APPUNTI RETI DI TELECOMUNICAZIONE

Internet e IP

Architettura di Internet

L'architettura di Internet è organizzata in strati:

1. Applicazioni (e-mail, ftp, telnet, www)
2. TCP/UDP (Strato di Trasporto)
3. IP (Strato di Rete)
4. Collegamento dati (es. Ethernet, X25, Aloha)
5. Fisico Questa struttura corrisponde al modello OSI semplificato, con IP che opera al livello di rete (strato 3).

Internet Protocol (IP) - RFC 791

Caratteristiche principali:

- Funziona a commutazione di pacchetto in modalità **connectionless**
- Gestisce la trasmissione di datagrammi da sorgente a destinazione attraverso reti eterogenee
- Identifica host e router tramite **indirizzi IP di 32 bit**
- Frammenta e riassembla i datagrammi quando necessario
- Offre un servizio **best effort** senza garanzie di affidabilità o controllo di flusso

Struttura degli indirizzi IP

- Lunghezza fissa di 32 bit
- Rappresentazione in formato **dotted decimal** (es. 137.204.212.1)
- Numero massimo teorico di indirizzi: **2^32** = 4.294.967.296
- Assegnati dalla **IANA** (Internet Assigned Numbers Authority)

Formato del pacchetto IP

Il pacchetto IP è composto da:

1. **Header** (intestazione)
2. **Payload** (dati utente)

Campi principali dell'header IP:

- **Prima riga (identificazione)**
    - **Version (4 bit)**: versione del protocollo IP (attualmente 4)
    - **IHL (Internet Header Length) (4 bit)**: lunghezza dell'intestazione in parole da 32 bit
    - **Type of Service (8 bit)**: indica il tipo di servizio richiesto (continua ad essere un problema non risolto infatti molti router ignoravano questo campo o lo trattavano in modi diversi, portando a un'applicazione inconsistente)
    - **Total Length (16 bit)**: lunghezza totale del datagramma in byte (fino a 65,535 byte)
- **Seconda riga (controllo di dimensione e segmentazione del pacchetto)**

    - **Identification (16 bit)**: identificatore univoco del datagramma (dato che un pacchetto potrebbe essere diviso in rete)
    - **Flags (3 bit)**: controllo della frammentazione (spiegati sotto)
    - **Fragment Offset (13 bit)**: posizione del frammento nel datagramma originale (indica la posizione del primo byte rispetto all'inizio)

- **Terza riga (controllo dell'errore)**

    - **Time to Live (TTL) (8 bit)**: numero massimo di hop consentiti (a livello funzionale potrebbe anche non esistere più perché la rete è molto efficiente ed i pacchetti non girano più a caso per essa, oggi vengono usati come strumenti di controllo)
    - **Protocol (8 bit)**: indica il protocollo di livello superiore
    - **Header Checksum (16 bit)**: per il controllo degli errori nell'intestazione

- **Quarta riga**

    - **Source Address (32 bit)**: indirizzo IP sorgente

- **Quinta riga**

    - **Destination Address (32 bit)**: indirizzo IP destinazione

- **Sesta riga opzionale (quasi mai usata)**

    - **Options (variabile)**: opzioni aggiuntive
    - **Padding**: bit di riempimento per allineare l'intestazione a 32 bit

Frammentazione dei datagrammi

Necessaria quando il datagramma è troppo grande per essere trasmesso su una rete, ciò può accadere perchè si lavora su reti eterogenee con infrastruttura fisica differente. Può essere effettuata da qualsiasi apparato di rete con protocollo IP, i frammenti vengono riassemblati solo dal terminale ricevente. Il campo "Fragment Offset" indica la posizione del frammento nel datagramma originale ed i campi "Identification"e "Flags" sono usati per gestire la frammentazione

Flags per la frammentazione:

- Bit 0: sempre 0
- Bit 1 (DF - Don't Fragment):
    - 0 = si può frammentare
    - 1 = non si può frammentare (nel caso fosse a 1 e fosse necessario frammentarlo lo distruggo)
- Bit 2 (MF - More Fragments):
    - 0 = ultimo frammento (aiuta a riordimare i paccheti in arrivo, è tecnicamente superfluo ma ci risparmia il calcolo di vedere quanto era lungo)
    - 1 = frammento intermedio

Calcolo del Fragment Offset: Il datagramma è diviso in blocchi di 8 byte (64 bit) l'offset è calcolato in unità di 8 byte dall'inizio del datagramma originale (non ho bisogno di mappare tutti i bit ma posso mapparli a blocchi di 8 byte per ridurre a 13 il numero di bit necessari a tenerne traccia, ciò implica che la frammentazione non potrà mai scendere sotto i 64 bit perché non sarei più in grado di ricomporre il pacchetto)

Time to Live (TTL): Imposta un limite al numero di hop che un pacchetto può attraversare,il valore iniziale tipicamente è 64 (massimo 255) decrementato di 1 ad ogni hop quando raggiunge 0, il pacchetto viene scartato

Riassemblaggio dei datagrammi: I frammenti possono arrivare fuori sequenza o con tempi diversi. Il riassemblaggio avviene solo al terminale di destinazione. Utilizza i campi **Identification**, **Flags** e **Fragment** Offset per ricostruire correttamente il datagramma originale

Problematiche dell'IP

Mobilità

- **Indirizzi riferiti alla rete di appartenenza**: Gli indirizzi IP sono legati alla rete a cui appartengono. Se un host viene spostato in un'altra rete, il suo indirizzo IP deve cambiare.
- **Configurazione automatica con DHCP**: Il Dynamic Host Configuration Protocol (DHCP) permette la configurazione automatica degli indirizzi IP, facilitando la gestione degli indirizzi in reti dinamiche.
- **Mobile IP**: Mobile IP è una tecnologia che permette agli utenti di spostarsi tra diverse reti mantenendo lo stesso indirizzo IP, garantendo la continuità delle sessioni di rete.

Sicurezza

- **Scarsa protezione del datagramma IP**: L'intestazione dei datagrammi IP è in chiaro, rendendo vulnerabili i dati in transito.
- **IPSec**: Il protocollo IPSec può essere applicato anche a IPv4 per migliorare la sicurezza delle comunicazioni, fornendo autenticazione e cifratura dei dati.

Dimensioni delle reti prefissate: Il subnetting e il Classless Inter-Domain Routing (CIDR) sono tecniche utilizzate per suddividere le reti in sottoreti più piccole e per ottimizzare l'uso degli indirizzi IP.

Esaurimento degli indirizzi IPv4: A causa dell'enorme diffusione di Internet, il numero di indirizzi IPv4 disponibili è insufficiente. Le reti IP private e il Network Address Translation (NAT) sono soluzioni temporanee per mitigare questo problema.

IPv6

Supportare molti miliardi di host: IPv6 è stato progettato per supportare un numero molto maggiore di indirizzi rispetto a IPv4.

Semplificare il routing: IPv6 mira a rendere il routing più efficiente e scalabile.

Offrire meccanismi di sicurezza: IPv6 include nativamente il supporto per IPSec, migliorando la sicurezza delle comunicazioni.

Offrire qualità di servizio (QoS): IPv6 fornisce meccanismi per garantire la qualità del servizio, essenziale per applicazioni multimediali.

Gestire multicast e broadcast: IPv6 migliora la gestione del multicast e del broadcast rispetto a IPv4.

Consentire la mobilità: IPv6 supporta la mobilità degli host, permettendo agli utenti di spostarsi tra diverse reti senza cambiare indirizzo IP.

Evoluzione futura e compatibilità: IPv6 è progettato per consentire future evoluzioni e garantire la compatibilità con le versioni precedenti.

Istradamento IP

Instradamento a pacchetto: Internet utilizza la commutazione a pacchetto per trasmettere dati. Esistono più percorsi per raggiungere una destinazione. Il **routing** (instradamento) avviene pacchetto per pacchetto, e i router decidono quale percorso seguire.

Componenti della Rete

Network IP: Internet è costituita da tante reti isolate (Network IP). Ogni network IP è un'isola che contiene host (calcolatori terminali). Questi host devono essere necessariamente in grado di comunicare tra di loro; il caso più estremo è un solo host (calcolatore) che parla con se stesso.

Router: Detti anche Gateway, collegano le isole e permettono la comunicazione tra reti diverse. Funzionano fino al livello 3 del modello OSI. In molti casi, il trasferimento di dati compie un percorso che passa per più gateway e probabilmente anche per più network. Due router connessi che a loro volta connettono altrettante Network IP possono essere visti come una Network IP di soli due calcolatori, questa visione semplifica molto il lavoro di astrazione poicè ci permette di vedere solo Network IP connesse tutte per gatway condivisi nei punti di "contatto".

Tecnologie di Implementazione

Wi-Fi: Wireless a breve distanza. (dal punto di vista dell'ip è un tipo di comunicazione 1a1 che passa per il centro stella e viene poi smistata)

ADSL/xDSL: Connessioni via cavo a media distanza.

Ethernet: Connessioni cablate locali.

GPRS/EDGE/LTE: Connessioni radio fornite da operatori pubblici.

Netmask: Funzionamento e Rappresentazione

L'indirizzo IP, usato per raggiungere una specifica network al di là dell'implementazione su cui lavora, è composto da due parti:

- **Net ID**: Identifica la rete (network IP), parte di sinistra dell'indirizzo.
- **Host ID**: Identifica l'host all'interno della rete (singolo calcolatore), parte destra dell'indirizzo.

La **Netmask** è un valore numerico che serve a separare la parte di **Net ID** dalla parte di **Host ID** in un indirizzo IP. Questa separazione permette di identificare la rete di appartenenza e gli host al suo interno.

Come funziona la Netmask: La Netmask è un indirizzo IP a 32 bit. Non viene trasportata nel datagramma, ma è parte della tabella di routing del nodo. Inizialmente, la divisione tra Net-ID e Host-ID era assoluta (Classfull), mentre successivamente si è passati a un approccio più flessibile (Classless).

Ogni bit della Netmask può essere:

- **1**: Indica che il bit corrispondente dell'indirizzo IP appartiene al **Net ID**.

- **0**: Indica che il bit corrispondente appartiene all'**Host ID**.

Insieme all'indirizzo IP, la Netmask determina:

- Quanti indirizzi sono disponibili in una rete.
- Quale intervallo di indirizzi appartiene a una specifica rete.

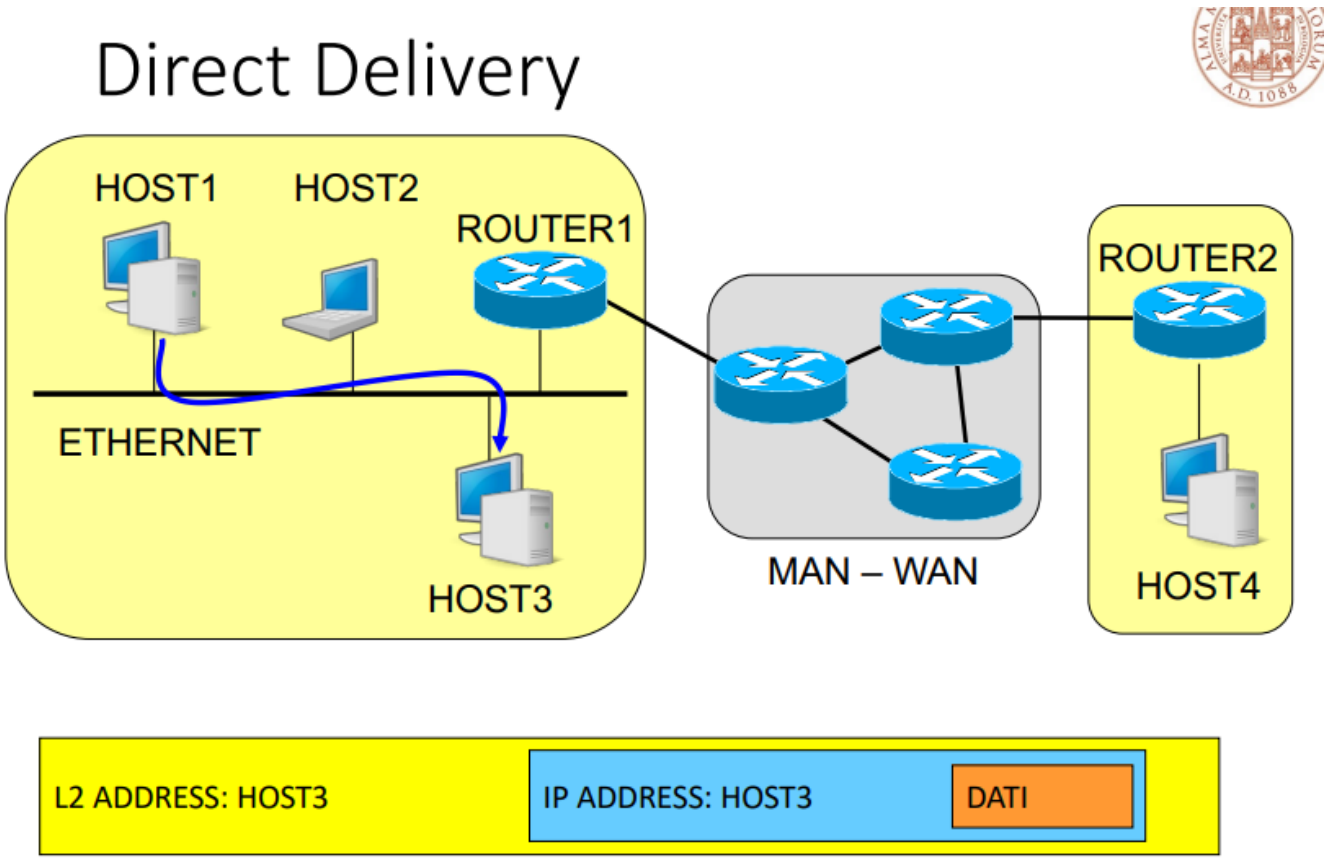
Rappresentazione della Netmask

1. **Formato decimale puntato**:
   - I 32 bit della Netmask sono divisi in 4 gruppi da 8 bit (ottetti) separati da punti, convertiti in notazione decimale.
   - Esempio: **255.255.255.0** (24 bit a 1 e 8 bit a 0).
2. **Notazione CIDR (Classless Inter-Domain Routing)**:
   - La Netmask è indicata con uno slash seguito dal numero di bit impostati a **1**.
   - Esempio: **/24** corrisponde a una Netmask di **255.255.255.0**.
   Utilizzo pratico della Netmask

- Identificare le sottoreti in un'organizzazione più ampia.
- Limitare gli indirizzi assegnabili all'interno di una rete per motivi di sicurezza o di ottimizzazione delle risorse.
- Supportare il routing attraverso reti diverse, consentendo ai router di riconoscere la rete di appartenenza di un pacchetto.

Routing e Instradamento

Direct Delivery: Quando l'IP sorgente e destinatario sono sulla stessa rete. Supponendo di essere in collegamento Ethernet in un network IP, inseriremo l'IP in un indirizzo di livello 2 contenente il MAC del calcolatore da raggiungere. Il MAC è fondamentale perché evita che tutti i calcolatori debbano ricevere tutti i pacchetti e verificare se l'IP è il loro, cosa che renderebbe gli host incapaci di fare qualsiasi altra cosa data la mole di lavoro. Questo MAC viene reperito grazie a una tabella contenuta nel calcolatore che mette in relazione IP con MAC. Se non è presente, lo richiede partendo dall'IP che vuole raggiungere grazie al protocollo ARP, che fa una richiesta broadcast. Questo scambio è una consegna diretta.



Indirect Delivery: Se l'IP destinatario è su un'altra rete, il pacchetto viene inviato a un router intermedio. A livello 1, l'IP di destinazione sarà quello del calcolatore obiettivo, ma a livello 2, il MAC sarà quello del gateway della propria rete. Poiché il gateway è un router, non scarterà il pacchetto nonostante l'IP di destinazione non corrisponda al proprio; invece, lo instraderà verso un altro router. Il primo e l'ultimo scambio, tra l'host spedente e il rispettivo router e tra l'host ricevente e il rispettivo router, sono scambi diretti. Tutti gli scambi intermedi sono indiretti e devono essere completati entro il limite di 255 hop imposto dal TTL. La decisione nei passaggi indiretti è simile a quella nei passaggi diretti: il router utilizzerà il protocollo ARP (pacchetti broadcast a livello data link) per ottenere l'indirizzo del gateway successivo, ovvero l'unico altro calcolatore della loro rete, per passargli il pacchetto. In questi casi, è opportuno avere un indirizzo IP /30, in modo tale che, tolti i 2 indirizzi proibiti, ne restino 2 per i 2 gateway della rete. Per determinare se è possibile effettuare una consegna diretta, si utilizza la tabella di instradamento IP. Grazie a essa, è possibile inviare una richiesta ARP, nella speranza di una ARP reply, attraverso l'interfaccia corretta e agli indirizzi che contengono l'IP dell'host, evitando una richiesta ARP broadcast che appesantirebbe eccessivamente l'infrastruttura di rete. In caso di mancanza di reply, dato che l'IP è un protocollo best effort, si scarta il pacchetto e si segnala l'errore.

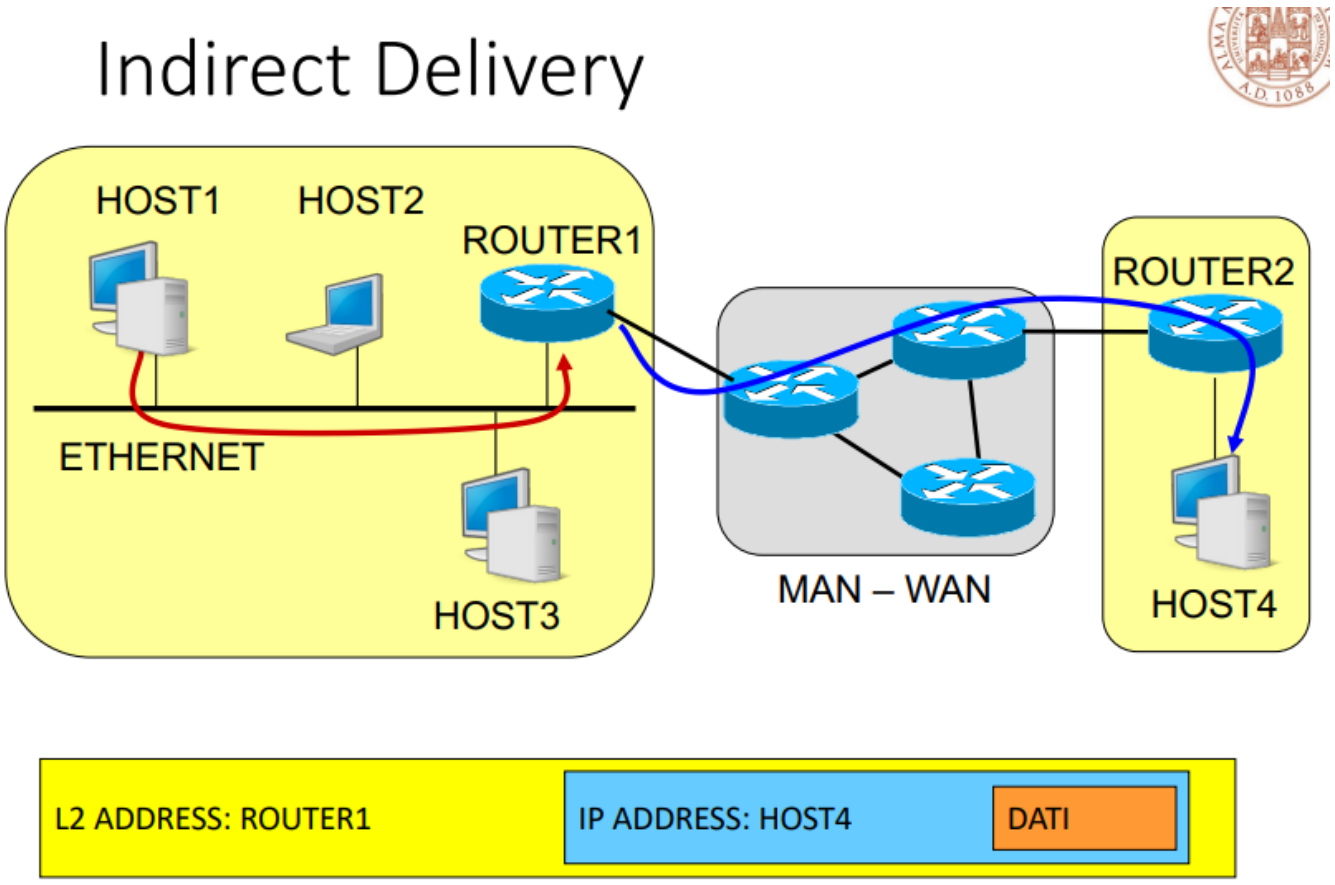


Tabella di Instradamento: Ogni nodo (host o router) ha una tabella che contiene informazioni sulle destinazioni possibili, netmask, gateway e interfacce. Le righe della tabella rappresentano le singole istanze di instradamento, mentre le colonne contengono le opzioni di instradamento. Tipicamente, la tabella ha cinque colonne principali:

- **Destination**: Contiene gli indirizzi IP o i gruppi di IP raggiungibili.
- **Netmask**: Indica la netmask che permette di interpretare correttamente l'IP.
- **Gateway**: L'IP del gateway successivo a cui fare riferimento.(Se si dovesse essere già un host finale ci possono esere più possibilità come per esempio il proprio ip, la scritta self ecc)
- **Interface**: L'interfaccia di rete attraverso cui inviare il pacchetto.(Mi dice da dove fare la richiesta Arp qualora fosse necessarai)
- **Metric**: Rappresenta il costo del percorso, utilizzato per determinare il percorso migliore quando sono disponibili più opzioni. Questa struttura permette ai nodi di instradare i pacchetti in modo efficiente, scegliendo il percorso ottimale basato sulle informazioni disponibili nella tabella di instradamento.

Utilizzo della Tabella di Instradamento da parte dei Gateway: I gateway utilizzano la tabella di instradamento per determinare il percorso ottimale per ogni pacchetto. La tabella contiene informazioni su destinazioni, netmask, gateway e interfacce. Quando un pacchetto arriva al gateway, questo esamina l'indirizzo IP di destinazione e lo confronta con le voci nella tabella di instradamento. Il gateway seleziona la voce con la netmask più lunga che corrisponde all'indirizzo di destinazione (**Longest Prefix Match**) e inoltra il pacchetto attraverso l'interfaccia appropriata. Questo processo evita il sovraccarico della rete con broadcast inutili, poiché il gateway invia il pacchetto solo all'interfaccia specifica che conduce verso la destinazione finale. In questo modo, i pacchetti vengono instradati in modo efficiente e preciso, riducendo il traffico di rete e migliorando le prestazioni complessive. Se non trova una corrispondenza, scarta il pacchetto e comunica un errore. Per trovare la corrispondenza migliore, avendo l'IP di destinazione, il gateway procede con il processo di **table lookup durante** il quale, partendo dalla netmask con valore più grande e andando a decrescere,

prende la netmask e fa l'AND bit a bit con l'IP di destinazione del datagramma e lo confronta con l'IP di destinazione della singola riga. Qualora il risultato fosse uguale, la corrispondenza è trovata (abbiamo trovato il ricevente); altrimenti, continua con le altre righe e tiene il risultato più simile che quindi avvicina di più all'host finale.

Longest Prefix Match: Per selezionare il percorso corretto, il nodo confronta l'indirizzo di destinazione con la netmask più lunga disponibile nella tabella.

ARP (Address Resolution Protocol)

Protocollo di rete utilizzato per mappare un indirizzo IP a un indirizzo MAC corrispondente all'interno di una rete locale (LAN). Funziona a livello **2 (Data Link)** e si interfaccia con il livello **3 (Rete)** del modello OSI, consentendo la comunicazione tra dispositivi in una rete Ethernet o simile.

Quando un dispositivo vuole comunicare con un altro sulla stessa rete:

1. Conosce l'indirizzo IP del destinatario (ad esempio 192.168.1.2).
2. Non conosce il corrispondente indirizzo MAC, necessario per inviare i pacchetti a livello di collegamento.
3. Usa il protocollo ARP per scoprire l'indirizzo MAC associato all'IP.

Quando un host deve inviare un pacchetto:

1. **Controllo della cache ARP**:
    - L'host verifica se l'indirizzo IP è già mappato a un indirizzo MAC nella propria cache ARP (una tabella locale).
    - Se trova un'associazione valida, utilizza l'indirizzo MAC e invia direttamente il pacchetto.
2. **Richiesta ARP (ARP Request)**:
    - Se l'indirizzo non è presente nella cache, l'host genera una richiesta ARP:
        - La richiesta è un messaggio broadcast inviato a **tutti i dispositivi** della LAN (MAC di destinazione = `FF:FF:FF:FF:FF:FF`).
        - Contiene l'indirizzo IP di cui si vuole conoscere il MAC.
3. **Risposta ARP (ARP Reply)**: Il dispositivo con l'indirizzo IP richiesto risponde con un messaggio unicast, fornendo il proprio indirizzo MAC.
4. **Aggiornamento della cache ARP**: L'host salva nella cache l'associazione IP-MAC per usi futuri.

Classless VS Classfull

Classi di indirizzi IP (Classfull)

- Durante le fasi iniziali di Internet, gli indirizzi IP erano suddivisi in **classi**:
    - **Classe A**: grandi reti (da 0.0.0.0 a 127.255.255.255) ed andavano letti come se avessero un netmask /8.
    - **Classe B**: reti di medie dimensioni (da 128.0.0.0 a 191.255.255.255) ed andavano letti come se avessero un netmask /16.
    - **Classe C**: piccole reti (da 192.0.0.0 a 223.255.255.255) ed andavano letti come se avessero un netmask /24.
    - **Classe D**: indirizzi multicast (da 224.0.0.0 a 239.255.255.255), riservati al multicast.
    - **Classe E**: sperimentale (da 240.0.0.0 a 255.255.255.255), riservati a casi sperimentali.

    - **Indirizzi riservati**: ad esempio, 127.x.x.x per loopback e 255.255.255.255 per broadcast.
- Dunque, la netmask dell'indirizzo era implicita nella classe dell'indirizzo stesso. Tuttavia, questo approccio presentava limitazioni significative, come la scarsa flessibilità nella gestione degli indirizzi IP e l'inefficienza nell'allocazione degli indirizzi. Per risolvere questi problemi, è stato introdotto il **Classless Inter-Domain Routing (CIDR)**, che permette una gestione più efficiente e flessibile degli indirizzi IP, eliminando la rigida suddivisione in classi e utilizzando netmask variabili.
- Con CIDR, la netmask è specificata esplicitamente utilizzando la notazione **slash** (ad esempio, /24), permettendo una suddivisione (**subnetting**) più granulare e ottimizzata degli indirizzi IP.
- Inoltre, CIDR facilita l'aggregazione delle rotte (**supernetting**), riducendo la complessità delle tabelle di routing e migliorando l'efficienza della rete.
- Per esempio, un indirizzo IP come 192.168.1.0/24 indica che i primi 24 bit dell'indirizzo sono utilizzati per identificare la rete, mentre i restanti 8 bit sono utilizzati per identificare gli host all'interno di quella rete.
- Questa flessibilità consente di adattare meglio la dimensione delle reti alle esigenze specifiche, evitando sprechi di indirizzi IP e migliorando la scalabilità della rete.

CIDR (Classless Inter-Domain Routing) (Classless)

Con la diffusione di Internet, la suddivisione rigida in classi si è dimostrata inefficiente, portando alla creazione di CIDR (**RFC 1519**). CIDR elimina la logica delle classi nei router e consente la **definizione variabile della dimensione del Net-ID**. Le tabelle di routing includono le netmask per una gestione più flessibile delle reti. Oggi, la distinzione tra host e net è locale a tal punto che dipende dal punto in cui si guarda, punto nel quale è contenuta la netmask di riferimento per quella specifica istanza. Dunque, uno stesso indirizzo ha rilevanza diversa in punti diversi della rete.

Routing Aggregato

La **semplificazione delle tabelle di routing** avviene aggregando più network in un’unica voce, riducendo la complessità per i router. Questo processo è noto come **supernetting** o **route aggregation**.

Vantaggi del Routing Aggregato:

- **Riduzione delle voci nelle tabelle di routing**: Aggregando le reti, si diminuisce il numero di voci che i router devono gestire, semplificando il processo di instradamento.
- **Miglioramento delle prestazioni**: Con meno voci da esaminare, i router possono prendere decisioni di instradamento più rapidamente, migliorando le prestazioni complessive della rete.
- **Minore utilizzo di memoria**: Le tabelle di routing più piccole richiedono meno memoria, liberando risorse per altre operazioni.
- **Scalabilità**: La rete diventa più scalabile, poiché l'aggiunta di nuove reti contigue può essere gestita facilmente attraverso l'aggiornamento della supernet esistente.
- **Riduzione del traffico di aggiornamento**: Con meno voci da aggiornare, si riduce il traffico di aggiornamento delle tabelle di routing tra i router, migliorando l'efficienza della rete.

Come si aggregano le reti:

1. **Identificazione delle reti contigue**: Per aggregare le reti, è necessario che queste siano contigue, ovvero che gli indirizzi IP siano consecutivi.
2. **Calcolo della supernet**: Si determina una nuova netmask che copra tutte le reti contigue. Ad esempio, se si hanno le reti 192.168.1.0/24 e 192.168.2.0/24, si può aggregarle in una singola rete 192.168.0.0/22,

ifatti:
    - **192.168.1.0/24**:
        - Netmask: `255.255.255.0` (24 bit).
        - Copre gli indirizzi da `192.168.1.0` a `192.168.1.255`.
    - **192.168.2.0/24**:
        - Netmask: `255.255.255.0` (24 bit).
        - Copre gli indirizzi da `192.168.2.0` a `192.168.2.255`.
    - `192.168.1.0` → `11000000.10101000.00000001.00000000`
    - `192.168.2.0` → `11000000.10101000.00000010.00000000`
    - I primi **22 bit** sono identici: `11000000.10101000.000000` (corrisponde a `192.168.0.0`).
3. **Aggiornamento delle tabelle di routing**: Le voci delle singole reti vengono sostituite da una voce unica che rappresenta la supernet.

Subnetting

La **subdivisione in sottoreti (subnetting)** consente di frammentare una rete principale in reti più piccole (subnet) per assegnarle a diverse sotto-amministrazioni all'interno di un'organizzazione. La **subnet mask** permette di personalizzare l'assegnazione dell'indirizzo IP, suddividendo l'Host-ID in due parti: una parte per la subnet e l'altra per l'host. L'Università di Bologna utilizza una rete di classe B (137.204.0.0) e divide l'Host-ID per creare 254 sottoreti di classe C, utilizzando la netmask 255.255.255.0.

Supernetting

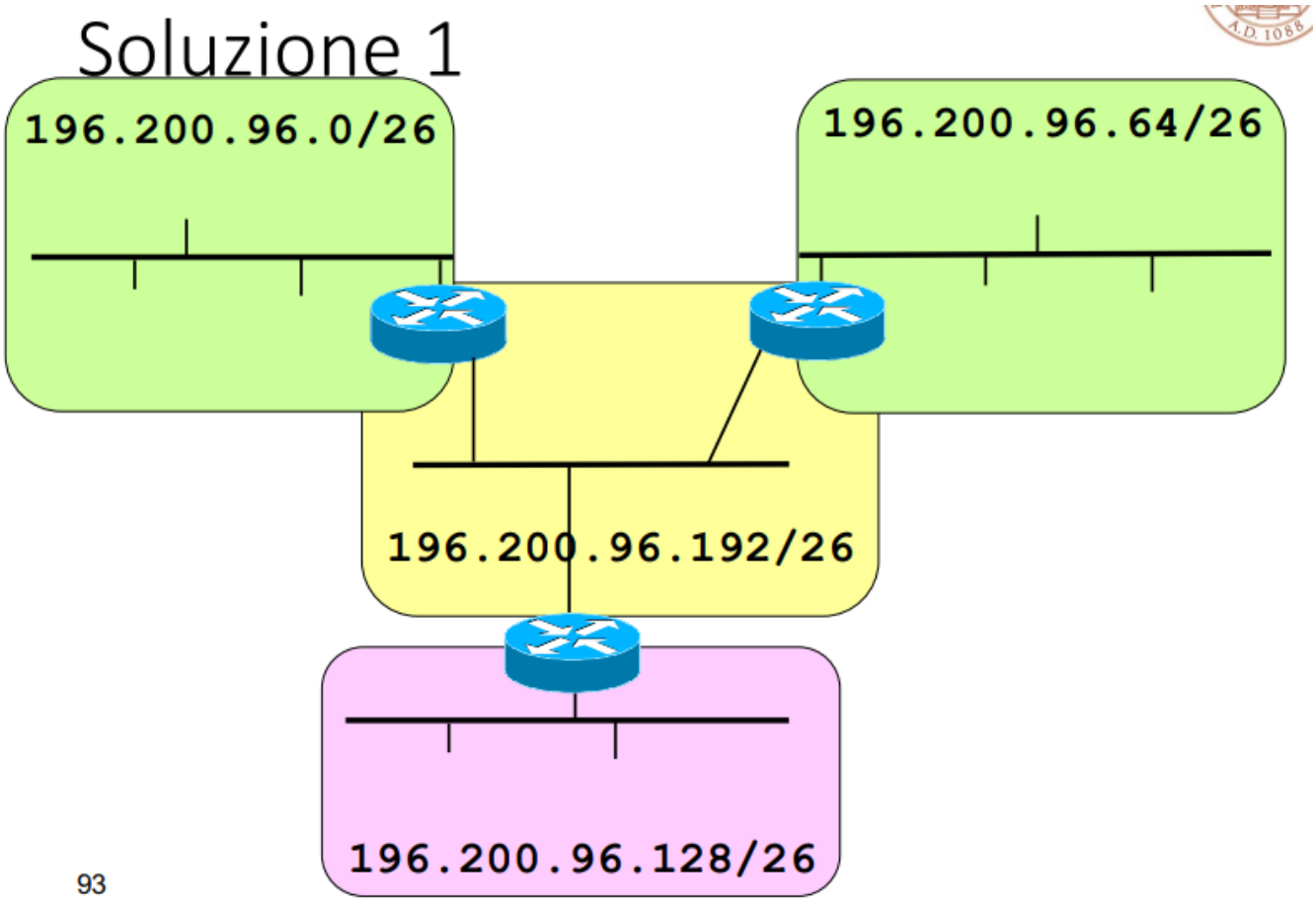
Il **supernetting** consente di unire più reti contigue per ridurre le voci nelle tabelle di routing. Ad esempio:

- Un'organizzazione ha bisogno di circa 2000 indirizzi IP: invece di una rete di classe B (64k indirizzi), è preferibile combinare 8 reti di classe C (2048 indirizzi).
- Supernetting consente di rappresentare queste reti come una singola super-rete: es. 194.24.0.0/21, con netmask 255.255.248.0.
- **Operazioni duali**:
    - Subnetting riduce la parte Host-ID per estendere il Net-ID.
    - Supernetting estende l'Host-ID per aggregare reti con Net-ID simili.

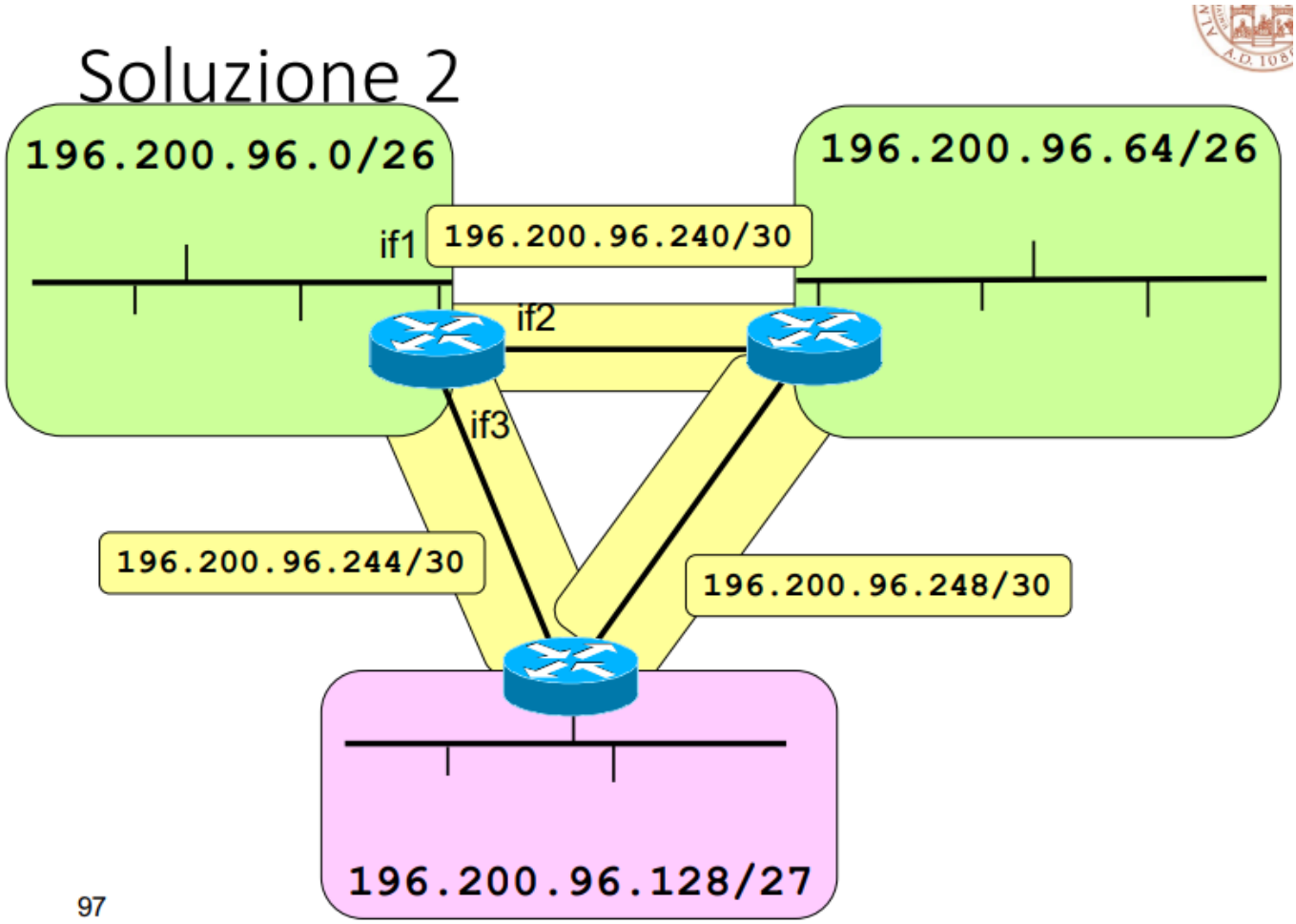
Progettazione di Reti Aziendali

Esempio di rete aziendale: Tre siti aziendali (S1, S2, S3) devono essere interconnessi con una rete a maglia completa. Gli indirizzi di classe C assegnati sono basati su 196.200.96.0/24. Con questa rete ho più IP del necessario, dato che ho 256 IP, ma con una /25 ne avrei avuti 128 e sarei stato troppo di misura.

Soluzione 1: Non avendo una sola rete fisica, non possiamo avere consegna diretta. Dovremmo usare dei gateway con una rete "comune" di collegamento tra questi ultimi. Avendo una /24, posso ottenere 4 reti /26, dunque 62 IP per blocco. Questa soluzione provoca un grande spreco nel blocco usato per il collegamento (uso 3 numeri per i gateway e i restanti 58 non servono a niente). Inoltre, se devo crescere, sarò in difficoltà perché se creo una nuova sede essa necessiterà di un nuovo blocco che non ho modo di creare. Se aumento i terminali nelle sedi già esistenti, posso arrivare solo a 62.



Soluzione 2: Potrei valutare netmask a grandezza differenziata. Ricordiamoci che più divido, più mi mangio numeri, dato che per ogni divisione il primo e l'ultimo numero sono non utilizzabili. Creerò dunque 2 reti /26 (metà degli indirizzi), 3 reti /27 (3/4 dei restanti indirizzi), 1 rete /28 (1/2 dei restanti indirizzi) e 3 reti /30 con le quali completerò gli indirizzi. Così facendo, le 2 reti /26 saranno usate per 2 sedi, 1 rete /27 per la terza sede e 3 reti /30 per i 3 gateway, mantenendo disponibili tutti gli altri indirizzi per il futuro. Se possibile, un'unica rete per tutti i gateway è preferibile a questa seconda soluzione, perché se dobbiamo fisicamente creare l'infrastruttura urbana, è più facile da realizzare. Fossero state 3 isole, forse fisicamente sarebbero state più comode 3 reti.



ICMP e Comandi di Rete

Protocollo ICMP (Internet Control Message Protocol)

ICMP è un protocollo incaricato non di corregge gli errori, ma fornire informazioni per diagnosticare problemi di rete.

- ICMP segnala errori come:
    - **Destination Unreachable (Type 3)**: quando un gateway non può raggiungere la rete o l'host.
    - **Time Exceeded (Type 11)**: quando il Time-to-Live (TTL) di un datagramma si azzera.
    - **Redirect (Type 5)**: un router segnala all'host sorgente una via più ottimale.
    - **Struttura pacchetto ICMP**:
        1. **IP Header**: Intestazione del protocollo IP.
        2. **Message Type**: Tipo di messaggio ICMP (8 bit).
        3. **Message Code**: Codice del messaggio ICMP (8 bit).
        4. **Checksum**: Controllo degli errori per l'intestazione ICMP (16 bit).
        5. **Additional Fields**: Campi aggiuntivi specifici per il tipo di messaggio ICMP.
        6. **Data**: Dati del messaggio ICMP.
- **Tipi di messaggi ICMP**:
    - **Host Unreachable (Code 1)**: Indica che l'host di destinazione non è raggiungibile.
    - **Protocol Unreachable (Code 2)**: Segnala che il protocollo specificato non è supportato dal dispositivo di destinazione.

- **Destination Unreachable (Type 3)**: Notifica l'inaccessibilità di host o sottorete.
- **Fragmentation Needed and Don't Fragment was Set (Code 4)**: Notifica che la frammentazione è necessaria ma il flag "Don't Fragment" è impostato, impedendo l'invio del pacchetto.
- **Source Route Failed (Code 5)**: Indica che il routing basato su un percorso sorgente specificato non è riuscito.
- **Echo/Echo Reply (Type 8/0)**: Utilizzati per determinare lo stato di raggiungibilità di un host.
- **Time Exceeded (Type 11)**: Notifica il superamento del TTL o il timeout per il riassemblaggio dei frammenti.
- **Timestamp Request/Reply (Type 13/14)**: Misura il tempo di transito nella rete.

PING

Verifica se un host è raggiungibile inviando pacchetti ICMP di tipo "echo" e ricevendo "echo reply".

Opzioni: definire il numero di pacchetti, timeout, dimensione pacchetti, ecc.

Parametri principali: `-n` (numero di pacchetti), `-t` (ping continuo), `-a` (risoluzione DNS), `-l` (dimensione del pacchetto).

TRACEROUTE

Mostra il percorso dei pacchetti verso una destinazione, utilizzando pacchetti ICMP con TTL crescente. Mostra il nome DNS e l'indirizzo IP dei nodi intermedi. Traceroute invia pacchetti con un valore TTL (Time To Live) inizialmente impostato a 1. Ogni router lungo il percorso decrementa il TTL di 1. Quando il TTL raggiunge 0, il router scarta il pacchetto e invia un messaggio **ICMP "Time Exceeded"** al mittente. Traceroute incrementa quindi il TTL e invia un nuovo pacchetto, ripetendo il processo fino a raggiungere la destinazione finale. Questo permette di identificare ogni hop (router) lungo il percorso.

Parametri principali: `-m` (TTL massimo), `-q` (numero di query per hop), `-w` (timeout per risposta).

Protocollo DHCP (Dynamic Host Configuration Protocol)

DHCP: Automatizza l'assegnazione dinamica di IP, netmask, gateway e DNS. Processo chiave:

- **DHCPDISCOVER**: l'host cerca un server DHCP inviando un messaggio di richiesta in broadcast.
- **DHCPOFFER**: i server DHCP rispondono proponendo un indirizzo IP.
- **DHCPREQUEST**: l'host accetta una delle offerte e richiede l'indirizzo IP.
- **DHCPACK**: il server DHCP conferma la configurazione con un messaggio di risposta.

Protocollo APIPA (Automatic Private IP Addressing)

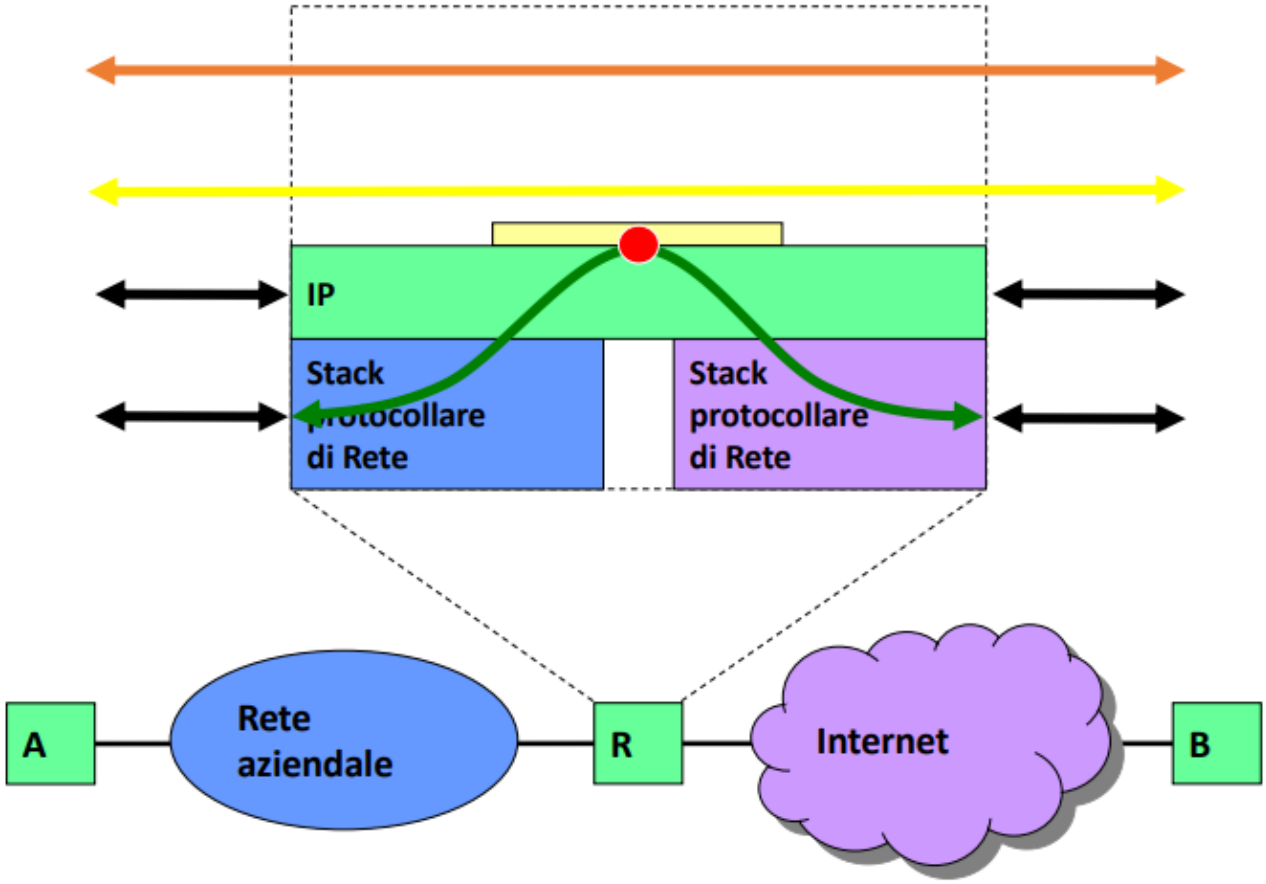
APIPA: Una funzione di fallback che consente a un host di assegnarsi automaticamente un indirizzo IP nella rete privata **169.254.0.0/16** quando un server DHCP non è disponibile. Questo permette agli host di comunicare tra loro all'interno della stessa rete locale, ma senza accesso esterno (es. Internet).

Filtraggio dei Pacchetti

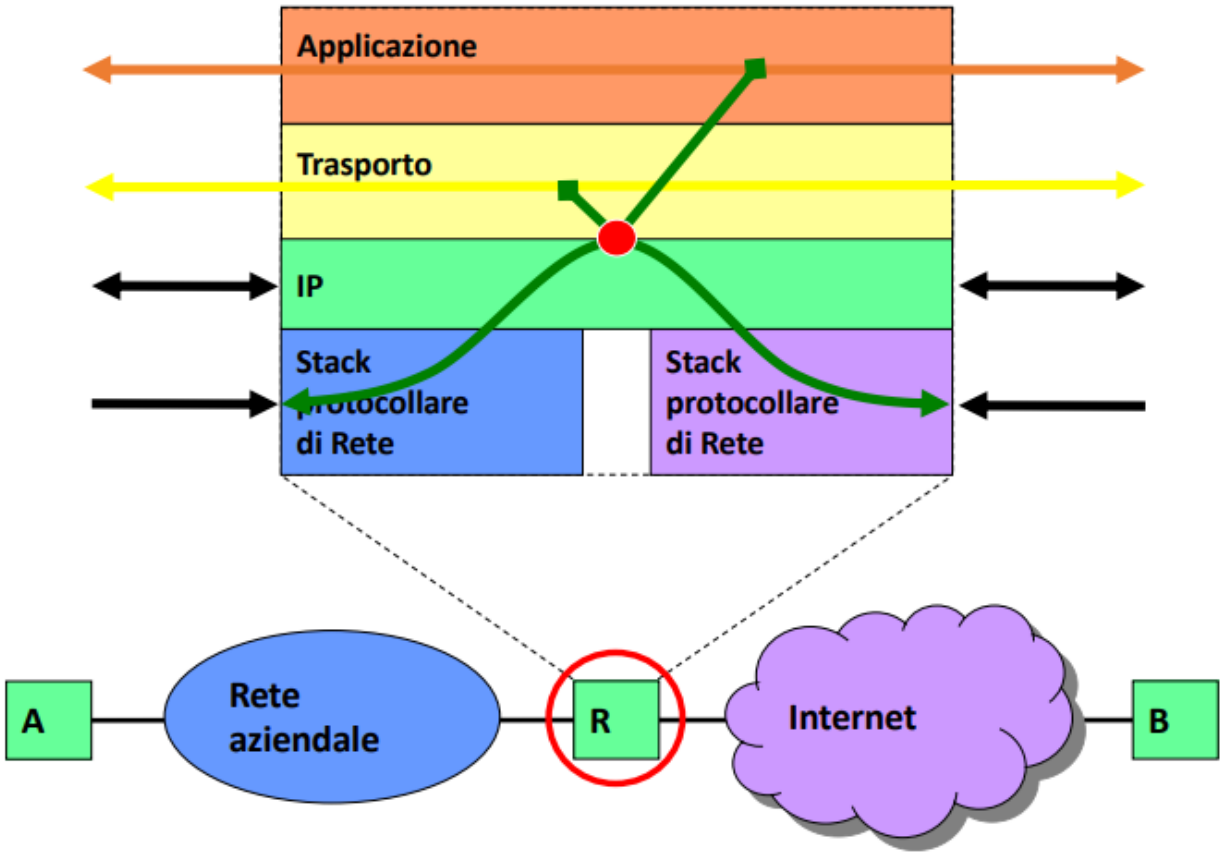
Le **metodologie di filtraggio dei datagrammi** sono tecniche utilizzate per controllare il traffico di rete in base a criteri predefiniti. Questi criteri possono includere indirizzi IP, numeri di porta, protocolli e altre

informazioni contenute nei pacchetti. In questo contesto, i gateway fungono da punti di controllo per il traffico di rete, applicando le regole di filtraggio per garantire che solo il traffico autorizzato possa attraversare la rete. Queste metodologie sono fondamentali per implementare firewall e altre soluzioni di sicurezza di rete, garantendo che solo il traffico autorizzato possa attraversare i confini della rete.

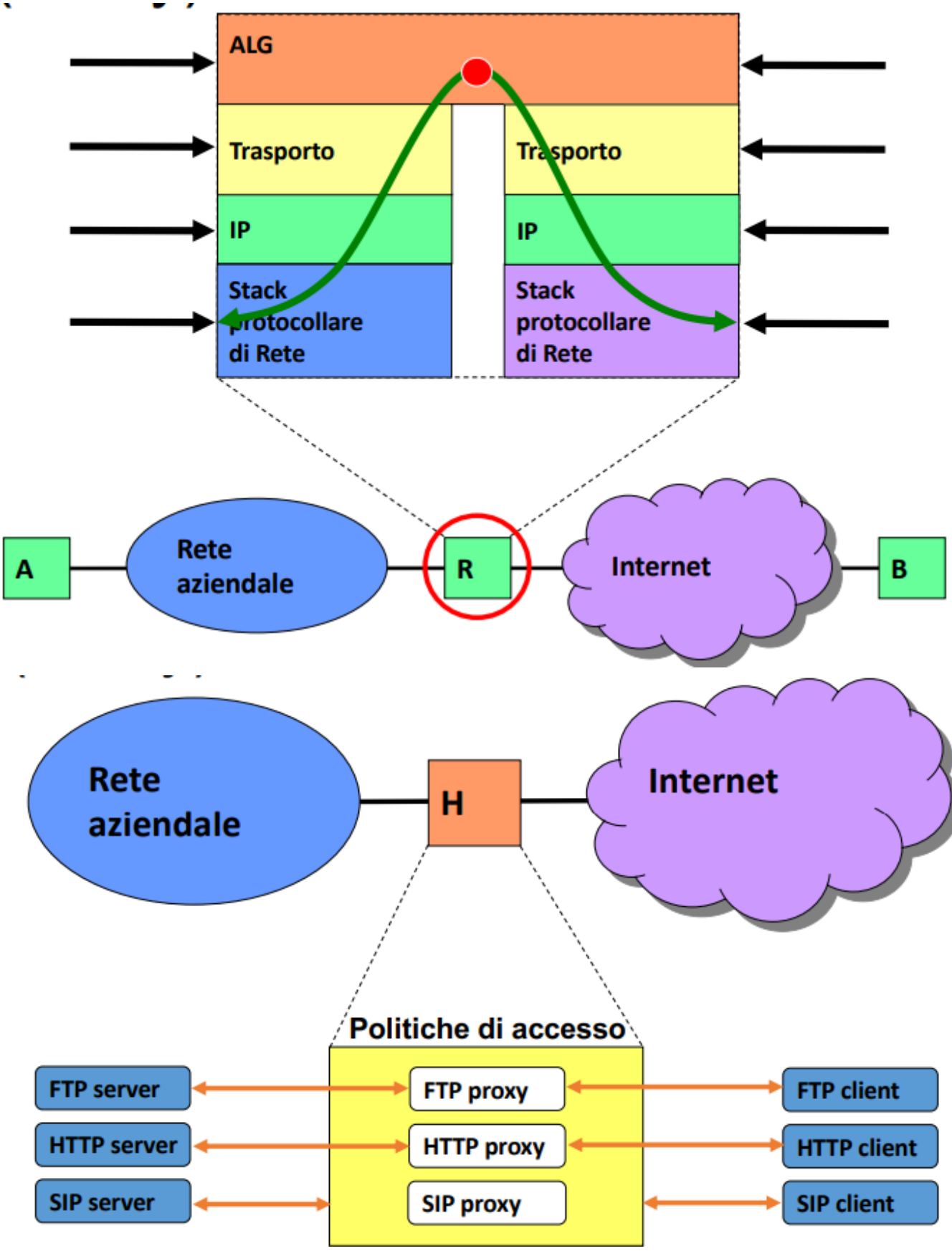
Packet Filter: Controlla l'accesso a determinati servizi o indirizzi in base alle regole impostate sugli IP, protocolli o porte. È detto instradamento selettivo e opera a livello IP basando le sue decisioni sulla natura dell'IP stesso come il TTL, i tipi di indirizzi ecc. Il vantaggio è che a livello di gateway basta implementare il filtro a livello software, ma esistono situazioni in cui i filtri a livello IP non sono sufficienti.



Stateful Packet Inspection (SPI): Monitora lo stato delle connessioni e adatta dinamicamente le regole di filtraggio. Adattando opportunamente il software, si può andare più a fondo nel pacchetto guardando, per esempio, il tipo di protocollo, attuando così filtri semanticamente più efficaci. Ciò viola il protocollo OSI dato che vado a leggere dati più profondi del livello IP.



Application Layer Gateway (Proxy): Monitora le connessioni applicative (ad esempio, FTP, HTTP, SIP), garantendo controllo e sicurezza a livello applicativo. In questo caso, il gateway agisce come un host che scompone il pacchetto fino al livello applicativo e poi lo reinstrada se non è destinato a lui. A differenza dei normali gateway con implementazioni specifiche, un proxy a livello applicativo è più complesso sia a livello hardware che software.



Le tre differenti versioni vengono adottate a necessità dato che la prima è la più leggera a livello computazionale e la più facile da implementare ma quella meno efficace, e viceversa per la terza.

Firewall

Il firewall o portatagliafuoco ci difende combinando le tecnologie precedentemente descritte, può essere software (per accessi domestici) o hardware (per reti aziendali).

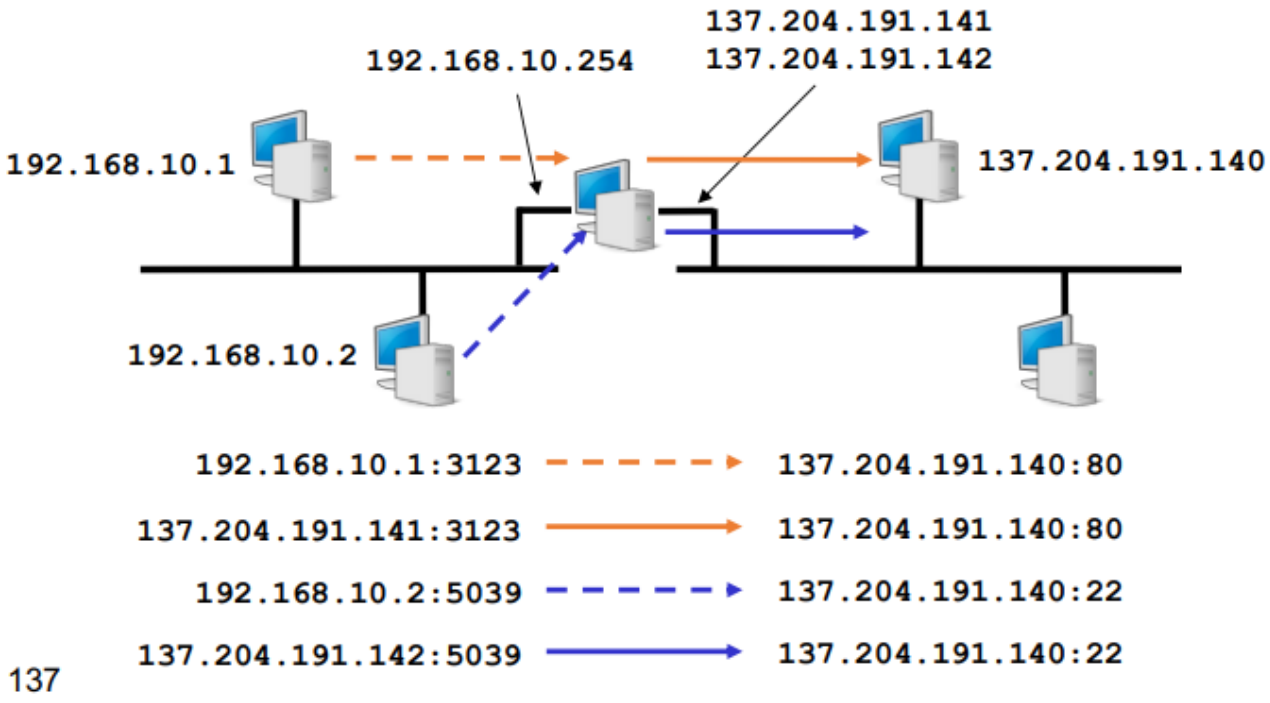
Politiche di sicurezza:

- **Default deny**: Blocca tutto eccetto ciò che è esplicitamente permesso.
- **Default permit**: Permette tutto eccetto ciò che è esplicitamente bloccato.

Network Address Translation (NAT)

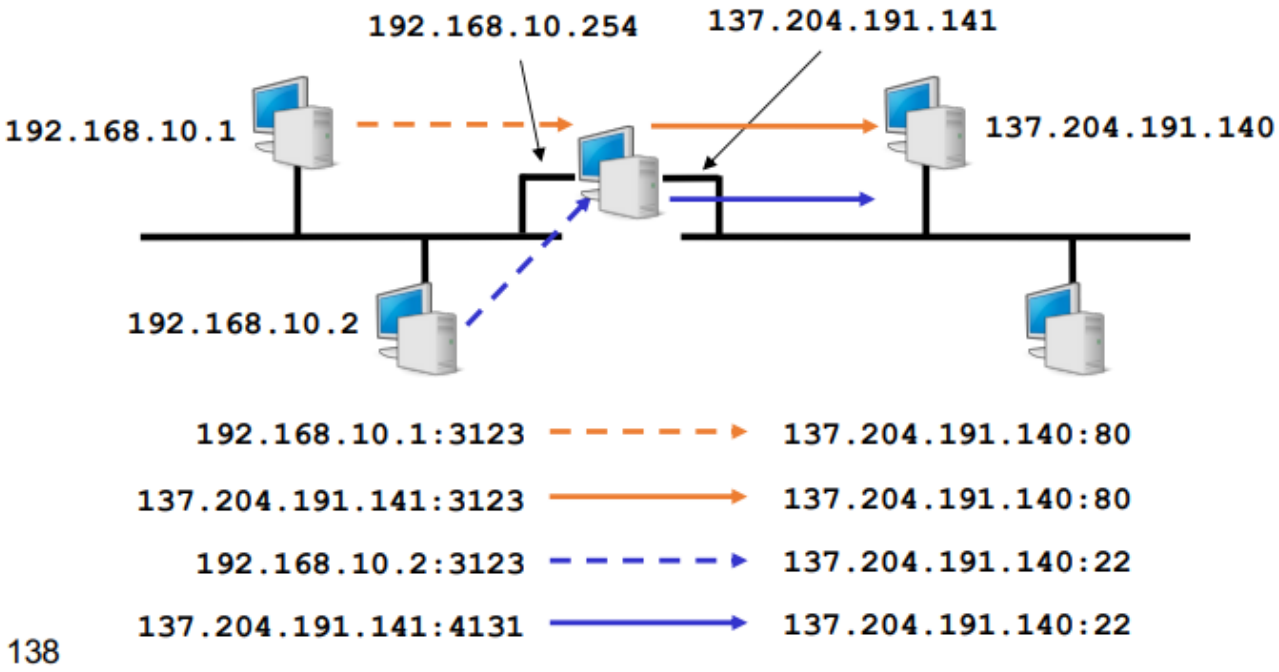
Il **Network Address Translation (NAT)** è un gateway con funzioni di **packet filtering** che si interpone tra due network, modificando il contenuto dei pacchetti, in particolare gli indirizzi IP e i numeri di porta, in base alla specifica implementazione. NAT è definito a livello concettuale, ma non fisico o implementativo, poiché può essere realizzato in modi diversi. La sua funzione principale è mascherare gli indirizzi IP interni, consentendo a reti private di accedere a reti pubbliche senza esporre direttamente i dispositivi interni.

Basic NAT - Conversione di indirizzo: Il Basic NAT si trova tra due network e agisce come gateway. Modifica l'indirizzo sorgente nei pacchetti in uscita, sostituendo l'indirizzo IP privato con uno pubblico configurato. Quando il pacchetto di risposta torna, il NAT riconverte l'indirizzo pubblico nell'originale indirizzo privato utilizzando una tabella di conversione. Questo approccio consente comunicazioni unidirezionali: i dispositivi interni possono avviare comunicazioni verso l'esterno, ma non viceversa, a meno che non siano configurate regole specifiche. Originariamente ideato per risparmiare indirizzi IP pubblici, offre anche un livello base di protezione nascondendo i dispositivi interni.



Network Address and Port Translation (NAPT): Conosciuto anche come **Port Address Translation (PAT)**, il NAPT estende il Basic NAT aggiungendo la traduzione dei numeri di porta. Questa tecnica permette a più dispositivi all'interno di una rete privata di condividere un unico indirizzo IP pubblico. Il router associa ogni combinazione di indirizzo IP privato e numero di porta interna a una combinazione univoca di indirizzo IP pubblico e numero di porta esterna. Quando un pacchetto ritorna, il router utilizza il numero di porta esterna per identificare il dispositivo interno corretto. Questo approccio consente a decine di migliaia di dispositivi di

accedere simultaneamente a Internet, limitando però il numero di flussi distinguibili a 65.536, pari al massimo delle porte disponibili. NAPT è particolarmente utile per conservare indirizzi IP pubblici e fornisce un ulteriore livello di sicurezza nascondendo gli indirizzi IP privati dall'esterno.



(MANCANO 24 MIN DELLA LEZIONE DEL 16 OTTOBRE POICHè NON HO TROVATO LE SLIDE)

Routing

Teoria dei grafi e rappresentazione della rete:Le reti possono essere rappresentate come grafi orientati o non orientati.Il peso degli archi rappresenta il costo de l collegamento.

Funzioni di IP

Indirizzamento: L'IP fornisce un sistema di indirizzamento univoco per identificare dispositivi sulla rete.

Frammentazione: L'IP può dividere i pacchetti di dati in frammenti più piccoli per adattarsi alla dimensione massima del pacchetto supportata dai vari segmenti della rete.

Instradamento:

- Decidere che percorso un datagramma deve seguire per raggiungere la destinazione.
- Utilizza le **PCI (Protocol Control Information)** dei datagrammi,ovvero le informazioni di controllo aggiunte ai dati per gestire la trasmissione e il corretto instradamento del datagramma attraverso la rete. Queste informazioni sono incluse nell'intestazione del datagramma.
- Determina il comportamento della funzione di commutazione nei nodi.
- Il problema dell'instradamento è più generale rispetto al protocollo di livello 3.
- Gli **Algoritmi di instradamento** hanno come biettivi: semplicità, robustezza, stabilità, efficienza.

Algoritmi:

- **Senza tabella**: Flooding, Random, Deflection routing, Source routing.
- **Con tabella**:

    - **Instradamento fisso e centralizzato** detto anceh **Statico**: Utilizzato per sistemi estremamente statici, dove i dati rimangono invariati per un tempo molto più lungo della singola comunicazione. Questo metodo risulta sempre uguale dal punto di vista dell'utente.
    - **Instradamento dinamico a distanza minima**: I percorsi vengono aggiornati periodicamente per adattarsi ai cambiamenti della rete dunque risulta più dinaico del precedente.

Flooding

Flooding è una tecnica di instradamento in cui ogni nodo della rete ritrasmette ogni pacchetto ricevuto su tutte le sue porte, eccetto quella da cui il pacchetto è arrivato. Questo metodo garantisce che tutte le possibili strade vengano percorse, assicurando che almeno una copia del pacchetto raggiunga la destinazione.

- Garantisce:
    - **Affidabilità**: Flooding garantisce che il pacchetto raggiunga la destinazione anche se alcuni percorsi sono interrotti.
    - **Percorso più breve**: Il primo pacchetto che raggiunge la destinazione lo fa percorrendo il percorso più breve disponibile.
    - **Semplicità**: L'algoritmo è semplice da implementare poiché non richiede tabelle di instradamento complesse.
- Contro:
    - **Proliferazione dei pacchetti**: La rete può essere sovraccaricata da un numero eccessivo di pacchetti duplicati, causando congestione.
    - **Inefficienza**: L'invio di pacchetti su tutte le porte può risultare inefficiente in termini di utilizzo della larghezza di banda.
- Utilizzato:
    - **Broadcasting**: Flooding è utile per inviare messaggi di broadcast, dove l'obiettivo è raggiungere tutti i nodi della rete.
    - **Scenari di emergenza**: In situazioni in cui è cruciale che il messaggio raggiunga la destinazione, indipendentemente dall'efficienza.

Soluzioni per il Flooding

- Non ritrasmettere il pacchetto da dove è arrivato.
- Identificazione dei pacchetti (indirizzo sorgente + numero di sequenza).
- Uso di un TTL per evitare pacchetti infiniti. È importante ricordare che all'aumentare di queste soluzioni il protocollo si complica, andando via via a perdere di utilità a causa del suo complicarsi.

Random e Deflection Routing

Random Routing: Il prossimo hop è scelto casualmente. Questo metodo è molto inefficiente e raramente utilizzato.

Deflection Routing: Il pacchetto viene inviato sulla linea con meno pacchetti in attesa. Questo metodo è stato studiato per reti a griglia (Manhattan), dove si dimostra essere una buona soluzione.

Problemi: I pacchetti possono arrivare fuori sequenza o entrare in cicli infiniti.

Store-and-Forward

Il pacchetto viene verificato, memorizzato e confrontato con la tabella di instradamento. Dopo l'elaborazione, si seleziona un'uscita e il pacchetto viene inserito in coda. Tutto questo avviene in una coda che gestisce l'elaborazione.

Shortest Path Routing

L'instradamento a percorso più breve implica l'associazione di una lunghezza a ciascun collegamento e la ricerca dei percorsi a costo minimo utilizzando algoritmi come Bellman-Ford e Dijkstra. Questo può essere implementato in modo **centralizzato** o **distribuito**, sia in maniera **sincrona** che **asincrona**. Quando i nodi di rete vengono accesi, conoscono solo la configurazione delle loro interfacce, che può essere statica o dinamica tramite DHCP. Con queste informazioni, popolano la tabella di instradamento iniziale. Per implementare il routing a percorso più breve (shortest path) verso qualsiasi destinazione, devono utilizzare uno o più protocolli di routing per scambiarsi informazioni e apprendere la topologia della rete, e uno o più algoritmi per il calcolo dei percorsi più brevi basati sulle informazioni ottenute.

Routing Distance Vector

Il Routing Distance Vector è una definizione teorica di algoritmi ri souting che si basano sullo scambio di **Distance Vector**. Basato sull'algoritmo Bellman-Ford, ogni nodo invia un vettore con le distanze agli altri nodi. Questo metodo è piuttosto datato e presenta diversi problemi, ma su piccoli sistemi questi non emergono, rendendolo interessante in casi specifici, ovvero con dati statici, privi di variazioni in corso d'opera, e in cui possiamo conoscere l'intera struttura, cosa oggi impossibile dato che la rete è dinamica e distribuita. In questo metodo, ogni nodo ha una lista con la distanza dagli altri nodi. Inizialmente, questa lista è composta solo dalla distanza da se stesso, ovvero 0. Successivamente, i nodi (router) condivideranno con i nodi a cui sono direttamente collegati i propri dati detti **Distance vector**, aggiornando così le tabelle dei vicini. Questo processo continua finché non si reperiscono informazioni da tutti i nodi, passando per i vicini e ottenendo i percorsi migliori nel sistema.

Problemi:

- **Cold start e convergenza lenta**: La convergenza si raggiunge dopo un numero di iterazioni pari al numero di nodi. Questo comporta una lenta convergenza su reti grandi, poiché gli aggiornamenti tra nodi non possono essere inviati continuamente, ma devono lasciare che anche i messaggi circolino, ritardando così la convergenza.
- **Conteggio all'infinito**: In alcuni casi, si potrebbe tentare di convergere all'infinito. Ad esempio, se ci sono tre router in fila e si rompe il collegamento tra due di essi, gli altri due potrebbero scambiarsi aggiornamenti di distanza dal terzo all'infinito. Questo li porta a convincersi reciprocamente che per raggiungere il terzo router debbano usare l'altro a cui sono collegati, finendo per passarsi all'infinito pacchetti e aggiornamenti di distanza, andando a bruciare capacità computazionale. Per ovviare, si sceglie una distanza tra nodi superata la quale si considera la distanza come infinita ed implementare un Triggered Update,ovvero un aggiornamento istantaneo del distance vector qualora ci fosse una variazione di distanza.

Soluzioni - **Split Horizon**: Questa tecnica evita di informare un nodo su una destinazione raggiungibile solo tramite esso. In pratica, un router non pubblicizza una rotta a un nodo se quella rotta è stata appresa proprio da quel nodo. Questo riduce la possibilità di creare loop di routing. Si inviano distance vector differenziati in cui si omettono tutte le distanze da nodi che vedono il ricevente come gateway. - **Triggered Update**: Invece di aspettare il prossimo aggiornamento periodico, un router invia immediatamente un aggiornamento

quando rileva un cambiamento nella topologia della rete. Questo accelera la convergenza della rete, riducendo il tempo in cui le informazioni di routing sono incoerenti.

Queste tecniche combinate migliorano la stabilità e l'affidabilità del protocollo RIP, riducendo la probabilità di loop di routing e accelerando la convergenza della rete. La presenza di clicli potrbbe comprometterne l'efficacia, dunque si è reso indispensabile trovare un' alternativa alla soluzione del routing distance vector.

Routing Link State

Un protocollo di routing di tipo link-state, nonostante entrambe siano definizioni ideali dei prtocolli e non implementative, funziona in modo diverso rispetto ai protocolli di routing a Distance Vector infatti in questa nuova soluzione, si separano nettamente il protocollo e l'algoritmo. Abbiamo una logica in cui, tramite uno specifico protocollo, i nodi scoprono altri nodi, estrapolano informazioni da questi ultimi e condividono tali informazioni con altri nodi. Questo processo permette a tutti i nodi di avere una visione completa della rete.Solo a questo punto si utilizzano algoritmi di routing come Dijkstra per scoprire i percorsi più rapidi. Questo approccio comporta un maggiore utilizzo di memoria e una maggiore complessità computazionale. Tuttavia, se ogni nodo conosce tutta la rete, sarà in grado di reagire opportunamente in caso di guasto.

Conoscenza della Topologia Completa:Ogni router mantiene una mappa completa della topologia della rete, conosciuta come la Link-State Database (LSDB). Questa mappa include informazioni su tutti i router e i collegamenti nella rete.

Annunci di Stato del Collegamento (LSA):I router inviano periodicamente annunci di stato del collegamento (Link-State Advertisements, LSA) ai loro vicini.Gli LSA contengono informazioni sui collegamenti diretti del router, come lo stato del collegamento e il costo associato.

Dijkstra: Ogni router utilizza l'algoritmo di Dijkstra per calcolare il percorso più breve verso ogni destinazione nella rete. L'algoritmo di Dijkstra utilizza le informazioni contenute nella LSDB per costruire un albero dei percorsi più brevi, noto come Shortest Path Tree (SPT).

Vantaggi del Routing Link State

Convergenza rapida: Poiché ogni nodo ha una visione completa della rete, le modifiche nella topologia vengono propagate rapidamente.

Percorsi ottimali: Utilizzando algoritmi come Dijkstra, i percorsi calcolati sono generalmente più efficienti.

Maggiore affidabilità: La conoscenza completa della rete permette di gestire meglio i guasti e le variazioni nella topologia.

Svantaggi del Routing Link State

Maggiore utilizzo di memoria: Ogni nodo deve memorizzare una copia completa della topologia della rete.

Maggiore complessità computazionale: Gli algoritmi di calcolo dei percorsi, come Dijkstra, richiedono più risorse computazionali.

Overhead di comunicazione: La necessità di scambiare informazioni di stato tra i nodi può generare un significativo overhead di comunicazione.

Processo di Routing Link State

1. **Scoperta dei vicini**: Ogni nodo scopre i nodi vicini tramite messaggi di **Hello Packet**.
2. **Misurazione della distanza dai vicini**: Calcolo della distanza dai vicini tramite un messaggio **Echo Packet**.
3. **Scambio di informazioni**: I nodi scambiano informazioni di stato tramite pacchetti di **Link State Advertisement (LSA)** contenenti: la lista dei propri vicini ed il peso del loro collegamento. I pacchetti LSA sono trasmessi con il flooding (simile al broadcast con alcune attenzioni in più), facendo attenzione a non rimandarli da dove sono già provenuti, a scartare pacchetti già visti o temporalmente più vecchi di altri già ricevuti.
4. **Dijkstra** : A questo pinto abbiamo il nostro grafo su cui applicare Dijkstra:
    1. **Inizializzazione**:
    - Assegna una distanza iniziale di 0 al nodo sorgente e di infinito a tutti gli altri nodi.
    - Crea un insieme di nodi non visitati.
    2. **Selezione del nodo corrente**:
    - Seleziona il nodo non visitato con la distanza minore (inizialmente il nodo sorgente).
    3. **Aggiornamento delle distanze**:
    - Per ogni nodo adiacente al nodo corrente, calcola la distanza totale dal nodo sorgente passando per il nodo corrente.
    - Se questa distanza è minore della distanza attualmente registrata per il nodo adiacente, aggiorna la distanza.
    4. **Marcatura del nodo come visitato**:
    - Una volta esaminati tutti i nodi adiacenti, marca il nodo corrente come visitato (non sarà più considerato).
    5. **Ripetizione**:
    - Ripeti i passaggi 2-4 fino a quando tutti i nodi sono stati visitati o la distanza minore tra i nodi non visitati è infinita.
    6. **Costruzione del percorso**:
    - Una volta completato l'algoritmo, la distanza registrata per ogni nodo rappresenta la distanza minima dal nodo sorgente.
    - È possibile ricostruire il percorso più breve tracciando indietro dai nodi di destinazione al nodo sorgente utilizzando le distanze registrate.

Esempi di Protocolli Link State

- **OSPF (Open Shortest Path First)**: Un protocollo di routing link state ampiamente utilizzato nelle reti IP.
- **IS-IS (Intermediate System to Intermediate System)**: Un altro protocollo di routing link state utilizzato principalmente nelle reti di grandi dimensioni.

Router IP

Funzioni dei router

Routing: Determina il percorso ottimale per i pacchetti di dati attraverso la rete utilizzando algoritmi e tabelle di instradamento volto allo scambio di informazioni in maniera ottimale.

Forwarding: Inoltra i pacchetti di dati ricevuti verso la loro destinazione finale basandosi sulle informazioni contenute nella tabella di forwarding.

Switching: Gestisce il trasferimento dei pacchetti tra le diverse interfacce del router, garantendo un flusso di dati efficiente, ovvero l'istaradamento fisico sull'opportuna interfaccia.

Trasmissione: Invio fisico dei pacchetti di dati attraverso la rete utilizzando i protocolli di livello inferiore, come Ethernet o Wi-Fi.

Classificazione dei Router

- **SOHO (Small Office/Home Office)**:Router progettati per piccoli uffici o ambienti domestici.
    - **Caratteristiche**: Solitamente offrono funzionalità di base come NAT, firewall, e supporto per connessioni Wi-Fi.
    - **Prestazioni**: Capacità di gestire un numero limitato di dispositivi e traffico moderato. Velocità di throughput tipicamente tra 100 Mbps e 1 Gbps.
- **Access Router**: Router utilizzati per connettere dispositivi finali a una rete più ampia.
    - **Caratteristiche**: Supportano funzionalità avanzate come QoS (Quality of Service), VPN (Virtual Private Network), e gestione delle VLAN (Virtual Local Area Network).
    - **Prestazioni**: Progettati per gestire un numero maggiore di dispositivi rispetto ai router SOHO, con throughput che può variare da 1 Gbps a 10 Gbps.
- **Enterprise Router**: Router destinati a grandi aziende e organizzazioni.
    - **Caratteristiche**: Offrono funzionalità avanzate di sicurezza, gestione del traffico, e supporto per protocolli di routing complessi come OSPF e BGP.
    - **Prestazioni**: Capacità di gestire un elevato volume di traffico e numerosi dispositivi. Velocità di throughput tipicamente superiori a 10 Gbps, con supporto per connessioni multiple ad alta velocità.
- **Backbone Router**: Router utilizzati nelle dorsali di rete per instradare il traffico tra diverse reti.
    - **Caratteristiche**: Progettati per alta affidabilità e prestazioni, con supporto per protocolli di routing avanzati e capacità di gestire grandi volumi di traffico.
    - **Prestazioni**: Velocità di throughput estremamente elevate, spesso superiori a 100 Gbps. Capacità di gestire migliaia di connessioni simultanee e instradare traffico su lunghe distanze.

Tabelle di Routing e Forwarding

Routing table: Conosciuta anche come **RIB** (Routing Information Base), contiene i prefissi di routing, i next hop, e le metriche. È quindi un insieme di dati grezzi su cui si basano i calcoli di instradamento. Queste informazioni derivano da una serie di protocolli o canali considerati affidabili, sia in termini assoluti che relativi rispetto ad altri.

Forwarding table: Nota anche come **FIB** (Forwarding Information Base), è ottimizzata per l'inoltro rapido dei datagrammi. Su di essa si basa lo scambio di pacchetti, ed è generata a partire dalla RIB. Da quest'ultima si estraggono, tra tutte le informazioni considerate affidabili, quelle più utili all'inoltro dei pacchetti. Questo processo avviene grazie alla funzione chiamata **Route Selection Process**, che seleziona le rotte migliori per la FIB. Contestualmente, la produzione della FIB genera anche dati di output per i protocolli consentendo di decidere quali informazioni comunicare agli altri nodi. Questo meccanismo offre una notevole flessibilità nel recepire, filtrare e inviare informazioni in base alle esigenze specifiche di ogni singolo router.

Instradamento nell’Internet globale

Routing gerarchico: In Internet, il routing è organizzato gerarchicamente in **sistemi autonomi (AS)**, ciascuno identificato da un numero progressivo. Ogni AS gestisce autonomamente le proprie politiche di routing, risolvendo internamente i problemi e importando solo le soluzioni identificate all'esterno. Questo approccio è necessario per gestire la rete in modo efficiente, data la diversità degli oggetti operanti in rete.

Protocolli di routing:

- **Interior Gateway Protocol (IGP)**: Gestisce il routing all’interno di un AS.
- **Exterior Gateway Protocol (EGP)**: Gestisce il routing tra AS diversi, presenta diverse limitazioni, tra cui la mancanza di supporto per il routing dinamico e la scalabilità limitata.
- **Border Gateway Protocol (BGP)**: Successore di EGP.

Sistemi Autonomi (AS)

Un AS è un insieme di router gestiti da un’unica amministrazione e usa un unico protocollo di routing. Con CIDR, un AS è identificato da un insieme di prefissi IP gestiti in modo unitario. In sintesi estrema potremmo dire che è l'insieme di un prefisso di network. GARR (rete italiana degli enti di ricerca), infatti l'Unibo da sola non è un AS ma passa attraverso il GARR come tante altre università finendo per risultare un unico AS.

Un AS svolge compiti di import e di export rispettivamente:

- **Import**: L'AS riceve e accetta le rotte pubblicizzate da altri AS ritenuti affidabili, aggiornando le proprie tabelle di routing per includere queste nuove rotte.
- **Export**: L'AS pubblicizza le proprie rotte e le rotte apprese da altri AS verso i suoi vicini che, qualora lo ritenessero affidabile, permetterebbero loro di aggiornare le proprie tabelle di routing con queste informazioni. (RADb sito per sperimentare questo genere di cose)

Internet Service Provider (ISP)

Organizzazione che fornisce servizi per l'utilizzo di Internet e che solitamente si registra come AS.

Classificazione:

- **Tier 1**: ISP con copertura globale, non necessariamente tutto il mondo, ma grandi coperture su intere **internet region**, ovvero porzioni di aree geografiche coperte da una connessione internet, senza necessità di acquistare connettività.
- **Tier 2**: Acquista connettività da Tier 1.
- **Tier 3**: ISP locali che acquistano connettività da Tier 2 o altri ISP locali.

Peering e interconnessione: Il peering tra ISP non implica pagamenti diretti; è una relazione neutrale. Gli ISP nelle loro zone di pertinenza hanno dei POP (Points of Presence) che sono punti di raccolta collegati tra loro da maglie. Tali POP si trovano in punti strategici come città e snodi commerciali. Se ci sono più ISP in una stessa internet region, i POP saranno in posizioni limitrofe per entrambi gli ISP. Tuttavia, non è quasi mai possibile farli comunicare direttamente, poiché gli ISP si propongono come AS e quindi sarà necessario far avvenire la comunicazione in un punto di "contatto" che talvolta potrebbe essere molto distante dal POP geograficamente più vicino. Tale collegamento unico deve essere molto robusto data la sua unicità. Esso è fornito da compagnie dette **Internet Exchange** che forniscono tale infrastruttura detta **Internet Exchange Point** (IXP).

Stub Area e Routing verso l'Esterno

Le **stub area** sono progettate per ottimizzare le risorse di rete in configurazioni con un solo punto di uscita. Il routing verso l'esterno si basa su un **default route**, riducendo la dimensione delle **tabelle di routing** e il carico sui router di bordo, ideali per le aree con basse risorse di memoria.

Multicast e IP Multicast

Multicast rappresenta una soluzione efficace per la trasmissione di dati a più destinatari simultaneamente, riducendo il carico di traffico di routing. A differenza del broadcast, che invia informazioni a tutti i nodi della rete, il multicast consente di inviare pacchetti solo ai gruppi specifici di destinatari che si sono registrati per riceverli. Questo approccio è particolarmente utile in applicazioni come lo streaming video e le videoconferenze.

Indirizzi multicast: Gli indirizzi IP multicast sono assegnati a un intervallo specifico, compreso tra 224.0.0.0 e 239.255.255.255. Questi indirizzi permettono l'identificazione di gruppi multicast e sono utilizzati dai router per instradare i pacchetti solo ai nodi interessati, contribuendo così a una gestione più efficiente della larghezza di banda.

Internet Group Management Protocol (IGMP)

L'IGMP è un protocollo fondamentale per la gestione dei gruppi multicast. Consente agli host di comunicare con i router multicast, dichiarando la loro appartenenza a specifici gruppi. Attraverso IGMP, gli host possono anche abbandonare i gruppi a cui non desiderano più partecipare. Questo processo è cruciale per mantenere l'efficienza della rete, poiché garantisce che solo gli host interessati ricevano i dati multicast.

Protocollo RIP (Routing Information Protocol)

RIP è un protocollo di routing di tipo **distance vector**, il che significa che le sue decisioni di routing si basano sulla distanza in termini di hop count. Utilizza messaggi di tipo **Request** per richiedere informazioni di routing e **Response** per inviare aggiornamenti agli altri router della rete. Questi aggiornamenti vengono inviati periodicamente, come risposta a una richiesta esplicita e quando un'informazione di routing cambia (triggered update). RIP è semplice da configurare e gestire, ma presenta limiti significativi. Non supporta il **Classless Inter-Domain Routing (CIDR)**, che consente un uso più efficiente degli indirizzi IP, e ha problemi di sicurezza poiché le informazioni di routing vengono trasmesse in chiaro. Inoltre, in reti di grandi dimensioni, il tempo necessario per convergere può diventare critico, portando a potenziali loop di routing e inefficienze.

Struttura del pacchetto: I pacchetti RIP hanno una lunghezza variabile fino a 512 byte e sono strutturati su parole da 32 bit:

- **Command**: Indica se il pacchetto è una richiesta (Request) o una risposta (Response).
- **Version**: Specifica la versione del protocollo RIP utilizzata.
- **Zero**: Campo riservato, impostato a zero.
- **Address Family Identifier (AFI)**: Indica il tipo di indirizzo contenuto nel campo di indirizzo IP.
- **IP Address**: L'indirizzo IP della rete di destinazione.
- **Metric**: Il numero di hop necessari per raggiungere la rete di destinazione.

Ogni pacchetto RIP può contenere fino a 25 voci di routing, ciascuna delle quali descrive una singola rotta.

Tabella di routing: Ogni tabella di routing contiene:

- **Indirizzo di destinazione**: Un indirizzo IP a 32 bit.
- **Distanza dalla destinazione (metrica)**: In termini di hop-count (ogni link ha peso = 1). La distanza massima (∞) per RIP è pari a 16, al fine di limitare il conteggio all'infinito, rendendolo adatto per reti relativamente piccole.
- **Next-hop**: Il router vicino a cui inviare i datagrammi per la destinazione.
- **Timeout**: Se una route non viene aggiornata dopo un certo numero di secondi (default 180 s), la sua distanza è posta all'infinito (si ipotizza una perdita di connettività).
- **Garbage-collection timer**: Se dopo ulteriori secondi (default 120 s) la route non viene aggiornata, viene eliminata del tutto dalla tabella.

Aggiornamento delle tabelle di routing con RIP: I router RIP inviano periodicamente aggiornamenti delle loro tabelle di routing a tutti i router vicini. Quando un router riceve un aggiornamento, confronta le nuove informazioni con la propria tabella di routing. Se trova una rotta più breve o una nuova rotta, aggiorna la propria tabella di conseguenza. Questo processo continua finché tutte le tabelle di routing nella rete non sono sincronizzate.

Problematiche del Protocollo RIP Il protocollo RIP presenta diverse problematiche che ne limitano l'efficacia e la sicurezza, specialmente nelle reti di grandi dimensioni:

- **Split Horizon**: RIP utilizza la tecnica dello split horizon per prevenire loop di routing. Tuttavia, le risposte (RESPONSE) inviate dalle diverse interfacce possono variare, complicando la gestione delle tabelle di routing.
- **Triggered Update**: RIP supporta gli aggiornamenti immediati (triggered update) per ridurre il tempo di convergenza. In questi aggiornamenti, non è necessario includere tutte le voci della tabella di routing, ma solo quelle appena modificate. Questo può portare a una maggiore efficienza, ma anche a una complessità aggiuntiva nella gestione degli aggiornamenti.
- **Mancanza di Supporto per CIDR**: RIP non supporta il **Classless Inter-Domain Routing (CIDR)**, limitando la flessibilità nella gestione degli indirizzi IP e portando a un uso inefficiente dello spazio di indirizzamento.
- **Sicurezza**: RIP è considerato un protocollo insicuro. Chiunque trasmetta datagrammi dalla porta UDP 520 viene considerato come un router autorizzato. Questo può portare a vulnerabilità significative, come nel seguente esempio di malfunzionamento indotto:
    - Un router non autorizzato trasmette messaggi indicando una distanza di 0 tra se stesso e tutti gli altri nodi della rete.
    - Dopo un certo periodo, tutti i percorsi ottimali convergono su questo router non autorizzato, causando potenziali disservizi e problemi di sicurezza.

Protocollo RIP versione 2

RIP versione 2 introduce miglioramenti significativi rispetto alla versione 1, affrontando alcune delle sue limitazioni principali. Le modifiche includono:

Supporto per Subnetting e CIDR: RIP v2 supporta il subnetting e il Classless Inter-Domain Routing (CIDR), permettendo una gestione più efficiente degli indirizzi IP.

Autenticazione: RIP v2 include meccanismi di autenticazione per migliorare la sicurezza delle informazioni di routing. Questo aiuta a prevenire l'inserimento di informazioni di routing non autorizzate.

Trasporto di Maschere di Sottorete: RIP v2 trasporta le maschere di sottorete insieme agli indirizzi IP, consentendo una maggiore flessibilità nella configurazione delle reti.

- **Struttura dei Pacchetti RIP v2**: I pacchetti RIP v2 mantengono una struttura simile a quella della versione 1, ma con alcune aggiunte:
    - **Command**: Indica se il pacchetto è una richiesta (Request) o una risposta (Response).
    - **Version**: Specifica la versione del protocollo RIP utilizzata (2 per RIP v2).
    - **Zero**: Campo riservato, impostato a zero.
    - **Address Family Identifier (AFI)**: Indica il tipo di indirizzo contenuto nel campo di indirizzo IP.
    - **Route Tag**: Campo aggiuntivo per identificare le rotte esterne.
    - **IP Address**: L'indirizzo IP della rete di destinazione.
    - **Subnet Mask**: La maschera di sottorete associata all'indirizzo IP.
    - **Next Hop**: L'indirizzo IP del prossimo hop verso la destinazione.
    - **Metric**: Il numero di hop necessari per raggiungere la rete di destinazione.

Protocollo Open Shortest Path First (OSPF)

Protocollo di routing largamente adottato, standardizzato nella versione 2 (RFC 2328), e tra i più diffusi nell'ambito delle **reti interne (IGP)**. È di tipo **link-state** e usa pacchetti **Link State Advertisement (LSA)** per condividere informazioni di rete con altri router. OSPF è incapsulato direttamente nel **protocollo IP**, con un protocol number di valore 89 per distinguere i pacchetti OSPF dagli altri. OSPF semplifica il **routing** in reti complesse suddividendole in **aree**, interconnesse tramite un'**area backbone** (Area 0). Questa suddivisione crea una struttura **gerarchica** che riduce il carico sui router e consente la **comunicazione tra aree** tramite router specifici. I principali tipi di router in OSPF includono:

- **Internal Router**, interni a un'area specifica
- **Area Border Router (ABR)**, che collegano più aree
- **Backbone Router**, che gestiscono le connessioni con l'area centrale
- **AS Boundary Router (ASBR)**, responsabili della comunicazione con **Autonomous Systems (AS)** esterni utilizzando protocolli **EGP**

OSPF gestisce vari tipi di **route**:

- **Route intra-area**: informazioni di routing interne all'area
- **Route inter-area**: aggiornamenti tra aree diverse
- **Route esterne**: route da altri protocolli o AS, inoltrate tramite l'**ASBR**

Le aree di OSPF possono assumere configurazioni diverse per ottimizzare il routing:

- **Area normale**: accetta tutte le route
- **Stub area**: utilizza un **default route** per destinazioni esterne, con minori requisiti di memoria
- **Totally stub area**: consente solo route interne e il default route
- **Not So Stubby Area (NSSA)**: permette di importare alcune route esterne, mantenendo limitata la propagazione

OSPF offre funzionalità aggiuntive per migliorare l'efficienza della rete:

- **Bilanciamento del carico**: ripartisce il traffico su percorsi multipli di uguale costo
- **Autenticazione**: protegge lo scambio di informazioni con **password** o **crittografia**

- **Quality of Service (QoS)**: seleziona percorsi in base al **Type of Service**, consentendo livelli di servizio differenziati

Tipologie di Reti Supportate da OSPF

OSPF supporta **reti punto-punto** e **reti multi-accesso**, tra cui **Broadcast Multi-Access (LAN 802)** e **Non-Broadcast Multi-Access** (ad esempio, X.25, ATM). In queste reti, utilizza una struttura a **stella virtuale** per ridurre le connessioni necessarie. In reti multi-accesso, si usano due ruoli chiave:

Designated Router (DR), per ottimizzare la comunicazione. Qui i nodi si accorderanno su che debba essere considerato il disegnato in modo tale da usarlo come centro ed evitare di sovraccaricare gli altri con un flusso inutilmente elevato di pacchetti.

Backup Designated Router (BDR), per garantire **affidabilità** dato che di fatto il diseganto non ha alcuna peculiarità rispetto agli altri.

Identificatori e Priorità dei Router

Ogni router OSPF ha un **Router ID** univoco e può avere una **priorità** (da 0 a 255) per determinare il **Designated Router (DR)**, si anrà infatti a sciegliere chi ha la priorità più alta come ruoter disignato. Nelle reti multi-accesso, il DR coordina le comunicazioni e ottimizza lo scambio di informazioni tra **router adiacenti** ovvero tutti quei router connessi in maniaera diretta e che utilizzano effettivamente tale connessione per comunicare, se non lo facessere nonostante siano collegati direttamente sarebbero detti **router vicini**.

Struttura del Pacchetto OSPF

Il pacchetto OSPF è composto da diverse sezioni chiave, ciascuna con un ruolo specifico nel protocollo:

Header OSPF:

- **Version**: La versione del protocollo OSPF.
- **Type**: Il tipo di pacchetto OSPF (Hello, Database Description, Link State Request, Link State Update, Link State Acknowledge).
- **Packet Length**: La lunghezza totale del pacchetto OSPF.
- **Router ID**: L'identificatore univoco del router che invia il pacchetto.
- **Area ID**: L'identificatore dell'area OSPF da cui proviene il pacchetto.
- **Checksum**: Un valore di controllo per verificare l'integrità del pacchetto.
- **Authentication Type**: Il tipo di autenticazione utilizzato.
- **Authentication**: I dati di autenticazione.

Dati Specifici del Tipo di Pacchetto:

- **Hello Packet**: Contiene informazioni sui vicini, l'intervallo Hello, e il Dead Interval.
- **Database Description Packet**: Include una descrizione del database di stato dei collegamenti.
- **Link State Request Packet**: Richiede informazioni specifiche sullo stato dei collegamenti.
- **Link State Update Packet**: Trasporta aggiornamenti sullo stato dei collegamenti.
- **Link State Acknowledge Packet**: Conferma la ricezione degli aggiornamenti sullo stato dei collegamenti.

Protocolli di Comunicazione in OSPF

OSPF utilizza tre **sottoprotocolli** principali:

- **Hello**: scopre i router vicini e far sapere della propria presenza agli altri, avvia l'elezione del DR e del BDR e costantemente verifica la presenza dei vicini
- **Exchange**: sincronizza i database di **link-state** tra router adiacenti ed avviene solo all'inizio
- **Update**: diffonde le informazioni di routing in tutta la rete via flooding, così facendo si vaa costruire debtro ad ogni router la mappa intera della rete.

I **pacchetti principali** di OSPF includono:

- **Hello** (Tipo 1), per rilevare i vicini
- **Database Description** (Tipo 2), per descrivere il database
- **Link State Request** (Tipo 3) e **Link State Update** (Tipo 4) per l'aggiornamento delle informazioni di routing
- **Link State Acknowledge** (Tipo 5), per confermare la ricezione

Protocolli EGP (Exterior Gateway Protocols)

I protocolli di tipo EGP si distinguono dai protocolli di tipo IGP per le loro finalità e logiche operative:

- All'interno di un Autonomous System (AS), si mira principalmente all'ottimizzazione dei percorsi.
- Nel routing tra AS, si devono considerare soprattutto le politiche di instradamento:
    - Ogni AS preserva la propria autonomia e indipendenza dalle decisioni di altri.
    - Alcuni AS limitano il transito del traffico da altri AS attraverso le loro reti, ciò può dipendere da diversi fattori come per esempio dinamiche geopolitiche o più generalmente da accordi tra AS rendendo dunque lo shorter path non prioritario.
    - In determinati contesti, si seguono accordi internazionali per la gestione del traffico.

Due protocolli principali di tipo EGP utilizzati in Internet sono:

- **Exterior Gateway Protocol (EGP)**, molto vecchio e praticamente abbandonato.
- **Border Gateway Protocol (BGP)**

Border Gateway Protocol (BGP)

Sviluppato per sostituire EGP e attualmente è disponibile nella versione 4 (RFC 1771). I router BGP utilizzano connessioni TCP (porta 179), chiamate sessioni BGP, per uno scambio affidabile delle informazioni di routing:

- **Sessioni BGP esterne (eBGP)** tra router in AS diversi.
- **Sessioni BGP interne (iBGP)** tra router nello stesso AS.

BGP scambia informazioni di raggiungibilità per reti IP secondo lo schema **classless** (CIDR), permettendo un instradamento flessibile e dettagliato.

BGP e Path Vector

BGP utilizza un protocollo di tipo **Path Vector**, un'evoluzione del distance vector, che offre l'**elenco degli AS nel percorso** contenente l'elenco esaustivo degli AS da attraversare per raggiungere uno specifico AS, risolvendo i cicli e permettendo politiche di routing più efficaci. La necessità di conoscere nel dettaglio tutte le path ha portato a un problema di grandezza delle tabelle. La frammentazione degli indirizzi ha reso necessario conservare in memoria "fette" di indirizzi sempre più frammentate, portando a tabelle con righe

nell'ordine di quasi 10^6. Questo comporta una lettura di tali tabelle per l'instradamento di ogni singolo pacchetto. Inoltre, il fenomeno della crescita esponenziale della banda dei collegamenti aggrava la situazione. La combinazione di aumento esponenziale della grandezza delle tabelle e del numero di pacchetti trasportati per secondo rischia di mettere in crisi l'infrastruttura di collegamento.

Politiche di routing:

- **Export policies**: permette il transito solo verso destinazioni consentite.
- **Import policies**: esclude percorsi che coinvolgono AS non conformi alle politiche di routing o non considera le informazioni da esso ricevute.
- **Struttura dei Path Vector**:
    - **Origin**: indica l'origine del percorso (IGP, EGP o incomplete).
    - **AS path**: elenca gli AS da attraversare per raggiungere una destinazione.
    - **Next hop**: specifica l'indirizzo del router di bordo dell'AS che deve essere utilizzato come prossimo passo verso la destinazione.

Caratteristiche degli attributi dei Path Vector:

- **Well-known**: attributi che devono essere riconosciuti da tutti i router BGP.
    - **Mandatory**: attributi well-known che devono essere presenti in ogni aggiornamento BGP.
    - **Discretionary**: attributi well-known che possono essere presenti o meno in un aggiornamento BGP.
- **Optional**: attributi che non devono essere necessariamente riconosciuti da tutti i router BGP.
    - **Transitive**: attributi optional che devono essere trasmessi anche se non riconosciuti.
    - **Non-transitive**: attributi optional che non devono essere trasmessi se non riconosciuti.

Formato dei Messaggi BGP

I messaggi BGP sono strutturati in un formato specifico per garantire la corretta comunicazione tra i router. Ogni messaggio BGP inizia con un header comune, seguito da campi specifici a seconda del tipo di messaggio. L'header comune include:

- **Marker (16 byte)**: Campo utilizzato per la sincronizzazione e la sicurezza.
- **Length (2 byte)**: Lunghezza totale del messaggio BGP, compreso l'header.
- **Type (1 byte)**: Tipo di messaggio BGP (Open, Update, Notification, Keepalive).

A seconda del tipo di messaggio, l'header è seguito da campi specifici:

- **Open**: Include l'ID dell'AS, il numero di versione BGP, il tempo di hold, l'ID del router e i parametri opzionali.
- **Update**: Contiene informazioni sulle rotte da aggiungere o rimuovere, inclusi i prefissi IP e gli attributi del percorso.
- **Notification**: Fornisce dettagli sugli errori riscontrati e chiude la connessione.
- **Keepalive**: Messaggio semplice utilizzato per mantenere attiva la connessione senza trasmettere nuove informazioni di routing.

BGP: Tipi di Messaggi

I messaggi di BGP posso essere di tipo:

Open: inizia una connessione BGP e include identificazione dell'AS, timeout e autenticazione.

Update: trasmette il path vector e relativi attributi.

Notification: notifica errori e chiusura della connessione.

Keepalive: conferma la connessione attiva senza nuove informazioni di routing.

Ifrastruttura regionale italiana

In Italia, l'infrastruttura degli AS è distribuita tra reti private, reti pubbliche e diversi punti di interscambio fondamentali per il traffico Internet nazionale e internazionale. Gli AS italiani sono numerosi e variano per dimensione e scopo: dai provider di servizi Internet (ISP) alle reti aziendali, fino alle reti gestite dalle pubbliche amministrazioni. Due strutture cardine che facilitano l'interconnessione e migliorano l'efficienza del traffico Internet in Italia sono il **Milan Internet Exchange (MIX)** e la rete **LEPIDA**.

Il Ruolo del MIX

Il MIX è uno dei più importanti punti di interscambio di traffico Internet in Italia e uno dei maggiori a livello europeo. Situato a Milano, permette l'interconnessione diretta tra AS di vari operatori, riducendo la latenza e ottimizzando il routing del traffico Internet a livello nazionale e internazionale. Il MIX è una struttura neutrale e indipendente che offre **servizi di peering pubblico e privato**, consentendo ai provider di scambiarsi traffico direttamente. Ciò riduce la necessità di instradare il traffico verso AS esteri, favorendo una maggiore autonomia della rete italiana e migliorando l'efficienza di trasmissione tra reti locali. Questo snodo è particolarmente importante per garantire la connettività tra le grandi reti italiane e l'infrastruttura globale di Internet.

La Rete LEPIDA

LEPIDA è una rete regionale di proprietà pubblica, gestita dalla società Lepida S.p.A., che supporta il sistema di interconnessione digitale per le pubbliche amministrazioni dell'Emilia-Romagna. Nasce con l'obiettivo di interconnettere le amministrazioni pubbliche regionali, migliorando la qualità dei servizi digitali rivolti ai cittadini e garantendo la sicurezza e la gestione diretta delle reti di pubblica utilità. LEPIDA opera anche come AS e stabilisce connessioni con altri AS nazionali e internazionali, facilitando l'accesso a risorse e servizi pubblici in tutta Italia. Grazie a LEPIDA, la Regione Emilia-Romagna gode di un'infrastruttura autonoma e indipendente, riducendo la dipendenza da operatori privati e aumentando la resilienza della rete regionale.

In questo scenario, MIX e LEPIDA contribuiscono a una maggiore autonomia della rete italiana. Il MIX facilita l'interconnessione tra grandi reti commerciali e nazionali, mentre LEPIDA supporta un'infrastruttura dedicata alla pubblica amministrazione, assicurando una comunicazione efficiente e sicura per il settore pubblico e migliorando il servizio per i cittadini e le imprese a livello regionale.

Virtualizzazione di Rete

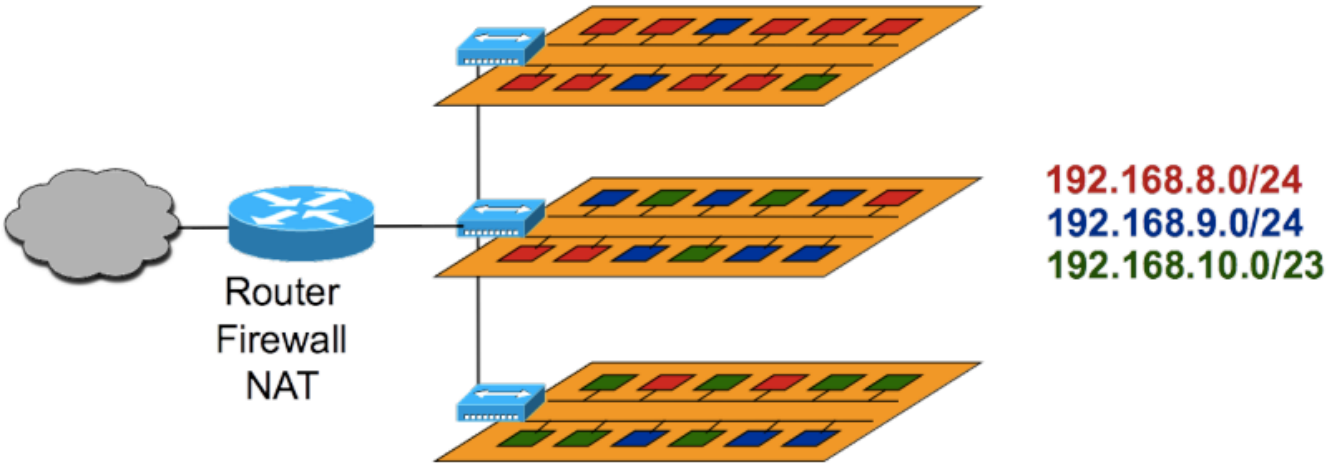
La virtualizzazione di rete permette la creazione di **versioni virtuali di infrastrutture di computazione, memorizzazione e reti**, realizzando componenti che si comportano come sistemi software indipendenti dall'hardware fisico. Questo approccio garantisce vantaggi significativi come la condivisione delle risorse fisiche e il disaccoppiamento tra progetto software e hardware, migliorando flessibilità, mobilità e scalabilità.

Tuttavia, la virtualizzazione comporta criticità legate alla sicurezza e all'isolamento dei sistemi che condividono lo stesso hardware fisico.

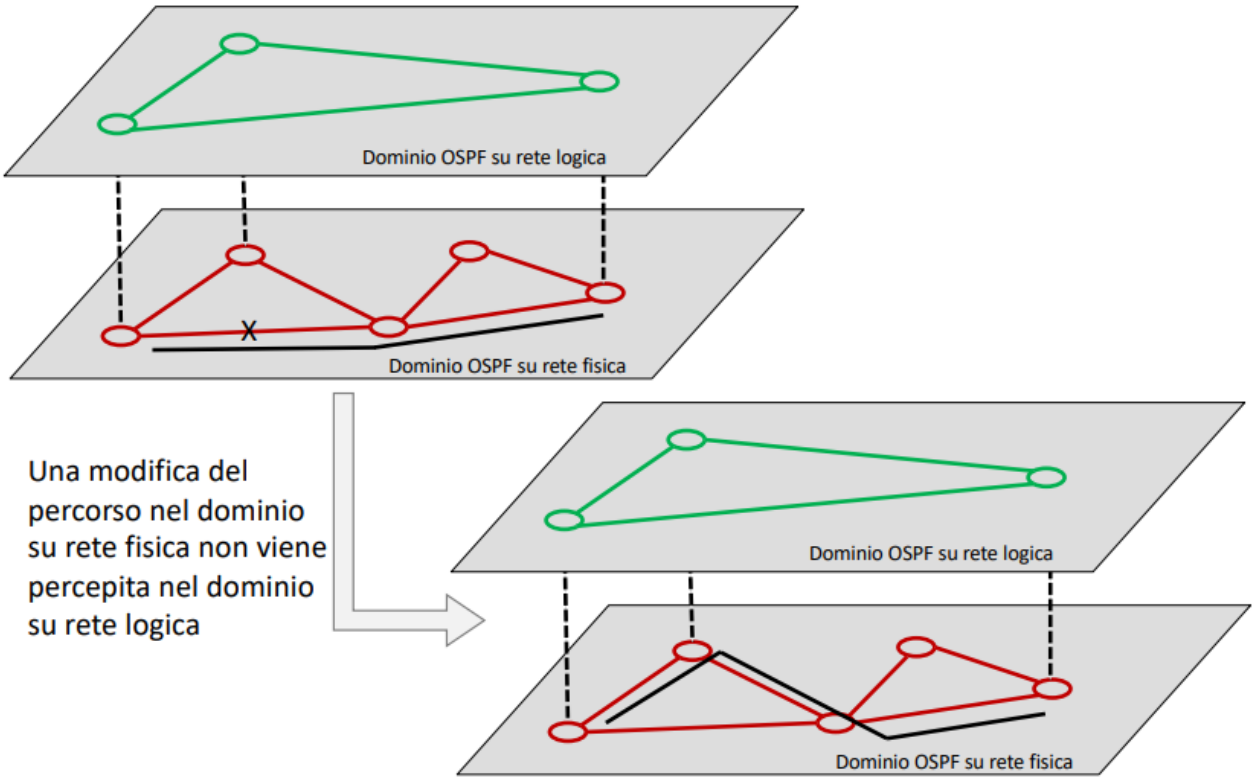
Obiettivo e Tecniche della Virtualizzazione di Rete: La virtualizzazione di rete risponde alla crescente complessità dei requisiti di servizio dell'utenza, consentendo di realizzare topologie o funzionalità su infrastrutture esistenti, altrimenti difficili da modificare. Questo approccio spesso si basa su **reti overlay**, ovvero reti logiche sovrapposte all'infrastruttura fisica per creare funzionalità aggiuntive, le network IP nel loro piccolo ne sono un esempio. Tra le tecnologie che consentono questo tipo di virtualizzazione troviamo **VLAN (IEEE 802.1Q)**, **GRE (RFC 1701)**, **VXLAN (RFC 7348)** e **VPN**, che rappresentano alcune delle soluzioni per segmentare, incapsulare e isolare il traffico di rete virtuale.

Reti Overlay: VLAN, GRE e VXLAN

VLAN (Virtual Local Area Network): Le VLAN creano domini di broadcast separati all'interno della stessa rete fisica, migliorando sicurezza e prestazioni. VLAN statiche e dinamiche permettono una gestione ottimizzata delle risorse, mentre l'uso del protocollo IEEE 802.1Q facilita l'instradamento su più switch.



GRE (Generic Routing Encapsulation): GRE permette l'incapsulamento di pacchetti su protocollo IP, creando un overlay di routing che separa logica e rete fisica, se analizzassimo dunque il pacchetto non vedremmo l'originale indirizzo IP ma quello che gli abbiamo attribito. Il GRE ha un header specifico che gli permette di specificare il protocollo contenuto ed altri parametri opzionali. Grazie al GRE potrò creare dei tunnel fittizi che vanno a modellare la topologia della rete, così facendo posso astrarre una rete fittizia che non varia al variare, dovuto per esempio ad una rottura, della rete fisica.



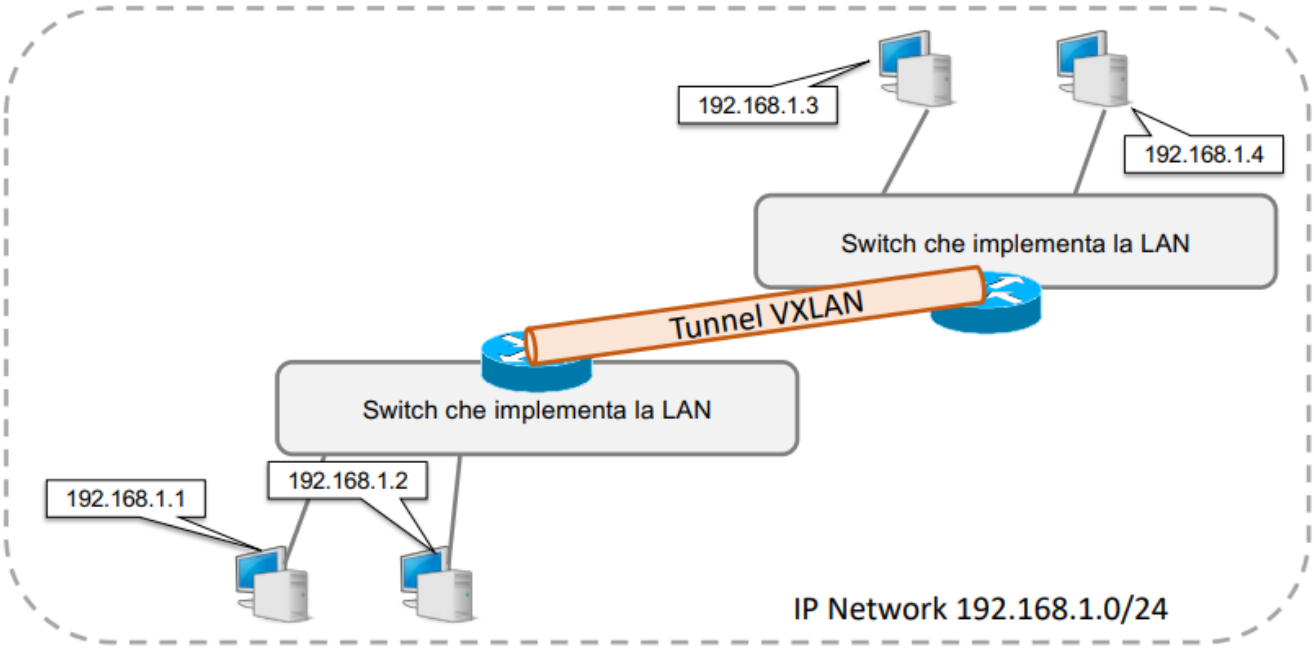
VXLAN (Virtual eXtensible LAN): VXLAN, ampiamente usato nel cloud computing, consente l'incapsulamento di traffico Layer 2 in pacchetti UDP, garantendo un isolamento scalabile con identificatori unici per ciascun segmento. Creado un tunnel VXLAN ottengo la fusione di 2 LAN distinte dato che grazie al tunnel esse **risponderanno alla stessa ARP request**. Il tunnel VXLAN funziona incapsulando i frame Ethernet in pacchetti UDP, che vengono poi trasmessi attraverso una rete IP. Ogni segmento VXLAN è identificato da un **VXLAN Network Identifier (VNI)**, che consente di isolare il traffico tra diversi segmenti. I dispositivi che terminano i tunnel VXLAN, noti come **VXLAN Tunnel Endpoints (VTEP)**, aggiungono e rimuovono l'incapsulamento VXLAN. Quando un frame Ethernet entra in un VTEP, viene incapsulato in un pacchetto UDP con un header VXLAN e inviato attraverso la rete IP. Il VTEP di destinazione rimuove l'incapsulamento e inoltra il frame Ethernet alla rete locale.

Nonostante i vantaggi, l'uso di VXLAN può introdurre alcuni problemi di prestazione:

Overhead di Incapsulamento: L'aggiunta di header VXLAN e UDP aumenta la dimensione dei pacchetti, riducendo l'efficienza della trasmissione e aumentando il carico sulla rete.

Latenza: L'incapsulamento e il decapsulamento dei pacchetti richiedono tempo di elaborazione aggiuntivo, che può aumentare la latenza end-to-end.

Fragmentazione dei Pacchetti: L'aumento della dimensione dei pacchetti può causare la frammentazione, che a sua volta può ridurre le prestazioni e aumentare il rischio di perdita di pacchetti.



Virtual LAN

Una VLAN permette di creare più LAN separate su un unico switch. Ogni VLAN è un dominio di broadcast separato. Se una VLAN corrisponde a una rete IP, i broadcast di una rete non raggiungono gli host di un'altra. Senza VLAN, i broadcast inviati da un host possono raggiungere tutti gli altri host sulla stessa rete fisica, causando congestione e riducendo le prestazioni. Con le VLAN, i broadcast sono limitati al **broadcast domain** (dominio broadcast) della VLAN specifica, migliorando l'efficienza della rete e riducendo il traffico non necessario. Questo impatta anche sulla sicurezza, dato che un soggetto di un dominio broadcast non potrà conoscere attraverso un broadcast soggetti esterni al suo dominio.

Classificazione delle VLAN

VLAN statiche (Port-Based):

- Ogni porta dello switch è associata a una VLAN specifica.
- Gli host appartengono alla VLAN corrispondente alla porta a cui sono connessi.
- Cambiare VLAN di un host richiede la riconfigurazione dello switch.
- Lo switch determina la VLAN di un host in base alla configurazione della porta di connessione.
- Configurazione tipica per semplificare la gestione in ambienti con strutture di rete fisse.

VLAN dinamiche:

- Prateicamente non più utilizzata.
- L'appartenenza alla VLAN dipende dall'indirizzo dell'host (MAC o IP).
- Gli host rimangono nella VLAN assegnata indipendentemente dalla porta di connessione.
- Cambiare VLAN richiede la modifica della configurazione associata all'indirizzo dell'host.

LAN Estesa e Gestione delle VLAN tra Switch

- **Definizione**: Una LAN estesa utilizza più switch per gestire una rete più ampia, mantenendo separazione tra VLAN.

- **Problema**: Come assicurare che le VLAN rimangano distinte e funzionino correttamente su switch multipli.

Protocollo IEEE 802.1Q

- **Funzione**: Consente l'uso delle stesse VLAN su più switch interconnessi.
- **Tagging VLAN**:
    - Aggiunta di un'etichetta (tag) nell'intestazione Ethernet per identificare la VLAN di appartenenza.
    - **Header IEEE 802.1Q**:
        - **4 byte** aggiunti al frame Ethernet:
            - **Tag Protocol Identifier (TPID)**: 16 bit, solitamente 0x8100.
            - **Priority**: 3 bit per la priorità del traffico.
            - **CFI**: 1 bit, formato del MAC address.
            - **VID**: 12 bit, identifica la VLAN (da 0 a 4095).
- **Modalità delle porte di uno switch**

1. **Access Mode**:
    - Porta associata a una sola VLAN.
    - Nessun tagging 802.1Q richiesto.
    - Ideale per porte collegate agli host.
2. **Trunk Mode**:
    - Porta associata a VLAN multiple.
    - Richiede il tagging 802.1Q per identificare la VLAN dei frame Ethernet.
    - Configurazioni:
        - Una VLAN "untagged" per il traffico non taggato.
        - Più VLAN "tagged".
    - Tipica per connessioni tra switch o router.

Reti Private Virtuali (VPN) e la Sicurezza del Tunneling

Le **VPN** sono reti sovrapposte su reti pubbliche che garantiscono connessioni sicure attraverso il **tunneling cifrato** e l'**autenticazione**. Esistono principalmente due tipologie di VPN:

Roadwarrior VPN: Questo tipo di VPN è configurato per offrire accesso sicuro a utenti singoli che si collegano da punti remoti, creando connessioni sicure punto-punto verso un server VPN dedicato capace di gestire una rete a stella tra client molteplici. Tuttavia, questa configurazione, se utilizzata da un elevato numero di dispositivi, può comportare un **overhead significativo** poiché richiede un tunnel per ogni dispositivo. Lo si può utilizzare per emulare un'altra posizione geografica grazie al fatto che, se il server si trova in un'internet region diversa dalla propria, il ricevente è convinto che i propri messaggi arrivino da quell'internet region. Questa metodologia è funzionale solo se gli host si trovano de-localizzati sulla rete; se invece sono co-localizzati ci sarà un grande spreco di computazione.

Net-to-Net VPN: Le Net-to-Net VPN collegano intere LAN o reti IP tramite un unico tunnel cifrato, sfruttando un canale sicuro su rete pubblica, agendo sui gateway di uscita dalla nostra network IP e quelli di ingresso dell'host ricevente. I pacchetti vengono criptati nel tunnel, mentre l'indirizzamento IP reale può essere mascherato, garantendo così privacy e sicurezza nelle connessioni tra sedi aziendali distribuite. Questo tipo di

VPN è particolarmente adatto per reti aziendali, poiché consente di ridurre il numero di connessioni dirette necessarie.

IPsec per la Sicurezza delle VPN

Lo standard **IPsec (Internet Protocol Security)** è il principale protocollo per la cifratura e autenticazione dei dati trasmessi su reti pubbliche tramite VPN. Offre due modalità principali: **Transport Mode** (che protegge solo i dati dell'utente) e **Tunnel Mode** (che protegge l'intero pacchetto IP). Gli elementi principali di IPsec sono:

IKE (Internet Key Exchange): È il protocollo di negoziazione che autentica i partecipanti alla VPN, negoziando algoritmi crittografici e chiavi, utilizzando UDP che supporta porta sorgente e destinazione 500, ciò comporta che se sulla path troviamo una NAT si potrebbe incappare in una problematica data dal cambio di porta.

AH (Authentication Header) e **ESP (Encapsulating Security Payload)**: AH assicura autenticità, integrità dei pacchetti e identità del mittente, mentre ESP include anche la riservatezza attraverso la cifratura icapsulando il pacchetto e dunque esponedolo a frammentazione durante il trasporto dato che ne aumenta le dimensioni. Con **ESP Transoprt** cifro solo il contenuto mentre con **ESP Tunnel** cifro l'intero pacchetto comprensivo di IP.

Mezzi Trasmissivi

La **Legge di Edholm** prevede che la larghezza di banda delle reti di telecomunicazione raddoppi ogni 18 mesi.

Attenuazione

L'attenuazione è la riduzione della potenza del segnale man mano che si propaga attraverso un mezzo trasmissivo. L'attenuazione è misurata in decibel per kilometro (dB/km). L'attenuazione è un parametro critico nella progettazione delle reti di telecomunicazione, poiché influisce sulla qualità e sulla distanza massima di trasmissione del segnale.

L'**attenuazione sul rame** crese esponenzialmente con la lunghezza del collegamento e con la radice della frequeza del seganle, avrà dunque un fattore di dispersione olto altro che si quantifica con la formula:

$$A = 10 \log_{10} \left(\frac{P_t}{P_r} \right) = a \sqrt{f} L$$

Per limitare l'attenuazione di usa la tecnica del **twined pair** che consiste nel arrotolare a spirale le coppie per contenere la dimendione del campo generato e dunque la sua dispersione, ne esistono di 2 tipi: **STP** schemati da un conduttore e **UTP** non schermati. I **Coassiali** permettono di raggiungere distaze maggiori.

L'**attenuazione delle Radio Comunicazioni** è la diminuzione della potenza del segnale radio mentre si propaga attraverso l'aria o altri mezzi. Questo fenomeno è influenzato da vari fattori, tra cui la distanza tra il trasmettitore e il ricevitore, la frequenza del segnale, le condizioni atmosferiche e la presenza di ostacoli fisici come edifici o montagne. Ad esempio, l'attenuazione cresce in maniera polinomiale con il quadrato della frequenza, e le antenne diventano più efficaci quando la frequenza aumenta.

Comunicazione Satellitare

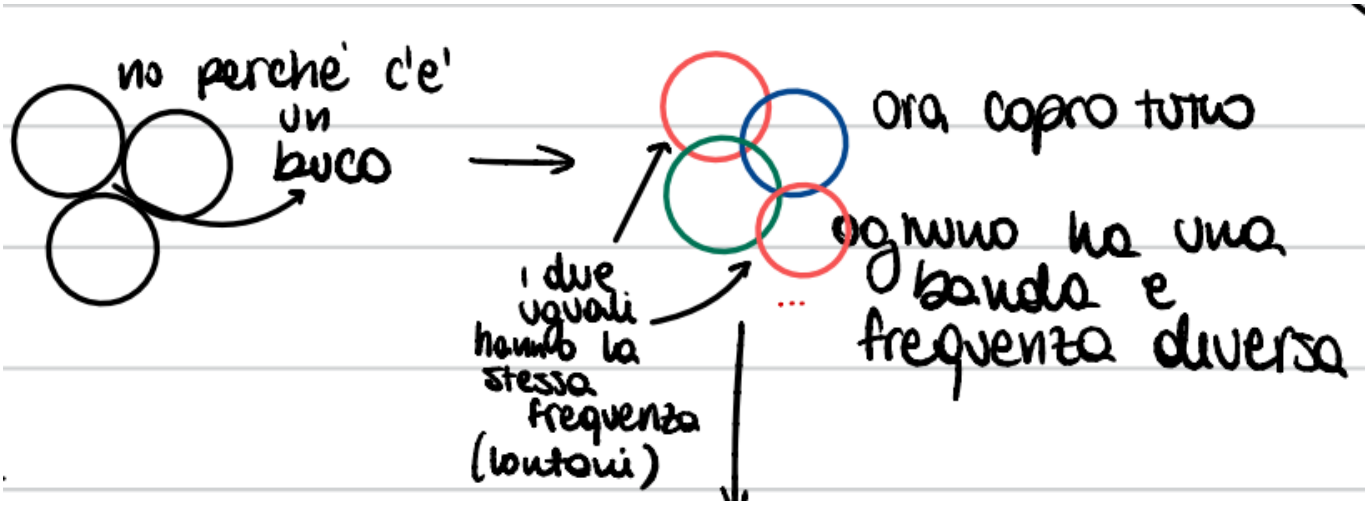
La **propagazione ionosferica** è un fenomeno in cui le onde radio vengono riflesse o rifratte dalla ionosfera, uno strato dell'atmosfera terrestre carico di particelle ionizzate. Questo tipo di propagazione permette alle onde radio di coprire distanze molto maggiori rispetto alla propagazione diretta, rendendola utile per le comunicazioni a lunga distanza, come quelle utilizzate nelle trasmissioni radio a onde corte. Attualmente, l'utilizzo della ionosfera è stato superato grazie ai **satelliti in orbita geostazionaria**, che svolgono lo stesso lavoro ad un'altezza maggiore e con una portata più ampia. Tuttavia, poiché le orbite geostazionarie sono limitate, si possono utilizzare **satelliti non stazionari** che orbitano più vicino alla Terra. Questi satelliti sono più facili da installare ma non rimangono fissi, quindi è necessario averne un numero maggiore per garantire una copertura continua.

Telefonia Cellulare

L'obiettivo iniziale della telefonia cellulare era incrementare il numero di terminali per ridurre i costi elevati della tecnologia e delle infrastrutture, rendendo il servizio più accessibile a un numero crescente di utenti.

Sviluppo delle Celle: per aumentare l'efficienza e ridurre i costi, le reti cellulari sono state organizzate in celle, piccole aree coperte ciascuna da un'antenna. Questa struttura permette di servire molti utenti all'interno di un'area circoscritta, migliorando la capacità complessiva della rete e permettendo un uso efficiente delle frequenze disponibili.

Gestione della Copertura: ogni cella è progettata per supportare un certo numero di chiamate simultanee, e le celle sono posizionate in modo da garantire che, anche se un utente si sposta da una cella all'altra, il servizio rimanga continuo. Le celle si sovrapporranno dunque in alcuni punti, questo va però ad evitare che si formino degli spazi non coperti.



Fibra Ottica

La fibra ottica ha rivoluzionato le reti di telecomunicazione, sostituendo progressivamente il rame nella rete di trasporto a partire dagli anni 2000. Con una larghezza di banda significativamente superiore, la fibra ottica supporta la trasmissione di grandi quantità di dati su lunghe distanze con una minima perdita di segnale, migliorando drasticamente la qualità e l'affidabilità delle comunicazioni.

Caratteristiche: le fibre ottiche sono sottili filamenti di vetro o plastica che trasportano dati sotto forma di impulsi luminosi. La fibra offre un'elevata capacità di trasporto dati e una bassa attenuazione, rendendola ideale per le tratte di lunga distanza. Negli anni, la tecnologia della fibra ha permesso di superare i limiti fisici delle trasmissioni terrestri e transoceaniche, anche in condizioni complesse come il fondo marino.

Innovazioni: grazie alla tecnica del **multiplexing a lunghezza d'onda (WDM)**, è possibile trasmettere simultaneamente più flussi di dati su diverse frequenze di luce all'interno dello stesso cavo in fibra ottica. Questo approccio sfrutta la scarsa selettività della fibra rispetto al colore della luce, permettendo a una singola fibra di trasportare diversi flussi di dati ad alta velocità, aumentando così la capacità totale di trasmissione senza necessità di nuovi cavi.

Manutenzione e Sicurezza della Fibra Ottica

- **Giunzione e Allineamento**: le fibre ottiche devono essere giuntate con estrema precisione per evitare perdite di segnale e dispersione della luce, che potrebbero compromettere la qualità della trasmissione. Le giunzioni possono essere permanenti o temporanee, ma in entrambi i casi è fondamentale un allineamento perfetto tra i segmenti di fibra per garantire un'efficienza ottimale.
- **Problemi di Sicurezza nelle Lunghe Tratte**: nelle tratte di lunga distanza, specialmente nelle trasmissioni transoceaniche, emergono problemi di sicurezza e manutenzione. Le lunghe distanze e la difficoltà di accesso rendono complicato il monitoraggio e la protezione delle fibre da potenziali danni o manomissioni. Per garantire sicurezza e affidabilità, sono necessari sistemi di sorveglianza avanzati e misure di protezione che preservino l'integrità del segnale su queste distanze estese.

Micro-Electro-Mechanical Systems

I MEM (Micro-Electro-Mechanical Systems) sono dispositivi miniaturizzati che combinano componenti meccanici ed elettrici su un singolo chip di silicio. Funzionano attraverso l'integrazione di sensori, attuatori e circuiti elettronici, permettendo la rilevazione e la manipolazione di segnali fisici. Nei sistemi di telecomunicazione, i MEM vengono applicati in matrici per creare **switch ottici**, utilizzati per instradare segnali luminosi nelle reti in fibra ottica. Questi switch sfruttano micro-specchi mobili per deviare i fasci di luce, consentendo una commutazione rapida e precisa dei segnali ottici senza conversione elettrica, migliorando l'efficienza e la velocità delle reti di comunicazione.

Arrayed Waveguide Grating

L'Arrayed Waveguide Grating (AWG) è un dispositivo ottico utilizzato nelle reti di telecomunicazione per la multiplazione e demultiplazione di segnali ottici. Funziona sfruttando la differenza di percorso ottico tra una serie di guide d'onda disposte in modo da creare interferenze costruttive e distruttive. Questo permette di separare o combinare diverse lunghezze d'onda della luce, rendendo l'AWG fondamentale per il **Wavelength Division Multiplexing (WDM)**. Grazie alla sua capacità di gestire molteplici canali ottici simultaneamente, l'AWG è essenziale per aumentare la capacità di trasmissione delle reti in fibra ottica, migliorando l'efficienza e la scalabilità delle comunicazioni ottiche.

Divisione Geografica in Zone Bianche, Grigie e Nere

La divisione geografica in zone bianche, grigie e nere è una classificazione utilizzata per identificare le aree in base alla disponibilità e alla qualità delle infrastrutture di rete a banda larga. Le **zone bianche** sono aree in cui non esiste alcuna infrastruttura di rete a banda larga e non sono previsti investimenti privati nei prossimi tre anni qui sarà necessario un interveto publico per costruire un infrastruttura che ad un ente privato potrebbe risultare non conveniente. Le **zone grigie** sono aree in cui è presente un solo operatore di rete a banda larga, con una copertura limitata e una qualità del servizio che potrebbe non essere sufficiente per soddisfare le esigenze future. Le **zone nere** sono aree in cui sono presenti almeno due operatori di rete a banda larga che offrono servizi competitivi e di alta qualità. Questa classificazione è utilizzata per indirizzare gli investimenti

pubblici e privati, promuovendo lo sviluppo delle infrastrutture di rete nelle zone meno servite e garantendo un accesso equo e diffuso alla banda larga su tutto il territorio.

Multiprotocol Label Switching

I **Router** instradano datagrammi IP usando la tecnica del **longest prefix match** e supportano funzionalità come il **filtering dei pacchetti** e la **qualità del servizio (QoS)**, gli **Switch** invece si occupano di instradamento semplice in base ad indirizzi statici, con un rapporto costo/prestazioni più vantaggioso rispetto ai router. Il Multiprotocol Label Switching (MPLS) mira a combinare la velocità dello switching con la flessibilità dell'instradamento IP, migliorando il costo/prestazioni nella rete, ciò è basato sui protocolli di rete convenzionali e associazione delle etichette (label) sulla base delle quali si utilizza hardware veloce per l'identificazione ed istradamento.

Vantaggi di MPLS:

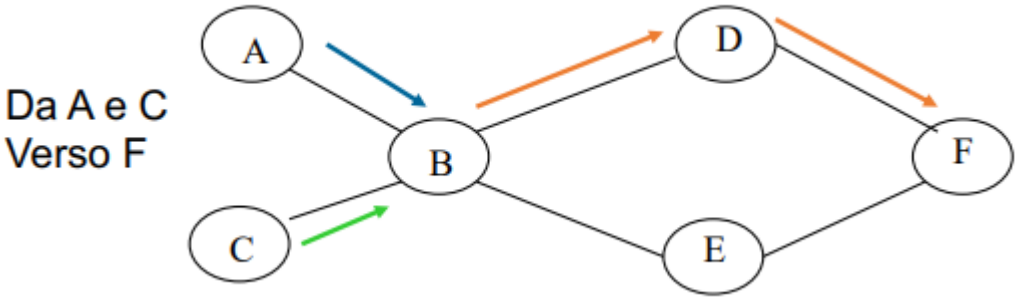
- Supporta protocolli standard di routing (OSPF, BGP) mantenendo scalabilità e flessibilità.
- Trasferimento veloce dei pacchetti tramite l'utilizzo di tecniche di switching veloce, permettendoci di utilizzare quei router che per via del routing rimanevano a disposizione per mera ridondanza.

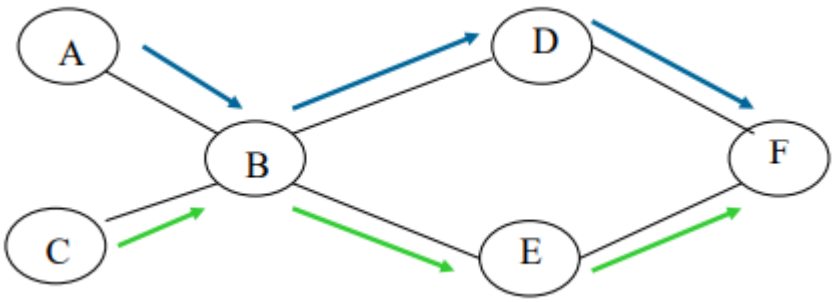
Realizzazione: MPLS utilizza la commutazione orientata alla connessione, la **label** è una breve entità che identifica i flussi di dati e non codifica gli indirizzi IP, essa viene aggiunta al pacchetto, attraverso un header aggiuntivo con dimensione 32 bit, e la usiamo per instradare sostituendola all'indirizzo IP.

Label-Switching Router (LSR): router che supporta MPLS.

Label Edge Router (LER): router che collega la rete MPLS con reti esterne, attribuendo o rimuovendo le etichette.

Label-Switched Path (LSP): percorso seguito dai pacchetti appartenenti a una FEC, stabilito tramite etichette.





Flusso di pacchetti

Un **flusso (flow)** è una sequenza di datagrammi inviati da una particolare sorgente a una particolare destinazione, accomunati da:

- Medesimo instradamento (route)
- Uniformi richieste di qualità di servizio
- Insieme delle politiche di gestione richieste nei router (priorità, ecc.)

LSR: utilizza una **tabella di instradamento (LFIB)** per associare label in ingresso e in uscita ai pacchetti.

LER: all'ingresso assegna una label al pacchetto e alla sua uscita rimuove la label.

Forwarding Equivalence Classes (FEC)

Raggruppamento di flussi con destinazione e requisiti di qualità di servizio simili. Ogni pacchetto o flusso associato a una FEC viene instradato nella stessa direzione attraverso i router. Questo permette ai router di ragionare per "percorsi" e non più per destinazioni, riducendo le tabelle di instradamento da milioni di voci a decine di voci. Inoltre, nel mondo IP, la dinamicità deve essere calcolata di volta in volta, mentre con le FEC possiamo scegliere in base alle necessità.

Gestione delle Label in MPLS

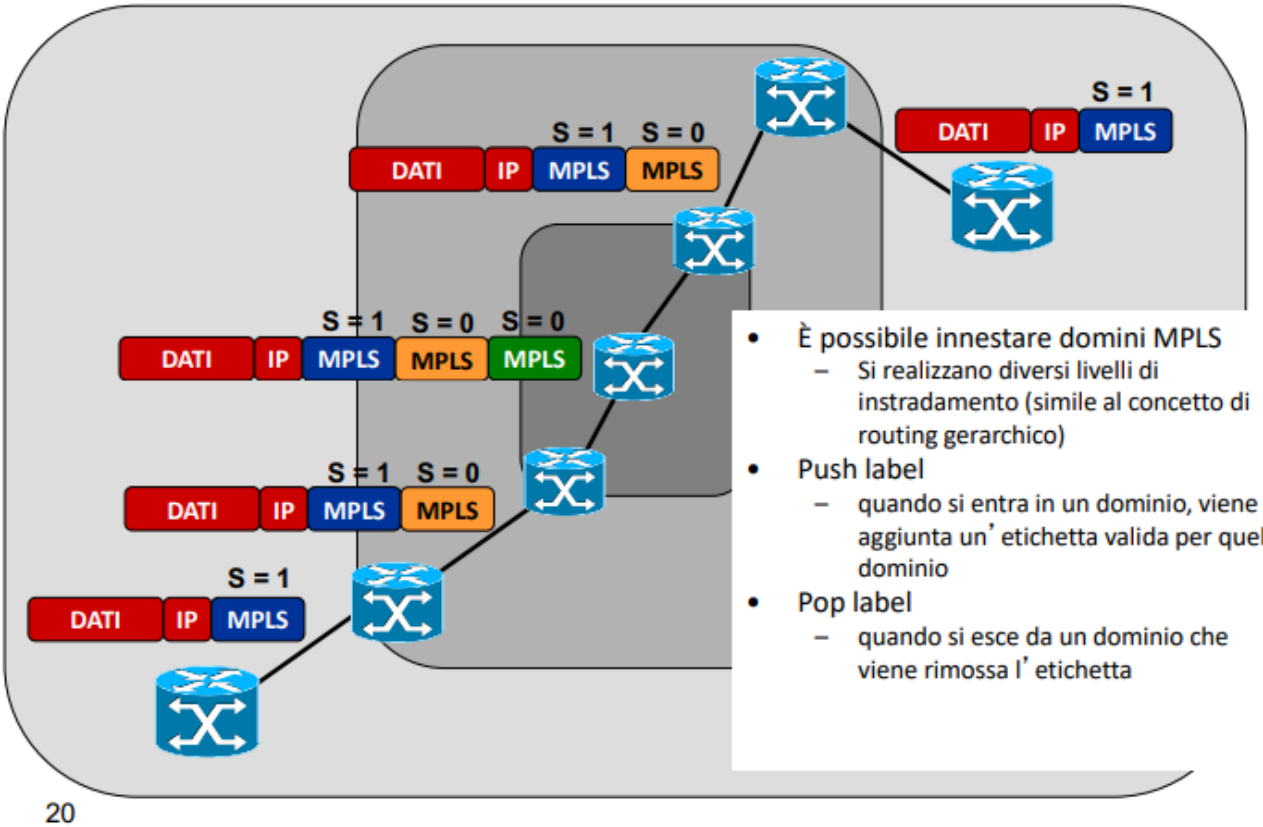
MPLS (Multiprotocol Label Switching) semplifica l'instradamento dei pacchetti evitando di valutare la FEC (Forwarding Equivalence Class) a ogni hop. Questo è reso possibile grazie al meccanismo di **label swapping**, che associa a ogni pacchetto una label di uscita per il prossimo hop.

Principi di funzionamento:

- **Assegnazione delle label**: Le label vengono allocate e gestite dal router a valle. Durante una fase iniziale di **handshake**, i router MPLS decidono quale etichetta assegnare ai flussi di ingresso su ciascuna interfaccia e quale utilizzare per l'uscita.
- **Instradamento basato su label**: Una volta che i dati iniziano a circolare, i router operano esclusivamente sulle etichette, senza analizzare gli indirizzi IP.

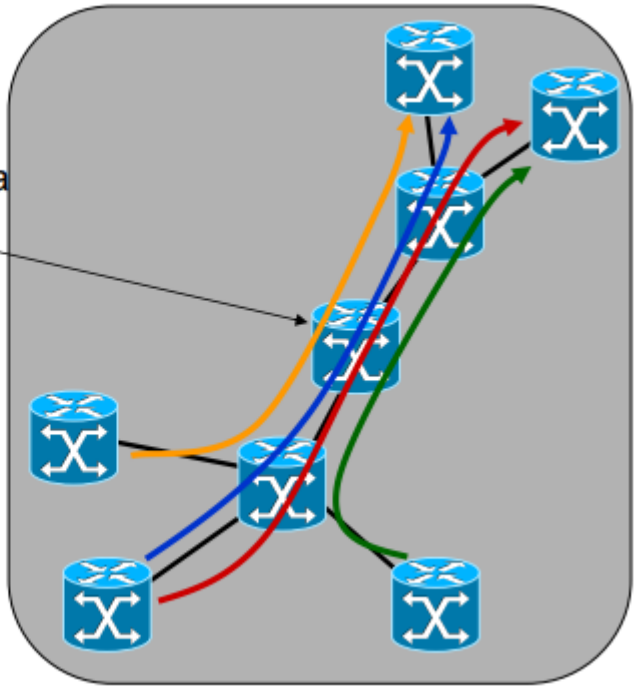
Funzionalità avanzate:

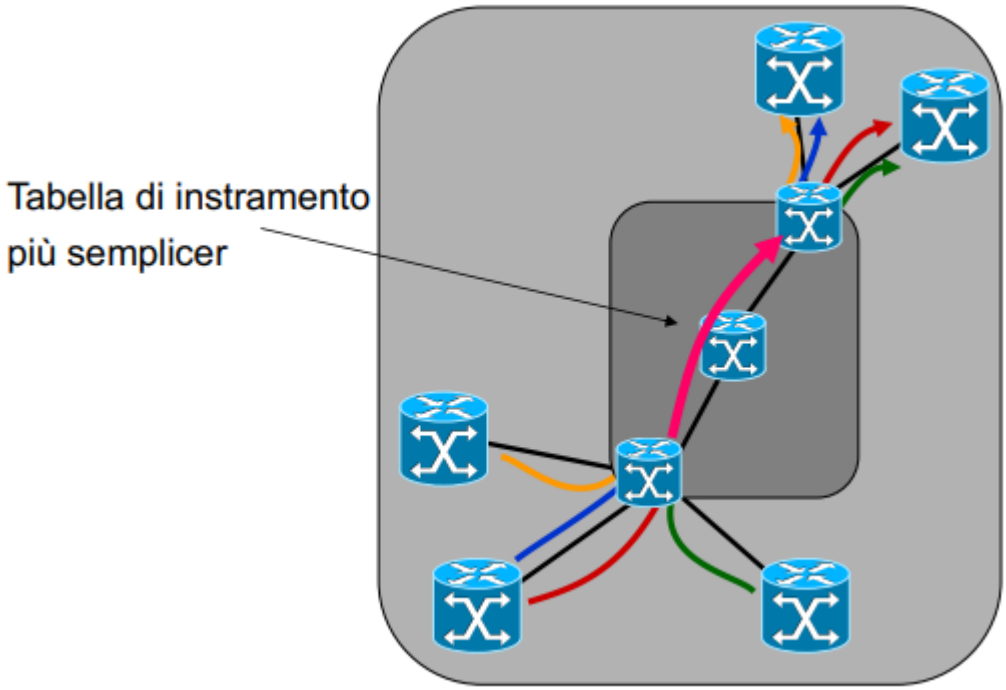
- **Innestamento di domini (label stacking)**: MPLS supporta la sovrapposizione di più livelli di instradamento, simile al routing gerarchico. Le label possono essere aggiunte (**push**) o rimosse (**pop**) quando i pacchetti entrano o escono da un dominio MPLS.
- **Aggregazione (label merging)**: Consente di unire flussi di traffico in un unico flusso, ottimizzando l'uso delle risorse.
- Il **TTL** (Time-to-Live) viene monitorato e decrementato a ogni hop attraversato da un LSR (Label Switch Router). Alla fine del percorso MPLS, il TTL viene ripristinato per garantire un controllo efficace sul numero di hop complessivi.



20

Deve avere in memoria tutte le FEC





Prestazioni dei Protocolli di Telecomunicazione

Affidabilità nei protocolli

I **protocolli** di comunicazione sono progettati per garantire la **trasmissione affidabile** dei dati. Questo risultato si ottiene attraverso:

Controllo degli errori, che comprende: **CRC (Cyclic Redundancy Check)**, una tecnica per verificare la correttezza dei dati trasmessi ed **Internet checksum**, utilizzato per rilevare errori nei pacchetti.

Recupero degli errori, realizzato mediante: **ARQ (Automatic Repeat reQuest)**, tecnica che richiede la ritrasmissione dei dati non ricevuti correttamente e consguente **ritrasmissione**.

Controllo di flusso e sequenza, che assicura l'ordine corretto dei dati inviati e ricevuti:

- **Acknowledgment (ACK)**, una conferma di ricezione per ogni pacchetto.
- **ARQ**, che gestisce ritardi e ripetizioni.

Funzionalità e Prestazioni

I protocolli devono soddisfare due esigenze fondamentali:

Funzionalità: devono risolvere problemi legati all'**accesso** e all'**utilizzo del canale** per garantire una trasmissione affidabile.

Prestazioni: devono ottimizzare l'uso della **capacità dello strato fisico**, assicurando che la trasmissione avvenga in modo efficiente e senza perdite significative.

Gestione delle richieste in un sistema

Un sistema di comunicazione deve gestire diverse tipologie di **richieste**:

Richieste offerte ($a(t)$): rappresentano il flusso di dati inviati al sistema.

Richieste accettate ($s(t)$): sono quelle che il sistema può effettivamente processare.

Richieste perdute ($r(t)$): sono richieste rifiutate o non accettate, calcolate come $r(t) = a(t) - s(t)$.

Il **tempo di servizio** (Θ) è un parametro cruciale che rappresenta il tempo necessario a completare una **PDU (Protocol Data Unit)**, esso potrà essere deterministico (dimensione dei pacchetti fissa) o aleatorio (dimesione dei pacchetti variabile).

La **frequenza media di servizio** ($\mu = \frac{1}{\Theta}$) indica quanto velocemente il sistema smaltisce le richieste in condizioni operative, dunque potrà essere considerato come la capacità massima di servizio offribile.

Sistema a coda

Nelle **reti a pacchetto**, un modello frequente è quello di un sistema a **coda** con un singolo servitore. In questo contesto:

- L'utente trascorre un **tempo totale nel sistema**, che comprende:
  - **Attesa in coda** (T_A): il tempo prima di essere servito.
  - **Tempo di servizio** ($\bar{\Theta}$): il tempo effettivo per completare l'operazione.
  - Relazione complessiva: $\bar{\Theta}_{totale} = \bar{\Theta} + T_A$.
- Le prestazioni del sistema dipendono da:
  - **Frequenza media degli arrivi** (λ), cioè il ritmo con cui le richieste entrano nel sistema.
  - **Tempo medio di servizio** ($\bar{\Theta}$), ovvero la durata media per completare ogni richiesta.
  - Il prodotto $A = \lambda \cdot \bar{\Theta}$ determina il traffico medio, secondo il **teorema di Little**, il traffico è determinato dal rapporto tra la capacità di trasporto e la quantità di dati trasportati ed essendo una quantità a dimensionale ne è preferibile l'utilizzo (si usa come unità di misura lo Erlang).

Efficienza del protocollo

L'efficienza di un protocollo dipende dalla capacità di ottimizzare il rapporto tra risorse utilizzate e dati utili trasmessi:

Capacità teorica: è determinata dalla velocità del **canale** (C) e dalla lunghezza del **pacchetto** (L), calcolata come $\bar{\Theta}_{min} = \frac{L}{C}$.

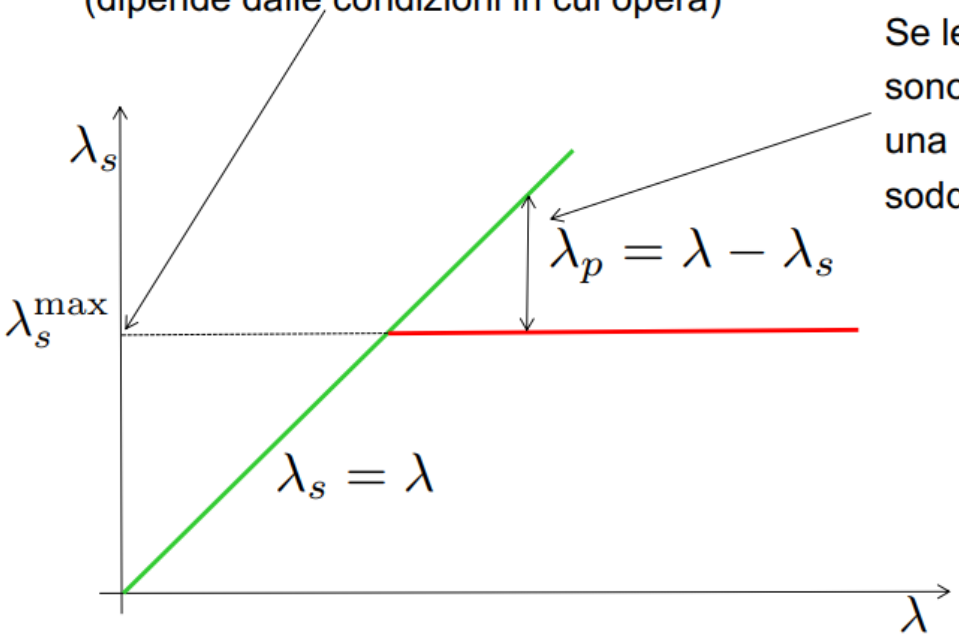
Riduzione di efficienza: si verifica in presenza di fattori come:

- **PCI** (Protocol Control Information).
- **Errori di trasmissione** che richiedono ritrasmissioni.
- **Tempi morti** dovuti a dinamiche del protocollo o attese per l'accesso al canale.

In un sistema ideale

Il sistema ha una capacità massima finita di smaltire richieste
(dipende dalle condizioni in cui opera)

Se le richieste offerte sono eccessive una parte non può essere soddisfatta

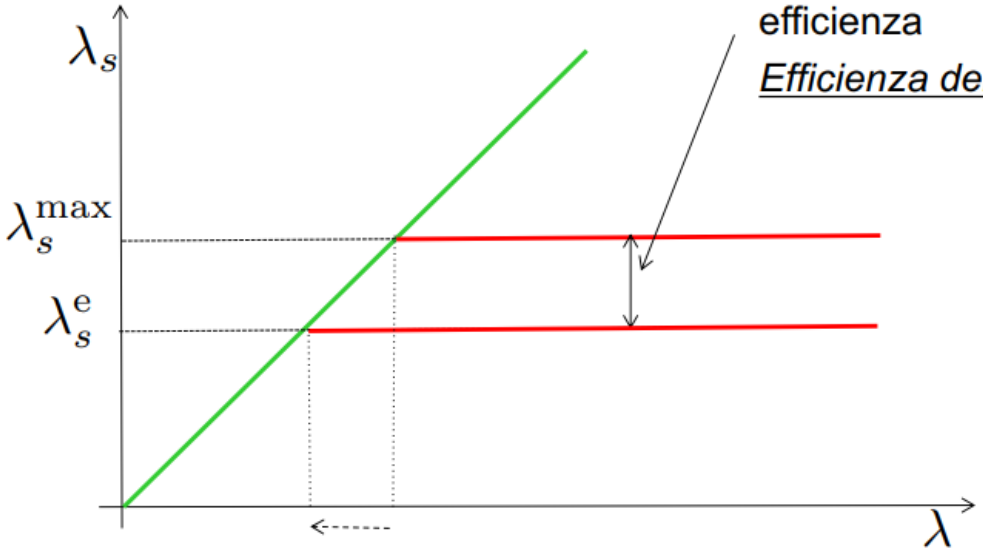


In un sistema reale

La riduzione di capacità si interpreta come perdita di efficienza

Efficienza del protocollo

$$\eta = \frac{\lambda_s^{\mathrm{e}}}{\lambda_s^{\max}} \leq 1$$



La riduzione di capacità obbliga il livello superiore a limitare la proprie richieste pena la perdita dei dati

19

Utilizzazione

L'**utilizzazione** di un sistema di comunicazione rappresenta la misura dell'efficienza con cui le risorse del sistema vengono impiegate per trasmettere dati utili. È definita come il rapporto tra il tempo in cui effettivamente trasporto delle informazioni ed il tempo totale misurato ($p = \frac{B(T)}{T}$) e potrà assumere un valore che oscilla tra 0 e 1.

Alta Utilizzazione: Indica che il sistema sta operando vicino alla sua capacità massima.

Bassa Utilizzazione: Può suggerire un uso inefficiente delle risorse disponibili, di conseguenza indica anche il numero medio di utenti serviti nel tempo.

L'ideale sarebbe avere un'utilizzazione media che si discosta del 20-30% da quella massima per evitare che si creino disservizi legati all'immissione in coda di utenti. Al diminuire del tempo di servizio ovvero della lunghezza dei pacchetti dimunuirà il tempo di attesa in coda, dunque conviene mandare tanti piccoli pacchetti su pochi router con una grandissima capacità piuttosto che distribuire quella capacità su molti più router lenti.

Reti Local Area Network (LAN)

Le **LAN (Local Area Network)** rappresentano un'infrastruttura di telecomunicazioni progettata per consentire la comunicazione tra dispositivi indipendenti in un’area geografica limitata. Queste reti sfruttano un canale condiviso ad alta velocità, garantendo tassi di errore contenuti.

Caratteristiche principali delle LAN

Area limitata: Le LAN operano in un contesto geografico circoscritto, spesso privato, come uffici, abitazioni o campus,questo consente prestazioni elevate grazie alla vicinanza fisica tra i dispositivi. Le LAN offrono velocità di trasmissione elevate con tassi di errore contenuti, grazie alle brevi distanze fisiche e alla qualità del canale.

Canale fisico condiviso: Un unico canale è utilizzato da tutti i dispositivi connessi, questa condivisione consente trasmissioni simultanee, ma richiede meccanismi per evitare collisioni.

Trasmissioni broadcast: La rete supporta comunicazioni "da uno a tutti".

Indipendenza: I dispositivi nelle LAN non seguono un'architettura master-slave, operando invece come entità autonome.

Traffico offerto e capacità del sistema

Quando il numero di utenti che utilizzano il servizio supera la capacità massima del servitore, il sistema accumula lavoro in coda. Le curve temporali di utenti attivi e lavoro del servitore differiscono, ma la loro **media** coincide. Questa media è chiamata **traffico offerto** (A_0) e rappresenta un valore centrale per il dimensionamento delle reti. Anche quando gli utenti diventano zero, il servitore continua a lavorare per smaltire le richieste accumulate, compensa il sovraccarico continuando a elaborare i dati accumulati fino al completo smaltimento.

Scelte progettuali delle LAN

Mezzo trasmissivo

- **Fibre ottiche**: Offrono maggiore banda, minore interferenza e una maggiore affidabilità rispetto al rame. Tuttavia, il costo di interconnessione e installazione può risultare più elevato, rallentandone l’adozione per le LAN.

- **Coppie intrecciate (twisted pairs)**: Continuano a essere utilizzate per gli "ultimi metri" di connessione grazie al costo contenuto e alla semplicità di utilizzo.
- **Mezzo radio**: Negli anni recenti, le tecnologie wireless stanno guadagnando importanza per la flessibilità e i costi ridotti.

Topologie

- **Stella**: un nodo centrale collega tutti i dispositivi.
- **Maglia**: garantisce alta ridondanza, con ogni nodo collegato a più nodi vicini.
- **Gerarchica**: struttura a livelli, utile per ambienti complessi.
- **Punto-multipunto**: utilizzato nelle prime LAN con mezzi condivisi, come bus bidirezionali o anelli, oggi reoutato non adatto.

Accesso Multiplo nelle LAN

Le reti locali (LAN) utilizzano tecniche di accesso multiplo per gestire l'utilizzo di un canale condiviso tra più dispositivi. Queste tecniche garantiscono l'efficienza della comunicazione e riducono il rischio di collisioni.

1. **Canalizzazione** La canalizzazione divide le risorse del canale in modo predeterminato, evitando interferenze tra le trasmissioni. Le principali tecniche sono:
    - **FDMA (Frequency Division Multiple Access)**: Ogni trasmissione utilizza una porzione distinta della banda di frequenze disponibile. È adatto a scenari con trasmissioni continue e prevedibili.
    - **TDMA (Time Division Multiple Access)**: Il canale è suddiviso in slot temporali assegnati ai dispositivi in modo ciclico. Questo approccio è utile quando le trasmissioni sono intermittenti.
    - **CDMA (Code Division Multiple Access)**: I dati vengono separati utilizzando codici univoci. Permette trasmissioni simultanee sullo stesso canale, riducendo le interferenze grazie alla codifica.
2. **Accesso Dinamico** L'accesso dinamico alloca le risorse in tempo reale, adattandosi alle esigenze della rete. Si divide in:
    - **Accesso ordinato**: Basato su meccanismi che regolano l'accesso al canale per evitare collisioni.
    - **Accesso a contesa**: I dispositivi competono liberamente per l'accesso al canale, rischiando collisioni. Tecniche come **CSMA/CD (Carrier Sense Multiple Access with Collision Detection)** vengono utilizzate per rilevare e gestire le collisioni.

Prestazioni e parametri chiave delle LAN

La scelta dell’algoritmo di controllo e accesso è determinata da un compromesso tra **complessità** e **prestazioni**.

1. L: lunghezza del pacchetto.
2. C: velocità di trasmissione del canale.
3. D: distanza massima tra due nodi della rete.
4. v: velocità di propagazione del segnale (tipicamente vicino alla velocità della luce nell’aria).

In un sistema senza collisioni e con coordinamento perfetto, tutte le richieste vengono soddisfatte fino alla saturazione del canale.

Propagazione reale nella topologia bus

Nella **topologia bus**, il tempo di attraversamento di una trama sulla LAN non è istantaneo.

Tempi di trasmissione:
1. t: il nodo **A** inizia la trasmissione.
2. $t + L/C$: il nodo **A** completa la trasmissione.
3. $t + d/v$: il nodo **B** riceve il primo bit.
4. $t + L/C + d/v$: il nodo **B** riceve l'ultimo bit.

Efficienza del MAC ideale

Una trama impegna la **LAN** per un tempo T_0, limitando l'uso totale del canale. Il canale può essere utilizzato al massimo per T secondi ogni T_0.

Formula dell'efficienza del MAC:

$$\eta = \frac{T}{T_0} = \frac{L/C}{L/C + d/v} = \frac{1}{1+a}$$

- Dove $a = C \cdot d/v \cdot L$
- a rappresenta la **lunghezza della LAN** in termini di PDU.

L'efficienza pone un limite massimo al traffico che la LAN può smaltire (A_s).

Traffico smaltito dalla LAN

La quantità di traffico smaltito dipende dal rapporto A_0 (traffico offerto) e $1/(1+a)$:

1. **Se** $A_0 < 1/(1+a)$:
   - Tutte le trame in arrivo vengono trasmesse.
   - $S = G = A_0$.
2. **Se** $A_0 \geq 1/(1+a)$:
   - Il MAC non è in grado di trasmettere tutte le trame.
   - Una parte delle trame viene accodata.
   - $A_s = h = 1/(1+a)$.

Questi limiti dipendono dalla **lunghezza della LAN** e dal comportamento del **canale di trasmissione**.

Efficienza delle LAN

Il parametro **a** influenza direttamente le prestazioni della LAN.

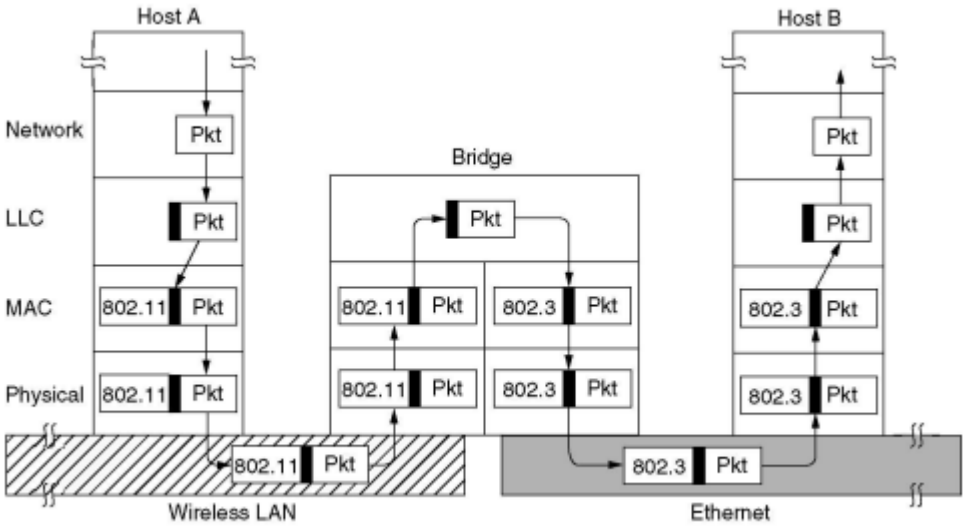
Lunghezza del canale: maggiore è la lunghezza in termini di trame, minore è il traffico massimo smaltibile (massimo throughput).

I protocolli ad **accesso multiplo** sono efficienti se le distanze e le velocità di trasmissione sono limitate.

Interconnessione di LAN

Apparati di interconnessione:

- **Repeater:**
  - Livello 1 OSI, rigenera segnali.
  - Estende la topologia LAN (entro i limiti di standard, es. 2500m in Ethernet).
- **Bridge:**
  - Livello 2 OSI, separa domini di collisione.
  - Learning bridge: impara gli indirizzi sorgenti per filtrare le trame.



Switch: - Bridge multiporta, commutazione su indirizzi MAC. - Permette comunicazioni simultanee migliorando prestazioni rispetto agli hub. - Capacità aggregata superiore (es. switch Fast Ethernet: 200 Mbps vs 100 Mbps degli hub).

Differenze Hub vs Switch:

- **Hub:** bus condiviso, trasmissione broadcast.
- **Switch:** selettività nella ritrasmissione, maggiore capacità aggregata.

Protocollo a contesa: ALOHA

Sviluppato nel 1970 per connettere università delle Hawaii utilizzando stazioni terrestri e un satellite geostazionario.

Modalità di funzionamento:

- **CAP** (Channel Access Procedure):
  - Le stazioni trasmettono senza verificare la disponibilità del canale.
  - Il satellite ritrasmette i dati verso tutte le stazioni.
  - La stazione trasmittente riceve la propria trama come conferma di trasmissione riuscita.
- **CRA** (Collision Resolution Algorithm):
  - Collisioni avvengono quando più stazioni trasmettono contemporaneamente.
  - Il satellite scarta le trame danneggiate.
  - Le stazioni che rilevano una collisione avviano un **algoritmo di back-off**, ritrasmettendo in un momento scelto casualmente in un intervallo T_b.

Prestazioni di ALOHA

Traffico generato:

- Gli arrivi di trame alle stazioni seguono un **processo di Poisson** con frequenza media λ.
- Tenendo conto delle ritrasmissioni, il traffico effettivo verso il satellite è $\lambda_r > \lambda$.

Intervallo di vulnerabilità:

- Definito come $T_v = 2T$, rappresenta il periodo durante il quale una trasmissione può subire collisioni.

Throughput di ALOHA

Probabilità di trasmissione senza collisioni:

$$P_0 = e^{-2G}$$

Traffico smaltito (A_s):

$$A_s = G \cdot e^{-2G}$$

Massimo throughput:

$$A_{Smax} = \frac{1}{2e} \approx 0.18 \quad \text{per } G = 0.5$$

Slotted ALOHA

Miglioramento:

- Il tempo è diviso in **slot** di lunghezza T.
- Le trame sono trasmesse in istanti predefiniti, riducendo l'intervallo di vulnerabilità a T.

Calcolo:

- Probabilità di trasmissione senza collisioni:

$$P_0 = e^{-G}$$

- Traffico smaltito (A_s):

$$A_s = G \cdot e^{-G}$$

Massimo throughput:

$$A_{Smax} = \frac{1}{e} \approx 0.36 \quad \text{per } G = 1$$

Algoritmi di back-off

Aloha classico:

- Ritrasmissione casuale nell'intervallo $[0, T_b]$, con $T_b \gg T$ per minimizzare collisioni.

Aloha slotted:

- Due approcci:
    - Ritrasmissione in uno slot scelto casualmente.

- Ritrasmissione nel primo slot disponibile con probabilità p_b.

Stabilità del sistema

Equilibrio: In condizioni stabili sarà $A_0 = A_s$, se $A_0 > A_{Smax}$, il sistema accumula traffico non smaltito, portando a instabilità.

Numero finito di stazioni: Il traffico offerto A_0 dipende dal numero di stazioni attive (k) e dalle condizioni del sistema.

Controlled Aloha

Back-off esponenziale:

- Aumenta progressivamente T_b in caso di collisioni, raddoppiando l'intervallo dopo ogni tentativo fallito.
- Garantisce stabilità ma può introdurre problemi di equità.

Derivati del protocollo ALOHA

Applicazioni: Utilizzabile su qualsiasi mezzo trasmissivo e topologia ed è adatto per reti con alti ritardi di propagazione (es. satelliti).

CSMA (Carrier Sensing Multiple Access):

- Sfrutta la rilevazione di segnale sul canale prima della trasmissione.
- Prevede algoritmi di back-off in caso di collisione.

CSMA (Carrier Sensing Multiple Access)

Principi di funzionamento:

Carrier sensing:

- Ogni stazione prima di trasmettere rileva la presenza di segnali sul bus condiviso.
- La trasmissione avviene solo se il bus risulta libero.
- Se il bus è occupato, la stazione aspetta la fine della trasmissione in corso.
    - **Caso 1-persistent**: la stazione trasmette immediatamente dopo che il bus si libera.
    - **Caso non-persistent**: la stazione attiva un algoritmo di back-off per evitare collisioni.
    - **Caso p-persistent**: la stazione trasmette con una probabilità p e, in caso contrario, attiva l'algoritmo di back-off.

Gestione delle collisioni:

Durante la trasmissione, i dati inviati possono collidere con quelli di un'altra stazione per via del ritardo di propagazione non nullo tra le stazioni. Sul bus manca un meccanismo immediato per rilevare le collisioni è dunque necessario affidarsi a sistemi come gli **Acknowledgements (ACK)** per rilevare e gestire errori di trasmissione.

Algoritmo di back-off:

Simile a quello utilizzato nel protocollo Aloha e richiede che il tempo di back-off (T_b) sia maggiore di due volte il tempo di propagazione (2τ).

Intervallo di vulnerabilità nel CSMA:

Consideriamo due stazioni, **A** e **Z**, le più distanti sul bus, τ rappresenta il tempo di propagazione tra A e Z, sommato al tempo necessario per rilevare il segnale.

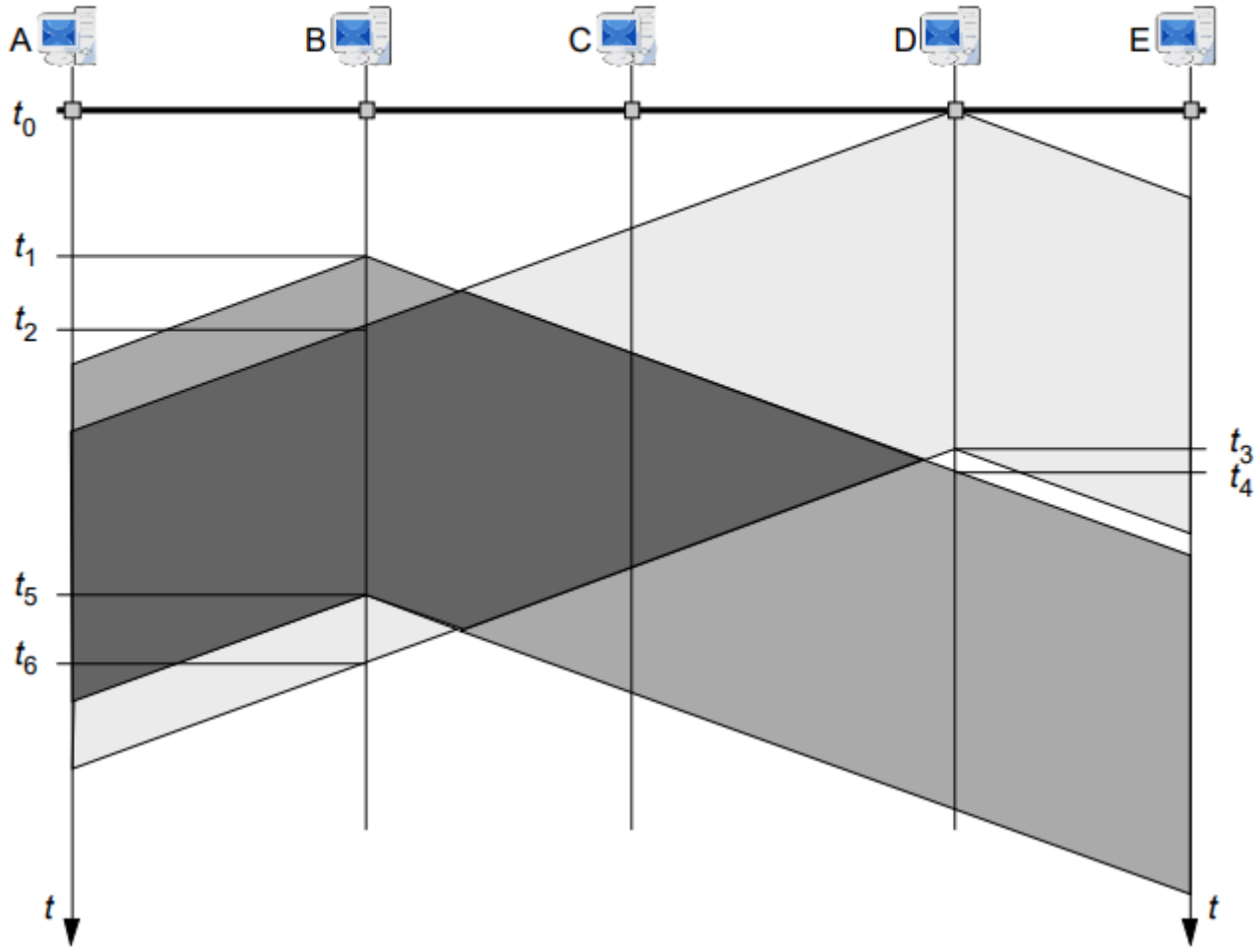
Situazione di vulnerabilità: Se **A** inizia a trasmettere al tempo t_A, ma **Z** rileva il canale libero e trasmette tra t_A e $t_A + \tau$, si verifica una collisione, analogamente, se **Z** trasmette tra $t_A - \tau$ e t_A, **A** non rileverà il segnale e inizierà a trasmettere, causando collisioni.

Intervallo di vulnerabilità: è pari a 2τ, le prestazioni miglioreranno rispetto all'Aloha tanto più è valida la relazione $\tau/T < 1$, dove T è il tempo di trasmissione della trama.

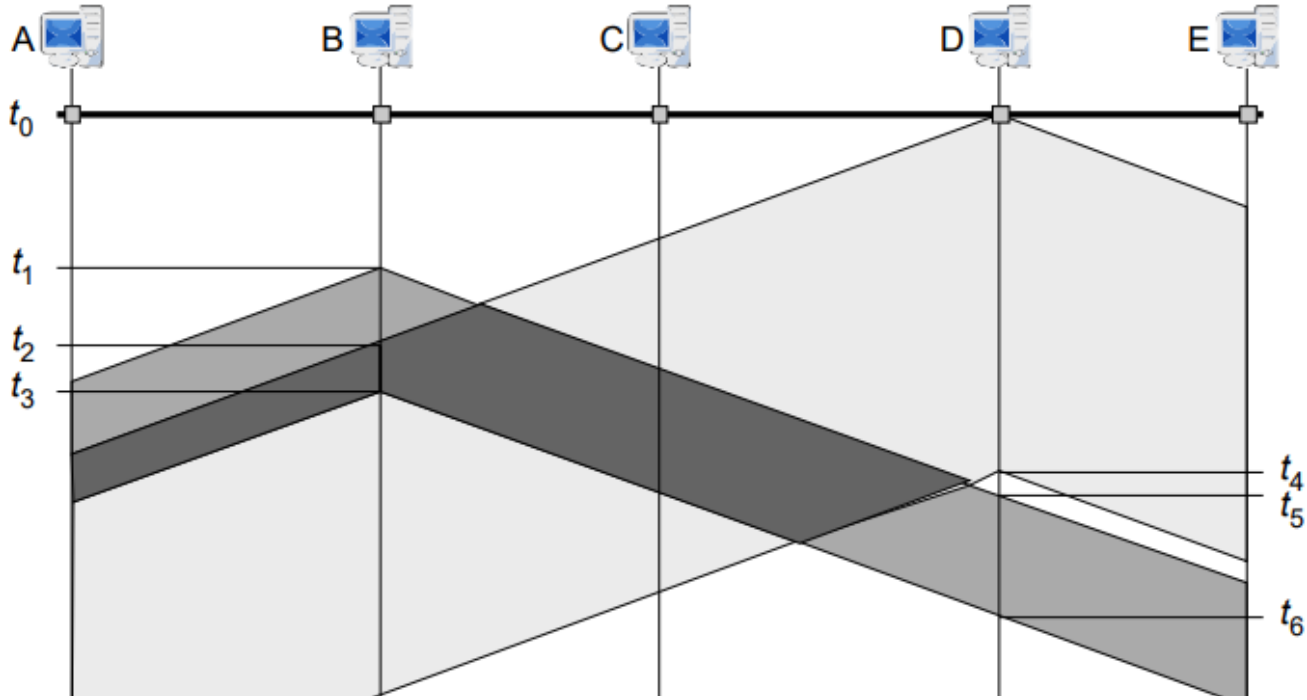
Versione slotted del CSMA:

Utilizza uno slot temporale pari a τ, lL'intervallo di vulnerabilità si riduce da 2τ a τ e nonostante ciò, permangono problemi di stabilità, tipici dei protocolli a contesa. Può essere adottato un algoritmo di back-off esponenziale per migliorare la gestione delle collisioni.

CSMA



CSMA-CD



CSMA/CD (Carrier Sensing Multiple Access with Collision Detection)

Migliora il protocollo permettendo il rilevamento immediato delle collisioni e rappresenta lo standard de facto per le reti LAN grazie alla semplicità e robustezza del protocollo.

Collision Detection (CD): Una stazione monitora il canale durante la trasmissione per rilevare variazioni di potenza (indicative di collisioni), il tutto è facilitato dall'uso della **codifica di Manchester**, che garantisce transizioni regolari del segnale.

In caso di collisione: La stazione interrompe subito la trasmissione per evitare sprechi di banda ed invia una sequenza di bits chiamata **jamming signal** per avvisare le altre stazioni della collisione.

Vantaggi rispetto al CSMA: In caso di collisione, il canale è inutilizzato solo per l'intervallo di vulnerabilità (τ) e per il tempo di rilevamento della collisione e della sequenza di jamming (T_{CD}) mentre nel CSMA puro il canale restava inutilizzato per un tempo pari all'intera durata della trama (T).

Codifica di Manchester:

Caratteristiche del segnale:

- **Bit "0" logico**: Segnale basso per metà tempo del simbolo e alto per l'altra metà.
- **Bit "1" logico**: Segnale alto per metà tempo del simbolo e basso per l'altra metà.

Vantaggi:

- Ogni bit ha una transizione centrale che facilita:
  - **Sincronizzazione**: semplifica l'acquisizione del clock.
  - **Carrier sensing** e **collision detection**.
- Simboli aggiuntivi (alto-alto e basso-basso) rappresentano segnali di non-dati.

Svantaggi: La necessità di un clock al doppio della velocità di trasmissione: per 10 Mbit/s serve un clock a 20 MHz.

Token Ring e IEEE 802.5

Token Ring:

HA topologia fisica a **stella**, ma logica ad **anello** ed è basato sul concetto di **token**, ovvero un diritto di trasmissione che circola lungo l'anello. Ogni stazione attende il passaggio di un token libero che una volta ricevuto permetterà alla stazione di aggiunge i dati da trasmettere per poi rilasciare il token una volta completata la trasmissione.

Definizioni dei tempi principali nel Token Ring

Tempo di trasmissione (T): È il tempo necessario per trasmettere una trama di lunghezza massima e dipende dalla velocità di trasmissione della rete e dalla dimensione massima della trama consentita.

Tempo di accesso (T_{acc}): È il tempo che una stazione deve attendere per vedere il token libero e quindi poter trasmettere. In presenza di n stazioni al meglio la stazione attende solo il rilascio del token dalla stazione precedente al peggio: deve aspettare che tutte le $n-1$ stazioni utilizzino il token.

- Formula:

$$T_{acc} = T_1 + T_2 \leq n \cdot T_{HT} + T_{lat}$$

  Dove:
- T_1: tempo per il rilascio del token dalla stazione corrente.
- T_2: tempo per il ritorno del token.

Tempo di latenza (T_{lat}): È il tempo impiegato da un bit per completare un giro completo dell'anello e dipende dalla lunghezza fisica dell'anello e dal ritardo introdotto dalle stazioni.

Tempo di detenzione del token (T_{HT}): È il tempo massimo durante il quale una stazione può trattenere il token per trasmettere dati ed è determinato dalla dimensione massima delle trame e dalle strategie di rigenerazione del token.

Tempo di rotazione del token (T_{RT}): È il tempo impiegato dal token per compiere un giro completo dell'anello, include il tempo di detenzione (T_{HT}) delle n stazioni e il tempo di latenza (T_{lat}):

$$T_{RT} = n \cdot T_{HT} + T_{lat}$$

Rimozione delle trame nell'anello

Necessità di rimozione: Ogni trama deve essere rimossa dall'anello una volta che è stata ricevuta per evitare congestione.

Modalità di rimozione:

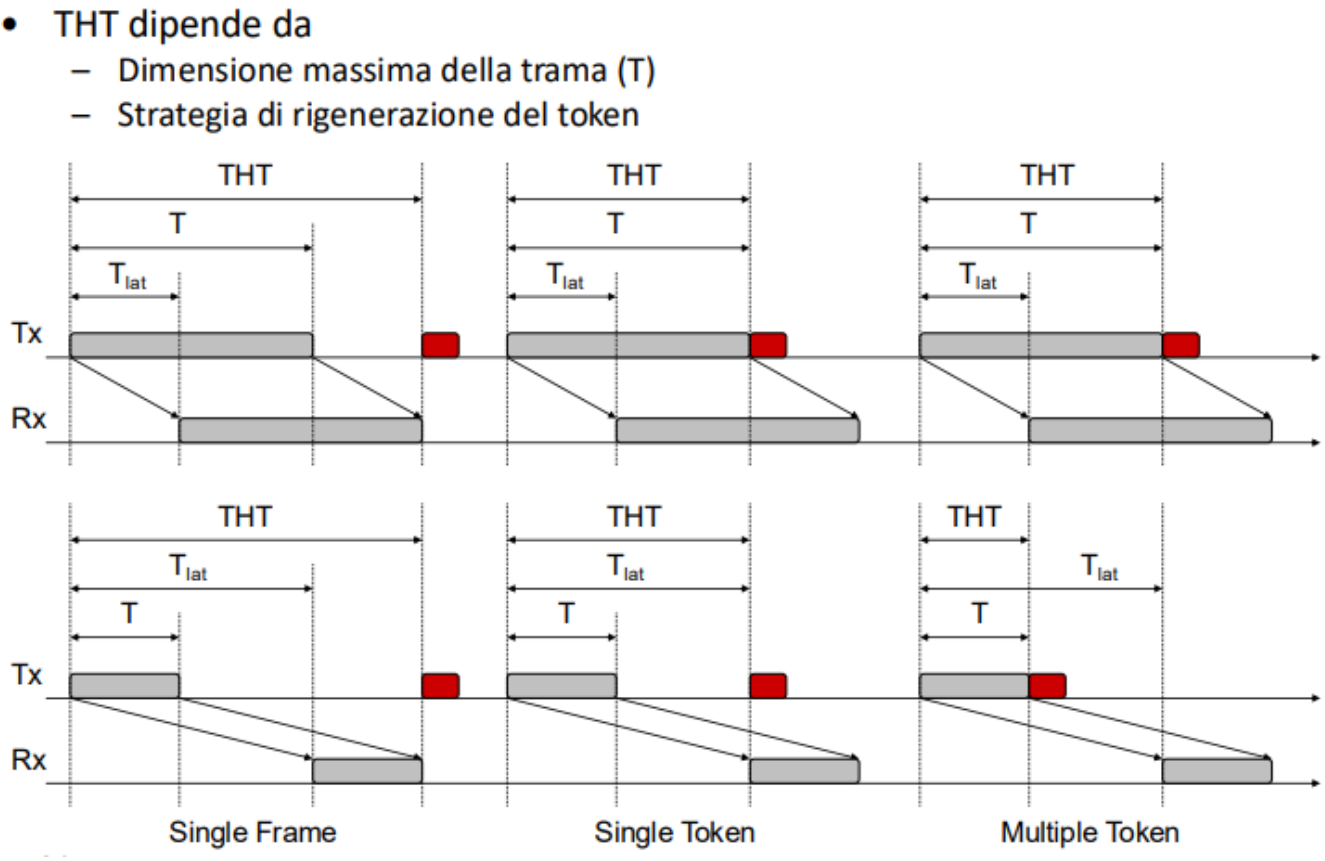
- **Diffusiva**: La trama viene rimossa dalla stazione trasmittente che libera anche il token, c'è la possibilità di aggiungere un **ACK** alla trama da parte della stazione ricevente.
- **Parzialmente diffusiva**: La trama viene rimossa dalla stazione ricevente che libera anche il token.
  - Vantaggi: il token si libera più velocemente.
  - Svantaggi:
    - Cambiamento dell'ordine di trasmissione.
    - Aumento del tempo di latenza.
    - Maggiore aleatorietà nel tempo di accesso.
    - Mancanza di verifica della corretta trasmissione.
    - Aumento del tempo di latenza a causa della necessità di leggere l'indirizzo del destinatario.

Strategie di rigenerazione del token

Single Frame: Il token viene rigenerato quando la stazione trasmittente ha ricevuto l'intera trama trasmessa.

Single Token: Il token viene rigenerato quando la stazione trasmittente ha ricevuto il token associato alla trama.

Multiple Token: Il token viene rigenerato subito dopo la trasmissione della trama, risulta efficiente solo quando T_{lat} è maggiore del tempo di trasmissione (T).



Monitor nel Token Ring

Ruolo del monitor: È responsabile della gestione delle emergenze causate da malfunzionamenti delle stazioni rimuovendo le trame errate o duplicate dall'anello.

Problematiche gestite:

- **Trama non rimossa**: Se una stazione non rimuove una trama, che continua a circolare il monitor identifica la trama tramite un bit M e la rimuove se necessario.
- **Token perduto o duplicato**: In assenza di un token valido, il monitor genera un nuovo token in caso di token duplicato, il monitor elimina quello superfluo.

Implementazione del bit M: Ogni token generato ha $M = 0$ il monitor imposta $M = 1$ quando rileva problemi.

Sincronizzazione nel Token Ring

Sincronizzazione asservita: Ogni stazione si sincronizza con il segnale ricevuto e lo utilizza per ritrasmettere i dati.

Buffer elastico: Una stazione (spesso il monitor) gestisce un buffer elastico per mantenere il sincronismo.

Problemi di latenza: La ritrasmissione immediata di ogni bit aiuta a minimizzare il tempo di latenza ma potrebbe ritrasmettere errori.

Token Bus

Principio di funzionamento: Simula un anello logico su una topologia fisica a bus in questa topologia logica ogni stazione ha un predecessore e un successore logici.

Gestione dinamica: La stazione corrente effettua un **polling** per invitare le stazioni che vogliono entrare nella rete mentre coloro che vogliono uscire comunicano la loro intenzione al predecessore e al successore.

Vantaggi rispetto al Token Ring: Ciò migliora la flessibilità nella gestione delle stazioni ed è decisamente più adatto per applicazioni real-time grazie all'assenza di collisioni.

Confronto tra protocolli a contesa e collision-free

Protocolli a contesa (es. CSMA):

- **Vantaggi**: Semplicità di implementazione e maggiore efficienza a basso traffico.
- **Svantaggi**: Collisioni e aleatorietà nei tempi di trasmissione.

Protocolli collision-free (es. Token Ring, Token Bus):

- **Vantaggi**: Determinismo nei tempi di consegna delle trame, non presentano problemi di stabilità ed utilizzo ottimizzato del canale ad alto traffico.
- **Svantaggi**: Maggiore complessità ed esposizione ai guasti del monitor.

Progetto IEEE 802

Obiettivi:

- Creato nel 1980 per definire standard per reti locali (LAN).
- Introduzione di una struttura gerarchica:
    - **Strato 2 (Data Link Layer)** diviso in:
        - **LLC (Logical Link Control)**: indipendente dal mezzo fisico e dalla topologia.
        - **MAC (Medium Access Control)**: specifico per il mezzo e il protocollo di accesso.

Standard principali:

- **IEEE 802.3**: Basato su CSMA/CD, ispirato a Ethernet.
- **IEEE 802.5**: Basato su Token Ring.
- **IEEE 802.11**: Wireless LAN (Wi-Fi).
- **IEEE 802.15**: Personal Area Networks (Bluetooth).

Rete Ethernet:

- Sviluppata nel 1976 dalla **Xerox** e successivamente adottata da DEC, Intel e Xerox.
- Standardizzata nel 1983 come **IEEE 802.3**.

Formato del Frame Ethernet (IEEE 802.3)

Campi del Frame:

- **Preamble (7 byte):** sincronizza clock trasmettitore/ricevitore.
- **Start Frame Delimiter (1 byte):** indica l'inizio del frame.
- **Destination Address (6 byte):** indirizzo destinazione (unicast, multicast o broadcast).
- **Source Address (6 byte):** indirizzo sorgente.
- **Length/Type (2 byte):** indica la lunghezza del campo dati (IEEE 802.3) o il tipo di payload (Ethernet).
- **Pad:** riempie frame <64 byte fino a questa dimensione.
- **Frame Check Sequence (4 byte):** verifica errori tramite un codice polinomiale.

Ordine di Trasmissione: Preamble → Destination Address → Source Address → Type → Data → Frame Check Sequence.

Collision Domain e Broadcast Domain

Collision Domain: Area in cui le stazioni possono collidere durante la trasmissione, leimensioni dipendono dalla velocità di trasmissione e dalla dimensione delle trame.

Broadcast Domain: Insieme di stazioni che ricevono una trama con **Destination Address: ff-ff-ff-ff-ff-ff**, normalmente coincidente con una singola LAN.

Evoluzione dell'Ethernet

Ethernet Classica a 10 Mbps

- **10base5 (Thick Wire):**
    - Utilizza cavi coassiali spessi con segmenti lunghi fino a 500 metri, supportando un massimo di 100 stazioni.
    - Le stazioni sono connesse mediante transceiver (collegati tramite "drop cable").
    - Sebbene robusta, questa tecnologia richiedeva cavi rigidi e difficili da installare, rendendola meno pratica nei cablaggi moderni.
- **10base2 (Thin Wire):**
    - Sfrutta un cavo coassiale più sottile e flessibile, consentendo segmenti di lunghezza massima di 180 metri e un massimo di 30 stazioni.
    - Le stazioni sono collegate in serie (topologia "a catena") tramite connettori BNC e connettori a T.
    - Richiede l'uso di terminatori per evitare riflessioni del segnale.
- **10baseT (Twisted Pair):**
    - Utilizza cavi **UTP** (Unshielded Twisted Pair) di categoria 3, con lunghezza massima di 100 metri per singolo collegamento.
    - Ogni stazione è connessa a un hub tramite connettori RJ45, formando una topologia a stella.
    - Gli hub funzionano da multiport repeater, permettendo una gestione più semplice rispetto alle soluzioni basate su cavo coassiale.
- **10baseF (Fibra Ottica):**
    - Impiega cavi in fibra ottica multimodo, consentendo connessioni fino a 2000 metri.
    - È spesso utilizzata per cablaggi verticali, specialmente in edifici, ma il costo dei connettori e degli adattatori la rende una soluzione meno comune per gli utenti finali.

Fast Ethernet (IEEE 802.3u - 100 Mbps) Introduce una maggiore velocità mantenendo la compatibilità con le reti Ethernet classiche. Offre diverse varianti: - **100baseT4:** - Utilizza 4 coppie di cavi UTP di categoria 3, con una lunghezza massima di 100 metri. - La trasmissione sfrutta una codifica **8B/6T**, che converte 8 bit in 6 simboli ternari.

```
- **100baseTX:**
  - Richiede cavi UTP di categoria 5 o superiore.
  - Utilizza 2 coppie per trasmissione dati (una per direzione) e offre
comunicazioni full-duplex fino a 100 metri.

- **100baseFX:**
  - Si basa sulla fibra ottica multimodo, con una portata massima di 2000 metri.
  - È ideale per connessioni tra edifici o cablaggi backbone.
```

Gigabit Ethernet (IEEE 802.3z - 1 Gbps) Progettata per incrementare la velocità a 1 Gbps mantenendo la semplicità di Ethernet. - **1000baseSX:** Utilizza fibra ottica multimodo per distanze fino a 550 metri. - **1000baseLX:** Compatibile sia con fibra multimodo che monomodo, estende le connessioni fino a 5000 metri con quest'ultima. - **1000baseCX:** Sfrutta 2 coppie di cavi intrecciati schermati (STP) ma è più costosa e meno performante rispetto alla fibra ottica. - **1000baseT:** Impiega 4 coppie di cavi UTP di categoria 5, con una lunghezza massima di 100 metri ed utilizza una codifica innovativa che associa 2 bit a un simbolo con 5 livelli, garantendo una velocità netta di 1 Gbps.

10 Gigabit Ethernet (IEEE 802.3ae) È progettata esclusivamente per la fibra ottica, con velocità dieci volte superiori rispetto al Gigabit Ethernet. - **Caratteristiche principali:** Supporta connessioni su fibra ottica con distanze che variano da pochi chilometri fino a diverse decine di chilometri, a seconda del tipo di fibra e della modalità di trasmissione. È prevalentemente utilizzata per backbone in reti aziendali o per Metropolitan Area Networks (MAN). L'elevato costo e l'hardware specifico rendono difficile l'adozione su larga scala per dispositivi comuni, riservandola principalmente a infrastrutture critiche.

Carrier Ethernet Estende Ethernet oltre il contesto delle LAN per essere utilizzata come tecnologia di trasporto nei provider di rete. - **Nuove Funzionalità:** Indirizzamento multilivello gerarchico per migliorare la scalabilità ed introduzione di meccanismi di segnalazione, gestione e recupero dei guasti. - **Applicazioni:** È ideale per reti backbone, trasporto su lunghe distanze e reti aziendali distribuite. - **Alternative:** Lo standard IEEE 802.17 (RPR, Resilient Packet Ring) è stato proposto come opzione alternativa per backbone MAN.

Multigigabit Ethernet Ethernet continua a evolversi con velocità superiori a 10 Gbps, supportando infrastrutture avanzate: - **Stato attuale:** Studi e implementazioni su velocità fino a 400 Gbps ed è già ampiamente utilizzata in data center e reti backbone.

Cablaggio delle LAN Moderne

Caratteristiche Generali:

- Un unico cablaggio strutturato per tutti i servizi di telecomunicazione.
- Basato su UTP (tipicamente 4 coppie) con terminazioni RJ45 o RJ11.
- Standard: **EIA/TIA 568** e **ISO 11801**.

Struttura del Cablaggio:

- **Prese a muro:** punto di accesso per le stazioni.
- **Cablaggio orizzontale:** collega prese a muro all'armadio di rete (topologia a stella).
- **Cablaggio verticale:** connette diversi armadi di rete (backbone).
- **Armadio di rete:**
    - Contiene switch, patch panel e altre apparecchiature attive.
    - **Patch panel:** consente di organizzare e distribuire le connessioni dei cavi UTP.
    - **Patch cord:** collega le porte dei patch panel agli switch.

Tecnologie Attive:

- Switch con porte Ethernet UTP (es. 100 Mbps, 1 Gbps) o fibra ottica per il backbone.

Wirless LAN (Wi-Fi)

Standard IEEE 802.11

- Introdotto nel 1997 per accesso radio alle reti locali.
- **Strato fisico 802.11:**
    - Trasmissione trame, interazione con MAC per attività del canale.
    - Tecniche iniziali (1-2 Mbps): Infrarossi, FHSS, DSSS.
    - Banda ISM (2.4 GHz, 83.5 MHz): senza licenze per usi industriali, scientifici e medici.
    - Regolamentazioni:
        - Limiti di potenza.
        - Tecniche Spread Spectrum (FHSS: 79 canali; DSSS: gain ≥ 10 dB).
    - Banda ISM in Italia: autorizzazione obbligatoria solo su suolo pubblico (D.M. 28 Maggio 2003).

Standard successivi:

- **802.11a (1999):** banda 5 GHz, OFDM, 12 canali da 20 MHz, bit rate da 6 a 54 Mbps.
- **802.11b (1999):** banda 2.4 GHz, HR-DSSS, 14 canali (5 MHz), bit rate fino a 11 Mbps, Dynamic Rate Shifting.
- **802.11g (2003):** banda 2.4 GHz, OFDM/HR-DSSS, bit rate da 1 a 54 Mbps.

Architettura di rete 802.11

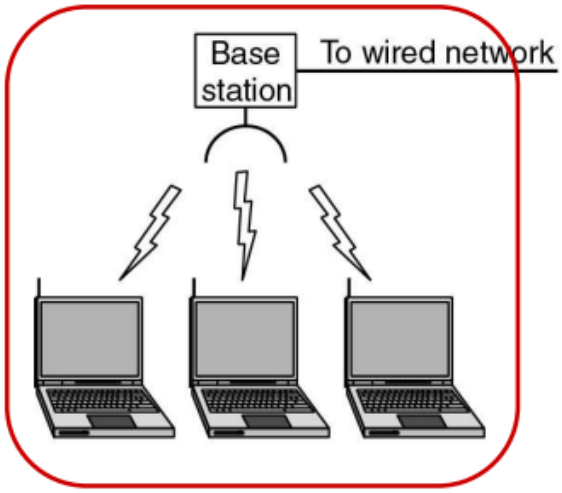
Nomenclatura:

- **Basic Service Set (BSS):** Un insieme di stazioni wireless che comunicano tra loro tramite un Access Point (AP).
- **Access Point (AP):** Dispositivo che funge da ponte tra le stazioni wireless e la rete cablata, gestendo il traffico di rete.
- **Distribution System:** Sistema di distribuzione che collega più BSS, permettendo la comunicazione tra stazioni in diverse BSS.
- **Wireless Station:** Dispositivo finale che si connette alla rete wireless, come laptop, smartphone o tablet.

Modalità:

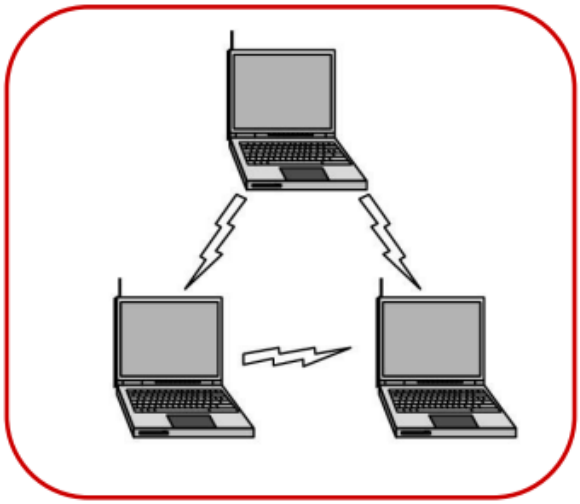
- **Infrastrutturata (BSS):** stazioni comunicano tramite un Access Point (AP).
- **Ad-Hoc (IBSS):** comunicazione diretta tra stazioni.

Modalità Infrastrutturata (Infrastructure BSS)



Le stazioni comunicano attraverso l'AP (anche se non si vedono direttamente)

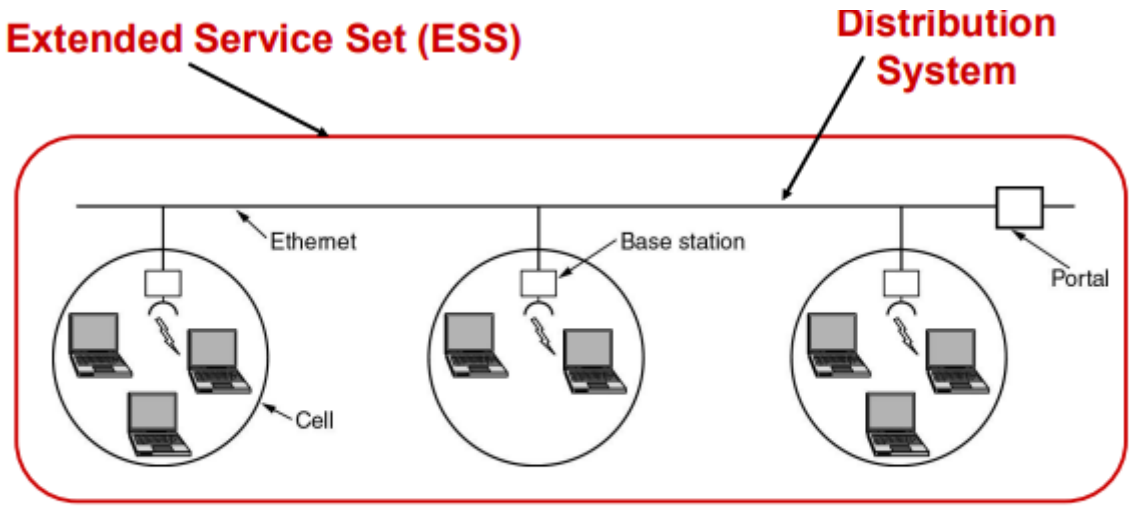
Modalità Ad-Hoc (Independent BSS)



Le stazioni comunicano in modalità peer-to-peer e solo se si vedono direttamente

Extended Service Set (ESS):

- Coordinamento di più AP per mobilità trasparente.
- AP come bridge tra WLAN e LAN (unico dominio broadcast).



Occorre gestire l'associazione delle stazioni agli AP
Permette la mobilità delle stazioni trasparente agli strati superiori
Gli AP sono configurati come bridge tra WLAN e LAN, così l'intero ESS è visto come un'unica LAN (unico dominio di broacast)

Problemi di accesso multiplo nelle WLAN

Problemi specifici rispetto alle LAN cablate:

- **Stazione nascosta:** il carrier sensing risulta limitato.
- **Stazione esposta:** difficoltà nell'utilizzo del canale.
- Half-duplex impedisce collision detect.

Accesso al canale (CSMA/CA):

- **DCF:** accesso distribuito (RTS/CTS per evitare collisioni, ACK per confermare trame ricevute).
- **PCF:** AP gestisce il polling e trasmette beacon per sincronizzazione e associazione.

Protocollo MAC 802.11

Protocollo MAC 802.11 – DCF (Distributed Coordination Function)

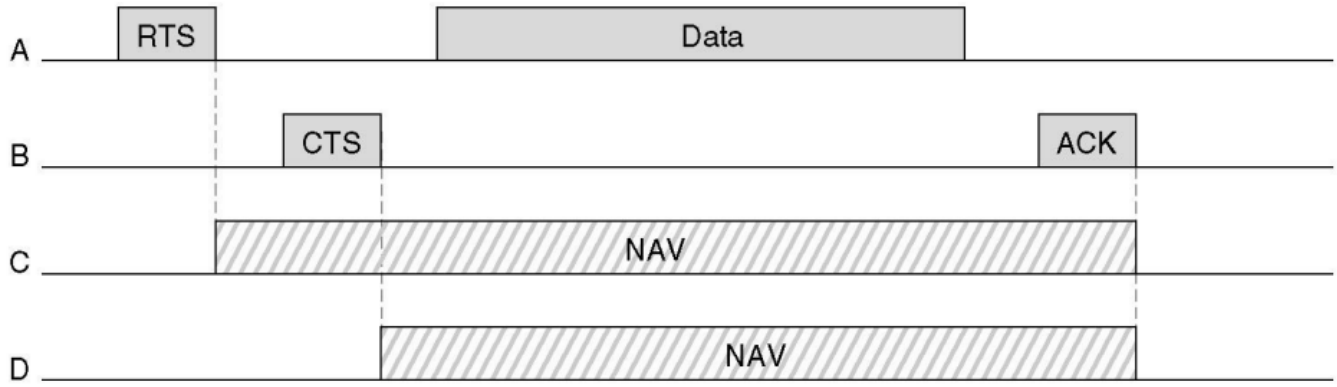
Request to Send (RTS): Prima che un mittente invii una trama, invia un RTS al destinatario. Questo avvisa le altre stazioni che il canale sta per essere occupato e indica la durata dell'occupazione.

Clear to Send (CTS): Se il destinatario è pronto a ricevere, risponde con un CTS. Questo avviso viene ricevuto anche dalle stazioni che vedono il destinatario ma non il mittente, informandole che il canale sarà occupato per un certo periodo.

ACK (Acknowledgment): Solo il ricevitore può rilevare se una trama è errata, inviando un ACK al mittente per ogni trama ricevuta correttamente. Se scade il timeout prima dell'ACK, il mittente ritrasmette la trama, preceduta da un nuovo RTS.

Carrier Sensing Virtuale (NAV): Le stazioni che non vedono direttamente il canale, ma lo percepiscono attraverso il NAV, evitano di trasmettere durante il periodo di occupazione del canale.

Backoff Esponenziale Binario: In caso di collisione tra RTS, viene applicato un backoff esponenziale, in cui il tempo di attesa aumenta esponenzialmente con ogni tentativo di trasmissione fallito (2^n).



Protocollo MAC 802.11 – PCF (Point Coordination Function)

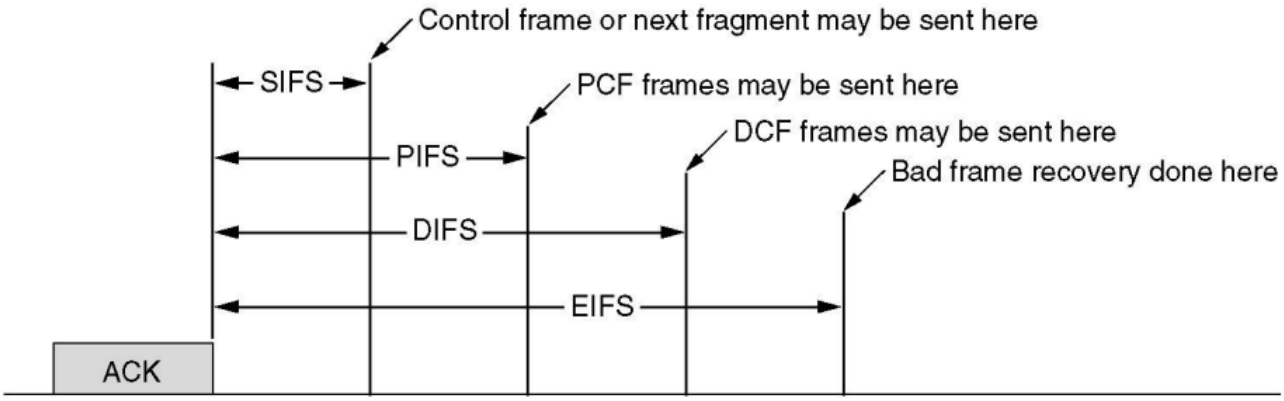
Gestione del Canale da parte dell'Access Point (AP): In modalità infrastrutturata, l'AP gestisce il canale a polling, assegnandolo a turno alle stazioni che devono trasmettere.

Beaconing: L'AP invia periodicamente segnali di beacon che consentono la sincronizzazione delle stazioni, la rilevazione della presenza dell'AP e la possibilità di entrare nel processo di polling.

Scansione Canali: Quando una stazione si attiva, scandisce i canali disponibili per cercare i beacon di un AP con cui associarsi. Il beacon mostra anche l'SSID (se impostato), che identifica l'AP.

Tempi di Spaziatura tra i Frame:

- **SIFS (Short InterFrame Spacing):** Utilizzato per i frame di risposta rapida come ACK, CTS o frammenti di trama successivi.
- **PIFS (PCF InterFrame Spacing):** Usato per i frame gestiti dall'AP durante il polling.
- **DIFS (DCF InterFrame Spacing):** Usato per l'accesso al canale da parte delle stazioni.
- **EIFS (Extended InterFrame Spacing):** Usato quando una stazione riceve un frame inatteso, segnalando l'errore.



Dato che la possibilità di collisione si limita ai pacchetti di richiesta e non ai dati veri e propri, il problema si riduce notevolmente poiché i pacchetti sono decisamente più piccoli e dunque temporalmente meno lunghi da trasmettere.

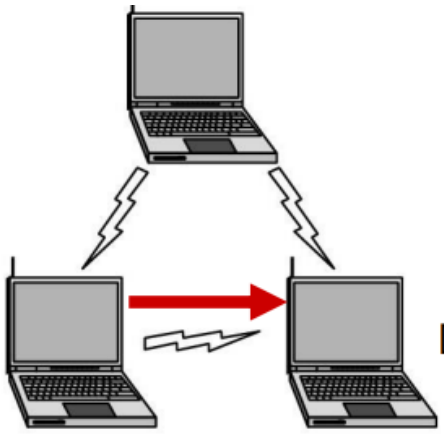
Struttura della Trama: La struttura della trama presenta quattro campi per gli indirizzi. Questo è dovuto al fatto che la consegna avviene in maniera indiretta tra mittente e ricevente. A differenza del modello IP, dove utilizziamo il data link, qui dobbiamo salvare gli indirizzi dell'intermediario, ovvero l'**access point** (indirizzo 3). Inoltre, qualora fossimo in un **Wireless Distribution System**, ci servirà anche un secondo access point (indirizzo 4).

Indirizzamento

IBSS (Ad-Hoc):

- SA = Mittente e trasmettitore
- DA = Destinatario e ricevitore
- Address 1 = DA, Address 2 = SA
- BSSID = Casuale, generato da una stazione dell'IBSS

IBSS (Ad-Hoc)



DA = destinatario e Rx

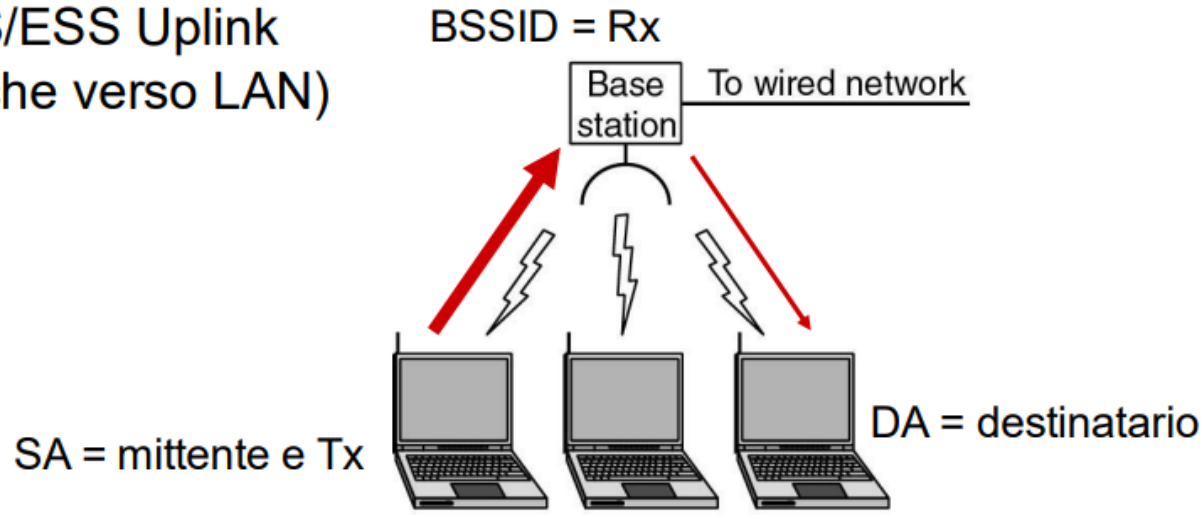
SA = mittente e Tx

Address 1 = DA
Address 2 = SA
Address 3 = BSSID (casuale generato da una delle stazioni nell'IBSS)
Address 4 = N/A
To DS = 0
From DS = 0

BSS/ESS (Uplink verso LAN):

- SA = Mittente e trasmettitore
- DA = Destinatario
- Address 1 = BSSID (Indirizzo MAC dell'AP)
- To DS = 1, From DS = 0

BSS/ESS Uplink
(anche verso LAN)

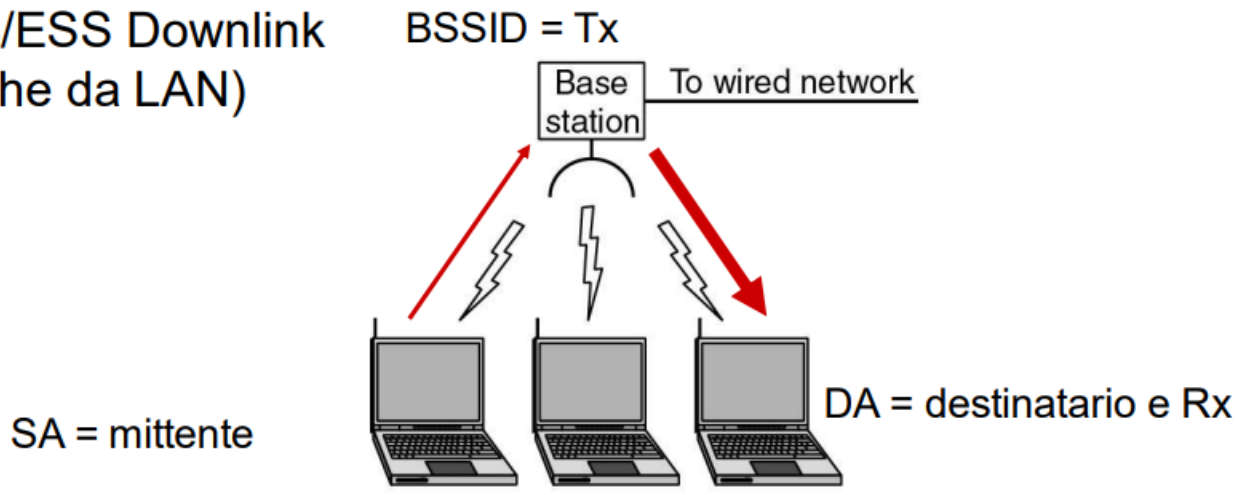


Address 1 = BSSID (MAC address dell'AP)
Address 2 = SA
Address 3 = DA
Address 4 = N/A
To DS = 1
From DS = 0

BSS/ESS (Downlink da LAN):

- SA = Mittente
- DA = Destinatario e ricevitore
- Address 1 = DA, Address 2 = BSSID (AP)
- To DS = 0, From DS = 1

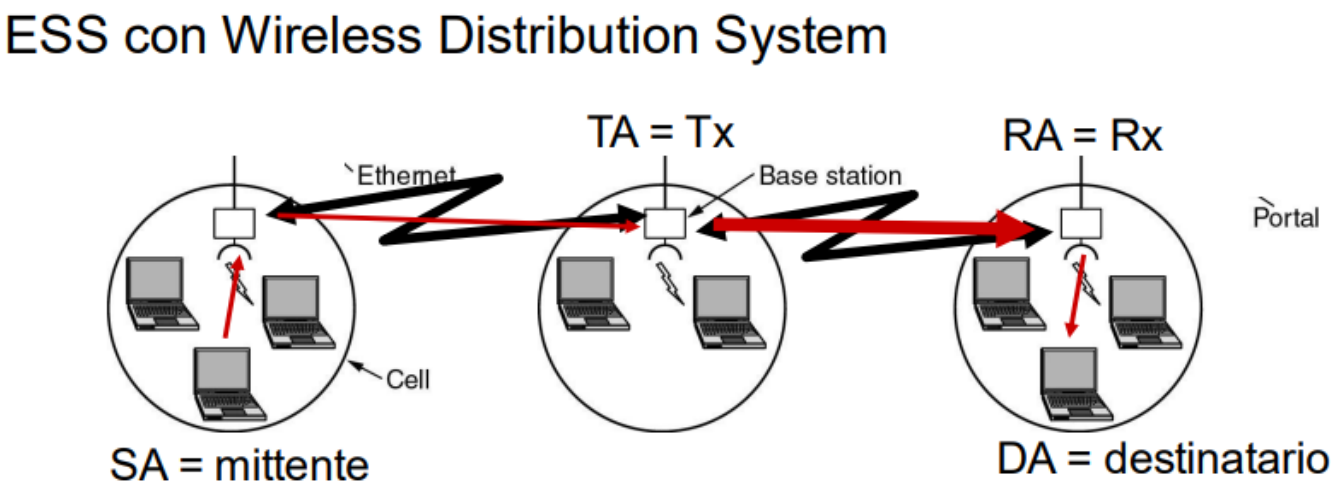
BSS/ESS Downlink
(anche da LAN)



Address 1 = DA
Address 2 = BSSID (MAC address dell'AP)
Address 3 = SA
Address 4 = N/A
To DS = 0
From DS = 1

ESS con Wireless Distribution System:

- SA = Mittente, DA = Destinatario
- Address 1 = RA (Ricevitore), Address 2 = TA (Trasmettitore)
- To DS = 1, From DS = 1



Address 1 = RA
Address 2 = TA
Address 3 = DA
Address 4 = SA
To DS = 1
From DS = 1