RETI DI TELECOMUNICAZIONI

PROF. FRANCO CALLEGATI

AA 2018/2019

Appunti di Greta Bucciarelli

SOMMARIO

1 - INTRODUZIONE ALLE RETI DI TELECOMUNICAZIONE 4
Il canale e la rete 4
Reti e Servizi 5
Multiplazione, Codifica e QoS 6
Le reti di calcolatori 8
2 – MEZZI TRASMISSIVI 13
Introduzione ai mezzi trasmissivi 13
Rame 13
Radiocollegamento 14
Fibra Ottica 16
3 – CANALE DI COMUNICAZIONE 20
Canale di Comunicazione 20
Controllo dell'Errore 20
Protocollo ARQ (Authomatic Repeat Request) 22
4 – PRESTAZIONI ED EFFICIENZA DEI PROTOCOLLI DI STRATO 2 24
Prestazioni dei protocolli ARQ 24
5 – INTERNET E IP 26
I protocolli di Internet 29
L'instradamento IP 31
Classless VS Classfull: la logica degli indirizzi IP 34
6 – PROTOCOLLI E TECNOLOGIE CORRELATE A IP 37
ARP (Address Resolution Protocol) 37
Configurazione dell'Interfaccia IP 37
Protocollo ICMP 38
Packet filter e firewall 39
NAT (Network Address Translation) 40
VPN (Virtual Private Network) 42
IPV6 43
7 – ROUTING 44
Instradamento delle reti IP 44
Il router IP 48
8 – PROTOCOLLI DI ROUTING 49
Instradamento dell'internet Globale 49
Interior Gateway Protocols (IGP) 49
Exterior Gateway Protocols (EGP) 52

9 – LAN (Local Area network) 55
MAC 55
Progetto IEEE 802 56
ETHERNET e IEEE 802.3 56
Soluzioni per lo strato fisico dell'Ethernet 57
Il Cablaggio delle LAN moderne 59
Wireless LAN (WI-FI) 60
Interconnessione di LAN E Virtual LAN (VLAN) 61
10 – VIRTUALIZZAZIONE 63
Virtualizzazione di rete 63

1 - INTRODUZIONE ALLE RETI DI TELECOMUNICAZIONE

Il canale e la rete

Canali di comunicazione →mezzo di trasporto dei flussi informativi tra nodi

Flusso informativo:

- monodirezionale: una sola direzione → es: streaming
- bidirizezionale:
  - simmetrici: uguale capacità per entrambe le direzioni → es: telefono
  - asimmetrici: diversa capacità per entrambe le direzioni → es: adsl
- punto-punto: da un punto a un altro → es: posta elettronica
- punti-multipunto: da un punto a tanti →es: broadcast, multicast

Non c'è corrispondenza tra servizio e canale

Unicast: unico destinatario, **Multicast**: gruppo di destinatari, **Broadcast**: tutti

Componenti della Rete

→Terminali (codificano l'informazione in modo consono ad essere trasferita in rete)

→Mezzi trasmissivi (insieme di canali che permettono il trasferimento di uno a molti flussi di informazioni)

→Nodi di comunicazione (utilizzo mezzi trasporti al fine di creare canali di comunicazione sulla base delle richieste degli utenti)

Topologie di Rete → la rete è descrivile tramite un *grafo* ed è composta da *rami* e *nodi*

- Maglia completa
  - Collegamenti per ogni coppia di nodi
  - N nodi implicano $\frac{N(N-1)}{2}$ collegamenti
- Stella
  - N collegamenti
  - Centro stella smista informazioni
- Anello
  - Anelli monodirezionali
    - Collegamento si interrompe se la rete si guasta
  - Anelli bidirezionali
    - Maggiore complessità per maggiore resistenza ai guasti
- Bus
  - Attivo/passivo
    - Semplice, economico, poco resistente
  - Bidirezionale
    - Mezzo di trasmissione condiviso
    - Necessario definire opportuno protocollo di accesso (MAC)
- Rete gerarchica
  - Terminali connessi a nodi periferici
  - Interconnessione a lunga distanza

Rete di accesso →la parte di rete destinata al collegamento fra la sede dei singoli utenti finali fino alla prima centrale di commutazione e più in generale al collegamento tra un utente e il suo provider

Rete di transito → si indica la parte di una rete di telecomunicazioni deputata al trasporto dei dati degli utenti

Backbone → è un collegamento ad alta velocità di trasmissione e capacità tra due server o router di smistamento informazioni e appartenente normalmente alla rete di trasporto di una rete di telecomunicazioni.

Funzioni di Rete

- Trasmissione
  - Trasferimento fisico del segnale
- Commutazione
  - Instradamento delle informazioni all'interno della rete al fine di permettere la comunicazione fra punti terminali
- Segnalazione
  - Scambio delle informazioni necessarie per la gestione della comunicazione e della rete
    - Segnalazione in formato pacchetto utente e rete
    - Segnalazione interna alla rete
- Gestione
  - Tutto ciò che permette il mantenimento delle funzioni della rete: allacciamento rete, riconfigurazione, ecc.)

Reti e Servizi

Integrazione → trasporto unificato dell'informazione: se una rete trasporta un bit, allora trasporta qualsiasi tipo di servizio

Elaborazione → i segnali digitalizzati sono trattabili come sistemi di elaborazione elettronica (inserimento di nuove informazioni, compressione, cifratura, …)

Le reti si sono evolute in base al servizio

- Diversi servizi → reti separate (diversi tecnologie, diversi apparati, diversi gestori e schemi tariffari)
- Minore dipendenza tra reti e servizi

→ offerta dei servizi molto aumentata nell'ultimo decennio, perché gli utenti fanno un uso intensivo de servizi.

Esistono caratteristiche comuni e differenze

- Tipologia di iterazione nella comunicazione
- Modalità con cui fluiscono le informazioni
- Topologia di informazioni

Esempi:

- Diffusione radio/tv
  - Tradizionale → televisore, digitale terrestre (DVB-T), satellitare (DVB-S)
  - Ricezione tramite apparati radiomobili per telefonia (DVB-H)
  - Ricezione tramite rete di trasmissione (streaming, podcasting)
- Comunicazione vocale
  - Telefonia fissa (ISDN)
  - Telefonia mobile
  - Telefonia tramite reti di dati (VoIP)
- Comunicazione dati
  - Computer connessi in rete
  - Collegamento rete telefonica o LAN
  - Telefoni cellulari o altri dispositivi portatili

Servizio

- Monomediale (unico segnale e informazioni di un unico tipo →es TV)
- Multimediale (trasporta informazioni di almeno due tipologie diverse e sono trasportate dalla medesima rete con modalità distinte→ es VIDEOCONFERENZA)

Tassonomia dei servizi ITU

- Servizi interattivi →tramite destinatario
  - Conservazione: scambio informativo in tempo reale (telefonata)
  - Messaggistica: scambio informativo in tempo differito (SMS)
  - Consultazione: scambio informativo con flusso controllato (WWW)
- Servizi distributivi
  - Senza controllo di presentazione →non controlla ordine di prestazione
  - Con controllo di presentazione → utente di destinazione può controllare l'ordine con cui ricevere le informazioni

Qualità dei servizi

- Trasparenza
  - Semantica → integrità delle informazioni trasportate
  - Temporale → variabilità dei ritardi di transito
- QoS (Quality of Service) → qualità della comunicazione percepita dall'utente del servizio (minimo di ritardo sempre presente)
  → indicatori di QoS:
  - Applicazioni non real-time:
    - Bassa probabilità di errore → trasparenza semantica
  - Applicazioni real-time:
    - Basso ritardo e Jitter → trasparenza temporale
    - Isocroni: servizi che richiedono la trasparenza temporale per la corretta interpretazione dell'informazione

Servizio e canale

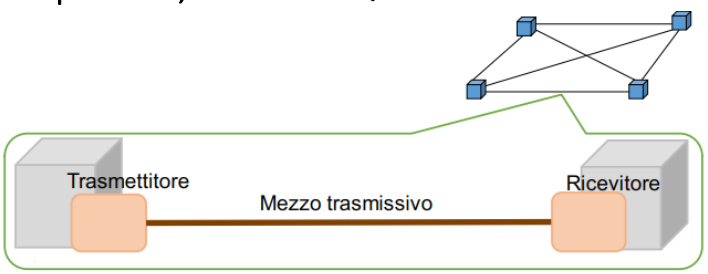
→ non esiste diretta corrispondenza fra tipologia di canale e tipologia di servizio: Es: stesso servizio multicast può essere implementato con canali broadcast, canali punto-punto o architettura mista

Integrazione

→ servizi diversi = diversi requisiti

→ una rete integrata nei servizi deve essere flessibile nella Allocazione della banda e la gestione della qualità di servizio

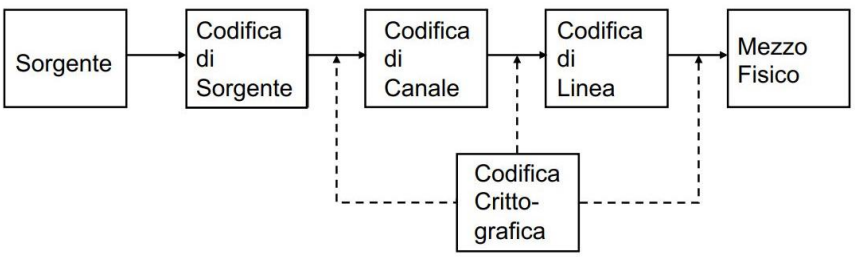
Multiplazione, Codifica e QoS



→ i nodi di rete sono connessi tramite collegamenti

→ collegamento caratterizzato dal mezzo trasmissivo: rame, fibra ottica, radio collegamento

Codifica



1. Ognuno di questi blocchi corrisponde decodifica
2. Operazioni di codifica/decodifica combinate in vari nodi (canale/linea, sorgente/canale, ...)
3. Crittografia può essere inserita in diverte parti

CODIFICA DI SORGENTE:

- Elimina ridondanza
- Diminuire velocità emissione senza compromettere la fruibilità delle informazioni

CODIFICA DI CANALE

- Aggiunge bit di controllo dell'errore

CODIFICA DI LINEA

- Trasforma sequenza di bit in sequenza di simboli per adattare a mezzo trasmissivo

CODIFICA CRITTOGRAFICA

- Trasformazione sequenza di simboli rendendola incomprensibile a chi non ha le chiavi

Multiplazione →più condizioni trasporto stesso mezzo trasmissivo

Si può realizzare utilizzando (dal punto di vista teorico tutte queste modalità sono equivalenti):

- Tempo → time division multiplexing (TDM)
- Frequenza → frequency division multiplexing (FDM)
- Codice → code division multiplexing (CDM)
- Spazio

→ Differiscono per modalità di implementazione

La tecnologia di implementazione rende più o meno conveniente una soluzione rispetto alle altre

TDM (multiplazione a divisione di tempo)

- Slotted → slot prefissati, unità formative hanno la stessa lunghezza commisurata allo slot
- Unslotted → lunghezza variabile, sistema esplicito di delimitazione delle unità formative
- Framed → divisi in frame, sincronizzi la trama (frame) e non lo slot
- Unframed → slot si susseguono senza struttura, occorre un unità di sincronizzazione

Assegnazione della Banda

- Assegnazione statica
  - Banda dedicata
  - La banda non può cambiare a comunicazione in corso
  - La richiesta complessiva della banda è ben controllabile
- Assegnazione dinamica
  - Condividono la banda in base alla necessità
  - La banda può cambiare a comunicazione in corso
  - La richiesta di banda può diventare intollerabile (congestione)

S-TDM (Synchronous Time Division Multiplexing)

- Le unità informative vengono trasferite periodicamente con ritardo costante
  - Ogni periodo è uguale alla durata del frame

A-TDM (Asynchronous Time Division Multiplexing)

- Occorre definire la modalità di assegnazione della banda
- Modalità di gestione delle situazioni di contesa

La velocità di flusso dei bit (bit rate) è determinata da un **oscillatore locale** → errore contenuto dentro una tolleranza → Possibili soluzioni:

- **Reti plesiocrone:** oscillatori posti su nodi distinti sono indipendenti e forniscono velocità leggermente diverse
- **Reti sincrone:** oscillatori su tutti i nodi, velocità uguali (a meno del rumore)

Le reti di calcolatori

Sistemi Chiusi (produttori di calcolatori vendevano a banche e governi)

→ Incompatibilità (ostacoli alla comunicazione)

→ **Standard ISO OSI** (inserimento di uno standard come soluzione)

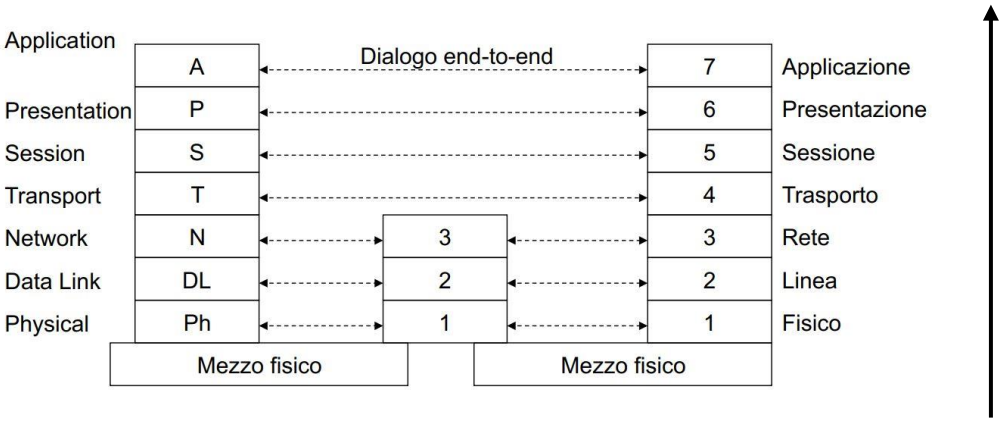
- Problemi
  - Diversità delle reti →Calcolatori non riescono a comunicare, non riescono ad interpretare segnali di altri, no cooperazione in sistema distribuito
- Soluzione
  - Realizzazione di standard unificati →realizzazione di Sistemi Aperti (cioè realizzare una rete di calcolatori in cui qualunque terminale comunica con qualunque fornitore di servizi mediante qualunque rete)
    1. Modello di riferimento → architettura a strati
       a. Scompone il problema in sotto-problemi, più semplici da trattare
       b. Livelli indipendenti
       c. Servizi e interfacce
    2. Stabilire regole comuni → standard

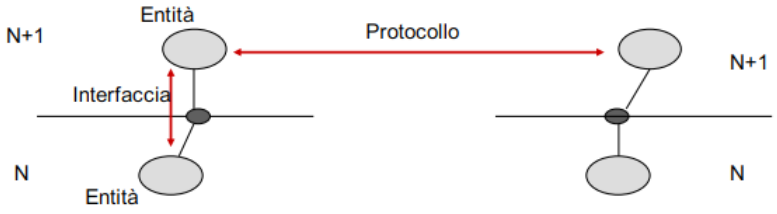
Le definizioni contenute nell'OSI coinvolgono 3 livelli di astrazione:

- Modello di riferimento: *schema concettuale, numero di strati coinvolti, definizione funzioni strati*
- Definizione di servizi: *ciò che viene fornito un servizio da uno strato*
- Specifiche di protocolli e interfacce: *come viene fornito un servizio da uno strato*

Modello di riferimento

- 1,2,3 sono *lower*
- 4 è il raccordo tra i due
- 5,6,7 sono *upper*



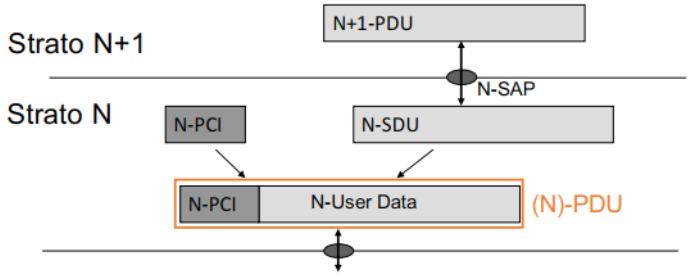


Entità: ogni elemento attivo in uno strato, identificato da numero simbolico (title)

Protocollo: regole dialogo tra entità dello stesso livello

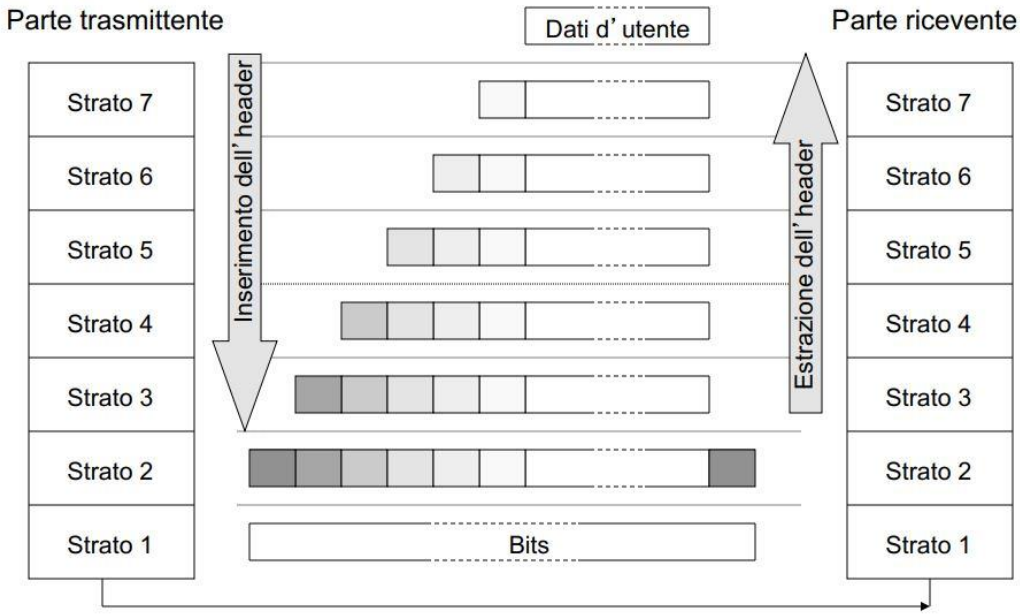
Interfacce: regole di dialogo tra entità di livelli vicini → con quelli comunicanti

Trasferimento dei dati



- PDU (n-Protocol Data Unit) →dati trasferiti tra entità di strato n
- SDU (n-Service Data Unit) →dati passati dallo strato n allo strato n+1
- SAP (n-Service Access Unit) →indirizzo di identificazione del flusso dati tra n+1 e n
- PCI (n-Protocol Control information): info aggiuntive per il controllo del dialogo a livello n
- ENCAPSULATION: N-PDU = N-PCI+N-SDU

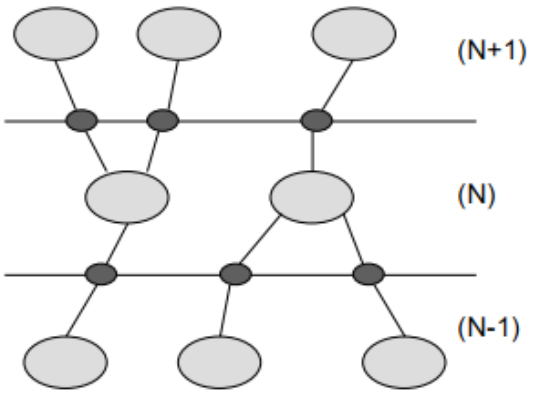
Flusso delle Informazioni



Un entità di strato N può servire a più (N)-SAP contemporaneamente

Un utilizzatore di strato N può servirsi di più (N)-SAP contemporaneamente

Dello stesso (N)-SAP non è permesso connettere più (N)-user



Modalità di Servizio

- Connection oriented: instaurazione →trasferimento →chiusura
- Connectionless: per ogni accesso al servizio fornite tutte le info per il trasferimento dei dati. Ogni unità viene trasferita in modo indipendente

Modalità di dialogo

- Confermato: *esplicita conferma*
- Non confermato: *no esplicita conferma*
- Parzialmente confermato: *richiesta confermata dal Service-Provider*

Segmentazione e Riassemblamento: divedere e il contenuto di una SDU in una o più PDU → per conformarsi alla lunghezza massima dei messaggi (dopo c'è la riunione dei vari segmenti)

Multiplazione: più connessioni di strato n mappate in uno strato n-1, condivisione di risorse

Splitting: criterio, aumenta flessibilità e velocità di trasferimento die dati

Strati ISO/OSI

Strato 1 - strato fisico: *porta in giro i bit*

- Trame
- Compito: ATTIVARE, MANTENERE e DISATTIVARE connessioni tra entità di strato 2
- Specifica modalità di invio dei singoli bit sul mezzo trasmissivo
- Per fare questo deve specificare le caratteristiche:
    - Meccaniche
    - Elettriche
    - Funzionali
    - Procedurali

Strato 2- datalink: *gestione mezzo fisico*

- Frame
- Compito: ATTIVARE, MANTENERE e DISATTIVARE la connessione tra due entità di strato 3
- Rendere affidabile il collegamento fra i nodi d rete
- Funzioni:
    - Strutturazione flusso di dati →frames
    - Controllo e gestione di errori di trasmissione
    - Controllo di flusso
    - Controllo di sequenza

Strato 3- rete: *implementazione delle strade*

- Datagrammi
- Compito: far giungere i pacchetti al destinatario scegliendo la strada all'interno della rete
    - Commutazione di pacchetto →ROUTING
    - Necessario individuare i destinatari →schema di indirizzi (deve essere universale in una rete globale)

Strato 4- trasporto: *è il camion che trasporta i dati*

- Segmenti
- Compito: fornire un canale sicuro end-to-end, svincolando strati superiori da tutti i problemi
- Adottare la dimensione dei frammenti forniti dagli strati superiori (files) a quella dei pacchetti (richiesta dalle reti) →funzione di Pacchettizzazione (segmentazione/riassemblamento)
- Altre funzioni: controllo errore flusso, gestione dati prioritari
- Non tutte le applicazione hanno bisogno delle stesse funzioni →classi di traporto

Strato 5- sessione: *gestire complessità della comunicazione*

- Messaggi
- Compito: Suddivide il dialogo in unità logiche →sessioni
- Permetta chiusura ordinata (soft) del dialogo
- Introduce punti di sincronizzazione
- Molte funzioni più o meno complete rispetto le richieste

Strato 6- presentazione: *traduttore*

- Messaggi
- Compito: Adatta il formato (sintassi) dei dati usato dagli interlocutori preservando il significato (semantica)
- Da sintassi locale a sintassi di trasporto

Strato 7- applicazione: *utente della rete*

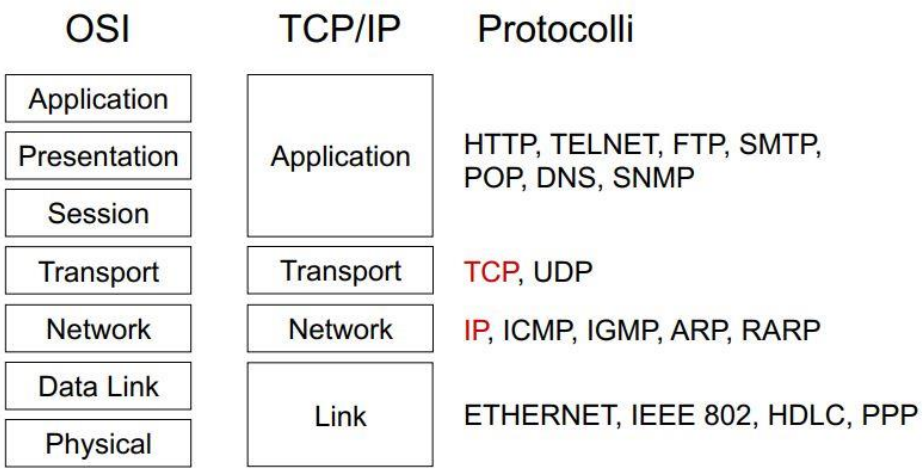
- Messaggi
- Rappresenta il programma applicativo (Applicazione)
- Non può essere completamente standardizzato →solo su richiesta di gruppi utenti interessati

Rete universale → diffusa e unica a livello mondiale

  - Strato *Transport* deve essere unico
  - Strato di *Rete* (internetworking) deve essere unico
- Osi definisce i protocolli che devono essere adottati da tutti i computer per creare una rete aperta universale
  - Protocollo IP e protocollo di Trasporto

Effetti della diffusione di Internet

- Mentre il modello di riferimento è stato universalmente adottato come modo di organizzare le architetture dei protocolli, il protocollo IP di OSI ed il Transport non hanno avuto successo
- La causa è stata la diffusione di Internet e del suo protocollo, il TCP/IP
- TCP è un protocollo di Transport e IP è il protocollo di interconnessione di reti, incompatibili ed in concorrenza con quelli di OSI.
- TCP/IP non si occupa dei protocolli degli strati inferiori che possono essere progettati usando le regole di OSI
- L'architettura TCP/IP non usa gli strati di Sessione e presentazione ma si interfaccia direttamente con l'Applicazione



La rete

Obbiettivo della rete: consentire una comunicazione tra una qualunque combinazione di terminali (riconfigurazione dinamica della struttura) con un livello accettabile di QoS (assegnazione delle risorse, controllo del canale di comunicazione).

Ipercubo della rete

la comunicazione tra utenti rappresenta solo una parte delle informazioni che viaggiano in rete:

- Garantire corretto comportamento della rete
- Gestione riconfigurazioni e malfunzionamenti
- Gestione gli aspetti economici (trafficazione)

Tecniche di commutazione → insieme di funzionalità/tecniche per il funzionamento logico dei nodi

- **Di Circuito**: canale di comunicazione dedicato, ritardo iniziale per instaurare il circuito
  → Dopo è garantita la trasparenza temporale per l'utente
  - PRO
    - Circuito dedicato che garantisce sicurezza ed affidabilità
    - Trasparenza temporale
    - Procedure di controllo a inizio e fine chiamata
  - CONTRO
    - Se le sorgenti hanno basse attività, circuito sottoutilizzato
    - Non si può variare la capacità del canale
- **Di Pacchetto** (o di messaggio): informazioni in forma numerica + informazioni di segnalazione
  - I messaggi vengono suddivisi in sotto-blocchi con una lunghezza massima prefissata per
    - Motivi di linea: evitare frammenti troppo lunghi per rumore
    - Motivi di rete: limitare tempi di attesa nei nodi
  - Tecniche di commutazione
    - Connection oriented →Circuito virtuale
      - Scambio di informazioni →procedura di segnalazione in cui viene stabilito il percorso dei pacchetti da un'origine a una destinazione
      - *Numero di Circuito virtuale* →Tutti i pacchetti percorrono questo percorso
    - Connectionless →Datagramma
      - Ogni pacchetto viene gestito in modo indipendente, senza relazione con gli altri pacchetti (anche della stessa connessione)
      - Ogni pacchetto ha tutte le informazioni di indirizzamento per arrivare a destinazione
      - Pacchetti diversi possono seguire percorsi diversi e (possono avere tempi di percorrenza diversi)
  - PRO
    - Maggiore utilizzazione dei collegamenti, stessa linea condivisa da più chiamate
    - Rete supporta diverse velocità
    - Trasparenza semantica →meccanismi di errori
  - CONTRO
    - Non adatto per il real-time→ tempo di transito non garantito

2 – MEZZI TRASMISSIVI

Introduzione ai mezzi trasmissivi

Legge di Moore o di Edholm

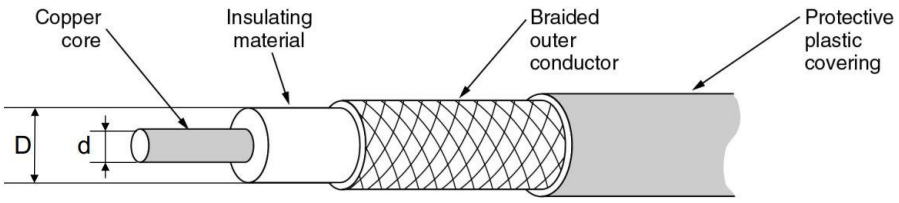
Ogni circa 18 mesi la banda a disposizione dell'utente raddoppia, a costo circa costante

Attenuazione

- Qualunque mezzo trasmissivo degrada il segnale elettromagnetico mentre questo si sposta
- Misura di questo degrado si dice Attenuazione e si misura la perdita di potenza del segnale in db/Km
- Nelle linee in rame: l'attenuazione cresce esponenzialmente con la lunghezza del collegamento e con la radice della frequenza del segnale → quindi molto difficile portare lontano segnali ad alta frequenza

Rame

- Cavo coassiale
  - Attenuazione cresce esponenzialmente con lunghezza
  - Più è maggiore D, tanto maggiore è il costo e tanto migliori sono le prestazioni
  - Multiplatore a divisione di frequenza (FDM)



da Tanenbaum

D=diametro conduttore esterno, d=diametro conduttore interno → due conduttori cilindrici coassiali

- Cavo bifilare
  - Coppie intrecciate da posare in cavi →problema della diafonia
  - Costruite per le linee telefoniche anni 80

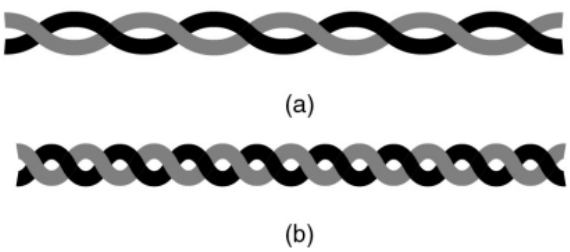
Twisted Pairs (coppie intrecciate)

➔ STP (shilded twisted pairs)
- Ogni coppia nel cavo è avvolta in un conduttore che fa da schermo
- Più costoso
- Lo schermo deve essere emesso a massa

➔ UTP (unshilded twisted pairs)
- Meno costose e più semplici da posare

Vengono studiati modi per migliorare le prestazioni

- Aumentare il diametro dei conduttori e migliorare la qualità del dielettrico
- Migliorare la regolarità e infittire l'avvolgimento

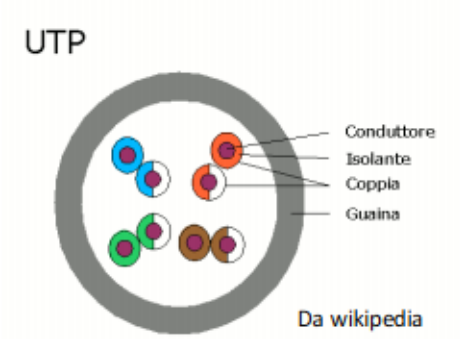


da Tanenbaum

(a) Category 3 UTP.
(b) Category 5 UTP.

Vengono definiti livelli di qualità → **Categoria** → da categoria 1 a categoria 7

- Categoria 1: (TIA/EIA-568-B). Usato per la Rete telefonica generale, ISDN e per i citofoni.
- Categoria 3: (TIA/EIA-568-B). Usata per reti con frequenze fino a 16 MHz, molto diffusa per le reti Ethernet a 10 Mbit/s.
- Categoria 5 (non riconosciuta). Usata per reti con frequenze fino a 100 MHz; come ad esempio ethernet a 100 Mbit/s.
- Categoria 5e (TIA/EIA-568-B). Usata per reti con frequenze fino a 200 MHz, come ad esempio fast ethernet e gigabit ethernet.
- Categoria 6 (TIA/EIA-568-B). Usata per reti con frequenze minima per certificazione 250 MHz.
- Categoria 6a (TIA/EIA-568-B). Usata per reti con frequenze fino a 500 MHz.
- Categoria 7 (ISO/IEC 11801 Class F), nome informale. Lo standard specifica 4 STP all'interno di un unico cavo. Concepito per trasmissioni sino a 600 MHz.Categoria
- 7a (ISO/IEC 11801). Usata per reti con frequenze fino a 1 GHz.



Radiocollegamento

- **VANTAGGI**
  - mezzo broadcast → vantaggioso per i servizi diffusivi
  - mezzo adatto alla mobilità → non esiste vincolo fisico
  - metodo meno costoso e più veloce per distribuire il mezzo, anche in zone remote e poco popolate
- **SVANTAGGI**
  - problema della condivisione dello spettro → lo spettro radio è uno solo e il mezzo è condiviso → numero limitato di canali
  - attenuazione dei radio collegamenti
    - cresce con la distanza
    - cresce con il quadrato della frequenza
    - le attenne sono più efficienti quando la frequenza cresce
  - vulnerabile ai disturbi → possibili sabotaggi e fenomeni atmosferici
  - forti problemi di banda
- le onde elettromagnetiche si propagano in linea retta
    - > 3 MHz: visibilità diretta
    - 3 – 30 MHz: propagazione isoterica
    - < 30 MHz: solo visibilità diretta (ponti radio)

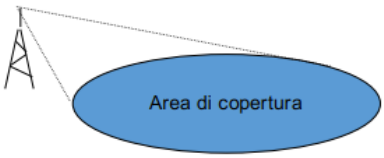
Evoluzione

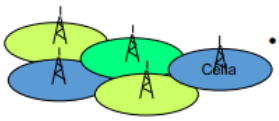
- 1895: esperimento di Marco ed invenzione delle radio-comunicazioni
- 1901: prima trasmissione transatlantica
  - All'inizio viene usata per portare segnali telegrafici (telegrafo)
  - Applicazione ai mezzi mobili (navi)
  - Con i progressi dell'elettronica diventa possibile creare le trasmissioni
    - Radiodiffusione → voce e musica
    - Telediffusione → immagini e suoni
- Anni '90: servizi di radiocomunicazione mobile per telefonia (cellulare)

Servizi su comunicazione radio

- trasmissioni punto-multipunto
- mobilità
- limitazione delle risorse → lo spettro radio è finito

- Diffusione radiofonica/televisiva
  - Raggiungere la maggior quantità di utenti possibili con un solo segnale
  - Pianificazione della localizzazione delle emittenti

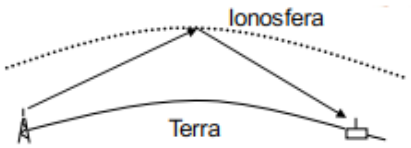




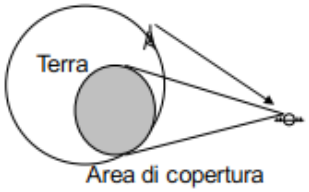
- Sistemi radiomobili
  - Segnale confinato in un' area limitata per poter riutilizzate lo spettro radio

Grande distanza

- Propagazione ionosferica
  - Servizio di radiodiffusione ad onda corta



- Radiocomunicazione via satellite
  - 1957 : Sputnik primo satellite artificiale
- Satelliti per TLC
  - Anni '60 : Intelsat
    - orbita geostazionaria (GEO = Geostationary Earth Orbit)
  - Anni '70-' 80
    - Satelliti molto semplici e stazioni a terra sofisticate e costose
      - Collegamenti televisivi transatlantici e mondovisione
  - Anni '90
    - Satelliti sofisticati con buona potenza in trasmissione
      - La stazione a terra può diventare molto economica
        - Global Position System (GPS)
        - Diffusione diretta da satellite (DBS)
        - Accesso ad internet tramite satellite
  - Oggi
    - Costellazioni di satelliti sofisticati che formano una rete
    - MEO: Medium-Earth Orbit (da 10000 a 5000 Km di altezza)
    - LEO: Low-Earth Orbit (<5000 Km di altezza)



Sistemi cellulari

→ la principale applicazione dei radio collegamenti e la telefonia mobile

- piccola potenza trasmessa
- segnali interferiscono solo con le celle adiacenti
- frequenze possono essere riusate in celle non adiacenti → gruppi di celle (cell cluster)
  - grazie a un centinaio di canali si può servire moltissimi utenti
- sono necessari terminali sofisticati

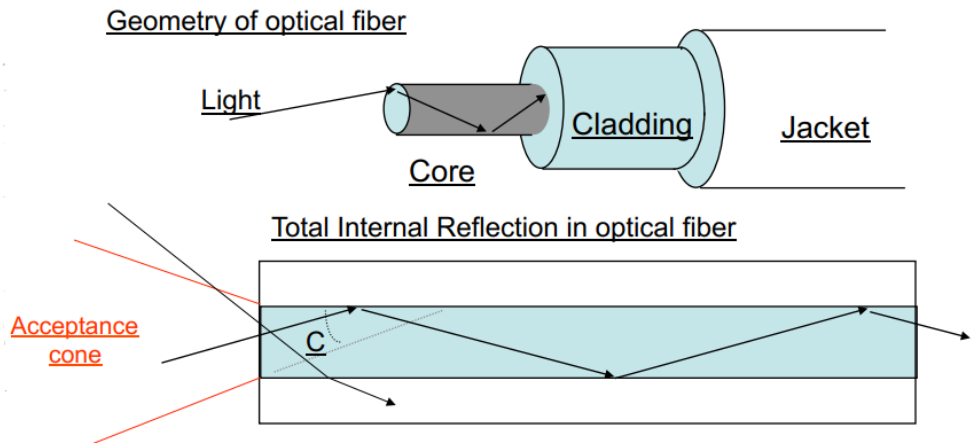
→ **ETACS** a 900 MHz: copertura nazionale, analogico

→ **GSM** (global system mobile): copertura mondiale, digitale

Ci sono diverse generazioni (III, IV, V)→ terminali con capacità multimediali

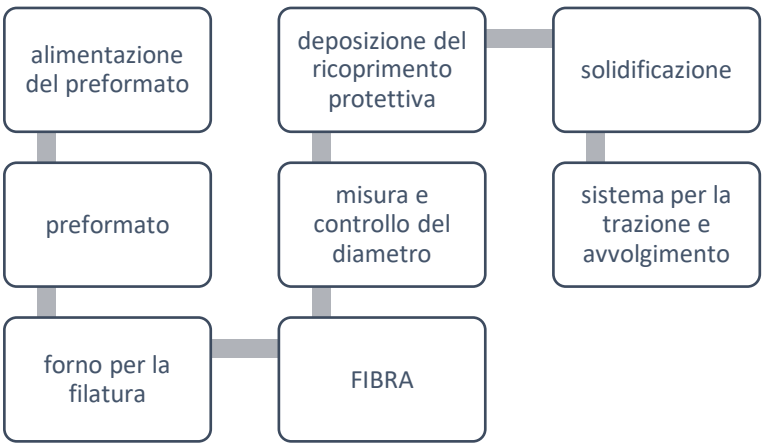
Fibra Ottica

- ➔ Sfruttano la riflessione totale della luce in corrispondenza dello strato di separazione fra uno strato interno (core) e uno esterno (cladding)
- ➔ Tanta banda
- ➔ Diafonia completamente assente
- ➔ Costo del cavo basso
- ➔ Filamento di **vetro** o **plastica**
- ➔ Utilizzata per i collegamenti a lunga distanza
    - Molto sottile
    - A densità differenziata
    - Diametro di 125 µm (poco più grande di una capello → 80 µm)

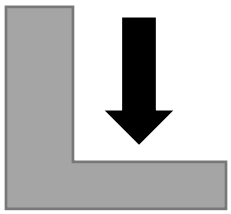


- ➔ **Core** (ha un indice di rifrazione più grande del cladding)
- ➔ I raggi di luce che colpiscono la discontinuità ad un angolo inferiore a quello critico sono completamente riflessi
- ➔ Il vetro assorbe parte della luce che lo attraversa → densità diminuisce a mano a mano che attraversa il vetro
- ➔ Strada che può percorrere un raggio luminoso prima che si dimezzi la sua intensità:
    - 3 cm in vetro comune → 10000 db/km
    - 3 m in vetro HQ → 1000 db/km
    - 15 km in fibra ottica di media qualità → 0.2 db/km

Come si costruisce la fibra

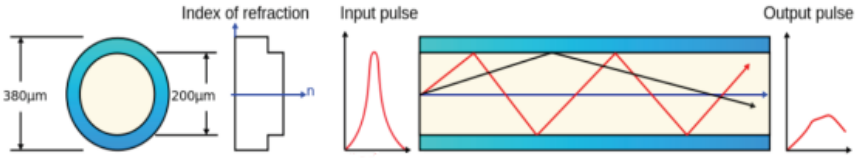


tutto questo viene svolto su un supporto meccanico (a forma di L) dall'alto verso il basso

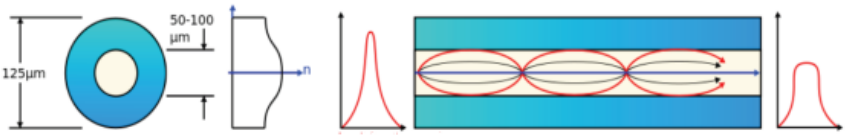


Tipi di fibre ottiche

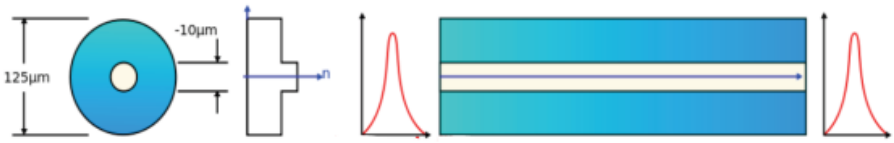
- **Multimode fiber**
  - **Step index fiber**



  - **Granded index fiber**

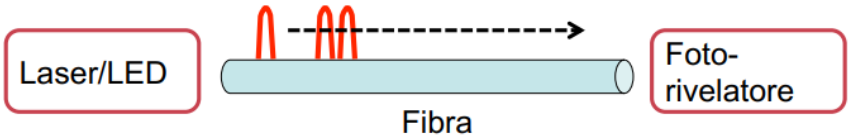


- **Singlemode fiber**



Sistema di trasmissione

➔ <u>Sorgente di luce:</u> laser, led generano gli impulsi
➔ <u>Impulsi</u>: si propagano per grandi distanze, generati ad alta velocità
➔ <u>Rilevatore</u>: fotodiodo riceve gli impulsi



Paradosso: <u>aumento esponenziale delle prestazioni con aumento dei costi circa nullo</u>

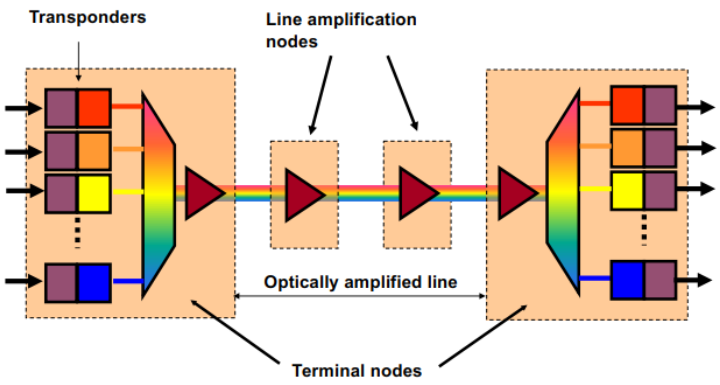
Problema → le fibre ottiche sono più difficili da giuntare (elemento critico → stabilità dell'allineamento)

- Giunto stabile: flash ottico che fonde le due fibre formandone una (Fusion Splicing Machine)
  - Perdita < 0,01 db
- Giunto Temporaneo: Connettori per unire le fibre (ma temporanei)
  - Perdita <0,1 db

WDM: Wavelenght Division Multiplexing

→ si trasmettono più flussi di informazione, utilizzando diversi colori della luce, che convivono sulla fibra senza danneggiarsi

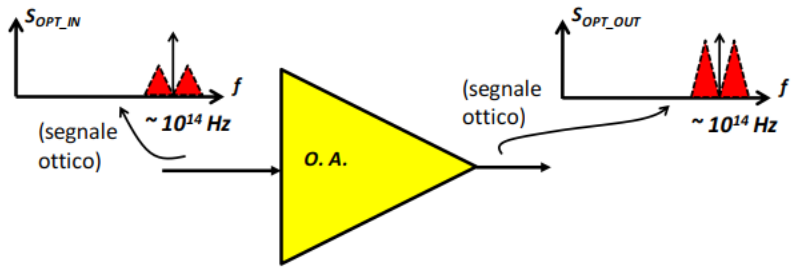
- È un modo alternativo per FDM
- Multiplazione di diversi flussi su diversi ambiti di frequenze (o di lunghezze d'onda)
- Permette di aumentare molto la capacità della rete senza installare nuove fibre



Principi del WDM

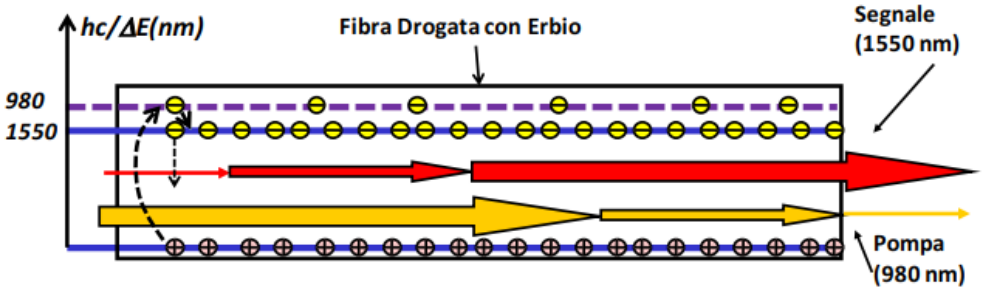
- Utilizzo dei diversi colori della luce per trasmettere più flussi
- I vari flussi convivono senza danneggiarsi sulla stessa fibra
- Più flussi uso, più informazione viene trasportata

Amplificatore Ottico



- Vantaggi
  - Maggior banda trasmettibile: segnale mantenuto a livello ottico
  - Segnale WDM ha tutti i canali che vengono amplificati
- Svantaggi
  - L'amplificatore effettua solo re-amplifying → necessario combattere dispersione e non-linearità
    → introducendo qualche stadio "3R" e prendendo contromisure per la dispersione (reticoli, fibre compensatrici…)

EDFA (amplificatore in fibra drogata all'erbio) → soluzione più utilizzata per segnali WDM



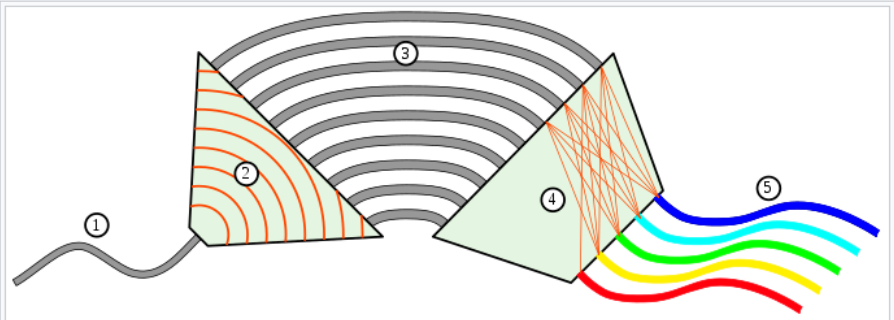
- Drogaggio di Erbio
  - Alcuni livelli instabili e un livello metastabile.
  - Laser di pompa → elettroni a livello instabile
  - Inversione di popolazione → da livello instabile a livello metastabile
  - Il segnale attraversa la fibra → amplificazione per emissione stimolata
- Amplificazione tramite diversi drogaggi
- Tecnologia consolidata per un segnale 1550 nm → guadagno di decine di db (cifra di rumore<10db)

Commutazione WDM

- Trasporto flussi informativi di diversi clienti su diversi colori → utilizzo il colore per distinguere punto di partenza e punto di arrivo
- Sono necessari apparati capaci di selezionare il colore della luca in modo comandato (ROADM)

ROADM → apparati che selezionano il colore della luce in modo complicato

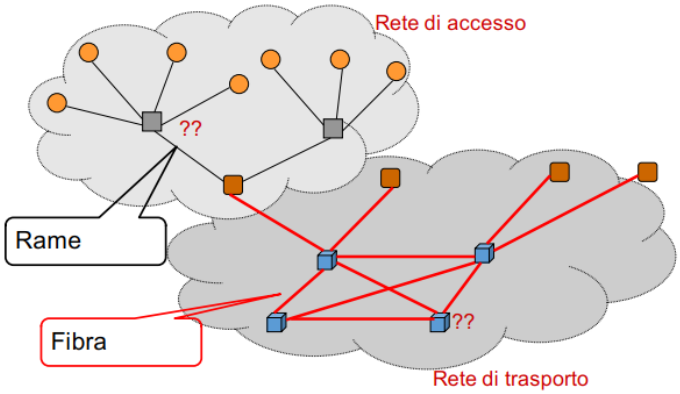
AWG → Arrayed Waveguide Gratings



La luce in entrata **(1)** attraversa uno spazio libero **(2)** ed entra in un fascio di fibre ottiche o guide d'onda del canale **(3)** . Le fibre hanno una lunghezza diversa e quindi applicano un diverso sfasamento all'uscita delle fibre. La luce attraversa quindi un altro spazio libero **(4)** e interferisce con le entrate delle guide d'onda di uscita **(5)** in modo tale che ciascun canale di uscita riceva solo luce di una certa lunghezza d'onda. Le linee arancioni illustrano solo il percorso della luce. Il percorso della luce da **(1)** a **(5)** è un demultiplexer, da **(5)** a **(1)** un multiplexer.

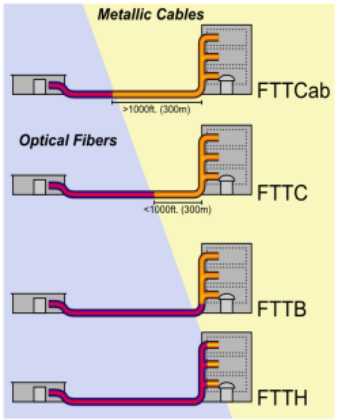
MEM → sposto la luce con piccoli specchi che si muovono autonomamente. Brevi tempi di reazione

Le reti di oggi sono formare così:



Come sostituire la rete di accesso in rame? → **FTTExchange, FTTCab, FTTC, FFTBuilding, FFTHome**

- Classificate in base alla localizzazione dell'interfaccia elettro/ottica (EOI)
  - Fiber To The Exchange (FTTE): EOI in centrale
  - Fiber To The Cab (FTTCab): EOI in the equivalent of the PSTN cabinet
  - Fiber To The Curb (FTTC): EOI in the equivalent of the PSTN distribution point
  - Fiber To The Building (FTTB): EOI at the basement
  - Fiber To The Home (FTTH): EOI in the NIU



Accesso in fibra

- Attivo: nel percorso elementi attivi che consumano energia, costoso ma efficiente
- Passivo: solo elementi passivi nel percorso, più economico e affidabile, meno

3 – CANALE DI COMUNICAZIONE

Canale di Comunicazione

Protocolli Data Link: sequenziale a banda costante di tipo punto-punto o punto-multipunto

- Le trame arrivano nella stessa sequenza con cui sono inviate a meno degli errori
- Tutti sperimentano ritardi di propagazione circa uguali

Protocolli Trasporto: canale non sequenziale a capacità variabile

- Perdita di dati (errori di trasmissioni, scarto dei nodi)
- Duplicazione dei dati
- Ritardi variabili
- Arrivi fuori sequenza

Controllo del canale: strato 2

→ I servizi di controllo del canale intendono rendere affidabile e sicuro il servizio di collegamento che lo strato 2 offre alle entità di strato 3

Funzioni (non tutti i protocolli di strato 2 hanno tutte queste funzioni)

- Strutturazione del flusso dati, controllo e gestione degli errori, controllo di flusso, controllo di sequenza

Problematiche di Sincronismo

→ nelle trasmissioni numeriche per riconoscere i bit in ricezione occorre determinare gli istanti di campionamento per ricostruire il **sincronismo di cifra**. Un circuito nel ricevitore estrae il segnale di sincronismo ma ha bisogno di **agganciarsi.** Possibili mobilità: Il canale può essere tenuto sempre pieno di bit o il canale può avere momenti di vuoto di segnale.

Sincronismo di Trama

Il sincronismo di cifra garantisce la corretta lettura dei singoli bit, ma rimane il problema di distinguere le varie PDU. Si deve garantire il sincronismo di trama: protocolli **asincroni** a livello di trama e protocolli **sincroni** a livello di trama

Garantire affidabilità

→ Come garantire affidabilità? Prima di consegnare i dati allo strato superiore si controllano → errori di trasmissione, sequenzialità dei dati e flusso dei dati

Controllo dell'Errore

Codici di blocco: si applica codifica a blocchi di kbit di informazione vengono calcolati r bit di ridondanza come funzione combinatoria dei kbit e vengono trasmessi $n = k + r$ bit

Codici Convoluzionali: r bit calcolati mediante reti logiche sequenziali

Gestione dell'errore: la codifica di canale → tipicamente si applica codifica a blocchi

$\boldsymbol{k}$ bit vengono codificati in una parola di $\boldsymbol{n}$ bit aggiungendo $\boldsymbol{r = n - k}$ bit

$\boldsymbol{2^n}$ Parole di codice per trasportare $\boldsymbol{2^k}$ messaggi

- $\boldsymbol{2^k}$ Sono parole di codice ammesse → valide
- $\boldsymbol{2^n - 2^k}$ Sono le parole di codice non ammesse → non valide

- Codici a rilevazione d'errore (protocolli di linea o di trasporto)
  → *Numero limitato bit aggiuntivi, necessaria ritrasmissione*
  - Ricezione di parola di codice invalida, indica la presenza di errori di trasmissione
  - Non si può dire quanti bit di errori
  - Per gestire la trasparenza semantica è necessario ritrasmettere dati errati
- Codici di correzione d'errore (strato fisico)
  →*Richiede numero abbastanza alto di bit aggiuntivi*
  →Protocollo linea e trasporto, conviene con canale affidabile, dove ci sono pochi errori
  - Una parola di codice invalida indica
    - Presenza di errori trasmissione
    - Permette di individuare la parola valida corrispondente
    - Garantire la trasparenza semantica in tutti i casi in cui errore è correggibile

Codici lineari

- Dati due messaggi di k bit m1 e m2
- Ricavate le parole di codice c1 e c2
- Il codice si dice lineare se $m3 = m1 + m2$ da origine a $c3 = c1 + c2$

Codificatori sistematici

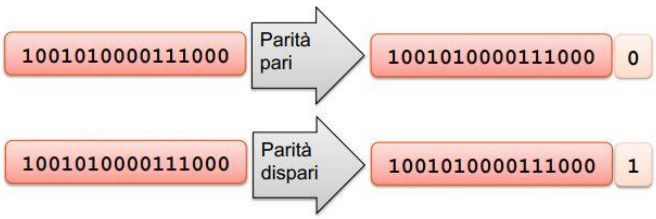
- Nella sequenza di n bit da trasmettere i k bit di informazione, mantenuti distinti dagli r bit di ridondanza, vengono trasmessi inalterati

Rbit = in ricezione → NO ERRORE

Bit di parità →Dati k bit di informazione $b_0 , b_1 , \dots , b_{k-1}$

$$b_k = b_0 \oplus b_1 \oplus \dots \oplus b_{k-1}$$ → parità pari

b_k = NOT $[b_0 \oplus b_1 \oplus \dots \oplus b_{k-1}]$ → parità dispari



- Dove $\oplus$ è l'operazione di OR esclusivo
- r = 1 un solo bit di ridondanza per qualunque dimensione del blocco dati k
- Rileva sempre un numero diverso di errori, fallisce con i numeri pari

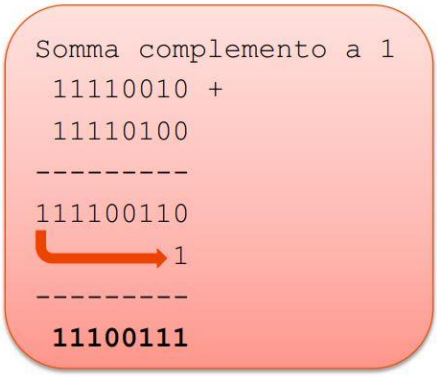
Internet Checksum

- Nei protocolli Internet sono stati usati codici a blocchi sistematici
- Estensioni bit di parità > prestazione
- Si applica su parole di 16 bit, indipendenti dalla lunghezza complessiva del blocco dati

Somma a complemento a 1

La somma complemento a 1 è simile al calcolo binario intero senza segno (somma complemento a 2) ma differisce per l'uso dei riporti

→ Se una somma genera un riporto questo viene aggiunto al risultato



- Blocco dati fatto di byte A, B, C, D, E, F, G, …
- Parole di 16 bit $[A,B],[C,D],[E,F],[G,H]$
  - Proprietà commutativa e associativa
    - $[A,B]+[C,D] = [C,D]+[A,B]$
    - $([A,B]+[C,D])+[E,F] = [A,B]+([C,D]+[E,F])$
  - Indipendenza dall'ordine dei byte
    - $[A,B]+[C,D] = [X,Y]\ allora\ [B,A]+[D,C] = [Y,X]$

→ Questa proprietà è molto importante perché rende il calcolo indipendente dalla rappresentazione del numero a livello di sistema hardware "big-endian" o "little-endian"

Algebra Binaria e codici polinomiali → si utilizzano cifre 0 e 1

Operazioni → Or esclusivo ⊕ (somma e sottrazione) e Moltiplicazione

Utilizzata per la rilevazione dell'errore

Errori a Burst → nelle reti di telecomunicazione gli errori sono distribuiti in modo non uniforme (frequentemente)

- filotto di bit lungo k, cui bit intermedi sono inaffidabili (supponiamo abbiano una probabilità di essere errati al 50%)
- si possono avere i seguenti casi:
  - k-1 < r: l'errore viene sempre rilevato
  - k-1 = r: si ha resto nullo se E(x)=Gr(x)
  - k-1 > r: il resto ha valore casuale e l'errore non viene rilevato se è nullo (r bit a 0)

Protocollo ARQ (Authomatic Repeat Request)

→ Usato da strato datalink e transport insieme con una codifica a rilevazione di errore

- Obiettivo: rendere canale comunicativo affidabile
  - Identifica errori trasmissivi
  - Riconosce perdita di informazioni
  - Riconosce perdite di sequenza
- Il canale tipicamente è:
  - Singolo collegamento seriale su data link →flusso seriale di bit
  - Connessione end-to-end nel livello di trasporto →cascate di nodi e collegamenti con diverse prestazioni e caratteristiche
- La diversità del canale rendono le problematiche dei protocolli di trasporto più complesse, ma esistono molti elementi comuni
- Il flusso formativo viene diviso in PDU:
  - Ogni PDU porta PCI che contengono informazioni relative a protocolli ARQ
  - Per il corretto funzionamento sono necessarie delle PDU speciali destinate esclusivamente alla segnalazione interna al protocollo
- Frame livello datalink (HDLC, PPP, …)
- Segmenti Livello trasporto (TCP)

Controllo degli errori

- Alle PDU viene applicata una codifica di canale
- Ricevitore
  - Verifica la correzione delle PDU ricevute grazie al codice di canale
  - Ignorare PDU errate
  - Può far partire procedure di ritrasmissione

- Trasmettitore
    - Ritrasmette le trame non correttamente ricevute
        - Su indicazione ricevitore
        - Alla scadenza time-out

Numerazione → i protocolli ARQ numerano sequenzialmente le unità informative (UI) da consegnare ai protocolli superiori

Numerano:

- PDU
- Unità informative standard

Trasmettitore e ricevitore mantengono due contatori:

- S: conta in modo sequenziale le unità informative inviate
- R: conta le unità informative ricevute in modo corretto

Conferma (ACKNOWLKEDGE) → incremento r solo se è corretto

- Esplicita ACK → ogni PDU corretta genera conferma
- Implicita (cumulativa) → ogni PDU di conferma con r=n conferma ricezione fino a n-1
- In PiggyBacking → viaggia inserita in una PDU contenente dati utili ("a cavalluccio")

Gli ACK sono PDU specializzate che non portano dati di utente ma solamente informazioni di controllo per il protocollo. Servono qualora il protocollo ARQ non possa usare il Piggybacking e il ricevitore non abbia dati da trasmettere. → non è necessario numerare gli ACK.

I protocolli ARQ tipicamente confermano la ricezione delle PDU che portano dati d'utente, non confermano la ricezione degli ACK → non è necessario controllare la sequenza degli ACK.

Finestra Scorrevole

Funzioni di controllo (errore, flusso, sequenza)

Possono essere implementate con l'uso sinergico di:

- Codici di linea
- Numerazione unità informative
- Conferma di ricezione

W_t= numero massimo trame che il trasmettitore può inviare senza ricevere conferma.

La numerazione delle trame viene effettuata modulo M (M=2^n n bit usati numerazione). Si può procedere alla trasmissione di nuove trame solo al ricevimento della conferma, per garantire unicità numerazione.

Dimensione della finestra

→ Per garantire unicità di numerazione delle trame, bisogna Imporre W finito e sospendere la trasmissione delle trame → Perché ha dimensioni limitate → Se si continuasse a trasmettere all'infinito non si avrebbe più una corrispondenza biunivoca trame-numero. → le trame con uguale numerazione sono indistinguibili.

Numero di trame = Grandezza finestra →Se per l'ordinamento vengono utilizzati numeri a sequenza a m bit, allora la grandezza massima della finestra sarà 2^m.

Efficacia Numerazione a finestra

Permette:

- La gestione automatica del controllo di flusso
- Di riconoscere l'errata ricezione/perdita di dati

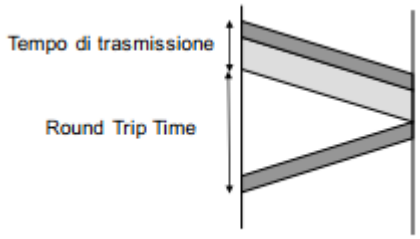
- Ricostruire in ricezione la corretta sequenza dei dati

Controllo del flusso

Accorda la velocità del trasmettitore a capacità ricevitore (e della rete). Il **ricevitore** deve essere in grado di gestire un'intera finestra e accorda il flusso di trame in arrivo tramite le conferme.

Go-back-n ARQ → il trasmettitore ritrasmette a partire da perdita. Quindi ritrasmetto tutto il blocco. Vantaggi: semplicità operativa, ridotta complessità nel ricevitore. Svantaggio: inefficienza → si ritrasmette anche quando non è necessario.

Selective Repeat ARQ →il trasmettitore ritrasmette solo le trame perse→ memoria trame fuori ordine. Vantaggi: maggiore efficienza. Svantaggi: complessità del ricevitore → deve tenere in memoria le trame correttamente ricevute.



Round Trip Time → tempo andata e ritorno (RTT)

→ variabilità: è praticamente deterministico per lo strato 2 e può variare da segmento a segmento per lo strato 4

Time out → il protocollo può entrare in stallo (deadlock) ed è necessario un time out per riprendere il dialogo.

Va relazionato al RTT. Se è troppo **breve**, non si attende l'arrivo dell'ACK e non è necessario di trame duplicate. Se è troppo **lungo**, inutile attesa prima di ritrasmettere le trame errate → in entrambi i casi si spreca capacità di trasmissione e degrado delle prestazioni

4 – PRESTAZIONI ED EFFICIENZA DEI PROTOCOLLI DI STRATO 2

In un sistema ideale → capacità massima finita, riduzione della capacità = perdita efficienza

Capacità massima → teorica = velocità canale, parte della capacità viene usata dai protocolli per scopi propri, quindi **capacità efficiente** $\leq$ **capacità teorica**

Efficienza → rapporto: tempo invio solo dati utente / tempo per invio corretto PDU

Prestazioni dei protocolli ARQ

- Protocollo Stop-and-wait → equivale a un protocollo a finestra scorrevole con finestra unitaria. Il canale di andata e quello di ritorno possono essere diversi
- Tempo trasmissione dati utente

$$Td = \frac{D}{C}$$

- Efficienza

$$\eta = \frac{D}{D+O}$$

- Overhead

$$O = 2H + 2IC$$

- Numero medio errori consecutivi

$$E[K] = \frac{Pf}{1-Pf}$$

- Efficienza massima

$$\eta max = \frac{D}{(D+O) + (D+O)\frac{FPe}{1-FPe}}$$

- Efficienza ottima

$$\eta = \frac{D_{ott}}{D_{ott} + 20}, \qquad D_{ott} = \sqrt{\frac{O}{Pe}}$$

Esercizio 1

- Protocollo Stop and Wait
  - Velocità della linea: **C = 4 Kbit/s**
  - Ritardo di elaborazione e propagazione: **I = 20 ms**
  - **H ≃ A ≃ 0**
- **Determinare la dimensione della trama tale che l'efficienza $\eta > 50\%$**
- **Formula dell'efficienza:**

$$\eta = \frac{D}{T_0 C};$$

$$T_0 = \frac{F}{C} + I + \frac{A}{C} + I;$$

- Sviluppando i termini:

$$\eta = \frac{D}{F + 2IC + A} = \frac{D}{D + H + 2IC + A};$$

- Nell'ipotesi che A ≃ H:

$$\eta = \frac{D}{D + \underbrace{2H + 2IC}_{O}};$$

- Con O si indica l'overhead, cioè la quantità di dati aggiuntivi introdotti dal protocollo

- Sostituendo i dati di progetto forniti dal testo:

$$\eta = \frac{D}{D + 2H + 2IC} \cong \frac{D}{D + 2IC} \geq 0.5$$
$$\Rightarrow D \geq 0.5D + IC \Rightarrow 0.5D \geq IC$$
$$\Rightarrow D \geq 2IC = 2 \cdot 4 \cdot 10^3 \cdot 20 \cdot 10^{-3} = 8 \cdot 20 = 160$$

- Affinché sia soddisfatto il vincolo richiesto sull'efficienza ($\eta > 50\%$), la trama deve essere lunga almeno 160 Bit

5 – INTERNET E IP

Internet → rete inaffondabile

ARPANet → 1969: Il dipartimento della difesa USA (DoD) attraverso l'Agenzia per i Progetti di Ricerca Avanzati (ARPA), finanzia la sperimentazione di una rete di calcolatori (ARPANET) fra:

- UCLA (University of California at Los Angeles)
- Stanford Research Center
- UCSB (University of California at Santa Barbara)
- Università dello Utah

Enti di Gestione di Internet

→ non esistono veri e propri enti che svolgono la funzione di gestione, ma sono enti di coordinamento delle attività di ricerca e di sviluppo che ora convergono nella internet Society

IAB (Internet Advisory Board) composto da:

- **IETF** (Internet Engineering task Force): con lo scopo di coordinare le attività di ingegnerizzazione ed Implementazione
- **IRTF** (Internet research task Force): con lo scopo di coordinare le attività di ricerca

RFC (Request For Comment)

I protocolli sono frutto del lavoro di gruppi di ricerca e sono definiti in documenti chiamati *Request For Comment*

→ sono rigorosamente approvati. Essi sono distribuiti liberamente a chiunque li richieda.

Altri Enti:

- **InterNIC**: *ente con lo scopo di fornire servizi specifici per l'internet* (es. registrazione nuove reti e domini, servizi infornativi riguardo la rete, ecc.)
- **IANA**: *Internet Assigned Number Authority* → mantiene DB significati convenzionati nei protocolli internet

Indirizzamento → Si utilizzano degli indirizzi, standardizzati e numerici per coinvolgere le entità in una comunicazione

In internet tipicamente dobbiamo distinguere da:

- Locator (URL): indirizzo necessario per localizzare tale risorsa
- Identifer (URI): identificativo di una certa risorsa di rete

Alcuni esempi:

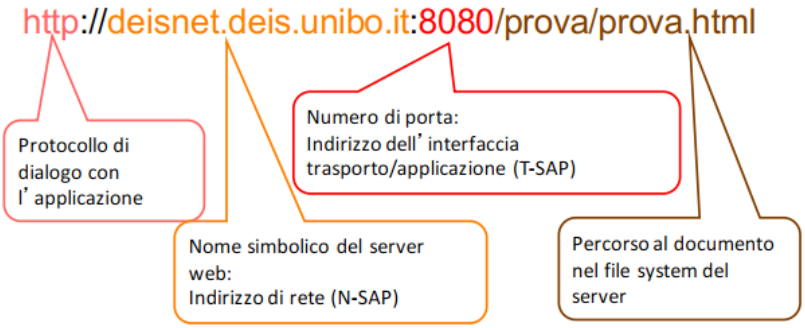
- Mobilità: *un terminale si sposta da una rete all'altra (*Locator → cambia nel tempo)
- Multi-homing: *un terminale è connesso a più interfacce a infrastrutture diverse* (molti locator attivi contemporaneamente)

Indirizzo:

- Globale
  - È valido in tutta la rete
  - Deve essere univoco
  - Va assegnato con una procedura di gestione *globale* per evitare la replicazione
- Locale
  - Può non essere univoco
  - È valido per una certa sotto porzione di rete, quindi è limitato
  - Assegnato con una procedura puramente *locale*

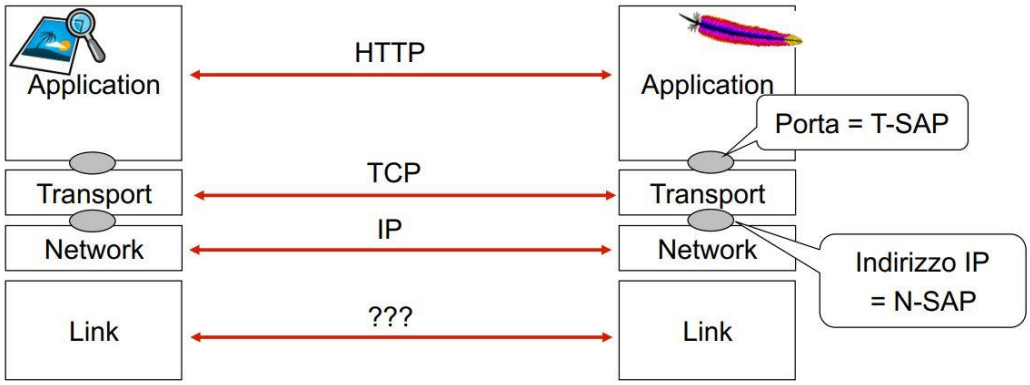
Indirizzamento nel web

URL → la risorsa è univocamente identificata da un indirizzo che la localizza



Protocolli ed Interfacce

- Le applicazioni sono locali al calcolatore (terminale)
- Il calcolatore viene indentificato univocamente su internet



Analisi di Protocollo → esistono strumenti software per analizzare il traffico di rete (Es: Wireshark)

Protocollo di trasporto → TCP (Transmission data protocol), UDP (User data protocol), RTP (real-time protocol)

- Protocollo di trasporto si occupa del trasporto di dati end-to-end
  - Trasporta i dati pertinenti a una qualsiasi applicazione
- *Numero di porta* →distingue i vari flussi di dati delle diverse applicazioni
  - Indirizzo si 16 bit → valori decimali da 0 a 65535
  - Locale al singolo calcolatore, ripetute su tutti i calcolatori
  - Condiviso fra tutti i protocolli di trasporto
  - Classificazione
    - Da 1 a 1023: riservati (per i server)
    - Da 1024 a 49151: registrati (per i servizi o per i client)
    - Da 49152 a 65535: ad uso dei client

Protocollo di rete → IP

- Garantisce il corretto indirizzamento ed instradamento dei dati
- Deve essere unico in una rete globale

Indirizzo IP

- Indirizzo lunghezza fissa **32 bit** →scritti convenzionalmente come sequenza di 4 numeri decimali, con valori da 0 a 255 separati da un punto
    - 2^{32} Numero teorico massimo →ma in realtà si riesce a sfruttare un numero molto inferiore
- Interfacce di Rete: indirizzo identifica i punti di interfacce di un host con la rete
- Multi-Home Hosts: host con due o più interfacce di rete

Infrastruttura Fisica di accesso alla rete

- Tipicamente un calcolatore si connette alla rete tramite una rete LAN (*local Area Network)*
    - Strato 1 e 2 di ISO OSI canale trasmissione/ricezione condiviso tra calcolatori
    - Le tecnologie LAN oggi più comuni sono state sviluppate adottando un canale di trasmissione/ricezione condiviso fra tutti i calcolatori della LAN.

Canale Condiviso

- Implicazioni → broadcast: uno parla e tutti sentono
- Problemi →controllo dell'accesso al canale e limitazione della quantità di dati da elaborare per lo strato 3
- Necessita un indirizzo LAN → interfaccia di strato 2 (che parla e riceve con la LAN) legge e passa allo strato 3 sono quello che gli serve

Gli indirizzi LAN→ MAC Address

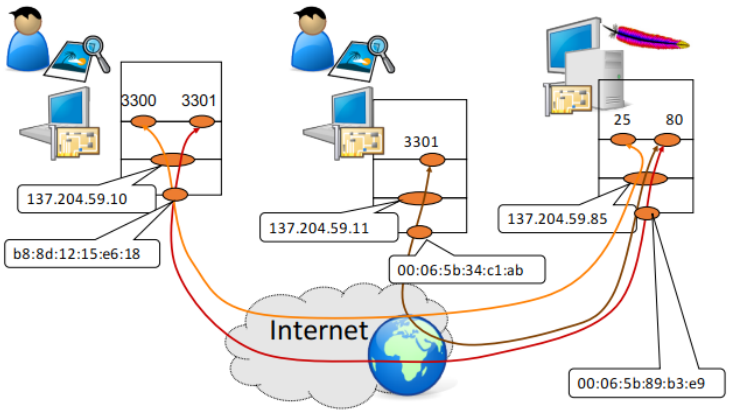
- MAC ADDRESS 48 bit, sono cablati nella schede di rete e sono univoci a livello mondiale → primi 3 byte individuano il costruttore
- È possibile specificare:
    - Un singolo destinatario → unicast→ 00-60-b0-78-e8-fd
    - Un indirizzo di gruppo → multicast → primo bit a 1
    - Invio a tutte le stazioni → broadcast → ff-ff-ff-ff-ff-ff

Connessione

Per identificare un singolo flusso è necessario conoscere:

- IP sorgente e destinatario
- Porta sorgente e destinatario

ESEMPIO



Dato questo flusso di comunicazione, le connessioni sono:

- 137.204.59.10:3300 ⟺ 137.204.57.85:25
- 137.204.59.10:3301 ⟺ 137.204.57.85:80
- 137.204.59.11:3301 ⟺ 137.204.57.85:80

Implementazioni dei servizi internet

→ Comunicazioni fra calcolatori (Host) = scambio di messaggi fra processi applicativi (Applicazioni)

- Client-Server: *gli host sono classificabili in client (ospitano applicazioni che si connettono al server per le informazioni) e server (mettono a disposizione risorse e dati)*
  → il Server si predispone a ricevere una connessione eseguendo una **apertura passiva**
  → il Client esegue una **apertura attiva** tentando di collegarsi al processo server di destinazione
    - Variante P2P: *gli host sono sia client che server verso gli altri host della rete. Qualsiasi nodo mette a disposizione e richiede informazioni in rete*

Ricerca della destinazione

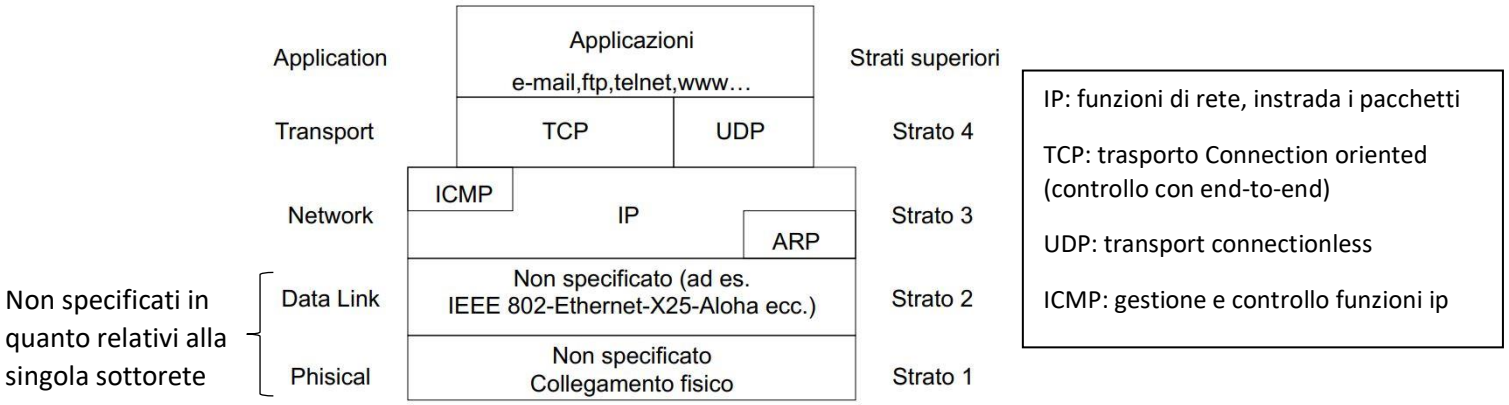
→ il client deve conoscere indirizzo IP e il numero di porta del server di destinazione → sono specificati nell'URL (protocollo applicativo, eventuale numero di porta non standard, numero IP o nome del server)

Conclusione

- Utente finale interagisce con software applicativo
- L'applicazione dialoga con una o più applicazioni remote utilizzando i protocolli
- I protocolli applicatici sfruttano il trasporto dei protocolli di traporto per raggiungere le applicazioni remote
- Protocollo di trasporto utilizzo le capacità di instradamento di IP per la consegna dei dati al calcolatore remoto dove risiede l'applicazione
- IP consegna i dati sfruttando l'infrastruttura di rete a cui gli host sono connessi tramite l'interfaccia LAN

I protocolli di Internet

Protocollo TCP/IP

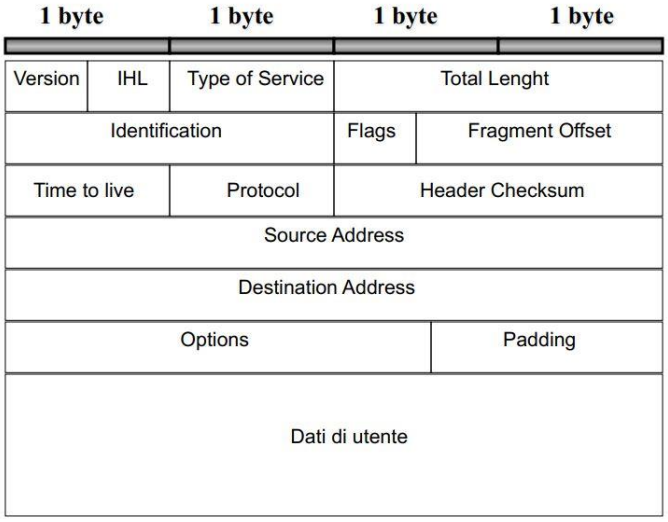


Protocollo IP (Internet Protocol) → livello di Rete

- Progettato per funzionare a **commutazione di pacchetto** in modalità connectionless
- Si prende carico di trasmettere i datagrammi da sorgente a destinazione, attraverso reti eterogenee
- Identifica host e router tramite indirizzi di lunghezza fissa, raggruppandoli in reti IP
- Frammenta e Riassembla datagrammi quando necessario
- Offre servizio best-effort cioè non sono previsti meccanismi per:
  - Aumentare affidabilità del collegamento end-to-end
  - Eseguire controllo flusso o sequenza

Struttura indirizzi IP → lunghezza fissa: 32 bit

- Scritti come sequenza di 4 decimali separati (con valori da 0 a 255) da punto
- Massimo numero teorico: 2^{32} Indirizzi, ma se ne riesce a sfruttare molti meno
- Assegnati da **IANA**



Formato pacchetto IP

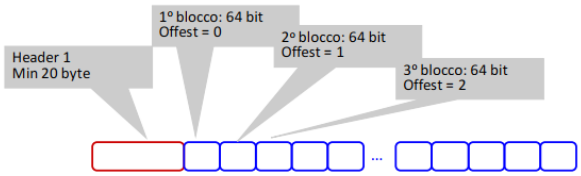
- **Version:** indica il formato dell'intestazione, attualmente la versione in uso è la 4
- **IHL:** lunghezza dell'intestazione, espressa in parole di 32 bit; lunghezza minima = 5
- **Type of service:** indicazione sul tipo di servizio richiesto, usato anche come sorta di priorità
- **Total length:** lunghezza totale del datagramma, misurata in bytes; lunghezza massima = 65535 byte, ma non è detto che tutte le implementazioni siano in grado di gestire questa dimensione
- **Identification:** valore intero che identifica univocamente il datagramma
    - Indica a quale datagramma appartenga un frammento (fragment)
- **Flag:**
    - Bit 0 → sempre a 0
    - Bit 1 → Don't fragment (DF)
        - DF = 0 si può frammentare
        - DF = 1 non si può frammentare
    - Bit 2 → More Fragments (MF)
        - MF = 0 ultimo frammento
        - MF = 1 frammento intermedio
- **Fragment offset:** indica quale è la posizione di questo frammento nel datagramma, come distanza in unità di 64 bit dall'inizio
- **TTL (time to live):** massimo numero di nodi attraversabili
    - Il nodo sorgente attribuisce un valore maggiore di 0 a TTL (normalmente = 64, massimo 255)
    - Ogni nodo che attraversa il datagramma pone TTL = TTL -1
    - Il primo nodo che vede TTL =0, distrugge il datagramma
- **Protocol:** indica il protocollo di livello superiore a cui appartengono i dati del datagramma
- **Header Checksum:** controllo di errore della sola intestazione, viene ricalcolato da ogni nodo
- **Source and destination address:** indirizzi di sorgente e e destinazione
- **Options:** contiene opzioni relative al trasferimento del datagramma, quindi è di lunghezza variabile
- **Padding:** bit privi di significato aggiunti per far in modo che l'intestazione sia con certezza multipla di 32 bit

<u>Fragment offset</u> → specifico

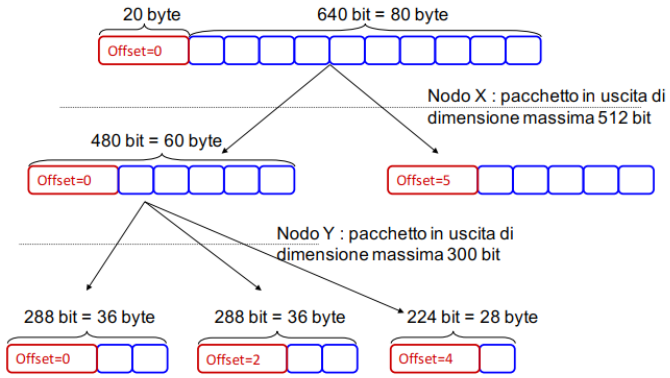
- Datagramma virtualmente diviso in sotto-blocchi da 8 byte (64 bit)
- Per la sorgente o nodo intermedio che trasmette l'IP → Numerazione sequenziale a partire dallo 0 per i sottoblocchi
- Il numero logico del primo blocco viene memorizzato nel fragment offset del datagramma

Implementazione

- Chi frammenta i datagrammi?
  - Qualunque apparato di rete dotato di protocollo IP può frammentare un datagramma
  - Tipicamente i nodi intermedi non riassemblano, ma lo fa solamente il terminale ricevente
- Frammentazioni multiple
  - Un datagramma può essere frammentato a più riprese in nodi successivi
- La numerazione tramite "offset" permette di rinumerare facilmente frammenti di un frammento



Calcolo dell'offset



L'instradamento IP

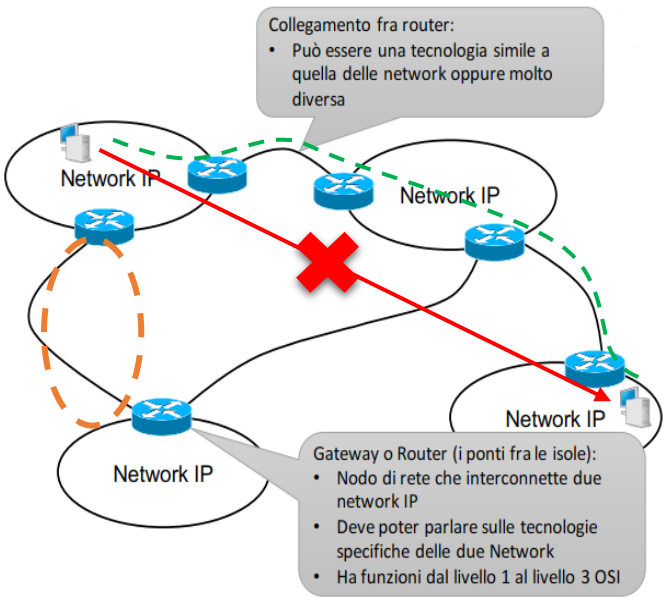
→ la rete internet è una rete a commutazione di pacchetto

→ In generale esistono più modi per raggiungere una destinazione da una certa sorgente. Come si decide il percorso da seguire?

Come funziona Internet → È una grande rete di reti, la componente elementare è la **network IP**. Ognuna di queste è come un'isola che contiene calcolatori che fungono da nodi terminali detti **HOST**. Le isole sono connesse tra di loro tramite **router** o **gateway** che svolgono la funzione di ponte. Ogni Network IP può essere realizzata con una tecnologia specifica (es: WIFI, ADSL, Ethernet, LTE, …) grazie alla quale tutti gli host posso comunicare tra di loro. I calcolatori di una network IP sono connessi dalla stessa infrastruttura di rete fisica (livello 1 e 2).

- Rete **logica**: la network IP a cui un host appartiene logicamente
- Rete **fisica**: la rete (tipicamente LAN) a cui un host è effettivamente connesso
  - Tipicamente ha capacità di instradamento e può avere indirizzi locali (MAC)

L'architettura a strati nasconde gli indirizzi fisici e consente all'applicazione di lavorare solo con indirizzi IP.



Interconnessone delle Network IP

È necessario che:

- Vi siano collegamenti tra le isole stesse, spesso realizzati con tecnologie diverse
- Vi siano degli apparati che permettono di usare questi collegamenti
- Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere.

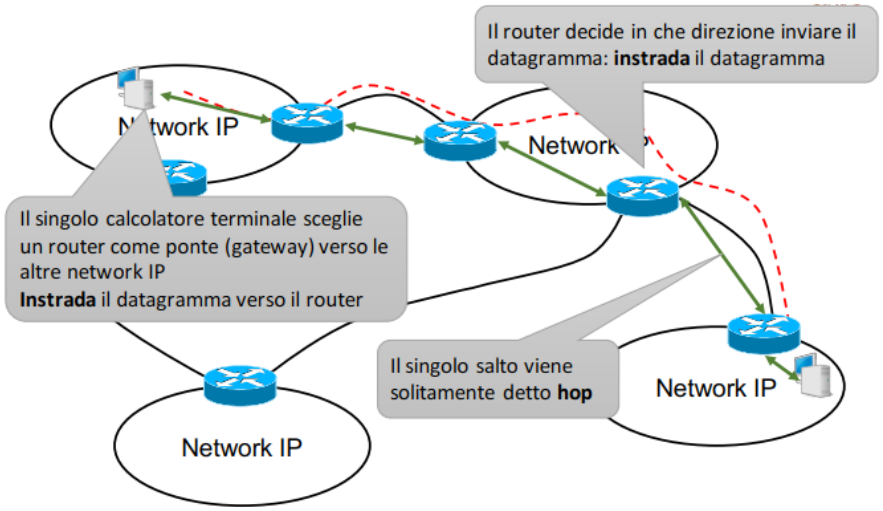
Percorso **rosso**: non si possono connettere due isole direttamente senza rispettare i router.

Percorso **verde**: Percorso End-to-End

Cerchio **arancione**: network IP fra i router (c'è tra ogni router)

Cosa fa IP?

L'obbiettivo dell'IP è quello di rendere possibile il dialogo fra network a prescindere dalla loro implementazione e localizzazione → concepito per lavorare indifferentemente su più tecnologie



Ho un pacchetto da trasmettere. Deve andare sulla mia network oppure devo usare un ponte?

Ogni nodo di internet ha un database di destinazioni possibili, quando deve inviare un datagramma parte dall'IP di destinazione, legge il database e decide l'azione da intraprendere. → la tecnologia della propria network può essere utilizzata per raggiungere la destinazione finale o per raggiungere il primo ponte.

Indirizzi e interfacce di rete →indirizzo identifica i punti di interconnessione di un host (quindi una delle sue interfacce di rete) →per ogni N indirizzi IP ci sono N interfacce di rete

Semantica indirizzo IP →logicamente suddiviso in due parti:

- Network (Net) ID
  - Prefisso che indica rete d'appartenenza → tutti gli indirizzi di una network IP hanno lo stesso Net ID
- Host ID
  - Identifica host (interfaccia) di una certa rete

→ vengono utilizzati bit contigui (Net ID occupa la parte a sinistra dell'indirizzo e Host ID la destra)

Reti IP private (RFC 1918)

Alcuni gruppi di IP sono riservati a reti IP private

- Non sono raggiungibili da rete pubblica
- I router di internet non instradano datagrammi destinati ad altri indirizzi
- Possono essere riutilizzati in reti isolate
  - Da 10.0.0.0 a 10.255.255.255
  - Da 172.16.0.0 a 172.312.255.255
  - Da 192.168.0.0 a 192.168.255.255

Come si distingue Net ID da Host ID?

Viene usato la netmask: al numero IP viene associata una maschera di 32 bit → I bit a 1 rappresentano i bit dell'IP che fanno parte del Net ID (la netmask si può scrivere con notazione dotted-decimal, esadecimale, abbreviata)

```
            137.204.191.25
10001001.11001100.10111111.00011001
11111111.11111111.11111111.11000000
Net-ID                              Host-ID
```

La Tabella di instradamento IP (Tabella di Routing)

- Base di Dati in formato tabella
  - Righe → dette route, entry, record
    - Insieme di informazioni relative alla singola informazione di instradamento
  - Colonne → dette campi
    - Informazioni del medesimo tipo relative a diverse opzioni di instradamento

Formato dipende dal Sistema Operativo e dall'implementazione → le informazioni sono sempre loro e può diverso il modo di rappresentarle ed elaborarle

Route

- D: Destinazione → numero IP valido
- N: Netmask → maschera di rete valida

Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	ppp0	1
137.204.64.0	255.255.255.0	137.204.64.254	en0	1
137.204.65.0	255.255.255.0	137.204.65.254	en1	1
137.204.66.0	255.255.255.0	137.204.66.254	en2	1
137.204.67.0	255.255.255.0	137.204.67.254	en3	1
192.168.10.0	255.255.255.252	192.168.10.2	ppp0	1

- G: Gateway → numero IP a cui consegnare datagramma
  - Indica tipo consegna da effettuare
- IF: Interfaccia di rete →interfaccia da utilizzare per la consegna del datagramma
- M: Metrica → specifica il "costo" di quel particolare Route

Uso della tabella di routing

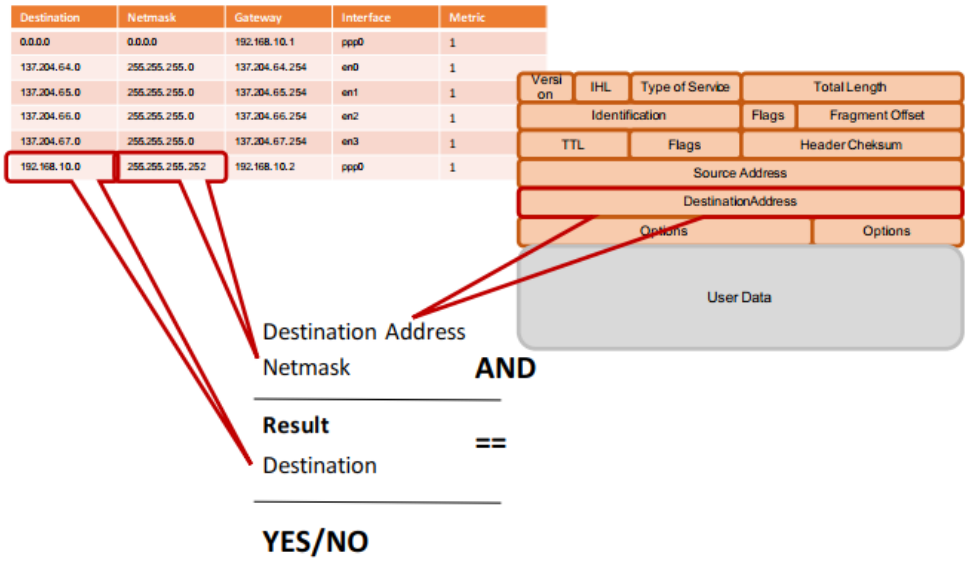
Nodo riceve datagramma:

1. Estrae IP-D
2. Seleziona il route per tale IP-D confrontandolo con i campi D presenti nella tabella (processo di **table lookup**)
3. Se il route esiste e segue instradamento usando campi G e IF
4. Se il route non esiste genera messaggio di errore → ICMP - *Destination Unreachable*

Table Lookup

La ricerca nella tabella avviene confrontando:

- IP-D del datagramma
- D di ciascun route
- N del route



procedura di "*Logest prefix match*"

- IP-D AND N=R
  - Indirizzo di destinazione del datagramma e netmask di ciascuna riga
- R = D ?

Yes → route selezionata e processo termina
No → si passa a route successivo

L'ordine per leggere i route: dalla riga che presenta una netmask cin un numero maggiore di bit a uno

Semplificazione tabelle → Non è necessario che un router conosca nello specifico le reti connesse al suo vicino, dato che sono collegati tra loro (ipotizzando che non ce ne siano altri) dato che router invia comunque i datagrammi tramite il suo vicino è sufficiente un'informazione "riassuntiva". I route verso le network possono essere aggregati in una sola, quindi il router le vede come una sola vedendo il suo vicino collegato alle network come un gateway.

Perché ordinare i route?

Così è possibile implementare eccezioni a regole generali che possono convivere nella medesima tabella. L'ordinamento in funzione delle netmask garantisce di considerare l'ordine: 1) singoli host, 2) reti piccole, 3) reti grandi. → dare priorità alle route più specifiche.

Il ruolo del Gateway → Responsabile consegna datagramma

1. Table lookup sceglie D i-esima = D_i
2. La funzione di instradamento invia il datagramma a IF_i, con l'obbiettivo di consegnarlo al gateway G_i
3. IF_i non è sufficiente perché normalmente l'instradamento Io è basato sulle network, gli host nella medisima network possono comunicare direttamente, mentre se sono di network differenti allora devono utilizzare un router.

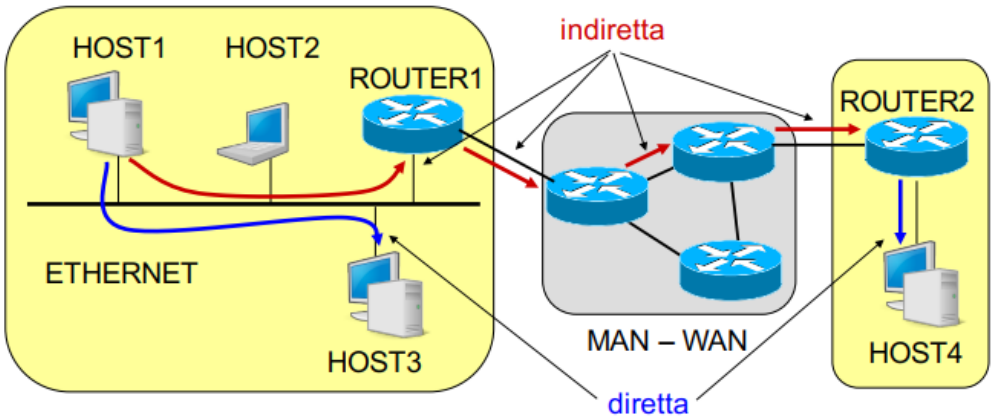
Routing → scelta percorso su cui inviare dati

- Direct Delivery: IP sorgente e destinatario su stessa rete fisica, **non ci sono intermediari**
- Indirect Delivery: IP sorgente e destinatario non sono sulla stessa rete fisica, **ci sono router intermedi**

Il campo Gateway nella Routing table specifica il tipo di instradamento

- Instradamento Diretto → Windows: IP LOCALE, Linux: 0.0.0.0
- Instradamento Indiretto → IP router intermedio

Da **Mittente** a **Destinatario** c'è sempre una consegna diretta → possono esserci 0-N consegne indirette



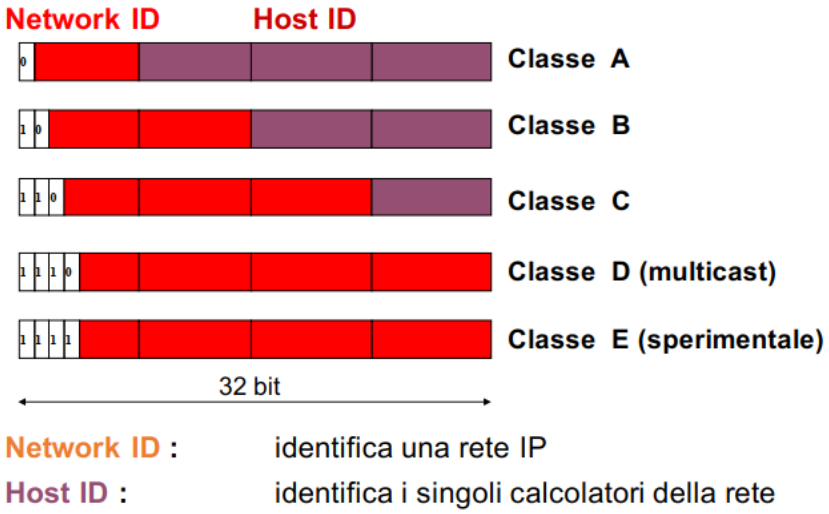
Classless VS Classfull: la logica degli indirizzi IP

IP e netmask

- IP pubblico unico in internet → il numero IP ha un valore assoluto nella rete
- IP sorgente e destinatario caratterizzano datagramma in quanto parte intestazione
- Network relativa al singolo nodo
    - Ai medesimi indirizzi possono corrispondere a netmask diverse in nodi diversi → route aggregations

Non è sempre stato così… Prima suddivisione net-ID e host-ID assoluta.

Classe delle reti



Definite diverse **classi** di network differenziate per **dimensione** → La parte inziale del net ID differenzia le classi:

- 0 classe A
- 10 classe B
- 110 classe C

→ definizione standard delle classi (nota a tutti)

→ i router riconoscono la classe di una rete dai primi bit dell'indirizzo (quindi ricavano il net-ID)

Intervalli di indirizzi

- Classe A: da 0.0.0.0 a 127.255.255.255
- Classe B: da 128.0.0.0 a 191.255.255.255
- Classe C: da 192.0.0.0 a 223.255.255.255
- Classe D: da 224.0.0.0 a 239.255.255.255
- Classe E: da 240.0.0.0 a 255.255.255.255

Indirizzi riservati (RFC 1700)

- 0.0.0.0 indica l'host corrente senza specificarne l'indirizzo
- Host-ID tutto a 0 viene usato per indicare la rete
- Host-ID tutto a 1 è l'indirizzo di broadcast per quella rete
- 0.x.y.z indica un certo Host-ID sulla rete corrente senza specificare il Net-ID
- 255.255.255.255 è l'indirizzo di broadcast su Internet
- 127.x.y.z è il loopback, che ridirige i datagrammi agli strati superiori dell'host corrente

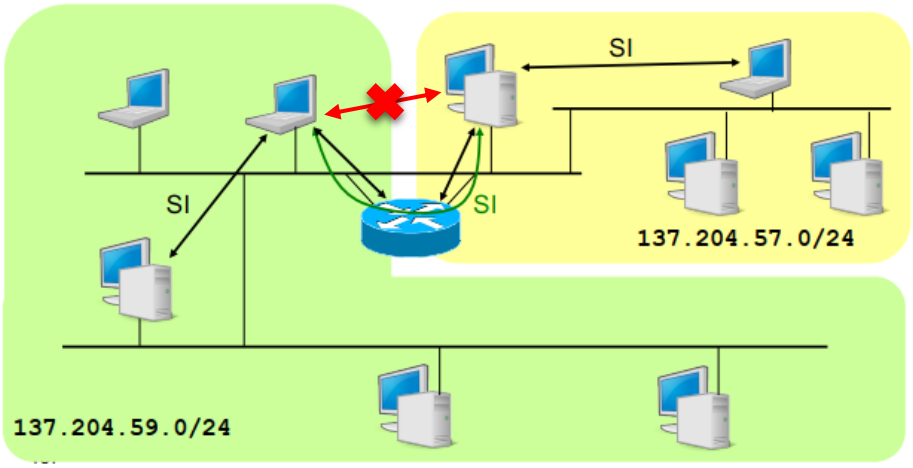
Le Sottoreti → frammentare la network in **sub-network** da assegnare alle **sotto-amministrazioni**

Si decide localmente una sotto-riparazione Net/Host ID indipendente delle classi. SI frammenta Host ID in due parti:

- La prima indentifico **subnet-ID**
- La seconda identifico l'host

La riparazione deve essere locale e reversibile, internet vede una certa network come entità unitaria.

Subnetting → suddivisione locale alla singola interfaccia



- Netmask con tutti i bit prefisso (NetID e subNet ID)

→ La configurazione delle netmask è fondamentale per il funzionamento corretto dell'instradamento.

- Riconoscere il proprio Net-ID
- Decidere fra instradamento **diretto** (nero) o **indiretto** (verde)

CIDR (Classless InterDomain Routing) → con la grande diffusione di internet la rigida suddivisione delle tre classi rende l'instradamento poco flessibile e scalabile

- Si rompe logica delle classi
- La dimensione di net-ID può essere qualunque
- Le tabelle di Routing devono comprendere le netmask
- Generalizzazione di subnetting/supernetting (reti IP definite da Net-ID/Netmask)

Obiettivi CIDR

- Allocazione reti IP di dimensione variabile →utilizzo più efficiente spazio indirizzi
- Accorpamento delle informazioni di Routing
- Miglioramento di 2 situazioni critiche:
  - Limitatezza classi A e B
  - Crescita esplosiva delle dimensioni delle tabelle di Routing

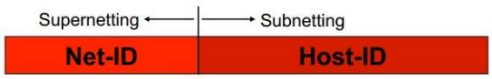
Supernetting → raggruppare reti con indirizzi consecutivi

Es. Un ente ha bisogno di circa 2000 indirizzi IP
- una rete di classe B è troppo grande (64K indirizzi)
- meglio 8 reti di classe C (8 × 256 = 2048 indirizzi) dalla 194.24.0.0 alla 194.24.7.0

Supernetting: si accorpano le 8 reti contigue in un' unica super-rete:
- Identificativo: 194.24.0.0/21
- Supernet mask: 255.255.248.0
- Indirizzi: 194.24.0.1 – 194.24.7.254
- Broadcast: 194.24.7.255

Subnetting e Supernetting sono operazioni duali:

- Subnetting → n bit del Host-ID diventano parte del Net-ID
- Supernetting → n bit del Net-ID diventano parte dell'host-ID



Accorpamento di N reti IP (N=2^n) → **contigue** o **allineate** secondo i multipli di 2^n

6 – PROTOCOLLI E TECNOLOGIE CORRELATE A IP

ARP (Address Resolution Protocol)

→ un software di basso livello nasconde gli indirizzi fisici e consente ai livelli superiori di lavorare solo con indirizzi IP.

→ gli host lavorano attraverso una rete fisica, quindi devono conoscere gli indirizzi fisici. Quindi come si ricavano se si hanno solo gli indirizzi IP?

1. Il nodo sorgente invia una trama contenente l'IP di destinazione (**ARP request**)
2. Tutte le stazioni della rete LAN leggono la trama broadcast
3. Il destinatario risponde al mittente inviando un messaggio contenente l'indirizzo fisico (**ARP reply**)
4. Ogni host mantiene una tabella con le corrispondenze fra indirizzi logici e fisici (**cache ARP**)

Comando ARP: **arp -a** → visualizza il contenuto della cache ARP con le corrispondenze

Configurazione dell'Interfaccia IP

Configurazione delle interfacce di rete

- Comando di **configurazione** → configura i parametri dell'interfaccia di rete
  - `Ipconfig` (windows)
  - `Ifconfig` (unix)
- Comando **route** → visualizza la tabella di routing dell'host
  - `Route print` (Windows)
  - `Route -n` (Unix)

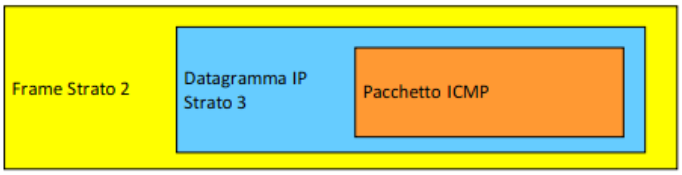
`route -p add DEST mask NETMASK GATEWAY` → aggiunge alla tabella di routing Window una entry permanente relativa alla destinazione DEST indicandone la NETMASK e il GATEWAY attraverso il quale raggiungerla

Tabella di Routing

Nell'host la tabella si ottiene da configurazione interfacce → numero IP e netmask identificano la network di appartenenza mentre il default gateway indentifica il router per la connessione fuori dalla propria network

Nei router → le tabelle devono contenere informazioni su più destinazioni dipendenti dalla tipologia id rete (possono essere create a mano in casi semplici (statiche) o vengono create in automatico dai protocolli di routing)

Protocollo ICMP



IP necessita di un protocollo di controllo per **gestione anomalie**, **notifica errori** o **irraggiungibilità destinazione**, **scambio informazioni di rete.** Dato che offrendo un servizio di best effort non garantisce la corretta consegna dei datagrammi (se necessario si affida a protocolli affidabili di livello superiore – TCP)

- offre servizi a IP
- Segnala solamente errori e malfunzionamenti ma non esegue correzioni→**Non rende affidabile IP**

I pacchetti ICMP sono incapsulati in datagrammi IP (ICMP è l'utente IP)

Formato pacchetto ICMP

IP header	20 - 60 byte
Message Type	1 byte
Message Code	1 byte
Checksum	2 byte
Additional Fields (optional)	variabile
Data	variabile

- Type: definisce il tipo di messaggio ICMP
  - Messaggi di errore
  - Messaggi di richiesta di informazioni
- Code: descrive il tipo di errore e ulteriori dettagli
- Checksum: controlla i bit errati nel messaggio ICMP
- Add. Fields: dipendono dal tipo di messaggio ICMP
- Data: intestazione e parte dei dati del datagramma che ha generato l'errore

Tipi di errore

- **Destination Unreachable** (Type = 3)
  - Codici errore
    - 0 = sottorete non raggiungibile
    - 1 = host non raggiungibile

    } Generato dal gateway
    - 2 = protocollo non disponibile
    - 3 = porta non disponibile
    - 4 = frammentazione necessaria ma bit don't fragment settato

    } Generato dall'host
- **Time Exceeded** (Type = 11)
  - Generato da un router quando supera TTL (time-to-Live)
  - Generato da un host quando un timer si azzera in attesa dei frammenti da riassemblare
- **Source Quench** (Type = 4)
  - I datagrammi arrivano troppo velocemente rispetto alla capacità di essere processati
- **Redirect** (Type = 5)
  - Generato da un router per indicare all'host sorgente un'altra strada più conveniente per arrivare a destinazione

Tipi di richiesta informazioni

- **Echo** (Type = 8)
- **Echo Reply** (Type = 0)
  - L'host sorgente invia la richiesta ad un altro host o ad un gateway
  - La destinazione deve rispondere immediatamente
  - Metodo usato per determinare lo stato di una rete e dei suoi host, la loro raggiungibilità e il tempo di transito nella rete
  - Additional Fields:
    - Identifier: identifica l'insieme degli echo appartenenti allo stesso test
    - Sequence Number: identifica ciascun echo nell'insieme
    - Optional Data: usato per inserire eventuali dati di verifica

- **Timestamp Request** (Type = 13)
- **Timestamp Reply** (Type = 14)
    - Receive Timestamp che indica l'istante in cui la risposta è stata ricevuta
    - Transmit Timestamp che indica l'istante in cui la risposta è stata inviata
    - Serve per valutare il tempo di transito nella rete, al netto del
      Tempo di processamento = $T_{transmit} - T_{receive}$

- **Address Mask Request** (Type = 17)
- **Address Mask Reply** (Type = 18)
    - Inviato dall'host sorgente all'indirizzo di broadcast (255.255.255.255) per ottenere la subnet mask da usare dopo aver ottenuto il proprio indirizzo IP tramite RARP o BOOTP
- **Router Solicitation** (Type = 10)
- **Router Advertisement** (Type = 9)
    - Localizzatore Router

Applicazioni di ICMP

- Comando **`ping DEST`**: permette di controllare se l'host destinatario è raggiungibile o meno dall'host sorgente
    1. Sorgente invia a destinatario un pacchetto ICMP di tipo **echo**
    2. Se destinatario è raggiungibile da sorgente, allora risponde inviando un pacchetto ICMP di tipo **echo reply**
- Comando **`traceroute DEST`:** permette di conoscere il percorso dei pacchetti inviati dall'host sorgente a quello destinatario
    1. Sorgente invia a destinatario degli ICMP di tipo **echo** con un **TTL** da 30 (default)
    2. Ogni nodo intermedio decrementa **TTL**
    3. Se il nodo rileva **TTL=0** invia a sorgente un pacchetto ICMP di tipo **TIME EXCEEDED**
    4. Sorgente costruire una lista dei nodi attraversati fino al destinatario
    5. L'output mostra il **TTL**, nome **DNS**, indirizzo **IP** dei nodi intermedi e il Round-Trip Time (**RTT**)

Protocolli e dispositivi per il controllo della numerazione IP

Dispositivi di rete: DHCP, Packet Filter, Proxy, Firewall e NAT

DHCP → (server su porta 67 UDP) permette ad un host di ottenere una configurazione IP **automatica** e **dinamica** di: indirizzi IP, netmask, broadcast, hostname, default gateway, server DNS

- Quando host attiva interfaccia di rete invia in modalità broadcast un messaggio **DHCPDISCOVER** in cerca di un server DHCP
- Ciascun server DHCP risponde con **DHCPOFFER** con cui propone un indirizzo IP
- L'host accetta una delle proposte e manda un messaggio **DHCPREQUEST** in cui richiede la config, specificando il server
- Il server risponde con **DHCPACK** specificando parametri di configurazione

Packet filter e firewall

Firewall → combinazione dei dispositivi di rete DHCP, Packet Filter e Proxy. Protegge le risorse interne dagli accessi esterni

- Pocket filter: dispositivo di rete che permette/blocca l'invio di pacchetti da/verso determinati indirizzi. Protegge la rete dal traffico "Vagante". Filtra i pacchetti seguendo politiche stabilite, i filtri generalmente configurati staticamente ì, la maggior parte delle configurazioni non permettono pacchetti per porte non standard (IANA)

- State full packet inspection: Mantiene il contesto dei pacchetti sia nel trasporto che nello strato applicativo adattando dinamicamente specifiche dei filtri
- Application layer Gateway (ALG) o Proxy: Controlla la comunicazione a livello applicativo. Monitora le connessioni: analizza il contenuto dei protocolli applicativi (a scapito di connessione sicuro end-to-end), adatta dinamicamente specifiche dei filtri
- Per ogni Layer dello stack possono essere applicate specifiche diverse

Protezione di host → firewall è un filtro SW/HW che serve a proteggersi da accessi indesiderati provenienti dall'esterno della rete.

- Può essere semplicemente programma installato su PC, tipicamente usata per accessi domestici a banda larga (ADSL, FTTH)
- Oppure può essere una macchina dedicata che filtra tutto il traffico della rete locale.
- Tutto il traffico tra la rete locale e internet deve essere filtrato perché solo il traffico autorizzato deve attraversare il firewall, ma si deve comunque permettere che i servizi di rete necessari siano mantenuti.
- Il firewall deve essere per quanto possibile immune da problemi sicurezza dell'host.

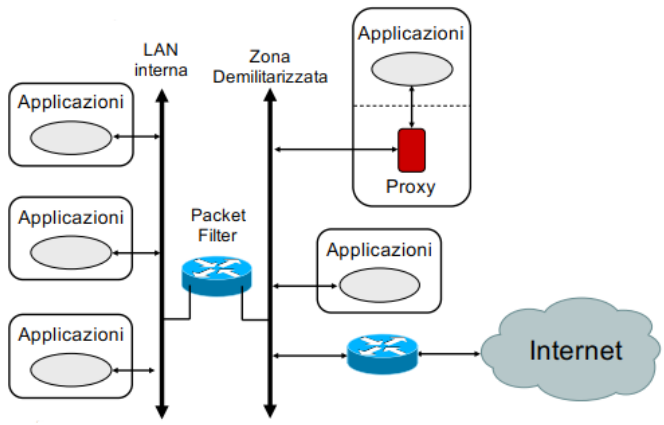
Configurazione della politica di default per i servizi di ete:

- Default **deny**: tutti i servizi non esplicitamente permessi sono negati
- Default **Permit**: tutti i servizi non esplicitamente negati sono permessi

Un firewall può essere implementato come:

→ Packet filter:

- Si interpone fra router locale e internet
- Sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
- Il filtro scorta i datagrammi sulla base di:
  - IP sorgente e destinatario
  - Tipo di server a cui il datagramma è destinato (porta TCP/UDP)
  - Interfaccia di prov e dest

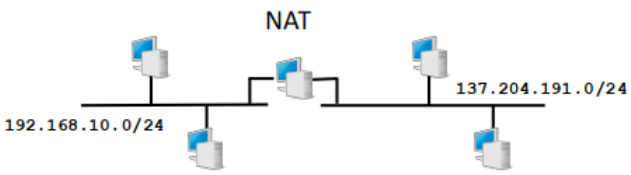


→ Proxy server:

- Nella rete protetta accesso consentito solo ad alcuni host
- Si interpone proxy server per realizzare la comunicazione a tutti gli host
- Il proxy server evita un flusso diretto di datagrammi tra internet e le macchine della rete locale

- Application level: viene impiegato un proxy server dedicato per ogni servizio che si vuole garantire
- Circuit level gateway: proxy server generico in grado di inoltrare le richieste relative a molti servizi

NAT (Network Address Translation)



→ Tecnica per il filtraggio di pacchetti IP con sostituzione degli indirizzi (mascheramento) → indirizzi e porte
Permette a Reti IP private l'accesso a reti IP pubbliche tramite un apposito gateway. Utile per risparmiare indirizzi IP pubblici e riutilizzare i privati.

- Efficiente uso di spazio degli indirizzi
- Condividere uno o pochi indirizzi

- Uso indirizzi privati nella LAN locale
- Security:
    - Rendere host interni non accessibili dall'esterno
    - Nascondere indirizzi e strutture rete
- Include un pocket filter, stateful pocket inspection configurate autonomamente

Basic NAT – conversione di indirizzo

- Il NAT può fornire una semplice conversione di indirizzo IP (statica o dinamica)
- Conversioni contemporanee limitate dal numero di indirizzi IP pubblici o dispositivi del gateway NAT

Conversione di indirizzo e porta

- Il NAT può fornire anche conversione di indirizzo IP e porta TCP o UDP
- Conversioni contemporanee possibili anche con un solo indirizzo IP

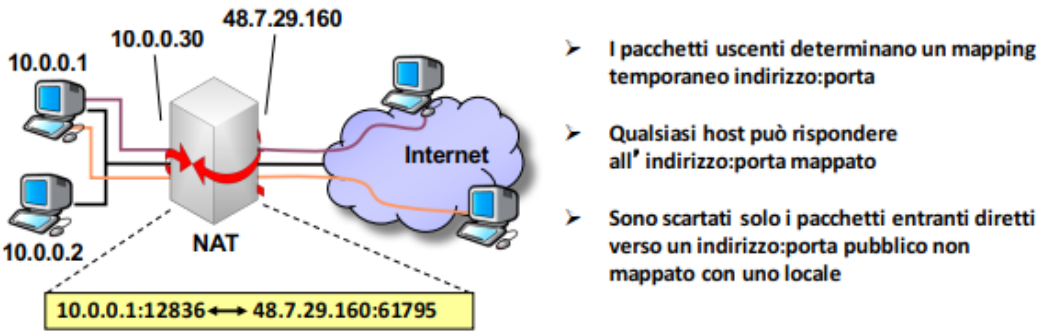
Direzione delle connessioni

- Tipicamente da rete privata verso pubblica, si occupa di effettuare la conversione inversa quando arrivano le risposte e registra le corrispondenze in corso in una tabella.
- In generale non è possibile contattare dalla rete pubblica un host sulla privata, solo configurazioni esplicite nel NAT

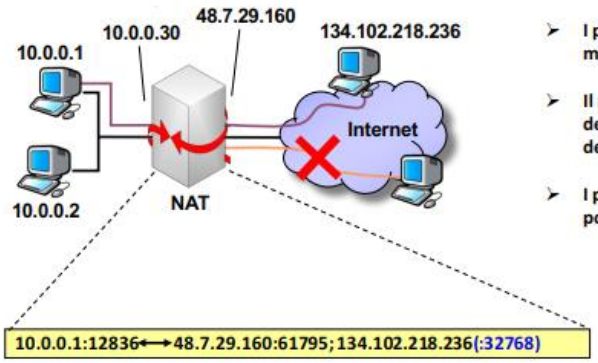
NAT e applicazioni di rete

- Il NAT è trasparente per l'applicazione, modifica intestazione IP e TCP/UDP, ma non il payload → questo è un problema in alcuni casi specifici
- Applicazioni non sono trasparenti al NAT
    - Contengono IP e numeri di parte nel payload
    - FTP uso 2 connessioni parallele, i parametri della seconda sono specificati nei dati trasmessi nella prima
- Il tipo di traffico permesso dipende dal tipo di NAT:

Full Cone NAT: Mapping indirizzo: porta locale ←→ indirizzo: porta pubblica. Accetta tutti i pacchetti provenienti dall'esterno diretti verso indirizzo : porta pubblica (solo se è mappato con indirizzo: porta privato)

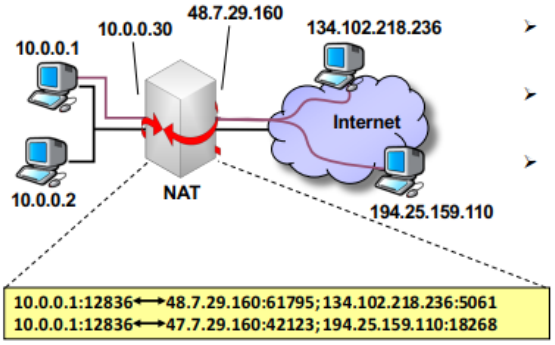


(port) **Restricted Cone NAT**: Cone Full come NAT ma la mappatura tiene conto della destinazione, vengono scartati tutti pacchetti provenienti da host non preventivamente contattati da un host locale



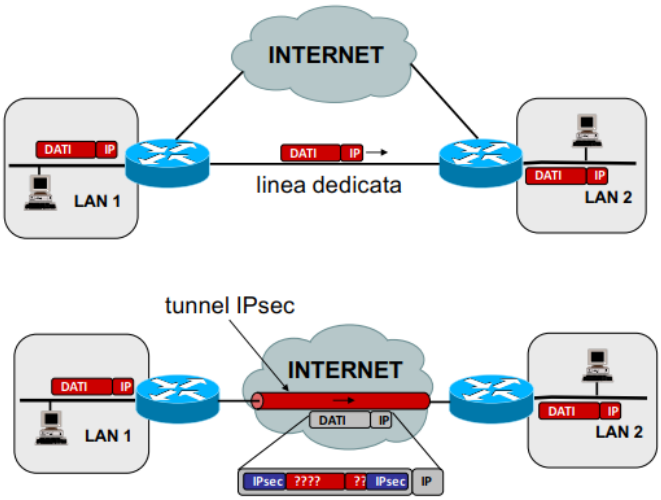
- I pacchetti uscenti determinano un mapping temporaneo indirizzo:porta
- Il mapping tiene conto anche dell'indirizzo (ed opzionalmente della porta) di destinazione
- I pacchetti provenienti da host (e/o porte) differenti vengono scartati

Symmetric NAT: NAT crea una differente mappatura indirizzo: porta locale e pubblico per ogni destinazione. Accetta connessioni da host esterni solo se l'host interno ha specificato precedentemente una connessione con essi



- Stesso comportamento del Port Restricted Cone NAT
- Diverso mapping per diverse destinazioni
- I pacchetti entranti sono scartati se non esiste una mappatura appropriata

VPN (Virtual Private Network)



Reti provate Virtuale

• La soluzione tradizionale per le aziende o enti di dimensioni medio grandi che hanno bisogno di interconnettere tra loro in maniera sicura sul territorio, è molto costosa (reti private affittate dagli operatori)
• Alternativa più economica: utilizzo di tunnel sicuri attraverso le reti pubbliche (VPN)
→ flusso punto-punto di pacchetti autenticati (informazioni criptate) incapsulati in pacchetti tradizionali

IPV6

Problematiche indirizzamento IP

- Mobilità
  - Indirizzi riferiti rete di appartenenza
    - Se host spostano in altra parte, IP deve cambiare (Configurazione automatica con DHCP e Mobile IP)
- Sicurezza
  - Scarsa Indirizzi più lungi: 16 protezione del diagramma IP (intestazione in chiaro) →IP sec
- Dimensioni reti prefisse
  - Subnetting e CIDR
- Data enorme diffusione di internet, il numero di indirizzi possibili è troppo basso
  - Reti IP private NAT

IPv6 → Non si sa quando verrà adottato in modo estensivo

Dati i vari problemi dell'IPV4 utilizzati ora, gli **obiettivi** della nuova versione sono**:**

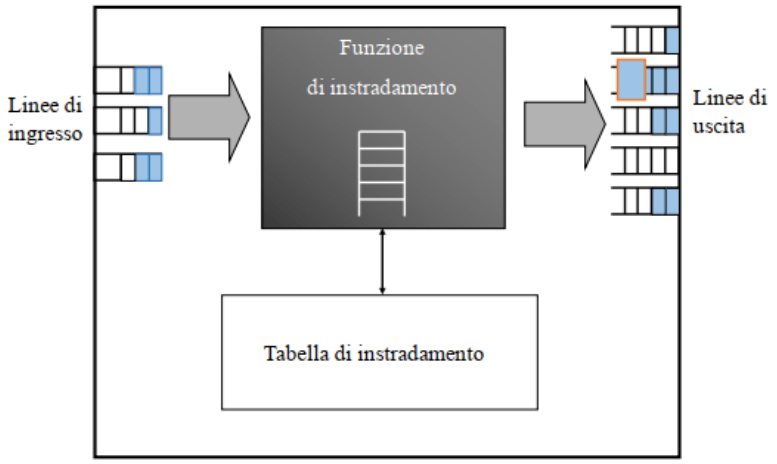
- Supportare molti miliardi di host
- Semplificare Routing
- Meccanismo sicurezza
- Qualità servizio (multimedialità)
- Gestire bene Multicast e broadcast
- Consentire mobilità
- Fare tutto ciò consentendo future evoluzioni e garantendo compatibilità col passato

Principali **caratteristiche**:

- Indirizzi più lunghi: 16 byte
- Semplificazione intestazione obbligatoria →meno campi di v4, no frammentazione, lunghezza minima comunque 10 righe
- Possibilità di diversi header opzionali
- Meccanismi di sicurezza e qualità servizio

7 – ROUTING

Instradamento delle reti IP



Funzioni di IP

- Indirizzamento
- Frammentazione
- instradamento
    - decidere che percorso deve seguire un datagramma
    - utilizza le PCI dei datagrammi
    - determina il comportamento della funzione di commutazione dei nodi

← nodo di commutazione a pacchetto nell'immagine

Store-and-forward → una vola memorizzato il pacchetto entrante si estraggono le informazioni di instradamento, vengono confrontate con la **routing table (**database per il confronto**)** e poi viene inserito nella cosa relativa all'uscita giusta.

Flooding → ogni nodo ritrasmette su tutte le porte di uscita ogni pacchetto ricevuto → quindi sicuramente prima o poi arriva anche a quello del destinatario arrivando a tutti i nodi.

→ Il primo pacchetto che arriva a un nodo è quello che ha fatto minore strada, perché vengono percorse tutte le strade possibili (molto adatto per broadcasting)

Miglioramenti per evitare **profilazione pacchetti** (in ogni singolo nodo il pacchetto viene copiato tante volte quante le interfacce, e quindi il numero cresce esponenzialmente)

- un nodo non ritrasmettere direzione dalla quale è giunto il pacchetto
- id pacchetto → ogni nodo lo memorizza, così lo trasmettere pacchetto una sola volta
- contatore TTL per ogni pacchetto, così si evita che giri all'infinito.

Deflection Routing (hot potato) → quando nodo riceve pacchetto lo ritrasmette sulla linea di uscita avente minore numero di pacchetto in attesa di essere trasmessi

Adatto reti:

- Con nodi di commutazione con poca memoria
- In cui si desidera minimizzare tempo permanenza dei pacchetti nei nodi

Problemi:

- Possibilità arrivo fuori sequenza
- Alcuni pacchetti percorrono all'infinito un certo nella rete, perché quelle vie sono poco utilizzate

→ Non tiene conto della destinazione finale del pacchetto

→ Si deve prevedere il TTL per limitare la vita dei pacchetti → evitare cicli

L'implementazione di **flooding** e **hot potato** è semplice, non sono necessari particolari scambi di info con nodi vicini, algoritmi e protocollo di routing pressoché inutili

Shortest path routing → algoritmo che cerca la strada di lunghezza minima fra ogni mittente e ogni destinatario (si utilizzano bellman- ford e Dijkstra)

Si assume che ogni collegamento della rete possa avere una lunghezza (numero che serve a caratterizzare il peso di quel collegamento nel determinare la funzione di costo del percorso totale di trasmissione)

L'implementazione può avvenire in modalità:

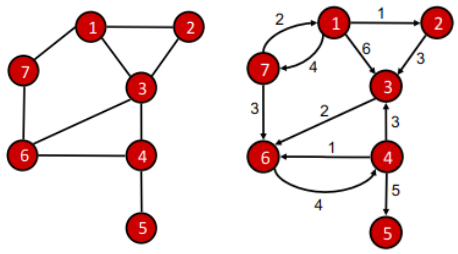
- Distribuita → ogni nodo esegue i calcoli per conto suo (sincrona e asincrona)
- Centralizzata → un solo nodo esegue i calcoli per tutti

Rappresentazione della rete

A una Rete di telecomunicazione si può associare un **grafo orientato**

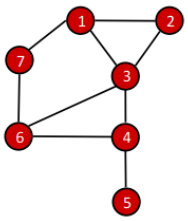
- **Nodi** = terminali e nodi di commutazione
- **Archi** = collegamenti
- **Direzione archi** = direzione di trasmissione
- **Peso archi** = costo collegamenti espresso in vari modi
    - Numero nodi attraversati
    - Distanza geografica
    - Ritardo introdotto da collegamento
    - Costo di un certo instradamento
    - Combinazione dei precedenti

Rete → Insieme di **nodi** di commutazione interconnessi da **collegamenti**

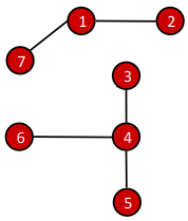


- **Grafo**
    - Orientato o non orientato → coppie ordinate $(i,j) \neq (j,i)$ o coppie non ordinate $(i,j) = (j,i)$
    - Pesato → quando ogni arco ha associato un numero reale detto peso (costo, distanza).

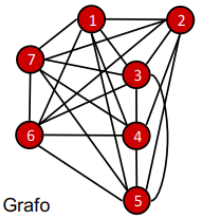
- **Cammino** → Sequenza di nodi
    - **Cammino semplice**: se non contiene solo nodi distinti (quindi che si ripetono una volta)



Grafo connesso e ciclico



Grafo non connesso e aciclico



Grafo completamente connesso

- **Ciclo** → Cammino di lunghezza > = 3 in cui il primo e l'ultimo nodo coincidono (un grafo è aciclico se non contiene cicli)
- **Connettività**
    - **Connesso**: se per ogni coppia di nodi esiste sempre un qualche cammino dal primo al secondo
    - **Completamente connesso**: se ogni nodo è connesso direttamente a tutti gli altri

- **Sotto-grafi** → solo una parte di un certo grafo
    - G sotto-grafo di G1, se l'insieme dei nodi di G è sotto-insieme dei nodi di G1 e uguale per tutti gli archi
- **Alberi** → è un grafo connesso e aciclico
- **Spanning tree** (albero di ricoprimento)→ Sotto-grafo connesso non orientato e aciclico (quindi albero) avente lo stesso insieme di nodi del grafo padre
- **MST**→ Minimum Spanning tree
    - Spanning tree di peso minimo, cioè tale che il peso totale dell'albero è il minimo possibile
        - Algoritmi di calcolo di tipo "**Greedy**"
            - Kruskal → ordina gli archi secondo peso crescente, parte da sotto-grafo vuoto ed a ogni passo aggiunge l'arco di peso minimo, senza creare cicli. Possibilità di grafo non connesso nei passi intermedi

- Prim → parte da un nodo radice e ad ogni passo l'arco connesso a quel nodo di peso minore, senza creare cicli. Albero sempre connesso, anche durante i passi intermedi

- **Shortest Path** → Cammino di peso minimo tra X e Y
  - **Peso del cammino**: somma dei pesi degli archi
  - **Principio di ottimalità**: Ogni sotto-nodo dello SP vedrà il pezzo del percorso successivo ad esso stesso come il suo minor percorso
  - **Routing shortest** path nel mondo IP → Quando I nodi di rete vengono accesi conoscono solamente la configurazione delle loro interfacce. Con queste informazioni popolano la tabella di instradamento iniziale.
    → Per implementare il routing shortest path verso una destinazione si devono utilizzare dei **protocolli** di routing per lo scambio di informazioni e **algoritmi** per il calcolo degli SP sulla base delle informazioni.

Algoritmo Bellman-Ford centralizzato

- Condizioni iniziali
$$D^0_i = \infty \ \ \forall\, i \neq 1$$
$$D^0_1 = 0$$
- Operazione 1
$$h = h+1$$
- Operazione 2
$$D^{h+1}_i = min_j[d_{ij} + D^h_j] \ \ \forall\, i$$
- Termino l'algoritmo se
$$D^{h+1}_i = D^h_i \ \ \forall\, i$$
- Il valore di D^h_i viene chiamato D_i, ed è la lunghezza del più breve percorso da i a 1

- Prendendo una sola destinazione → nodo 1
- Obiettivo: determinare il percorso di lunghezza minima di un nodo qualunque *i* al nodo 1.

Se non esistono cicli di lunghezza nulla o negativa, allora si può dimostrare che l'algoritmo ha un numero finito di alterazioni e la soluzione è unica.

Instradamento → per ottenere i percorsi, per ogni nodo i si sceglie l'argo e si applica l'equazione e si considera il sotto-grafo composto da questi N-1 archi. Partendo dal nodo i si seguono gli archi del sotto-grafo fino a raggiungere il nodo 1.

Routing Distance Vector → è un protocollo semplice che richiede poche risorse

→ utilizza l'algoritmo di Bellman-Ford nella versione **Distribuita** (i nodi eseguono sempre i calcoli degli SP) e **Asincrona** (l'esecuzione dei calcoli non è sincronizzata)

Implementa meccanismi di dialogo per far sì che:

- Ogni nodo sempre i suoi vicini e calcolo distanza da essi
- Ad ogni passo dell'algoritmo, ogni nodo invia ai vicini un vettore contenente la stima delle sue distanze dagli altri, così ogni nodo può eseguire RILASSAMENTO verso ogni altro nodo ad eventualmente aggiornare stime.

Problemi:

- Convergenza lenta, partenza lenta → cold start
- Problemi di stabilità → conteggio all'infinito

Cold Start e tempo di convergenza

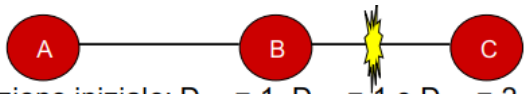
- All'inizio le tabelle dei singoli nodi contengono solo l'indicazione del nodo stesso a distanza 0 → da cui in poi il distance vector permette di creare tabelle sempre più complete. L'algoritmo converge al più dopo un numero di passi pari al numero di nodi nella rete. → più la rete è grande più il tempo è lungo, e se lo stato della rete cambia prima del tempo di convergenza dell'algoritmo **abbiamo un risultato imprevedibile e si ritarda la convergenza.**

Bouncing effect

Il link fra due nodi A e B cade:

- A e B si accorgono che il collegamento non funziona → pongono a infinito la sua lunghezza
- Se altri nodi mandano i loro distance vector si possono creare delle incongruenze temporanee → durata in base alla complessità della rete
    - Queste incongruenza possono dare luogo a dei cicli e quindi i nodi si scambiano datagrammi fino a **quando non terminare il TTL**

Count to infinity

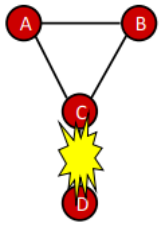


- Situazione iniziale: $D_{AB} = 1$, $D_{BC} = 1$ e $D_{AC} = 2$
    - Link BC va fuori servizio
    - B riceve il DV di A che contiene l'informazione $D_{AC} = 2$, per cui esso computa una nuova $D'_{BC} = D_{BA} + D_{AC} = 3$
    - B comunica ad A la sua nuova distanza da C
    - A calcola la nuova distanza $D_{AC} = D_{AB} + D'_{BC} = 4$
    - …

Questo conteggio può andare avanti fino all'infinito, si può risolvere imponendo che quando la distanza verso la destinazione supera un valore massimo **allora si suppone che il nodo di destinazione non sia raggiungibile.**

Meccanismi Migliorativi per il count to infinty

- **Split horizon:** tecnica semplice per risolvere in parte i problemi → questo algoritmo necessita che un router invii informazioni diverse ai diversi vicini → A omette la sua distanza da X nel distance vector che invia a B.
- **Triggered update:** Migliorare i tempi di invio del Distance Vector ai vicini → algoritmo che richiede di inviare periodicamente le informazioni delle distanze → un nodo deve inviare immediatamente le informazioni a tutti i vicini qualora si verifichi una modifica della propria tabella di instradamento



- Inizialmente, A e B raggiungono D tramite C
- Dopo il guasto, C mette a ∞ la sua dist. da D
- Dopo aver ricevuto il DV da C, A crede di poter raggiungere comunque D tramite B
- Idem per B che crede di poter usare A
- Stavolta A e B trasmettono i propri DV a C
- Si crea di nuovo un loop e un problema di convergenza

<u>Non sono davvero risolutivi</u>

la convergenza è comunque troppo lenta o addirittura nulla in certe situazioni → si formano lo stesso **cicli** nel percorso dei pacchetti

Algoritmo di Dijkstra

- Sorgente singola: nodo A.

- Dato il grafo G
    - Sia F un sottografo e F' il suo complemento
        - $F \cup F' = G$
    - Sia M il sottografo dei nodi *i* tali che
        - $j \in F'$
        - $\exists\ i \in F$ tale che $d_{ij} \neq 0$
- Al passo 0
    - $F_0 = \{a\}$
- Al passo h
    - $F_h = F_{h-1} \cup \{j \in M$ tale che $d_{ij} \leq d_{ik}\ \forall i \in F$ e $\forall k \in M\}$
    - $F'_h = F'_{h-1} - j$
- Termina quando
    - $F' = \varnothing$

- Obiettivo: determinare il percorso di lunghezza minima da A verso un nodo qualunque

Protocolli routing Link State: utilizzando un determinato algoritmo di routing, ogni nodo si procura un'immagine della topologia della rete (immagine del grafo della rete). Sulla base di essa calcola tabella di Routing utilizzando un opportuno algoritmo di routing.

1. Raccolta delle informazioni dei vicini
    a. Hello Packet: raccolta dei loro indirizzi
    b. Echo Packet: misurare la distanza tra di loro
2. In seguito: ogni router costruisce un pacchetto con lo stato delle linee (Link State Packet o LSP) contenente la lista dei vicini e le lunghezze dei collegamenti per raggiungerli.
3. Diffusione ed elaborazione delle informazioni tra i router della rete (i pacchetti LSP li avranno tutti)
   → vengono Trasmessi con Flooting a cui vengono aggiunte informazioni e poi si usa Dijkstra per calcolo cammini minori e quindi i router saranno in grando di costruire l'immagine della rete.

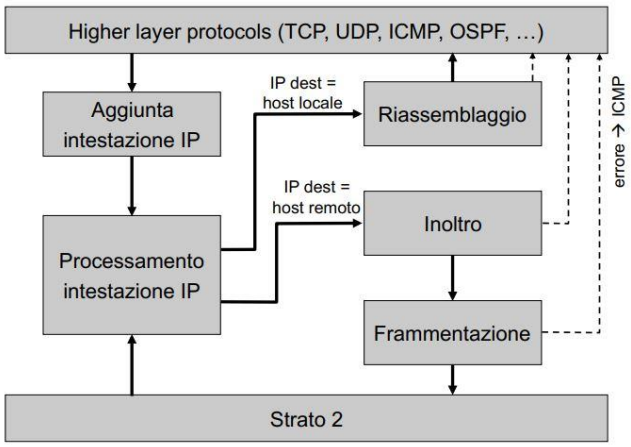
→ **Funzione**: gestione rete, convergenza, traffico

Il router IP

Router IP: nodo di commutazione a pacchetto nelle reti IP

Classificazione dei router

- SOHO: utilizzo domestico o piccoli uffici → interfaccia sulla LAN (switch poche porte FastEthernet e Wi-Fi)
- Router d'accesso: ISP, ha un alto numero di porte a velocità medio- bassa (max 10Mbps), diversi protocolli d'accesso
- Enterprise/campus router: interconnessione tra LAN di media dimensione, poche porte ad elevata velocità (Fast o GigaBit Ethernet)
- Backbone router: per reti di trasporto e connessioni inter-domain, poche porte ad elevata velocità (maggiore di 1Gbps), equipaggiato con sistemi di garanzia dell'affidabilità (monitoraggio remoto, …)



Le 4 funzioni del router

- Routing:
    - Scambio di info con altri router
    - Elaborazione locale (algoritmi di routing)
    - Popolazione tabelle di routing
- Forwarding = trasferimento
    - IP
        i. Table lookup
        ii. Header update
- Switching:
    - Trasferimento del datagramma da interfaccia di input a interfaccia di output
- Trasmissione
    - Trasferimento del datagramma sul mezzo fisico

Routing table (RIB): informazioni topologie di rete influenzate dalle informazioni ottenute dal dialogo con gli altri router

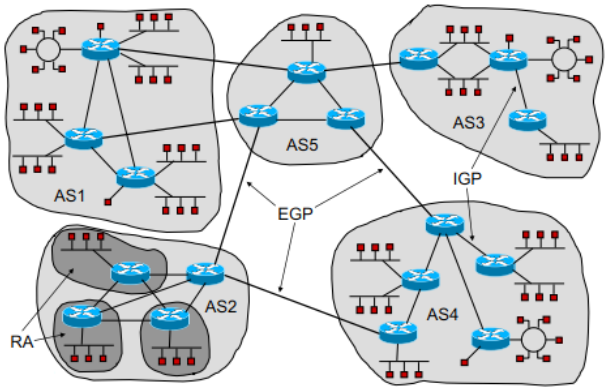
Forwarding table (FIB): ottenuta come ottimizzazione per il lookup della RIB. È più corta e veloce da leggere → tabella aggregata → si ottiene dalla Routing table

→ determinano strategia di indirizzamento usata dai nodi

8 – PROTOCOLLI DI ROUTING

Instradamento dell'internet Globale

In internet si usa il **Routing gerarchico** e le aree di Routing sono chiamate **AUTONOMOUS SYSTEM (AS)**



- Può essere ulteriormente suddiviso in porzioni dette Routing area (RA) interconnesse da un backbone (dorsale)
- Ogni network IP è interamente contenuta in un SA o RA (tradizionalmente secondo la classe, oggi secondo il CIDR)
- Gli AS decidono in autonomia protocolli e politiche Routing da adottare all'interno
- I vari enti di gestione si devono accordare per protocolli di dialogo tra router che interconnettono AS
- I protocolli di Routing all'interno di un AS sono Interior Gatway Protocol (IGP)
- I protocolli di Routing tra AS sono Exterior Gateway Protocol (EGP)

Cos'è un AS? → Originariamente insieme di router gestiti da un'unica amministrazione

Nuova definizione (1996):

- Gruppo connesso di una o più reti IP (classless) gestite da uno o più operatori ma con identiche e ben definite politiche di Routing
- Ovvero modalità con cui si prendono decisioni nel resto della rete sulla base delle informazioni prov. Da un AS (un EPG)

Protocolli di Routing

IGP → un AS deve implementare il routing al suo interno e lo fa usando uno o più protocolli di routing detti IGP

- RIP: Routing Information Protocol
- OSPF: Open Shortest Path First

EGP → un AS deve comunicare con gli altri AS per implementare il routing tra AS e lo fa usando un protocollo di routing pensato appositamente detto EGP

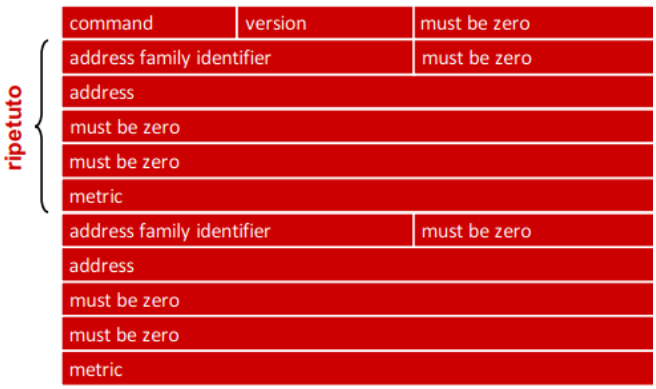
- EGP: Exterior Gateway Protocol
- BGP: border gatway protocol

Interior Gateway Protocols (IGP)

RIP (routing information protocol): protocollo distance vector → versione vecchia

- Diffuso in passato perché codice di implementazione diffuso è libero
- Usato solo su reti TCP/IP
- Messaggi (trasportatati UDP, porta 520):
  - REQUEST: richiedere informazioni ai nodi vicini
  - RESPONSE: invia i distance Vector (destinazione + distanza), quindi per inviare le informazioni di routing
    - Viene inviato periodicamente ogni 30 secondi con uno scarto per evitare troppi aggiornamenti, come risposta a una REQUEST e quando cambia una informazione di routing (triggered update)

Formato pacchetto: max 512 byte con parole di 32 bit, campi ridondanti



→ i bit sono molto ridondanti rispetto alla quantità di informazioni da inviare, i campi fissi sono tutti a 0.

- **Command**: distinguere fra REQUEST (1) e RESPONSE (2)
- **Version**: versione del RIP
- **address family id**: tipo di indirizzo di rete utilizzato
- **address**: destinazione per la distanza indicara
- **metric**: distanza per la destinazione indicata

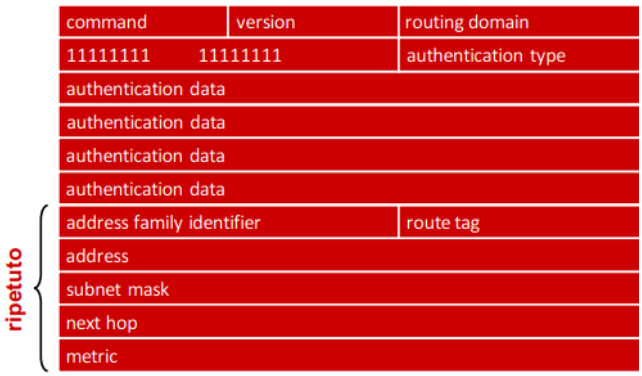
Tabella di Routing → Ogni riga: destinatario, distanza, next-hop router vicino, due contatori (Time-Out e Garbage-Collection Timer)

Aggiornamento della tabella di routing → ogni volta che si riceve un RESPONSE si controlla la correttezza dei dati, si considerano solo le distanze minori dell'infinito. Se esiste nella tabella una entry riguardo quella destinazione, si confronta il dato nuovo con quello vecchio, se è minore allora si aggiorna la distanza e si fa partire il timeout. Altrimenti si crea una nuova entry con la distanza segnalata e si fa partire il timeout.

problematiche

- Fa uso di split horizon (RESPONSE di interfaccia diverse possono essere diverse)
- Fa uso di triggered update (response con sole modifiche)
- Non supporta CIDR e non è un protocollo sicuro: Chiunque trasmetta datagrammi dalla porta UDP 520 viene considerato come un router autorizzato

Versione 2



- Miglioramenti → Subnetting (campo subnetmask) e CIDR e autenticazione
- Compatibilità verso il basso
- Possibilità di indicare proprio AS e scambiare messaggi con protocollo EGP (route tag e routering domain)
- Non adatto a AS grandi
- problemi di convergenza (perché rimane un distance vector)

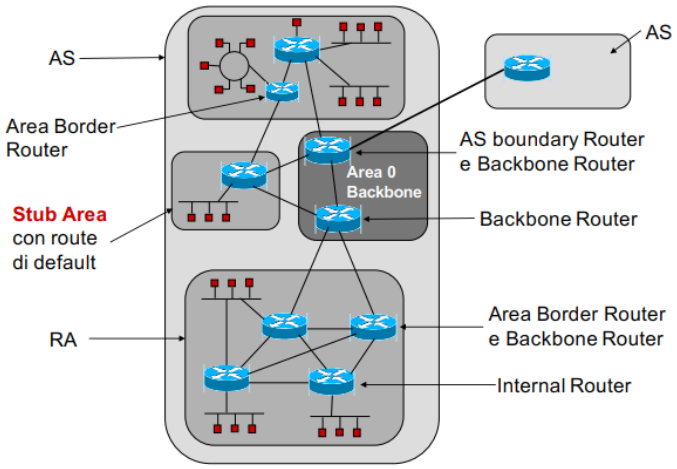
OSPF (open shortest path first)

Protocollo di tipo linkstate (invio di LAS a tutti gli altri router), più diffuso, incapsulato direttamente in IP

Progettato per:

- Semplificare Routing in reti grandi tramite suddivisione di aree
- Gestire reti punto-punto e punto-multipunto
- Superare logicamente gli host dai router

Aree di Routing → un AS può essere suddiviso in porzioni dette **Routing Area** (RA) interconnesse da un **backbone** (Area 0)



→ogni area risulta separata dalle altre per lo scambio di informazioni e per connetterle tra loro ci devono essere dei router connessi a più aree o al backbone

Classificazione dei router router secondo OSPF

- **Internal Router:** router interni a ciascun area
- **Area Border Router**: router da scambiare informazioni con altre aree
- **Backbone Router**: router che si interfacciano con backbone
- **AS Boundery Router**: Router che scambiano informazioni con altri AS usando un protocollo EGP

Tipi di route

- **Route intra-Area:** aggiornamento delle informazioni di Routing pertinenti all'area
- **Route Inter-Area**: aggiornamento delle informazioni di Routing pertinenti a diverse aree da quella considerata
- **Route Esterni**: aggiornamento informazioni di route provenienti da altri protocolli al di fuori del dominio OSPF

Tipi di Aree

- **Area Normale:** accetta tutti i tipi di route
- **Stub Area:** accetta rout intra e inter area
  - Tutti router della stub area usano un "default route" verso al di fuori dell'AS (Comunicato dall'area Border Router)
  - Requisiti di memoria dei router sono ridotti
- **Totally Stub area**: vengono propagati solamente intra-area ed il route di default
- **Not So Stubby area**: stub area che importa alcune route esterni, uno dei route è connesso a un AS diverso e diventa ASBR

Ulteriori caratteristiche di OSPF

- Bilanciamento del carico → se il carico viene ripartito sui router che hanno i percorsi verso una certa destinazione della stessa lunghezza
- Autenticazione → con password e crittografia
- Routing dipendente dal grado di servizio →i router scelgono il percorso per il pacchetto sulla base dell'indirizzo e sul valore di Type of Service dell'intestazione IP

tipologia di rete su cui opera

- Point-to-point
- Accesso multiplo → tutti gli N router connessi alla rete sono di fatto connessi a tutti gli altri
  - Broadcast multi-Access
  - Non-broadcast multi-Access

Vicinanza: due router che sono connessi alla medesima rete e possono comunque comunicare direttamente (punto-punto o punto-multipunto)

Adiacenza: due router che si scambiano informazioni di routing

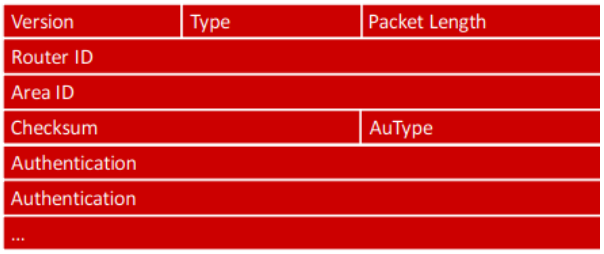
In una Rete ad accesso multiplo viene eletto un DR (designated router) fra gli N vicini, ogni router della LAN è adiacente solo al DR così lo scambio di informazioni di routing avviene solo tra router adiacenti perché il DR fa da tramite → backup adiacente a tutti i router locali (BDR)

Rete accesso multiplo conviene raggiungere nodo virtuale e adottare topologia a stella.

Router ID → Ogni router di AS utilizzante OSPF deve aver un ID univoco e priorità (utilizzate nell'elezione DR) di valori compreso in 8 bit. (default priorità 0)

OSPF: Link State db il grafo orientato dalla rete sul quale ciascun router calcola lo **shortest path tree** è rappresentato da Link State Database presente in ogni router

Protocolli → ivia messaggi usando protocollo IP (camp protocol = 89)



- **Version**: versione di OSPF
- **Type**: tipo di pacchettp (hello, db description, Link state request, link state update, link state acknowledge)
- **Packet length**: numero di byte del pacchetto
- **Router ID**: indirizzo IP che identifica il router mittente
- **Area ID**: area di appartenenza
- **Checksum**: calata su tutto il pacchetto escludendo il campo authentication
- **auType**: tipo di intestazione (nessuna, semplice o crittografata)

sotto-protocolli:

1. **Hello protocol**→ per controllare operatività dei link, scoprire/mantenere relazioni vicini e leggere DR e BDR
2. **Exchange protocol** → sincronizzazione asimmetrica link state db (master e a chi lo slave)
3. **Flooding protocol**→ link state update (inviato finché non arrivano link state ACK)
    - A fronte di un cambiamento nello strato di collegamento
    - A fronte di una link state request
    - Periodicamente →30 min

Stub Area → area con un solo punto di interconnessione con il resto della rete

Exterior Gateway Protocols (EGP)

Protocolli di tipo EGP → sono diversi da IGP, all'interno dell'AS si persegue l'ottimizzazione dei percorsi → bisogna tener conto delle **politiche di instradamento**

- EGP: Exterior Gateway Protocol → Obsoleto
- BGP: Border Gateway Protocol

Funzionalità principali

- Neighbor acquisition → Verificare se esiste un accordo per diventare vicini
- Neighbor reachability → Monitorare le connessioni con i vicini
- Network reachability → Scambiare informazioni sulle reti raggiungibili da ciascun vicino

Limiti di EGP

- Progettati per topologia specifica → dorsale
- Funzionare bene per topologie ad albero → ma non per reti a maglia complessa
- Non si adatta velocemente a modifiche topologia
- Nessun meccanismo di sicurezza →Chiunque può quello che vuole e un router guasto può danneggiare Routing di tutta la rete

BGP → creato per sostituire EGP (oggi versione 4)

I router BGP scambiano info tramite connessioni TCP (porta 179) chiamate **sessioni BGP** (funzionalità tramandate a livello trasporto):

- **Esterne**: instaurate tra route BGP appartenenti e AS diversi
- **Interne**: instaurate tra route BGP appartenenti e AS uguali

Le informazioni scambiate riguardano la raggiungibilità reti IP secondo lo schema classless (CIDR)

BGP: path vector → evoluzione distance vector → nel vettore sono elencati tutti gli AS da attraversa per raggiungere una destinazione → **evita cicli** (quando un router riceve un Path Vector controlla se il suo As è contenuto, se lo è quel path vector non viene considerato, altrimenti viene aggiornato e comunicato ai vicini)

Come si applicano politiche di Routing:

- Si comunicano ai vicini solo i path vector relativi alle destinazioni verso le quali si vuole permettere il transito (**export policies**)
- Dal path vector si può risalire agli AS da attraversare per arrivare a destinazione (ignoro incompatibily, **import policies**)

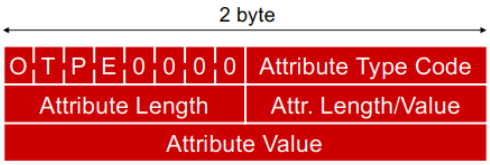
L'approccio è basato su percorso invece che sulla distanza non richiede la stessa metrica per tutti i router → scelte arbitrarie

Maggiore consuma banda, maggiori requisiti memoria router

Attributi associati al path vector → specificano la natura

- **Well-Known**: riconoscibile da tutte le implementazioni BGP, deve essere inoltrato assieme al path vector (dopo un eventuale aggiornamento)
  - Mandatory: deve essere presente nel path vector
  - Discretionary: può anche non essere indicato
- **Optional**: può non essere riconosciuto da alcuni router
  - Transitive: deve essere inoltrato anche se non riconosciuto
  - Non-transitive: deve essere ignorato se non riconosciuto
- **Partial**: si tratta di un attributo optional-transitive che è stato ritrasmesso senza modifiche da un router perché non lo ha riconosciuto (indica se un determinato path vector è stato riconosciuto o meno da tutti i router attraversati)

Gli attributi sono codificati da una **struttura** dalla lunghezza variabile all'interno del path vector.



alcuni attributi: **Origin** (code=1) indica come è stata ottenuta l'informazione se tramite EGP o IGP o in altro modo, **AS path** (code = 2) contiene l'elenco degli AS da attraversare verso la destinazione, **next hop** (Code = 3) indica l'IP del router del'AS che deve essere usato con next hop verso la destinazione

Formato dei messaggi

- **Marker**: campo per possibile schema di autenticazione
- **Length**: numero di byte del messaggio BGP, header incluso
- **Type**: indica il tipo di messaggio

Il campo type può assumere uno di questi valori:

- Open: primo messaggio trasmesso quando viene attivata una connessione verso un router BGP vicino, contiene
  - Informazioni di identificazione dell'AS di chi trasmette

    - Durata del timeout per considerare un vicino non più attivo
    - Dati di autenticazione
- Update: contiene il path vector e i relativi attributi
- Notification: messaggio di notifica di errori e/o di chiusura della connessione
- Keepalive: non contiene informazioni aggiuntive, ma è usato per comunicare ad un router BGP vicino, in assenza di nuove informazioni di Routing, che il trasmettitore è comunque attivo, anche se silente

9 – LAN (LOCAL AREA NETWORK)

→ infrastruttura di telecomunicazioni che consente ad apparanti indipendenti di comunicare.

- Indipendenti →non dipendono da altre architetture
- Area limitata →dimensioni moderate
- Canale fisico condiviso →unico mezzo fisico condiviso
- Elevata bit rate →uso esclusivo dell'intera banda anche se per intervalli brevi
- Bassi tassi d'errore →piccole distanze e quindi potenza elevata

Le LAN sono reti di calcolatori e devono essere implementate scegliendo protocolli per tutti gli strati dell'OSI → le dimensioni limitate rendono convenienti soluzioni particolari per gli strati 1 e 2. Bisogna Scegliere:

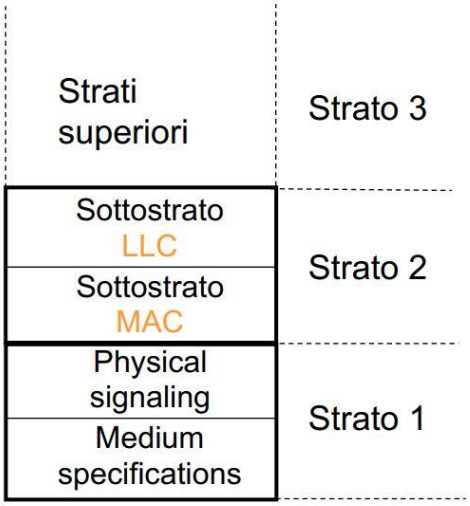
- **Mezzo trasmissivo**:
  - *Le fibre ottiche stanno pian piano sostituendo il* rame → maggiore banda e distanza, minore costo, interconnessione più complessa e costosa
  - Dato che la LAN è una rete piccola, il costo dell'attacco è più importante del costo del mezzo → la penetrazione delle fibre ottiche è più lenta e *quindi negli ultimi metri fino all'attacco sopravvivrebbero solamente le coppie intrecciate*
  - Radiocollegamento sta acquistando un'importanza sempre più crescente
- **Topologia**
  - WAN: Consigliate Stella, maglia più o meno completa, gerarchia
  - WAN: non adatte punto-multipunto = mezzo di condivisione condiviso = due caratteristiche peculiari → broadcast (tutti leggono i dati di tutti), collisione (essendo condiviso, più utenti inviano informazioni contemporaneamente)
  - Se ci sono pochi terminali non servono nodi di commutazione (BUS unidirezionale e bidirezionale, Doppio bus, Anello)
- **Eventuale protocollo di accesso**
  - Protocollo che regoli l'accesso al mezzo trasmissivo per evitare i fenomeni di collisione
    - Accesso multiplo a divisione di tempo

MAC

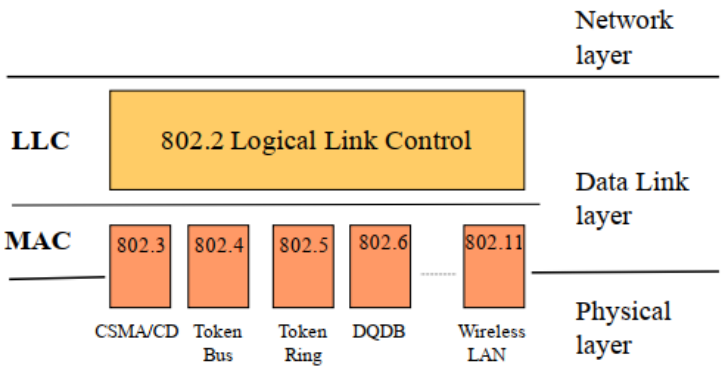
- Controllo **centralizzato** → coordinatore primario che coordina tutti gli altri
- Controllo **distribuito** → ogni terminale decide per se utilizzando il protocollo MAC
  - Assegnazione statica → per ogni connessione si usa un canale assegnato a priori in modo deterministico
  - Assegnazione Dinamica → la stazione utilizza il mezzo solo quando ne ha bisogno
    - Controlli di *collision free* → non ammettono collisioni
      - Token Ring
      - Token Bus
      - Utilizzati per scenari molto specifici
    - A contesa → ammettono collisioni e cercano di rimediare quando si verifica
      - ALOHA
      - CSMA/CD
      - CSMA/CA
    - CAP →insieme delle procedure che servono per realizzare l'accesso al canale
    - CRA →insieme delle procedure che servono per rivelare e riparare collisioni

Progetto IEEE 802

→Architetture master slave



- LLC= *logical link control* → Questo strato è indipendente dal mezzo fisico, dalla topologia e dal protocollo d'accesso
- MAC= *Medium Access Controll*



ETHERNET e IEEE 802.3

Rete Ethernet → Basato su protocollo d'accesso CSMA/CD

CSMA/CD

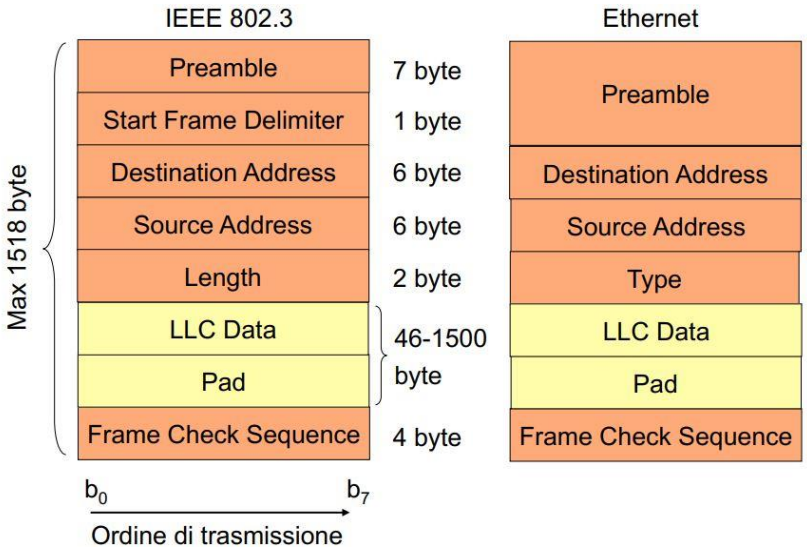
- Limita, ma non elimina possibilità che due stazioni parlino in contemporanea → Possibile collisione → Perdita frame
- Non è in grado di garantire i tempi di consegna del frame (ritardo di accesso)
- Permette un uso efficiente della banda disponibile

Frame

Dimensione minima = SLOT TIME → tempo necessario per trasmettere

- Solt time
  - 512 bit in reti a 10 e 100 Mbit/s
  - 4096 bit in reti a 1Gbit/s
- Trama deve avere una dimensione minima uguale allo slot time
- Sequenza di Jamming = 33 bit → abbastanza lunga per comprende rilevazione collisione
- Una volta fissata la dimensione del frame, ogni trama di dimensione minore viene scartata e viene imposto il tempo di propagazione massimo.

Campi del Frame



- Preamble →consente al ricevitore di sincronizzare il suo clock con quello del trasmettitore
- Sfd →flag di inizio Frame
- Lunghezza (IEEE 802.3) →numero di bit che ci sono nel campo dati/tipo(Ethernet)→payload
- Dati →contiene il payload del livello superiore
- Pad (=riempire) →se il frame è più corto di 64 byte, lo si porta a 64 byte
- Frame Checking sequence →bit per il controllo d'errore
- Indirizzi →sono cablati nella scheda di rete e sono composti di 6 byte (3 costruttore e 3 numero progressivo)

Delimitazione delle trame

Assenza di trame = assenza di segnale sul canale → inizio termine di un frame

Due frame devono essere separati almeno da un IFG (96 tempi di bit)

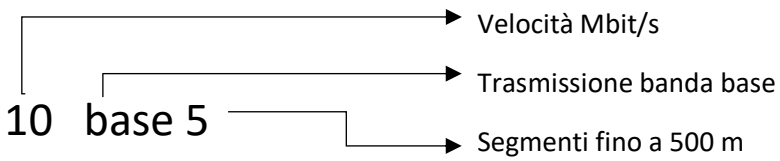
Collision Domain → insieme delle stazioni connesse alla medesima rete ethernet che possono collidere in trasmissione

- Per garantire corretto funzionamento di CSMA/CD
  - In funzione alla dimensione delle trame
  - In funzione alla velocità di trasmissione
- Mezzo trasmissivo impone dei vincoli sulle dimensioni dei collegamenti (attenuazione, rumore)
- La dimensione fisica del collision domain è conseguenza delle tecnologie adottate per lo strato fisico

Broadcast domain → è una trama **MAC** con destination address: ff.ff:ff.ff:ff:ff:ff

- Ricevuta da tutte le interfacce della LAN, realizza una comunicazione broadcast dalla sorgente a tutte le destinazioni della LAN (dominio di broadcast = stazione raggiungibili con l'invio della medesima trama)

Soluzioni per lo strato fisico dell'Ethernet



Ethernet Classica → 10 Mbits/s

- **10base5**
  - Cavo coassiale da 50 Ω, ϕ 6.15 mm → prese vampiro e drop cable fino 40 m
  - Cavo thin wire troppo rigido, non adatto per la cablazione di un edificio → occorrono prese a muro

- **10base2**
  - Cavo coassiale da 50 Ω, ϕ 2.95 mm → segmenti da 180 m con max 30 stazioni
  - Di solito si usa la 10base 5 per la *cablazione verticale* e la 10base2 per la *cablazione orizzontale*
  - Per raggiungere prese muro

Twisted pairs:

- **Schermato (STP)**
  - Nel cavo ogni coppia è avvolta in un conduttore per schermarlo
  - Maggiore costo
  - Schermo deve essere messo a massa
- **Non schermato (UTP)**
  - Più semplici da posare
  - Meno costoso

Studio dei nodi per maggiore prestazione → diametro, qualità dialettrico, regolarità ed infittire il passo di avvolgimento

Livelli di qualità → categorie da 1 a 7

- **10baseT,** twisted non schermato
  - UTP categoria 3 per arrivare a 100 m
  - Collegati a hub = repeater multi-porta per cablaggio orizzontale

- **10baseF,** fibra ottica multinodo
  - Fino a 2000 m di distanza
  - Costo alto di connettori ed attacchi
  - Usata spesso per cablaggio verticale

Cablaggio Strutturale → unico per tutti i servizi di telecomunicazione degli edifici (organizzato in gerarchia)

- EIA/TIA 568 (standard di mercato) → UTP: cavetti con diverse coppie finisco nelle prese a muro
- ISO 11801

Ethernet → 100 Mbit/s

- 802.3 tale e quale a 802 → rendendolo solo più veloce
- Ridefinirla con nuove caratteristiche 802.12 → Non ebbe successo

802.3u → diametro massimo collision domain 250 m

- **100baseT4,** 4 UTP categoria 3 (clock 25MHz) →lunghezza fino a 100 m
  - Codifica 8b/6T
  - Un UTP sempre in direzione hub-stazione →gli altri 2 vanno a rinforzare una direzione alternativa
- **100baseTX**
  - Due coppie UTP categoria 5, fino a 100 m
  - Clock 125 MHz →codifica 43/5b: 4bit mappati in 5
  - Velocità retta 100Mbit/s full duplex
  - Restano combinazioni libere per non dati
- **100baseFX**
  - Cavo fibra ottica multinodo
  - Fino 2000 m

GigaBit Ethernet 802.3z → Standard per definire una rete Ethernet a 1 Gbit/s

I collision domain dovrebbero diventare di 25 m per portali a 200 m →Si usa: carrier extension, frame bursting

- **1000baseSX** (fibra ottica multiuso) e **1000baseLX** (fibra ottica mono o multiuso)
  - Codifica 8b/10b
  - Generatori o Laser
  - Distanza 550 m o 500 m con LX mono-nodo
- **1000baseCX**, 2 coppie schermate STP, Soluzione costosa e meno performante

- **1000baseT**, 4 coppie UTP categoria 5, clock 125 MHz

  Codifica 2bit su 1 simbolo a 5 livelli

  - Disp 1 livello come non dato
  - Velocità netta 1Gbit/s

MultiGigaBit Ethernet → solo su fibra, diversi tipi e nodi di trasmissione

- Non sfruttabile dalla maggior parte dei pc sul mercato
- Moderna alternativa al MAN (backbone ≠ km)
- IEEE 802.17

Carrier Ethernet → nasce per le LAN, requisiti tecnologici ≠ per trasporto e accesso

Penetrazione dello strato di trasporto, richiede:

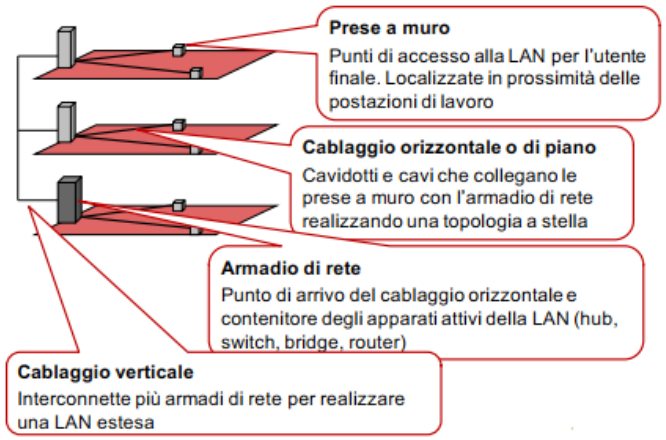
- Segnalazione e gestione
- Indirizzamento

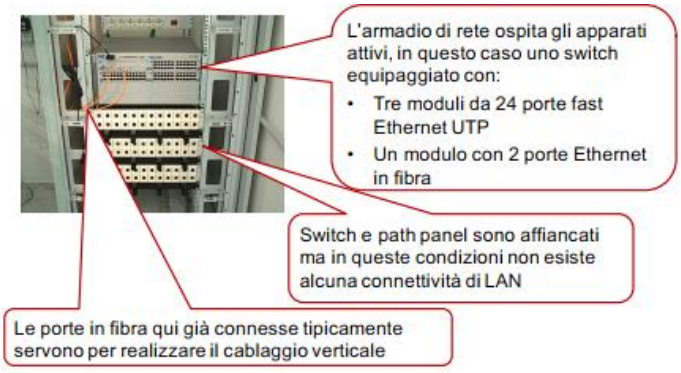
Sono in definizione nuovi standard per l'introduzione di altre funzioni (indirizzamento gerarchico multilivello, recupero guasti...)

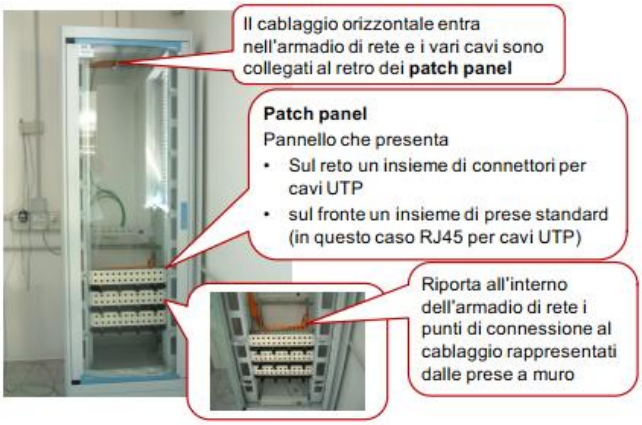
Il Cablaggio delle LAN moderne

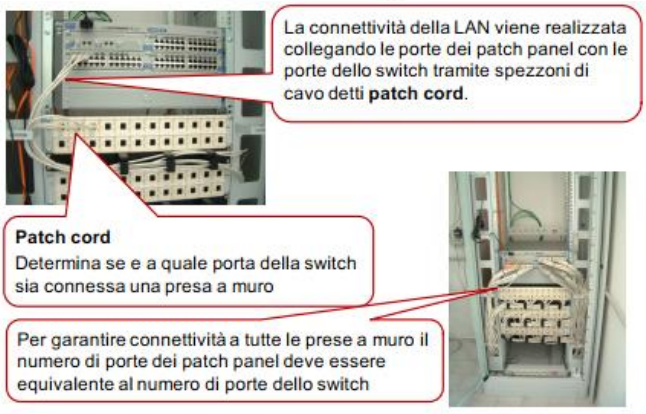
- Unico cablaggio per tutti i servizi di telecomunicazioni degli edifici → EIA/TIA 568 (standard di mercato), ISO 11801
- Soluzione più utilizzata basata su UTP → in un nuovo edificio vengono posati cavetti con diverse coppie e che poi finiscono nelle prese a muro per tutti i servizi Telecom.
- Cablaggio organizzato in modo gerarchico

Componenti, Armadio di rete, Apparati attivi nell'armadio e Patch cord e connettività









Wireless LAN (WI-FI)

IEEE 802.11 Wi-Fi nuovo standard 1997 per fornire LAN via radio

- Protocollo di accesso
- 1997 tre tecniche di trasmissione a 1 bit/s e 2 Mbit/s (infrarossi, FHSS, DSSS)
- Utilizza banda ISM a 2,4GHz (applicazioni industriali, scientifiche, mediche → NO licenze)
    - Uso libero →occorre regolamento per evitare abusi ed interferenze
        - Decreto 28/05/03 → richiesta al ministero per offrire
            - Wi-Fi su suolo pubblico
            - Obbligo identificazione utenti
            - No obbligo su privato di identificazione

802.11a → implementa Wi-Fi a banda larga → **ISM a 5GHz**, larghezza di banda 300 MHz

- Fa uso di OFDM
- Bit rate = **6, 9, 12, 18, 24, 36, 48, 54 Mb/s** →scelto in base alla distanza da coprire

802.11b → implementa Wi-Fi a banda larga → **ISM a 2.4GHz**, larghezza di banda 300 MHz

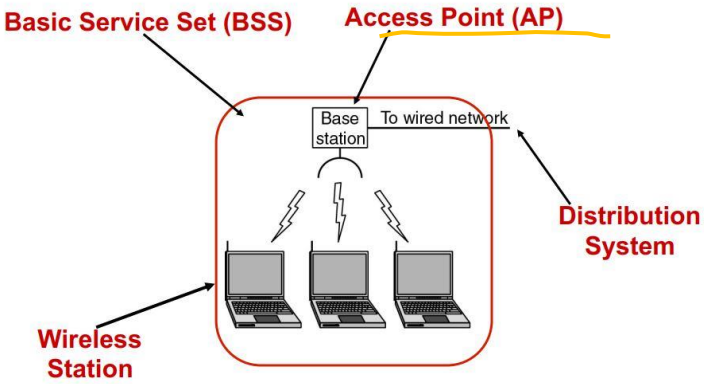
- High-rate DSSS

Bit rate = **1, 5.5, 11 Mb/s** → riesce ad adattare la bit rate alle condizioni del canale (Dynamic Rate Shifting)

802.11g → ISM 2.4GHz

- OFDM (bit rate come 802.11a) ma può essere anche HR-DSSS (bit rate come 802.11b)

Architettura 802.11



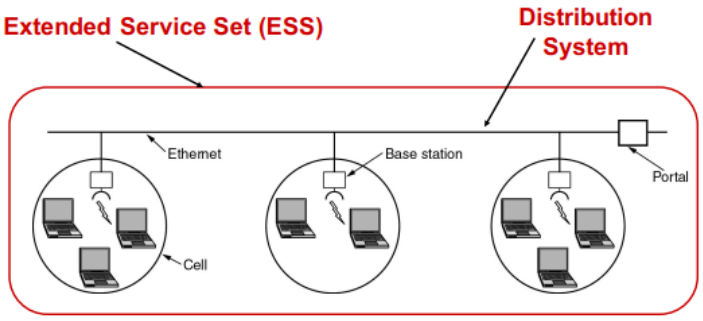
MODALITA' INFRASTRATTURATA:

Infrastructure BSS → Le stazioni comunicano attraverso Access Point (anche se non si vedono direttamente)

MODALITA' AD-HOC:

Independent BSS → Le stazioni comunicano in modalità P2P solo se si vedono direttamente

Extended service Set (ESS)



Occorre gestire l'associazione della stazione agli AP. Permette 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 broadcast

A differenza delle LAN cablate nelle WLAN ci sono problemi specifici:

- Stazione nascosta → raggio Wi-Fi
- Stazione esposta

Interconnessione di LAN E Virtual LAN (VLAN)

→ A volte può essere conveniente suddividere la LAN in più spezzoni

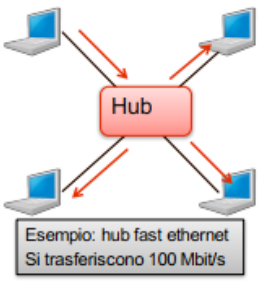
Strumenti di interconnessione di LAN

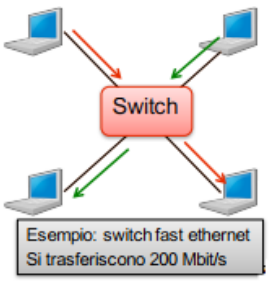
- **Repeater** → apparato attivo
  - Collega due o più mezzi di trasmissione
  - Opera a livello dello Strato 1 OSI
  - Permette l'estensione del mezzo di trasmissione
    - Amplifica segnale
    - Rigenera bit entranti e ti sincronizza
  - Permette di estendere la topologia LAN
  - Massimo 2500 m di diametro complessivo
- **Bridge**
  - Opera a livello dello Strato 2 OSI
  - Può Interconnette LAN di diverso tipo
    - Esegue protocolli MAC
  - Nel caso di reti Ethernet separa i domini di collisione
  - Learning bridge e Filtering bridge
    - Separa il traffico dei diversi domini di collisione
    - Invia la trama solo sulla porta di uscita del destinatario
    - Impara quali stazioni sono connesse ad una porta analizzando il "source address"
- **Router**
  - Opera a livello dello Strato 3 OSI
  - Domini Broadcast separati
  - Permette separazione LAN per efficienza e sicurezza
- **Gateway**

Switch → è un **bridge** ad alta densità di porte

- Per ogni porta una sola stazione
- Uno Switch ethernet svolge una funzione simile all'hub, ma garantendo maggiori prestazioni
- Capacità aggregata superiore a quella della singola porta

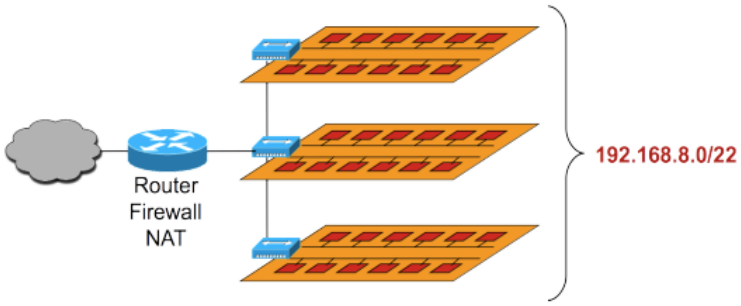
Hub → bus collassato = mezzo condiviso, capacità aggregata = capacità singola porta





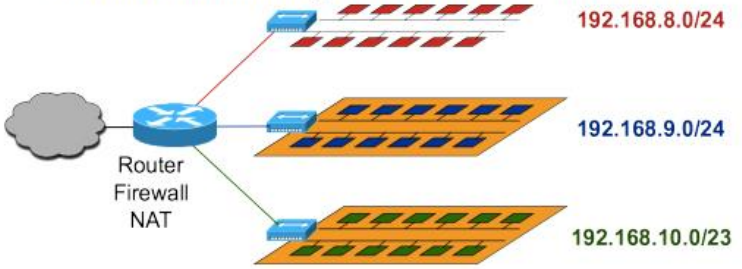
Interconnessione di LAN tramite switch

- Unico dominio broadcast
- Funzionalmente equivalente ad un'unica LAN



Interconnessione di LAN tramite router

- Domini broadcast separati
- Permette la separazione delle LAN per motivi di
  - efficienza
  - Sicurezza
- Limitata mobilità degli host da una LAN all'altra



10 – VIRTUALIZZAZIONE

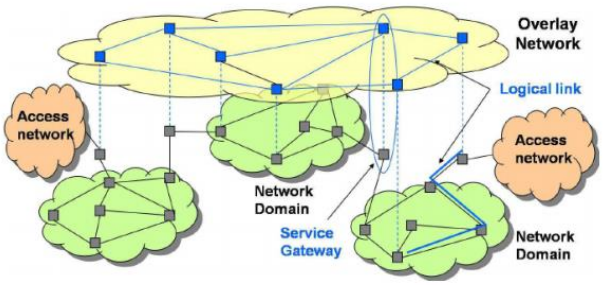
Virtualizzazione di rete

→ significa creare versioni "virtuali" di sistemi di computazione, di memorizzazione, di rete

- Versione virtuali di un sistema: il sistema viene eseguito come elemento software logicamente indipendente dall'hardware utilizzato
    - VANTAGGI
        - Condivisione di risorse fisiche
        - Maggiore mobilità, flessibilità e scalabilità
        - Disaccoppiamento del progetto software da quello hardware
    - SVANTAGGI
        - Isolamento fra sistemi distinti con lo stesso hardware
        - Sicurezza e privacy

→ **punto di partenza**: infrastruttura difficilmente modificabile su richiesta, le esigenze di servizio presentano complessità sempre crescente.

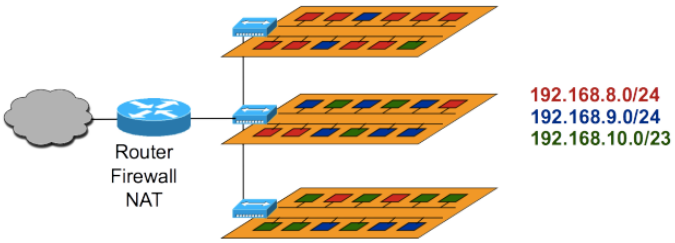
→ **obiettivo della virtualizzazione**: realizzare funzionalità/topologie diverse sull'infrastruttura.



Reti "**overlay**": sono sovrapposte logicamente all'infrastruttura fisica per realizzare funzionalità diverse da quelle normalmente fornite dalla stessa.

Tecnologie di virtualizzazione → VLAN, VXLAN, VPN, VPWS, VPLS

VLAN



- LAN virtuali separate all'interno dello stesso Switch
- Direct forwarding fra host della stessa VLAN
- Indirect forwarding tramite gateway fra host di VLAN diverse
- Ogni VLAN rappresenta un diverso dominio broadcast

Può essere:

- STATICA o port based
    - Ogni porta dello Switch è associata ad una VLAN
    - Un host appartiene alla VLAN corrispondente alla porta a cui è connesso
    - Per spostare un host bisogna lavorare sullo switch e modificare la VLAN a cui è associata la porta
- DINAMICA
    - L'appartenenza alle VLAN è stabilita in base all'indirizzo dell'host (MAC-based, IP-based)
    - Un host appartiene alla corrispondente VLAN indipendentemente dalla porta a cui è connesso
    - Per spostare un host bisogna lavorare sullo switch e modificare la VLAN associata all'indirizzo dell'host

IEEE 802.1Q

- Protocollo che permette utilizzo delle stesse VLAN su diversi Switch interconnessi tra loro
- Occorre specificare a quale VLAN appartiene una trama inviata ad un altro switchdatalinkp
- Etichetta tag su intestazione Ethernet che identifica a quale VLAN appartiene il frame

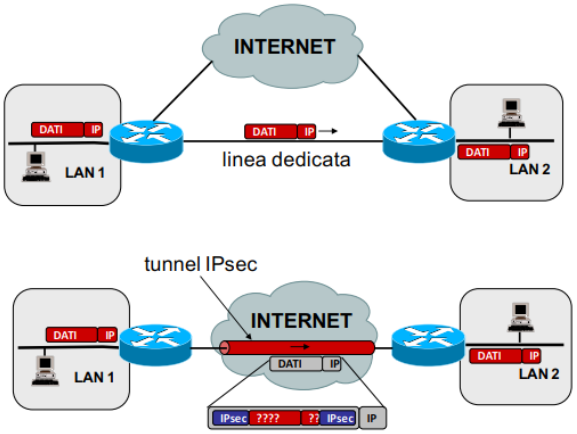
Inter-VLAN Routing

- In teoria un router dovrebbe avere un interfaccia dedicata per ciascuna VLAN
  - Ma è una soluzione inefficace e poco scalabile
- Uso interfacce virtuali a sub-interfacce

Porte dello switch

- **Access Mode:** porta associata ad una sola VLAN, tagging 802.1Q non necessario, modalità tipica per porte connesse agli host
- **Trunk Mode:** porta associata a VLAN multiple, tagging 802.1Q necessario per determinare la VLAN a cui appartiene ciascun frame ethernet, può essere associata contemporaneamente a una sola VLAN untagged e a più VLAN tagged, modalità tipica per porte connesse a switch e router

Reti private e reti private virtuali



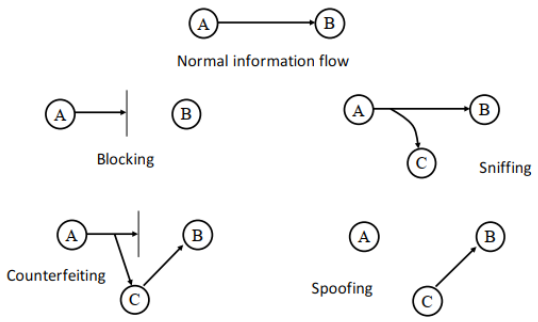
→ ci possono essere aziende di dimensioni medio/grandi che hanno necessità a connettere in maniera sicura sedi diverse e distanti tra loro

→ soluzione **tradizionale**: reti private (linee dedicate da affittare direttamente presso gli operatori). Implicano costi di acquisto e gestione dedicati

→ soluzione **alternativa**: reti private pubbliche – **VPN**. (utilizzo di una rete in "overlay" attraverso reti pubbliche).

- Flusso punto-punto di pacchetti autenticati. (con contenuto criptato) incapsulati in pacchetti tradizionali
- Diverse tecnologie
- Diversi protocolli di tunnelling: livello 2: PPTP, L2TP livello 3: IPsec

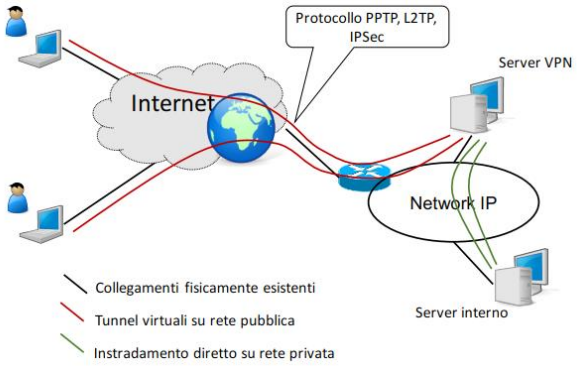
RISCHI della comunicazione remota



OBIETTIVI di una rete privata

- Riservatezza: non tutti possono leggere le informazioni
- Autorizzazione: definizione del sottoinsieme di coloro che sono in grado di leggere i dati
- Autenticazione: verifico chi sta leggendo i dati
- Paternità: garantisco l'origine dei dati

VPN Roadwarrior



- Su una rete viene configurato un server VPN
- Tutti i client si collegano a quel server da un punto qualsiasi di internet → tunnel sicuri punto a punto
- Sul server VPN si configura come una rete di comunicazioni sicure.

Problema → se ho molti host co-localizzati il roadwarrior è inefficiente. n host richiedono n tunnel.

VPN da rete a rete (**Net-to-Net**)

→ creazione di un tunnel cifrato su rete pubblica fra due LAN o fra due network IP.

- Rete pubblica → pacchetti vengono cifrati e l'indirizzamento mascherato

IPsec

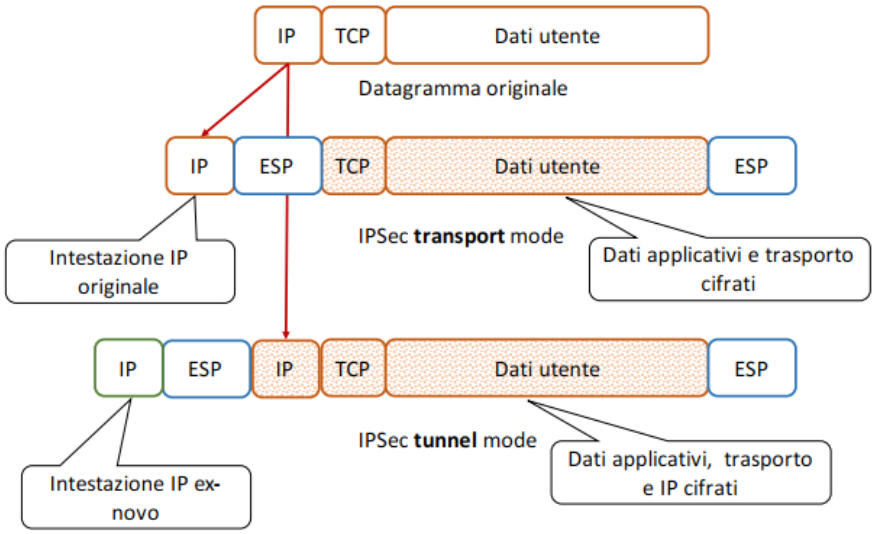
→ Security Association (SA) relazione unidirezionale tra mittente e destinatario definita da: SPI, IP destinazione, Security Protocol Identfier

→ due modalità di SA: Transport Mode e Tunnel Mode

Protocolli

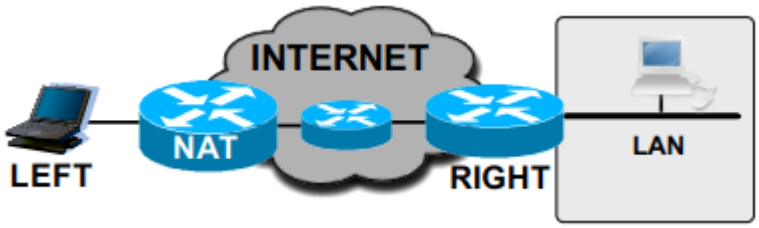
- IKE (Internet key Exchange): autenticazione dell'interlocutore e negoziazione tramite algoritmi e chiavi crittografiche.
  - Fase 1: negoziazione preliminare (uno dei server cerca di contattare l'altro e poi i due router si accordano sui parametri di sicurezza da usare in questa fase)
  - Fase 2: negoziazione della connessione (i due router VPN si accordano sui parametri di sicurezza della comunicazione e poi si generano/rinnovano le chiavi crittografiche)
- AH (Authentication Header): autenticazione dei pacchetti trasmessi in VPN garantendo integrità/autenticità dei dati e identità del mittente
- ESP (Encapsulating Security payload): come AH + riservatezza delle informazioni tramite crittografia

ESP: tunnel mode VS transport mode



IPsec attraverso un NAT

- La negoziazione IKE potrebbe non andare a buon fine, perché i pacchetti inviati da LEFT arrivano a RIGHT con un indirizzo IP diverso da quello atteso
- Il NAPT potrebbe cambiare la porta UDP sorgente di LEFT, mentre RIGHT potrebbe rifiutare traffico IKE da porte UDP ≠ 500
- La scadenza della tabella NAT potrebbe avvenire durante un periodo di silenzio, interrompendo così la connessione sicura
- Il NAPT non riesce a distinguere pacchetti ESP appartenenti a connessioni IPsec provenienti da LEFT diversi (ESP non usa porte)
- Nella modalità trasporto, la modifica di un indirizzo IP richiederebbe di aggiornare la checksum TCP o UDP (che fa uso di pseudo-header IP), ma questa è cifrata all'interno del payload IP



Soluzione da applicare ai terminali IPsec → non si ha controllo sul NAT

Problemi dovuti alla presenza di NAT vengono risolti con:

- Verifica delle capacità dei peer di eseguire NAT-Traversal
- **NAT-Discovery**: Verifica della presenza di NAT tra LEFT e RIGHT
- **NAT-Keepalive**: invio periodico di pacchetti per mantenere attive le connessioni nelle tabelle NAT
- Incapsulamento di ESP in UDP, utilizzando le stesse porte IKE → così il NAT riesce a distinguere connessioni diverse.