shutdown
exit
router eigrp 1
eigrp router-id 3.3.3.3
network 201.99.100.4 0.0.0.3
network 223.4.5.8 0.0.0.3
network 222.3.4.4 0.0.0.3
passive-interface g0/0
exit
exit
copy running-config startup-config
```

ROUTER3

```
hostname ROUTER3
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R3 - Accesso consentito solo al personale
autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 170.33.4.10 255.255.255.252
no shutdown
exit
interface GigabitEthernet0/1
ip address 192.168.2.254 255.255.255.0
no shutdown
exit
ip dhcp excluded-address 192.168.2.254
ip dhcp pool DHCP
network 192.168.2.0 255.255.255.0
default-router 192.168.2.254
domain-name CORSO.local
dns-server 8.8.8.8
exit
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
exit
copy interface GigabitEthernet0/0
ip address 170.33.4.10 255.255.255.252
no shutdown
exit
interface GigabitEthernet0/1
ip address 192.168.2.254 255.255.255.0
no shutdown
exit
ip dhcp excluded-address 192.168.2.254
ip dhcp pool DHCP
network 192.168.2.0 255.255.255.0
default-router 192.168.2.254
domain-name CORSO.local
dns-server 8.8.8.8
exit
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
access-list 20 permit 192.168.2.0 0.0.0.255
ip nat inside source list 20 interface GigabitEthernet0/0
overload
interface GigabitEthernet0/1
ip nat inside
exit
interface GigabitEthernet0/0
ip nat outside
exit
interface Tunnel0
tunnel mode gre ip
ip address 10.0.0.2 255.255.255.0
tunnel source gigabitEthernet 0/0
tunnel destination 201.99.100.6
no shutdown
exit
router eigrp 1
router-id 3.3.3.3
network 10.0.0.0
network 192.168.2.0
passive-interface GigabitEthernet0/0
exit
exit
copy running-config startup-config
```

ROUTER4

```
hostname ROUTER4
line console 0
password cisco
login
exit
line vty 0 15
password cisco
login
exit
enable secret cisco
service password-encryption
banner motd #R4 - Accesso consentito solo al personale
autorizzato#
ip domain-name router.local
crypto key generate rsa
1024
username admin cisco
line vty 0 15
login local
transport input ssh
exit
ip ssh version 2
interface GigabitEthernet0/0
ip address 201.99.100.6 255.255.255.252
no shutdown
exit
interface GigabitEthernet0/1
ip address 192.168.1.254 255.255.255.0
no shutdown
exit
ip dhcp excluded-address 192.168.1.254
ip dhcp pool DHCP
network 192.168.1.0 255.255.255.0
default-router 192.168.1.254
domain-name CORSO.local
dns-server 8.8.8.8
exit
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
access-list 10 permit 192.168.1.0 0.0.0.255
ip nat inside source list 10 interface GigabitEthernet0/0
overload
interface GigabitEthernet0/1
ip nat inside
exit
interface GigabitEthernet0/0
ip nat outside
exit
interface Tunnel0
tunnel mode gre ip
ip address 10.0.0.1 255.255.255.0
tunnel source gigabitEthernet 0/0
tunnel destination 170.33.4.10
no shutdown
exit
router eigrp 1
router-id 4.4.4.4
network 10.0.0.0
network 192.168.1.0
passive-interface GigabitEthernet0/1
exit
exit
copy running-config startup-config
```

Si consiglia un ripasso delle wild card mask e delle ACL Standard (Modulo 2 - Capitolo 7)

L'importante è ricordarsi che:
1) Una ACL per protocollo (IPv4 e IPv6)
2) Una ACL per direzione (IN o OUT)
3) Una ACL ad interfaccia

Il packet filtering controlla l'accesso a una rete analizzando i pacchetti in entrata e in uscita e inoltrandoli o scartandoli in base a determinati criteri. Il filtraggio dei pacchetti può avvenire in Layer 3 o Layer 4. Le ACL Standard filtrano solo al livello 3. Le ACL Extended filtrano a livello 3 e livello 4.

Gli ACL standard possono essere utilizzati per consentire o negare il traffico solo dagli indirizzi IPv4 di origine. La destinazione del pacchetto e le porte coinvolte non vengono valutate.
Le ACL Standard vengono creati in modalità di configurazione globale.

Le ACL Extended filtrano i pacchetti IPv4 in base a diversi attributi:
- ✓ Tipo di protocollo
- ✓ Indirizzo IPv4 di origine
- ✓ Indirizzo IPv4 di destinazione
- ✓ Porte TCP o UDP di origine
- ✓ Porte TCP o UDP di destinazione
- ✓ Informazioni sul tipo di protocollo opzionali per un controllo più preciso

Oltre a Standard ed Extended le ACL si dividono anche in:
Numbered:
- Da 1 a 99 e da 1300 a 1999: Standard
- Da 100 a 199 e da 2000 a 2699: Extended

Named:
- In nome può contenere caratteri alfanumerici
- Si suggerisce che il nome sia scritto in maiuscolo
- Il nome non può contenere spazi o segni di punteggiatura
- Le voci possono essere aggiunte o eliminate all'interno dell'ACL

La regola di semplificazione, ci dice che deneralmente le ACL Extended sono posizionate vicino alla sorgente del traffico da filtrare mentre le Standard vicino alla destinazione del traffico da filtrare.

ACL Numbered (Standard)
access-list 1 permit 192.168.1.0 0.0.0.254
interface Serial0/0/0
ip access-group 1 out
ACL Named
ip access-list standard NO_ACCESS ← **standard si può sostituire con extended**
deny host 192.168.1.69
permit any
exit
interface Gigabitethernet 0/0
ip access-group NO_ACCESS out
Verifichiamo le configurazioni con:
show ip interface Gigabitethernet 0/0
show access-lists

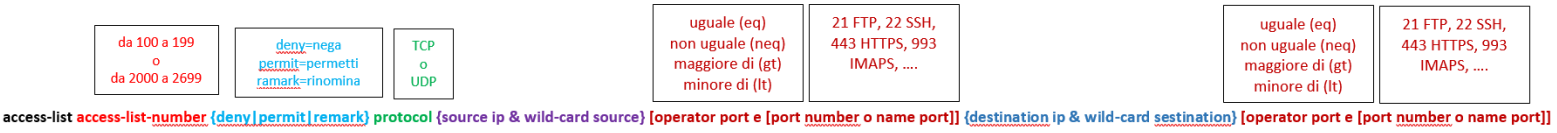
4.1.3.5 Packet Tracer - Configure Standard IPv4 ACLs.pdf
4.1.3.5 Packet Tracer - Configure Standard IPv4 ACLs.pka

Ecco Alcuni esempi di come un amministratore specifica un numero di porta TCP o UDP posizionandolo alla fine dell'istruzione ACL Extended. Le operazioni logiche possono essere utilizzate, ad esempio uguale (eq), non uguale (neq), maggiore di (gt) e minore di (lt).

access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20

access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telent
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data

Configurazione di un'ACL Extended



Esempio:
access-list 114 permit tcp 192.168.20.0 0.0.0.255 eq 22 any eq 22
è possibile aggiungere un ulteriore parametro opzionale **estabilished**, come nel seguente esempio:
access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 80
access-list 103 permit tcp 192.168.10.0 0.0.0.255 any eq 443
access-list 104 permit tcp any 192.168.10.0 0.0.0.255 estabilished

Tale parametro consente solo le risposte al traffico che provengono dalla rete 192.168.10.0/24 per tornare a quella rete. Una corrispondenza si verifica se il segmento TCP restituito ha i bit ACK o reset (RST) impostati, il che indica che il pacchetto appartiene a una connessione esistente. Senza il parametro **estabilished** nell'istruzione ACL, i client potrebbero inviare traffico a un server Web, ma non ricevere traffico di ritorno dal server web.
Dopo aver creato le varie ACL Extended, per applicarle all'interfaccia basta dare i seguenti comandi:

interface Gigabitethernet 0/1
ip access-list 103 in
ip access-list 104 out
exit

Per quanto riguarda l'esempio sopra ma con le ACL Extended Named

ip access-list extended WEB_SURF
permit tcp 192.168.10.0 0.0.0.255 any eq 80
permit tcp 192.168.10.0 0.0.0.255 any eq 443
exit
ip access-list extended BROWSING
permit tcp any 192.168.10.0 0.0.0.255 estabilished
exit
interface Gigabitethernet 0/1
ip access-group WEB_SURF in
ip access-group BROWSING out
exit

Se volgiamo editare una ACL Extended, prima diamo il comando
show access-lists
poi guardiamo il sequence number della regola che vogliamo editare es. ipotiziamo di voler editare la regola con il sequence number 10:
ip access-list extended WEB_SURF
no 10
10 permit tcp 192.168.10.0 0.0.0.255 any eq www
exit

4.2.2.10 Packet Tracer - Configuring Extended ACLs Scenario 1.pdf
4.2.2.10 Packet Tracer - Configuring Extended ACLs Scenario 1.pka
4.2.2.11 Packet Tracer - Configuring Extended ACLs Scenario 2.pdf
4.2.2.11 Packet Tracer - Configuring Extended ACLs Scenario 2.pka
4.2.2.12 Packet Tracer - Configuring Extended ACLs Scenario 3.pdf
4.2.2.12 Packet Tracer - Configuring Extended ACLs Scenario 3.pka
4.2.2.13 Lab - Configuring and Verifying Extended ACLs.pdf

Per quanto riguarda l'IPv6 le ACL Extended esistono solo Named.
Per progettazione su ogni interfaccia possono coesistere ACL IPv4 ed IPv6

ND: neighbor discovery – NS: Neighbor solicitation – NA: neigbor advertisement

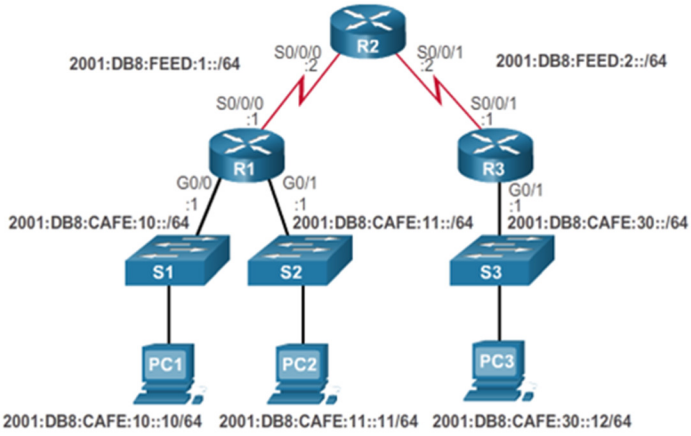
Per prima cosa impostiamo gli indirizzi ip delle varie interfacce (sempre a partire dalla configuration terminal)

ipv6 unicast-routing ← **Ricordiamoci che l'IPv6 routing è da abilitare**
interface gigabitethernet 0/0
ipv6 address 2001:db8:cafe:10::1/64
no shutdown
exit
interface serial 0/0/0
ipv6 address 2001:db8:feed:1::1/64 ← se il dispositivo è il DCE impostare anche il clock
no shutdown
exit
interface gigabitethernet 0/1
ipv6 address 2001:db8:cafe:11::1/64
no shutdown
exit
se diamo il comando
show ipv6 interface brief
noteremo che il sistema avrà attivato su ogni interfaccia anche un loopback address IPv6 per ogni interfaccia.

Vediamo ora come configurare l'ACL in IPv6 (sempre a partire dalla configuration terminal)

uguale (eq) uguale (eq)
ipv6 non uguale (neq) non uguale (neq)
o maggiore di (gt) maggiore di (gt)
TCP/UDP minore di (lt) minore di (lt)

{deny|permit} protocol {ipv6-sorgente/prefix|any|host ipv6-sorgente} [operator [porta]] {ipv6-destinazione/prefix|any|host ipv6-destinazione} [operator [porta]]



R1

ipv6 access-list NO_LAN3_ACCESS
deny ipv6 2001:db8:cafe:30::/64 any
permit ipv6 any any
exit
interface serial 0/0/0
ipv6 traffic-filter NO_LAN3_ACCESS in

altro esempio per bloccare il traffico FTP verso la rete 11

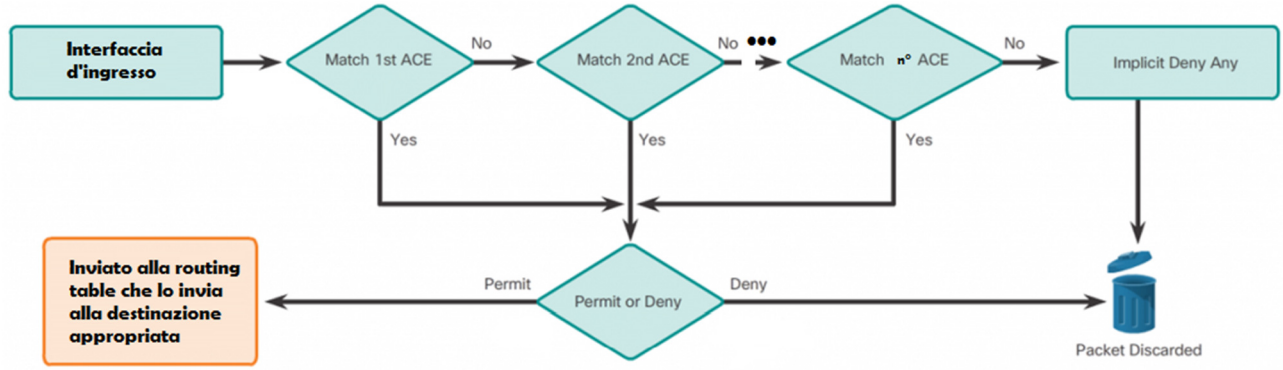
R1

ipv6 access-list NO_FTP_TO_11
deny tcp any 2001:db8:cafe:10::/64 eq ftp
deny tcp any 2001:db8:cafe:11::/64 eq ftp-data
permit ipv6 any any
exit
interface gigabitethernet 0/0
ipv6 traffic-filter NO_FTP_TO_11 in

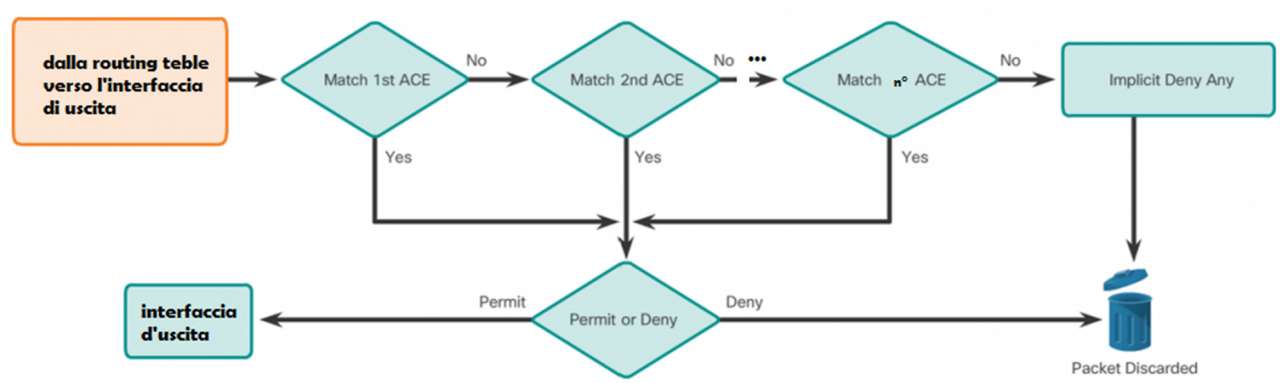
4.3.2.6 Packet Tracer - Configuring IPv6 ACLs.pdf
4.3.2.6 Packet Tracer - Configuring IPv6 ACLs.pka
4.3.2.7 Lab - Configuring and Verifying IPv6 ACLs.pdf

Ricordando che:
ACL: Access Control List
ACE: Access Control Entrie

INBOUD:



OUTBOUND:



4.4.2.9 Packet Tracer - Troubleshooting IPv4 ACLs.pdf
4.4.2.9 Packet Tracer - Troubleshooting IPv4 ACLs.pka
4.4.2.10 Packet Tracer - Troubleshooting IPv6 ACLs.pdf
4.4.2.10 Packet Tracer - Troubleshooting IPv6 ACLs.pka
4.4.2.11 Lab - Troubleshooting ACL Configuration and Placement.pdf
4.5.1.1 Packet Tracer - Skills Integration Challenge.pdf
4.5.1.1 Packet Tracer - Skills Integration Challenge.pka

NB: ricordarsi il comando **access-class** per limitare gli accessi alle VTY

FINE CAPITOLO 4

5.0.1.2 Class Activity - Network Maintenance Development Instructions.pdf

Le LAN Layer 2 sono spesso considerate un ambiente sicuro e protetto. Tuttavia, se il Livello 2 è compromesso, anche tutti i livelli sopra di esso sono interessati. Oggi, con l'utilizzo BYOD (bring your own device) e attacchi più sofisticati, le LAN sono diventate più vulnerabili.
I principali attacchi su LAN a licello Layer2 possono essere:

- CDP Reconnaissance Attack
  Il protocollo Cisco Discovery Protocol (CDP) è un protocollo di rilevamento link Layer 2 proprietario. È abilitato su tutti i dispositivi Cisco per impostazione predefinita. Tuttavia, le informazioni fornite da CDP possono essere utilizzate anche da un utente malintenzionato per scoprire le vulnerabilità dell'infrastruttura di rete. Le trasmissioni CDP vengono inviate non crittografate e non autenticate. Pertanto, un utente malintenzionato potrebbe interferire con l'infrastruttura di rete inviando frame CDP creati contenenti informazioni sui dispositivi fasulli ai dispositivi Cisco collegati direttamente.
  È consigliabile disabilitarlo se non è utilizzato:
  no cdp run ← per disattivarlo su tutto il router
  no cdp enable ← per disattivarlo su una sola interfaccia
  stesso discorso anche se viene utilizzato lldp
  no lldp run ← per disattivarlo su tutto il router
  no lldp transmit o no **lldp receive** ← per disattivarlo su una sola interfaccia
- Telnet Attacks: esistono 2 attacchi principali su telnet
  - Brute Force Password Attack
  - Telnet DoS Attack

  Per aumentare la protezione sul servizio telnet si consiglia:
  - Utilizzare SSH, anziché Telnet per le connessioni di gestione remota
  - Utilizza password complesse che vengono cambiate frequentemente
  - Limita l'accesso alle linee vty utilizzando un elenco di ACL che consente solo i dispositivi di amministrazione e nega tutti gli altri dispositivi
  - Autentica e autorizza l'accesso amministrativo al dispositivo utilizzando AAA con i protocolli TACACS+ o RADIUS
- MAC Address Table Flooding Attack: è uno degli attacchi switch LAN di base più comuni. Questo attacco è anche noto come attacco di overflow della tabella degli indirizzi MAC o attacco di overflow della tabella CAM. Configurare la sicurezza della porta sullo switch per mitigare gli attacchi di overflow della tabella degli indirizzi MAC (es. un singolo mac address per porta, attiviamo quindi il security port sullo switch)
- VLAN Attacks: un malintenzionato attiva sul suo device il protocollo 802.1Q e tenta di instaurare un trunk con lo switch per poi spacciarsi per un neigbor ed ottenere tutti i dati di rete. Per prevenire questi attacchi è bene:
  - Configurare esplicitamente i collegamenti di accesso
  - Disabilita esplicitamente il trunking automatico (disabilitare DPT)
  - Abilita manualmente i collegamenti trunk
  - Disabilitare le porte non utilizzate, fargli accedere alle porte e assegnarle a una VLAN non utilizzata
  - Modifica la VLAN nativa predefinita
  - Implementare la sicurezza della porta

- DHCP Attacks: DHCP è il protocollo che assegna automaticamente un host a un indirizzo IP valido da un pool DHCP.
  Esistono due tipi di attacchi DHCP:
  - DHCP spoofing attack: un utente malintenzionato configura un server DHCP falso sulla rete per inviare indirizzi IP ai client. Questo tipo di attacco costringe i client a utilizzare sia un server DNS (Domain Name System) falso sia un computer che è sotto il controllo dell'utente malintenzionato come gateway predefinito. Per limitare questo attacco, si utilizza snooping DHCP. Quando uno switch riceve un pacchetto DHCP su una porta non affidabile, lo switch confronta le informazioni del pacchetto sorgente con quelle contenute nel Database dei collegamenti snooping DHCP. L'opzione rifiuterà i pacchetti contenenti una delle seguenti informazioni:
    - Unauthorized DHCP server messages provenienti da una porta non affidabile
    - Unauthorized DHCP client messages non aderiscono al database di binding snooping DHCP o ai limiti di velocità. In una rete di grandi dimensioni, il Database di bindaggio snooping DHCP potrebbe richiedere del tempo per essere compilato dopo essere stato abilitato

    Lo snooping DHCP riconosce due tipi di porte:
    - Porte DHCP attendibili: devono essere esplicitamente identificate nella configurazione
    - Porte non attendibili: per impostazione predefinita, tutte le porte dello switch non sono attendibili
  - DHCP starvation attack: un utente malintenzionato inonda il server DHCP con richieste DHCP fasulle e alla fine affitta tutti gli indirizzi IP disponibili nel pool di server DHCP. Dopo che questi indirizzi IP sono stati emessi, il server non può rilasciare più indirizzi e questa situazione produce un attacco DoS (denial-of-service) poiché i nuovi client non possono ottenere l'accesso alla rete.
    ATTENZIONE: a volte gli utenti pensano di essere sotto questo attacco, ma semplicemente hanno un POOL d'IP molto ristretto ed un tempo di lease del DHCP molto elevato

    NB: DHCP starvation attack viene spesso utilizzato prima di un DHCP spoofing attack per negare il servizio al server DHCP legittimo. Ciò semplifica l'introduzione di un falso server DHCP nella rete.

Ricapitolando per aumentare il livello di sicurezza è bene:

1) Utilizzare sempre varianti sicure di questi protocolli come SSH, SCP, SSL, SNMPv3, SFTP, ecc…
2) Usa sempre password complesse e cambale spesso
3) Abilita CDP solo su porte selezionate
4) Utilizzare una VLAN di gestione dedicata in cui risiede solo il traffico di gestione
5) Utilizzare gli ACL per filtrare l'accesso indesiderato

Per impedire agli utenti malintenzionati di accedere a apparecchiature e servizi di rete sensibili, gli amministratori di rete devono abilitare il controllo degli accessi.
Esistono diversi metodi per implementare l'autenticazione su un dispositivo Cisco e ogni metodo offre vari livelli di sicurezza. Il framework Autenticazione, autorizzazione e contabilità (AAA) viene utilizzato per garantire l'accesso al dispositivo.
Cisco fornisce due metodi comuni per l'implementazione dei servizi AAA:

- Local AAA Authentication: utilizza un database locale per l'autenticazione. Questo metodo è talvolta noto come autenticazione autonoma. Memorizza nomi utente e password localmente nel router Cisco e gli utenti eseguono l'autenticazione con il database locale. AAA locale è ideale per reti di piccole dimensioni.
    a) Il client stabilisce una connessione con il router.
    b) Il router AAA richiede all'utente un nome utente e una password.
    c) Il router autentica il nome utente e la password utilizzando il database locale e l'utente viene fornito accesso alla rete in base alle informazioni nel database locale.
- Server-Based AAA Authentication: è una soluzione molto più scalabile. Il router accede a un server AAA centrale che contiene i nomi utente e la password per tutti gli utenti e funge da sistema di autenticazione centrale per tutti i dispositivi dell'infrastruttura.
    a) Il client stabilisce una connessione con il router.
    b) Il router AAA richiede all'utente un nome utente e una password.
    c) Il router autentica il nome utente e la password utilizzando un server AAA remoto.

Esiste un altro protocollo utilizzato per proteggere i computer che si connettono a una LAN.
Lo standard IEEE 802.1X definisce un protocollo di controllo degli accessi e autenticazione basato sulle porte.
Consente alle workstation non autorizzate di connettersi a una LAN tramite porte switch accessibili pubblicamente. Il server di autenticazione autentica ogni workstation connessa a una porta dello switch prima di rendere disponibili tutti i servizi offerti dallo switch o dalla LAN.

Con l'autenticazione basata su porta 802.1X, i dispositivi nella rete hanno ruoli specifici:

- Client (Supplicant): il dispositivo richiede l'accesso alla LAN ed ai servizi dello switch e risponde alle richieste dello switch.
- Switch (Authenticator): Controlla l'accesso fisico alla rete in base allo stato di autenticazione del client. Lo switch funge da intermediario (proxy) tra il client e il server di autenticazione. Richiede l'identificazione delle informazioni dal client, verifica le informazioni con il server di autenticazione e inoltra una risposta al client. Lo switch utilizza un agente software RADIUS, che è responsabile dell'incapsulamento e de-incapsulamento dei frame EAP (Extensible Authentication Protocol) e dell'interazione con il server di autenticazione
- Authentication server: esegue l'autenticazione del client. Il server di autenticazione convalida l'identità del client e lo notifica allo switch, indipendentemente dal fatto che il client sia autorizzato ad accedere alla LAN e a cambiare i servizi. Poiché lo switch funge da proxy, il servizio di autenticazione è trasparente per il client. *Il sistema di sicurezza RADIUS con estensioni EAP è l'unico server di autenticazione supportato*.

Il protocollo SNMP (Simple Network Management Protocol), consente agli amministratori di rete di monitorare e gestire le prestazioni della rete, individuare e risolvere i problemi di rete e pianificare la crescita della rete.
È un protocollo a livello di applicazione che fornisce un formato di messaggio per la comunicazione tra manager e agenti. Il sistema SNMP è composto da tre elementi:

- Gestore SNMP: fa parte di un sistema di gestione della rete (NMS), ed esegue il software di gestione SNMP
- Agenti SNMP (nodo gestito): trovana sui dispositivi client SNMP, è responsabile della fornitura dell'accesso al MIB locale.
- Management Information Base (MIB): trovana sui dispositivi client SNMP, i dati sul dispositivo e le statistiche operative e sono pensati per essere disponibili agli utenti remoti autenticati.

Il gestore SNMP esegue il polling degli agenti e interroga il MIB per gli agenti SNMP sulla porta UDP 161. Gli agenti SNMP inviano eventuali trap SNMP al gestore SNMP sulla porta UDP 162.

Vi sono due richieste primarie di gestore SNMP:

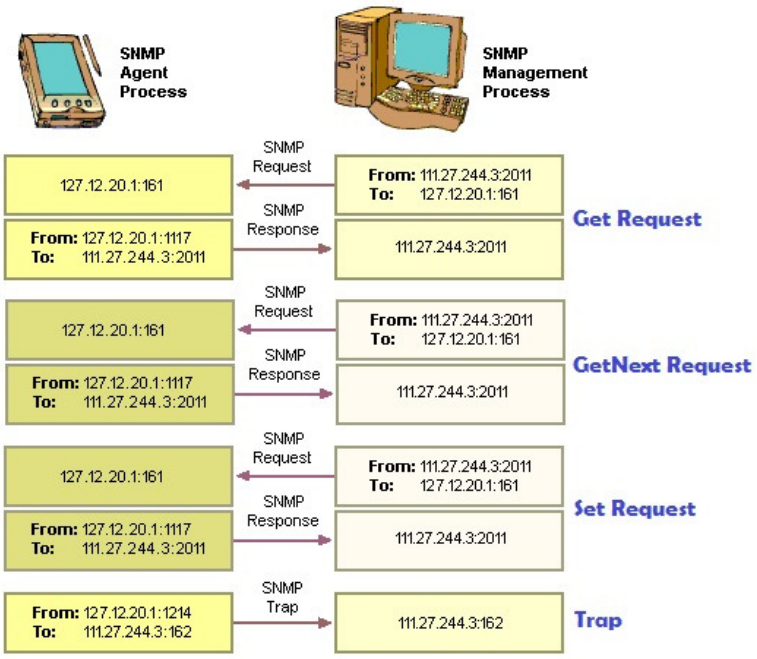
- get: viene utilizzata da NMS per interrogare il dispositivo per i dati.
- set: viene utilizzata da NMS per modificare le variabili di configurazione nel dispositivo agente. Una richiesta di set può anche avviare azioni all'interno di un dispositivo.

L'agente SNMP risponde alle richieste del gestore SNMP come segue:

- Get an MIB variable: L'agente SNMP esegue questa funzione in risposta a una GetRequest-PDU dal gestore di rete. L'agente recupera il valore della variabile MIB richiesta e risponde al gestore di rete con quel valore.
- Set an MIB variable: L'agente SNMP esegue questa funzione in risposta a una SetRequest-PDU dal gestore di rete. L'agente SNMP modifica il valore della variabile MIB sul valore specificato dal gestore di rete. Una risposta dell'agente SNMP a una richiesta di impostazione include le nuove impostazioni nel dispositivo.

Il polling SNMP periodico presenta degli svantaggi. Innanzitutto, c'è un ritardo tra il momento in cui si verifica un evento e il momento in cui viene rilevato (tramite il polling) da parte dell'NMS. In secondo luogo, c'è un compromesso tra frequenza di polling e utilizzo della larghezza di banda.

Per mitigare questi svantaggi, è possibile per gli agenti SNMP generare e inviare trap per informare immediatamente l'NMS di determinati eventi. Le trap sono messaggi non richiesti che avvisano il gestore SNMP di una condizione o evento sulla rete.



Il MIB organizza le variabili gerarchicamente. Le variabili MIB consentono al software di gestione di monitorare e controllare il dispositivo di rete. Formalmente, il MIB definisce ogni variabile come ID oggetto (OID). Gli OID identificano in modo univoco gli oggetti gestiti nella gerarchia MIB. Il MIB organizza gli OID basati sugli standard RFC in una gerarchia di OID, solitamente mostrata come un albero.
L'albero MIB per ogni dispositivo include alcuni rami con variabili comuni a molti dispositivi di rete e alcuni rami con variabili specifiche per quel dispositivo o fornitore.

Abbiamo che SNMPv3 offre le seguenti funzioni di sicurezza:
1. Integrità e autenticazione dei messaggi
2. Crittografia
3. Controllo accessi

5.2.1.9 Lab - Researching Network Monitoring Software.pdf

Vediamo ora alcuni comandi per impostare snmp sugli apparati CISCO
ROUTER1
snmp-server community mio_ufficio ro SNMP_ACL
snmp-server location SALA_CED
snmp-server contact Sistemisti DITTA
snmp-server host 192.168.1.3 version 2c mio_ufficio
snmp-server enable trap
ip access-list standard SNMP_ACL
permit 192.168.1.3

NB: l'ip del router è 192.168.1.1, mentre 192.168.1.3 è il device che voglio monitorare

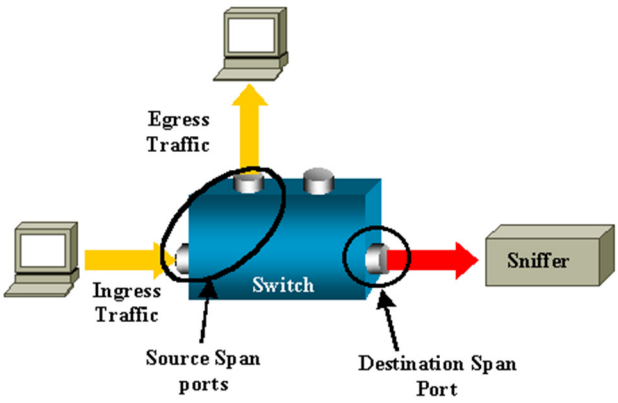
Per effettuare il thrubleshooting ecco i comandi:
show snmp
show snmp community

Best practice SNMP:
- SNMPv3 è consigliato perché fornisce autenticazione e crittografia di sicurezza.
- Assicurarsi che i messaggi SNMP non si diffondano oltre le console di gestione.

Comandi SNMPv3
1) **snmp-server group NOME_GRUPPO {v1 | v2c | v3 {auth | noauth | priv}}** crea un nuovo gruppo SNMP sul dispositivo, esempio:
   ip access-list standard ACL_CONTROL
   permit 192.168.1.3
   exit
   smtp-server view SMTP-RO iso included
   snmp-server group ADMIN-RO v3 priv read access ACL_CONTROL
2) **snmp-server user Nome_Utente NOME_GRUPPO v3 [encrypted] [auth {md5 | sha} auth-password] [priv {des |3des | aes {128 | 192 | 256}} priv-password]**
   snmp-server user god ADMIN-RO v3 auth md5 PWDtutti priv aes 256 Indovinami2018

5.2.2.6 Lab - Configuring SNMP.pdf

Abilitare il mirroring delle porte consente a uno switch di copiare e inviare frame Ethernet da porte specifiche alla porta di destinazione connessa a un analizzatore di pacchetti.



La funzionalità Switched Port Analyzer (SPAN) sugli switch Cisco è un tipo di mirroring delle porte che invia copie del frame che entrano in una porta, fuori da un'altra porta sullo stesso switch. SPAN consente agli amministratori o ai dispositivi di raccogliere e analizzare il traffico.

SPAN è comunemente implementato per fornire traffico a dispositivi specializzati tra cui:

- Analizzatori di pacchetti, come ad esempio Wireshark
- Sistemi di prevenzione delle intrusioni (IPS)

SPAN può essere implementato come:

- Local SPAN: si verifica quando il traffico su uno switch viene eseguito il mirroring su un'altra porta su tale switch. Una sessione SPAN è l'associazione tra le porte di origine (o VLAN) e una porta di destinazione. Il traffico che entra o esce dalla porta di origine (o VLAN) viene replicato dallo switch sulla porta di destinazione. Sebbene SPAN possa supportare più porte di origine nella stessa sessione o un'intera VLAN come sorgente di traffico, una sessione SPAN non supporta entrambe.
  Ci sono tre cose importanti da considerare quando si configura lo SPAN:
  1) La porta di destinazione non può essere una porta di origine e la porta di origine non può essere una porta di destinazione
  2) Il numero di porte di destinazione dipende dalla piattaforma
  3) La porta di destinazione non è più una normale porta dello switch

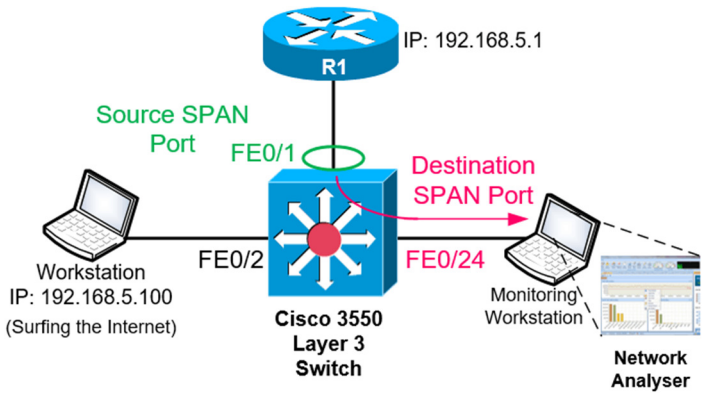
  La funzionalità SPAN è detta locale quando le porte monitorate si trovano tutte sullo stesso switch della porta di destinazione.
- Remote SPAN (RSPAN): consente alle porte di origine e di destinazione di trovarsi in diversi switch. RSPAN è utile quando l'analizzatore di pacchetti o IPS si trova su uno switch diverso rispetto al traffico monitorato. RSPAN utilizza due sessioni. Una sessione viene utilizzata come origine e una sessione viene utilizzata per copiare o ricevere il traffico da una VLAN. Il traffico per ogni sessione RSPAN viene trasferito su collegamenti trunk in una VLAN RSPAN specificata dall'utente che è dedicata (per quella sessione RSPAN) in tutte le opzioni partecipanti.

Vediamo come configurare local SPAN (sempre a partire dalla configuration terminal:

monitor session 1 source interface fastethernet 0/1
monitor session 1 destination interface fastethernet 0/24

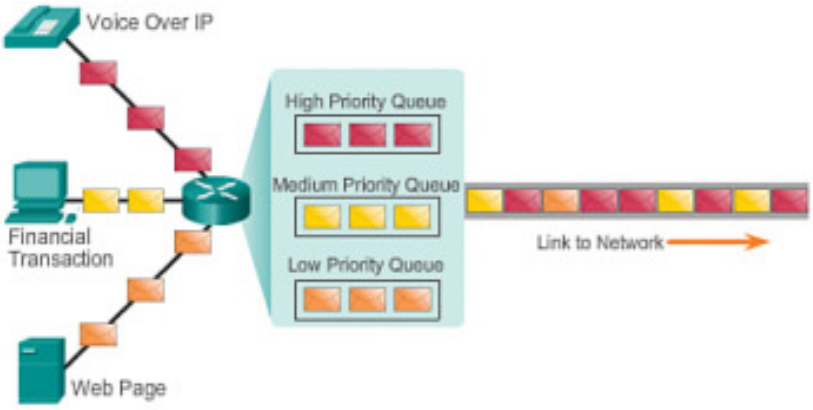
troubleshooting:

show monitor



5.3.2.3 Lab - Implement Local SPAN.pdf
5.3.3.2 Lab - Troubleshoot LAN Traffic Using SPAN.pdf

FINE CAPITOLO 5



La Quality of Service (QoS) è un requisito sempre crescente delle reti oggi. Quando il volume del traffico è maggiore di quello che può essere trasportato attraverso la rete, i dispositivi accodano o trattengono i pacchetti in memoria fino a quando le risorse diventano disponibili per trasmetterli. I pacchetti di accodamento causano un ritardo poiché i nuovi pacchetti non possono essere trasmessi finché non sono stati elaborati pacchetti precedenti. Se il numero di pacchetti da accodare continua ad aumentare, la memoria all'interno del dispositivo si riempie e i pacchetti vengono eliminati. Una tecnica QoS che può aiutare con questo problema è quella di classificare i dati in più code.

La larghezza di banda della rete (bandwidth) viene misurata nel numero di bit che possono essere trasmessi in un singolo secondo o bit al secondo (bps)

La congestione della rete provoca ritardi. Un'interfaccia sperimenta la congestione quando viene presentata con più traffico di quanto possa gestire. I punti di congestione della rete sono candidati forti per i meccanismi di QoS.

Ritardo o latenza si riferisce al tempo impiegato da un pacchetto per viaggiare dalla sorgente alla destinazione. Vi sono due tipi di ritardi: fissi e variabili. Un ritardo fisso è una quantità specifica di tempo impiegata da un processo specifico (esempio il tempo necessario per posizionare un bit sul supporto di trasmissione). Un ritardo variabile richiede una quantità di tempo non specificata ed è influenzato da fattori quali la quantità di traffico che viene elaborata.

Il jitter è la variazione del ritardo dei pacchetti ricevuti. Sul lato mittente, i pacchetti vengono inviati in un flusso continuo con i pacchetti distanziati in modo uniforme. A causa della congestione della rete, dell'accodamento improprio o degli errori di configurazione, il ritardo tra ogni pacchetto può variare anziché rimanere costante. Sia il ritardo che il jitter devono essere controllati e ridotti al minimo per supportare il traffico interattivo in tempo reale.

IMPORTANTE

Senza alcun meccanismo QoS, i pacchetti vengono elaborati nell'ordine in cui vengono ricevuti. Quando si verifica la congestione, i dispositivi di rete come router e switch possono rilasciare pacchetti. Ciò significa che i pacchetti sensibili al fattore tempo, come video e voce in tempo reale, verranno eliminati con la stessa frequenza dei dati che non sono sensibili al fattore tempo, come la posta elettronica e la navigazione sul Web.
Quando un router riceve un flusso audio digitale Real-Time Protocol (RTP) per Voice over IP (VoIP), deve compensare il jitter rilevato. Il meccanismo che gestisce questa funzione è il buffer del ritardo di riproduzione. Il buffer del ritardo di riproduzione deve bufferizzare questi pacchetti e quindi riprodurli in un flusso costante.
Se il jitter è così grande da far sì che i pacchetti vengano ricevuti fuori dal range di questo buffer, i pacchetti fuori range vengono scartati e i dropout vengono ascoltati nell'audio.
Per perdite piccole come un pacchetto, il processore di segnale digitale (DSP) interpola ciò che pensa che l'audio dovrebbe essere e nessun problema è udibile all'utente. Tuttavia, quando il jitter supera ciò che il DSP può fare per compensare i pacchetti mancanti, si sentono problemi audio.

I pacchetti voce devono ricevere una priorità più elevata rispetto ad altri tipi di traffico, la voce è molto sensibile ai ritardi e ai pacchetti interrotti per cui non c'è motivo di ritrasmettere la voce se i pacchetti vengono persi.
La voce può tollerare una certa quantità di latenza, jitter e perdita senza effetti evidenti. La latenza non deve essere superiore a 150 millisecondi (ms). Il jitter non deve superare i 30 ms e la perdita del pacchetto vocale non deve essere superiore all'1%. Il traffico vocale richiede almeno 30 Kbps di larghezza di banda.

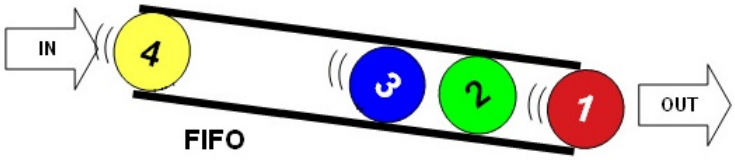
Il traffico video tende ad essere imprevedibile, incoerente ed improvviso rispetto al traffico voce. Rispetto alla voce, il video è meno resiliente alla perdita e ha un volume maggiore di dati per pacchetto.
Simile alla voce, il video può tollerare una certa quantità di latenza, jitter e perdita senza effetti evidenti. La latenza dovrebbe essere non più di 400 millisecondi (ms). Il jitter non deve essere superiore a 50 ms e la perdita di pacchetti video non deve essere superiore all'1%. Il traffico video richiede almeno 384 Kbps di larghezza di banda.

Le applicazioni dati che non tollerano la perdita di dati, come le e-mail e le pagine Web, utilizzano TCP per garantire che, se i pacchetti vengono smarriti durante il trasporto, verranno reindirizzati. Il traffico dati può essere fluido o esplosivo. Il traffico di controllo della rete è solitamente scorrevole e prevedibile. In caso di modifica della topologia, il traffico del controllo di rete potrebbe essere esplosivo per alcuni secondi.
I due fattori principali che un amministratore di rete deve valutare riguardo al flusso di traffico dati per garantire una buona QoE (Quality of Experience) di utilizzo della rete sono:

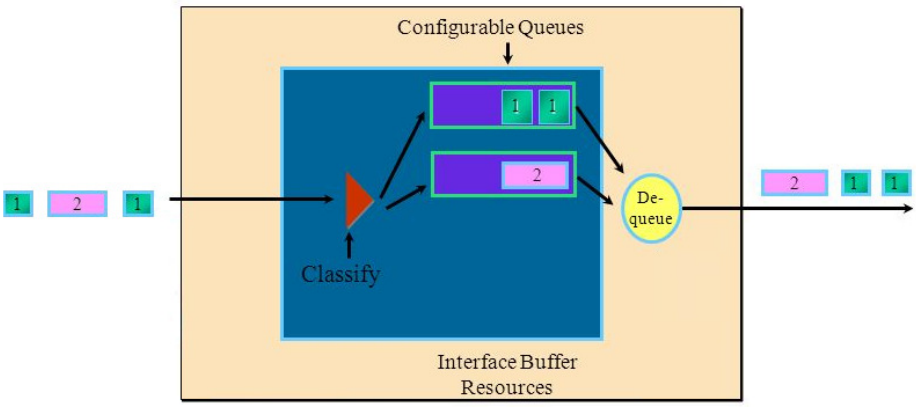
1. I dati provengono da un'applicazione interattiva?
2. L'importanza dei dati è critica?

La politica QoS implementata dall'amministratore di rete diventa attiva quando si verifica la congestione del collegamento. L'accodamento è uno strumento di gestione della congestione che può bufferizzare, assegnare priorità e, se necessario, riordinare i pacchetti prima di essere trasmessi alla destinazione.
Noi guarderemo i seguneti sistemi di accodamento:

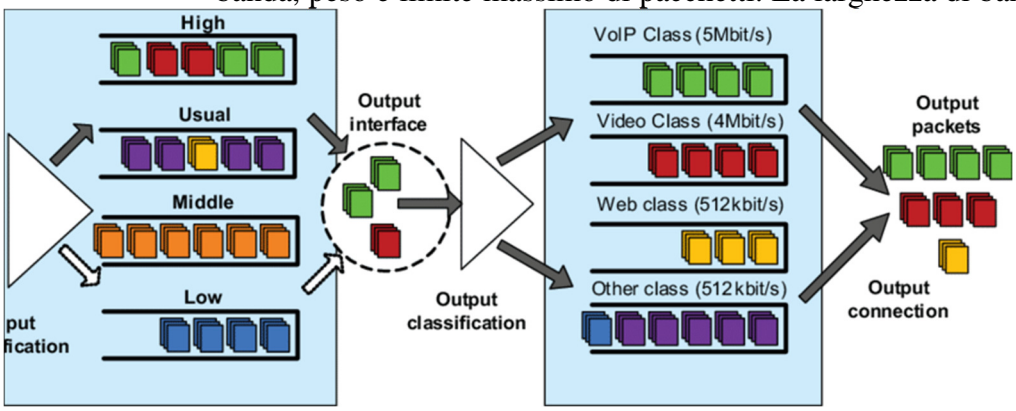
- First-In, First-Out (FIFO): non ha alcun concetto di priorità o classi di traffico e di conseguenza non prende decisioni sulla priorità dei pacchetti. C'è solo una coda e tutti i pacchetti sono trattati allo stesso modo. È il metodo più veloce di accodamento, è efficace per i link di grandi dimensioni che hanno un piccolo ritardo e una congestione minima.



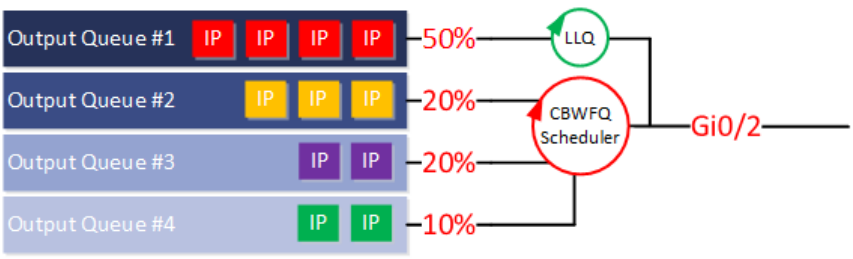
- Weighted Fair Queuing (WFQ): è un metodo di pianificazione automatizzata che fornisce un'equa allocazione della larghezza di banda a tutto il traffico di rete. WFQ applica priorità o pesi al traffico identificato e lo classifica in conversazioni o flussi. Determina quindi quanta larghezza di banda è consentita per ogni flusso rispetto ad altri flussi. L'algoritmo basato sul flusso utilizzato da WFQ pianifica simultaneamente il traffico interattivo nella parte anteriore di una coda per ridurre i tempi di risposta. Quindi condivide equamente la larghezza di banda rimanente tra i flussi ad alta larghezza di banda. Classifica il traffico in flussi diversi in base all'indirizzo di intestazione del pacchetto, incluse le caratteristiche come indirizzo IP di origine e di destinazione, indirizzi MAC, numeri di porta, protocollo e Type of Service (ToS). Il valore ToS nell'intestazione IP può essere utilizzato per classificare il traffico. WFQ non è supportato con tunneling e crittografia poiché queste funzionalità modificano le informazioni sul contenuto del pacchetto richieste da WFQ per la classificazione.



- Class-Based Weighted Fair Queuing (CBWFQ): ["Accodamento ponderato basato sulla classe"]: estende la funzionalità standard WFQ per fornire supporto per classi di traffico definite dall'utente. Si definiscono le classi di traffico in base ai criteri di corrispondenza, inclusi i protocolli, le ACL e le interfacce di input. I pacchetti che soddisfano i criteri di corrispondenza per una classe costituiscono il traffico per quella classe. Una coda FIFO è riservata per ogni classe e il traffico appartenente a una classe viene indirizzato alla coda per quella classe. Quando una classe è stata definita in base ai suoi criteri di corrispondenza, è possibile assegnarle caratteristiche. Per caratterizzare una classe, la si assegna larghezza di banda, peso e limite massimo di pacchetti. La larghezza di banda assegnata a una classe è la larghezza di banda garantita consegnata alla classe durante la congestione. Per caratterizzare una classe, si specifica anche il limite di coda per quella classe, che è il numero massimo di pacchetti consentiti per accumularsi nella coda per la classe.

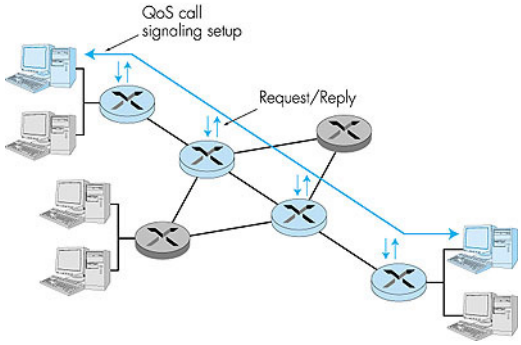


- Low Latency Queuing (LLQ): ha una rigorosa priority queuing (PQ) su CBWFQ. LLQ offre una coda di priorità rigorosa per CBWFQ, riducendo il jitter nelle conversazioni vocali, come mostrato nella figura. Con LLQ, i dati sensibili al ritardo vengono inviati per primi, prima che i pacchetti in altre code vengano trattati.



Il QoS (Quality of Service) può essere implementato in 3 modi:

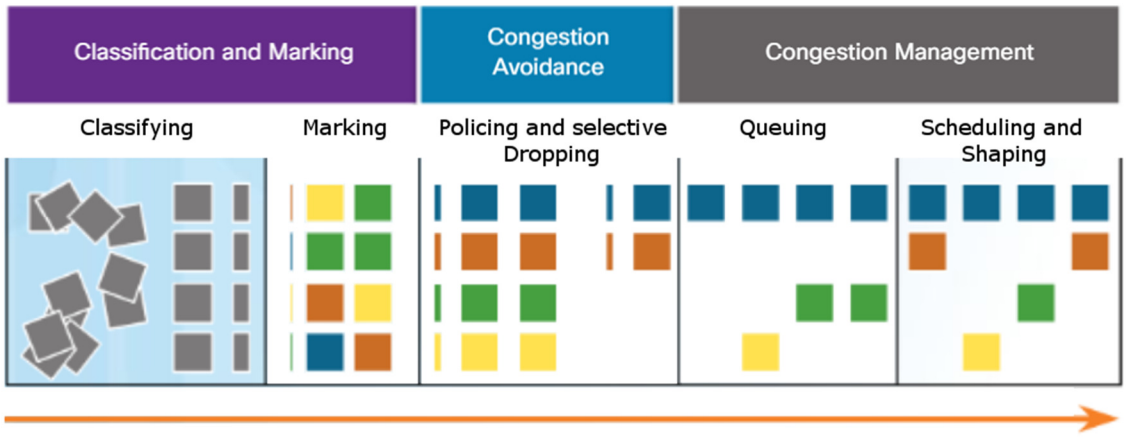
- Best-effort model
- Integrated services (IntServ): utilizza i meccanismi di prenotazione delle risorse e di controllo delle ammissioni come elementi costitutivi per stabilire e mantenere la QoS. Questa pratica è simile a un concetto noto come "hard QoS". Hard QoS garantisce le caratteristiche del traffico, come larghezza di banda, ritardo e velocità di perdita di pacchetti, da un capo all'altro. Hard QoS garantisce livelli di servizio prevedibili e garantiti per applicazioni mission-critical. Utilizza il protocollo RSVP (Resource Reservation Protocol) per segnalare le esigenze di QoS del traffico di un'applicazione lungo i dispositivi nel percorso end-to-end attraverso la rete. Se i dispositivi di rete lungo il percorso possono riservare la larghezza di banda necessaria, l'applicazione di origine può iniziare a trasmettere. Se la prenotazione richiesta non riesce lungo il percorso, l'applicazione di origine non invia alcun dato.
- Differentiated services (DiffServ): specifica un meccanismo semplice e scalabile per classificare e gestire il traffico di rete e fornire garanzie QoS sulle moderne reti IP. Non è una strategia di QoS end-to-end perché non può imporre garanzie end-to-end. Tuttavia, DiffServ QoS è un approccio più scalabile all'implementazione di QoS. A differenza di IntServ e hard QoS in cui gli host finali segnalano le loro esigenze di QoS alla rete, DiffServ non utilizza la segnalazione. Invece, DiffServ utilizza un approccio "soft QoS". Funziona sul modello QoS fornito, dove gli elementi di rete sono configurati per servire più classi di traffico, ciascuna con requisiti di QoS variabili. DiffServ applica e applica i meccanismi QoS su base hop-by-hop, applicando uniformemente il significato globale a ciascuna classe di traffico per fornire flessibilità e scalabilità.



QoS è davvero implementato in una rete quando sono utilizzati IntServ o DiffServ. IntServ fornisce la massima garanzia di QoS, ma è molto dispendioso in termini di risorse e quindi limitato nella scalabilità. Al contrario, DiffServ è meno dispendioso in termini di risorse e più scalabile. I due sono a volte co-implementati nelle implementazioni di QoS di rete.

La perdita di pacchetti è solitamente il risultato di una congestione su un'interfaccia. La maggior parte delle applicazioni utilizza il protocollo TCP per gestire questi problemi, in quanto TCP i segmenti TCP eliminati fanno sì che le sessioni TCP riducano le dimensioni delle finestre.
Ma per attenuare questo problema su applicazioni sensibili o che utilizzano UDP, possiamo utilizzare i seguenti approcci.

- Aumentare la capacità di collegamento per facilitare o prevenire la congestione.
- Garantire una larghezza di banda sufficiente e aumentare lo spazio del buffer (WFQ, CBWFQ e LLQ)
- Prevenire la congestione facendo cadere pacchetti a priorità più bassa prima che si verifichi la congestione (esempio - WRED: weighted random early detection)



Esistono tre categorie di strumenti QoS:

- Strumenti di classificazione e marcatura (Classification and marking):
- Strumenti per evitare la congestione (Congestion avoidance)
- Strumenti di gestione della congestione (Congestion management)

I pacchetti di ingresso (quadrati grigi) sono classificati e la loro intestazione IP è contrassegnata (quadrati colorati). Per evitare la congestione, i pacchetti vengono quindi allocati in base a politiche definite. I pacchetti vengono quindi messi in coda e inoltrati all'interfaccia di uscita in base alla loro politica di modellazione e politica di QoS definita.
NB: la classificazione e la marcatura possono essere eseguite all'ingresso o all'uscita, mentre altre azioni QoS come l'accodamento e la sagomatura vengono solitamente effettuate in uscita.

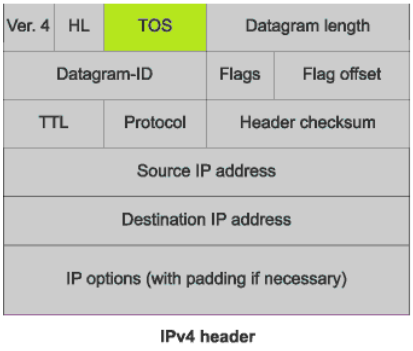
Marking:
Ci permettono di identificare o "marcare" tipi di pacchetti. La classificazione determina la classe di traffico a cui appartengono i pacchetti o i frame. Solo dopo che il traffico è stato segnato possono essere applicate politiche. I metodi per classificare i flussi di traffico ai livelli 2 e 3 includono l'uso di interfacce, ACL e mappe di classi. Il traffico può anche essere classificato ai livelli da 4 a 7 utilizzando Network Based Application Recognition (NBAR). Marcatura significa che stiamo aggiungendo un valore all'intestazione del pacchetto. La marcatura deve essere eseguita il più vicino possibile al dispositivo sorgente.
La decisione se contrassegnare il traffico ai livelli 2 o 3 (o entrambi) non è banale e dovrebbe essere presa dopo aver preso in considerazione i seguenti punti:

1. La marcatura Layer 2 dei frame può essere eseguita per il traffico non IP.
2. La marcatura Layer 2 dei frame è l'unica opzione QoS disponibile per gli switch che non sono "IP aware".
3. La marcatura di Layer 3 trasporterà le informazioni sulla QoS end-to-end.

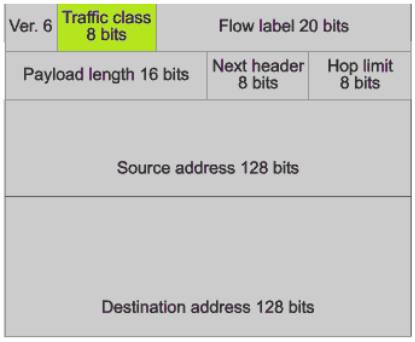
802.1Q è lo standard IEEE che supporta la codifica VLAN Layer2 su reti Ethernet. Quando viene implementato 802.1Q, due campi vengono aggiunti al frame Ethernet. Questi due campi vengono inseriti nel frame Ethernet seguendo il campo dell'indirizzo MAC di origine. Lo standard 802.1Q include anche lo schema di prioritizzazione QoS noto come IEEE 802.1p. Lo standard 802.1p utilizza i primi tre bit nel campo TCI (Tag Control Information). Conosciuto come il campo Priorità (PRI), questo campo a 3 bit identifica i CoS (Classe di servizio). Tre bit significa che un frame Ethernet Layer 2 può essere contrassegnato con uno degli otto livelli di priorità (valori 0-7)

CoS Value	CoS Binary Value	Description
0	000	Best-Effort Data
1	001	Medium-Priority Data
2	010	High-Priority Data
3	011	Call Signaling
4	100	Videoconferencing
5	101	Voice bearer (voice traffic)
6	110	Reserved
7	111	Reserved

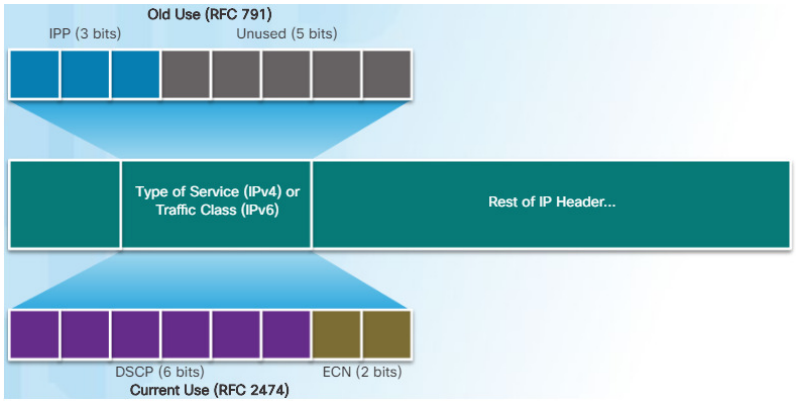
A Layer3 IPv4 e IPv6 specificano un campo a 8 bit nelle intestazioni dei pacchetti per contrassegnare i pacchetti. Sia IPv4 che IPv6 supportano un campo a 8 bit per la marcatura, il campo Tipo di servizio (ToS) per IPv4 e il campo Classe traffico per IPv6. Questi campi sono utilizzati per trasportare il contrassegno del pacchetto assegnato dagli strumenti di classificazione QoS. Il campo viene quindi indicato dai dispositivi riceventi per inoltrare i pacchetti in base alla politica QoS assegnata appropriata.



IPv4 header

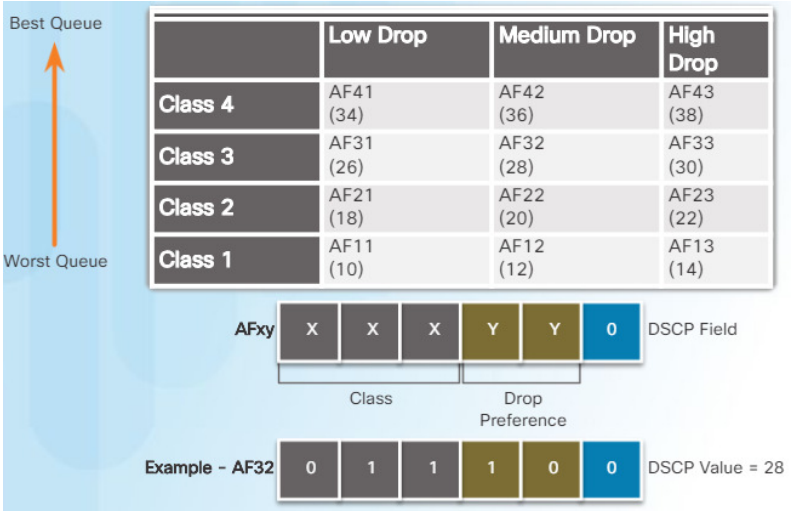


IPv6 header



La Figura accanto mostra il contenuto del campo a 8 bit. In RFC791, lo standard IP originale specificava il campo IP Precedence (IPP) da utilizzare per i contrassegni QoS. Tuttavia, in pratica, questi tre bit non hanno fornito una granularità sufficiente per implementare QoS.
RFC2474 sostituisce RFC791 e ridefinisce il campo ToS rinominando ed estendendo il campo IPP. Il nuovo campo, come mostrato nella Figura, ha 6 bit allocati per QoS. Tale campo è il DSCP (Differentiated Services Code Point), questi sei bit offrono un massimo di 64 possibili classi di servizio. I rimanenti due bit denominati Extended Congestion Notification (ECN) possono essere utilizzati dai router compatibili con ECN per contrassegnare i pacchetti invece di eliminarli. Il marchio ECN informa i router a valle della presenza di congestione nel flusso dei pacchetti.
I 64 valori DSCP sono organizzati in tre categorie:

- Best-Effort (BE): è l'impostazione predefinita per tutti i pacchetti IP. Il valore DSCP è 0. Il comportamento per-hop è il routing normale. Nessun piano QoS è implementato.
- Expedited Forwarding (EF): RFC3246 definisce EF come valore decimale DSCP 46 (binario 101110). I primi 3 bit (101) mappano direttamente al valore 5 CoS di Layer 2 utilizzato per il traffico vocale.
- Assured Forwarding (AF): RFC2597 definisce AF per utilizzare i 5 bit DSCP più significativi per indicare le code e la preferenza di rilascio. I primi 3 bit più significativi vengono utilizzati per designare la classe. La classe 4 è la migliore coda e la prima è la coda peggiore. Il 4° e il 5° bit più significativi sono usati per designare la preferenza di caduta. Il 6° bit più significativo è impostato su zero. La formula AFxy mostra come vengono calcolati i valori AF. Ad esempio, AF32 appartiene alla classe 3 (binario 011) e ha una preferenza di caduta media (binario 10). Il valore DSCP completo è 28 perché si include il sesto bit 0 (011100 binario).



Poiché i primi 3 bit più significativi del campo DSCP indicano la classe, questi bit vengono anche chiamati bit di selezione classi (CS).

IMPORTANTE

Si ricorda che è bene categorizzare/marcare il traffico il prima possibile (ossia il più vicino possibile alla sorgente) all'interno di una rete, in modo da facilitare il passaggio dei pacchetti all'interno degli apparati di rete.
Tutto questo per evitare una possibile e futura congestione della rete.
Questo anche per poter migliorare la gestione della rete attraverso configurazioni di shaping (modellazione) della rete.

Il traffic shaping mantiene i pacchetti in eccesso in una coda e pianifica l'eccesso per una successiva trasmissione su intervalli di tempo. Il risultato del traffic shaping è una velocità di uscita del pacchetto livellata.
NB: assicurarsi di avere memoria sufficiente quando si abilita la modellazione. Inoltre, la modellazione richiede una funzione di pianificazione per la successiva trasmissione di eventuali pacchetti ritardati. Questa funzione di pianificazione consente di organizzare la coda di shaping in diverse code. Esempi di funzioni di pianificazione sono CBWFQ e LLQ.
Shaping è un concetto in uscita

Il Policing è comunemente implementato dagli ISP e per semplificare il concetto è una limitazione alla banda in ingresso, ossia è come lo shaping, ma in ingresso, ed i pacchetti che non possono passare in quel determinato momento non vengono "cachati", ma persi

FINE CAPITOLO 6

Secondo CISCO, internet evolverà ancora fino a connettere oltre 50 miliardi di dispositivi nel mondo entro il 2020. Per adeguardi/avvicinarsi a tutto ciò CISCO ha ideato 6 pilastri per la gestione del sistema IoT.

1) Network Connectivity Pillar: identifica i dispositivi che possono essere utilizzati per fornire connettività IoT a molti settori e applicazioni diversi
2) Fog Computing Pillar: questo modello di rete IoT è l'evoluzione delle reti client-server e delle reti cloud, identifica un'infrastruttura di calcolo distribuita più vicina al bordo della rete. Consente ai dispositivi periferici di eseguire applicazioni localmente e prendere decisioni immediate. Ciò riduce l'onere di dati sulle reti poiché non è necessario inviare dati non elaborati tramite le connessioni di rete. Migliora la resilienza consentendo ai dispositivi IoT di funzionare quando si perdono le connessioni di rete. Migliora inoltre la sicurezza mantenendo i dati sensibili trasportati oltre il limite in cui è necessario.
   I modelli non si escludono a vicenda. Gli amministratori di rete possono utilizzare qualsiasi combinazione dei tre modelli per soddisfare le esigenze degli utenti della rete.
3) Security Pillar: l'IoT introduce nuovi vettori di attacco che normalmente non si incontrano con le normali reti aziendali. Il pilastro di sicurezza offre soluzioni scalabili di cybersicurezza, consentendo a un'organizzazione di scoprire, contenere e correggere rapidamente ed efficacemente un attacco per ridurre al minimo i danni.
   Queste soluzioni di sicurezza informatica includono:
   - Sicurezza specifica della tecnologia operativa (OT);
   - Sicurezza della rete IoT;
   - IoT Sicurezza fisica;
4) Data Analytics Pillar: l'IoT può collegare miliardi di dispositivi in grado di creare exabyte di dati ogni giorno. Per fornire valore, questi dati devono essere elaborati rapidamente e trasformati in informazioni fruibili. L'infrastruttura analitica è composta da componenti dell'infrastruttura di rete distribuita e interfacce di programmazione delle applicazioni (API) specifiche di IoT.
5) Management and Automation Pillar: l'IoT amplia notevolmente le dimensioni e la diversità della rete per includere i miliardi di oggetti intelligenti che rilevano, monitorano, controllano e reagiscono. Cisco offre un'ampia gamma di funzionalità di gestione e automazione IoT su tutta la rete estesa.
6) Application Enablement Platform Pillar: fornisce l'infrastruttura per l'hosting di applicazioni e la mobilità delle applicazioni tra cloud e Fog computing.

Servizi cloud

I servizi cloud sono disponibili in una varietà di opzioni, su misura per soddisfare le esigenze dei clienti. I tre principali servizi di cloud computing definiti sono:

- Software as a Service (SaaS): il fornitore di servizi cloud è responsabile dell'accesso a servizi forniti su Internet (esempio Office 365). L'utente deve solo fornire i propri dati.
- Platform as a Service (PaaS): il fornitore di servizi cloud è responsabile dell'accesso agli strumenti di sviluppo e ai servizi utilizzati per fornire le applicazioni.
- Infrastructure as a Service (IaaS): il fornitore di servizi cloud è responsabile dell'accesso alle apparecchiature di rete, ai servizi di rete virtualizzati e all'infrastruttura di rete di supporto.

NB: i fornitori di servizi cloud hanno esteso questo modello per fornire anche il supporto IT per ciascuno dei servizi di cloud computing (ITaaS).

Esistono quattro modelli di cloud primari:

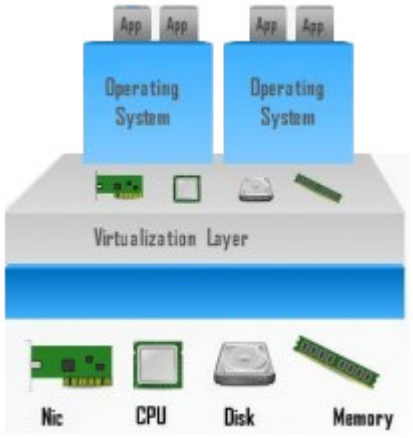
- ✓ Cloud pubbliche: le applicazioni e i servizi basati su cloud offerti in un cloud pubblico sono resi disponibili alla popolazione generale. I servizi possono essere gratuiti o offerti su un modello pay-per-use, come il pagamento per l'archiviazione online (es. google drive, dropbox, ecc..)
- ✓ Cloud privati: le applicazioni e i servizi basati su cloud offerti in un cloud privato sono destinati a un'organizzazione o entità specifica, ad esempio il governo. Un private cloud può essere configurato utilizzando la rete privata dell'organizzazione, sebbene possa essere costoso da costruire e mantenere. Un cloud privato può anche essere gestito da un'organizzazione esterna con una rigorosa sicurezza di accesso.
- ✓ Cloud ibrido: è composto da due o più nuvole (esempio: parte privata, parte pubblica), in cui ogni parte rimane un oggetto distintivo, ma entrambe sono connesse utilizzando un'unica architettura
- ✓ Cloud community: viene creato per uso esclusivo da una specifica comunità. Le differenze tra cloud pubblici e cloud community sono le esigenze funzionali che sono state personalizzate per la comunità.

La virtualizzazione del server sfrutta le risorse inattive e consolida il numero di server richiesti.
L'hypervisor è un programma, firmware o hardware che aggiunge un livello di astrazione all'hardware fisico reale. Il livello di astrazione viene utilizzato per creare macchine virtuali che hanno accesso a tutto l'hardware della macchina fisica come CPU, memoria, controller del disco e schede NIC. Ciascuna di queste macchine virtuali esegue un sistema operativo completo e separato.
Uno dei principali vantaggi della virtualizzazione è il costo complessivo ridotto poichè:

- Sono richieste meno apparecchiature;
- Meno energia viene consumata;
- È richiesto meno spazi sia fisico sia virtuale;

INOLTRE:

- Semplificazione della prototipazione
- Se viene commesso un errore, un amministratore può semplicemente ripristinare una versione precedente
- Provisioning server più veloce
- Aumento del tempo di attività del server
- Miglioramento del disaster recovery
- Supporto legacy



Lo schema accanto illustra l'impostazione di un sistema di virtualizzazione (figura Hypervisor di tipo 1)
Un hypervisor è un software che crea ed esegue istanze VM. Il computer su cui un hypervisor supporta una o più macchine virtuali è una macchina host. Gli hypervisor di tipo 2 sono anche chiamati hypervisor ospitati. Questo perché l'hypervisor è installato sul sistema operativo esistente, come Mac OS X, Windows o Linux (VMWare Player, VirtualBOX, VMWare Fusion, ecc…)

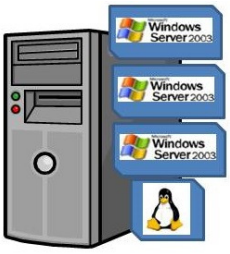
Gli hypervisor di tipo 1 sono anche chiamati "bare metal" perché l'hypervisor viene installato direttamente sull'hardware. Gli hypervisor di tipo 1 vengono generalmente utilizzati su server aziendali e dispositivi di rete del data center.
Gli hypervisor di tipo 1 hanno accesso diretto alle risorse hardware; quindi, sono più efficienti delle architetture ospitate, migliorano la scalabilità, le prestazioni e la robustezza.
Sono state sviluppate due principali architetture di rete per supportare la virtualizzazione della rete:

- Software Defined Networking (SDN) - Un'architettura di rete che virtualizza la rete. Il controller SDN è un'entità logica che consente agli amministratori di rete di gestire e stabilire in che modo il piano dati degli switch virtuali e dei router deve gestire il traffico di rete. Organizza, media e facilita la comunicazione tra le applicazioni e gli elementi di rete.
  Il controller SDN definisce i flussi di dati che si verificano nel piano dati SDN. Un flusso è una sequenza di pacchetti che attraversano una rete che condivide un insieme di valori di campo di intestazione. Ogni flusso che attraversa la rete deve prima ottenere l'autorizzazione dal controller SDN, che verifica che la comunicazione sia consentita in base al criterio di rete. Se il controller consente un flusso, calcola un percorso per il flusso da intraprendere e aggiunge una voce per quel flusso in ciascuno degli interruttori lungo il percorso.
  Tutte le funzioni complesse vengono eseguite dal controller.
- Cisco Application Centric Infrastructure (ACI): una soluzione hardware specifica per integrare il cloud computing e la gestione del data center. i tre componenti principali dell'architettura ACI sono:
  1) Application Network Profile (ANP): è una raccolta di gruppi di punti finali (EPG), le loro connessioni e le politiche che definiscono tali connessioni. Un ANP è spesso molto più complesso.
  2) Application Policy Infrastructure Controller (APIC): è considerato il cervello dell'architettura ACI. APIC è un controller software centralizzato che gestisce un tessuto cluster scalabile ACI. È progettato per la programmabilità e la gestione centralizzata. Traduce le politiche applicative nella programmazione di rete.
  3) Switch Cisco Nexus serie 9000: questi switch forniscono uno switch fabric sensibile alle applicazioni e funzionano con un APIC per gestire l'infrastruttura di rete virtuale e fisica.

Vi sono altre tecnologie di virtualizzazione della rete, alcune delle quali sono incluse come componenti in SDN e ACI:

- OpenFlow: è un elemento fondamentale nella creazione di soluzioni SDN
- OpenStack: questo approccio è una piattaforma di virtualizzazione e orchestrazione disponibile per creare ambienti cloud scalabili e fornire una soluzione di infrastruttura come servizio (IaaS). OpenStack è spesso utilizzato con Cisco ACI.
- Altri componenti: includono l'interfaccia al sistema di routing (I2RS), l'interconnessione trasparente di molti collegamenti (TRILL), Cisco FabricPath (FP) e IEEE 802.1aq Shortest Path Bridging (SPB).

Ricapitolando/Riassumento:



no virtualization without datacenter

no cloud without virtualization

FINE CAPITOLO 7

Quest'ultimo capitolo sarà un vademecum delle attività che è meglio fare o controllare per risolvere i problemi che possiamo incontrare nella realizzazione/implementazione/espansione delle reti.

8.0.1.2 Network Breakdown Instructions.pdf

Per consentire agli amministratori di rete di monitorare e risolvere i problemi di una rete, è necessario disporre di un set completo di documentazione di rete accurata e attuale.
Questa documentazione deve include:

- File di configurazione
- Diagrammi di topologia fisica e logica: tengono traccia della posizione, della funzione e dello stato dei dispositivi sulla rete. Una topologia di rete fisica mostra il layout fisico dei dispositivi connessi alla rete. È necessario sapere in che modo i dispositivi sono fisicamente collegati per risolvere i problemi del livello fisico. Una topologia di rete logica illustra come i dispositivi sono connessi logicamente alla rete, ovvero come i dispositivi trasferiscono effettivamente i dati attraverso la rete quando comunicano con altri dispositivi.
- Un livello di prestazioni di base: viene utilizzata per stabilire le normali prestazioni di rete o di sistema. Stabilire una base di riferimento delle prestazioni di rete richiede la raccolta di dati sulle prestazioni dalle porte e dai dispositivi essenziali per il funzionamento della rete. L'analisi dopo una linea di base iniziale tende anche a rivelare problemi nascosti.
  Per stabilire e acquisire un livello di prestazioni di base iniziale della rete, effettuare le seguenti operazioni:
  1) Determinare quali tipi di dati raccogliere
  2) Identificare dispositivi e porte di interesse
  3) Determinare la durata di registrazione delle prestazioni di base della rete: Il tempo necessario e le informazioni di base raccolte devono essere sufficienti per stabilire un'immagine tipica della rete. Le misurazioni non dovrebbero essere eseguite durante i periodi di modelli di traffico univoci, in quanto i dati fornirebbero un'immagine imprecisa delle normali operazioni di rete. L'analisi di base della rete dovrebbe essere condotta su base regolare.

Quando si documenta la rete, è spesso necessario raccogliere informazioni direttamente da router e switch. Ovviamente utili comandi di documentazione di rete includono ping, traceroute e telnet, nonché i seguenti comandi show.
show ip interface
show ip interface brief
show ipv6 interface
show ipv6 interface brief
show ip route
show ipv6 route
show cdp neighbors detail
show arp
show running-config
show port
show vlan
show tech-support
show ip cache flow
La raccolta manuale dei dati utilizzando i comandi show sui singoli dispositivi di rete richiede molto tempo e non è una soluzione scalabile, per questo vengono utilizzati software sofisticato di gestione della rete. Il software di gestione della rete o gli ispettori e gli sniffer del protocollo spesso funzionano continuamente nel corso del processo di raccolta dei dati.

8.1.1.8 Packet Tracer - Troubleshooting Challenge - Documenting The Network Instructions.pdf
8.1.1.8 Packet Tracer - Troubleshooting Challenge - Documenting The Network.pka

Esistono tre fasi principali del processo di risoluzione dei problemi:

A) Raccolta dei sintomi
B) Isolare il problema
C) Implementazione di azioni correttive

Se l'azione correttiva crea un altro problema o non risolve il problema, la soluzione tentata viene documentata, le modifiche vengono rimosse e l'amministratore di rete torna a raccogliere i sintomi e ad isolare il problema.
Queste fasi non si escludono a vicenda. In qualsiasi momento del processo, potrebbe essere necessario tornare alle fasi precedenti.

Scorporiamo ora le fasi sopra.
A - Raccolta dei sintomi: vi sono 5 passaggi da fare:

1) Raccolta di informazioni: raccogliere informazioni dalla trouble ticket, dagli utenti o dai sistemi finali interessati
2) Determinazione della proprietà: se il problema è sotto il controllo dell'organizzazione, passare alla fase successiva. Se il problema non rientra nei limiti del controllo dell'organizzazione (ad esempio, la connettività Internet persa), contattare un amministratore
3) Ridurre l'ambito: determinare se il problema si trova nel livello di base, di distribuzione o di accesso della rete.
4) Raccogliere i sintomi dai dispositivi sospetti - Utilizzando un approccio di risoluzione dei problemi stratificato, raccogliere i sintomi hardware e software dai dispositivi sospetti.
5) Documentare i sintomi - A volte il problema può essere risolto utilizzando i sintomi documentati.

B - Isolare il problema: dopo aver raccolto tutti i sintomi, se non viene identificata alcuna soluzione, l'amministratore di rete confronta le caratteristiche del problema con i livelli logici della rete per isolare e risolvere il problema. Modelli di rete logici, separano le funzionalità di rete in livelli modulari. Questi modelli a strati possono essere applicati alla rete fisica per isolare i problemi di rete durante la risoluzione dei problemi. Ad esempio, se i sintomi suggeriscono un problema di connessione fisica, il tecnico di rete può concentrarsi sulla risoluzione dei problemi del circuito che opera a livello fisico.

Per la risoluzione dei problemi dopo aver raccolto le informazioni, si posso utilizzare 3 principali metodologie:

- ✓ Bottom-up: si inizia con i componenti fisici della rete e si passa attraverso i livelli del modello OSI finché non viene identificata la causa del problema. Lo svantaggio è che è necessario controllare ogni dispositivo e interfaccia sulla rete finché non viene trovata la possibile causa del problema.
- ✓ Top-down: la risoluzione dei problemi top-down inizia con le applicazioni dell'utente finale e si sposta verso il basso attraverso i livelli del modello OSI fino a quando non viene identificata la causa del problema. Lo svantaggio con l'approccio top-down è la necessità di controllare ogni applicazione di rete finché non viene trovata la possibile causa del problema.
- ✓ Divide-and-conquer: l'amministratore di rete seleziona un livello OSI e verifica in entrambe le direzioni da quel livello. (esempio quando ci segnalano in problema remoto, dopo esserci collegati in VPN guardiamo se il serer è UP, nel caso lo sia, verifichiamo i suoi servizi ecc…)

Concetti di IP SLA
Gli amministratori di rete devono essere proattivi e monitorare e testare continuamente la rete. L'obiettivo è scoprire un errore di rete il prima possibile. Uno strumento utile per questa attività è il Cisco IOS IP Service Level Agreement (SLA).
IP SLA utilizza il traffico generato per misurare le prestazioni della rete tra due dispositivi di rete, più percorsi di rete o tra più percorsi di rete.
Le misurazioni fornite dalle varie operazioni IP SLA possono essere utilizzate per la risoluzione dei problemi delle reti fornendo misure coerenti e affidabili che identificano immediatamente i problemi e risparmiano tempo per la risoluzione.
Vi sono ulteriori vantaggi per l'utilizzo degli IP SLA:

- Monitoraggio, misurazione e verifica degli accordi a livello di servizio
- Monitoraggio delle prestazioni di rete per fornire misurazioni continue, affidabili e prevedibili per misurare il jitter, la latenza o la perdita di pacchetti nella rete
- Valutazione dello stato della rete del servizio IP per verificare che la QoS esistente sia sufficiente per i nuovi servizi IP
- Monitoraggio della disponibilità di rete da bordo a bordo per la verifica proattiva della connettività delle risorse di rete

Le informazioni IP SLA possono essere visualizzate utilizzando i comandi CLI o tramite SNMP.
Vediamo come configurare IP SLA
(dalla privileged exec)
show ip sla application
(dalla configuration terminal)
ip sla 34
icmp-echo 192.168.1.33
frequency 30
exit
ip sla schedule 1 start-time life forever
exit
Per verificare:
(dalla privileged exec)
show ip sla configuration 34
show ip sla statistics 34

8.2.1.5 Lab - Configure IP SLA ICMP Echo.pdf

8.2.4.12 Packet Tracer - Troubleshooting Enterprise Networks 1 Instructions.pdf
8.2.4.12 Packet Tracer - Troubleshooting Enterprise Networks 1.pka
8.2.4.13 Packet Tracer - Troubleshooting Enterprise Networks 2 Instructions.pdf
8.2.4.13 Packet Tracer - Troubleshooting Enterprise Networks 2.pka
8.2.4.14 Packet Tracer - Troubleshooting Enterprise Networks 3 Instructions.pdf
8.2.4.14 Packet Tracer - Troubleshooting Enterprise Networks 3.pka
8.2.4.15 Packet Tracer - Troubleshooting Challenge - Using Documentation to Solve Issues.pdf
8.2.4.15 Packet Tracer - Troubleshooting Challenge - Using Documentation to Solve Issues.pka
8.3.1.1 Documentation Development Instructions.pdf
8.3.1.2 Packet Tracer - CCNA Skills Integration Challenge Instructions.pdf
8.3.1.2 Packet Tracer - CCNA Skills Integration Challenge.pka

FINE CAPITOLO 8