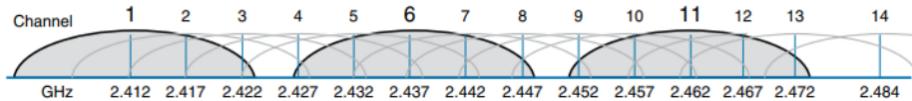


Domande esame

1. Quale dei seguenti è un servizio fornito da UDP:
 - Multiplexing
2. ACL che blocca il traffico TCP: access-list extended 100 deny tcp any any
3. Quale memoria dello switch contiene la running configuration:
 - RAM
4. L'instaurazione della connessione TCP si riferisce al processo di inizializzazione dei campi Sequence e Acknowledgment e all'accordo su:
 - Numeri di porta utilizzati
5. L'immagine mostra:

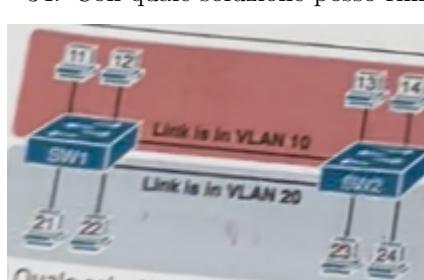


- Canali utilizzabili nel 2.5 Ghz
6. IPv6 prevede indirizzi lunghi:
 - 128 bit
 7. Converti da Hex a binario:
 - 8: 1000
 - F: 1111
 - 0: 0000
 8. Abbrevia F520:7F6B:A03F:0000:0000:0053:0000:2DCF:
 - F520:7F6B:A03F::53:0:2DCF
 9. Protocollo 802.1Q prevede al massimo quante VLAN:
 - 4096
 10. Scrivi il prefisso, non abbreviato, di 210F::AAAA:B080:7878:9009/64:
 - 210F:0000:0000:0000:0000:0000:0000:0000/64
 11. Quali indirizzi IPv6 funzionano in modo simile a quelli privati IPV4:
 - Unique local
 12. Metrica usata da OSPF per scegliere il percorso migliore:
 - Cost
 13. Scrivi il subnet ID di 172.16.150.41/18:
 - 172.16.128.0

14. Administrative distance di default per rotta statica è:
- 1
15. OSPF multiarea, caratteristiche di un Area Border Router:
- Sta sia nella backbone sia nella singola area
16. Converti da decimale a binario:
- 259: 100000011
 - 111: 1101111
 -
17. PortFast va attivato nelle porte destinate alla connessione con:
- PC
 - Notebook
18. Rota statica che mandi tutto il traffico destinato alla rete 192.168.15.0/24 verso 182.168.2.6:
- ip route 192.168.15.0 255.255.255.0 182.168.2.6
- 19.
20. Subnetting della rete 172.10.0.0/16 per consentire 800 host per sottorete:
- Classe:
 - Nuova maschera
 - Numero di sottoreti:
 - Host per subnet:
 - Subnet ID della prima sottorete:
 - Broadcast address della prima sottorete:
21. Quante reti IPv4 private di classe B esistono:
- 16
22. Classe dell'indirizzo 224.1.1.1:
- D
23. L'utilizzo di due link paralleli tra SW1 e SW2, non bloccati da STP è possibile grazie a cosa:
- PortFast
24. Se l'IP viene scelto dal Server tramite un pool e resta assegnato ad un certo MAC che tipo di DHCP è:
- Automatico
25. Comando per abilitare Telnet in aggiunta a SSH:
- transport input telnet ssh

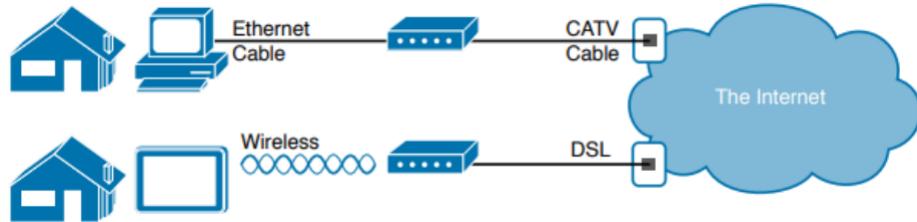
26. Quale modalità di VTP non è possibile creare VLAN:
- VTP client mode
27. Sinonimo di layer 3:
- Livello di rete
28. Il comando interface gigabitethernet 0/0 20 crea cosa:
- VLAN
29. Quale tra questo è un indirizzo IPv6 unique local:
- FD6D:8D64:AF0C:2::
30. Quale OSPF neighbor state è atteso quando lo scambio di informazioni sulla topologia è in corso:
- 2-way
31. I router non instradano i pacchetti di che tipo:
- Link local
- 32.
-
- 32) Gli switch A e B sono il core della rete e sono interconnessi da un link a 1000Mbps. Tutti gli altri link sono a 100Mbps. STP blocca il collegamento tra C e B per evitare loop. Quando alla rete viene aggiunto un nuovo switch (D) si vuole evitare che quest'ultimo venga eletto come nuovo Root Bridge, per garantire che il link 1000Mbps rimanga attivo.
Come ottengo questo risultato in maniera corretta?
○ Configurando BPDU guard su Switch C
○ Disabilitando STP su Switch D
○ Utilizzando PortFast
Configurando RootGuard su Switch C

configurare e manutenere innumerevoli VLAN all'interno di ...
È possibile ottimizzare questo processo?
- Configurando RootGuard su Switch C
33. Come si può ottimizzare il processo di manutenere e configurare innumerevoli VLAN:
- Usando VTP
34. Con quale soluzione posso rimuovere uno dei due link tra switch:



- Trunking
35. Scrivi accanto a ogni concetto il livello della pila TCP/IP a cui appartiene:
- Richiesta HTTP: Layer 5
 - Default gateway: Layer 3
36. NTP sta per:
- Network Time Protocol
37. Sinonimo per layer 4:
- Transport
38. A cosa può servire configurare una sottointerfaccia:
- Configurare il trunking o ROAS
39. Quale tra queste non è una fase del lavoro di OSPF
- Counting hops
40. Cos'è il roaming:
- Passaggio da una cella ad un'altra
41. Quale bridge IP vince le elezioni STP come root:
- 40097:0200:1000:1000
42. Host A è connesso alla VLAN 1 di SW1. Chi tipicamente ha un IP nella stessa subnet di A:
- interface vlan 1 dello switch
43. Il messaggio layer 2 è detto:
- frame
- 44.

Networking



Con il termine networking model si riferisce ad un insieme di documenti, ognuno dei quali descrive un aspetto di una rete.

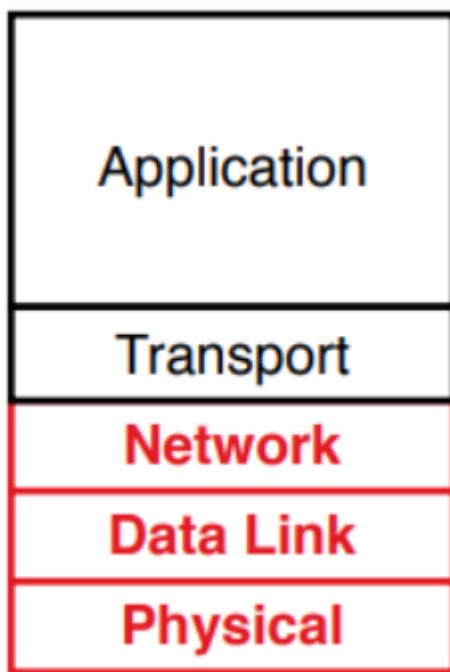
Un documento può descrivere un protocollo (insieme di regole logiche che i dispositivi devono seguire per comunicare) o requisiti fisici.

TCP/IP

Il modello supportato da tutti è TCP/IP che include una serie di protocolli per far comunicare tra loro i computer, i protocolli vengono definiti tramite i Requests For Comments (RFC).

TCP/IP include anche protocolli più vecchi non definiti tramite RFC, come l'Ethernet LAN, ma dal IEEE.

TCP/IP usa un modello a strati per rendere più comprensibile il network model:



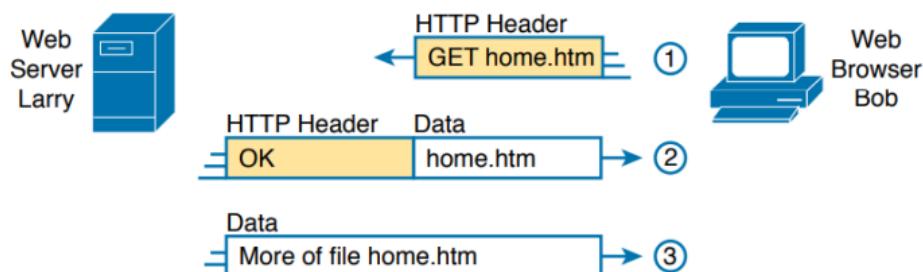
Il layer più basso si occupa della trasmissione dei bit su ogni canale fisico, il data link su una tipologia di link fisico (Ethernet o wireless), il network si occupa della consegna dei dati attraverso l'intero percorso e i due superiori riguardano le applicazioni che ricevono/inviano i dati.

TCP/IP Architecture Layer	Example Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internet	IP, ICMP
Data Link & Physical	Ethernet, 802.11 (Wi-Fi)

Application layer

I protocolli di questo livello forniscono servizi al software, NON definisce l'applicazione ma i servizi da essa usati.

Es: un applicativo browser usa il protocollo HTTP.

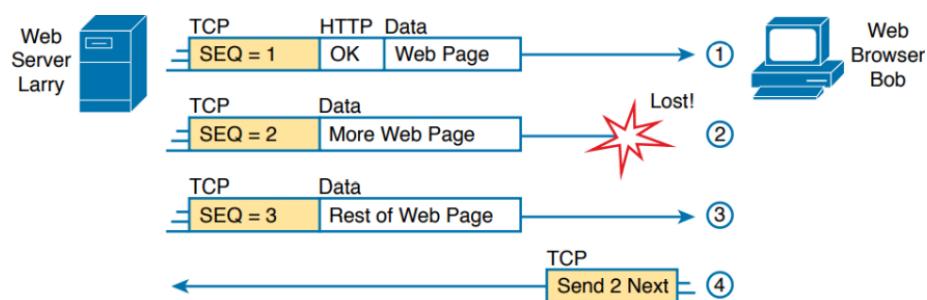


Notiamo come il terzo msg non ha un header perché il protocollo dopo il primo messaggio li omette.

Transport Layer

I protocolli di questo livello forniscono servizi a quelli superiori e sono due:

- TCP: prima di inviare si assicura di instaurare una connessione, si occupa anche della correzione dei messaggi infatti ogni messaggio gestito dal TCP contiene un numero che indica il numero di sequenza di invio (SEQ), se il client riceve un numero che non corrisponde a quello che avrebbe dovuto ottenere (Es: 1->2->3 ma ottiene 1->3) capisce che uno è andato perso e richiede il rinvio.



- UDP: meno usato e non si ha la certezza dell'arrivo dei messaggi.

Same/adjacent-layer interaction

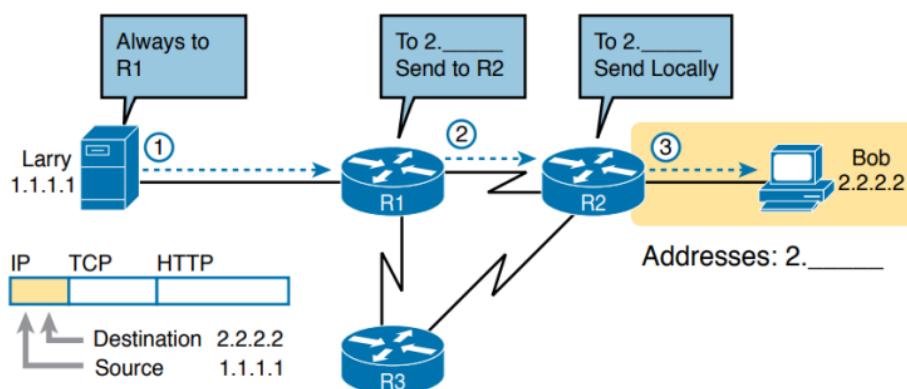
Il adjacent-layer interaction è quando livelli adiacenti (diversi) lavorino insieme sullo stesso computer; es: HTTP usa il ripristino degli errori di TCP.

Il same-layer interaction è quando due livelli uguali comunicano su due computer diversi e quindi utilizzano i loro header per scambiarsi messaggi; es: Larry e Bob usano i SEQ per controllare che i messaggi siano arrivati nell'ordine giusto.

Network layer

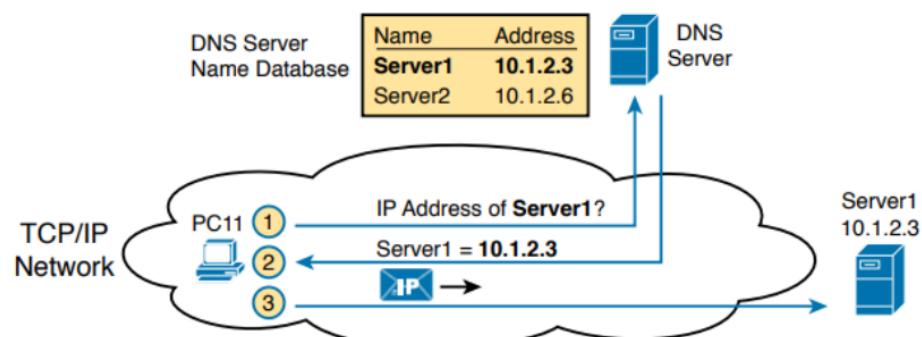
In questo livello il protocollo principale è IP, fra le principali funzionalità ci sono l'indirizzamento e l'instradamento.

Per funzionare IP definisce che ogni host deve avere un proprio indirizzo univoco in maniera da essere identificato in una rete, è composto da 4 numeri separati da punto (notazione dotted-decimal).



Altri protocolli di rete sono:

- DNS: serve per identificare i device grazie agli hostname.

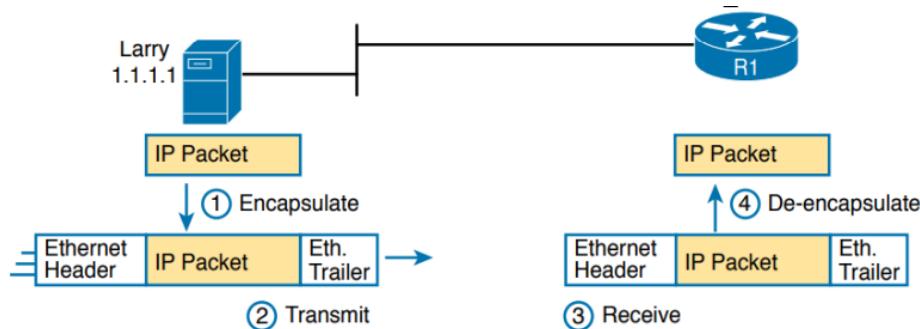


- ARP: serve per apprendere dinamicamente l'indirizzo MAC di qualsiasi macchina connessa alla rete, per farlo il protocollo invia un messaggio in broadcast chiedendo di chi è il MAC da cercare.
- PING: utilizza un altro protocollo chiamato ICMP, serve per testare la connessione fra due apparati.

Data-Link e Physical layer

Lavorano a stretto contatto per definire protocolli e tipo di hardware necessari per recapitare dati attraverso una rete fisica.

Il physical si occupa di aspetti di cablaggio e segnali elettrici, ma alcune convenzioni su questi argomenti spettano comunque al data-link.



Data encapsulation terminology

Indica il processo di aggiungere header e trailer attorno ai dati gestiti dai vari livelli.

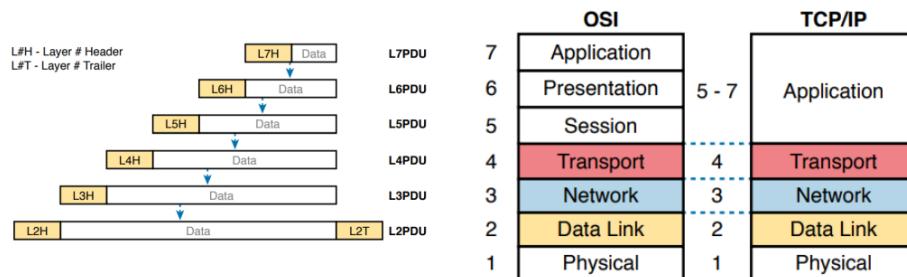
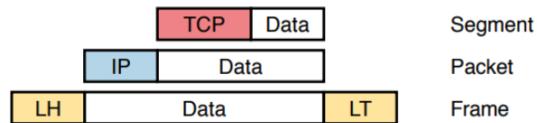
Ogni livello aggiunge qualcosa al dato:

- Application: un msg HTTP può restituire un OK nel header;
- Transport: il messaggio + header application viene processato dal transport che mette il proprio header TCP o UDP;
- Network: come prima al nuovo messaggio aggiungiamo un altro header che contiene i vari indirizzi IP;
- Data-Link: il data link aggiunge non solo un header ma anche un trailer finale
- Physical: non aggiunge nulla e si occupa di inviare il messaggio.

Ogni messaggio cambia nome in base a che header ha al momento:

- Data + TCP: Segmento;
- Data + IP: Pacchetto;
- Data + Data-Link trailer e header: Frame.

Data Encapsulation Terminology



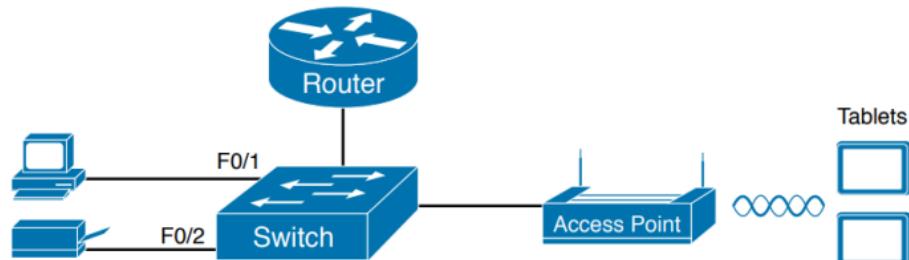
Oltre ai nomi detti sopra ogni PDU (il messaggio + header/trailer) può essere identificato con il numero del livello, es: Data + Data-Link = L2PDU (perchè livello 2).

Ethernet LAN

Lo standard ethernet non è solo rame, comprende diverse tipologie di cavi.

Noi vedremo lo standard applicato ad una LAN SOHO(small office/home office), per creare una LAN si necessita di un device detto Ethernet LAN switch, che ha porte dove connettere i cavi (necessariamente conformi allo standard ethernet).

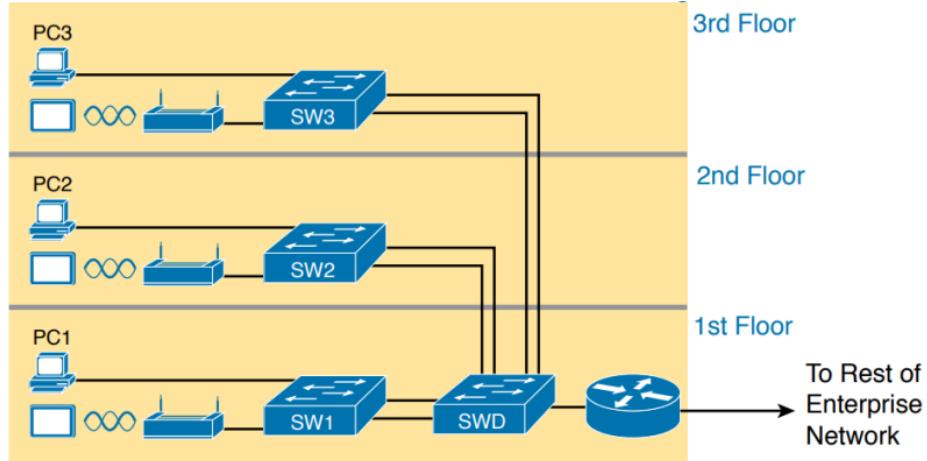
Nelle SOHO si usa un altro standard che è il wireless che può essere utilizzato insieme all'ethernet per fornire connessioni cablate e non, per utilizzare il wireless ci viene in aiuto l'access point (AP) che agisce come uno switch ma per i device senza cavi.



Quello appena detto è valido per le reti SOHO ma per quelle aziendali le esigenze

sono maggiori.

Prendendo come esempio un edificio a tre piani ogni piano dovrà avere uno switch LAN ethernet e un AP LAN wireless, per comunicare fra piano a piano si utilizza un altro switch che farà da collegamento fra i vari switch di piano e il router per uscire dalla rete.



Standard Ethernet nel physical layer

Come detto precedentemente l'Ethernet si riferisce a vari standard, eccone alcuni:

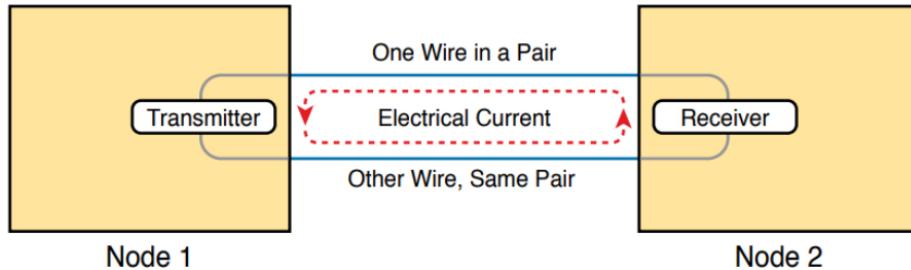
Speed	Common Name	Informal IEEE Standard Name	Formal IEEE Standard Name	Cable Type, Maximum Length
10 Mbps	Ethernet	10BASE-T	802.3	Copper, 100 m
100 Mbps	Fast Ethernet	100BASE-T	802.3u	Copper, 100 m
1000 Mbps	Gigabit Ethernet	1000BASE-LX	802.3z	Fiber, 5000 m
1000 Mbps	Gigabit Ethernet	1000BASE-T	802.3ab	Copper, 100 m
10 Gbps	10 Gig Ethernet	10GBASE-T	802.3an	Copper, 100 m

Tutti questi standard possono essere utilizzati anche insieme nella stessa rete nonostante le diverse velocità, questo perché Ethernet agisce come singola tecnologia visto che utilizza lo stesso standard a livello data-link.

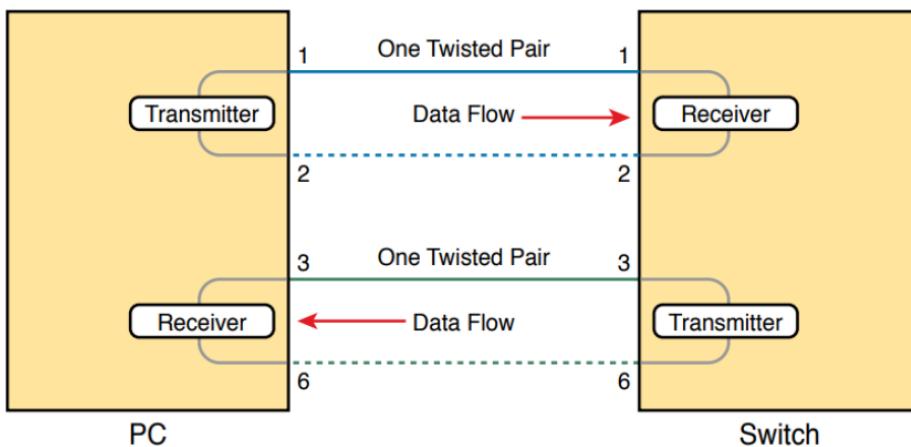
Cavi

UTP - Twisted Pairs

Sono composti da 2 o 4 coppie di fili in rame intrecciati su se stesse, le coppie rappresentano un circuito elettrico chiuso e come connettore si usa RJ45.



Gli standard 10BASE-T/100BASE-T utilizzano due coppie di fili in ogni cavo per ciascuna direzione, i trasmettitori delle Network Interface Card (NIC) utilizzano la coppia collegata ai pin 1,2 i ricevitori quella ai pin 3,6. Gli switch fanno l'opposto.

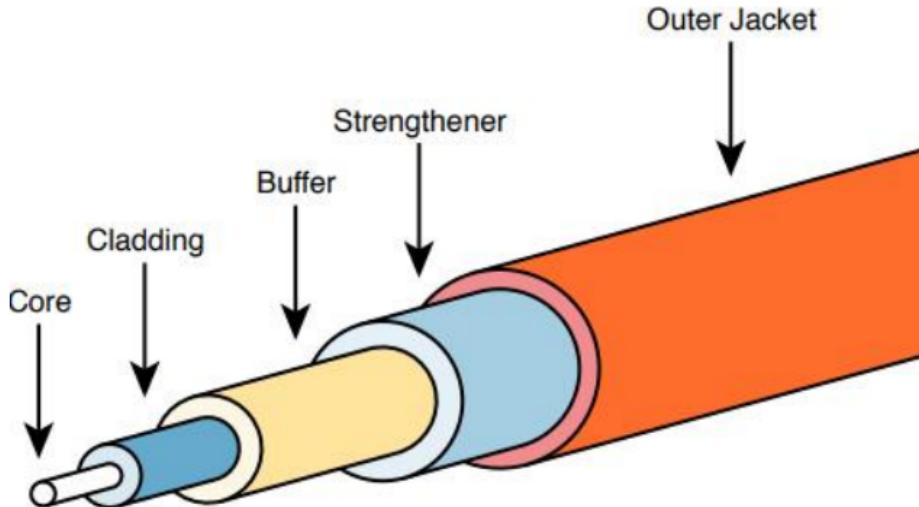


Un cavo straight-through funziona solo se i nodi utilizzano coppie opposte, quindi se provo a connettere due dispositivi simili con questo cavo la comunicazione non può avvenire perché usano gli stessi pin per ricevere/trasmettere, per questo è nato il crossover.

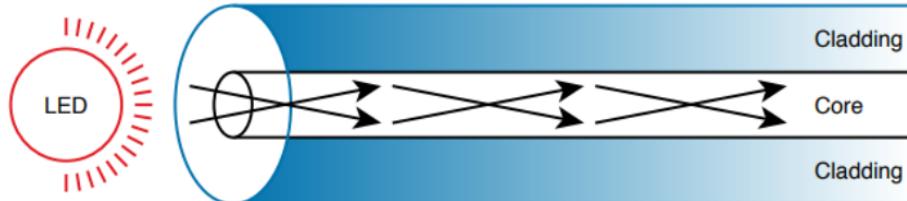
Gli switch Cisco hanno la possibilità di cambiare alcune porte dopo l'acquisto, come:

- Gigabit Ethernet Interface Converter (GBIC): rimovibile per interfacce gigabit;
- Small Form Pluggable (SFP): messo al posto del GBIC;
- Small Form Pluggable Plus (SFP+): come l'SFP ma utilizza interfacce da 10 Gbps.

Fiber Cabling



Il cavo può essere multimodale, cioè il core permette più angoli di trasmissione della luce e il segnale viene generato da un led:



Oppure monomodale con un core più sottile ($\frac{1}{4}$ del multimodale) e la trasmissione avviene tramite laser:



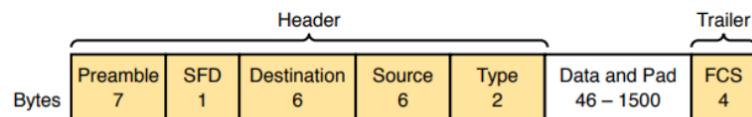
Prima di mostrare le caratteristiche va ricordato che è necessario avere due cavi uno per direzione e la porta di trasmissione su un dispositivo si collega a un cavo diretto verso una porta di ricezione sull'altro dispositivo e viceversa.

Standard	Cable Type	Max Distance*
10GBASE-S	MM	400m
10GBASE-LX4	MM	300m
10GBASE-LR	SM	10km
10GBASE-E	SM	30km

Criteria	UTP	Multimode	Single-Mode
Relative Cost of Cabling	Low	Medium	Medium
Relative Cost of a Switch Port	Low	Medium	High
Approximate Max Distance	100m	500m	40km
Relative Susceptibility to Interference	Some	None	None
Relative Risk of Copying from Cable Emissions	Some	None	None

Frame Ethernet

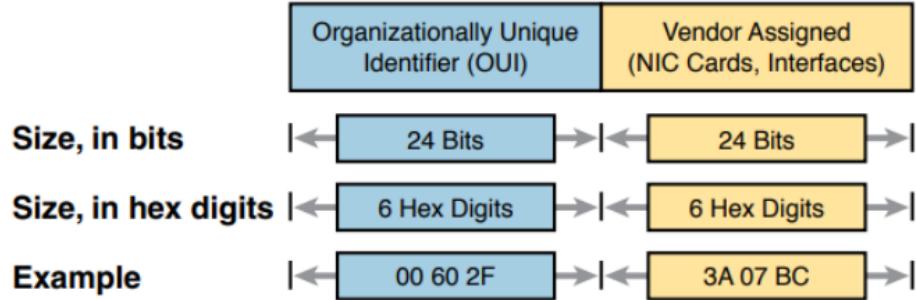
Il frame ethernet è composto da diversi campi, vediamoli nel dettaglio:



Field	Bytes	Description
Preamble	7	Synchronization.
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC Address field.
Destination MAC Address	6	Identifies the intended recipient of this frame.
Source MAC Address	6	Identifies the sender of this frame.
Type	2	Defines the type of protocol listed inside the frame; today, most likely identifies IP version 4 (IPv4) or IP version 6 (IPv6).
Data and Pad*	46– 1500	Holds data from a higher layer, typically an L3PDU (usually an IPv4 or IPv6 packet). The sender adds padding to meet the minimum length requirement for this field (46 bytes).
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine whether the frame experienced transmission errors.

Il MAC è un indirizzo formato da numeri binari (6 byte/48 bit) che identificano in maniera univoca e universale un apparato di rete.

Vengono scritti anche in esadecimale con 12 cifre divisi da punti per comodità (es: 0000.0C12.3456), dove i primi 3 byte identificano il produttore ed è detto OUI rilasciato dal IEEE ed è univoco, gli altri 3 sono creati dal produttore e anch'essi sono univoci ma solo per i prodotti dello stesso produttore.



Va puntualizzato che il FCS controlla solo se sono avvenuti errori per decidere se scartare o meno il frame, quindi non si occupa della correzione dell'errore.

Per funzionare il mittente applica una formula matematica nota al frame e mette il risultato dentro al campo frame, il ricevitore applica la stessa formula al frame e controlla il risultato con il campo FCS.

WAN

Più LAN distanti fra loro collegate formano una WAN, il primo tipo è la Leased-Line WANs, fornita da un provider e pagata tramite abbonamento, da parte del cliente sembra di lavorare come una normalissima connessione con cavo Ethernet ma in realtà può essere composta da un alto numero di device.

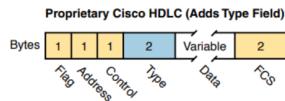
Name	Meaning or Reference
Leased circuit, Circuit	The words <i>line</i> and <i>circuit</i> are often used as synonyms in telco terminology; <i>circuit</i> makes reference to the electrical circuit between the two endpoints.
Serial link, Serial line	The words <i>link</i> and <i>line</i> are also often used as synonyms. <i>Serial</i> in this case refers to the fact that the bits flow serially and that routers use serial interfaces.
Point-to-point link, Point-to-point line	These terms refer to the fact that the topology stretches between two points, and two points only. (Some older leased lines allowed more than two devices.)
T1	This specific type of leased line transmits data at 1.544 megabits per second (1.544 Mbps).
WAN link, Link	Both of these terms are very general, with no reference to any specific technology.
Private line	This term refers to the fact that the data sent over the line cannot be copied by other telco customers, so the data is private.

La leased offre un servizio a layer 1, dove recapita i bit tra dispositivi collegati

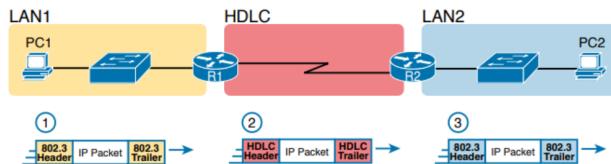
alla leased line stessa senza protocolli data-link.

Successivamente si è iniziato a offrire protocolli per il livello data-link tra cui High-Level Data Link (HDLC) e Point-to-Point (PPP).

HDLC



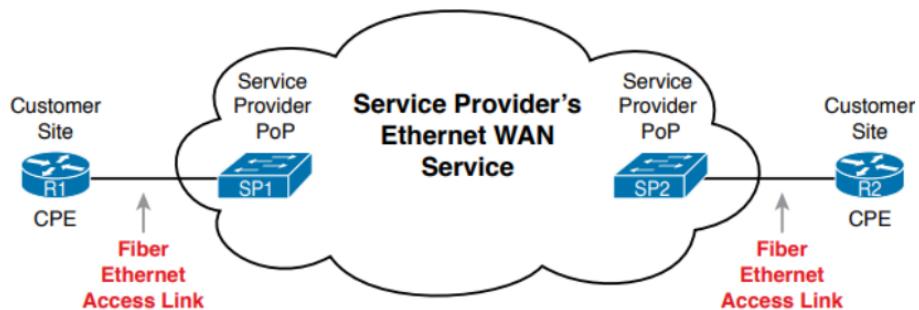
- 1) Per inviare il pacchetto IP al router R1, PC1 incapsula il pacchetto IP in un frame Ethernet che ha l'indirizzo MAC di destinazione di R1
- 2) Il router R1 rimuove il pacchetto IP dal frame Ethernet, incapsula il pacchetto in un frame HDLC utilizzando un'intestazione e un trailer HDLC e inoltra il frame HDLC al router R2
- 3) Il router R2 rimuove il pacchetto IP dal frame HDLC, incapsula il pacchetto in un frame Ethernet che ha l'indirizzo MAC di destinazione del PC2 e inoltra il frame Ethernet al PC2



Ethernet WAN

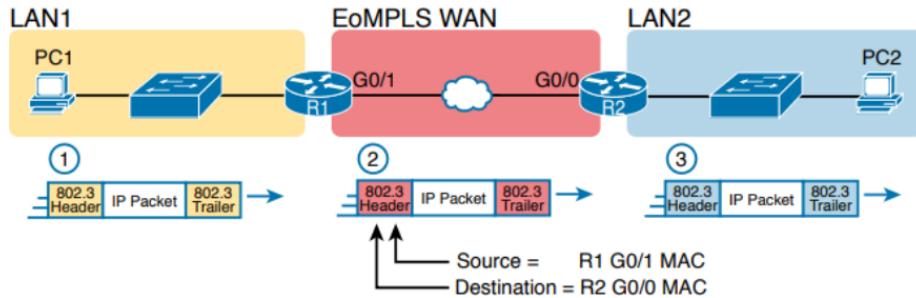
IEEE ha migliorato l'Ethernet per renderlo compatibile con la metodologia WAN. Per connettersi il cliente utilizza il router che tramite un collegamento in fibra lascia l'edificio per collegarsi al service provider tramite un PoP (point of presence) che normalmente è uno switch. Da questo punto il provider può utilizzare qualsiasi tecnologia per creare servizi WAN.

Logicamente è una connessione point-to-point fisicamente è come una connessione in fibra tra router.



Una tecnologia utilizzata dal provider tra i due router è la EoMPLS, un termine che si riferisce al Multiprotocol Label Switching, una tecnologia che viene usata per creare il servizio Ethernet per il cliente.

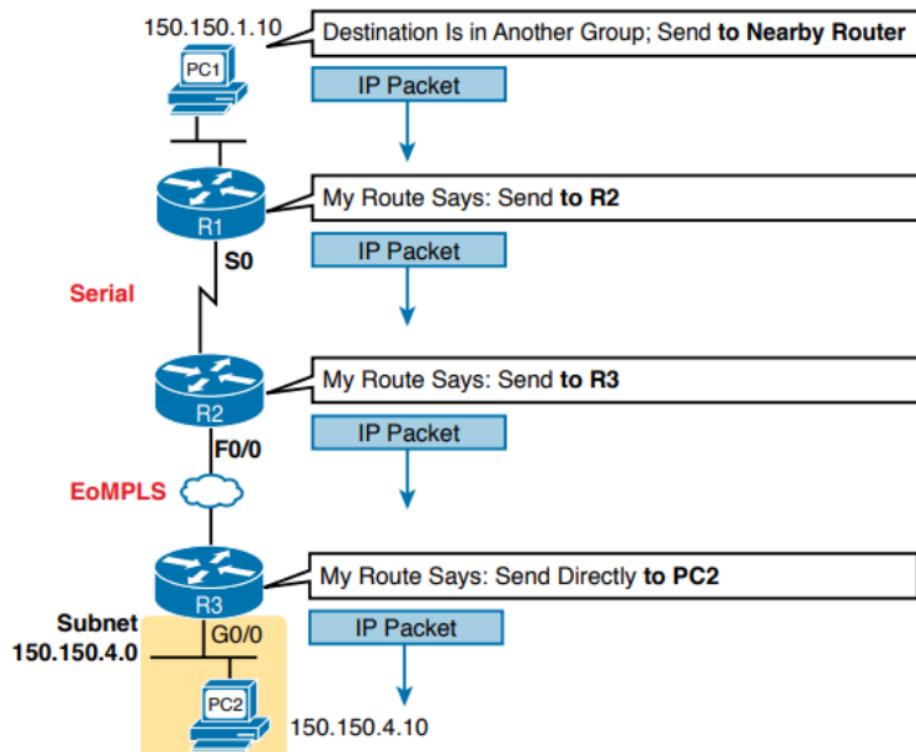
Il collegamento utilizza gli stessi header/trailer Ethernet usati per la LAN.



IP Routing

L'IP si occupa dei dettagli logici della consegna dei dati, nel dettaglio come i pacchetti viaggiano end-to-end su una rete TCP/IP anche passando attraverso LAN e WAN.

Per rendere possibile questo i router e pc lavorano insieme per eseguire il routing, infatti il PC ha un software che dice dove inviare i pacchetti, di solito al router più vicino e da lì in poi il router sceglie a chi inviarlo.



In questo esempio il PC1 nota che l'ind ip del PC2 non è nella sua sottorete per

questo invia il messaggio a qualcuno con il compito dell'instradamento, il router della sua LAN.

Il router è in grado di instradare correttamente il pacchetto perché al suo interno tiene traccia di tutti gli indirizzi ip delle reti con cui può comunicare e come raggiungerle, salvo tutto nella tabella di routing.

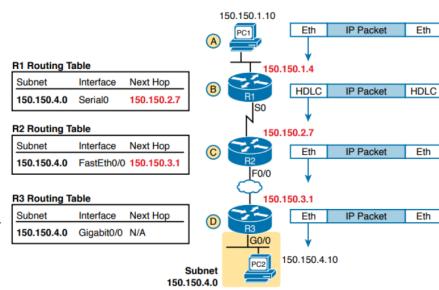
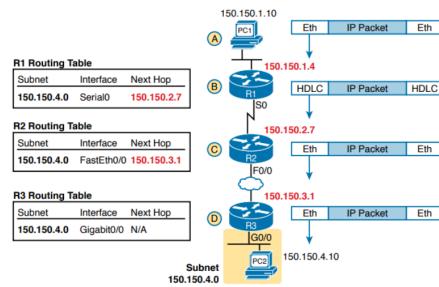
Ora vediamo i passaggi uno dopo l'altro con anche i vari incapsulamenti effettuati dai protocolli utilizzati:

1) PC1 invia il pacchetto al suo default router. La logica del livello di rete di PC1 crea il pacchetto IP, con indirizzo di destinazione 150.150.4.10 (PC2). Il livello di rete esegue anche l'analisi per decidere che 150.150.4.10 non si trova nella stessa subnet IP, quindi PC1 deve inviare il pacchetto a R1. PC1 inserisce il pacchetto IP in un data link frame, con l'indirizzo Ethernet di destinazione di R1. PC1 invia il frame Ethernet.

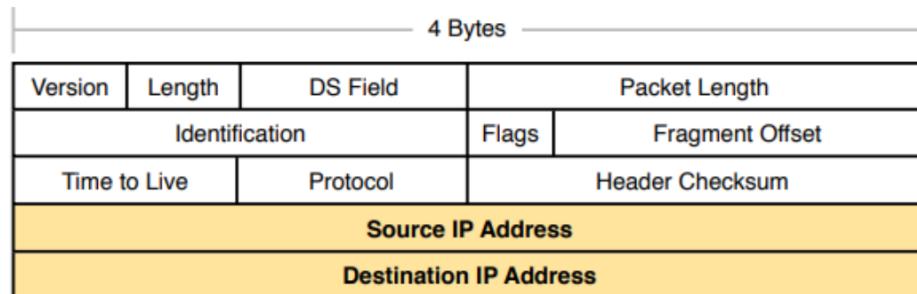
2) R1 elabora il frame in arrivo e inoltra il pacchetto a R2. Poiché il frame in entrata ha un MAC di destinazione uguale al MAC di R1, R1 decide di elaborare il frame. R1 verifica la presenza di errori grazie all'FCS del frame e, se il frame è valido, elimina l'intestazione e il trailer Ethernet. Successivamente, R1 confronta l'indirizzo di destinazione del pacchetto (150.150.4.10) con la propria tabella di instradamento e trova la voce per la sottorete 150.150.4.0. Poiché l'indirizzo di destinazione 150.150.4.10 si trova in quella sottorete, R1 inoltra il pacchetto all'interfaccia indicata in quella route(Serial0) al router R2 (150.150.2.7). R1 deve prima incapsulare il pacchetto IP in un frame HDLC.

3) R2 elabora il frame in arrivo e inoltra il pacchetto a R3. R2 ripete lo stesso processo generale di R1 quando riceve il frame HDLC. R2 controlla il campo FCS e rileva che non si sono verificati errori, quindi elimina l'intestazione e il trailer HDLC. Successivamente, R2 confronta l'indirizzo di destinazione del pacchetto (150.150.4.10) con la sua tabella di instradamento e trova la voce per la sottorete 150.150.4.0 (Fast Ethernet 0/0, next hop 150.150.3.1). R2 incapsula il pacchetto utilizzando l'indirizzo MAC di R2 e l'indirizzo MAC di R3 sul collegamento WAN rispettivamente come indirizzo MAC di origine e di destinazione.

4) R3 elabora il frame in arrivo e inoltra il pacchetto a PC2. Come R1 e R2, R3 controlla l'FCS, scarta la vecchia intestazione e il trailer del data link e cerca un percorso per la sottorete 150.150.4.0. La voce della tabella di routing di R3 mostra che l'interfaccia in uscita è l'interfaccia Ethernet di R3, ma non esiste un router next-hop perché R3 è connesso direttamente alla sottorete 150.150.4.0. Tutto ciò che R3 deve fare è incapsulare il pacchetto con un indirizzo di destinazione uguale all'indirizzo MAC di PC2.



L'header IP è così formato:



CLI

Possiamo collegarci ad uno switch per configurarlo tramite ssh o cavo.

Se il collegamento è via cavo usiamo un cavo azzurro detto cavo console

AAA

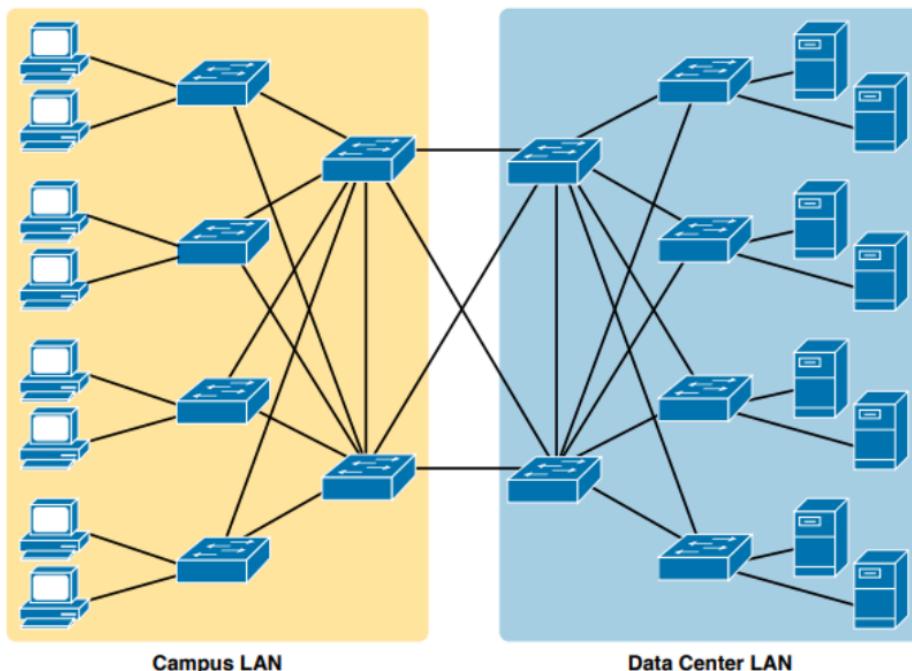
Se in una azienda sono presenti innumerevoli device con utenti replicati su ognuno, è possibile adottare un server per l'autenticazione.

“Authentication, authorization, and accounting (AAA) server”

Questo server ospita username e password in modo centralizzato. Quando un AAA server è configurato, lo switch invia un messaggio contenente username e password al server stesso, il quale risponde comunicando se l'accesso è autorizzato.

I più conosciuti sono RADIUS e TACACS+

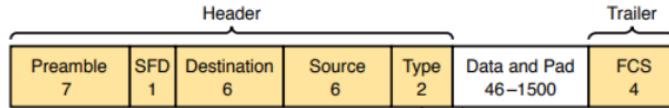
LAN SWITCHING



Le LAN permettono la comunicazione al loro interno e ad altre LAN tramite switch che sanno a chi inviare i messaggi tramite MAC Address.

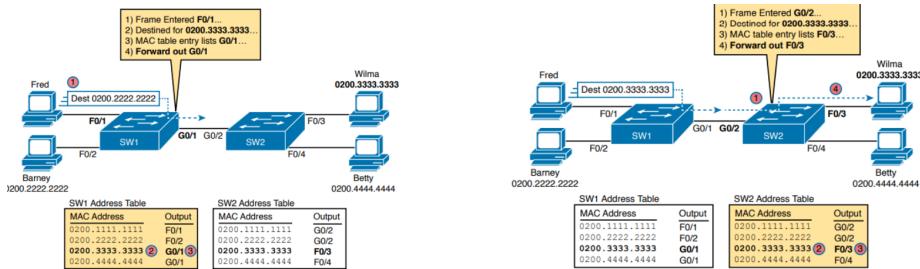
Def: tutti i device che si trovano sullo stesso broadcast domain

Il pacchetto che viene inviato dagli switch è di livello physical, ed è così strutturato:



Field	Bytes	Description
Preamble	7	Synchronization.
Start Frame Delimiter (SFD)	1	Signifies that the next byte begins the Destination MAC Address field.
Destination MAC Address	6	Identifies the intended recipient of this frame.
Source MAC Address	6	Identifies the sender of this frame.
Type	2	Defines the type of protocol listed inside the frame; today, most likely identifies IP version 4 (IPv4) or IP version 6 (IPv6).
Data and Pad*	46– 1500	Holds data from a higher layer, typically an L3PDU (usually an IPv4 or IPv6 packet). The sender adds padding to meet the minimum length requirement for this field (46 bytes).
Frame Check Sequence (FCS)	4	Provides a method for the receiving NIC to determine whether the frame experienced transmission errors.

La porta verso la quale inoltrare il frame viene individuata grazie ad una MAC address table, chiamata anche switching table. Questa tabella riporta una lista di indirizzi e la relativa porta da utilizzare per raggiungerli. Viene salvata in RAM e i record vengono salvati per 300 secondi.



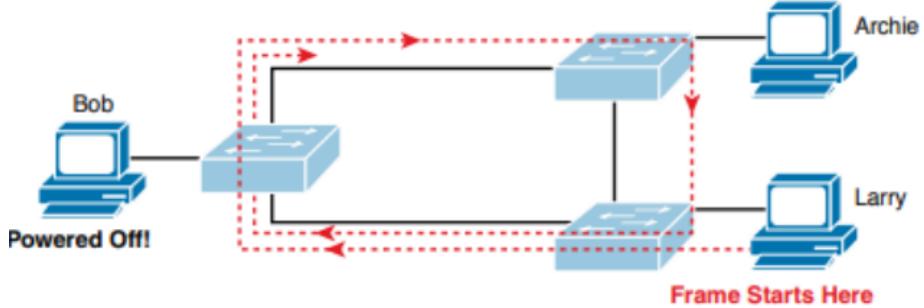
La costruzione della tabella avviene esaminando i source address dei frame che entrano nella varie porte (chi invia popola NON chi lo riceve).

Se un indirizzo non è presente nella tabella, una copia del frame viene inoltrata verso ogni porta dello switch (ad eccezione di quella dalla quale il frame è stato ricevuto). Questo processo si chiama flooding.

In questo modo il destinatario riceverà il messaggio e lo switch imparerà la corretta porta per raggiungere quel MAC nel momento in cui il destinatario invierà la risposta.

Usando il flooding può avvenire il problema del LOOP, dove il messaggio gira

all'infinito saturando la rete perchè la rete ha dei link ridondanti.



Per risolvere si usa il protocollo STP, dove alcuni link impediscono di rinviare i messaggi rendendo possibile solo un path per collegare due PC, nell'esempio sopra STP spegne Bob visto che Archie e Larry hanno un'altro modo per comunicare.

Switch interfaces

Se due switch in collegamento usano velocità differenti utilizzano un meccanismo di auto-negoziazione per decidere una velocità consona per entrambi, questo meccanismo funziona anche con i duplex (full, half, auto).

La autonegoziazione è definita da uno standard IEEE, Cisco non lo supporta perché le loro porte hanno un metodo loro per capire la velocità, ecc.

Nel dettaglio i duplex:

- Full: entrambi i comunicanti ricevono e inviano contemporaneamente.
- Half: in questo caso solo uno alla volta può trasmettere mentre l'altro ascolta. Viene usata dal Wi-Fi.

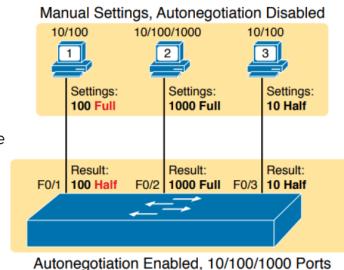
Per capire se un'interfaccia è collegata a qualcosa lo switch invia degli impulsi detti LIT o Normal Link Pulses (NLP); successivamente sono nati gli Fast Link Pulse.

Lo switch nella auto-negoziazione per capire la velocità usa il tipo di impulso che gli arriva fra NLP o FLP.

Esaminando ogni collegamento, da sinistra a destra:

- PC1: lo switch non riceve messaggi di autonegoziazione quindi rileva il segnale elettrico per capire che PC1 sta inviando dati a 100 Mbps. Lo switch utilizza il duplex predefinito basato sulla velocità di 100 Mbps (half duplex).
- PC2: lo switch utilizza gli stessi passaggi e la stessa logica del collegamento al PC1, tranne per il fatto che lo switch sceglie di utilizzare il full duplex perché la velocità è di 1000 Mbps.
- PC3: l'utente sceglie velocità di 10 Mbps e l'impostazione half-duplex. Tuttavia, lo switch Cisco rileva la velocità senza utilizzare la negoziazione automatica IEEE e successivamente utilizza l'impostazione predefinita duplex IEEE per i collegamenti a 10 Mbps (half duplex).

Per PC1 si è verificata una mancata corrispondenza duplex. I due nodi (PC1 e la porta G0/1 di SW1) utilizzano entrambi 100 Mbps. Tuttavia, PC1, utilizzando il full duplex, invia frame in qualsiasi momento. La porta dello switch F0/1, con half duplex, utilizza CSMA/CD. Di conseguenza, la porta dello switch F0/1 riterrà che si verifichino collisioni sul collegamento. La porta dello switch interromperà la trasmissione, attenderà, invierà nuovamente i frame e così via. Di conseguenza, il collegamento sarà attivo, ma funzionerà male.



STP

Nella terminologia STP: switch <=> bridge

Spanning Tree Protocol, protocollo per evitare che alcune porte propaghino frame in maniera indefinita e duplicando i pacchetti.

Il problema sussiste se ci sono più path per unire gli stessi device, per questo STP blocca le porte che non sono gli unici collegamenti con una parte della rete.

I problemi causati dai frame in loop sono:

- Broadcast storm: in questo caso i link risultano saturi andando a perdere i veri pacchetti a causa di troppi frame broadcast o simili;
- MAC table instability: in questa casistica le tabelle di indirizzi MAC cambiano in maniera incontrollata per via di frame con stesso source address MAC che gira e viene ricevuto su porte diverse.
- Multiple copies: semplicemente lo stesso end device ottiene lo stesso pacchetto più volte duplicato, andando a rompere applicativi.

Ogni volta che collegiamo un'interfaccia la verifichiamo prima che possa inviare qualsiasi pacchetto, e la mettiamo in modalità forwarding, operano normalmente, o blocking, processano solo frame STP/RSTP, (la modalità non influenza altre info della porta come il trunking).

Esistono altre due modalità (non stabili) con cui lo switch può impostare la porta, queste vengono usate durante il cambio da blocking a forwarding, e sono:

- listening: si comporta come in blocking ma durante il periodo in cui è in questa modalità lo switch cancella dalla tabella MAC le voci per le quali non vengono ricevuti frame;
- learning: si comporta come il blocking ma intanto ri-inizia a ripopolare la tabella con quello che riceve.

STP elegge uno switch root o root bridge con tutte le porte in forwarding, tutti gli altri switch della rete devono attivare una porta con cammino minimo (root

port) per arrivare al root bridge e metterla in forwarding.

Successivamente ogni switch rende la porta con root cost (costo per arrivare al root bridge) più basso la root port (in forwarding).

Con due switch collegati quello con root cost minore diventerà il designated switch con la designated port connessa con l'altro switch e andando a chiudere le altre.

Ogni switch ha un bridge ID (BID) da 8 byte (2 di priorità e 6 di ID) univoco, per scambiarsi gli BID dei vicini si usano messaggi STP detti BPDU, così composto:

Field	Description
Root bridge ID	The bridge ID of the switch the sender of this Hello currently believes to be the root switch
Sender's bridge ID	The bridge ID of the switch sending this Hello BPDU
Sender's root cost	The STP/RSTP cost between this switch and the current root
Timer values on the root switch	Includes the Hello timer, MaxAge timer, and forward delay timer

Il root bridge detto prima viene definito con il BID più basso, con BID uguali si prende il MAC più basso (contenuto nel BID nella parte ID).

Uno switch smette di inviare BPDU con il proprio BID se riceve un BID migliore da un altro perché capisce che non è lui il switch root.

Il root cost detto prima viene riportato in ogni BPDU ricevuto sulla stessa interfaccia, il costo è un numero associato ad una interfaccia.

Se il root cost è uguale esistono 3 regole per scegliere il percorso:

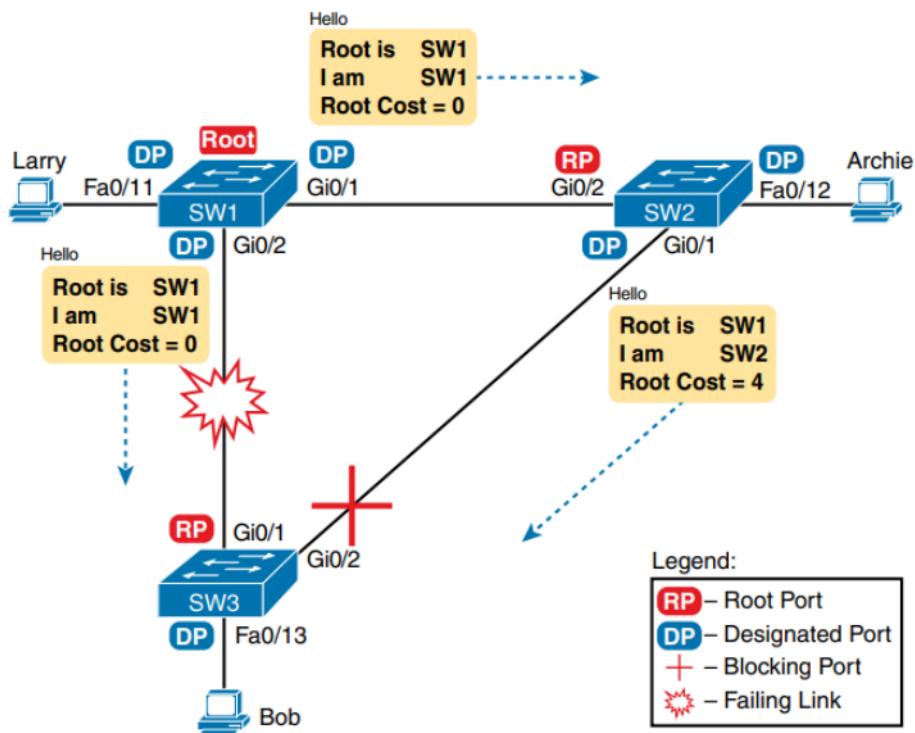
1. prendi il vicino con l'ID bridge migliore;
2. scegli in base alla priorità della porta;
3. scegli in base al numero di porta.

Sugli switch Cisco STP è attivo di default con un BID predefinito e le interfacce hanno un costo predefinito basati sulla velocità. Tutto ciò è comunque modificabile dal tecnico.

Riassumendo:

1. Lo switch root crea e invia un Hello BPDU, con un root cost pari a 0, tramite tutte le sue interfacce funzionanti (quelle in stato forwarding).
2. Gli switch non root ricevono l'Hello sulle loro root port. Dopo aver modificato l'Hello inserendo il proprio BID come mittente e modificando il root cost, inoltrano l'Hello a tutte le DP.
3. I passaggi 1 e 2 si ripetono finché qualcosa non cambia.

Questo avviene ogni 2 secondi
Quando un Hello non arriva o arriva con informazioni diverse dai precedenti, allora qualcosa è cambiato e lo switch reagisce di conseguenza



RSTP

Il Rapid Spanning Tree Protocol è l'altra versione del protocollo che si comporta normalmente tranne per alcune caratteristiche:

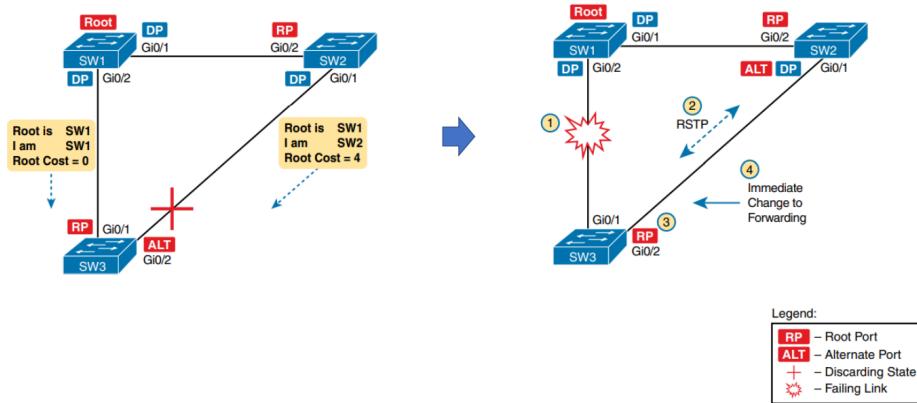
- è possibile che uno switch possa rimuovere la propria root port o sostituire la designated port senza attesa fra una modalità e l'altra (non sempre);
- nuovi tipi di porte:

Function	Port Role
Port that begins a nonroot switch's best path to the root	Root port
Port that replaces the root port when the root port fails	Alternate port
Switch port designated to forward onto a collision domain	Designated port
Port that replaces a designated port when a designated port fails	Backup port
Port that is administratively disabled	Disabled port

L'alternate è la seconda migliore scelta, andando a rimuovere i tempi di attesa al cambio della root port.

La backup port si usa solo se sono presenti hub nelle reti.

- gli switch generano i propri Hello (senza aspettare di riceverli) e possono fare query tra vicini.



1. Il collegamento tra SW1 e SW3 fallisce, quindi la root port corrente di SW3 (Gi0/1) fallisce.
2. SW3 e SW2 si scambiano messaggi RSTP per confermare che SW3 eseguirà la transizione della sua alternate port (Gi0/2) a root port. Questa azione fa sì che SW2 svuoti le voci della MAC address table interessate.
3. SW3 assegna a Gi0/1 il ruolo disabled e a Gi0/2 il ruolo di root port.
4. SW3 fa passare immediatamente Gi0/2 in stato forwarding, senza utilizzare lo stato learning, perché questo è un caso in cui RSTP sa che la transizione non creerà un loop.

Le porte fra i due tipi di protocolli hanno stati uguali e diversi, a volte cambiano i nomi:

Function	STP State	RSTP State
Port is administratively disabled	Disabled	Discarding
Stable state that ignores incoming data frames and is not used to forward data frames	Blocking	Discarding
Interim state without MAC learning and without forwarding	Listening	Not used
Interim state with MAC learning and without forwarding	Learning	Learning
Stable state that allows MAC learning and forwarding of data frames	Forwarding	Forwarding

Per evitare la convergenza (cambiamento all'interno della rete), si usano gli EtherChannel o PortChannel, quindi un canale con diversi backup. STP tratta i cavi come uno unico nonostante fisicamente c'è ne siano di più.

È possibile implementare il PostFast cioè al collegamento di un end device alla rete saltiamo tutta la procedura STP, è molto pericoloso per questo si usa solo con dispositivi che non provocano loop come PC o laptop.

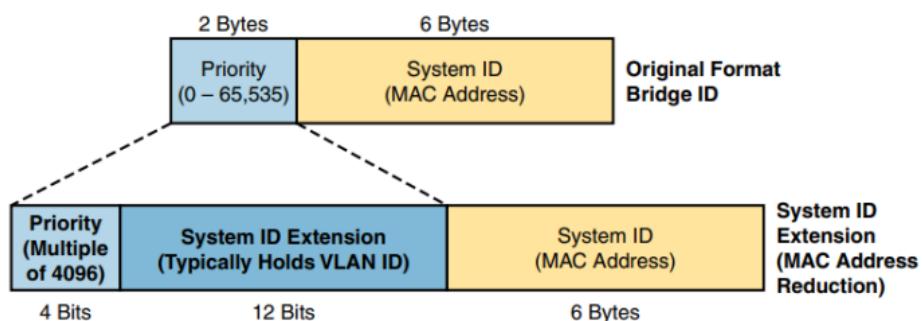
Cisco STP

Cisco ha creato protocolli paralleli ai due appena visto che funziona sui propri dispositivi che da la possibilità di creare istanze spanning tree per ogni VLAN:

Name	Based on STP or RSTP?	# Trees	Original IEEE Standard	Config Parameter
STP	STP	1 (CST)	802.1D	N/A
PVST+	STP	1/VLAN	802.1D	pvst
RSTP	RSTP	1 (CST)	802.1w	N/A
Rapid PVST+	RSTP	1/VLAN	802.1w	rapid-pvst
MSTP	RSTP	1 or more*	802.1s	mst

MSTP è come quelle di Cisco ma dell'IEEE.

Nelle versioni che supportano le VLAN il campo BID cambia:



Root Guard

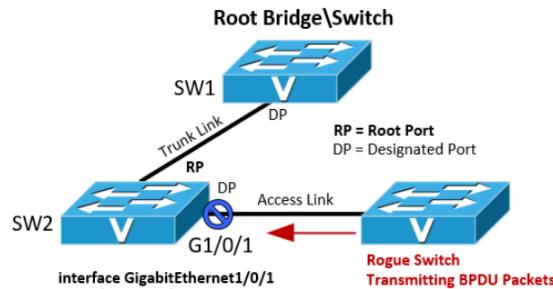
Modalità che evita che un nuovo switch appena inserito in rete diventi lo switch root. Può comunque stare connesso nella rete e utilizzare STP o RSTP.

BPDUs Guard

Nel caso una porta sia configurata con PortFast, potrebbero verificarsi problemi nel caso in cui alla porta stessa venga connesso uno switch e non il device di un utente.

Uno dei problemi potrebbe essere un loop temporaneo.

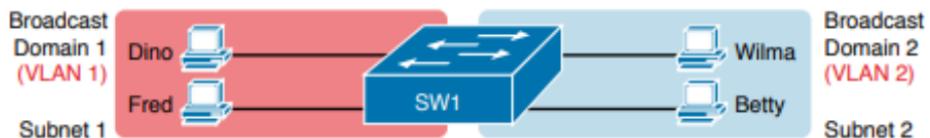
Per evitare ciò è possibile abilitare BPDU Guard sulla porta.



Praticamente spegne la porta quando nota che arrivano pacchetti tipici di uno switch con STP, l'unico modo per riattivare la porta è farlo a mano.

VLAN

Sono delle LAN virtuali quindi non fisicamente divisi da più switch, ma più PC connessi allo stesso switch che però divide le proprie porte in diverse LAN virtuali.



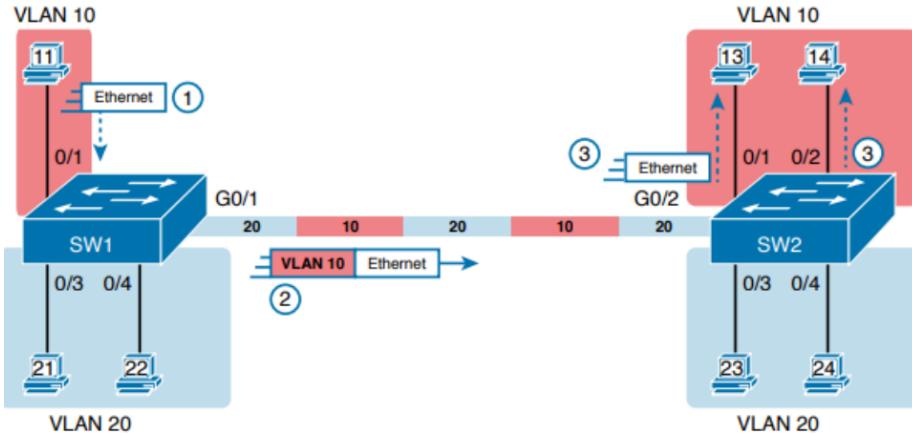
Le VLAN hanno diversi vantaggi:

- limitazione di device che ricevono messaggi inutili (messaggio broadcast);
- riduzione dei problemi di sicurezza (se una vlan viene infettata le altre sono separate);
- design di rete più flessibile.

Trunking

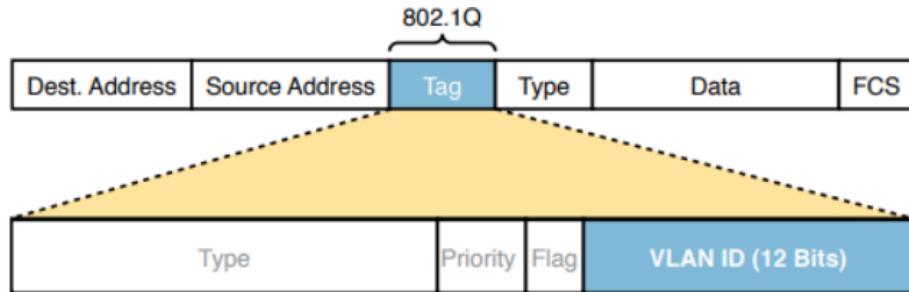
Se ho più switch posso comunque usare le VLAN anche se non fisicamente connessi allo stesso switch, questo è possibile dicendo che il link che connette gli switch faccia parte della VLAN.

Per evitare di creare tanti collegamenti fra switch per ogni VLAN usiamo il trunking, quindi usiamo un unico collegamento tra switch a switch dove facciamo passare le VLAN e per far capire verso quale VLAN il frame è diretto lo tagghiamo (header con ID della VLAN).



Il protocollo di trunking è il IEEE 802.1Q (oppure Dot1q), che prevede 4 extra byte nell'header ethernet.

12 di questi bit sono dedicati all'ID VLAN (possiamo gestire 4096 VLAN possibili). Cisco divide il range da 1 a 1005 alla normal range e dal 1006 al 4095 al extended range.



Il protocollo prevede una VLAN di default (di solito la 1 ma cambiabile) che non viene taggata questo per far sì di riuscire a comunicare con dispositivi che non supportano il trunking; infatti tutti i frame non taggati verranno indirizzati alla default.

NON è possibile che i messaggi riescano a passare da un layer all'altro tramite switch quindi layer 2, l'unico modo è utilizzare un router o uno switch multilayer che lavorano in layer 3.

Nel trunking esistono diversi tipi di cavi uno in access e uno in trunk più alcuni tipi dinamici

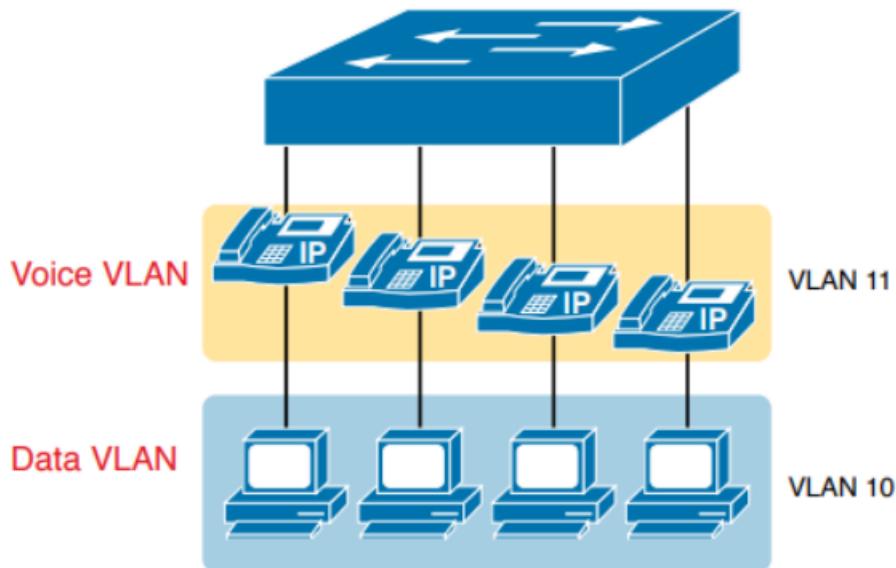
Command Option	Description
access	Always act as an access (nontrunk) port
trunk	Always act as a trunk port
dynamic desirable	Initiates negotiation messages and responds to negotiation messages to dynamically choose whether to start using trunking
dynamic auto	Passively waits to receive trunk negotiation messages, at which point the switch will respond and negotiate whether to use trunking

Administrative Mode	Access	Dynamic Auto	Trunk	Dynamic Desirable
access	Access	Access	Do Not Use ¹	Access
dynamic auto	Access	Access	Trunk	Trunk
trunk	Do Not Use ¹	Trunk	Trunk	Trunk
dynamic desirable	Access	Trunk	Trunk	Trunk

VLAN Voice

Cisco ha creato piccoli switch integrati nei telefoni fissi per ridurre al minimo le connessioni tra PC e switch.

In questo modo i PC e i telefoni saranno in due VLAN separate con il cavo che non può essere in access o in trunk e per questo esiste la modalità voice.



Per attivare questa modalità il comando è:

`switchport voice vlan [num]`

il resto dei comandi prima e dopo è uguale a quello per gestire le VLAN.

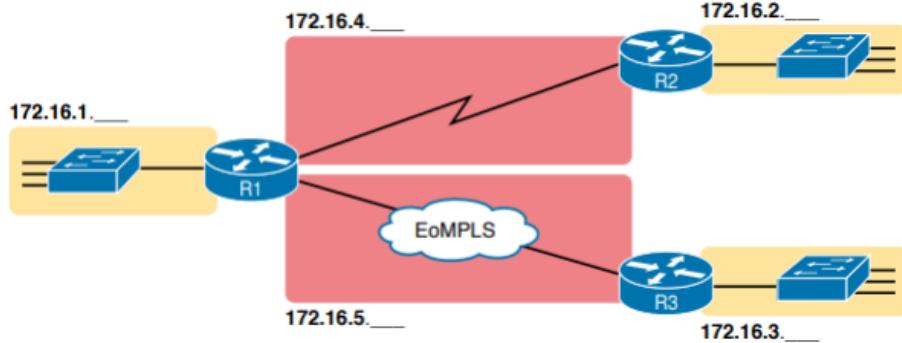
SUBNETTING

Una rete IP è una sequenza di indirizzi IP consecutivi che seguono una regola nota, es: ind di rete 172.16.0.0, gli indirizzi saranno: 172.16.0.1-2-3-ecc.

Una subnet è un sottoinsieme di una rete di classe A,B o C.

Una subnet di classe B può essere 172.16.1 e un'altra con 172.16.2. Per distinguere due sottoreti differenti oltre a vedere gli indirizzi IP possiamo ricordarci che due subnet DEVONO essere separate da almeno un router.

Ogni collegamento WAN (quello in rosso) per collegare ogni subnet è a loro volta una subnet, con i propri indirizzi che verranno usati dal router (i router avranno tanti indirizzi IP tante sono le subnet a lui collegate).

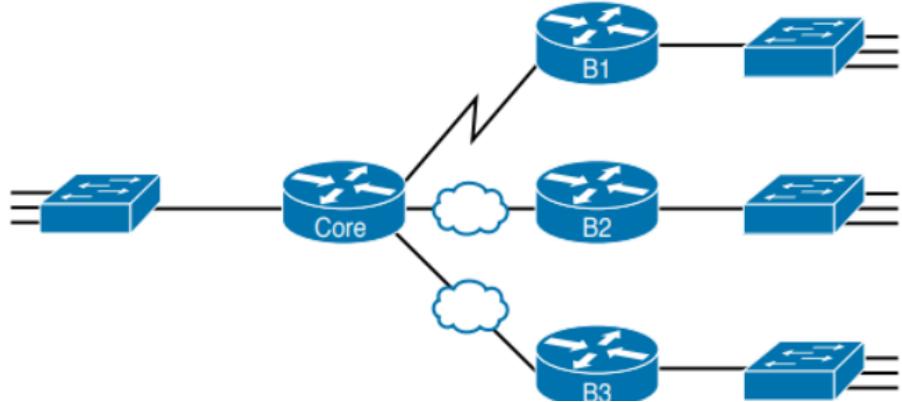


Per capire come dividere la mia rete in subnet procediamo a step:

- Analisi esigenze:

- quali host devono essere raggruppati in subnet;
- quante subnet richiede la rete;
- quanti indirizzi IP richiede ciascuna subnet;
- tutte le subnet saranno grandi uguali?

Per sapere il numero di subnet necessarie può venire in aiuto il numero di VLAN esistenti, infatti possiamo decidere di rendere ogni VLAN una subnet. Vanno contati anche i collegamenti WAN.



Per esempio in questo esempio (contando che per ogni switch ci sia una sola VLAN) saranno necessarie 7 subnet, 4 per ogni VLAN (switch) e uno per ogni collegamento WAN o seriale.

Ora dobbiamo chiederci quanti host ci saranno e quindi quanti IP devo riservare, un aiuto può arrivare contando quante persone dovranno lavorare sulla rete più

qualche server/stampante/ecc.

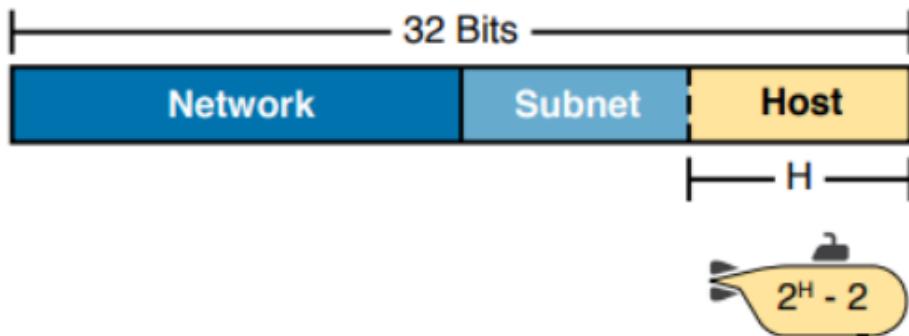
In conclusione decidiamo se dare ad ogni subnet la stessa dimensione o meno, la dimensione è semplicemente il numero di indirizzi IP utilizzabili. Normalmente si opta per avere tutte le subnet uguali per evitare errori.

L'ingegnere incaricato della creazione delle subnet assegna a ciascuna una maschera di sottorete (o subnet mask) che definisce la dimensione della subnet associata. la subnet mask identifica degli host bit, con lo scopo di identificare i diversi indirizzi IP degli host nella subnet.

La subnet mask definisce $2^H - 2$ indirizzi usabili dagli host, dove H sono gli host bit e i - 2 indirizzi sono riservati.

I due riservati sono il numero di sottorete (il più basso, es: 10.0.0.0) e l'ind. di broadcast (il più alto, es: 10.255.255.255).

Quindi i 32 bits di ogni indirizzo sono così divisi:



Per la subnet mask, dei 32 bit, lascio a 0 tutti i bit uguali agli host bit e metto a 1 tutti gli altri:



Se ho deciso di voler fare ogni subnet grande uguale per decidere quanti indirizzi riservare devo prendere la rete che avrà bisogno di più indirizzi e trovare un H abbastanza grande che lo contenga. Se ho una subnet che ha bisogno di 200 ind.

allora avrò un $H = 8$ ($2^8 - 2 = 254$).

Se le subnet saranno diverse allora faremo lo stesso procedimento ma per ogni subnet, in questo caso le maschere si chiamano VLSM (variable-length subnet

masks).

2. Design subnet:

- scegliere la rete;
- scegliere la maschera;
- elencare tutte le subnet.

3. Plan implementation.

Esempio di progettazione

Esempio di progettazione: rete 172.16.0.0, 200 sottoreti, 200 host:

- Utilizzare un'unica maschera per tutte le sottoreti
- Pianificare 200 sottoreti.
- Pianificare 200 indirizzi IP host per sottorete.
- Utilizzare la rete privata di classe B 172.16.0.0.

$$(2^8 = 256)$$



NAT

Agli albori di internet ad ogni azienda che voleva usare il servizio gli si dava un range di IP pubblici (es: tutti quelli con: 1.0.0.0) da utilizzare per evitare duplicati.

Quando gli indirizzi iniziavano a diventare sempre di meno sono nate 3 soluzioni:

1. nuova versione di IP (IPV6) con 128 bit per indirizzo;
2. invece di dare un'intera rete IP da ogni azienda gli diamo un solo sottoinsieme;
3. NAT protocollo per l'utilizzo di reti IP private.

Il NAT è l'idea che ha preso più piede perché permette a più aziende di utilizzare la stessa identica rete IP privata e per collegarsi all'esterno si usa un indirizzo pubblico che non è solo di un'azienda ma viene dato a diverse aziende in momenti diversi.

Classi

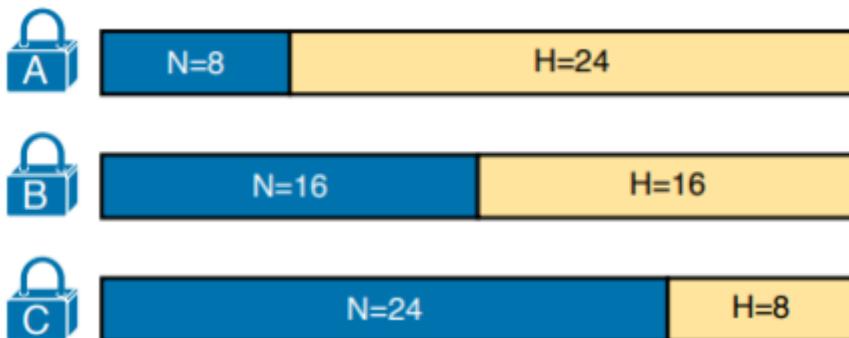
Class	First Octet Values	Purpose
A	1–126	Unicast (large networks)
B	128–191	Unicast (medium-sized networks)
C	192–223	Unicast (small networks)
D	224–239	Multicast
E	240–255	Reserved (formerly experimental)

	Class A	Class B	Class C
First octet range	1–126	128–191	192–223
Valid network numbers	1.0.0.0–126.0.0.0	128.0.0.0–191.255.0.0	192.0.0.0–223.255.255.0
Total networks	$2^7 - 2 = 126$	$2^{14} = 16,384$	$2^{21} = 2,097,152$
Hosts per network	$2^{24} - 2$	$2^{16} - 2$	$2^8 - 2$
Octets (bits) in network part	1 (8)	2 (16)	3 (24)
Octets (bits) in host part	3 (24)	2 (16)	1 (8)
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

Gli indirizzi IP privati utilizzabili sono:

Class of Networks	Private IP Networks	Number of Networks
A	10.0.0.0	1
B	172.16.0.0 through 172.31.0.0	16
C	192.168.0.0 through 192.168.255.0	256

Ogni classe divide i propri indirizzi in due parti una per la rete e una per gli host, i bit sono così divisi:



E l'ingegnere per creare le subnet prende in prestito alcuni bit dalla parte degli host e li riserva per identificare le subnet.

Ogni rete ha quattro numeri chiave che la descrivono.

Puoi derivare questi quattro numeri a partire da un solo indirizzo IP nella rete.

I numeri sono i seguenti: ID di rete, Primo indirizzo utilizzabile (numericamente più basso), Ultimo (numericamente più alto), Indirizzo broadcast

Passaggio 1. Determinare la classe (A, B o C) in base al primo ottetto

Passaggio 2. Dividere mentalmente gli ottetti (network e host) in base alla classe.

Passaggio 3. Per trovare il numero di rete, modificare gli ottetti relativi agli host dell'indirizzo IP ponendoli a 0.

Passaggio 4. Per trovare il primo indirizzo, aggiungi 1 al quarto ottetto dell'ID di rete.

Passaggio 5. Per trovare l'indirizzo broadcast, modificare gli ottetti host dell'ID di rete in 255.

Passaggio 6. Per trovare l'ultimo indirizzo utilizzabile sottrai 1 dall'indirizzo broadcast

Esempio:

Class ①	A	B	C
Divide ②			
Make Host=0 ③	10	17 . 18 . 21	
Add 1 ④	10	0 . 0 . 0	+1
Make Host=255 ⑤	10	255 . 255 . 255	-1
Subtract 1 ⑥	10	255 . 255 . 254	

Class ①	A	B	C
Divide ②			
Make Host=0 ③	172 . 16	8 . 9	
Add 1 ④	172 . 16	0 . 0	+1
Make Host=255 ⑤	172 . 16	255 . 255	-1
Subtract 1 ⑥	172 . 16	255 . 254	

Notazioni

DDN

La dotted-decimal notation converte ogni set di 8 bit in decimale, esempio:

11111111 0000000 0000000 0000000 -> 255.0.0.0

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
00000000	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Prefix

Si usa per identificare la maschera in forma compatta, sostanzialmente si mette dopo l'indirizzo IP una barra (/) seguita dal numero di 1 presenti della subnet mask, esempio:

X.X.X.X/8 -> 11111111 00000000 00000000 00000000 -> 255.0.0.0

Riassunto

Subnet mask

Riassunto

A cosa serve una subnet mask?

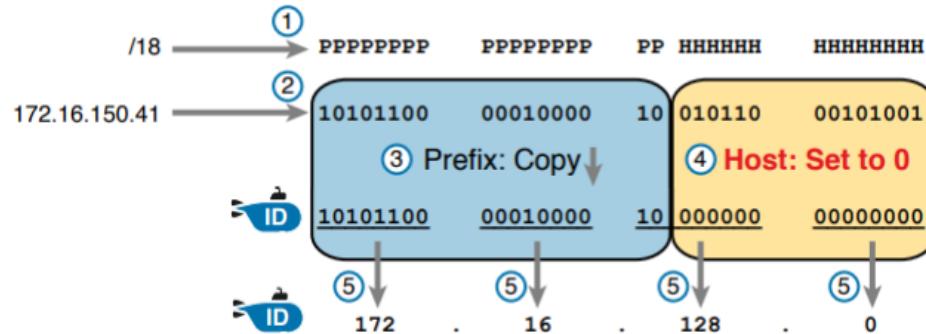
- Definisce la dimensione del prefisso (rete e sottorete combinate) in una sottorete
- Definisce la dimensione della parte host degli indirizzi nella sottorete
- Può essere utilizzato per calcolare il numero di host nella sottorete
- Fornisce un metodo che consente al progettista di rete di comunicare i dettagli del progetto (il numero di subnet e di bit host) ai dispositivi nella rete
- In determinate situazioni, può essere utilizzato per calcolare il numero di sottoreti nell'intera rete
- Può essere utilizzato nei calcoli dell'ID di sottorete e dell'indirizzo broadcast sottorete

Divisione ind.

Classless addressing: il concetto secondo cui un indirizzo IPv4 ha due parti, la parte del prefisso più la parte dell'host, come definito dalla maschera, senza considerazione della classe (A, B o C).

Classful addressing: il concetto secondo cui un indirizzo IPv4 è composto da tre parti: rete, sottorete e host, come definito dalla maschera e dalle regole di classe A, B e C.

Ricerca ind. sottorete o ID di sottorete



Senza convertirlo in binario, se abbiamo la maschera scritta in notazione DDDN possiamo fare:

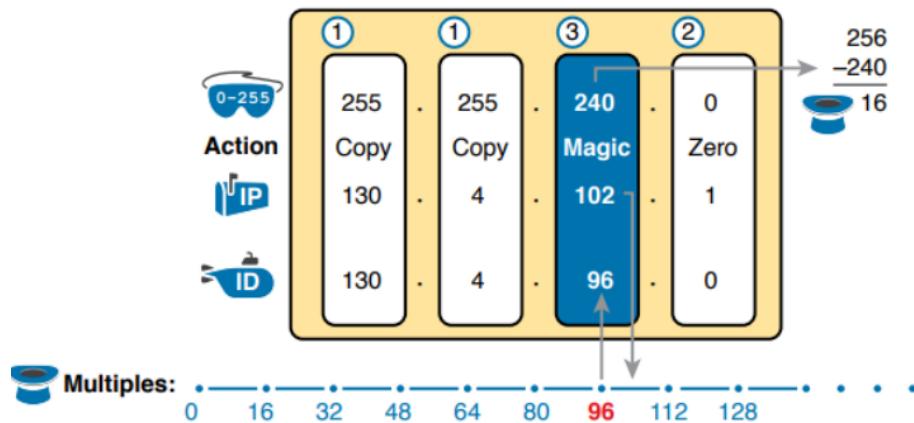
Passaggio 1. Se l'ottetto della maschera = 255, copiare l'indirizzo IP decimale.

Passaggio 2. Se l'ottetto della maschera = 0, scrivere uno 0 decimale.

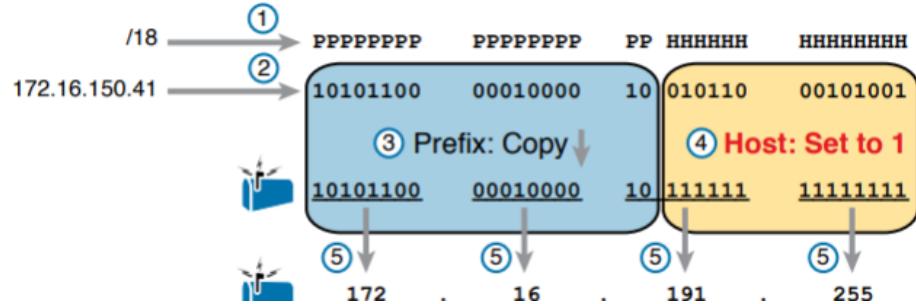
Passaggio 3. Se l'ottetto non è né 0 né 255, questo ottetto diventa l'interesting octet:

A. Calcola il magic number, cioè $256 - \text{maschera}$.

B. Scegli il valore dell'ID di sottorete individuando il multiplo del magic number più vicino al valore all'indirizzo IP, senza superarlo.



Ricerca ind. broadcast



Senza convertirlo in binario, se abbiamo la maschera scritta in notazione DDN possiamo fare:

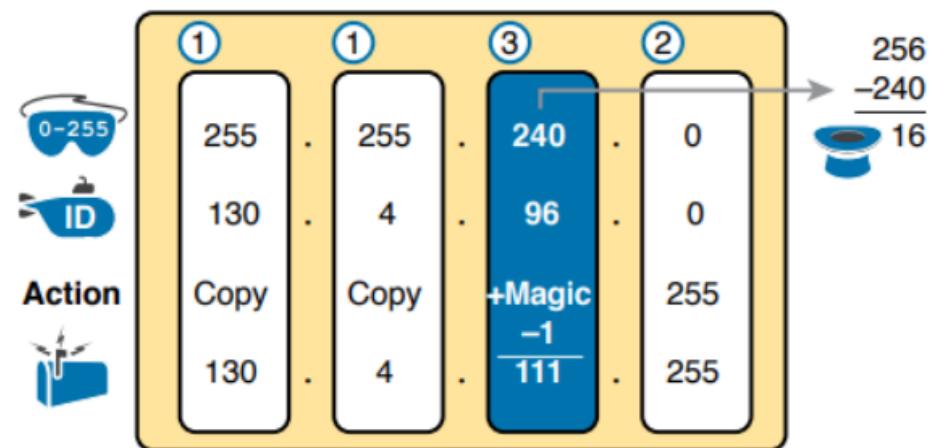
Passaggio 1. Se l'ottetto della maschera = 255, copiare l'ID della sottorete.

Passaggio 2. Se l'ottetto della maschera = 0, scrivere 255.

Passaggio 3. Se l'ottetto non è né 0 né 255, questo ottetto diventa l'interesting octet:

A. Calcola il magic number, cioè $256 - \text{maschera}$.

B. Prendi il valore dell'ID della sottorete, aggiungi il magic number e sottrai 1.



ROUTING

Per connettere più LAN come già detto si usano le WAN se collocate in maniera distante, per farlo si usano i router.

Router

Ogni router ha delle porte gigabit ethernet (2 di solito), seriali e almeno due slot vuoti dove inserire delle schede NIM, che permettono di configurare il router come si vuole; e si possono spegnere e accendere a piacimento (al contrario degli

switch).

Switch e Router condividono molti comandi e caratteristiche riguardanti la CLI, le differenze principali sono:

- conf ind. IP: ogni interfaccia può avere un ind. IP;
- i router hanno una porta AUX per collegare modem e linee telefoniche per configurarli a distanza;
- telnet e ssh disattivati di default (transport input none, per attivarla).

I router iniziano a instradare pacchetti appena viene inserito un indirizzo IP, se non è presente quella porta non riceve e non invia messaggi.

IP routing

L'IP routing è il processo di instradamento di un pacchetto da un punto A ad un punto B, utilizzando il layer 3.

L'host mittente crea un msg e lo invia al suo gateway predefinito, che a sua volta tramite le proprie tabelle di routing sa dove instradarlo correttamente.

Nel dettaglio:

Il processo di instradamento inizia con l'host che crea il pacchetto IP. Per prima cosa, l'host si pone la domanda «L'indirizzo IP di destinazione di questo nuovo pacchetto si trova nella mia sottorete locale?». L'host utilizza il proprio indirizzo IP/maschera per determinare il range di indirizzi della sottorete locale. In base a questo range l'host agisce come segue:

1. Se la destinazione è locale, invia direttamente:
 - A. Trova l'indirizzo MAC dell'host di destinazione. Utilizza la voce della tabella ARP (Address Resolution Protocol) già nota o utilizza i messaggi ARP per apprendere le informazioni.
 - B. Incapsula il pacchetto IP in un frame data-link, con l'indirizzo data-link di destinazione dell'host destinatario.
2. Se la destinazione non è locale, invia al gateway predefinito:
 - A. Trova l'indirizzo MAC del gateway predefinito. Utilizza la voce della tabella ARP (Address Resolution Protocol) già nota o utilizza i messaggi ARP per ottenere le informazioni.
 - B. Incapsula il pacchetto IP in un frame data-link, con l'indirizzo data-link di destinazione del gateway predefinito.

Il router ha più lavori da fare rispetto all'host:

- elabora i frame data link, solo se non presenta errori (controlla il FCS, se capisce che ci sono stati errori lo scarta) e se l'ind. di destinazione data-link è il suo;
- deincapsula il frame data-link, rimanendo con il pacchetto IP;
- decide dove inviarlo, tramite confronto con routing table e ind. di destinazione del pacchetto, se la sua tabella di routing ha una corrispondenza si procede;
- lo incapsula nuovamente in un frame data-link in base all'interfaccia di uscita;
- trasmette il frame nell'interfaccia che era precisata nella routing table.

Il router per aggiornare la sua tabella ha tre modi:

1. Connected routes: appena uso il comando di inserimento ind. ip in un'interfaccia il router sa che in quella interfaccia ci sarà tutta la rete che comprende l'ind appena messo.
2. Static routes: rotte che vengono messe in maniera manuale tramite comando ip route. Nel IOS alcune rotte possono essere nascoste anche se presenti nella tabella, se il link non è funzionante o comunque la rotta non viene usata.

Bisogna ricordare che:

I router utilizzano la rotta più specifica (mask + lunga)

3. Protocolli di routing: ci sono protocolli che scambiano messaggi fra router proprio per popolare la tabella.

Le floating static routes avvengono quando un router non ha rotte apprese dinamicamente, quindi prende quella con la distanza amministrativa migliore (quella messa tramite routing statico).

Se durante il comando ip route inserisco alla fine un numero viene messo come distanza amministrativa.

Le static default routes sono quelle rotte che fanno match con tutti gli indirizzi, in modo che se c'è un ind. che non ha nessuno match nella tabella viene inviato lì.

Item	Idea	Value in the Figure	Description
1	Classful network	10.0.0/8	The routing table is organized by classful network. This line is the heading line for classful network 10.0.0; it lists the default mask for Class A networks (/8).
2	Number of subnets	13 subnets	The number of routes for subnets of the classful network known to this router, from all sources, including local routes—the /32 routes that match each router interface IP address.
3	Number of masks	5 masks	The number of different masks used in all routes known to this router inside this classful network.
4	Legend code	C, L, O	A short code that identifies the source of the routing information. O is for OSPF, D for EIGRP, C for Connected, S for static, and L for local. (See Example 16-8 for a sample of the legend.)
5	Prefix (Subnet ID)	10.2.2.0	The subnet number of this particular route.
6	Prefix length (Mask)	/30	The prefix mask used with this subnet.
7	Administrative distance	110	If a router learns routes for the listed subnet from more than one source of routing information, the router uses the source with the lowest administrative distance (AD).
8	Metric	128	The metric for this route.
9	Next-hop router	10.2.2.5	For packets matching this route, the IP address of the next router to which the packet should be forwarded.
10	Timer	14:31:52	For OSPF and EIGRP routes, this is the time since the route was first learned.
11	Outgoing interface	Serial0/0/1	For packets matching this route, the interface out which the packet should be forwarded.

Per scegliere a chi inviare un messaggio controllando la tabella, cerca l'indirizzo con la mask più specifica (quella con più 1 in comune con l'indirizzo di destinazione) e se non basta perché ci sono delle rotte uguali allora guarda la distanza.

Esempio: bisogna inviare un msg all'indirizzo 172.16.254.5.

La tabella ha queste rotte:

- 172.16.1.1/32
- 172.16.1.0/24
- 172.16.0.0/22
- 172.16.0.0/26
- 0.0.0.0/8

In questo caso la scelta migliore è 172.16.1.0/24, perché ha più 1 in comune e non è una rotta specifica per un host come è la prima (172.16.1.1/32).

Se non ci fosse stato nessun match allora si sarebbe usata la static default route (0.0.0.0).

Protocolli

sono un insieme di messaggi, regole e algoritmi utilizzati dai router per apprendere i percorsi e per popolare le tabelle di routing, il cosiddetto routing dinamico.

Lo scopo fondamentale è apprendere e diffondere informazioni e scegliere il percorso migliore dopo aver ricevuto tutte le informazioni.

I protocolli possono essere interior, IGP (progettato per l'uso all'interno una AS) o exterior EGP (usati per collegare diversi sistemi autonomi).

L'unico EGP usato oggi è il BGP (Border Gateway Protocol) che usa un AS number per identificare le diverse AS univocamente.

Per gli IGP si usano OSPF e EIGRP.

I vari protocolli IGP si dividono in:

- distance vector: più vecchi, tempi di convergenza (modifica della rete) lenti, es: RIP
- distance vector advanced
- link-state: per esempio OSPF, hanno risolto i principali errori

Tabella comparativa IGP

Feature	RIPv2	EIGRP	OSPF
Classless/sends mask in updates/supports VLSM	Yes	Yes	Yes
Algorithm (DV, advanced DV, LS)	DV	Advanced DV	LS
Supports manual summarization	Yes	Yes	Yes
Cisco-proprietary	No	Yes ¹	No
Routing updates are sent to a multicast IP address	Yes	Yes	Yes
Convergence	Slow	Fast	Fast

Contemporaneamente all'introduzione di OSPF, Cisco ha creato un protocollo di routing

proprietario chiamato Enhanced Interior Gateway Routing Protocol (hybrid).

Metriche

I protocolli di routing, per raggiungere una sottorete, scelgono il percorso con la **metrica più bassa**.

Ad esempio, RIP utilizza un contatore del numero di router (**hops**) tra un router e la sottorete di destinazione, come mostrato nella prossima slide.

OSPF somma il costo associato a ciascuna interfaccia nel percorso end-to-end. Il costo è basato sulla larghezza di banda del collegamento.

IGP	Metric	Description
RIPv2	Hop count	The number of routers (hops) between a router and the destination subnet
OSPF	Cost	The sum of all interface cost settings for all links in a route, with the cost defaulting to be based on interface bandwidth
EIGRP	Calculation based on bandwidth and delay	Calculated based on the route's slowest link and the cumulative delay associated with each interface in the route

OSPF

Dopo che i router apprendono le info. delle reti vicine inviano a tutti gli altri (flooding) ciò che hanno appreso in modo che anche gli altri possano calcolare le loro rotte.

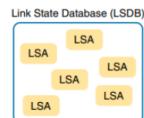
Informazioni sulla topologia e LSA (link-state advertisements)

I router che utilizzano i protocolli di routing link-state devono notificare praticamente ogni dettaglio sulla rete Internet a tutti gli altri router.

Alla fine del processo di invio delle informazioni a tutti i router, ogni router della rete internet ha le stesse identiche informazioni sulla rete stessa.

L'invio di molte informazioni dettagliate a tutti i router è un lavoro molto impegnativo rispetto a quello svolto dai protocolli di routing distance vector.

Open Shortest Path First (OSPF), il protocollo di routing IP link-state più diffuso, organizza le informazioni sulla topologia utilizzando gli LSA e il database link-state (LSDB). Ogni LSA è una struttura dati con alcune informazioni specifiche sulla topologia della rete; l'LSDB è la raccolta di tutti gli LSA noti a un router.



Durante l'invio di LSA è necessario evitare i loop, per questo prima dell'invio al prossimo router gli si chiede se già lo ha ricevuto. Gli LSA vengono rinviati ogni 30 minuti a meno che la rete non cambi prima.

Per elaborare le informazioni si usa il Dijkstra Shortest Path First.

Le tre fasi principali di come i router OSPF svolgono il lavoro di scambio di LSA e di calcolo delle rotte:

- **Becoming neighbors**: Una relazione tra due router che si collegano allo stesso link, creata in modo che i router vicini abbiano la possibilità di scambiare i loro LSDB.
- **Exchanging databases**: Il processo di invio di LSA ai vicini in modo che tutti i router apprendano gli stessi LSA.
- **Adding the best routes**: Ogni router esegue in modo indipendente SPF sulla propria copia locale dell'LSDB, calcola i percorsi migliori e li aggiunge alla tabella di routing IPv4.

I vicini OSPF sono router che utilizzano entrambi OSPF e che si trovano sullo stesso data link.

Due router possono diventare vicini OSPF se collegati alla stessa VLAN, allo stesso collegamento seriale o allo stesso collegamento WAN Ethernet.

Per diventare vicini OSPF, due router non devono semplicemente trovarsi sullo stesso collegamento, ma devono inviare messaggi OSPF e accettare di diventare vicini OSPF. A tal fine, i router inviano messaggi OSPF Hello, presentandosi al potenziale vicino. Gli Hello sono inviati in multicast all'indirizzo 224.0.0.5 e si aspetta di riceverli nello stesso indirizzo.

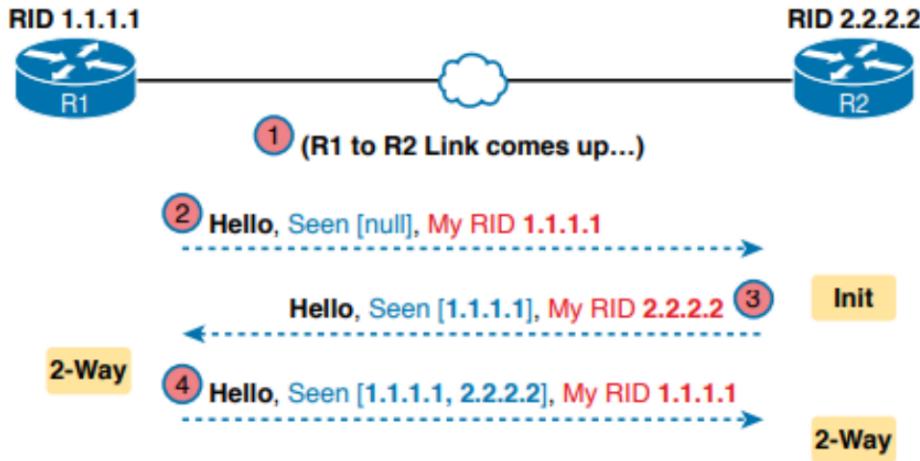
Gli Hello contengono l'ID router (RID) di ciascun router.

I RID di OSPF sono numeri a 32 bit. Di conseguenza, spesso sono mostrati come numeri decimali (DDN).

Per impostazione predefinita, IOS sceglie uno degli indirizzi IPv4 dell'interfaccia del router da utilizzare come RID. Tuttavia, il RID di OSPF può essere configurato manualmente.

Scelta del RID

1. Se è configurato il sottocomando `router-id rid`, questo valore viene utilizzato come RID.
2. Se le interfacce di **loopback** hanno un indirizzo IP configurato e l'interfaccia ha uno stato di up, il router sceglie l'indirizzo IP numericamente più alto tra queste interfacce di loopback.
3. Il router sceglie l'indirizzo IP numericamente più alto tra tutte le altre interfacce il cui codice di stato dell'interfaccia è **up**. (In altre parole, un'interfaccia in stato up/down viene inclusa da OSPF nella scelta del suo ID router).

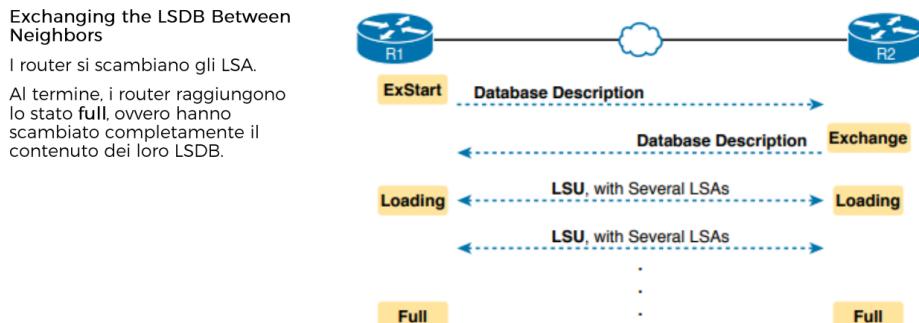


Lo stato 2-Way indica che:

- Il router ha ricevuto un Hello dal vicino, con indicato il RID del router stesso
- Il router ha controllato tutti i parametri dell'Hello ricevuto dal vicino, senza riscontrare problemi.
- Se entrambi i router raggiungono lo stato a 2-way, significa che entrambi i router

soddisfano tutti i requisiti di configurazione OSPF per diventare vicini. A questo punto

sono vicini e pronti a scambiarsi l'LSDB.



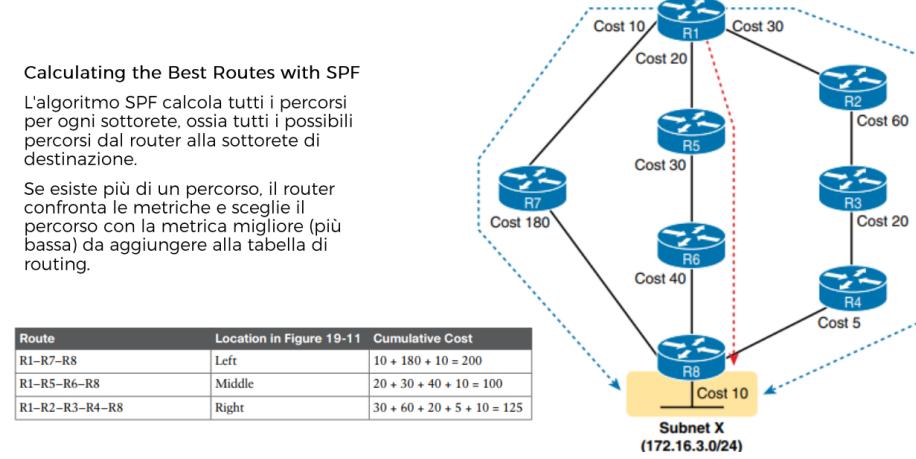
OSPF si comporta in modo diverso su alcuni tipi di interfacce in base a un'impostazione

chiamata network type.

Sui collegamenti Ethernet, OSPF utilizza per impostazione

predefinita un network type broadcast, che fa sì che OSPF elegga uno dei router della

stessa sottorete come router designato (DR) che svolge un ruolo fondamentale nel funzionamento del processo di scambio dei database, con regole diverse rispetto ai collegamenti punto-punto.

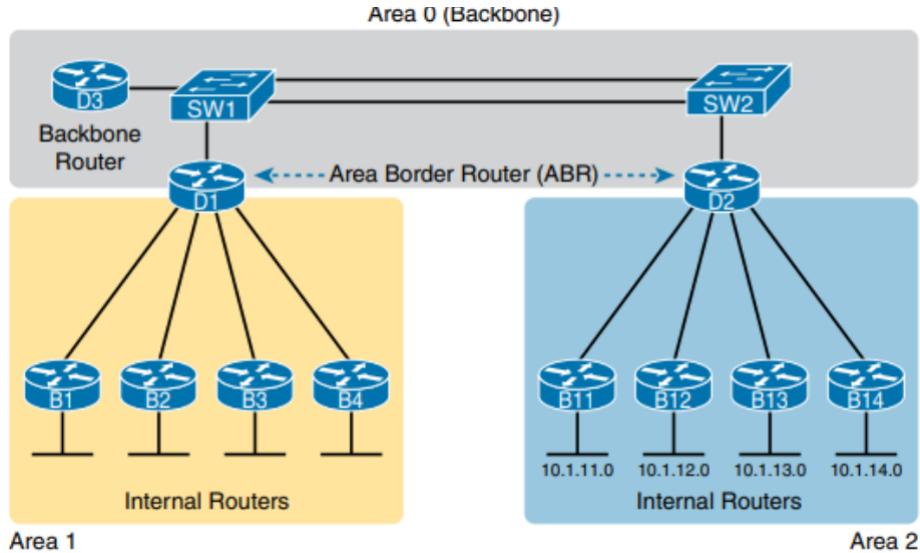


Se si lavora in un'unica area con tanti router, visto che ogni router deve sapere tutto di tutta la rete, il tempo di convergenza e la memoria per il database aumentano a dismisura.

Per risolvere, quando ci saranno più di 50 router di solito, si suddivide in aree la topologia.

Scegliere l'area per ogni interfaccia del router, come segue:

- Tutte le interfacce collegate alla stessa sottorete si trovano nella stessa area.
- Un'area deve essere contigua.
- Alcuni router possono essere interni a un'area, con tutte le interfacce assegnate a quella singola area.
- Alcuni router possono essere **Area Border Routers (ABR)** perché alcune interfacce si collegano all'area **backbone** e altre ad aree non backbone.
- Tutte le aree non backbone devono avere un percorso per raggiungere l'area backbone (area 0) con almeno un ABR collegato sia all'area backbone che all'area non backbone.



Term	Description
Area Border Router (ABR)	An OSPF router with interfaces connected to the backbone area and to at least one other area
Backbone router	A router connected to the backbone area (includes ABRs)
Internal router	A router in one area (not the backbone area)
Area	A set of routers and links that shares the same detailed LSDB information, but not with routers in other areas, for better efficiency
Backbone area	A special OSPF area to which all other areas must connect—area 0
Intra-area route	A route to a subnet inside the same area as the router
Interarea route	A route to a subnet in an area of which the router is not a part

Con tutte queste aree ora i router devono sapere un numero minore di informazioni, rimane il fatto che conosce le sottoreti esistenti, solo che non sa come sono fatte nello specifico.

Diminuisce il tempo di convergenza, c'è bisogno di meno CPU per elaborare LSDB, meno banda per comunicare, ecc.

I nuovi LSA si chiamano summary, utilizza informazioni sintetiche molto brevi sulle

sottoreti di altre aree. Questi LSA di riepilogo non includono informazioni sulla topologia

delle altre aree; tuttavia, ogni LSA di riepilogo contiene l'ID e la maschera di una

sottorete in un'altra area.

Gli LSA di riepilogo (summary) non richiedono alcuna elaborazione SPF.

Wildcard

Wildcard 0.0.0.0: confronta tutti e quattro gli ottetti. In altre parole, i numeri devono corrispondere esattamente.

Wildcard 0.0.0.255: Confronta solo i primi tre ottetti. Ignorare l'ultimo ottetto quando si confrontano i numeri.

Wildcard 0.0.255.255: Confronta solo i primi due ottetti. Ignorare gli ultimi due ottetti quando si confrontano i numeri.

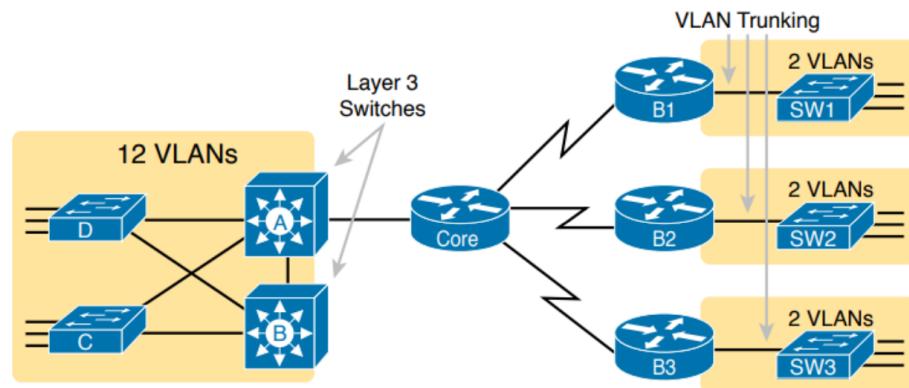
Wildcard 0.255.255.255: Confronta solo il primo ottetto. Ignora gli ultimi tre ottetti quando si confrontano i numeri.

Wildcard 255.255.255.255: Non confronta nulla; questa wildcard mask significa che gli indirizzi corrisponderanno al comando network.

ROAS

Se un router deve fare il routing fra diverse VLAN invece che collegare un cavo per ogni VLAN si può fare un trunk esattamente come per lo switch (router-on-stick o ROAS).

Ottiene con switch livello 3 che quindi permettono il routing senza avere un altro apparato.



Il ROAS funziona facendo un trunk tra switch e router, il collegamento fisico deve avere un ind. IP da parte del router, infatti si metterà un ind. per ogni VLAN che avrà un'interfaccia virtuale detta sottointerfaccia.

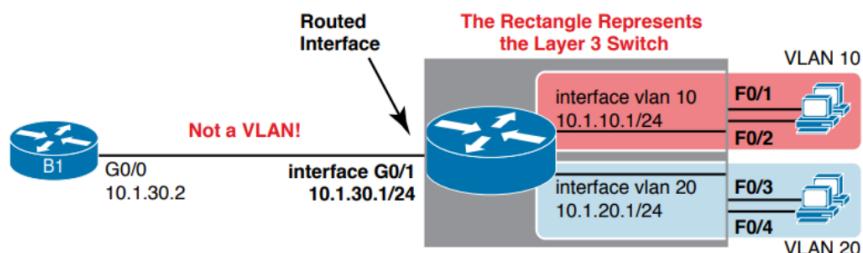


Layer 3 switch

Ogni VLAN ha bisogno di un'interfaccia virtuale (SVI) che si comporta come quella di un router con ind. IP e mask.

Lo switch layer 3 avrà anch'esso una routing table con le ruote collegate.

Implementazione delle Routed Interfaces sugli Switch



```
interface gigabitethernet 0/1
no switchport
ip address 10.1.30.1 255.255.255.0
```

TRANSPORT

Livello 4, fornisce error recovery e flow control.

TCP e UDP

I protocolli sono UDP e TCP, la differenza principale è che TCP fornisce un'ampia gamma di servizi alle applicazioni, mentre UDP non lo fa.

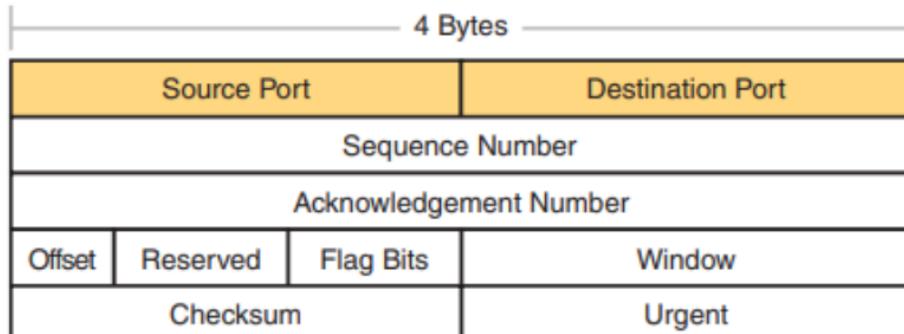
Ad esempio, i router scartano i pacchetti per molti motivi, tra cui errori di bit,

congestione e casi in cui non sono noti percorsi corretti. Infatti la maggior parte dei

protocolli data-link nota gli errori, ma poi scarta i frame che presentano errori.

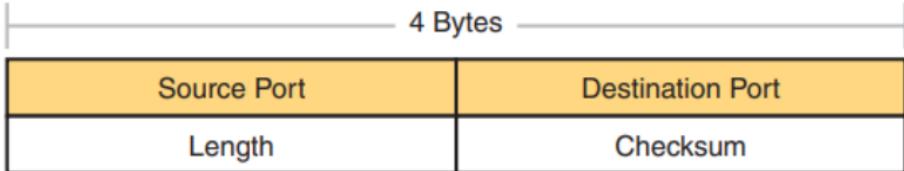
Il TCP fornisce un meccanismo di ritrasmissione e aiuta a evitare la congestione (controllo del flusso), mentre l'UDP non lo fa.

Il suo header:



UDP non è peggio di TCP solo perchè non offre servizi ma è utile visto la sua grossa versatilità e velocità.

Il suo header:



Servizi layer 4

(UDP solo multiplexing)

Function	Description
Multiplexing using ports	Function that allows receiving hosts to choose the correct application for which the data is destined, based on the port number
Error recovery (reliability)	Process of numbering and acknowledging data with Sequence and Acknowledgment header fields
Flow control using windowing	Process that uses window sizes to protect buffer space and routing devices from being overloaded with traffic
Connection establishment and termination	Process used to initialize port numbers and Sequence and Acknowledgment fields
Ordered data transfer and data segmentation	Continuous stream of bytes from an upper-layer process that is "segmented" for transmission and delivered to upper-layer processes at the receiving device, with the bytes in the same order

Multiplexing è l'utilizzo di porte per ogni applicazione che gira sul PC, così sappiamo a chi dare i pacchetti arrivati.

Le porte vengono assegnate dallo IANA, che divide le porte in:

- **Well Known (System) Ports:** Numeri da 0 a 1023, assegnati dalla IANA, con un processo di revisione più severo rispetto alle User Ports.
- **User (Registered) Ports:** Numeri da 1024 a 49151, assegnati dalla IANA con un processo meno rigido.
- **Ephemeral (Dynamic, Private) Ports:** Numeri da 49152 a 65535, non assegnati e destinati a essere allocati dinamicamente e utilizzati temporaneamente per un'applicazione client mentre l'applicazione è in esecuzione.

Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP ¹	DNS
67	UDP	DHCP Server
68	UDP	DHCP Client
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3

Connessione TCP

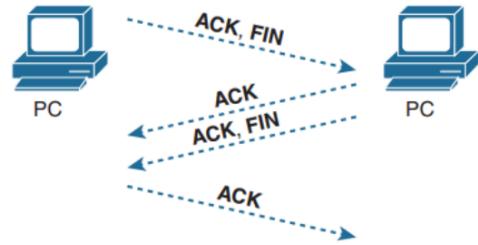
La creazione di una connessione TCP avviene prima che le altre funzioni TCP possano iniziare il loro lavoro.

L'instaurazione della connessione si riferisce al processo di inizializzazione dei campi **Sequence and Acknowledgment** e all'accordo sui numeri di porta utilizzati.



La figura mostra la terminazione della connessione TCP.

Questa sequenza di terminazione a quattro vie utilizza un flag aggiuntivo, chiamato bit FIN.



Error recovery

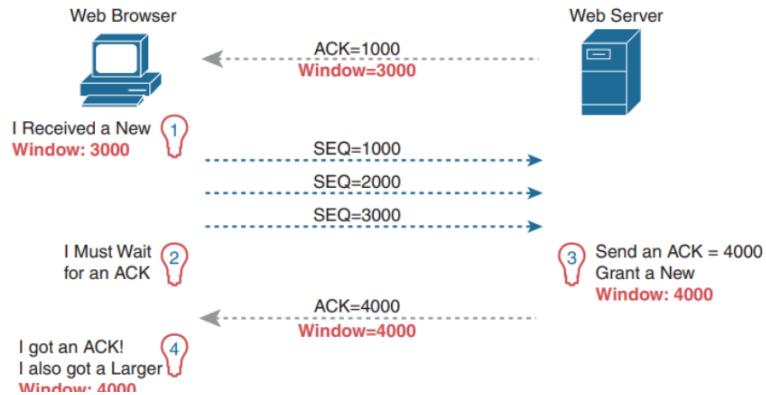
I PC durante la comunicazione TCP inviano in ogni pacchetto il numero di sequenza e se li riceve tutti, andando a controllare i numeri manda un ACK, nel caso ne manca uno lo richiede:



L'arrivo in ordine non è obbligatorio, infatti TCP può ordinare da solo i messaggi ricevuti.

Flow control

Il TCP implementa il controllo del flusso utilizzando il concetto di finestra. Il controllo si applica alla quantità di dati che possono essere in sospeso e in attesa di ack in un dato momento.



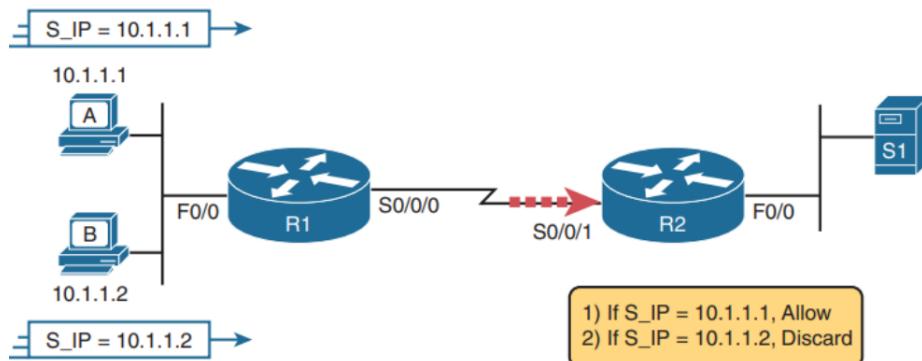
Quindi in caso la finestra sia troppo grande, e quindi il PC non riesce a starci dietro, il mittente può diminuire la finestra e mandare meno pacchetti. Al contrario, come avviene nell'immagine, è possibile aumentare la finestra diminuendo il numero di ack inviati e potendo riceverne di più prima di confermare.

ACL

Access control list, liste di indirizzi IP che sono consentiti o meno in ingresso o uscita ad alcune interfacce, sostanzialmente sono dei filtri.

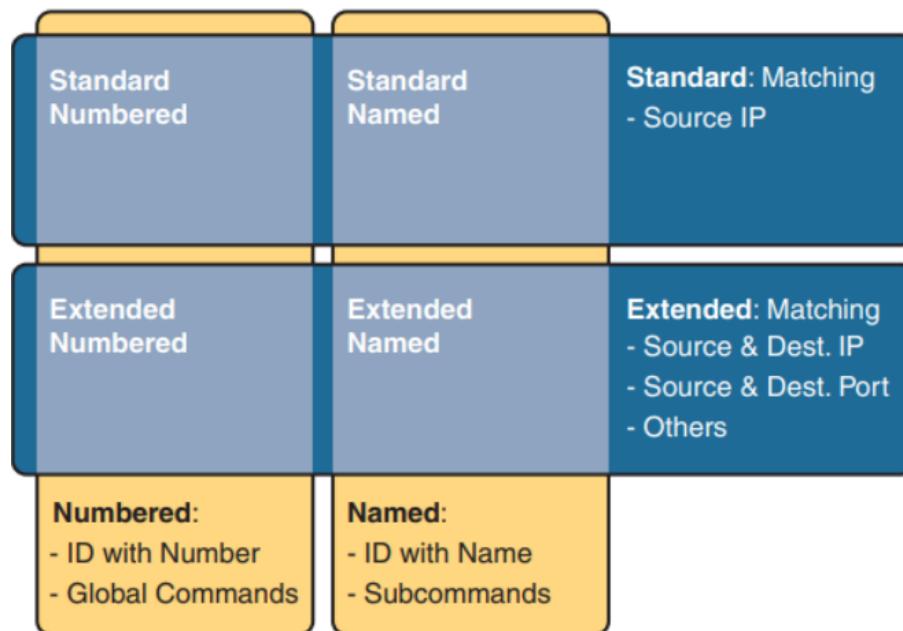
Le ACL hanno un verso, il controllo viene fatto prima (entrata) o dopo (uscita) che il router ha scelto il routing.

Un ACL è un comando che cerca determinati valori nell'intestazione e fa un'azione.



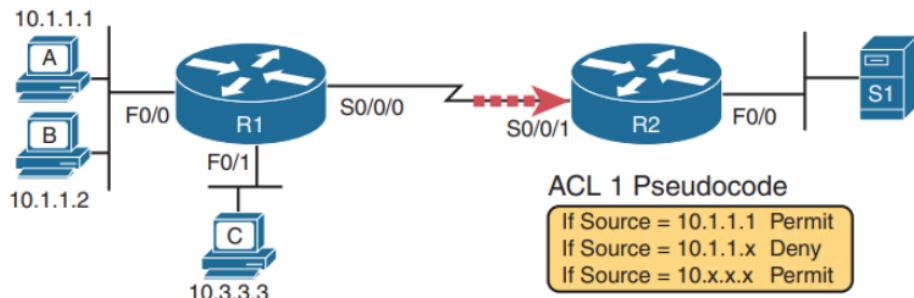
La parola chiave è deny o permit.

- Cisco IOS supporta le ACL IP fin dagli albori dei router Cisco.
A partire dalle ACL originali dei primi tempi, Cisco ha aggiunto molte funzioni, tra cui le seguenti:
- Standard numbered ACLs (1-99)
 - Extended numbered ACLs (100-199)
 - Additional ACL numbers (1300-1999 standard, 2000-2699 extended)
 - Named ACLs
 - Improved editing with sequence numbers



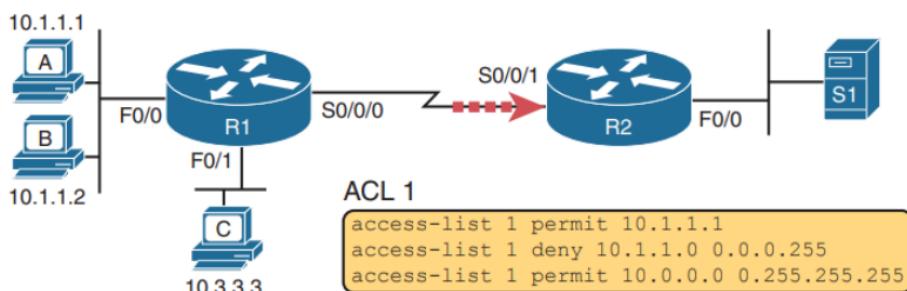
L'ordine delle ACL è importante

Possiamo farle direttamente su un indirizzo IP specifico:



Host A ✓ If Source = 10.1.1.1 Permit If Source = 10.1.1.x Deny If Source = 10.x.x.x Permit	Host B ✗ If Source = 10.1.1.1 Permit ✓ If Source = 10.1.1.x Deny If Source = 10.x.x.x Permit	Host C ✗ If Source = 10.1.1.1 Permit ✗ If Source = 10.1.1.x Deny ✓ If Source = 10.x.x.x Permit
--	--	--

Oppure su una subnet di un indirizzo tramite wild card:



Ad esempio, per la sottorete 172.16.8.0 255.255.252.0, utilizzare il numero di sottorete (172.16.8.0) come indirizzo, quindi eseguire i seguenti calcoli per trovare la wildcard mask:

255.255.255.255 -
255.255.252.0 =
0.0.3.255

Continuando l'esempio, un comando completo per questa stessa sottorete sarebbe il seguente:

```
access-list 1 permit 172.16.8.0 0.0.3.255
```

Step 1. Pianificare la posizione (router e interfaccia) e la direzione (in entrata o in uscita) su tale interfaccia:

- Le ACL standard devono essere posizionate vicino alla destinazione dei pacchetti, in modo da non scartare involontariamente pacchetti che non dovrebbero essere scartati.
- Poiché le ACL standard possono corrispondere solo all'indirizzo IP di origine di un pacchetto, è necessario esaminare solo gli indirizzi IP di origine dei pacchetti che vanno nella direzione desiderata.

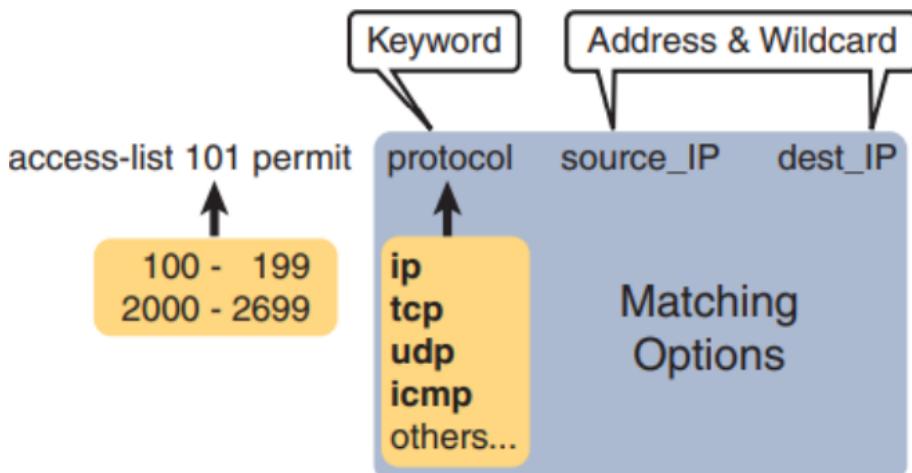
Step 2. Eseguire uno o più comandi di configurazione globale «access-list» per creare la ACL, tenendo presente quanto segue:

- L'elenco viene cercato in modo sequenziale, utilizzando la logica del first-match.
- L'azione predefinita, se un pacchetto non corrisponde a nessuno dei comandi, è quella di negare (scartare) il pacchetto.

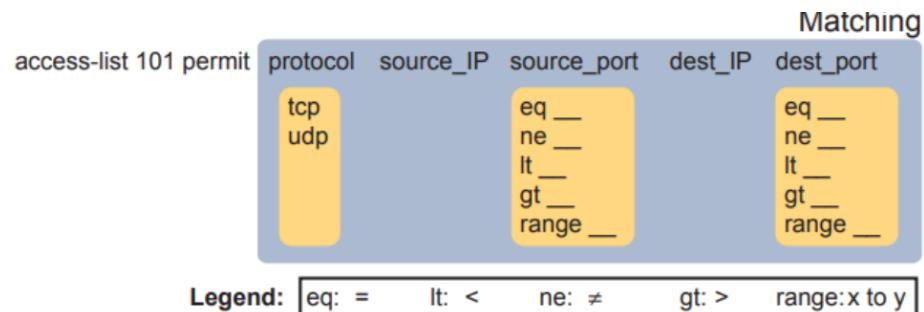
Step 3. Abilitare la ACL sull'interfaccia del router scelta, nella direzione corretta, utilizzando il sottocomando **ip access-group number {in | out} interface**.

Extended ACL

Ora il match si farà anche in base al destinatario, mittente e protocollo.



Si può fare match anche con le porte:



DHCP

Protocollo che fornisce in maniera dinamica gli indirizzi IP, mask, default gateway, ecc agli host della rete tramite server.

Può essere:

- statico: l'amministratore dice a quale MAC bisogna dare un determinato IP
- dinamico: una macchina ha un'ind. IP dato dal server per un certo periodo poi viene cambiato
- automatico: un PC riceve un IP random e lo terrà per sempre, anche dopo il riavvio.

Nel dinamico:

1. Il client richiede un IP tramite broadcast, DHCP REQUEST;
2. tramite DHCP OFFER il server invia un IP preso da un pool predefinito, messaggio inviato in unicast a livello 2.
3. il client replica in broadcast, tramite DHCP quale server ha scelto;
4. il server fa un ping all'indirizzo che darà al cliente per vedere se lo stanno già usando, se tutto va bene conferma al client tramite DHCP ACK, altrimenti invia un NACK e si ricomincia.

Le altre opzioni che il DHCP può offrire oltre all'IP sono dette option e sono numerate:

- Nelle slides 10 e 11 Services
- 66 - 105: usati nella chiamata IP, sono gli indirizzi del centralino.

NTP

Serve per sincronizzare orologi, sempre di tipo client/server. Basato su UDP, perché TCP comporta ritardi che annullerebbero l'efficacia del protocollo.

Il protocollo comunica con dei Primary Time Server che restituiscono l'orario corretto.

NTP:

1. rende tutte le macchine sincronizzate;
2. scalabile, perché è possibile avere più orologi;
3. accurato;

Esiste anche l'SNTP utilizzato per tutte le applicazioni che non necessitano di un orario perfetto.

NAT

Consente ad un host di ricevere un indirizzo IP pubblico per comunicare in maniera globale, su internet.

Praticamente il pacchetto IP con indirizzo privato viene incapsulato in uno con ind. pubblico e poi viene spaccettato per mostrare l'ind. privato ad destinazione.

NAT può essere:

- statico: si fa una associazione 1 a 1 per ogni indirizzo privato con uno pubblico (gli indirizzi pubblici vengono presi da un pool di ind. comprati dalla'azienda), si va avanti finchè non finisco gli ind. pubblici;
- dinamico: la mappatura tra indirizzo ip privato e pubblico viene fatta quando c'è una richiesta e non a priori;
- overloading: consente al NAT di scalare per supportare molti client con pochi ind. pubblici, per funzionare utilizza lo stesso ind. pubblico per più ind. privati ma utilizza diverse porte per differenziali [UNICO CHE RISOLVE IL PROBLEMA DEGLI IND. IPV4 IN ESAURIMENTO].

IPv6

Gli indirizzi pubblici di IPv4 stanno finendo per questo si è deciso di utilizzare una nuova tipologia di indirizzi che usa 128 bit invece che i 32 precedenti. IPv6 al posto di NAT è una soluzione definitiva al problema.

Il passaggio da IPv4 a IPv6 è difficile perché il vecchio protocollo ha un ecosistema che si basa su di esso. Infatti sarebbero da cambiare tutti quei protocolli che si basano su IPv4, esempio:

- OSPF, che ora ha la versione 3 che supporta IPv4 e IPv6;
- ICMP, aggiornato alla versione 6;
- ARP sostituito a NDP (Neighbor Discovery Protocol).

Routing Protocol	Defined By	Notes
RIPng (RIP next generation)	RFC	The “next generation” is a reference to a TV series, <i>Star Trek: the Next Generation</i> .
OSPFv3 (OSPF version 3)	RFC	The OSPF you have worked with for IPv4 is actually OSPF version 2, so the new version for IPv6 is OSPFv3.
EIGRPv6 (EIGRP for IPv6)	Cisco	Cisco owns the rights to the EIGRP protocol, but Cisco also now publishes EIGRP as an informational RFC.
MP BGP-4 (Multiprotocol BGP version 4)	RFC	BGP version 4 was created to be highly extendable; IPv6 support was added to BGP version 4 through one such enhancement, MP BGP-4.

L'IPv6 utilizza questi concetti allo stesso modo dell'IPv4:

- Per poter creare e inviare pacchetti IPv6 da un'interfaccia, i dispositivi degli utenti finali hanno bisogno di un indirizzo IPv6 su quell'interfaccia.
- Gli host degli utenti finali devono conoscere l'indirizzo IPv6 di un router predefinito, al quale l'host invia i pacchetti IPv6 se il destinatario si trova in una sottorete diversa.
- I router IPv6 deincapsulano e ri-incapsulano ogni pacchetto IPv6 durante l'instradamento del pacchetto.
- I router IPv6 prendono decisioni sull'instradamento confrontando l'indirizzo di destinazione del pacchetto IPv6 con la tabella di instradamento IPv6; il relativo percorso elenca le indicazioni su dove inviare successivamente il pacchetto.

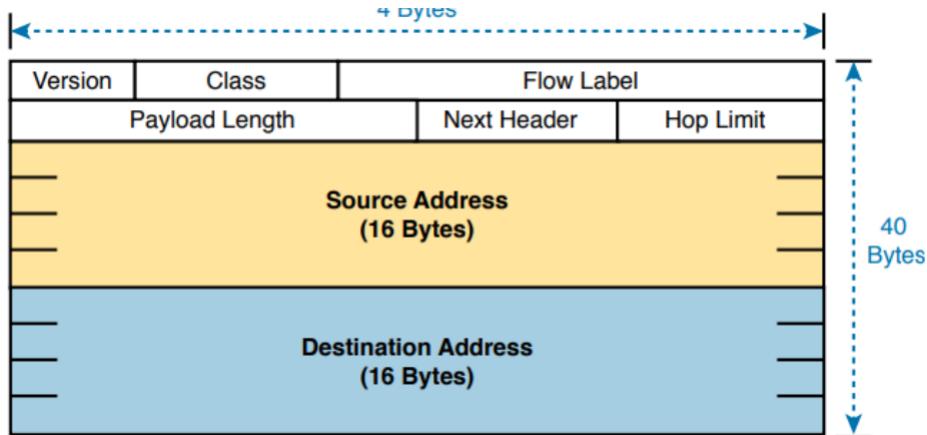
Gli indirizzi IPv6 sono espressi in esadecimale in modo da avere indirizzi più corti rispetto alla controparte decimale e divisi in 8 quartetti divisi dai ‘:’, es:

2345:1111:2222:3333:4444:5555:6666:AAAA

2000:1:2:3:4:5:6:A

FE80::1

L'header IPv6 è:



Visto che il nuovo indirizzo è espresso in hex, per renderlo più leggibile e corto si usa la notazione abbreviata che consiste nel togliere gli zero iniziali (a sinistra) di ogni quartetto e se rimangono più quartetti consecutivi con solo zero si usano i ‘::’ (doppi due punti) per rappresentarli:

FE00:0000:0000:0001:0000:0000:0000:0056

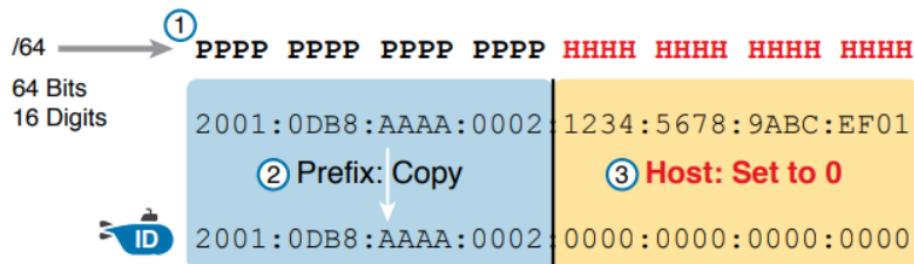
FE00:0:0:1:0:0:0:56

FE00:0:0:1::56

I DOPPI DUE PUNTI POSSO METTERLI SOLO UNA VOLTA PER INDIRRIZZO, e conviene metterli nel punto dove togliamo più zero consecutivi.

I prefissi funzionano esattamente come IPv6 e si rappresentano nello stesso modo (Ad esempio: /64 saranno 4 coppie cioè la metà perchè il totale è 128 bit).

Calcolare il Subnet ID



I prefissi saranno sempre multipli di 4, quindi spezzano sempre in base ai quartetti.

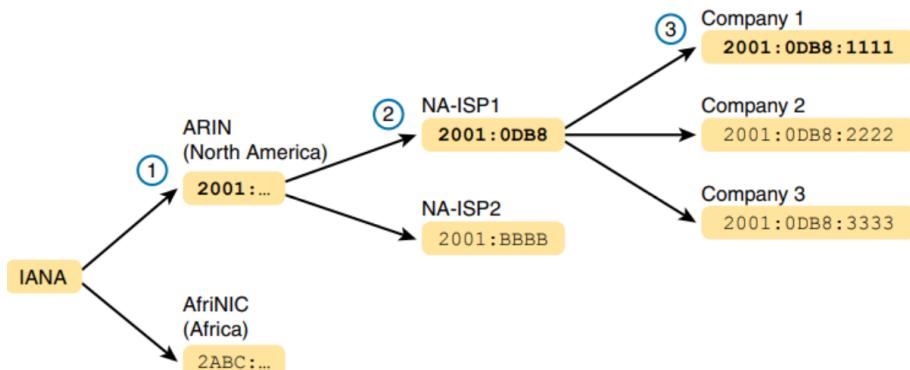
Anche IPv6 ha la propria versione di indirizzi pubblici detti Global Unicast, assegnato in maniera univoca ad un'organizzazione, viene assegnato come global routing prefix che contiene un blocco di indirizzi.

Al posto dei privati IPv4 ci sono gli Unique local (che iniziano con FD).

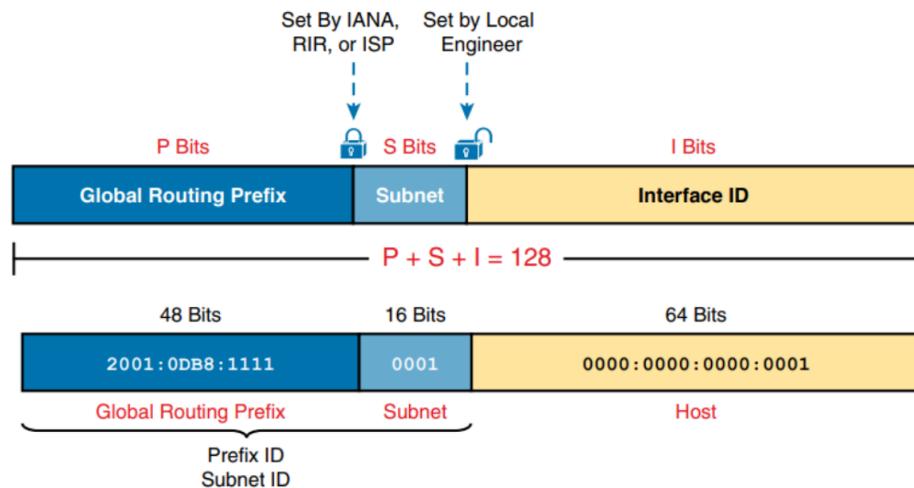
Address Type	First Hex Digits
Global unicast	2 or 3 (originally); all not otherwise reserved (today)
Unique local	FD
Multicast	FF
Link local	FE80

Gli indirizzi IPv6 global unicast consentono all'IPv6 di funzionare in modo simile al progetto originale dell'Internet IPv4. Ogni organizzazione richiede un blocco di indirizzi IPv6 che nessun altro può utilizzare. L'organizzazione suddivide poi il blocco di indirizzi in parti più piccole, chiamate sottoreti. Infine, per scegliere quale indirizzo IPv6 utilizzare per ogni host, il tecnico sceglie un indirizzo dalla sottorete giusta.

Il blocco riservato di indirizzi IPv6 - un insieme di indirizzi che solo un'azienda può utilizzare - è chiamato **global routing prefix** (prefisso di routing globale). Ogni organizzazione che vuole connettersi a Internet e utilizzare gli indirizzi unicast globali IPv6 deve richiedere e ricevere un prefisso di routing globale. In generale, si può pensare al prefisso di routing globale come a un ID di rete IPv4 di classe A, B o C della gamma di indirizzi IPv4 pubblici.

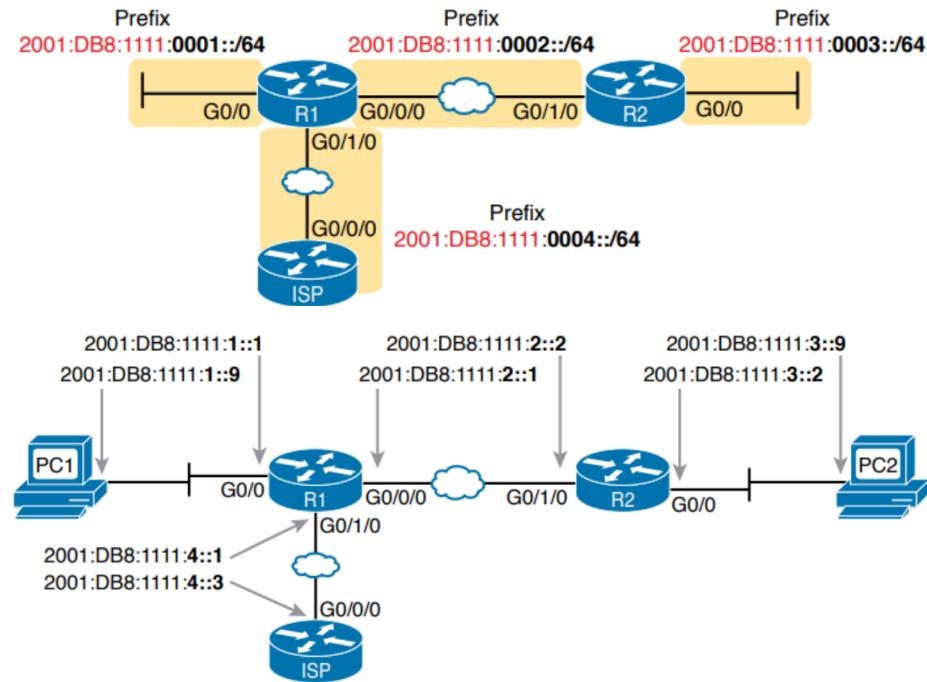


Il subnetting simile a quello IPv4:



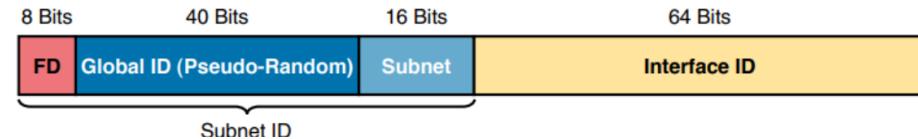
In questo esempio posso avere 2^{16} sottoreti.

Esempio di rete:

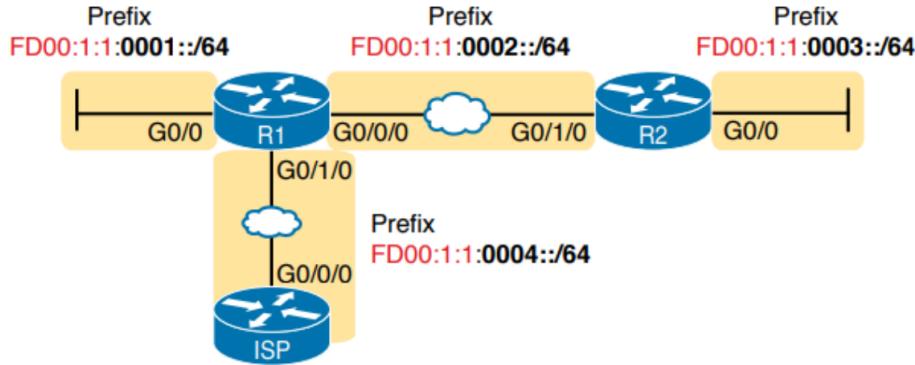


Per assegnare gli indirizzi alle interfacce faccio in modo analogo ad IPv4, in maniera statica (con lunghezza prefisso, DG e DNS) o con DHCP oppure SLAAC che è un meccanismo integrato in IPv6 (come DHCP ma stateless, quindi senza server).

Per creare gli indirizzi unique local (privati) uso questa sintassi:



In questo esempio è tutto deciso da noi TRANNE i primi 8 bit. Esempio:



Ora parliamo degli indirizzi link-local, sono indirizzi unicast usati però per l'overhead e l'instradamento. I pacchetti per gli indirizzi link-local non escono mai dalla LAN locale, vengono usati per comunicare all'interno della sottorete senza paura che esca proprio perchè non viene fatto il routing su di esso.

64 Bits	64 Bits
FE80 : 0000 : 0000 : 0000	Interface ID: EUI-64

L'indirizzo link-local deve sempre far parte del range FE80::/10.

Il neighbor discovery protocol (NDP) è la versione avanzata di ARP, ha le stesse funzionalità più:

Router Discovery: Gli host apprendono gli indirizzi IPv6 dei router disponibili nella stessa sottorete.

SLAAC: quando si utilizza la configurazione automatica dell'indirizzo stateless l'host utilizza i messaggi NDP per apprendere la sottorete (prefisso) utilizzata e la lunghezza del prefisso.

DAD: prima di utilizzare un indirizzo IPv6, gli host utilizzano NDP per eseguire un processo di Duplicate Address Detection (DAD), per assicurarsi che nessun altro host utilizzi lo stesso indirizzo IPv6.

Il neighbor MAC discovery in NDP funziona così:

Discovering Neighbor Link Addresses with NDP

Neighbor Solicitation (NS): Questo messaggio chiede all'host con un particolare indirizzo IPv6 (l'indirizzo di destinazione) di rispondere con un messaggio NA che contenga il suo indirizzo MAC.

Neighbor Advertisement (NA): Questo messaggio contiene gli indirizzi IPv6 e MAC del mittente. Può essere inviato in risposta a un messaggio NS e, in tal caso, il pacchetto viene inviato all'indirizzo IPv6 unicast dell'host che ha inviato il messaggio NS originale. Un host può anche inviare un NA non richiesto, annunciando i propri indirizzi IPv6 e MAC, nel qual caso il messaggio viene inviato a un particolare indirizzo multicast.

Il router discovery:

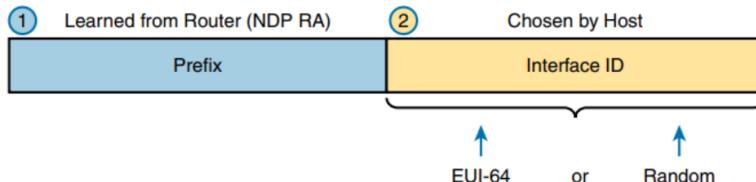
Discovering Routers with NDP

Router Solicitation (RS): Questo messaggio viene inviato all'indirizzo multicast "all-IPv6-routers" (FF02::2), in modo che il messaggio chieda a tutti i router, solo local link, di identificarsi.

Router Advertisement (RA): Questo messaggio, inviato dal router, contiene varie info, tra cui l'indirizzo IPv6 locale del router.
I router inviano anche messaggi RA, senza essere interpellati, all'indirizzo multicast "all-IPv6-hosts" (FF02::1).

Lo SLAAC:

1. Apprendere il prefisso IPv6 utilizzato sul link, da qualsiasi router, utilizzando i messaggi NDP RS/RA.
2. Costruire un indirizzo con il prefisso appreso più un interface ID, scelto utilizzando le regole EUI-64 o un valore casuale.
3. Prima di usare l'indirizzo, usare DAD per assicurarsi che nessun altro host stia già usando lo stesso indirizzo.



DAD (Discovery Duplicate Addresses):

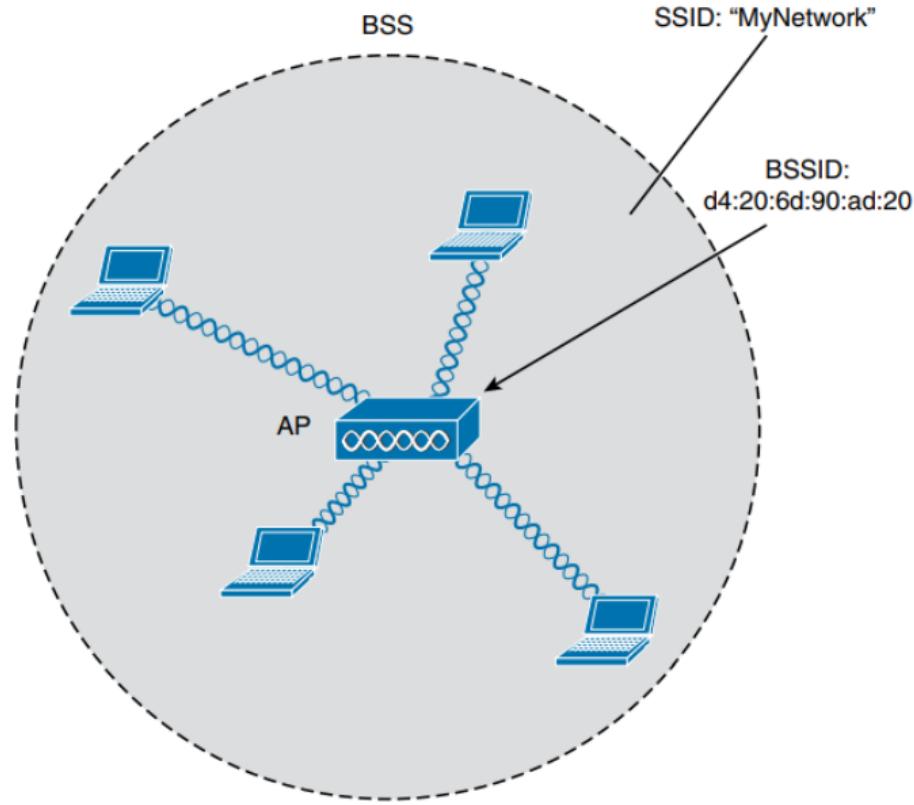
1. PC1, prima di utilizzare l'indirizzo 2001:DB8:1111:1::11, deve utilizzare DAD.
2. PC1 invia un messaggio NS, contenente l'indirizzo che PC1 vuole utilizzare (2001:DB8:1111:1::11) come destinazione.
3. PC2 riceve il messaggio NS, e invia un messaggio NA.
4. PC1, ricevendo il messaggio NA per il proprio indirizzo IPv6, si rende conto che esiste un indirizzo duplicato.

WIRELESS

Comunicazione senza cavi usando la radiofrequenza, due dispositivi devono essere nella stessa frequenza per comunicare.

Per comunicare i vari device devono attendere prima di comunicare se c'è già una comunicazione in corso. Quindi bisogna operare in modalità half-duplex usando anche lo standard 802.11 per decidere se comunicare o aspettare.

Per regolare le comunicazioni si raggruppano i dispositivi in BSS con al centro un access point (AP) che decide qual è il canale di comunicazione.



Quindi due client non possono comunicare direttamente fra loro ma devono passare dall'access point.

L'access point fa distribuzione di un segnale ed è possibile chiamarlo transitional bridge collegando il mondo wireless al mondo cablato (collegati a livello 2), e quindi mappare una VLAN con una SSID.

Si può fare trunking anche via etere con più SSID.

Normalmente, un AP non può coprire l'intera area in cui potrebbero trovarsi i client.

Quando gli AP sono collocati in posizioni geografiche diverse, possono essere tutti interconnessi da un'infrastruttura commutata.

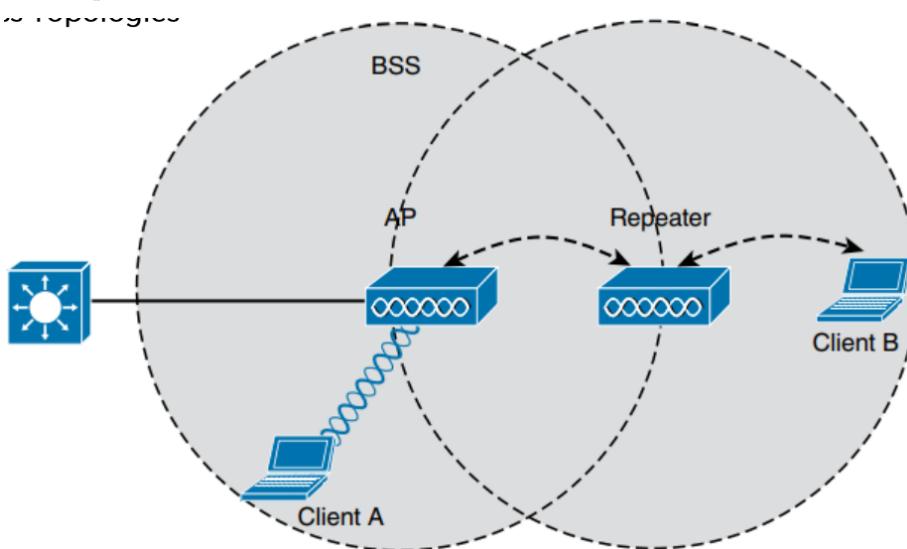
Lo standard 802.11 lo chiama "extended service set" (ESS).

L'idea è quella di far cooperare più AP in modo che il servizio wireless sia coerente e senza interruzioni dal punto di vista del client.

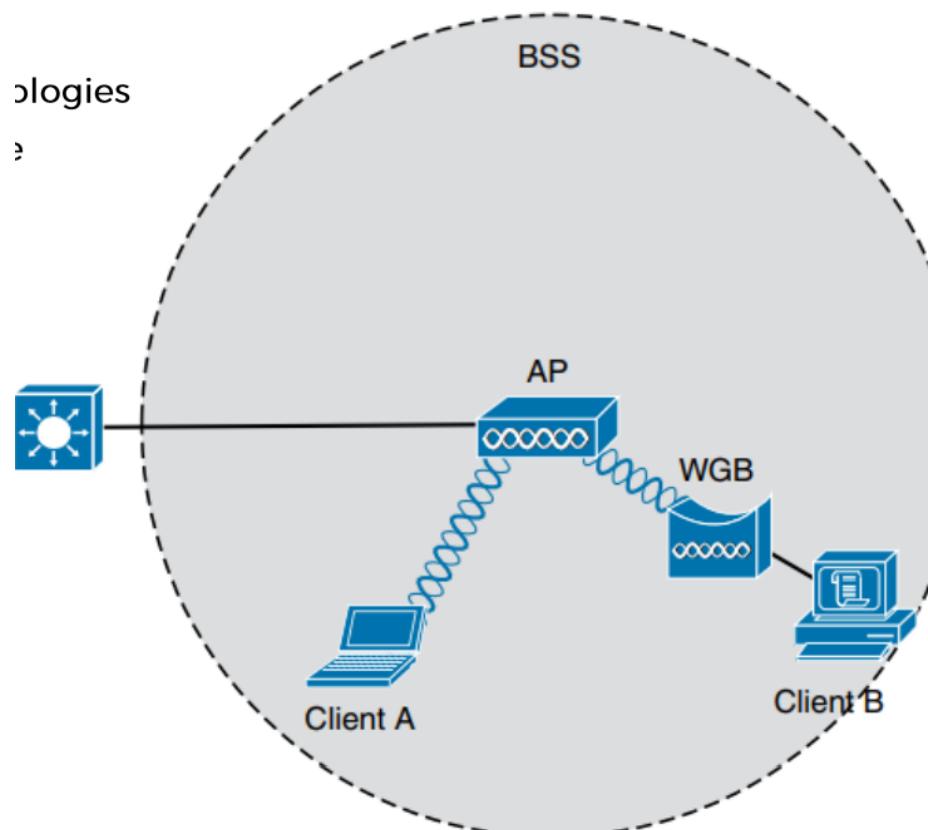
Il passaggio da un AP all'altro si chiama roaming

Esistono diverse topologie nel wireless:

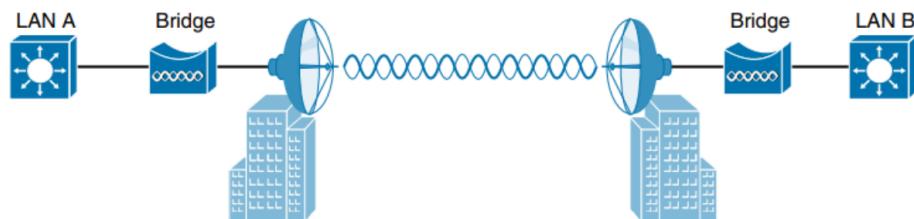
- repeater:



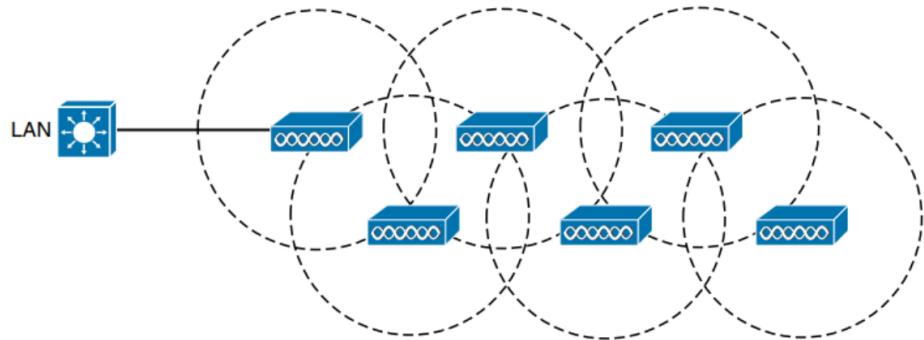
- workgroup bridge: si ha un apparato che mette in wireless computer che non possono farlo da soli



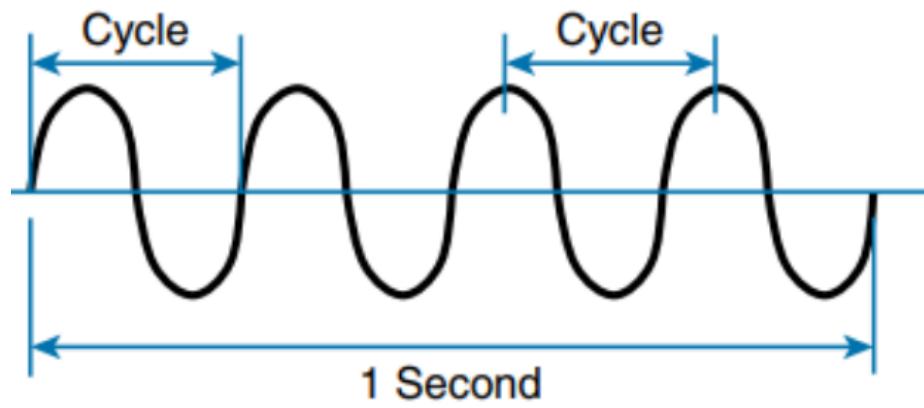
- outdoor bridge:



- mesh network:



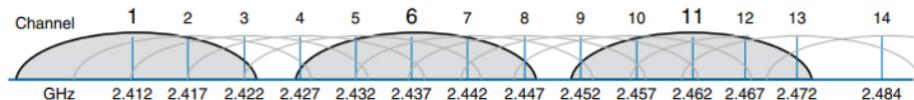
Un'onda radio è così fatta:



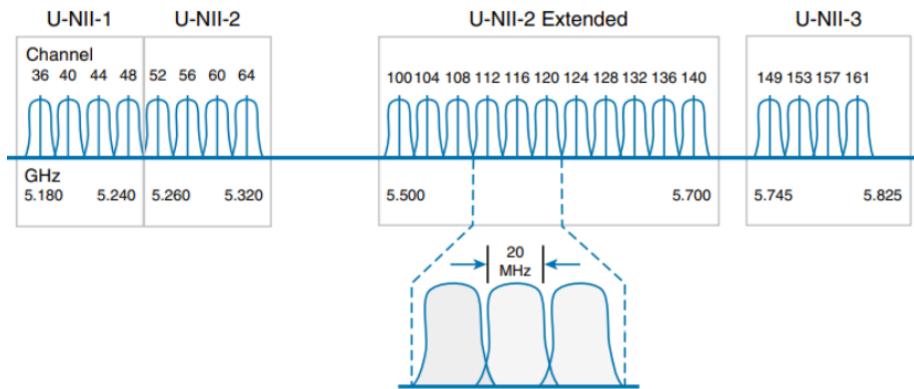
$$\begin{aligned} \text{Frequency} &= 4 \text{ cycles/second} \\ &= 4 \text{ Hertz} \end{aligned}$$

Le frequenze usate nel wireless sono la 2.4 e 5 GHz, dette libere, in realtà le bande comprendono più frequenze come 2,400 a 2,4835 per la prima e fra 5,150 e 5,825 la seconda.

Le bande 2,4 GHz sono divise in 14 canali dove i dispositivi ascoltano/trasmettono. Molti canali sono in overlapping, cioè più canali comprendono le stesse frequenze, per questo usiamo solo alcuni canali:



Nelle bande a 5 GHz non c'è questo problema e possiamo usare tutti i canali contemporaneamente:



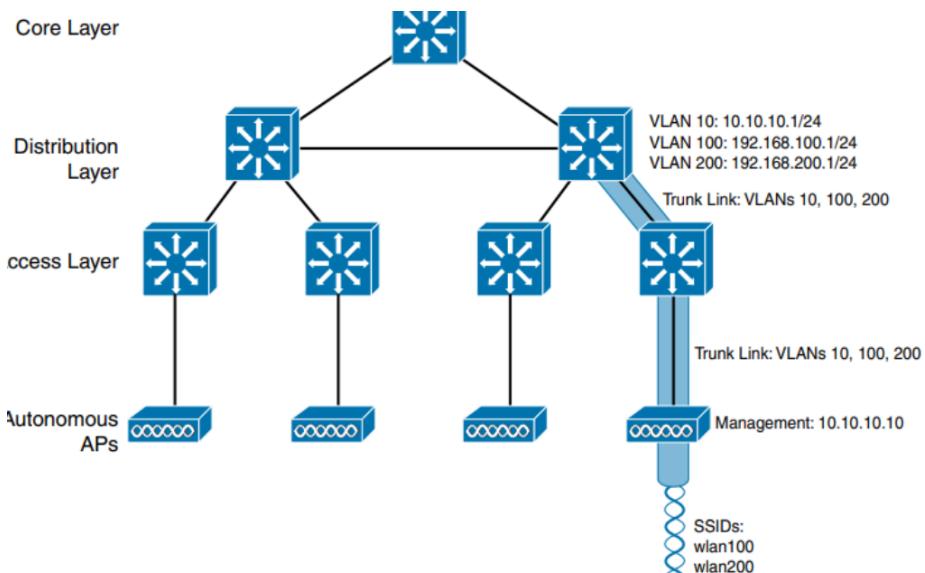
Autonomous AP Architecture

Un AP autonomo è dotato di hardware sia cablato che wireless, in modo che le associazioni dei client wireless possano essere terminate su una connessione cablata localmente all'AP.

Gli AP e le loro connessioni dati devono essere distribuiti nell'area di copertura e nella rete.

Gli AP autonomi offrono uno o più set di servizi di base (BSS) completamente funzionali e indipendenti.

Sono un'estensione naturale di una switched network, che collega i service set identifiers (SSID) alle LAN virtuali cablate (VLAN) al livello di accesso.



Split-MAC Architectures

L'amministratore di rete ha il compito di selezionare e configurare il canale utilizzato da ciascun AP e di rilevare e gestire eventuali AP che potrebbero interferire.

Deve anche gestire elementi come il livello di **potenza di trasmissione** per assicurarsi che la copertura wireless sia sufficiente, non si sovrapponga troppo e non ci siano buchi di copertura, anche quando un AP si guasta.

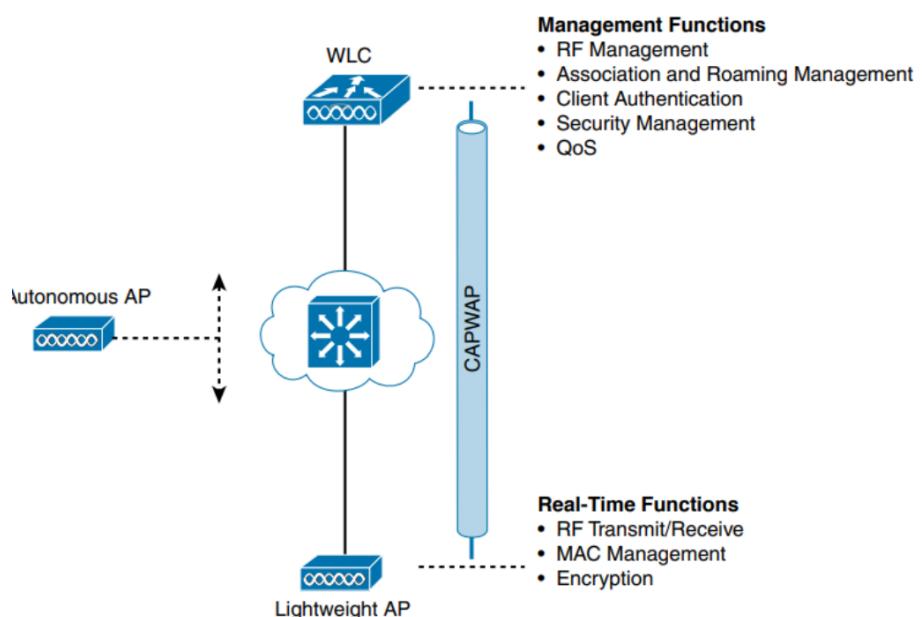
Per superare i limiti degli AP autonomi distribuiti, molte delle funzioni presenti negli AP autonomi devono essere spostate verso una **posizione centrale**.

Quando le funzioni di un AP autonomo vengono divise, l'hardware dell'AP viene chiamato **lightweight access point** ed esegue solo le operazioni 802.11 **in tempo reale**

Le funzioni di **gestione** sono solitamente svolte da un **controller LAN wireless (WLC)**, che controlla molti AP lightweight.

La divisione del lavoro tra AP lightweight e WLC è nota come **architettura split-MAC**.

In sostanza la figura centrale fa tutto e gli AP semplicemente ricevono e applicano ciò che dice il WLC



I due dispositivi devono utilizzare un protocollo di **tunneling** tra loro, per trasportare i messaggi relativi all'802.11 e anche i dati dei client.

L'AP e il WLC **possono** essere situati sulla stessa VLAN o subnet IP, ma non devono necessariamente esserlo.

Possono trovarsi su due sottoreti IP completamente diverse in due luoghi completamente diversi.

Il protocollo di tunneling **Control and Provisioning of Wireless Access Points (CAPWAP)** rende possibile tutto questo incapsulando i dati tra il LAP e il WLC in pacchetti IP.

La relazione CAPWAP consiste in realtà in due tunnel separati:

Messaggi di controllo CAPWAP: Trasporta i messaggi utilizzati per configurare l'AP e gestirne il funzionamento. I messaggi di controllo sono autenticati e crittografati, in modo che l'AP sia controllato in modo sicuro solo dal WLC appropriato.

Dati CAPWAP: Utilizzato per i pacchetti che viaggiano da e verso i client wireless associati all'AP. I pacchetti di dati vengono trasportati sul tunnel dei dati, ma non sono crittografati per impostazione predefinita. Quando la crittografia dei dati è abilitata per un AP, i pacchetti sono protetti con Datagram Transport Layer Security (DTLS).

Ogni AP e WLC deve inoltre autenticarsi reciprocamente con certificati digitali.

Attività del WLC:

Dynamic channel assignment: Il WLC può scegliere e configurare automaticamente il canale RF utilizzato da ogni AP, in base agli altri access point attivi nell'area.

Transmit power optimization: Il WLC può impostare automaticamente la potenza di trasmissione di ogni AP in base all'area di copertura necessaria.

Self-healing wireless coverage: Se un AP muore, il buco di copertura può essere "sanato" aumentando automaticamente la potenza di trasmissione degli AP circostanti.

Flexible client roaming: I client possono spostarsi tra gli AP con tempi di roaming molto rapidi.

Dynamic client load balancing: Se due o più AP sono posizionati per coprire la stessa area geografica, il WLC può associare i client all'AP meno utilizzato. In questo modo il carico dei client viene distribuito tra gli AP.

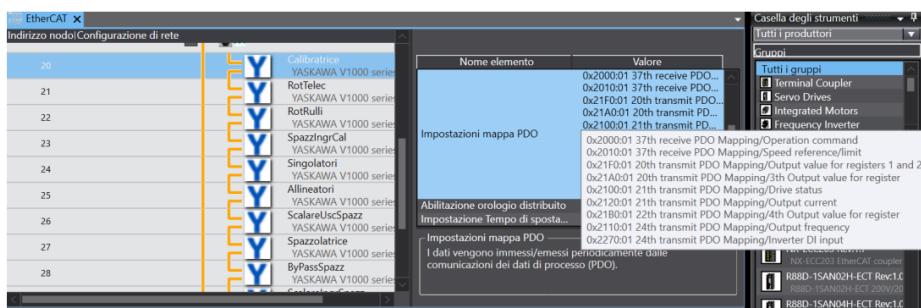
RF monitoring: Il WLC gestisce ogni AP in modo da scansionare i canali per monitorare l'utilizzo delle radiofrequenze. Ascoltando un canale, il WLC può raccogliere in remoto informazioni sulle interferenze RF, sul rumore, sui segnali degli AP vicini e sui segnali degli AP non autorizzati o dei client ad hoc.

Security management: Il WLC può autenticare i client tramite un servizio centrale e può richiedere ai client wireless di ottenere un indirizzo IP da un server DHCP affidabile prima di consentire loro di associarsi e accedere alla WLAN.

Wireless intrusion protection system: Sfruttando la sua posizione centrale, il WLC può monitorare i dati dei client per rilevare e prevenire attività dannose.

Unitec - Operational technology

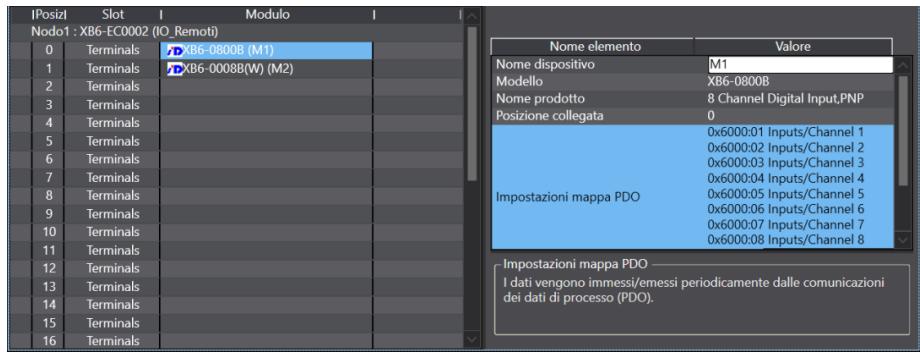
Esempi applicativi



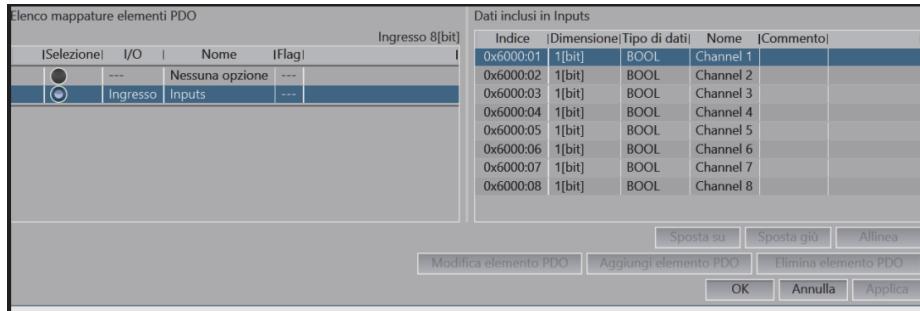
Nodi (in questo caso etherCat) con i rispettivi PDO, i messaggi con il mapping.

Nodo21	YASKAWA V1000 series						
	31th receive PDO Mapping_Operation command_2000_01	W	UINT	NV_21_Commandi		Variabili globali	
	31th receive PDO Mapping_Speed reference/motor_2100_01	W	UINT	NV_21_Velocita		Variabili globali	
	20th transmit PDO Mapping_Output value for registers_21F0_01	R	UINT	NV_21_OverCurre		Variabili globali	
	20th transmit PDO Mapping_3th Output value for register_21A0_01	R	UINT	NV_21_Hbb		Variabili globali	
	21th transmit PDO Mapping_Drive status_2100_01	R	UINT	NV_21_Stato		Variabili globali	
	21th transmit PDO Mapping_Output current_2120_01	R	UINT	NV_21_Corrente		Variabili globali	
	22th transmit PDO Mapping_4th Output value for register_21B0_01	R	UINT	NV_21_CodAll		Variabili globali	
	24th transmit PDO Mapping_Output frequency_2110_01	R	UINT	NV_21_FreqAct		Variabili globali	
	24th transmit PDO Mapping_Inverter DI input_2270_01	R	UINT	NV_21_Dinput		Variabili globali	

Mappa I/O (in questo caso di un inverter) che mostra i moduli I/O di un nodo a sinistra (parte hardware) e le relative variabili con il tipo a destra.



L'immagine mostra un elenco di moduli I/O remoti in un sistema di controllo basato su EtherCAT. L'elenco fornisce informazioni utili per la configurazione e la manutenzione del sistema di controllo; ad esempio, le impostazioni di mappatura PDO possono essere utilizzate per specificare come i dati vengono scambiati tra i moduli I/O remoti e il controller.



L'immagine mostra un elenco di input di dati in un sistema di controllo basato su EtherCAT. L'elenco fornisce informazioni utili per la configurazione e la manutenzione del sistema di controllo.

Processo produttivo

Insieme di lavorazioni (filiera o supply chain) che trasformano una materia prima in un prodotto finito.

I processi produttivi possono essere su commessa (fatto solo quando richiesto), a

lotti o intermittenti oppure continuo.

Nei processi produttivi l'automazione industriale ha un ruolo importante, permette il controllo di flussi di energia, materiali e informazioni senza l'aiuto dell'uomo.

OT

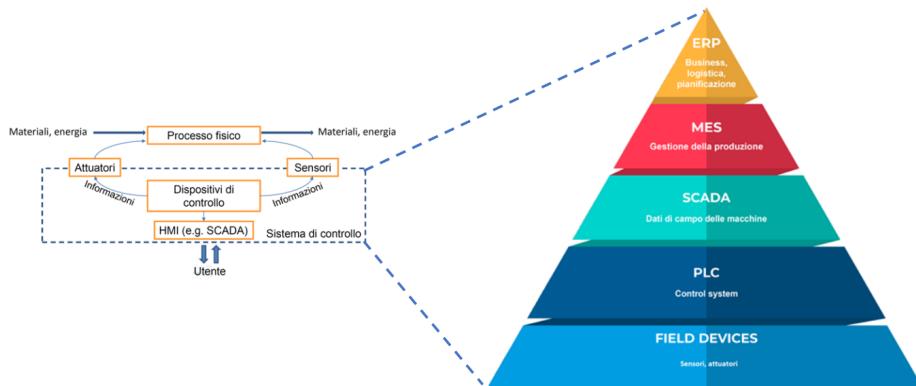
Operation Technology, tecnologia che gestisce i processi fisici nel mondo reale.

La differenza con l'IT è che qui si cerca un determinismo temporale maggiore e OT è tutto quello che riguarda gli ambienti industriali.

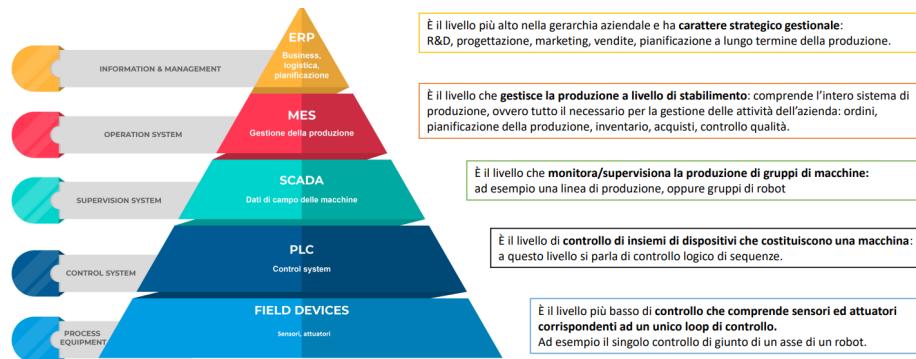
Computer Integrated Manufacturing (CIM)

Modello teorico che rappresenta l'integrazione tra l'informatica e la produzione (sistemi di automazione).

Il modello CIM è gerarchico e prevede il coordinamento fra i livelli.



Nel dettaglio:



Nel modello le informazioni salgono verso i livelli superiori, diminuendo piano piano; i comandi fanno il contrario, scendono e aumentano visto che la complessità

aumenta.

Nella piramide esistono tre tipi di reti:

- rete di campo: mette in comunicazione il PLC con i dispositivi di campo.
- rete di controllo: comunicazione fra macchine con pacchetti strutturati e vincoli temporali minori;
- rete aziendale: grossi dati e vincoli temporali quasi inesistenti.

Controllore logico

Un dispositivo che mette in relazione delle variabili (logiche) in ingresso con variabili (logiche) di uscita, mediante un insieme di algoritmi combinatori e/o sequenziali.

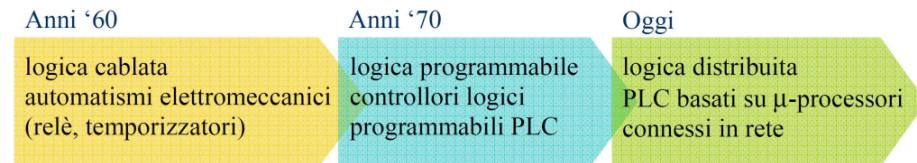
Sono statici, se le uscite del sistema ad un certo istante dipendono dal valore degli ingressi allo stesso istante (le equazioni che legano ingressi e uscite sono statiche).

Sono dinamici, se le uscite correnti dipendono anche dai valori passati degli ingressi (equazioni di tipo sequenziale).

Era implementato tramite i relè ma era una tecnologia troppo complessa e poco integrabile.

Per questo è nato il PLC, un controllore logico programmabile che usa una CPU e ha una memoria.

La differenza del PLC da un normale PC è che il primo utilizza un Real Time Operating System, OS mirato al real time, che evita deadlock e utilizza il multitasking pre-emptive con interruzioni in caso di errori; inoltre è un sistema deterministico grazie ai task che vediamo dopo



Oggi si parla anche di Soft-PLC, emulazioni via software del controllore senza una parte hardware.

Il PLC ha un bus con architettura di von neumann, fondamentale per la modularità. Il bus connette tutte le unità funzionali (memoria, processore e moduli I/O) tra di loro e permette un flusso continuo di informazioni da e verso la CPU. E' un insieme di linee elettriche suddivise per funzioni (linee per i dati, linee per gli indirizzi, linee per l'alimentazione). Generalmente, i bus dei PLC sono di tipo proprietario..

Nel PLC le fasi di acquisizione ingressi, elaborazione e aggiornamento uscite sono da considerarsi hard real-time, tutte le altre sono soft real-time.

Il PLC è deterministico grazie ai task:

Tipo	Descrizione
Primary periodic task	<ul style="list-style-type: none"> • E' il task a priorità più alta. • E' un task periodico, per cui viene eseguito ad intervalli fissi regolari. • E' il task con il minore periodo di esecuzione, che coincide con il periodo del ciclo EtherCAT.
Task periodico	Viene eseguito secondo un periodo fissato, negli intervalli di inattività del primary periodic task.
Task a evento	Viene eseguito al verificarsi di una specifica condizione

Determinismo temporale

Una rete si dice deterministica se è possibile calcolare un tempo massimo (deadline) entro il quale l'informazione inviata da un nodo arriva a destinazione. Il comportamento si dice quindi predicable.

Per rispettare i vincoli si usano algoritmi di scheduling, le principali famiglie di algoritmi sono:

- FIFO queueing: politiche di First In, First Out
- Priority queueing: politiche che gestiscono un ordinamento di priorità dei messaggi nei buffer
- Fair queueing: politiche di Round Robin, in cui si dedica ad ogni processo un intervallo temporale (quanto)

Un sistema Real Time è un sistema la cui correttezza logica non dipende solo dal suo output ma anche dall'istante temporale in cui viene reso disponibile, e deve avere queste caratteristiche:

- assegnamento priorità
- multitasking pre-emptive,
- evitare deadlock

Program Organization Unit

Lo standard IEC61131-3 definisce il POU: è un'unità elementare del programma utente all'interno del PLC. I tipi di POU sono tre:

- Funzioni (FUN): come quelle di C;
- Function Block (FB): simile alle FUN ma quando si vogliono usarli si crea un'istanza con memoria dello stato;

Funzioni (FUN):

- Non necessitano di istanza
 - Sono più semplici da utilizzare
 - Non occupano memoria dati
 - Possono essere utilizzati illimitatamente
 - Necessitano di un ingresso EN
 - Hanno sempre una variabile risultato

Function Block (FB)

- Necessitano di istanza per poter essere utilizzate nel programma
 - Occupano memoria dati
 - Il numero di istanze è limitato dalla memoria dati disponibile
 - Si usano quando è necessario memorizzare valori tra un ciclo e l'altro, o quando contengono FB nel codice (ad esempio timer o FB utente)

- Programmi (PRO): insieme di FUN e FB ed impossibile da evocare da un altro POU.

Poi ci sono le variabili che sono uguali a quelle di altri linguaggi, possono essere:

- Globali e possono essere pubblicate con tag e visibili ovunque.
 - Di sistema: predefinite, usate per monitorare lo stato di determinate funzionalità del dispositivo.

Sensori e attuatori

I primi sono l'input i secondi l'output.

Da slide 57 a 67, QUI

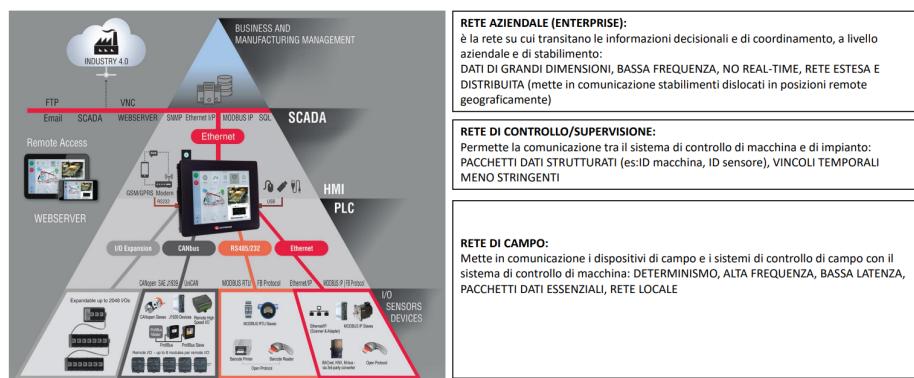
Gli inverter variano la frequenza del segnale elettrico e per esempio controllare la velocità del motore.

Gli attuatori pneumatici possono essere le elettrovalvola che tramite comando elettrico si attiva un cilindro che soffia un getto d'aria.

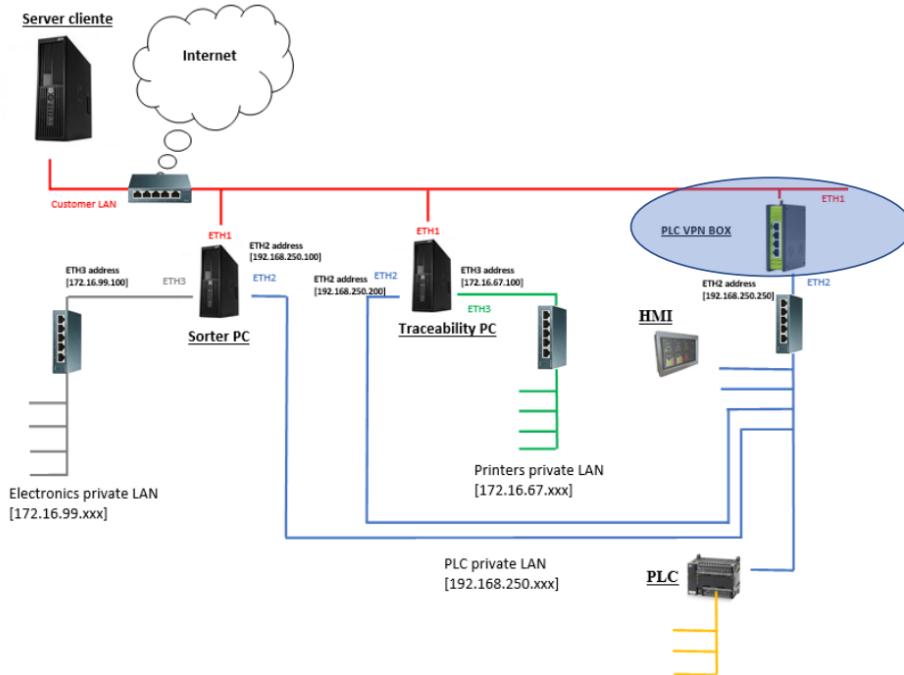
Moduli I/O

Permettono l'interfacciamento tra PLC con il sensore/attuatore

Le reti



Rete completa con tutti i tipi:



Giallo = rete di campo
= rete aziendale

Evidenziato = IoT gateway

Blu = rete di supervisione

Rosso

Fieldbus o bus di campo

La rete di campo, o bus di campo/fieldbus, è una LAN speciale con architettura multipunto tra livello 1 e livello 2.

Tutti coloro connessi a questa rete ricevono dati tramite un canale digitale, seriale e bidirezionale.

Esistono diversi dispositivi di interconnessione:

- hub: amplifica il segnale in tutte le porte
- switch: decide dove mandare i dati, è smart
- bridge (ponte): connette due reti che usano lo stesso protocollo ma che hanno layer differenti al livello inferiore [Modbus RS485 / Ethernet TCP-IP bridge]
- router (instradatore): connette due reti dello stesso tipo [Ethernet TCP-IP router]
- gateway (portale): connette due reti di tipo diverso [Ethernet / Modbus gateway]

Per evitare o limitare i fenomeni di collisione si rende necessario un protocollo

che regola l'accesso al mezzo trasmissivo (Medium Access Control o MAC), i criteri per accedere al mezzo sono:

1. quale dispositivo concede l'accesso, esempio:
 - Controllo centralizzato: Master Slave Un solo nodo della rete (MASTER) gestisce chi e quando può accedervi: gli altri nodi (SLAVE) sono in costante ricezione. Nel messaggio ricevuto dal slave è codificata l'informazione che permette o meno allo slave stesso di rispondere. Possono essere gestiti dal master interrogazioni cicliche agli slave per verificare eventuali dati da comunicare (polling)
 - Controllo distribuito:
 1. CSMA (Carrier Sense Multiple Access): protocollo MAC probabilistico in cui un nodo verifica che il canale sia libero prima di trasmettere su un canale condiviso come un bus elettrico.
 - Il Carrier Sense Multiple Access / Collision Detection (CSMA/CD) introduce la variante dell'ascolto durante la trasmissione. In caso di collisione, la trasmissione viene interrotta dopo un tempo prefissato (intervallo di jamming).
 - Il Carrier Sense Multiple Access / Collision Resolution (CSMA/CR) attraverso una definizione di priorità degli indirizzi, eventuali collisioni sono rilevate e risolte in favore del messaggio a priorità superiore, gestendo carichi maggiori della rete.
 - 2. Token Ring Sistema ad assenza di collisioni: Token Bus/Ring (IEEE 802.4/.5)
 - il token circola continuamente (-> stesso tempo deterministico tra due successive interrogazioni del canale da parte di ogni host)
 - un nodo trasmette quando è in possesso dell'abilitazione data dal token "originale": lo modifica e rispedisce in circolo assieme al frame del dato (e con un host destinatario)
 - 2. Con quale logica si concede l'accesso:
 - Assegnazione statica: per ogni connessione si usa un canale assegnato a priori in modo deterministico (ad esempio a slot temporali)
 - Assegnazione dinamica: la stazione impegna il mezzo solo quando ne ha bisogno (uso statistico)

Ogni bus di campo può avere protocolli diversi

Possiamo catalogare le reti industriali in 3 categorie/classi:

- Categoria A: basata su TCP/IP: encapsulamento pacchetti ad alto livello e inglobati in un pacchetto TCP o UDP.

A livello hardware si utilizza l'Ethernet standard.

Per garantire un livello di determinismo accettabile, il controllo sul processo di comunicazione viene effettuato dalle funzioni di alto livello. «Best Effort».

Esempi di protocolli: Modbus e EtherNet/IP.

- Categoria B: Ethernet MAC : utilizza Ethernet a livello fisico e MAC incapsula direttamente i dati, senza TCP/IP.

Riduzione overhead a vantaggio del determinismo temporale.

Può utilizzare TCP/IP per configurazione o dati non realtime.

Esempi di protocolli: Powerlink e Profinet.

- Categoria C: Ethernet modificata : modifica del livello 2 per incapsulare i dati in fasce temporali definite.

Si utilizza ASIC o FPGA per interfacce hardware.

Esempi di protocolli: EtherCAT e Sercos III.

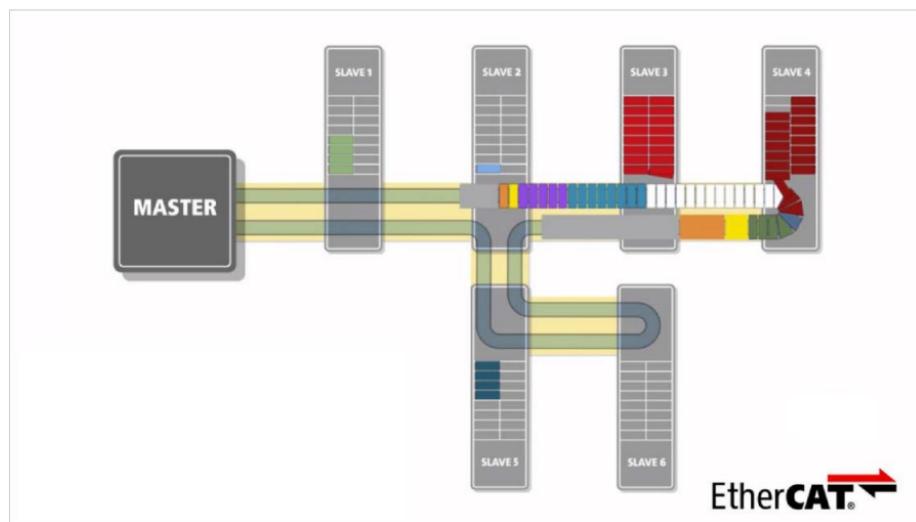
I cavi usati possono essere STP (schermati fuori, dentro e ogni coppia twisted) o UTP (schermati solo fuori) con plug RJ45 O M12.

Ethercat

Ethernet for Control Automation Technology, è una protocollo di rete industriale, basato su Ethernet modificato (Categoria C).

L'architettura è di tipo Master – Slave con velocità di trasmissione: 2 x 100 Mbit/s (Fast Ethernet, Full-Duplex).

Cavo formato da coppia intrecciata e schermata (STP) con 2 coppie di fili e connettori RJ45 o M12.



Il telegramma attraversa tutti i nodi e lettura/scrittura avviene al volo (on the fly), questo perché i dispositivi EtherCAT slave integrano un EtherCAT Slave Controller (ESC) in grado di processare i frame in modo puramente hardware e usando la tecnica on the fly.

Gli ESC sono realizzati tramite FPGA, ASIC; consentendo all'architettura di essere Real Time fino al livello di I/O.

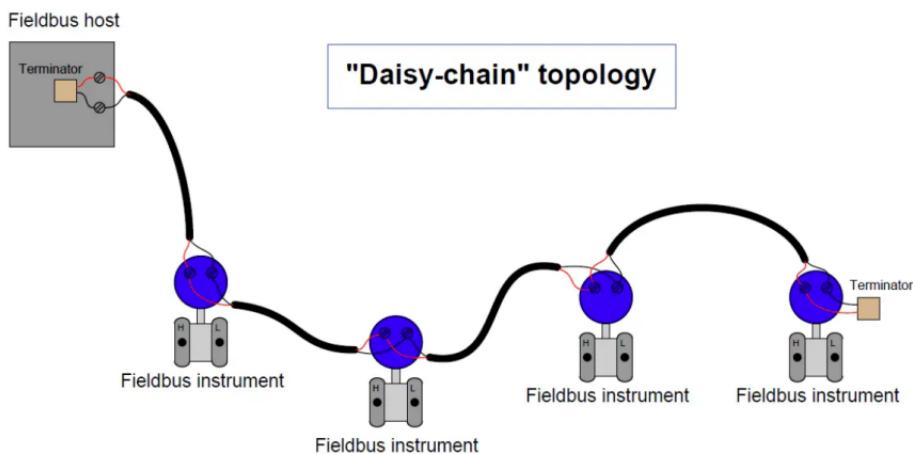
I dati trasmessi e scritti on the fly si chiamano PDO (Process Data Object) che hanno una struttura definita in modo che siano interpretati istantaneamente.

EtherCAT per sincronizzare i vari nodi si basa sull'approccio dei distributed clock (DC), con un alto grado di tolleranza nei confronti del jitter di comunicazione.

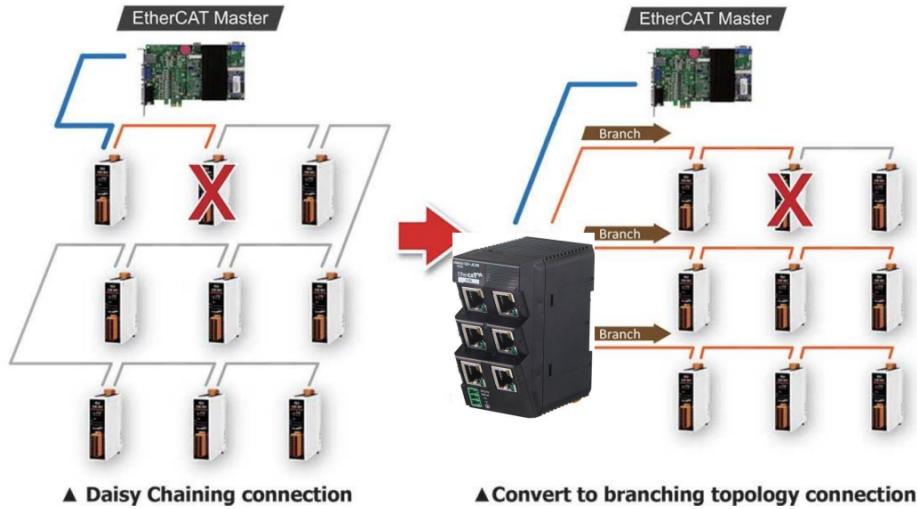
La calibrazione dei clock avviene via hardware e il timestamp del master è distribuito ciclicamente a tutti gli slave.

Con questo meccanismo, i clock degli slave possono essere sincronizzati precisamente a quello del clock di riferimento. Il jitter di sincronizzazione risultante è inferiore a $1\mu\text{s}$. Poiché il riferimento temporale inviato dal reference clock giunge agli altri slave con un certo ritardo di propagazione, quest'ultimo deve essere misurato e compensato per ogni slave in modo da garantire sincronismo e simultaneità.

Le topologie possibili sono tante ma la più usata è la Daisy-chain (a margherita):



Il problema è, che essendo a catena, se uno slave cade quelli successivi non sono raggiungibili, per questo usiamo gli switch (detto in questo caso Junction Slave):



Ricordiamo che lo switch essendo sulla rete EtherCAT è uno slave

I moderni sistemi di comunicazione non solo realizzano il trasferimento deterministico dei dati di controllo, ma consentono anche lo scambio di dati critici per la sicurezza sullo stesso mezzo fisico. EtherCAT utilizza a questo scopo il protocollo Safety over EtherCAT (FSoE = Fail Safe over EtherCAT) e rende quindi possibile condividere, in un unico sistema di comunicazione i dati di controllo e quelli di sicurezza.

Ethernet/IP

EtherNet/IP (**Ethernet Industrial Protocol**) è un protocollo di rete industriale che utilizza il Common Industrial Protocol (CIP) su Ethernet standard (categoria A).

Di seguito le principali caratteristiche:

- Facile da implementare
- Compatibile con dispositivi standard (switch Ethernet, ...)
- Utilizzo dei TAG
- Protocollo *non completamente real-time*

EtherNet/IP utilizza:

- porta TCP per *messaggistica esplicita* (messaggistica in cui l'invio di dati è in risposta ad una specifica richiesta)
- porta UDP per *implicit messaging* - comunicazioni di sistema inviate da posizioni di memoria preimpostate ad un certo intervallo di tempo prestabilito.

L'utilizzo di TAG permette di accedere ai PLC Data senza utilizzare indirizzi.

CIP è un protocollo indipendente e object-oriented che utilizza un modello di comunicazione master/slave, orientato all'interoperabilità fra sistemi differenti.

Ogni oggetto CIP ha attributi (i dati), servizi (comandi), connessioni e comportamenti.

Scada

Un sistema SCADA (Supervisory Control And Data Acquisition) è un insieme di componenti software e hardware che, in maniera locale o remota, consentono di acquisire dati su un processo in esecuzione o effettuare operazioni di supervisione su di esso. Lo scada è composto da:

- Database del processo;
- Driver di comunicazione;
- HMI (interfaccia operatore);
- Gestione allarmi/ricette.

Questi sistemi in genere consentono a un operatore di interfacciarsi con il processo tramite una HMI sfruttando i sistemi di controllo : tali dispositivi sono connessi via rete a uno o più dispositivi di supervisione

I dispositivi di controllo raccolgono e storizzano i dati, li presentano all'operatore tramite HMI e/o informazioni riassuntive, e forniscono un supporto alla decisione per la gestione dell'impianto

Spesso lo SCADA presenta i dati all'operatore tramite una HMI, che in genere comprende:

- Quadri sinottici, con elementi statici e dinamici (a seconda che l'aspetto grafico vari in base al dato)
- Pannelli di controllo, consentono all'operatore di interagire con l'impianto in maniera intuitiva (manopole, pulsanti, slider...)

MES

Manufacturing Execution System sistema che acquisisce e distribuisce infor. per ottimizzare le attività produttive.

Le sue funzioni principali:

- gestione ordini;
- gestione risorse;
- gestione dipendenti
- reportistica

Reti di controllo/supervisione

Per mettere in comunicazione SCADA e le reti di supervisione si usano i gateway, dei middleware che stanno fra i due livelli.

Alcuni gateway possono essere:

Protocolli proprietari:

- Ethernet:
 - Omron FINS protocol (**F**actory **I**nterface **N**etwork **S**ervice)
 - Siemens S7 Protocol
- Seriali:
 - Omron Hostlink

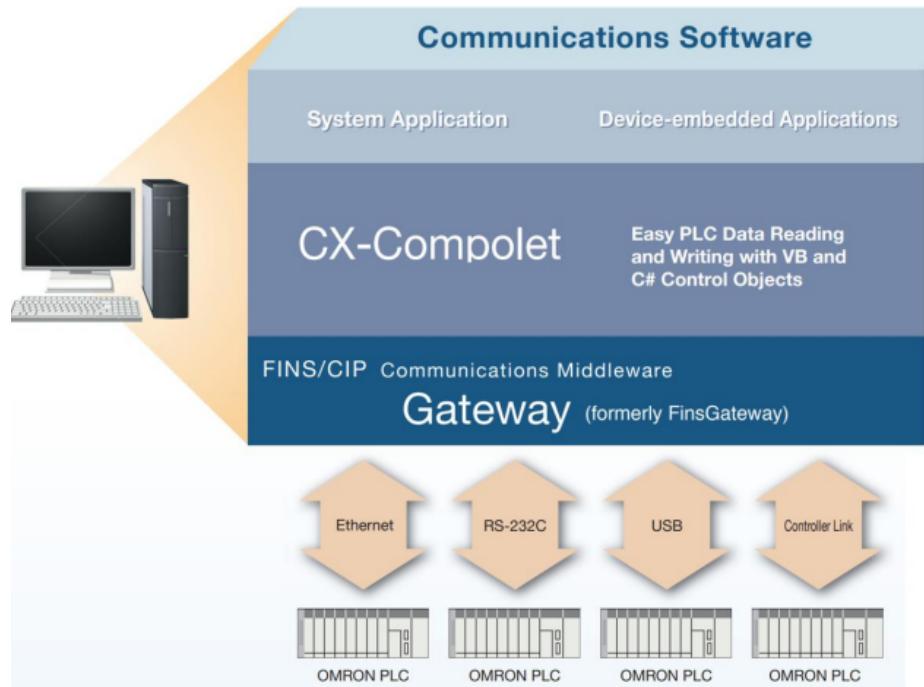
Protocolli interoperabili:

- MODBUS
- CIP (**C**ommon **I**ndustrial **P**rotocol)

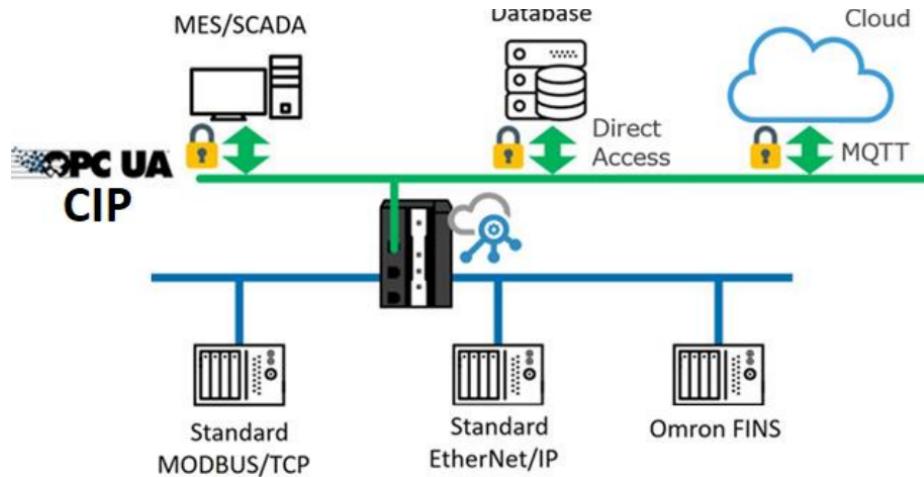
Interoperabili cioè utilizzabili senza avere tutti i dispositivi della stessa azienda.

Esistono diverse soluzioni di implementazione:

- Soluzione A:

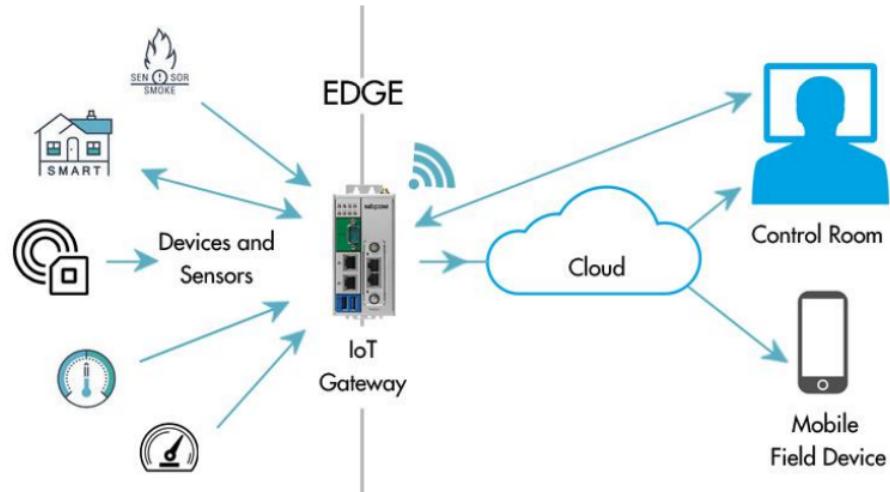


- Soluzione B: con il PLC che comunica direttamente con i livelli superiori



- Soluzione C: con l'utilizzo di un IOT Gateway, si può usare quando abbiamo 1 o + impianti con PLC di diversi vendor e sono in grado di trasferirli a sistemi MES/ERP eterogenei che possono trovarsi in siti/country differenti.

Supportano il cloud che viene usato per connessioni tramite VPN.



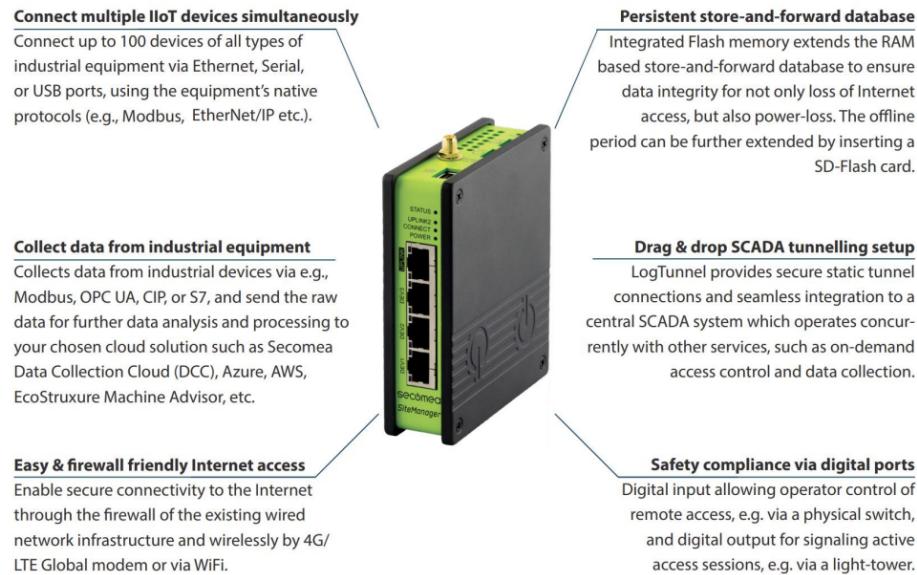
Protocolli e termini usati spiegati sotto

IIoT

L'IoT ma applicato a livello industriale, è una sottocategoria che rappresenta l'anello di congiunzione fra IT e OT.

IoT Gateway

Dispositivi che implementano da un lato i protocolli di campo/controllo, dall'altra protocolli di alto livello che permettono l'interfacciamento con diverse nature come il cloud.



OPC

Open Platform Communication, standard object oriented che fornisce le specifiche di comunicazione di dati real-time tra dispositivi di diversa provenienza manifatturiera

Utilizza un'architettura Client-Server, che facilita l'interoperabilità.

I due programmi che seguono questa architettura sono:

- OPC-Client: monitora le variabili, chiamate tag/item, scelte. Il client dovrà impostare le variabili che si intendono monitorare e con quale frequenza, update rate, aggiornare i valori.
- OPC-server: eseguibile che parte automaticamente durante la connessione tra client e PLC. Grazie al Gateway fornisce al client tutte le variabili e i valori relativi presi dal PLC.

La specifica OPC Data Access descrive l'interfaccia di accesso ai dati ed è utilizzata per leggere e scrivere dati real-time.

OPC UA

Erede del precedente, che incrementa l'indipendenza dalla piattaforma, consentendo l'integrazione facile in Windows, Linux, Mac, Android e altre piattaforme.

MQTT

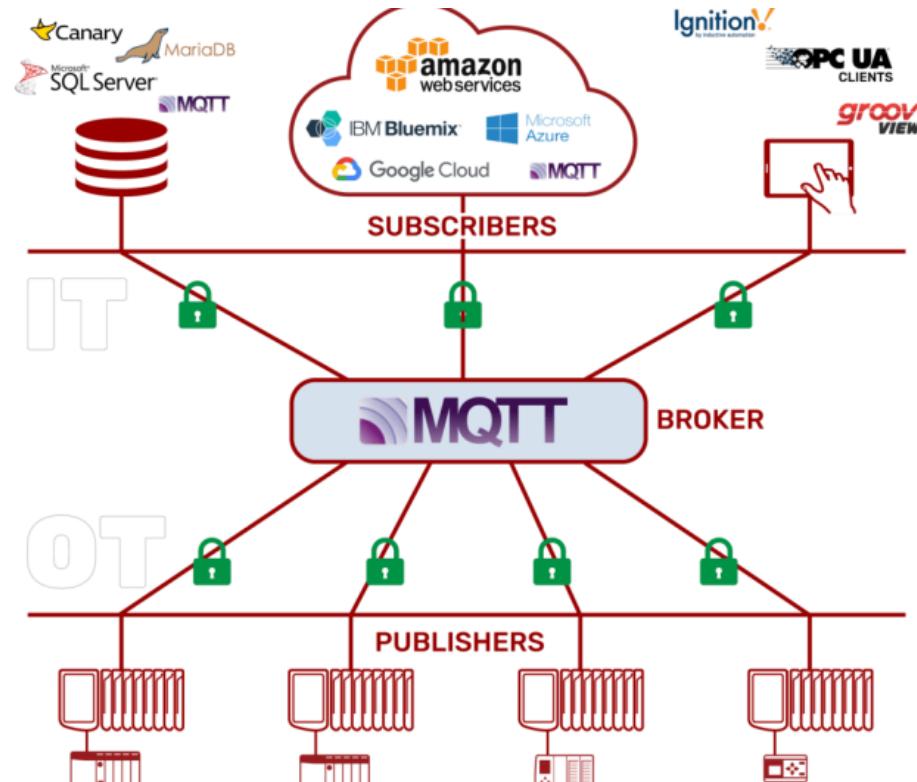
Message Queuing Telemetry Transport Protocol, protocollo di messaggistica leggero, progettato per la telemetria quindi M2M (machine to machine) in

contesti con risorse limitate.

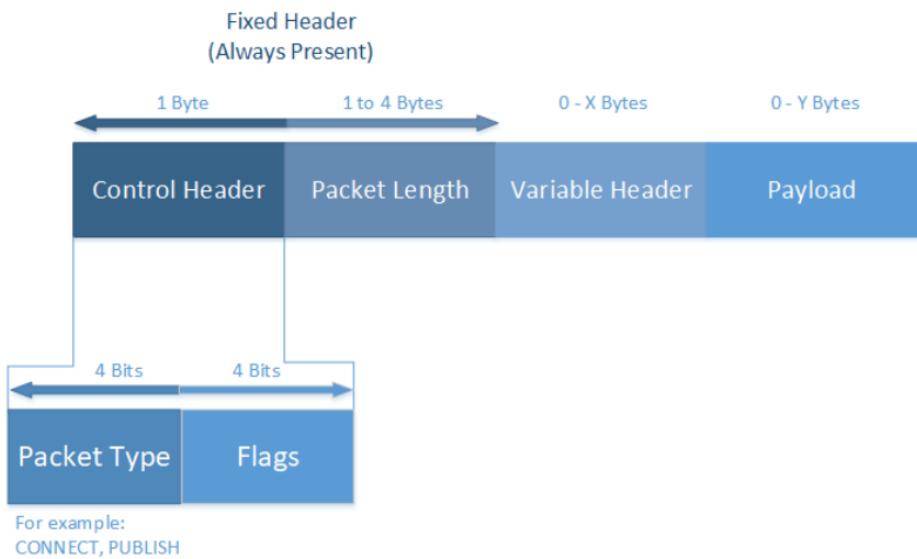
MQTT 3.1 basato su TCP e MQTT-SN su UDP.

Gli attori sono:

1. Publisher (client) : producono i dati e li inviano ai broker
2. Subscriber (client) : si sottoscrivono ad un topic di interesse e ricevono notifiche
3. Broker : filtrano dati sulla base dei topic e li distribuiscono in rete



Il messaggio è così strutturato:



Con il packet type che indica il tipo di messaggio e il payload che può contenere qualsiasi tipo di dato.

ERP

Enterprise Resource Planning, software gestionali in grado di gestire i processi di business di un'azienda.