

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
- bidirezionale:
 - 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 descritta tramite un *grafo* ed è composta da *rami* e *nodi*

- Maglia completa
 - Collegamenti per ogni coppia di nodi
 - $N(N-1)/2$ 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

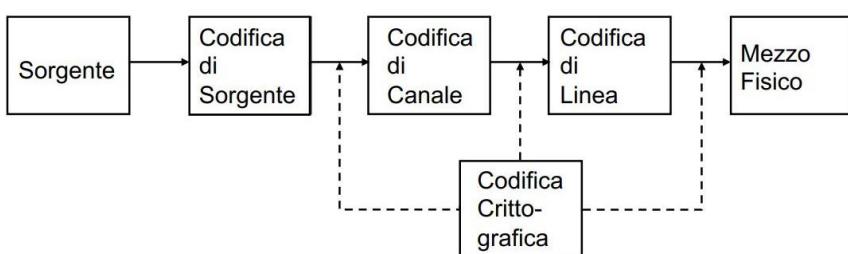
→ una rete integrata nei servizi deve essere flessibile nella Allocazione della banda e la gestione della qualità di servizio

Multiplazione, Codifica e QoS



→ i nodi di rete sono connessi tramite collegamenti
→ collegamento caratterizzato dal mezzo trasmittivo: 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 diverse 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, sincronizzati 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 plesiocrono:** 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)

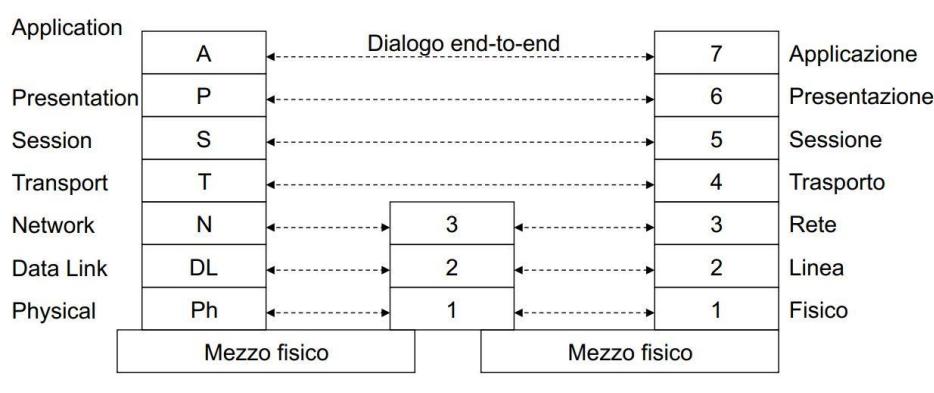
- Problemi
 - Diversità delle reti → Calcolatori non riescono a comunicare, non riescono ad interpretare segnali di altri, no cooperazione in sistema distribuito
- Soluzione
 - Realizzazione di standard unificati → realizzazione di Sistemi Aperti (cioè realizzare una rete di calcolatori in cui qualunque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

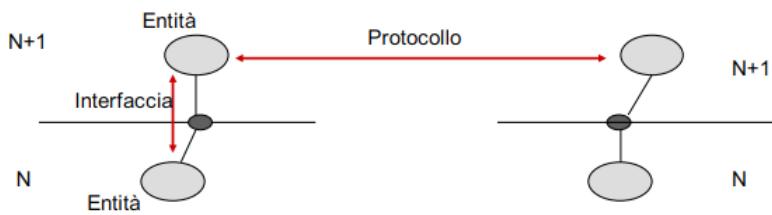
Le definizioni contenute nell'OSI coinvolgono 3 livelli di astrazione:

- 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*



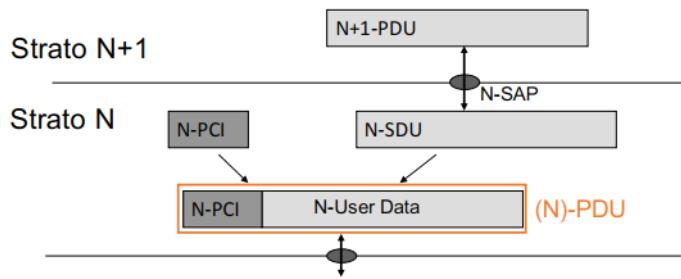


Entità: ogni elemento attivo in uno strato, identificato da numero simbolico (title)

Protocollo: regole dialogo tra entità dello stesso livello

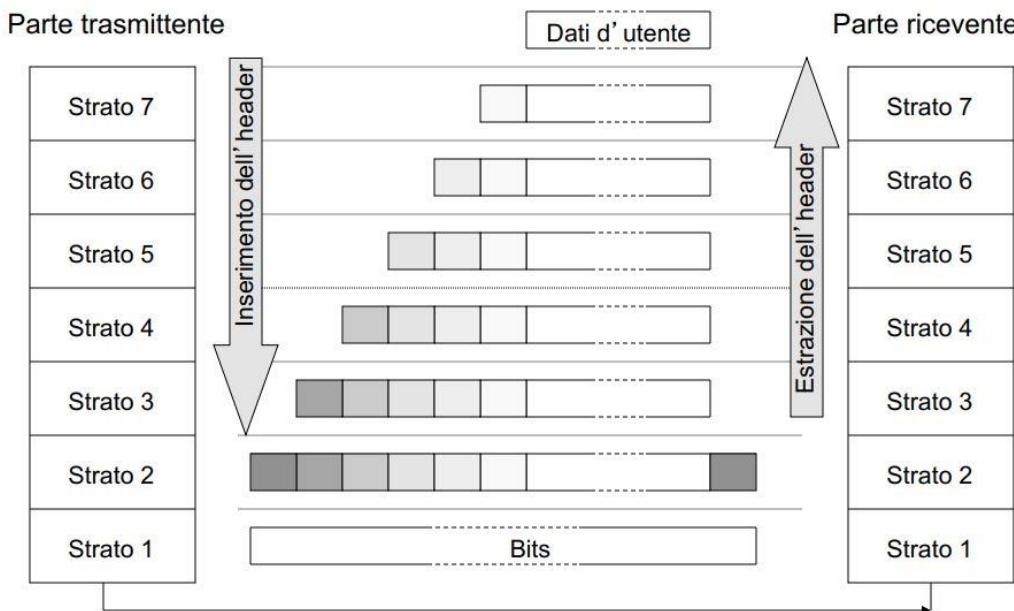
Interfacce: regole di dialogo tra entità di livelli vicini → con quelli comunicanti

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 Point) → 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

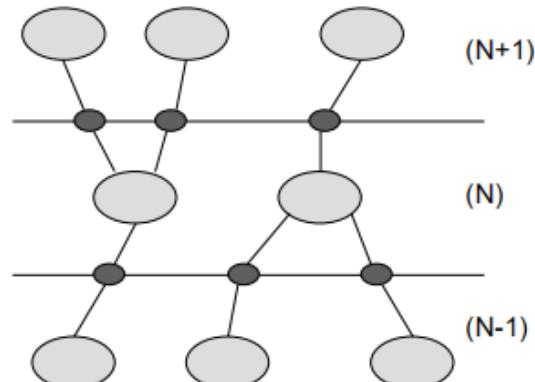
Flusso delle Informazioni



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: dividere 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 dei 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 di 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/riassembramento)
- Altre funzioni: controllo errore flusso, gestione dati prioritari
- Non tutte le applicazioni hanno bisogno delle stesse funzioni → classi di trasporto

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

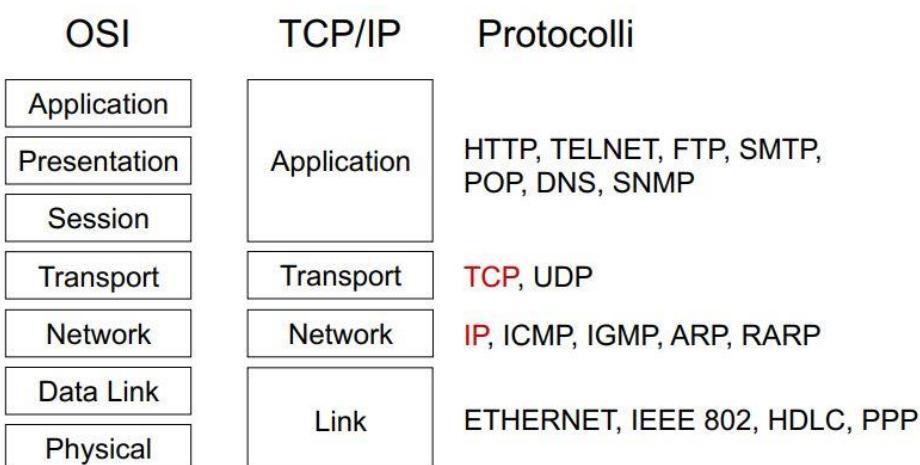
- Messaggi
- Rappresenta il programma applicativo (Applicazione)
- Non può essere completamente standardizzato → solo su richiesta di gruppi utenti interessati

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

Obiettivo 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
 - *Numeri 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

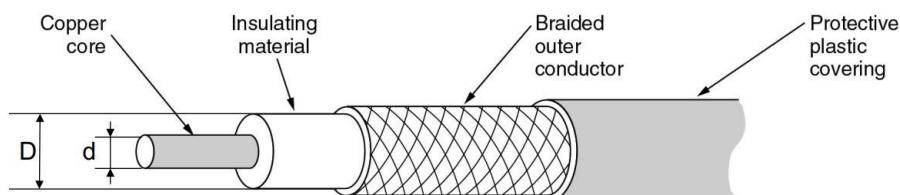
Ogni circa 18 mesi la banda a disposizione dell'utente raddoppia, a costo circa costante

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

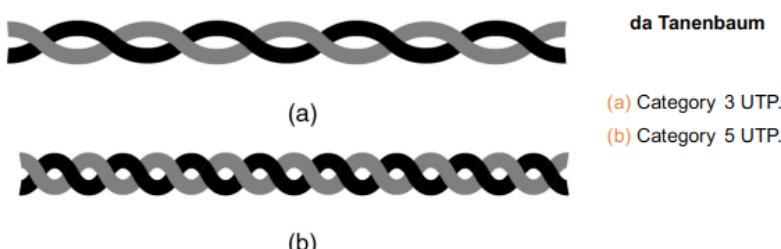
- Cavo bifilare
 - Coppie intrecciate da posare in cavi → problema della diafonia
 - Costruite per le linee telefoniche anni 80

Twisted Pairs (coppie intrecciate)

- ➔ STP (shielded 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 (unshielded 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

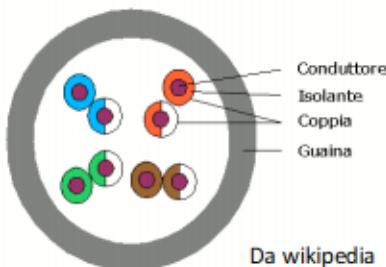
(a) Category 3 UTP.

(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.

UTP



Da wikipedia

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 antenne 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)

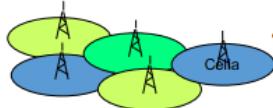
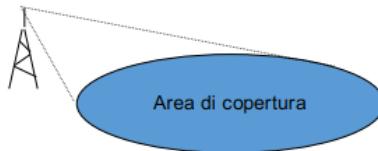
Evoluzione

- 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

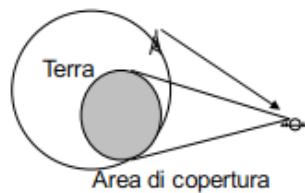
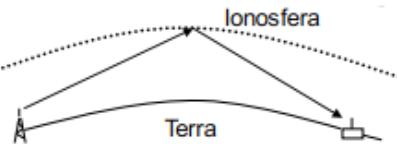
- Diffusione radiofonica/televisiva
 - Raggiungere la maggior quantità di utenti possibili con un solo segnale
 - Pianificazione della localizzazione delle emittenti



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

Grande distanza

- Propagazione ionosferica
 - Servizio di radiodiffusione ad onda corta
- Radiocommunicazione 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

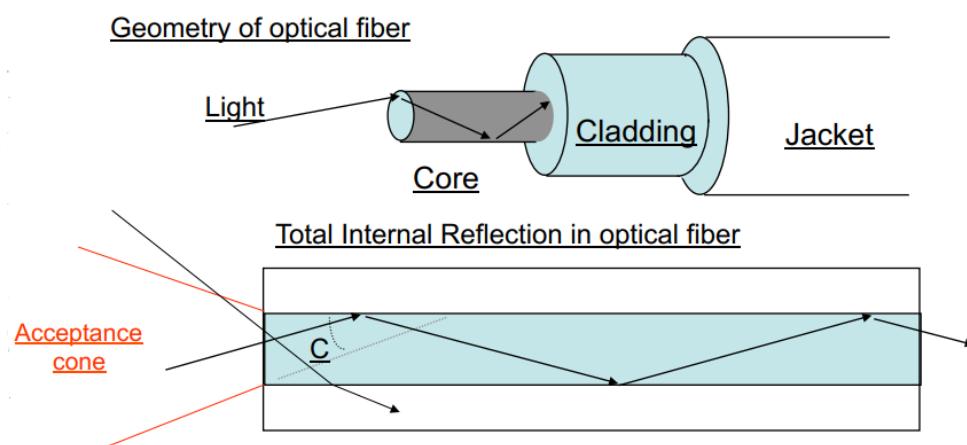
→ **ETACS** a 900 MHz: copertura nazionale, analogico

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

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

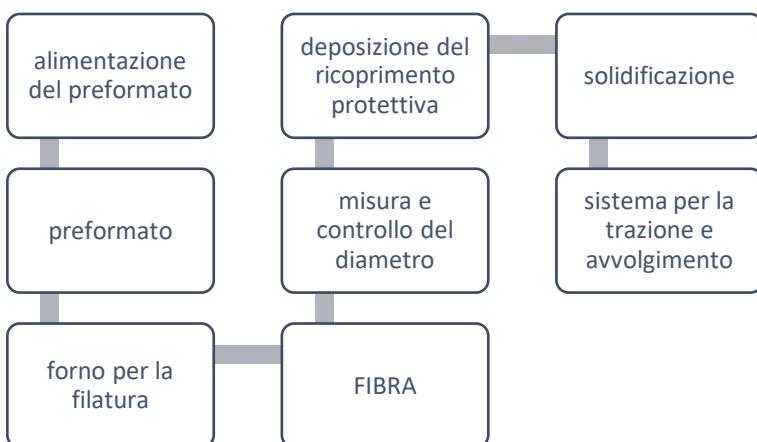
Fibra Ottica

- 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)

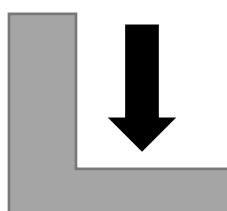


- **Core** (ha un indice di rifrazione più grande del cladding)
- I raggi di luce che colpiscono la discontinuità ad un angolo inferiore a quello critico sono completamente riflessi
- Il vetro assorbe parte della luce che lo attraversa → densità diminuisce a mano a mano che attraversa il vetro
- Strada 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



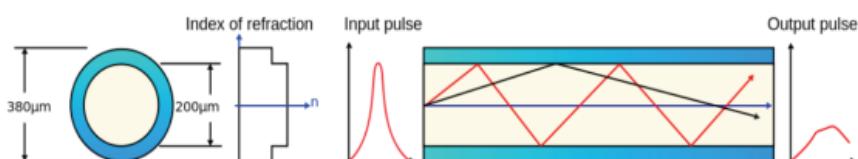
tutto questo viene svolto su un supporto meccanico (a forma di L) dall'alto verso il basso



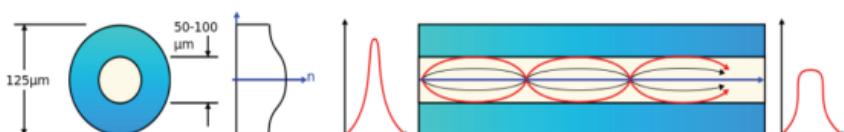
Tipi di fibre ottiche

- **Multimode fiber**

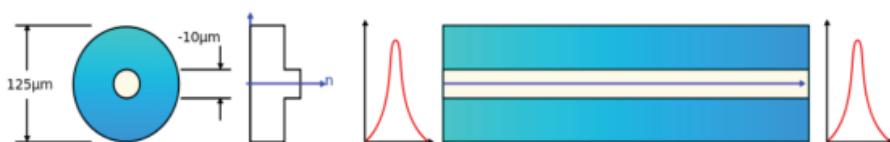
- **Step index fiber**



- **Graduated index fiber**

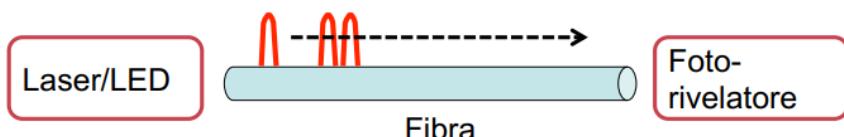


- **Singlemode fiber**



Sistema di trasmissione

- Sorgente di luce: laser, led generano gli impulsi
- Impulsi: si propagano per grandi distanze, generati ad alta velocità
- Rilevatore: fotodiodo riceve gli impulsi



Paradosso: aumento esponenziale delle prestazioni con aumento dei costi circa nullo

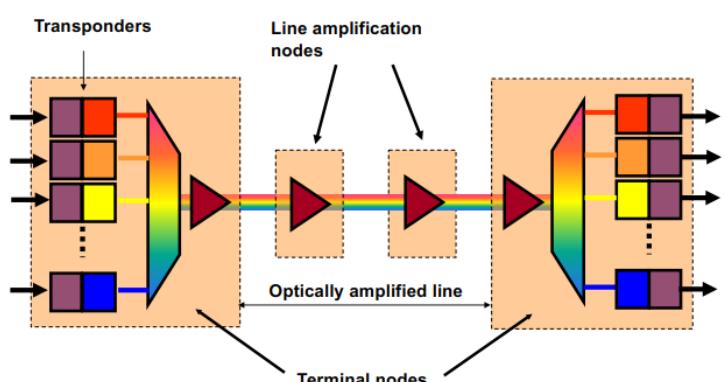
Problema → le fibre ottiche sono più difficili da giungere (elemento critico → stabilità dell'allineamento)

- 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: Wavelength Division Multiplexing

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

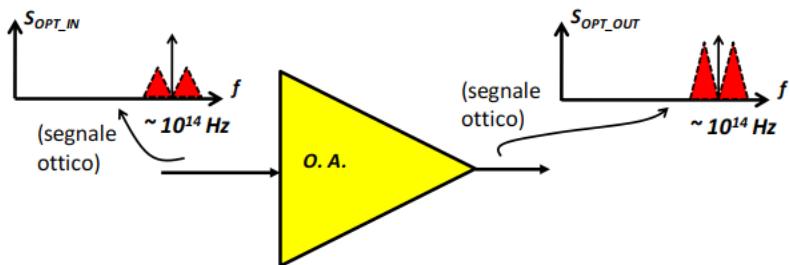
- È un modo alternativo per FDM
- Multiplazione di diversi flussi su diversi ambiti di frequenze (o di lunghezze d'onda)
- Permette di aumentare molto la capacità della rete senza installare nuove fibre



Principi del WDM

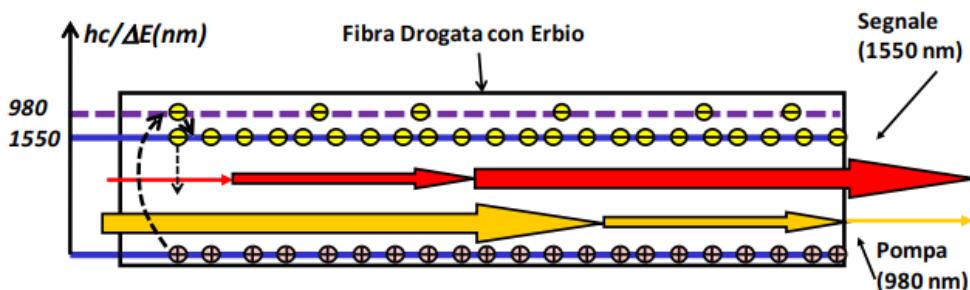
- Utilizzo dei diversi colori della luce per trasmettere più flussi
- I vari flussi convivono senza danneggiarsi sulla stessa fibra
- Più flussi uso, più informazione viene trasportata

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



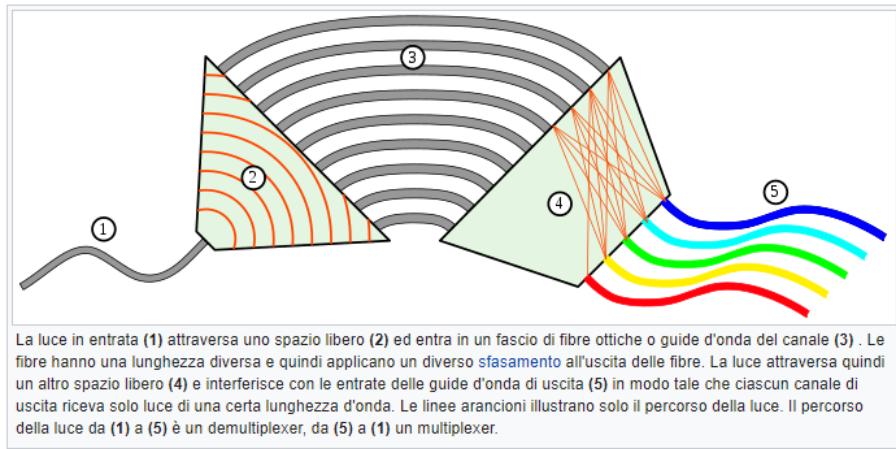
- Drogaggio di Erbio
 - Alcuni livelli instabili e un livello metastabile.
 - Laser di pompa → elettroni a livello instabile
 - Inversione di popolazione → da livello instabile a livello metastabile
 - Il segnale attraversa la fibra → amplificazione per emissione stimolata
- Amplificazione tramite diversi 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 luce in modo comandato (ROADM)

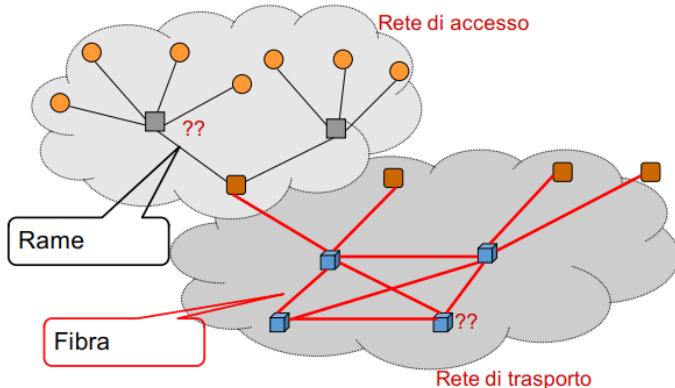
ROADM → apparati che selezionano il colore della luce in modo complicato

AWG → Arrayed Waveguide Gratings



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

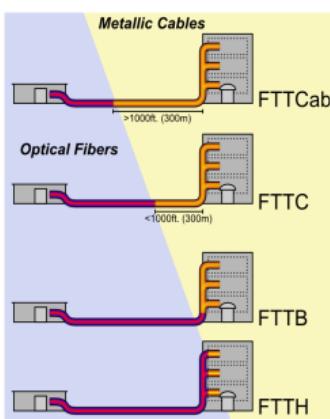
Le reti di oggi sono formate così:



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

- Classificate in base alla localizzazione dell'interfaccia elettrico/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 Convolutionali: r bit calcolati mediante reti logiche sequenziali

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

k bit vengono codificati in una parola di **n** bit aggiungendo **r = n - k** bit

2^n Parole di codice per trasportare **2^k** messaggi

- 2^k Sono parole di codice ammesse → valide
- $2^n - 2^k$ 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 m_1 e m_2
- Ricavate le parole di codice c_1 e c_2
- Il codice si dice lineare se $m_3 = m_1 + m_2$ da origine a $c_3 = c_1 + c_2$

Codificatori sistematici

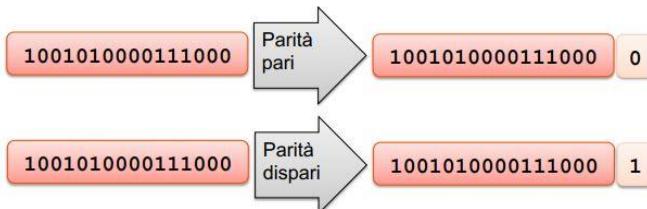
- Nella sequenza di n bit da trasmettere i k bit di informazione, mantenuti distinti dagli r bit di ridondanza, vengono trasmessi inalterati

Rbit = in ricezione → NO ERRORE

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

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

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



- 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

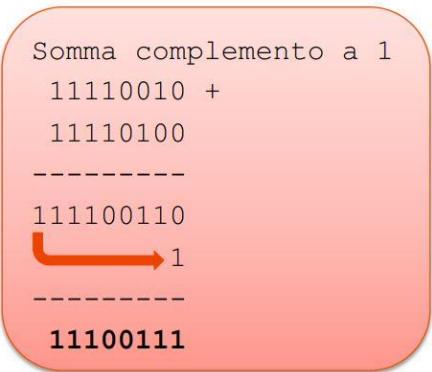
Internet Checksum

- 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 \oplus (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 (Automatic 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 (ACKNOWLEDGE) → 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 impostare 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.

Numeri 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

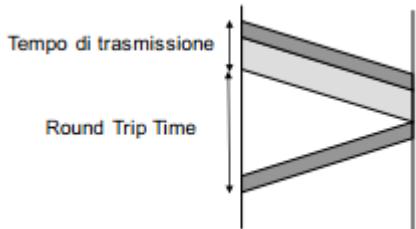
- Ricostruire in ricezione la corretta sequenza dei dati

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. Svantaggio: 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** ≤ **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

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

Esercizio 1

- Protocollo Stop and Wait
 - Velocità della linea: $C = 4 \text{ Kbit/s}$
 - Ritardo di elaborazione e propagazione: $I = 20 \text{ ms}$
 - $H \approx A \approx 0$
- 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 $A \approx H$:

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

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

- Sostituendo i dati di progetto forniti dal testo:

$$\eta = \frac{D}{D + 2H + 2IC} \approx \frac{D}{D + 2IC} \geq 0.5$$

$$\Rightarrow D \geq 0.5D + IC \Rightarrow 0.5D \geq IC$$

$$\Rightarrow D \geq 2IC = 2 \cdot 4 \cdot 10^3 \cdot 20 \cdot 10^{-3} = 8 \cdot 20 = 160$$

- 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 informativi 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
- Identifier (URI): identificativo di una certa risorsa di rete

Alcuni esempi:

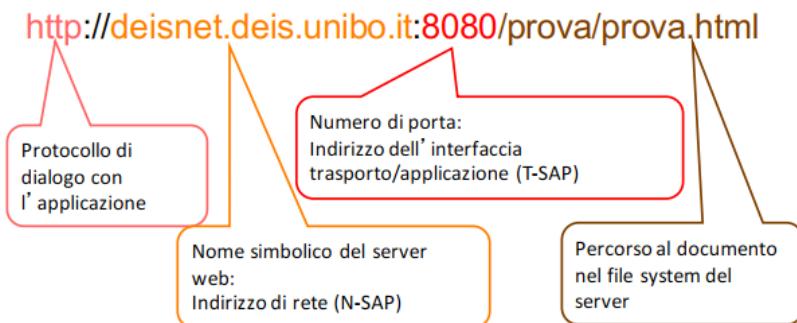
- Mobilità: un terminale si sposta da una rete all’altra (Locator → cambia nel tempo)
- Multi-homing: un terminale è connesso a più interfacce a infrastrutture diverse (molti locator attivi contemporaneamente)

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*

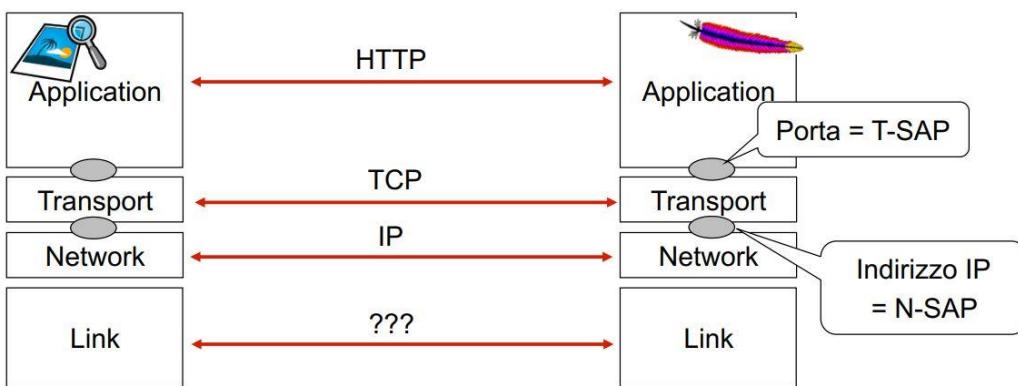
Indirizzamento nel web

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 identificato 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

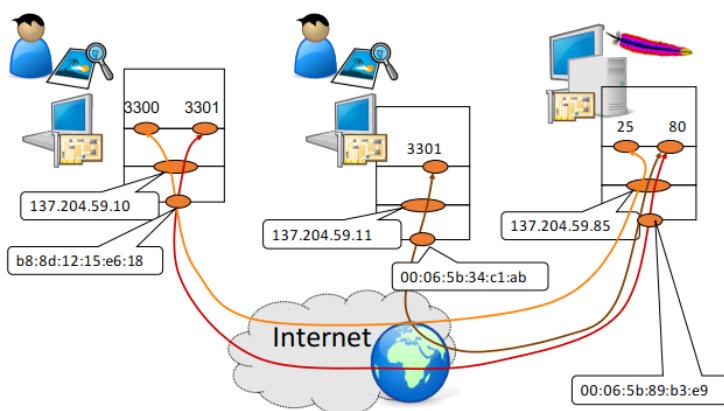
- MAC ADDRESS 48 bit, sono cablati nella schede di rete e sono univoci a livello mondiale → primi 3 byte individuano il costruttore
- È possibile specificare:
 - Un singolo destinatario → unicast → 00-60-b0-78-e8-fd
 - Un indirizzo di gruppo → multicast → primo bit a 1
 - Invio a tutte le stazioni →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

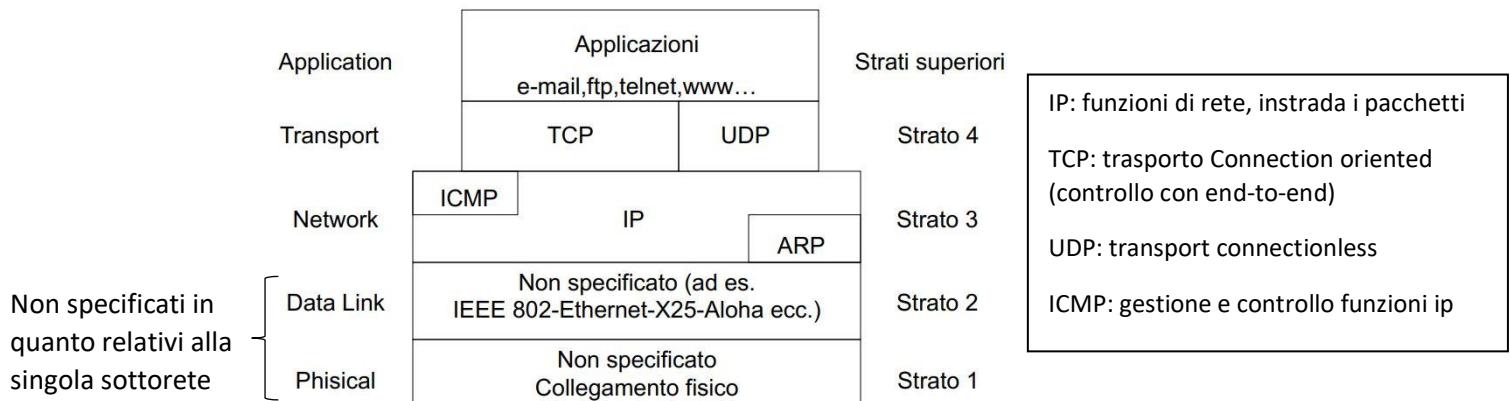
→ il client deve conoscere indirizzo IP e il numero di porta del server di destinazione → sono specificati nell'URL (protocollo applicativo, eventuale numero di porta non standard, numero IP o nome del server)

Conclusione

- Utente finale interagisce con software applicativo
- L'applicazione dialoga con una o più applicazioni remote utilizzando i protocolli
- I protocolli applicativi sfruttano il trasporto dei protocolli di traporto per raggiungere le applicazioni remote
- Protocollo di trasporto utilizza 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

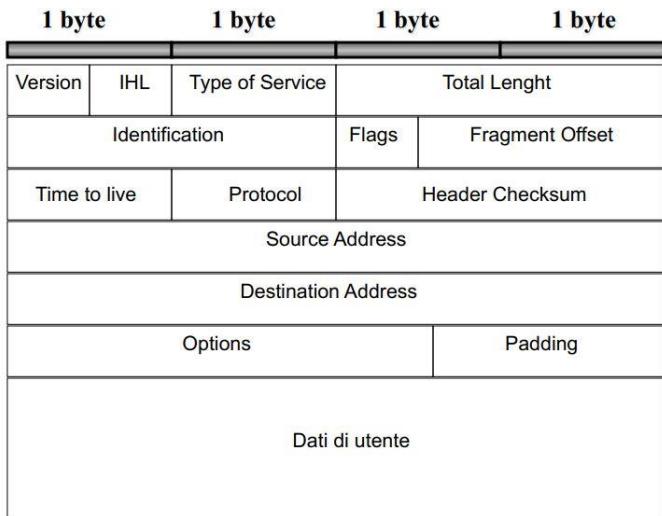


Protocollo IP (Internet Protocol) → livello di Rete

- 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 Riassembra 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

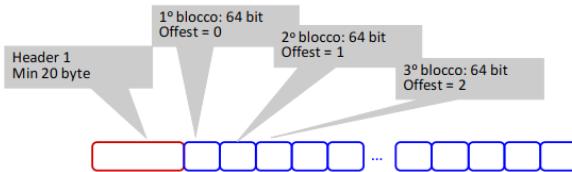
- **Version:** indica il formato dell'intestazione, attualmente la versione in uso è la 4
- **IHL:** lunghezza dell'intestazione, espressa in parole di 32 bit; lunghezza minima = 5
- **Type of service:** indicazione sul tipo di servizio richiesto, usato anche come sorta di priorità
- **Total length:** 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 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

Fragment offset → specifico

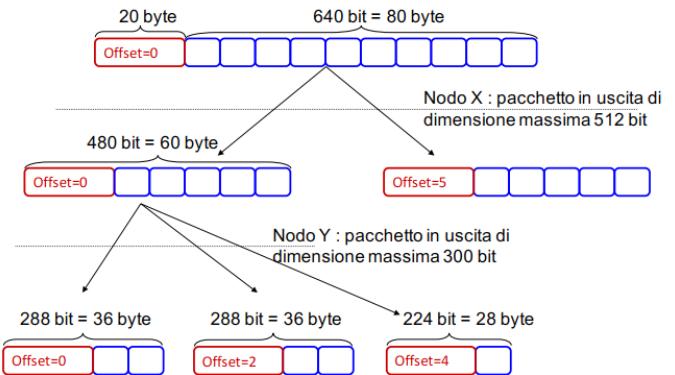
- Datagramma virtualmente diviso in sotto-blocchi da 8 byte (64 bit)
- Per la sorgente o nodo intermedio che trasmette l'IP → Numerazione sequenziale a partire dallo 0 per i sottoblocchi
- Il numero logico del primo blocco viene memorizzato nel fragment offset del datagramma

Implementazione

- Chi frammenta i datagrammi?
 - Qualunque apparato di rete dotato di protocollo IP può frammentare un datagramma
 - Tipicamente i nodi intermedi non riassemlano, 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

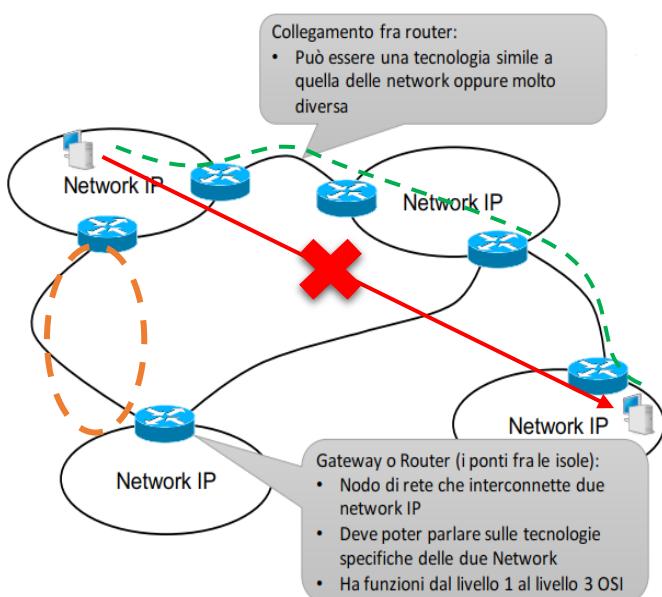
→ la rete internet è una rete a commutazione di pacchetto

→ 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 possono 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.



Interconnessione 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.

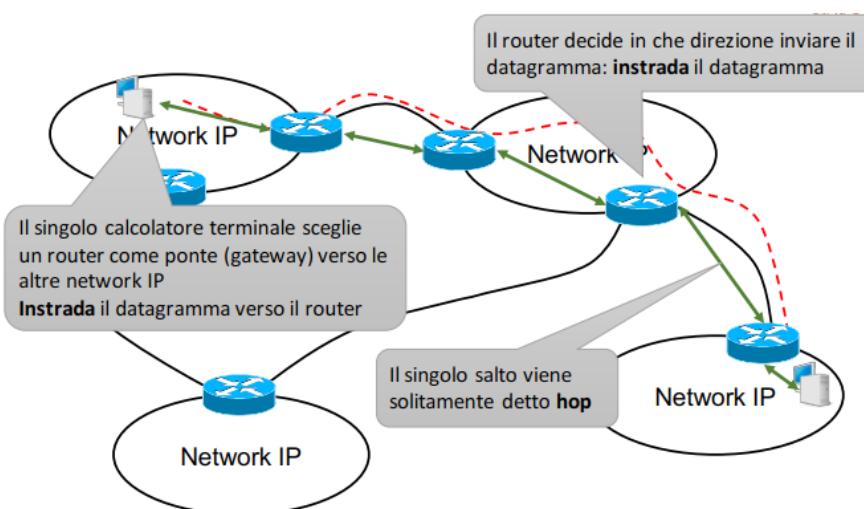
Percorso **rosso**: non si possono connettere due isole direttamente senza rispettare i router.

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

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

Cosa fa IP?

L'obiettivo 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 172.31.255.255
 - 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

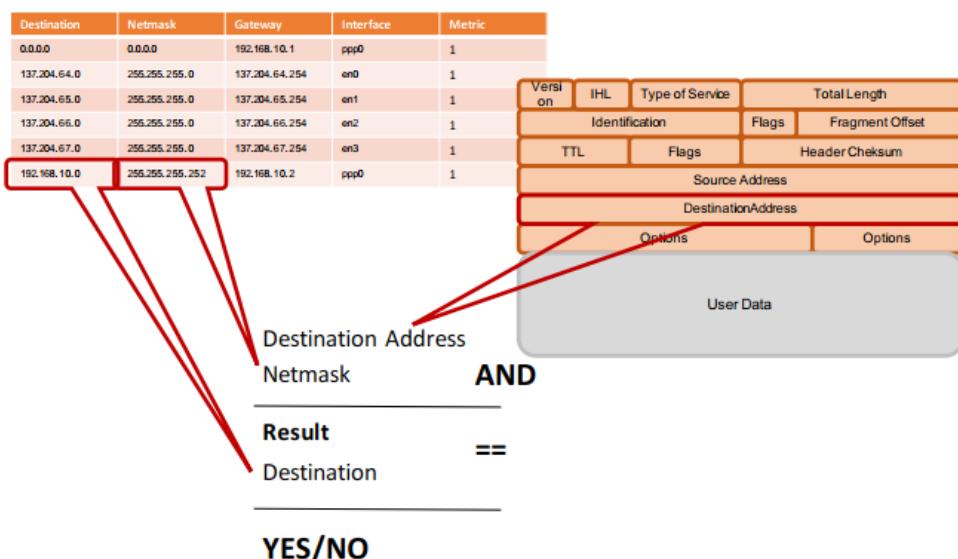
Nodo riceve datagramma:

1. Estraie 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 con 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
2. La funzione di instradamento invia il datagramma a IF_i , con l'obiettivo di consegnarlo al gateway G_i
3. IF_i non è sufficiente perché normalmente l'instradamento lo è basato sulle network, gli host nella medesima network possono comunicare direttamente, mentre se sono di network differenti allora devono utilizzare un router.

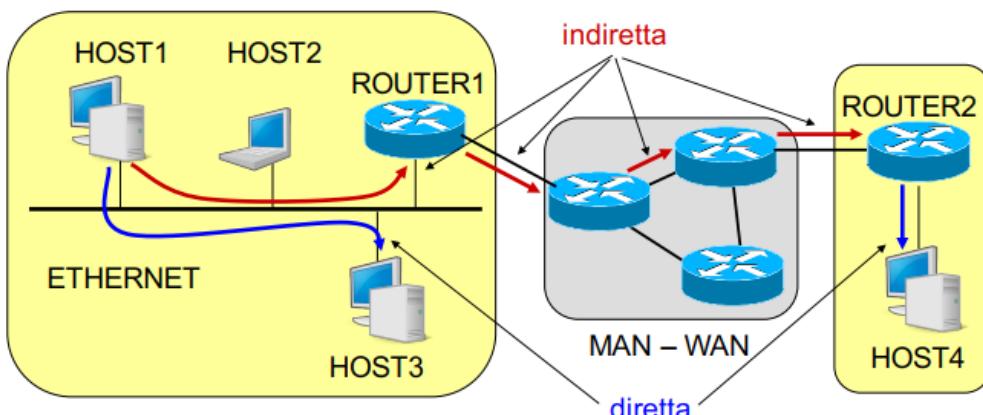
Routing → scelta percorso su cui inviare dati

- 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



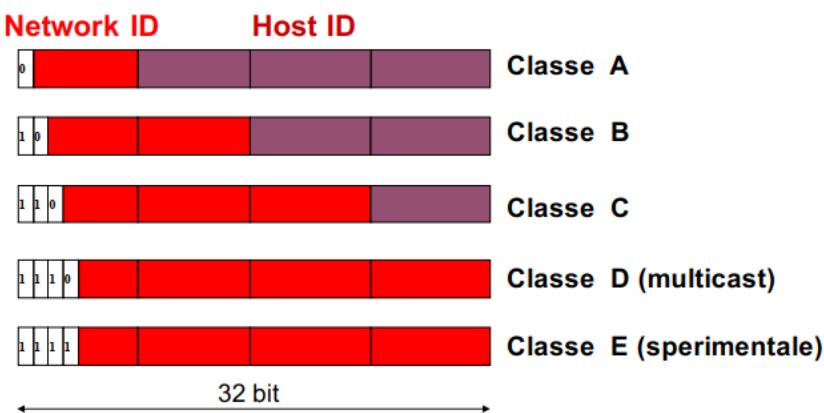
Classless VS Classfull: la logica degli indirizzi IP

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



Network ID : identifica una rete IP

Host ID : identifica i singoli calcolatori della rete

Definite diverse **classi** di network differenziate per **dimensione** → La parte iniziale 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

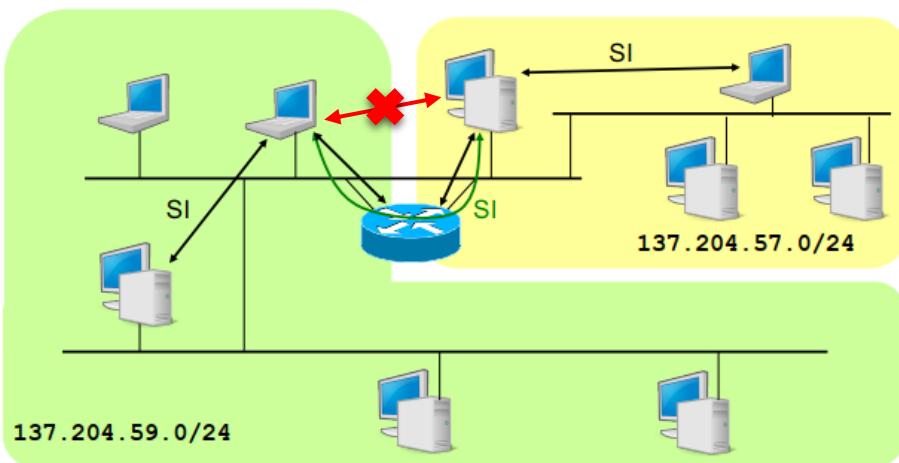
Le Sottoreti → frammentare la network in **sub-network** da assegnare alle **sotto-amministrazioni**

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

- La prima identifico **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

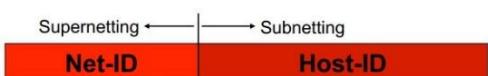
- una rete di classe B è troppo grande (64K indirizzi)
- meglio 8 reti di classe C ($8 \times 256 = 2048$ indirizzi) dalla 194.24.0.0 alla 194.24.7.0

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)

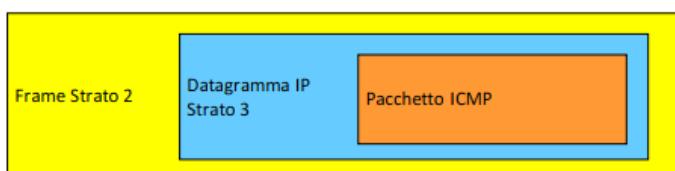
route -p add DEST mask NETMASK GATEWAY → aggiunge alla tabella di routing Window una entry permanente relativa alla destinazione DEST indicandone la NETMASK e il GATEWAY attraverso il quale raggiungerla

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 identifica 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
 - 2 = protocollo non disponibile
 - 3 = porta non disponibile
 - 4 = frammentazione necessaria ma bit don't fragment settato
- **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

$$\text{Tempo di processamento} = T_{transmit} - T_{receive}$$
- **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 decremente **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 **DHCPPACK** 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

- Packet 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; 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.

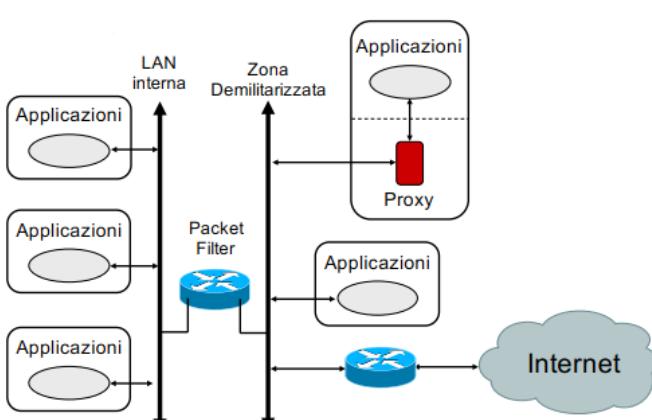
Configurazione della politica di default per i servizi di ete:

- 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:

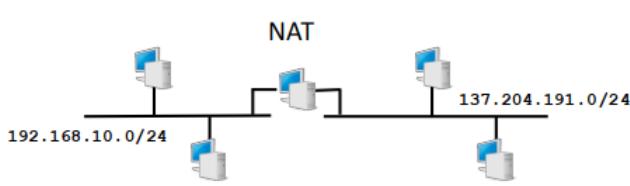
- Si interpone fra router locale e internet
- Sul router si configura un filtro sui datagrammi IP da trasferire attraverso le varie interfacce
- Il filtro scorta i datagrammi sulla base di:
 - IP sorgente e destinatario
 - Tipo di server a cui il datagramma è destinato (porta TCP/UDP)
 - Interfaccia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

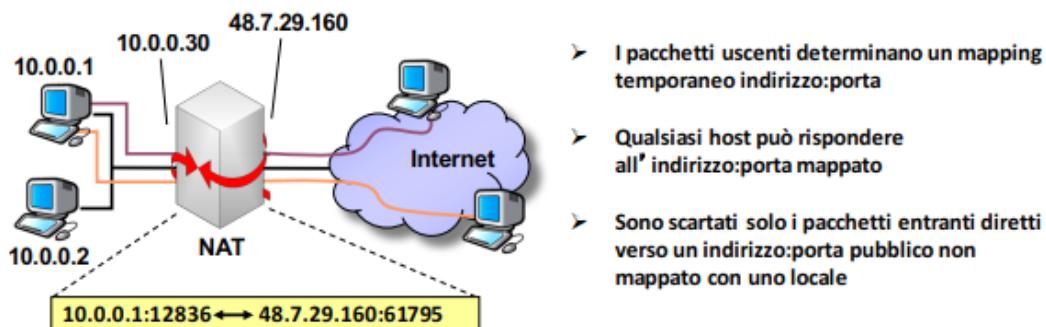
Direzione delle connessioni

- 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

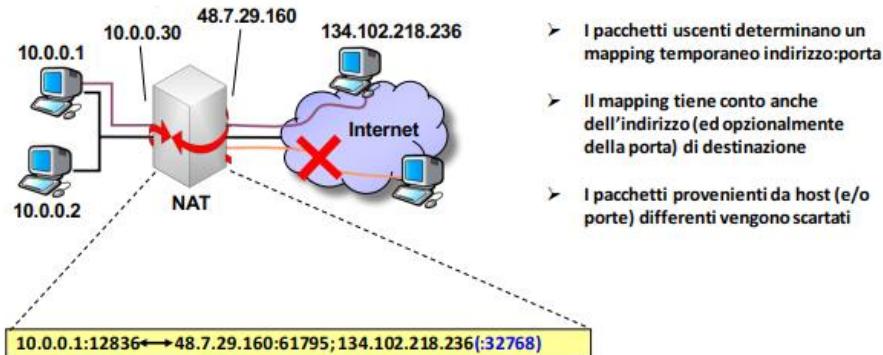
NAT e applicazioni di rete

- 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:

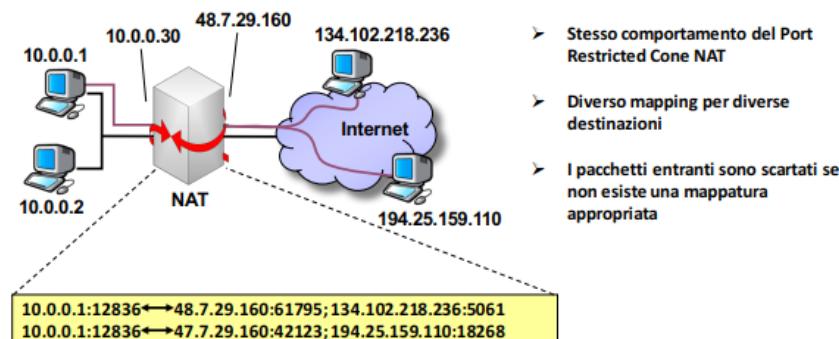
Full Cone NAT: Mapping indirizzo: porta locale \leftrightarrow indirizzo: porta pubblica. Accetta tutti i pacchetti provenienti dall'esterno diretti verso indirizzo : porta pubblica (solo se è mappato con indirizzo: porta privato)



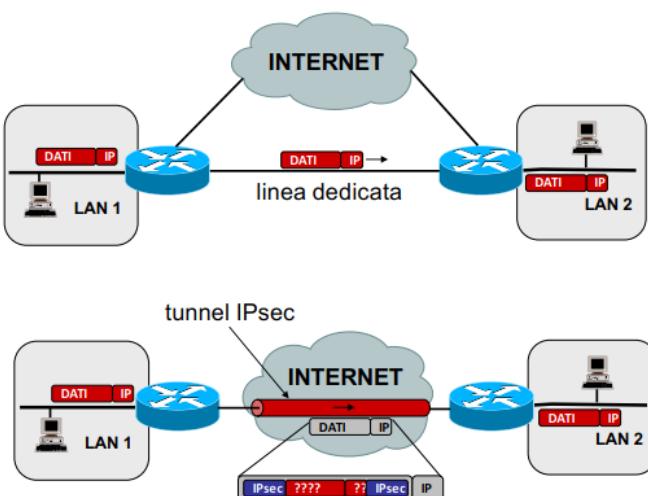
(port) **Restricted Cone NAT:** Cone Full come NAT ma la mappatura tiene conto della destinazione, vengono scartati tutti pacchetti provenienti da host non preventivamente contattati da un host locale



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



VPN (Virtual Private Network)



Reti private 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 lunghi: 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:

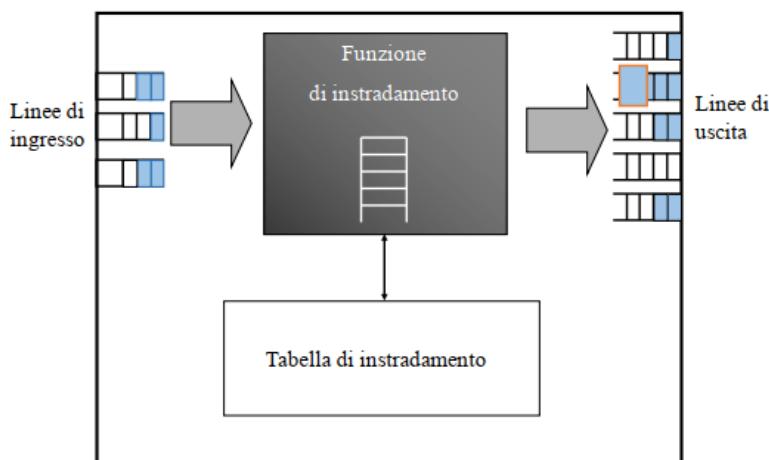
- Supportare molti miliardi di host
- Semplificare Routing
- Meccanismo sicurezza
- Qualità servizio (multimedialità)
- Gestire bene Multicast e broadcast
- Consentire mobilità
- Fare tutto ciò consentendo future evoluzioni e garantendo compatibilità col passato

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 volta 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:

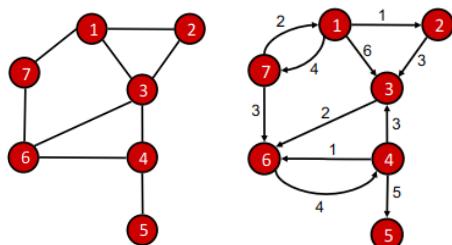
- Distribuita → ogni nodo esegue i calcoli per conto suo (sincrona e asincrona)
- Centralizzata → un solo nodo esegue i calcoli per tutti

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 traversati
 - Distanza geografica
 - Ritardo introdotto da collegamento
 - Costo di un certo instradamento
 - Combinazione dei precedenti

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

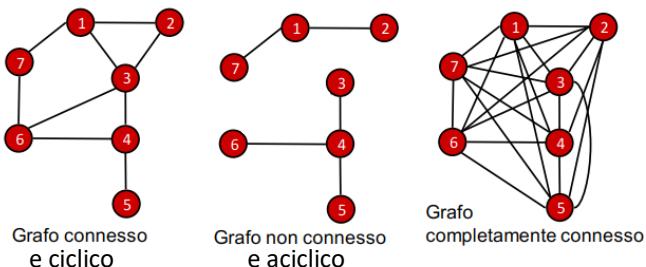


• Grafo

- 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)



- **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 G_1 , se l'insieme dei nodi di G è sotto-insieme dei nodi di G_1 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

$$D^0_i = \infty \quad \forall i \neq 1$$

$$D^0_1 = 0$$

- Operazione 1

$$h = h+1$$

- Operazione 2

$$D^{h+1}_i = \min[d_{ij} + D^h_j] \quad \forall i$$

- Termino l'algoritmo se

$$D^{h+1}_i = D^h_i \quad \forall i$$

- Il valore di D^h_i viene chiamato D_i , ed è la lunghezza del più breve percorso da i a 1

composto da questi $N-1$ archi. Partendo dal nodo i si seguono gli archi del sotto-grafo fino a raggiungere il nodo 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.

Intradamento → per ottenere i percorsi, per ogni nodo i si sceglie l'argo e si applica l'equazione e si considera il sotto-grafo

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

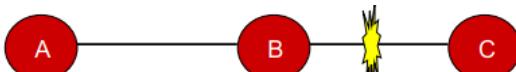
- All'inizio le tabelle dei singoli nodi contengono solo l'indicazione del nodo stesso a distanza 0 → da cui in poi il distance vector permette di creare tabelle sempre più complete. L'algoritmo converge al più dopo un numero di passi pari al numero di nodi nella rete. → più la rete è grande più il tempo 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 incongruenze possono dare luogo a dei cicli e quindi i nodi si scambiano datagrammi fino a quando non terminare il TTL

Count to infinity

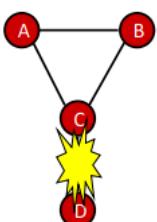


- Situazione iniziale: $D_{AB} = 1$, $D_{BC} = 1$ e $D_{AC} = 2$
 - Link BC va fuori servizio
 - B riceve il DV di A che contiene l'informazione $D_{AC} = 2$, per cui esso computa una nuova $D'_{BC} = D_{BA} + D_{AC} = 3$
 - B comunica ad A la sua nuova distanza da C
 - A calcola la nuova distanza $D_{AC}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

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 infinity

- **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

Non sono davvero risolutivi

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
 - $F_h = F_{h-1} \cup \{j \in M \text{ tale che } d_{ij} \leq d_{ik} \quad \forall i \in F \text{ e } \forall k \in M\}$
 - $F'_h = F'_{h-1} - j$
- Termina quando
 - $F' = \emptyset$
- 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 Floating a cui vengono aggiunte informazioni e poi si usa Dijkstra per calcolo cammini minori e quindi i router saranno in grado di costruire l'immagine della rete.

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

Il router IP

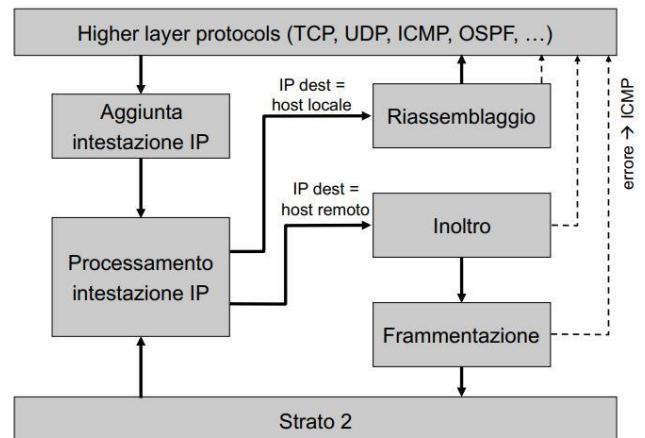
Router IP: nodo di commutazione a pacchetto nelle reti IP

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

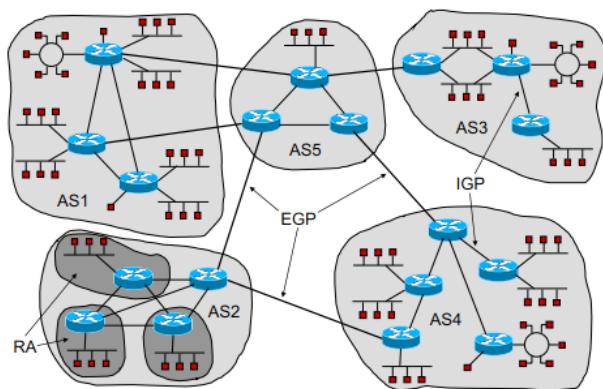
Forwarding table (FIB): ottenuta come ottimizzazione per il lookup della RIB. È più corta e veloce da leggere → tabella aggregata → si ottiene dalla Routing table

→ 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 Gateway 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 gateway 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 (trasportati 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

ripetuto

command	version	must be zero
address family identifier		must be zero
address		
must be zero		
must be zero		
metric		
address family identifier		must be zero
address		
must be zero		
must be zero		
metric		

→ 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 indicata
- **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

command	version	routing domain
11111111	11111111	authentication type
authentication data		
address family identifier		route tag
address		
subnet mask		
next hop		
metric		

- 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 routing domain)
- Non adatto a AS grandi
- problemi di convergenza (perché rimane un distance vector)

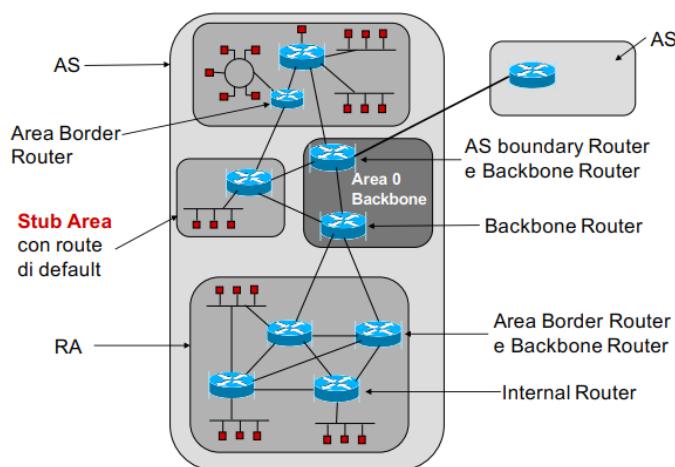
OSPF (open shortest path first)

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

Arene 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 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 Boundary 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 Arene

- **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 → invia messaggi usando protocollo IP (camp protocol = 89)

Version	Type	Packet Length
Router ID		
Area ID		
Checksum	AuType	
Authentication		
Authentication		
...		

- **Version:** versione di OSPF
- **Type:** tipo di pacchetto (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 trasmessa a livello trasporto):

- **Esterne**: instaurate tra route BGP appartenenti a diversi AS
- **Interne**: instaurate tra route BGP appartenenti allo stesso AS

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 attraversare 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 (ignora incompatibilità, **import policies**)

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

Maggiore consumo 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.

2 byte	
O T P E 0 0 0 0	Attribute Type Code
Attribute Length	Attr. Length/Value
Attribute Value	

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 dell'AS che deve essere usato con next hop verso la destinazione

Formato dei messaggi

# byte	HEADER COMUNE
16	Marker
2	Length
1	Type

- **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 apparati 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:

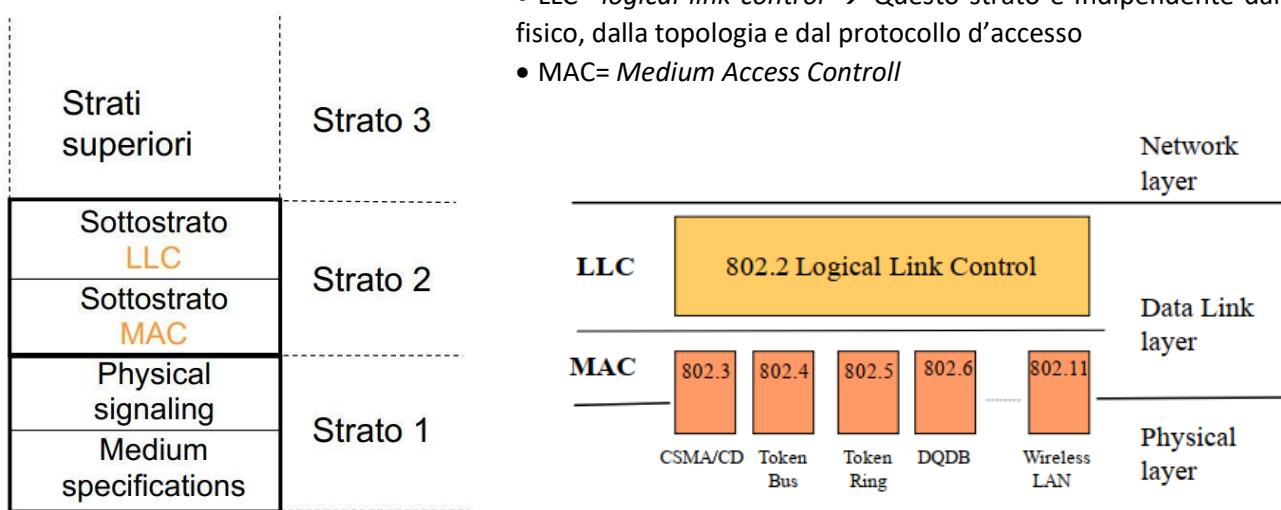
- **Mezzo trasmissivo:**
 - *Le fibre ottiche stanno pian piano sostituendo il rame* → maggiore banda e distanza, minore costo, interconnessione più complessa e costosa
 - Dato che la LAN è una rete piccola, il costo dell'attacco è più importante del costo del mezzo → la penetrazione delle fibre ottiche 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 sé 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



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

- Slot 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 comprendere 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

IEEE 802.3		Ethernet	
Preamble	7 byte	Preamble	Max 1518 byte
Start Frame Delimiter	1 byte	Destination Address	
Destination Address	6 byte	Source Address	
Source Address	6 byte	Type	
Length	2 byte	LLC Data	
LLC Data	46-1500 byte	Pad	
Pad		Frame Check Sequence	
Frame Check Sequence	4 byte		
$b_0 \rightarrow b_7$		Ordine di trasmissione	
<ul style="list-style-type: none"> • <u>Preamble</u> → consente al ricevitore di sincronizzare il suo clock con quello del trasmettitore • <u>Sfd</u> → flag di inizio Frame • <u>Lunghezza</u> (IEEE 802.3) → numero di bit che ci sono nel campo dati/tipo(Ethernet) → payload • <u>Dati</u> → contiene il payload del livello superiore • <u>Pad</u> (=riempire) → se il frame è più corto di 64 byte, lo si porta a 64 byte • <u>Frame Checking sequence</u> → bit per il controllo d'errore • <u>Indirizzi</u> → sono cablati nella scheda di rete e sono composti di 6 byte (3 costruttori e 3 numeri progressivi) 			

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)

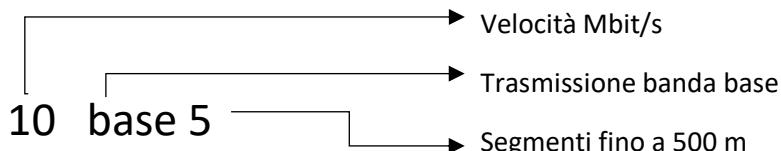
Collision Domain → insieme delle stazioni connesse alla medesima rete ethernet che possono collidere in trasmissione

- Per garantire corretto funzionamento di CSMA/CD
 - In funzione alla dimensione delle trame
 - In funzione alla velocità di trasmissione
- Mezzo trasmittivo 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 50Ω , Ø 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 50Ω , Ø 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:

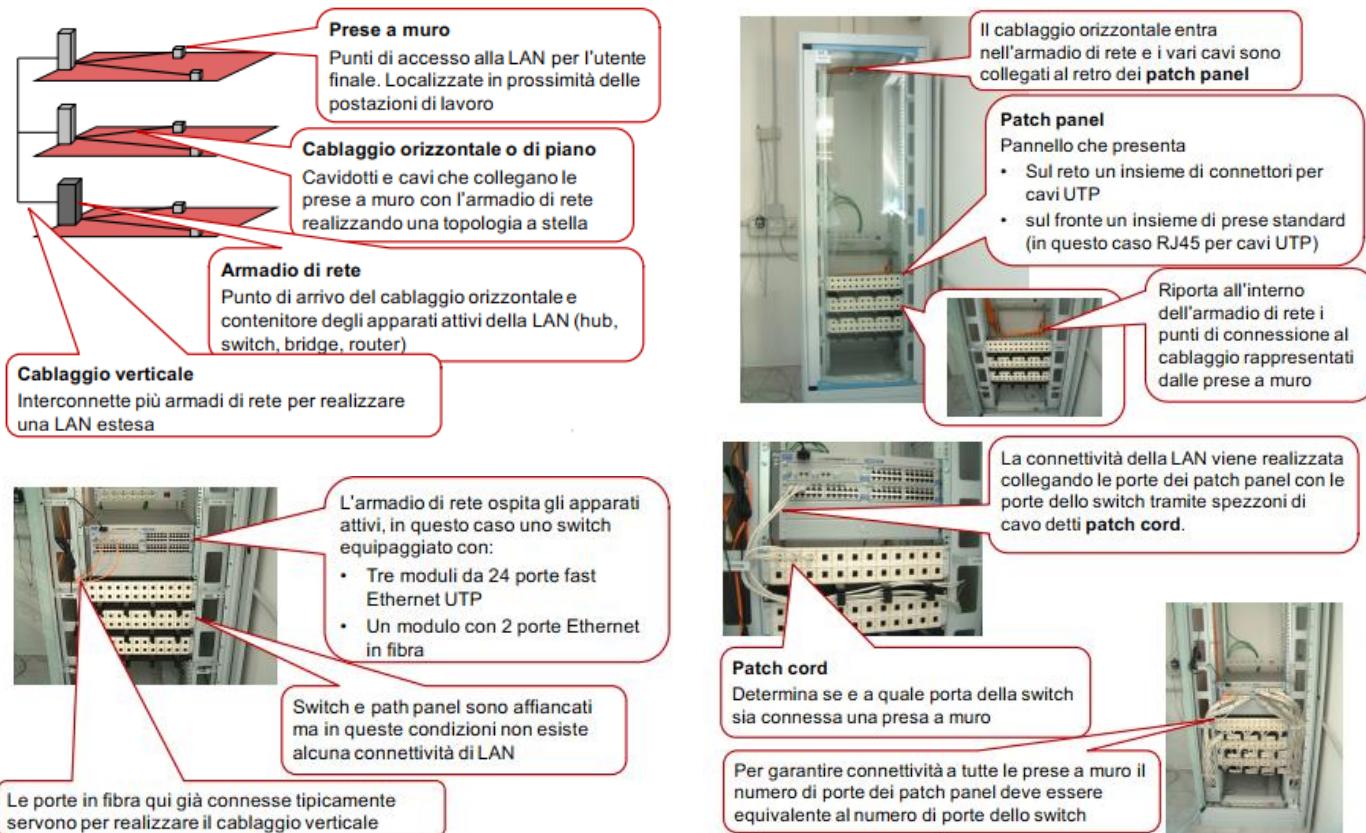
- Segnalazione e gestione
- Indirizzamento

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

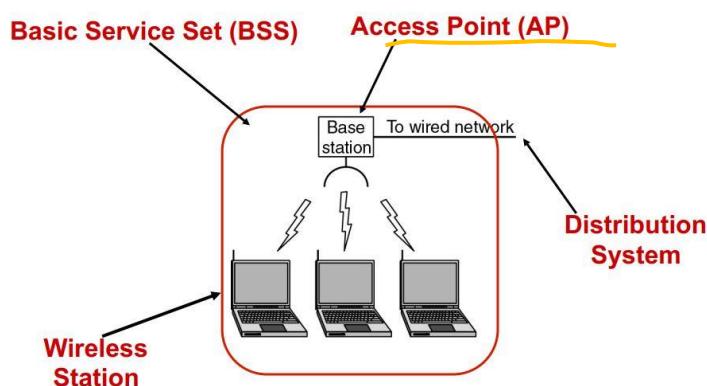
- High-rate DSSS

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



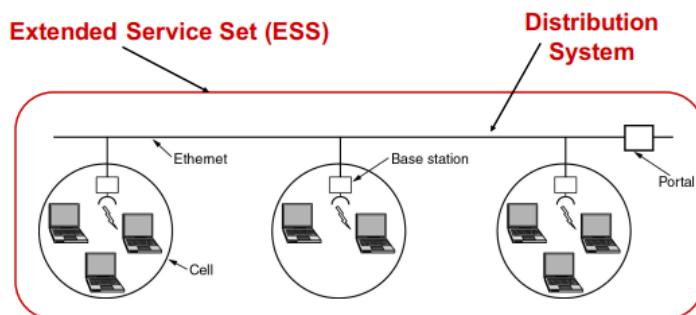
MODALITA' INFRASTRUTTURATA:

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

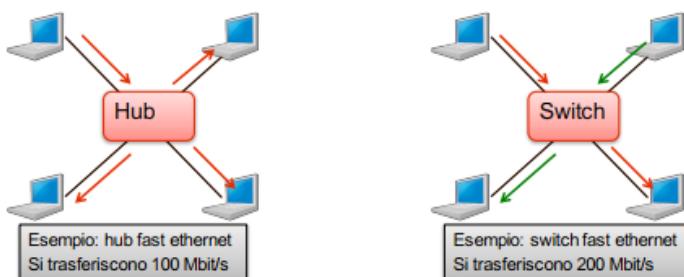
Strumenti di interconnessione di LAN

- **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 Interconnettere 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

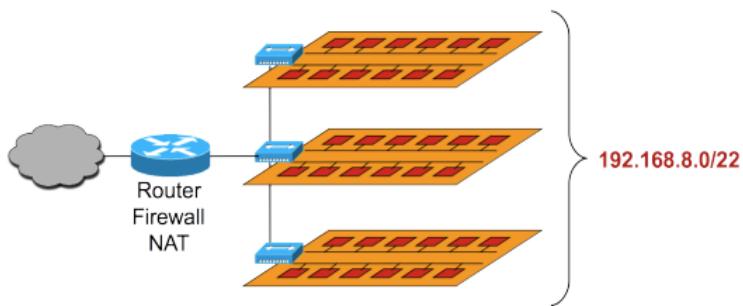
- Per ogni porta una sola stazione
- Uno Switch ethernet svolge una funzione simile all'hub, ma garantendo maggiori prestazioni
- Capacità aggregata superiore a quella della singola porta

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



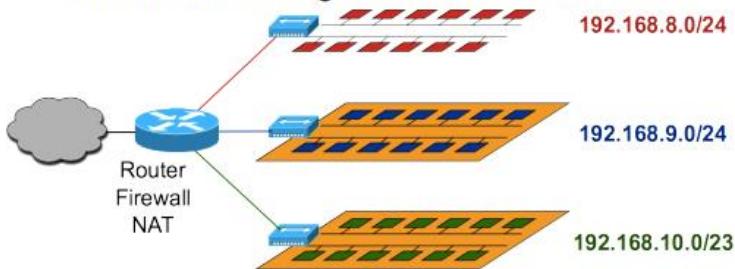
Interconnessione di LAN tramite switch

- 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

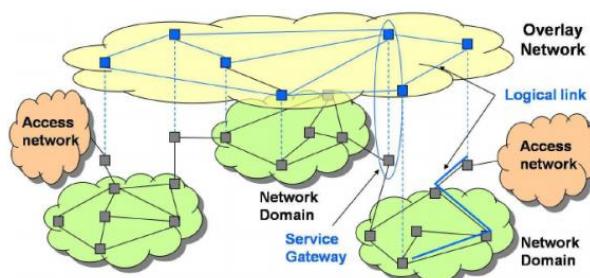
Virtualizzazione di rete

→ 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.

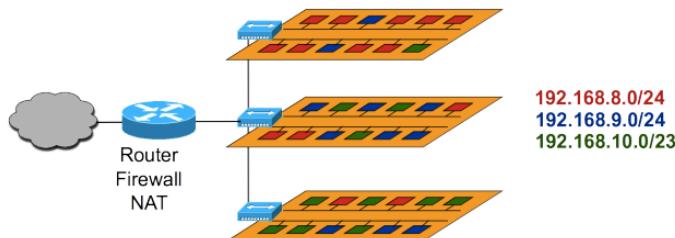
→ **obiettivo della virtualizzazione:** realizzare funzionalità/topologie diverse sull’infrastruttura.



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:

- STATICHE 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
- DINAMICHE
 - 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 switch
- Etichetta tag su intestazione Ethernet che identifica a quale VLAN appartiene il frame

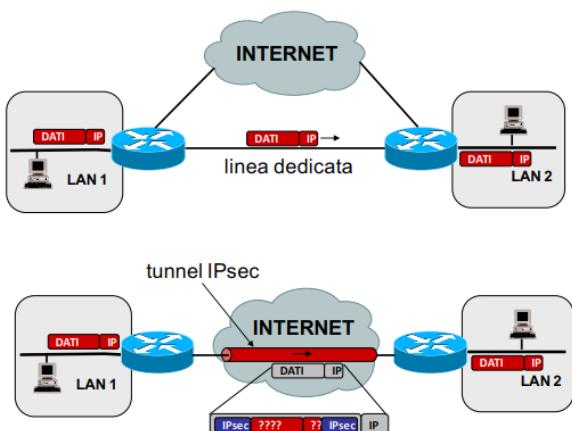
Inter-VLAN Routing

- In teoria un router dovrebbe avere un interfaccia dedicata per ciascuna VLAN
 - Ma è una soluzione inefficiente 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



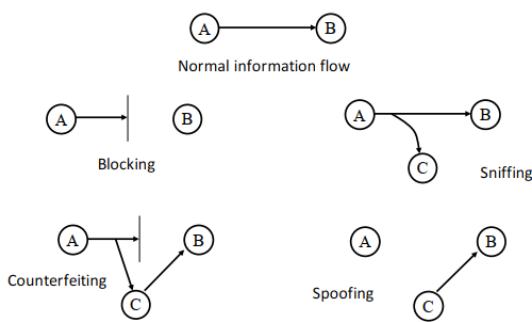
→ ci possono essere aziende di dimensioni medio/grandi che hanno necessità a connettere in maniera sicura sedi diverse e distanti tra loro

→ 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

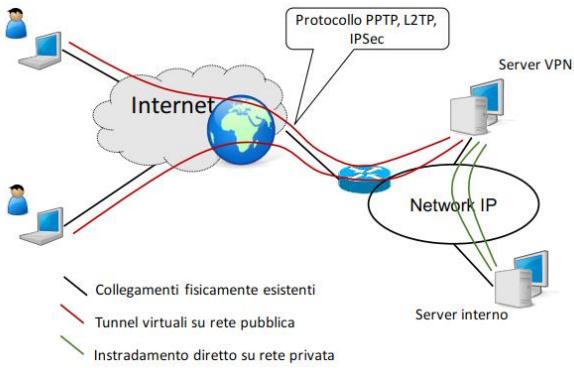
RISCHI della comunicazione remota



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

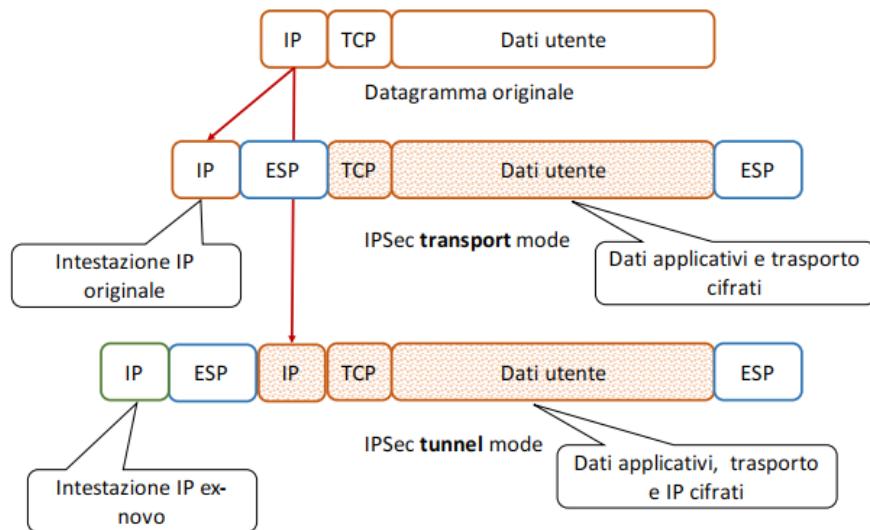
→ Security Association (SA) relazione unidirezionale tra mittente e destinatario definita da: SPI, IP destinazione, Security Protocol Identifier

→ due modalità di SA: Transport Mode e Tunnel Mode

Protocolli

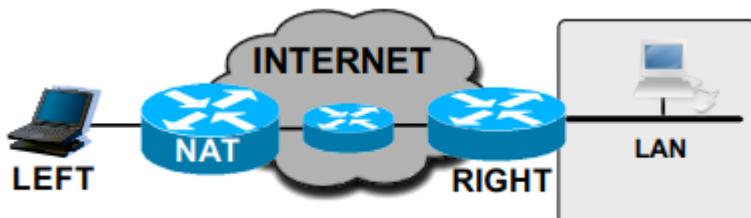
- IKE (Internet key Exchange): autenticazione dell'interlocutore e negoziazione tramite algoritmi e chiavi crittografiche.
 - Fase 1: negoziazione preliminare (uno dei server cerca di contattare l'altro e poi i due router si accordano sui parametri di sicurezza da usare in questa fase)
 - Fase 2: negoziazione 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.

Domanda aperta 1

Il “table lookup” è essenziale al corretto funzionamento di ogni nodo IP. Nell’ipotesi di considerare un moderno router che supporta il CIDR, spiegare:

1. Quale sia in termini generali lo scopo di tale funzione
2. Cosa si intende con i termini “tabella di instradamento” e “rotta/route”
3. Quali informazioni vengono utilizzate dal router IP per svolgere questa funzione e dove si trovano (tabella di instradamento o pacchetto IP)
4. Se vi sia un ordine preciso nell’uso delle informazioni presenti nella tabella di instradamento
5. Se sia possibile che l’operazione di table lookup non dia alcun risultato e, se si, cosa accada di conseguenza

Domanda aperta 2

Con riferimento all’applicazione PING spiegare:

1. A quale scopo viene usata
2. Quale protocollo viene utilizzato per la sua implementazione
3. Quali messaggi utilizza tale protocollo
4. Quali informazioni sia possibile ottenere eseguendo l’applicazione
5. Per quale motivo su molti sistemi server moderni tale applicazione sia disabilitata

Domanda aperta 3

Con riferimento all’applicazione TRACEROUTE spiegare

1. A quale scopo viene usata
2. Quale protocollo viene utilizzato per la sua implementazione
3. Quali messaggi utilizza tale protocollo
4. Se e quali campi dell’intestazione IP vengono utilizzati per il suo funzionamento
5. Quale sia il principio di tale funzionamento

Risposte domanda 1

1. È una funzione che permette di ricavare il prossimo hop nel percorso che deve fare il pacchetto per arrivare ad una certa destinazione facendo uso della tabella di instradamento
2. La tabella di instradamento è una base di dati dove vengono memorizzate le rotte in un certo nodo della rete, può essere aggiornata manualmente o attraverso dei protocolli di routing.

Le rotte sono le singole righe della tabella di instradamento e ha come campi:

- Ip destinazione
 - La netmask
 - Il gateway
 - L'interfaccia fisica
 - La metrica
3. Le informazioni che utilizziamo sono:
- Ip destinazione preso dalla tabella di instradamento
 - Netmask dalla tabella di instradamento
 - Ip destinazione preso dal pacchetto
4. Precisando che la tabella di instradamento è ordinata in modo crescente rispetto al numero di bit a 1 presenti nella netmask l'operazione di table lookup si esegue considerando a partire dalla fine della tabella
5. Questa eventualità può avvenire nel caso non vi sia una rotta di default nella tabella: verrà inviato un messaggio ICMP di errore

Risposte domanda 2

1. L'applicazione PING serve a verificare la raggiungibilità di una specifica destinazione
2. Si usa il protocollo ICMP
3. Usa i messaggi di informazione ICMP echo request e echo reply
4. Ottiene le seguenti informazioni
 - Il TTL
 - Il tempo per ogni pacchetto
 - Il tempo totale
 - La percentuale di pacchetti persi
5. È opportuno disabilitare il PING sui server perchè potrebbero essere vittima di attacchi in cui ricevono tantissimi ping e rimangono occupati a rispondere a questi invece che soddisfare le reali richieste (attacco DOS)

Risposte domanda 3

1. TRACEROUTE viene utilizzata per risalire al percorso che effettua un pacchetto per arrivare da una sorgente ad una destinazione
2. Si usa il protocollo ICMP
3. Utilizza il messaggio echo request e time exceeded
4. Si usa il campo Time-To-Live
5. Inizialmente invia un pacchetto ICMP di echo request con TTL = 1 in questo modo riceverà una risposta di time exceeded dal primo nodo sul percorso del pacchetto verso la destinazione, poi continua così aumentando progressivamente il valore del TTL in modo da ricevere un messaggio time exceeded anche da tutti gli altri nodi prima della destinazione

Domande primo capitolo

Un servizio di tipo broadcast

- Viene preferibilmente realizzato utilizzando canali punto-punto
- Se realizzato utilizzando un canale di tipo broadcast che “copre” una certa area geografica, permette la fruizione del servizio in mobilità nell’area
- Può essere realizzato con qualunque tipologia di canale, anche se risulta più efficiente utilizzare un canale broadcast
- Deve necessariamente essere realizzato con un canale punto-multipunto

2. Il primo cavo transatlantico telefonico

- Non so
- Fu realizzato verso la metà del XX secolo, dopo l’invenzione del transistor e l’avvento dell’elettronica allo stato solido
- Fu realizzato nei primi anni del XX secolo, in seguito al successo delle prime applicazioni del servizio telefonico
- Fu realizzato verso la fine del XIX secolo, insieme al primo cavo transatlantico telegrafico

3. Secondo il modello OSI le PCI

- Vengono aggiunte da tutti gli strati ai dati loro consegnati dagli strati immediatamente superiori
- Vengono aggiunte da tutti gli strati ai dati loro consegnati dagli strati immediatamente inferiori
- Vengono aggiunte solamente dallo strato di applicazione ai dati utente
- Non so

4. I sistemi cellulari

- Sono stati introdotti per effettuare trasmissioni dati via radio a grandi distanze
 - Sono stati introdotti per fornire accessi a Internet tramite la rete telefonica
- Non so
- Sono stati introdotti per consentire servizi conversazionali mediante un numero limitato di canali radio utilizzati più volte in aree diverse

5. Le reti cellulari sono state introdotte

- per effettuare trasmissioni dati via radio a grandi distanze
- per fornire accessi a Internet tramite la rete telefonica
- per fornire servizi di tipo telefonico mediante un numero limitato di canali radio riutilizzati più volte in aree diverse

6. Le reti di telecomunicazioni geografiche hanno tipicamente una struttura

- Di tipo gerarchico in cui si può riconoscere una rete di accesso tipicamente a stella ed una di transito con interconnessioni a maglia
- A stella con un solo centro stella per semplificare la gestione
- Non so

- A maglia completa per rendere massima l'affidabilità
- 2. Le grandi reti di telecomunicazioni geografiche hanno tipicamente una topologia
 - Di tipo gerarchico in cui si può riconoscere una rete di accesso tipicamente a stella ed una di transito con interconnessioni a maglia
 - Non so
 - di tipo a stella
 - di tipo gerarchico in cui si può distinguere una sezione cosiddetta di accesso tipicamente con topologia a maglia ed una sezione cosiddetta di trasporto con topologia a stella
- 2. Le grandi reti di telecomunicazioni geografiche hanno tipicamente una topologia
 - di tipo gerarchico in cui si può distinguere una sezione cosiddetta di accesso tipicamente con topologia a stella ed una sezione cosiddetta di trasporto con topologia a maglia
 - di tipo a stella
 - di tipo gerarchico in cui si può distinguere una sezione cosiddetta di accesso tipicamente con topologia a maglia ed una sezione cosiddetta di trasporto con topologia a stella
- 3. Le linee bifilari in rame di tipo UTP categoria 5
 - Sono utilizzate per la realizzazione di cablaggi strutturati negli edifici
 - Non so
 - Sono tipicamente utilizzate per la rete di accesso telefonica analogica
 - Sono tipicamente utilizzate per la rete di trasporto
- 4. Le linee bifilari in rame di tipo UTP categoria 5 sono tipicamente utilizzate
 - Per la realizzazione di cablaggi strutturati negli edifici
 - Per la rete di accesso telefonica analogica
 - Per la rete di trasporto
- 5. Le linee bifilari UTP
 - sono cavi non schermati
 - sono cavi schermati
 - sono cavi che possono essere sia schermati sia non schermati
- 6. Le linee bifilari intrecciate o doppini
 - Migliorano la loro qualità quando sono intrecciate con molta cura, diminuendo gli accoppiamenti elettromagnetici mutui
 - Sono particolarmente economiche e semplici da installare
 - Sono classificati in categoria in base alla qualità della loro realizzazione, secondo precisi standard internazionali
 - Nel corso del XX secolo sono state usate per realizzare la rete di accesso telefonica

7. I cavi coassiali
 - Sono stati progressivamente soppiantati dalle fibre ottiche
 - Sono mezzi trasmissivi con ottima immunità ai disturbi elettromagnetici, migliore rispetto ai doppini (Twisted Pairs)
 - Sono composti da due conduttori concentrici separati da un materiale isolante (ad esempio plastica)
 - Hanno in generale un costo per chilometro minore rispetto alle fibre
8. Le prime reti di calcolatori sviluppate negli anni '70
 - Non facevano uso di architetture a strati
 - Erano regolate da standard sviluppati in ambito ITU
 - Utilizzavano gli stessi protocolli dell'attuale rete Internet
 - Erano reti proprietarie chiuse sorte per lo più da iniziative dei grandi costruttori di calcolatori
9. Per garantire una qualità di servizio accettabile per servizi di comunicazione vocale fra umani una rete deve
 - Essere assolutamente ideale per quanto riguarda trasparenza semantica e temporale
 - Non so
 - Annullare il ritardo di propagazione
 - Privilegiare la garanzia di una buona trasparenza temporale

Domande secondo capitolo

Considerando l'efficienza di un protocollo ARQ a finestra scorrevole con dimensione della finestra pari ad 1, che trasmette trame di dimensione D, su un canale avente velocità $C=64$ kbit/s, ritardo di propagazione $I=0,1$ ms e probabilità di errore per bit $P_e=10^{-4}$, trascurando la dimensione delle PCI ($D=F$) e il tempo di elaborazione del ricevitore ($E=0$), si può dire che

- L'efficienza è tanto maggiore quanto è maggiore D
 - L'efficienza non ha mai valore superiore a 0,7
 - L'efficienza può raggiungere un valore superiore a 0,8 se la dimensione viene scelta in modo ottimale nell'interno degli 800 bit
 - Non so
2. Il controllo di flusso in un protocollo ARQ
 - Si realizza per effetto del fatto che il ricevitore, tramite l'invio delle conferme, determina il ritmo con cui vengono inviate le nuove trame
 - Non serve perchè il ricevitore ha sempre un grande buffer di ricezione
 - Funziona correttamente a patto che il ricevitore possa memorizzare un numero di trame pari alla dimensione della finestra
 3. L'efficienza di un protocollo ARQ di tipo stop-and-wait

- diminuisce al crescere del ritardo di propagazione trame
 - aumenta all'aumentare della capacità del canale
 - Aumenta al crescere delle PCI
4. La massima efficienza di un protocollo ARQ che trasporta trame di lunghezza $F=500$ byte di cui $H=10$ byte di intestazione
 - Risulta pari al 98% solo se la finestra viene correttamente dimensionata
 - Risulta pari al 98% qualunque sia la dimensione della finestra
 - Non so
 - Risulta pari al 95% qualunque sia il valore della finestra
5. Un protocollo ARQ a finestra scorrevole che trasmette, su di un collegamento di capacità C , trame di dimensione pari a F bit di cui D di dati utente e H di PCI
 - Ha sempre efficienza $D/(D+H)$
 - Ha efficienza $D/(D+H)$ solamente se il tempo di trasmissione di una finestra (WF/C) è superiore al tempo che intercorre fra l'inizio della trasmissione e la ricezione del primo ACK
 - Ha efficienza $D/(D+H)$ solamente se il tempo di trasmissione di una finestra (WF/C) è inferiore al tempo che intercorre fra l'inizio della trasmissione e la ricezione del primo ACK
 - Non so
6. Il codice a rivelazione d'errore detto "bit di parità"
 - Rivela solamente gli errori su due bit consecutivi
 - Rivela tutti gli errori su un numero dispari di bit
 - Non so
 - Rivela tutti gli errori su un numero pari di bit
7. In un protocollo di strato 2 in cui la rivelazione di errore viene effettuata usando il polinomio generatore x^2+1
 - I bit di ridondanza sono 3
 - Non so
 - I bit di ridondanza sono 2
 - I bit di ridondanza sono 4
8. Un codificatore polinomiale con polinomio generatore $G(x) = 1 + x$, deve codificare la sequenza 1100101011, il risultato è la sequenza
 - 11001010110
 - 11001010111
 - 110010101101
 - Non so
9. Nei più diffusi standard per i protocolli di livello 2 (o di linea), nelle attuali reti di telecomunicazioni quali la rete Internet:

- Si utilizzano tipicamente codici a rivelazione di errore
- Non so
- Non si usano mai codici per la gestione dell'errore
- Si utilizzano tipicamente codici a correzione di errore

10. Quali di questi sono compiti tipici dello strato di linea (DL layer)

- Rivelazione di errore
- Controllo di flusso
- Sincronizzazione del flusso di bit sul canale

11. L'internet checksum

- Viene calcolato suddividendo i dati in parole di 32 bit
- Utilizza l'operazione di somma binaria modulo 1
- Viene utilizzato nei vari protocolli della rete Interne dove necessario

2. L'internet checksum

- viene calcolato suddividendo i dati in parole di 32 bit
- utilizza l'operazione di somma binaria complemento a 1
- viene utilizzato nei vari protocolli della rete Internet quando sia necessario controllare l'errore di trasmissione

Domande terzo capitolo

Un router riceve un datagramma IP di 1100 byte, di cui 20 di header, con FRAGMENT OFFSET = 3000 e che deve essere inviato su di una rete che accetta datagrammi di lunghezza massima pari a 400 byte

- Se il flag DON'T FRAGMENT vale 1 non invia il datagramma e ritorna un errore all'host sorgente
- Se il flag DON'T FRAGMENT vale 0 frammenta il datagramma in 3 parti con FRAGMENT OFFSET rispettivamente 3000, 3380, 3760
- Se il flag DON'T FRAGMENT vale 0 frammenta il contenuto del datagramma in 3 parti di 380, 380 e 320 byte che verranno inviati in altrettanti datagrammi

3. L'applicazione Traceroute

- Utilizza il campo TTL del datagramma IP ed i messaggi di errore ICMP per svolgere le sue funzioni
- Serve per comprendere quale sia il percorso seguito da un datagramma fra una sorgente ed una destinazione
- Permette di verificare l'efficienza dei protocolli e degli algoritmi di routing

4. Nell'intestazione (header) del datagramma IP il campo Versione

- Occupa 1 byte
- Occupa 4 bit
- È un campo opzionale

2. Nell'intestazione (header) del datagramma IP
 - Occupa 1 byte
 - E' presente un campo per il numero di datagramma inviato ed uno per il numero di datagramma ricevuto
 - Occupa 4 bit
 - Sono presenti due indirizzi di lunghezza fissa per sorgente e destinazione
 - È un campo opzionale
 - E' presente un campo per la conferma della ricezione di altri datagrammi (acknowledge).
3. Un host appartenente ad una rete connessa ad Internet tramite un NAT ha attribuito all'interfaccia di rete l'indirizzo 192.168.0.1 ed ha attiva una connessione sulla porta TCP 51321
 - Nei datagrammi che riceve da trasmettere su Internet per la connessione il NAT deve necessariamente modificare il numero IP sorgente e, in funzione del tipo di configurazione e delle connessioni esistenti, potrebbe modificare il numero di porta sorgente
 - Dal NAT verso la rete Internet non vengono mai trasmessi datagrammi con porta sorgente 51321
 - Dal NAT verso la rete Internet vengono trasmessi datagrammi con IP sorgente 192.168.0.1
4. Un datagramma con il flag DON'T FRAGMENT = 1
 - qualora dovesse essere frammentato, viene scartato producendo un messaggio di errore
 - viene frammentato solo se necessario
 - Non so
 - Verrà sempre consegnato senza essere frammentato
2. Un datagramma con il flag DON'T FRAGMENT = 0
 - viene frammentato solo se necessario
 - verrà sempre consegnato senza essere frammentato
 - viene frammentato solo se necessario
3. Il Dipartimento di un ente ottiene per l'indirizzamento IP la rete 137.204.57.128/27.
Ne consegue che
 - Non può utilizzare per l'interfaccia di un host l'indirizzo IP 137.204.57.159 ○
Potrebbe scegliere come indirizzo IP del gateway di default il numero 137.204.57.129
 - La netmask dei relativi host va configurata al valore 255.255.255.224
2. Il Dipartimento di un ente ottiene per l'indirizzamento IP la rete 137.204.57.128/26.
Ne consegue che
 - potrebbe scegliere come indirizzo IP del gateway di default il numero 137.204.57.129

- la netmask dei relativi host va configurata al valore 255.255.255.224
 - non puo' utilizzare per l'interfaccia di un host l'indirizzo IP 137.204.57.159
3. Il messaggio DHCPACK
- Non so
 - Viene inviato dal client DHCP e termina la fase di configurazione dell'interfaccia IP del client
 - Viene inviato dal server DHCP e termina la fase di configurazione dell'interfaccia IP del client
 - Viene inviato dal client DHCP e serve a identificare a quale server si chiede la configurazione dell'interfaccia IP
4. Nell'intestazione (header) del datagramma IP il campo Time to live
- Cresce ad ogni nodo (hop) attraversato dal pacchetto
 - Permette di attribuire un maggior tempo di vita ai pacchetti a priorita' più' alta
 - Limita il tempo di permanenza di un pacchetto in Internet
5. Un router riceve un datagramma IP di 1500 byte con FRAGMENT OFFSET = 0. IL datagramma deve essere inviato su di una rete che accetta datagrammi di lunghezza massima pari a 512 byte. Ne consegue che:
- Se il campo FRAGMENT OFFSET vale 0 frammenta il datagramma in 3 parti con FRAGMENT OFFSET rispettivamente 0, 64, 128
 - Se il flag DON'T FRAGMENT vale 1, il router non invia il datagramma e ritorna un messaggio di errore all'host sorgente
 - Se il campo FRAGMENT OFFSET vale 0 frammenta il datagramma in 2 parti con FRAGMENT OFFSET rispettivamente 0, 512
6. Il messaggio ICMP di errore "Time exceeded" può indicare che
- L'attesa dei frammenti per riassemblare un datagramma si è protratta troppo a lungo, oltre un valore limite prefissato
 - Il Time-To-Live di un datagramma si è azzerato ed il datagramma viene distrutto
 - Il tempo necessario ad instradare il datagramma ha superato un valore limite prefissato
 - Il datagramma è rimasto memorizzato in un router senza essere instradato per un tempo che ha superato un valore limite prefissato
7. Applicare la netmask 255.255.255.224 alla rete ip 192.168.1.0 significa
- Suddividere la rete in 3 sottoreti
 - Che l'indirizzo IP 192.168.1.31 è indirizzo di broadcast per una subnet
 - Suddividere la rete in 8 sottoreti
8. Un datagramma viene inviato con TTL=1 nell'intestazione
- Verrà instradato dal primo router che incontra
 - Verrà bloccato nel primo router che incontra generando un messaggio ICMP di errore

- Potrebbe essere generato dall'applicazione TRACEROUTE**
9. Quale fra i seguenti è un indirizzo valido per un host in una rete IP con numerazione privata?
- 0.1.220.198
 - 137.256.121.0
 - 192.168.1.1**
10. Il messaggio DHCPDISCOVER
- Viene inviato da un client che deve configurare la propria interfaccia di rete in modalità broadcast sulla LAN**
 - Viene inviato in modalità broadcast da un server DHCP per scoprire se vi sono altri server DHCP attivi sulla LAN
 - Viene inviato da un client che deve configurare la propria interfaccia di rete all'indirizzo mac del server DHCP, come configurato dall'utente
11. L'indirizzo IP 190.240.20.254
- Non so
 - È un indirizzo privato di classe C
 - È un indirizzo di classe B**
 - È un indirizzo pubblico di classe C
12. Nell'intestazione (header) del datagramma IP il campo MORE FRAGMENTS (MF)
- Occupa 1 byte
 - Se vale 1 allora indica che il datagramma presente è l'ultimo frammento di un datagramma di maggiori dimensioni che è stato frammentato lungo il percorso in rete
 - Occupava 1 bit**
13. Con il termine "Direct Forwarding" si intende
- La capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router**
 - La capacità di un host di inviare datagrammi che i router tratteranno in modo prioritario
 - La capacità di un host di consegnare datagrammi interagendo direttamente con un gateway
14. La modalità di instradamento dei datagrammi nella rete Internet
- Viene fatta sulla base dell'indirizzo IP di sorgente
 - Garantisce che tutti i datagrammi di una medesima connessione seguano il medesimo percorso
 - Viene fatta sulla base dell'indirizzo IP di destinazione**
15. Nell'intestazione (header) del datagramma IP è presente il campo IDENTIFICATION, che contiene un numero che identifica il datagramma, quale delle seguenti affermazioni sono vere al riguardo
- Occupava 2 byte**

- Serve per consentire la eventuale frammentazione e riassemblaggio dei datagrammi
- Serve per consentire di fornire gli acknowledgement dei datagrammi

16. Un host connesso in rete utilizzando il protocollo IP

- Deve avere solamente un'interfaccia di rete ed il relativo numero IP
- Può avere più interfacce di rete assegnando a tutte il medesimo numero IP
- Può avere una o più interfacce e ad ognuna deve essere assegnato un numero IP

17. Il protocollo ARP

- Viene utilizzato solamente per raggiungere il router di default
- Viene utilizzato ogni volta che si deve inviare un datagramma ad un host il cui indirizzo IP non compare nella tabella ARP
- Viene utilizzato solamente quando si debbano inviare datagrammi ad host raggiungibili tramite instradamento diretto

18. Nell'intestazione (header) del datagramma IP il campo Header Checksum

- Deve essere ricalcolato ad ogni hop, ossia ogni volta che il datagramma attraversa un router
- Verifica la correttezza della sola intestazione del pacchetto e pertanto viene calcolato sui soli byte delle PCI del datagramma
- Verifica la correttezza del pacchetto

19. L'interfaccia di rete di un host ha configurato il numero IP a 192.168.20.12 e d il parametro NETMASK al valore 255.255.255.224, ne consegue che

- L'indirizzo della rete a cui appartiene l'host è 192.168.20.0
- La network IP può contenere al più 30 host (oppure 29 host ed il gateway)
- La network IP a cui appartiene l'host utilizza 5 bit per indirizzare i singoli host

2. Il numero IP 224.0.0.9

- è un indirizzo multicast, utile per inviare un datagramma a più host contemporaneamente
 - è utilizzato dal RIP versione 2 per inviare i distance vector
- è utilizzato da OSPF per inviare i pacchetti link state

3. La consegna di un datagramma con instradamento indiretto

- Non avviene se i due host appartengono alla medesima network IP
- Implica il coinvolgimento di almeno un router
- Richiede l'invio di un messaggio di ARP Request all'host di destinazione

2. La consegna di un datagramma con instradamento diretto

- avviene se i due host appartengono alla medesima network IP
- implica il coinvolgimento di almeno un router

- richiede sempre l'invio di un messaggio di ARP Request all'host di destinazione
3. Nell'intestazione (header) del datagramma IP il campo FRAGMENT OFFSET
- Indica la lunghezza del frammento in byte
 - Indica la distanza del frammento dall'inizio del datagramma in parole di 32 bit
 - Indica la distanza del frammento dall'inizio del datagramma in gruppi di 8 byte
4. I messaggi del protocollo ICMP
- Vengono trasportati utilizzando una connessione TCP
 - Vengono incapsulati direttamente nella trama Ethernet
 - Vengono trasportati direttamente su IP senza utilizzare un protocollo di trasporto
5. Nell'elaborazione del routing table lookup
- Si fa uso del campo IP DESTINATION nonché del contenuto dei campi NETMASK e DESTINATION delle tabelle di instradamento
 - Si fa uso esclusivamente delle informazioni del campo IP DESTINATION ○ Si fa uso esclusivamente delle informazioni del campo IP SOURCE
6. La tabella ARP in un host
- Viene aggiornata dal DNS
 - Viene configurata all'attivazione dell'host e non può essere modificata ○ Contiene corrispondenza fra numeri IP e indirizzi MAC
7. Un router riceve un datagramma IP di 1500 byte con FRAME OFFSET = 0. Il datagramma deve essere inviato su di una rete che accetta datagrammi di lunghezza massima pari a 512 byte. Ne consegue che:
- Se il flag DON'T FRAGMENT vale 1, il router non invia il datagramma e ritorna un messaggio di errore all'host sorgente
 - Se il campo FRAGMENT OFFSET vale 0, frammenta il datagramma in 2 parti con FRAGMENT OFFSET rispettivamente 0 e 512
 - Se il campo FRAGMENT OFFSET vale 0, frammenta il datagramma in 3 parti con FRAGMENT OFFSET rispettivamente 0, 64 e 128
8. Il comando PING
- Serve per controllare se un host IP è raggiungibile su internet
 - Serve per misurare le dimensioni di una rete
 - Serve per riconoscere il percorso fra una rete e l'altra
9. Per il corretto funzionamento dell'interfaccia di rete di un host vanno configurati almeno i seguenti parametri
- Numero IP, Netmask e default gateway
 - Numero IP e default gateway

- Numero IP e Netmask

10. Nell'intestazione (header) del datagramma IP

- Sono presenti due indirizzi di lunghezza fissa per sorgente e destinazione ○
È presente un campo per la conferma della ricezione di altri datagrammi (acknowledge)
- È presente un campo per il numero di datagramma inviato ed uno per il numero di datagramma ricevuto

11. Una rete IP di classe C

- Usa 3 byte per l'indirizzo della rete e 1 byte per l'indirizzo dell'Host
- Ha un indirizzo il cui primo byte comincia con 101
- Non può essere divisa in sottoreti (subnet)

12. La completa configurazione dell'interfaccia IP di un host richiede di specificare

- Numero IP, Netmask, default gateway e server DNS
- Numero IP e default gateway
- Numero IP e server DNS

Domande quarto capitolo

1. L'algoritmo di Dijkstra

- Permette di ricavare i percorsi di lunghezza minima fra una qualunque coppia di nodi
- Permette di ricavare la topologia della rete
- Richiede la conoscenza della topologia della rete

2. Il concetto di distanza nel routing in Internet

- Può essere un qualunque valore numerico il cui significato viene convenzionalmente definito
- È un valore numerico generato casualmente
- Deve necessariamente essere pari a 1 per ogni collegamento fra router
- Non so

3. Qualora si utilizzi in una rete un protocollo di routing di tipo flooding

- Tutte le possibili destinazioni vengono sicuramente raggiunte
- Ciascun nodo di commutazione deve assolutamente ritrasmettere un pacchetto sul collegamento da cui l'ha ricevuto
- Si ottiene il corretto instradamento dei pacchetti con l'utilizzazione minima possibile delle risorse di rete

4. I protocolli della famiglia Link State

- Non so

- Sono protocolli dinamici
 - Prevedono che ogni router trasmetta ai propri vicini la propria distanza da tutti i nodi della rete
 - Prevedono che ogni router trasmetta a tutti i nodi della rete la distanza dai propri vicini
 - Richiedono che ogni router conosca a priori la distanza dai suoi vicini
- 5. Per l'organizzazione di Internet un Autonomous System
 - Non so
 - È l'unità fondamentale in cui sono suddivisi i domini dei nomi degli host
 - È un dominio di routing che comunica con l'esterno utilizzando un Exterior Gateway Protocol quale il BGP
 - Deve contenere network IP tutte delle stessa classe
- 6. Quali di questi campi sono contenuti nei pacchetti di tipo Link State prodotti dal protocollo OSPF
 - Indirizzo del destinatario
 - Numero di sequenza
 - Indirizzo del mittente
 - Età del pacchetto
- 7. I protocolli di routing
 - Servono per creare e manutenere le tabelle di routing nei nodi
 - Logicamente sono protocolli di livello applicativo che fanno parte del piano di controllo della rete
 - Nella rete Internet vengono impiegati solamente all'interno degli Autonomous System
- 8. I messaggi del protocollo OSPF
 - Hanno tutti un'intestazione comune, seguita da informazioni specifiche che dipendono dal tipo di pacchetto
 - Vengono utilizzati per l'implementazione del protocollo di HELLO che permette ai router di scoprire i propri vicini
 - sono di due soli tipi REQUEST e RESPONSE
- 9. Il messaggio RESPONSE nel RIPv2 contiene nelle PCI un campo VERSION che ha lunghezza
 - 8 bit
 - 4 bit
 - 16 bit
- 10. Un messaggio RIPv2 di tipo RESPONSE
 - può prevedere dati di autenticazione del router che lo ha inviato
 - è riconoscibile perché nella prima parola di 32 bit delle PCI contiene il numero della versione del protocollo

- trasporta gli elementi del Distance Vector come insiemi di parole di 20 byte

11. Il protocollo OSPF

- È un protocollo Distance Vector
- Viene usato come Interior Gateway Protocol
- Viene usato come Exterior Gateway Protocol

12. Il protocollo BGP

- È un protocollo di tipo Path Vector
- Garantisce l'assenza di cicli nella determinazione delle rotte
- È usato come Interior Gateway Protocol

13. I protocolli della famiglia Distance Vector

- Richiedono che ogni router conosca a priori la distanza dai suoi vicini
- Sono protocolli statici
- Prevedono che ogni router trasmetta ai propri vicini la propria distanza da tutti i nodi della rete
- Prevedono che ogni router trasmetta a tutti i nodi della rete la propria distanza dai vicini
- Non so

14. Quali fra i protocolli elencati in seguito sono protocolli di Routing utilizzati in Internet?

- RIP
- BGP
- TCP

15. Quali fra i protocolli elencati in seguito sono protocolli di Routing utilizzati in Internet?

- UMTS
- RIP
- TCP

16. Quali delle seguenti descrizioni può essere ritenuta corretta per le funzioni delle tabelle di routing utilizzate nei nodi a commutazione di pacchetto

- Associare ad ogni indirizzo di destinazione una porta d'uscita
- Associare ad un identificativo di circuito virtuale una porta di ingresso e una di uscita
- Associare ad ogni indirizzo di destinazione e ad ogni porta di uscita un costo convenzionalmente definito
- Associare ad ogni indirizzo di sorgente e destinazione un costo convenzionalmente definito

17. Quali delle seguenti affermazioni puo' essere ritenuta corretta per le funzioni delle tabelle di instradamento utilizzate nei nodi a commutazione di pacchetto tipici di Internet (router IP)

- Associare ad ogni indirizzo di destinazione uno specifico gateway ed una porta di uscita del nodo

- Associare ad un indirizzo di destinazione e alla relativa porta di ingresso un costo convenzionalmente definito
- Associare ad uno specifico indirizzo di destinazione una porta di ingresso ed una di uscita del nodo

18. Il flooding

- Non riesce in generale a trovare la strada più breve da una sorgente verso una specifica destinazione
- È il modo più semplice per spedire un pacchetto a tutti gli host di una rete
- Viene usato come algoritmo ausiliario in alcuni protocolli di routing standardizzati da IETF

19. Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si può dire che

- I distance vector si adattano più velocemente ai cambiamenti della rete
- I distance vector richiedono maggior potenza di elaborazione
- I link state richiedono più memoria del router

20. Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si può dire che

- Le due tipologie sono sostanzialmente equivalenti qualunque sia la topologia e la dimensione della rete considerata
- In generale i protocolli DV garantiscono un funzionamento migliore di quelli LS
- In generale i protocolli LS garantiscono un funzionamento migliore di quelli DV

21. Un algoritmo di routing si dice statico quando

- Il router costruisce la tabella di routing sulla base delle informazioni che può ottenere misurando le proprie code di uscita
- Associa ogni specifico ingresso ad una particolare uscita in modo fisso e non modificabile
- Non permette l'aggiornamento delle tabelle di routing da parte dell'operatore
- Il router fa uso di una tabella di routing definita a priori in fase di configurazione

22. Il routing nella rete Internet

- Non so
- Viene implementato in modo dinamico e distribuito da tutti i nodi di rete utilizzando un unico algoritmo senza scambio di informazioni
- Viene implementato in modo statico da un nodo speciale che calcola le tabelle di instradamento per tutti gli altri nodi della rete
- Viene implementato in modo dinamico e distribuito da tutti i nodi della rete, utilizzando sia scambio di informazioni sia opportuni algoritmi, secondo diverse modalità per diverse sezioni della rete

23. I termini protocollo e algoritmo di instradamento

- Indicano rispettivamente i metodi di scambio delle informazioni sulla topologia della rete e di calcolo delle tabelle di instradamento
- Indicano rispettivamente i metodi di calcolo delle tabelle di instradamento e di scambio delle informazioni sulla topologia della rete
- Sono equivalenti

1. Quali di questi protocolli di Routing sono stati usati in Internet

- Hot potato
- QPSX
- BGP

Domande quinto capitolo

1. In un collegamento IPSec tunnel mode
 - Viene cifrato sia il contenuto sia l'intestazione dei datagrammi IP
 - Viene cifrata solamente l'intestazione dei datagrammi IP
 - Viene cifrato solamente il contenuto dei datagrammi IP
 - Non so
2. In base all'evoluzione dei sistemi di cablaggio, una rete LAN in un edificio aziendale si può dire che tipicamente è realizzata con
 - Cablaggio interamente in fibra ottica
 - Cablaggio orizzontale di piano in fibra ottica e interconnessione fra piani in cavo UTP
 - Cablaggio orizzontale di piano con cavo UTP e interconnessione fra piani con cavo UTP o fibra ottica
 - Non so
3. Un'azienda ha quattro reti LAN in quattro capannoni contigui, realizzate con quattro switch Ethernet, uno per capannone. Si vuole interconnettere le LAN realizzando un'unica rete che corrisponderà ad un'unica network IP
 - Non so
 - È necessario connettere i quattro switch delle LAN tramite un router
 - È preferibile connettere i quattro switch delle LAN tramite uno switch
 - È preferibile connettere i quattro switch delle LAN ad un solo HUB
4. Uno switch risulta più efficiente rispetto ad un hub poiché invia le trame solamente sulla porta a cui è effettivamente connesso il calcolatore a cui sono destinate (in base all'indirizzamento MAC). Questo è possibile perché
 - il gestore di rete configura a priori una tabella nello switch che associa a ciascuna porta un ben preciso indirizzo MAC di destinazione
 - utilizzando il protocollo ARP può apprendere in autonomia i MAC dei calcolatori connessi alla varie interfacce
 - lo switch impara mano a mano che riceve le prime trame quali sono gli indirizzi MAC dei calcolatori collegati sulle varie porte grazie alla presenza del Mac sorgente nelle PCI della trama
5. Secondo la terminologia dello standard IEEE 802.11 un BSS è
 - Un'area dove viene implementata una rete ad hoc se si parla di Independent BSS
 - Un'area in cui una serie di stazioni mobili possono colloquiare grazie ad un access point se si parla di Infrastructured BSS
 - Un'area dove più access point mettono in comunicazione stazioni nascoste le une dalle altre
6. Si dice bridge
 - Non so

- Un dispositivo per l'interconnessione di reti locali operante a livello 3
- Un dispositivo per l'interconnessione di reti locali operante a livello 1
- **Un dispositivo per l'interconnessione di reti locali operante a livello 2**

7. Secondo la terminologia Wi-Fi un ESS

- È un sistema di più access point funzionanti come un'unica LAN
- È una particolare tipologia di stazione wireless con caratteristiche estese rispetto alle altre della LAN
- È la stazione base di una LAN infrastrutturata
- Non so

8. In una LAN wireless del tipo IEEE 802.11 (Wi-Fi) il canale radio

- Viene suddiviso in due canali a diverse frequenze, uno dei canali è usato dalla stazione base (downlink) e l'altro dalle stazioni di utente (uplink)
- Viene completamente utilizzato dalla stazione base o dalle stazioni di utente in modo alternativo (TDMA)
- Viene completamente utilizzato dalla stazione base o dalle stazioni di utente con un sistema di multiplazione a divisione di codice (CDMA)

9. Stazioni ethernet che appartengono al medesimo dominio di collisione

- Sono tipicamente collegate tramite uno switch
- Sono tipicamente collegate tramite un hub
- Se trasmettono contemporaneamente danno luogo a collisione

1. Una LAN in cui tutti i calcolatori appartengono al medesimo dominio di collisione:

- e' tipicamente implementata con un apparato di tipo SWITCH
- **e' tipicamente implementata con un apparato di tipo HUB**
- e' tipicamente implementata con un apparato di tipo ROUTER

1. Su una certa LAN si possono rendere disponibili:

- uno ed un solo server DHCP
- **un numero qualunque di server DHCP**
- al piu' due server DHCP

2. Il dispositivo denominato HUB

- È ormai in disuso in quanto fornisce prestazioni inferiori rispetto agli switch
- Può essere utile se si vuole monitorare il traffico sulla LAN
- Separa i domini di collisione in una LAN ethernet

3. Un protocollo di accesso si definisce a contesa quando la procedura di accesso

- È assente poiché i calcolatori della LAN possono sempre inviare le proprie trame senza collisione
- Non so

- È distribuita e garantisce l'assenza di collisioni
 - È distribuita e non garantisce l'assenza di collisioni
- 4. Una rete Ethernet 1000baseT
 - Prevede una velocità di trasmissione pari a 1 Gbit/s
 - Prevede come mezzo trasmissivo il doppino incrociato non schermato (UTP) di categoria 5E o superiore
 - Prevede come mezzo trasmissivo la fibra ottica monomodale
- 5. Quali fra questi campi sono contenuti nella trama MAC dello standard IEEE 802.3
 - Padding
 - Starting delimiter
 - Access control
- 6. Secondo gli standard IEEE 802 gli indirizzi MAC sono tali che
 - Sono associati in modo univoco alle schede di rete
 - Sono associati in modo univoco ai singoli host della rete locale a prescindere dal numero di interfacce di rete con cui sono equipaggiati ○ Permettono di individuare il costruttore delle schede
- 7. Fra i mezzi trasmissivi usati nelle reti in area locale (LAN) ci sono
 - Copie bifilari avvitate (Twisted pairs)
 - Canale radio ○ Fibre ottiche
- 8. Un ethernet switch a 4 porte 100baseT
 - Fornisce prestazioni superiori rispetto ad un hub
 - Redirige i pacchetti sulle uscite in base all'indirizzo MAC destinazione
 - Crea un unico dominio di collisione fra tutti i calcolatori ad esso collegati
- 9. Con il nome di rete ethernet si indica una tecnologia che corrisponde a
 - Non so
 - Uno standard della ISO
 - Uno standard della IEEE
 - Uno standard della ITU
- 10. Le dimensioni di una LAN sono tipicamente
 - Dell'ordine del metro
 - Dell'ordine dei chilometri
 - Dell'ordine delle centinaia di metri
 - Non so
- 11. Il progetto IEEE 802

- Definisce tutti gli standard che sono necessari per far funzionare una rete locale di calcolatori
 - Ha definito un'architettura originale per le reti locali incompatibile con il modello OSI
 - Definisce, per le reti locali di calcolatori, gli standard relativi ai mezzi trasmissivi e agli strati 1 e 2 del modello OSI
 - Non so
- 12. In una LAN IEEE 802.11 implementata con più Access Point operanti con WDS la trama diretta all'access point a cui è connessa la stazione di destinazione
 - Ha come primo indirizzo MAC quello dell'access point di destinazione
 - Ha come primo indirizzo MAC quello dell'access point di provenienza
 - Ha come quarto indirizzo MAC quello dell'access point di provenienza
 - Non so
- 13. In una VPN funzionante in modalità roadwarrior un utente della VPN
 - Non so
 - Può collegarsi alla VPN solamente dall'interno della rete aziendale
 - Può collegarsi alla VPN da un qualunque punto di internet tramite un'opportuna procedura di autenticazione (username e password tipicamente)
 - Necessita di un router specifico per poter raggiungere la VPN
- 14. Una rete 802.11 infrastrutturata
 - Prevede che le stazioni comunichino fra loro direttamente ed una stazione venga designata a fare da ripetitore del segnale fra le stazioni eventualmente nascoste
 - Prevede che le stazioni comunichino fra loro direttamente
 - Non so
 - Prevede che le stazioni comunichino fra loro tramite una stazione base che riceve il segnale su un canale di uplink e lo ripete su un canale di downlink

Aggiunte da me

1. Su uno switch a 8 porte configuro due VLAN. La VLAN 1 sulle porte 1, 2, 3, 7 e la VLAN 2 sulle porte 4, 5, 6, 8. Cio' significa che
 - Un calcolatore connesso alla porta 1 non puo' comunicare con un calcolatore connesso alla porta 7 a meno che non utilizzi ulteriori apparati
 - Un calcolatore connesso alla porta 1 puo' comunicare con un calcolatore connesso alla porta 2 senza la necessità di ulteriori apparati
 - Un calcolatore connesso alla porta 1 non puo' comunicare con un calcolatore connesso alla porta 4 a meno che non utilizzi ulteriori apparati

2. In un LAN implementata secondo le moderne tecnologie di cablaggio qual è il ruolo dei patch cord
 - Collegare i punti di arrivo delle prese a muro nei patch panel con le corrette porte degli apparati attivi presenti nell'armadio di rete
 - Collegare le prese a muro con l'armadio di rete
 - Collegare tra loro gli apparati attivi in diversi armadi realizzando il cablaggio verticale
3. Nella terminologia OSPF un ABR e'
 - Un router che annuncia verso il resto dell'AS gli indirizzi IP delle reti facenti parte della propria area
 - Un router che ha almeno un'interfaccia connessa alla propria area ed un'interfaccia connessa all'area di backbone o ad un'altra area
 - Un router che interconnette fra loro tutte le aree dell'AS
4. Il protocollo BGP viene utilizzato per gestire il routing fra gli AS. Viene detto di tipo path vector. Questo significa che
 - I router quando vedono un'informazione di router in cui compare il loro AS la ignorano onde evitare cicli
 - I messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la lista degli AS che vanno attraversati per raggiungerli
 - I messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la distanza da tutti gli AS noti
5. Quali sono le principali differenze fra RIP versione 1 e versione 2:
 - Il RIP v2 supporta l'autenticazione dei router mentre il RIP v1 no
 - Il RIP v2 supporta il CIDR mentre il RIP v1 interpreta gli indirizzi IP solamente con la logica classfull
 - Nessuna; i due protocolli sono identici
6. Il protocollo RIP esiste in due versioni, la versione 1 (o v1) e la versione 2 (v2). Paragonando le due versioni quali delle seguenti affermazioni sono vere:
 - il RIP v2 permette l'autenticazione dei messaggi di Response, mentre il RIP v1 no
 - il RIP v2 prevede un formato dei messaggi completamente diverso da quello del RIP v1 senza alcuna parte in comune
 - il RIP V1 permette di comunicare anche la destinazione di reti IP conformi al CIDR mentre il RIP v2 no
7. Tra due router viene configurata la rete 10.0.0.4/30. Ne consegue che Scegli un'alternativa:
 - I router avranno indirizzi 10.0.0.5 e 10.0.0.6
 - I router avranno indirizzi 10.0.0.0 e 10.0.0.4
 - I router avranno indirizzi 10.0.0.4 e 10.0.0.5

8. Per il collegamento diretto fra due router viene scelto di utilizzare per l'indirizzamento delle interfacce la network 10.0.0.4/30. Ne consegue che
- I router avranno indirizzi 10.0.0.5 e 10.0.0.6
 - I router avranno indirizzi 10.0.0.1 e 10.0.0.2
 - I router avranno indirizzi 10.0.0.4 e 10.0.0.5
9. Un router SOHO è concepito per essere utilizzato:
- in ambienti domestici o piccolo uffici
 - nella rete di accesso degli operatori
 - nella rete di trasporto degli operatori
10. Youtube si può classificare, secondo la tassonomia dei servizi ITU, come un servizio di telecomunicazioni tipo:
- interattivo di consultazione
 - interattivo con scambio dell'informazione in tempo differito con memorizzazione
 - interattivo con scambio dell'informazione in tempo reale
11. Se in un calcolatore con sistema operativo Unix si esegue il comando "arp -a" cosa si ottiene
- l'elenco delle coppie "numeri IP - numero MAC" corrispondenti note all'host in quel momento
 - L'elenco dei numeri MAC degli altri host della network
 - l'indirizzo MAC del gateway della network
12. Nelle PCI del protocollo IP compaiono 16 bit dedicati al controllo dell'errore calcolati utilizzando l'Internet checksum:
- sui soli bit dell'header (PCI) del datagramma suddivisi in parole di 16 bit
 - sui soli bit di dati (escludendo le PCI) che compongono il datagramma suddivisi in parole di 16 bit
 - su tutti i bit che compongono il datagramma suddivisi in parole di 16 bit
13. Un protocollo ARQ per il recupero dell'errore può utilizzare il metodo cosiddetto Selective Repeat. Qualora sia identificata come perduta la trama numero N, in questo caso
- viene ritrasmessa la sola trama numero N
 - vengono ritrasmessi meno dati rispetto alla politica Go Back N
 - vengono ritrasmesse tutte le trame a partire dalla numero N
14. Un certo numero di calcolatori connessi tutti allo stesso switch, in assenza di VLAN, si dice che appartengono tutte la medesimo dominio di broadcast. Questo significa che:
- se uno di loro invia un messaggio di ARP request, tutti lo ricevono
 - se due di loro trasmettono contemporaneamente un messaggio di ARP request avviene una collisione

- se due di loro inviano contemporaneamente una trama qualunque avviene sempre una collisione
- 15. Il routing distance vector ha alcune limitazioni. Quando si parla di "convergenza lenta" si intende:
 - che quando si verifica un guasto in rete che rende non funzionante il collegamento fra una due router potrebbero essere necessari vari minuti per ripristinare un percorso alternativo
 - che quando si modifica la topologia di rete i nuovi percorsi di lunghezza minima vengono calcolati con una certa lentezza
 - che i router sono relativamente lenti a instradare i pacchetti
- 16. Una rete utilizza un sistema di moltiplicazione a divisione di tempo con allocazione statica della banda. Ne consegue che e la rete e' tendenzialmente adatta:
 - per fornire servizi di tipo real time conversazionali poiche' garantisce una buona trasparenza temporale
 - per fornire servizi in tempo differito poiche' non garantisce una buona trasparenza temporale
 - per fornire servizi diffusivi perche' permette di implementare facilmente canali di tipo broadcast
 - non so
- 17. Secondo la logica di Internet una "network IP" e':
 - un insieme di calcolatori che hanno interfacce di rete a cui sono attribuiti numeri IP con prefisso comune
 - un insieme di calcolatori che hanno interfacce di rete utilizzanti tutte il medesimo indirizzo
 - un insieme di calcolatori che hanno interfacce di rete a cui sono attribuiti numeri IP con una parte dei bit avente valore "1"
- 18. La tecnologia utilizzata per lo sviluppo della rete pubblica a larga banda detta FTTH prevede che la fibra ottica raggiunga
 - la casa dell'utente
 - no so
 - gli armadi di interconnessione presenti in strada che raccolgono collegamenti da numerose unità abitative (isolati)
 - la centrale di rete pubblica piu' vicina all'utente
- 19. Se si vuole implementare un codice a rivelazione di errori che sia in grado di rilevare errori su un singolo bit e su due bit per trame, si puo':
 - utilizzare un codice polinomiale con il polinomio generatore suggerito dall'ITU $x^{16}+x^{12}+x^5+1$
 - utilizzare il bit di parita' dispari poiche' il bit di parita' pari non rileva errori su numeri pari di bit
 - utilizzare un codice polinomiale con polinomio generatore $x+1$

20. Nell'implementazione di un protocollo che prevede la rilevazione d'errore implementata con codice polinomiale si utilizza il polinomio generatore $x^8+x^4+x^2+1$. Ne consegue che:

- Sarà sempre possibile rilevare l'errore su un singolo bit
- Sarà sempre possibile rilevare l'errore su 6 bit consecutivi.
- Qualora 10 bit consecutivi risultino errati potrebbe avvenire che il codice non rilevi l'errore.

21. Il campo TTL nell'intestazione del dagramma IP ha dimensione pari a

- 8 bit
- 4 bit
- 16 bit

22. Con riferimento agli Autonomous System (AS) quando si parla di peering si intende

- un'interconnessione per scambiarsi traffico direttamente
- un accordo per scambiarsi informazioni di routing con opportune regole di import ed export
- una modalità specifica per l'interconnessione dei router interni agli AS

23. Secondo la terminologia OSI una Protocol Data Unit (PDU) di livello N è composta da

- due parti denominate PCI e SDU
- dai soli dati d'utente
- dai SAP e dai dati d'utente

1. Quali delle seguenti affermazioni sono pertinenti se si considera un Internet Service Provider

- È un soggetto economico che fornisce a pagamento interconnessioni intercontinentali ad altri gestori di rete
- È un soggetto economico che fornisce a pagamento l'accesso alla rete Internet agli utenti finali
- Ha un'infrastruttura presente sul territorio in particolari punti detti Point of Presence o PoP

2. Il messaggio DHCP OFFER

- Viene inviato dal client DHCP e serve a identificare a quale server si chiede la configurazione dell'interfaccia IP
- Viene inviato dal server DHCP e termina la fase di configurazione dell'interfaccia IP del client
- Viene inviato dal server DHCP e serve al client per identificare a quale server rivolgersi per la configurazione dell'interfaccia

3. In un protocollo ARQ quando il ricevitore riceve una trama:

- Qualora la trama risulti errata la scarta e può inviare al trasmettitore un messaggio di Acknowledge negativo
- Qualora la trama risulti errata la scarta e può non fare null'altro

- Controlla che sia corretta verificando le PCI per la rivelazione di errore
- 4. In un tipico router di Internet la Routing Information Base (RIB) viene compilata:
 - Dal router designato durante la fase di start up del protocollo OSPF
 - Dal router stesso, in base alle informazioni ottenute dall'esecuzione dei vari protocolli di router
 - Dal nodo di controllo centrale di tutta la rete
- 5. Un flusso dati fra due istanze applicative nella rete Internet è univocamente identificata da
 - Coppia di numeri di porta sorgente e destinazione
 - Coppia di numero IP e porta sorgente e numero IP e porta destinazione
 - Coppia di numeri IP sorgente e IP destinazione
- 6. L'OSPF utilizza più di un protocollo per svolgere completamente le sue funzioni.
Quali dei seguenti sono protocolli che fanno parte di OSPF
 - Exchange Protocol
 - Hello Protocol
 - Distance protocol
- 7. Il protocollo DHCP viene utilizzato per
 - Configurare i parametri dell'interfaccia di rete di un calcolatore su una certa network IP
 - Configurare le credenziali di accesso alla rete Wi-Fi
 - Configurare il sistema operativo del calcolatore all'avvio
- 8. La dimensione dell'indirizzo MAC utilizzato nelle LAN Ethernet ha dimensione pari a
 - 6 byte
 - non so
 - 4 byte
 - 8 byte
- 9. Le due network IP 137.204.6.0/24 e 137.204.7.0/24 potrebbero essere aggregate nella network
 - 137.204.6.0/23
 - 137.204.7.0/23
 - 137.204.6.0/25
- 10. In una LAN IEEE 802.11 implementata come BSS, la trama diretta all'access point
 - Ha come primo indirizzo MAC quello dell'access point
 - Ha come primo indirizzo MAC quello del calcolatore che la sta inviando
 - Ha come primo indirizzo MAC quello del calcolatore a cui è destinata

11. All'interfaccia di rete di un calcolatore e' attribuito un certo numero IP. Per determinare il Network ID corrispondente, secondo le regole dell'indirizzamento CLASSFULL (precedente al CIDR)
- E' sufficiente interpretare correttamente i primi bit dell'indirizzo
 - E' necessario utilizzare la NETMASK
 - E' necessario utilizzare il DEFAULT GATEWAY
12. Nella rete internet si parla fra gli altri di ISP e IXP. Quale delle seguenti affermazioni sono corrette al riguardo:
- IXP e' acronimo di Internet Exchange Point
 - ISP e IXP sono di fatto acronimi diversi per identificare i medesimi soggetti.
 - Gli ISP sono le amministrazioni statali che decidono sulle politiche da applicare alla rete Internet in una nazione
13. Quali delle seguenti affermazioni sono corrette con riferimento all'applicazione PING:
- Viene implementato utilizzato il protocollo ICMP
 - Permette di avere una stima del Round Trip Time fra due nodi della rete Internet
 - Permette di misurare la distanza geografica fra due nodi della rete Internet
14. In un codice polinomiale il polinomio generatore
- Deve essere noto a priori a ricevitore e trasmettitore
 - Determina le capacità di rilevazione dell'errore
 - Determina il numero minimo di bit da dedicare al controllo dell'errore nelle PCI
15. Un protocollo Stop-and-wait
- E' un protocollo a finestra scorrevole in cui la finestra ha valore $W=1$
 - Garantisce sempre la stessa efficienza di un protocollo ARQ che lavori con finestra $W>1$
 - Generalmente risulta poco efficiente se velocità di trasmissione (C) e ritardo di propagazione (I) sono molto elevati
16. In un protocollo ARQ la finestra ha dimensione W e lo spazio di numerazione delle trame è modulo M (tale che sono disponibili M numeri). Ne consegue che deve essere
- $W < M$
 - $W = M$
 - $W \geq 1$
17. Un protocollo ARQ a finestra scorrevole:
- Permette di realizzare automaticamente il controllo di flusso se la finestra è correttamente dimensionata
 - Ha sempre efficienza massima
 - Per funzionare correttamente necessita di essere accoppiato ad un codice a correzione d'errore

18. Un protocollo ARQ opera su di un canale di capacità $C=512$ Kbit/s e ritardo di propagazione di $R=0.8$ ms. In prima approssimazione si ipotizza che il protocollo utilizzi trame di dimensione fissa pari a $F=8$ byte. Ne consegue che il protocollo ha massima efficienza nell'uso del canale se la finestra W ha dimensione almeno uguale a

- 6
- 2
- 4

19. Un protocollo di livello 2 (DATA LINK) di tipo ARQ utilizza trame di lunghezza $D = 256$ bit che si possano trascurare le PCI del protocollo ed opera su di un canale di capacità nominale $C = 56$ Kbit/s. Le due entità si trovano ad una distanza tale da provocare un ritardo di propagazione da una all'altra $I = 500$ us (microsecondi). Nell'ipotesi che il canale sia pressoché ideale, ossia privo di errori di trasmissione e che si possano trascurare le PCI del protocollo, quale sarà l'efficienza nel caso di finestra $W = 3$.

- 1
- 0.9
- 0.85

20. Un canale su cui viene utilizzato un protocollo ARQ di tipo STP-AND-WAIT (finestra $W=1$) è caratterizzato da una probabilità di perdita, indipendente da bit a bit e costante pari a $P_b=0.1\%$ (1 bit su mille). L'overhead dovuto alle PCI e al tempo di propagazione delle trame sul canale ammonta in prima approssimazione a $O=20$ bit. Ne consegue che la dimensione ottimale della trama (trascurando le PCI) risulta essere:

- Circa 140 bit
- Circa 200 bit
- Circa 80 bit

21. Quando si dice "paradosso delle fibre ottiche" si intende che

- Le fibre ottiche rappresentano uno dei pochi esempi di tecnologie per cui ad un forte incremento di prestazioni rispetto alle tecnologie concorrenti, corrisponde una sostanziale diminuzione di costo
- E' un paradosso che le fibre ottiche non siano state immediatamente dispiegata nella rete di accesso in considerazione del basso costo e della semplicità dei relativi connettori
- Le fibre ottiche permettono velocità di trasmissione paradossali

22. Per realizzare collegamenti su lunghe distanze e' preferibile:

- utilizzare le fibre ottiche in virtù della loro bassa attenuazione
- utilizzare cavi UTP in virtù del loro basso costo
- cavi coassiali in virtù della loro immunità ai disturbi elettromagnetici

23. Secondo il modello ISO OSI un protocollo di livello N

- stabilisce le regole di dialogo fra due entità di livello N

- stabilisce le regole di dialogo tra le entita' di livello N e quelle di livello N-1
 - non e' necessario che sia standardizzato in quanto strettamente dipendente dall'implementazione
24. Servizi quali la posta elettronica, whats, telegram ecc. secondo la tassonomia dei servizi ITU sono classificabili come:
- interattivi con scambio dell'informazione in tempo differito con memorizzazione
 - Distributivi con controllo di presentazione
 - Non so
 - interattivi con scambio dell'informazione in tempo reale
25. Servizi quali e-mail, WhatsApp, Telegram ecc. secondo la tassonomia dei servizi ITU sono classificabili come:
- interattivi con scambio dell'informazione in tempo differito con memorizzazione
 - distributivi con controllo di presentazione
 - interattivi con scambio dell'informazione in tempo reale
26. Un canale di tipo broadcast può essere utilizzato in presenza di N terminali
- per permettere la comunicazione da un terminale a tutti gli altri
 - solamente per realizzare il collegamento fra due e solo due degli N terminali
 - solamente per realizzare il collegamento fra un terminale ed un sottoinsieme degli altri
27. Quando si parla dei soggetti coinvolti nella realizzazione dell'architettura della rete Internet si parla fra gli altri di ISP e IXP. Quale delle seguenti affermazioni sono corrette al riguardo:
- IXP e' acronimo di Internet Exchange Point
 - gli ISP sono le amministrazioni statali che decidono sulle politiche da applicare alla rete Internet in una nazione
 - ISP e IXP sono di fatto acronimi diversi per identificare i medesimi soggetti
28. Per controllare gli errori di trasmissione e' possibile adottare codifiche a correzione o a rivelazione di errore. Considerando come misura di prestazione, e quindi di efficienza, la quantita' complessiva di bit aggiunti dall'operazione di codifica, queste due tecnologie sono tali che:
- una risulta piu' o meno efficiente dell'altra in funzione dei valori di probabilita' di perdita per bit
 - la rivelazione e' sempre piu' efficiente della correzione
 - la correzione e' sempre piu' efficiente della rivelazione
29. Con riferimento allo split horizon quali delle seguenti affermazioni sono vere:
- migliora le prestazioni del protocollo
 - è una tecnica che si applica ai protocolli di routing Distance Vector;

- costringe un router ad inviare le stesse informazioni di routing da tutte le interfacce

30. In un sistema di multiplazione TDM slotted

- le unita' informative hanno tutte la stessa dimensione prefissata e definita dalla rete
- l'asse dei tempi non e' suddiviso a priori in intervalli che determinano obbligatoriamente l'inizio e la fine di una unità informativa
- e' necessario un sistema esplicito di delimitazione delle unita' informative

31. Quale fra i seguenti e' un indirizzo valido per un host in una rete IP con numerazione privata

- 10.0.0.100
- 137.256.121.0
- 192.168.1.256

32. Il protocollo 802.1q viene utilizzato

- per identificare a quale VLAN appartengano le trame scambiate fra switch della stessa LAN
- per identificare il protocollo di routing utilizzato fra i router della LAN
- per autenticare un utente quanto tenta l'accesso alla LAN

33. Il servizio VoIP dal punto di vista della qualita' richiesta alla rete si puo' classificare come

- sensibile ai ritardi e quindi tale da richiedere buona trasparenza temporale
- sensibile agli errori e quindi tale da richiedere buona trasparenza semantica
- sensibile agli errori e ai ritardi e quindi tale da richiedere ottima trasparenza sia semantica sia temporale

34. Con riferimento ad un Internet Exchange Point (IXP) possiamo dire che

- deve essere dotato di importanti infrastrutture di connettività in uno spazio sorvegliato ed in grado di garantire un'ottima continuità al servizio
- svolge un ruolo di interconnessione neutrale fra ISP operanti in una certa area geografica
- un esempio di Internet Exchange Point (IXP) in Italia il MIX di Milano

35. Nella rete Internet italiana il MIX svolge il ruolo

- Internet exchange point
- ente di gestione degli autonomous system italiani
- internet service provider

36. In una LAN implementata con cablaggio strutturato l'armadio di rete contiene tipicamente:

- Patch cord, cavi utilizzati per collegare le prese dei patch panel alle porte degli apparati attivi

- Apparati attivi quali switch e router opportunamente connessi ai calcolatori della LAN
 - patch panel, punti di arrivo del cablaggio orizzontale all'interno dell'armadio
37. In una LAN implementata con cablaggio strutturato l'armadio di rete contiene tipicamente:
- 0.0.0.0 0.0.0.0 192.168.200.1 en0
 - 192.168.1.0 255.255.255.0 192.168.0.254 en0
 - 192.168.200.0 255.255.255.0 192.168.10.254 en1
38. Un'azienda realizza la propria infrastruttura di rete utilizzando un solo router ed un solo switch, ma intende creare due LAN virtuali tramite opportuna configurazione dello switch. Ne consegue che:
- il router può avere una o più porte connesse allo switch, ma nel primo caso questa deve necessariamente essere configurata in modalità trunking
 - le porte dei calcolatori connessi alla LAN devono essere configurate in modalità "trunking"
 - il router deve avere necessariamente una sola porta connessa allo switch
39. Il servizio VoIP dal punto di vista della qualita' richiesta alla rete si puo' classificare come
- sensibile ai ritardi e quindi tale da richiedere buona trasparenza temporale
 - sensibile agli errori e quindi tale da richiedere buona trasparenza semantica
 - sensibile agli errori e quindi tale da richiedere buona trasparenza semantica
40. L'efficienza di un protocollo misura:
- la riduzione di capacità, rispetto alla capacità massima nominale del canale, dovuta alle dinamiche del protocollo ed alla presenza delle PCI
 - la capacità del protocollo di effettuare frammentazione dei pacchetti in modo efficiente
 - la capacità del protocollo di evitare situazioni di deadlock
41. I pacchetti di LINK STATE ADVERTISEMENT in un protocollo di routing link state vengono numerati poiche':
- i router devono poter capire se un pacchetto che arriva e' meno recente di uno gia' ricevuto in modo da trascurarlo.
 - i router comprendono se un pacchetto arriva duplicato e lo trascurano
 - i router controllano che non ne evada perso neppure uno

Il primo cavo transatlantico telefonico:

fu realizzato verso la metà del XX secolo, dopo l'invenzione del transistor e l'avvento dell'elettronica allo stato solido.

Un servizio di tipo broadcast:

può essere realizzato con qualunque tipologia di canale, anche se risulta più efficiente utilizzare un canale broadcast

se realizzato utilizzando un canale di tipo broadcast che "copre" una certa area geografica, permette la fruizione del servizio in mobilità nell'area.

Le reti di telecomunicazioni geografiche hanno tipicamente una struttura:

di tipo gerarchico in cui si può riconoscere una rete di accesso tipicamente a stella ed una di transito con interconnessioni a maglia.

Secondo il modello OSI le PCI:

vengono aggiunte da tutti gli strati ai dati loro consegnati dagli strati immediatamente superiori.

Le prime reti di calcolatori sviluppate negli anni '70:

erano reti proprietarie chiuse sorte per lo più iniziative dei grandi costruttori di calcolatori

Le linee bifilari intrecciate o doppini:

Migliorano la loro qualità quando sono intrecciate con molta cura, diminuendo gli accoppiamenti elettromagnetici mutui.

Nel corso del XX secolo sono state usate per realizzare la rete di accesso telefonica.

Sono particolarmente economiche e semplici da installare.

Sono classificati in categorie in base alla qualità della loro realizzazione, secondo precisi standard internazionali.

Le linee bifilari in rame di tipo UTP categoria 5:

sono utilizzate per la realizzazione di cablaggi strutturati negli edifici.

Per garantire una qualita' di servizio accettabile per servizi di comunicazione vocale fra umani una rete deve:

privilegiare la garanzia di una buona trasparenza temporale.

I sistemi cellulari:

Sono stati introdotti per consentire servizi conversazionali mediante un numero limitato di canali radio riutilizzati più volte in aree diverse

I cavi coassiali:

Sono composti da due conduttori concentrici separati da un materiale isolante (ad esempio plastica).

Sono mezzi trasmissivi con ottima immunità ai disturbi elettromagnetici, migliore rispetto ai doppini (Twisted Pairs).

Sono stati progressivamente soppiantati dalle fibre ottiche.

Considerando l'efficienza di un protocollo ARQ a finestra scorrevole con dimensione della finestra pari a 1, che trasmette trame di dimensione, su un canale avente velocità C=64Kbit/s, ritardo di propagazione I=0.1 ms e probabilità di errore per bit Pe=10-4, trascurando la dimensione delle PCI (D=F) e il tempo di elaborazione del ricevitore (E=0), si può dire che:

l'efficienza può raggiungere un valore superiore a 0.8 se la dimensione viene scelta in modo ottimale
nell'interno degli 800 bit.

Il controllo di flusso in un protocollo ARQ:

si realizza per effetto del fatto che il ricevitore, tramite l'invio delle conferme, determina il ritmo con cui vengono inviate le nuove trame.

funziona correttamente a patto che il ricevitore possa memorizzare un numero di trame pari alla dimensione della finestra.

La massima efficienza di un protocollo ARQ che trasporta trame di lunghezza F=500 byte di cui H=10 di intestazione:

risulta pari al 98% solo se la finestra viene correttamente dimensionata.

Un protocollo ARQ a finestra scorrevole che trasmette, su di un collegamento di capacità C, trame di dimensione pari a F bit di cui D di dati di utente e H di PCI:

ha efficienza $D/(D+H)$ solamente se il tempo di trasmissione di una finestra (WF/C) è superiore al tempo che intercorre fra l'inizio della trasmissione e la ricezione del primo ACK.

In un protocollo ARQ quando il ricevitore riceve una trama:

controlla che sia corretta verificando le PCI per la rivelazione di errore
qualora la trama risulti errata la scarta e può non fare null'altro

Il codice a rivelazione d'errore detto "bit di parità":

rivela tutti gli errori su un numero dispari di bit

In un protocollo di strato 2 in cui la rivelazione di errore viene effettuata usando il polinomio generatore x^2+1 :

i bit di ridondanza sono 2.

Un codificatore polinomiale con polinomio generatore $G(x) = 1+x$, deve codificare la sequenza 1100101011; il risultato è la sequenza:

11001010110

Nei più diffusi standard per i protocolli di livello 2 (o di linea), nelle attuali reti di telecomunicazioni quali la rete Internet:

si utilizzano tipicamente codici a rivelazione di errore.

Il comando PING:

Serve per controllare se un host IP è raggiungibile su Internet.

Nell'intestazione (header) del datagramma IP:

Sono presenti due indirizzi di lunghezza fissa per sorgente e destinazione.

Il messaggio DHCPDISCOVER:

Viene inviato da un client che deve configurare la propria interfaccia di rete in modalità broadcast sulla LAN.

Per il corretto funzionamento dell'interfaccia di rete di un host vanno configurati almeno i seguenti parametri:

numero IP e Netmask.

Il messaggio ICMP di errore "Time exceeded" può indicare che:

il Time-to-Live di un datagramma si è azzerato ed il datagramma viene distrutto.
l'attesa dei frammenti per riassemblare un datagramma si è protratta troppo lungo, oltre un valore limite prefissato.

Il Dipartimento di un ente ottiene per l'indirizzamento IP la rete 137.204.57.128/27. Ne consegue che:

potrebbe scegliere come indirizzo IP del gateway di default il numero 137.204.57.129
la netmask dei relativi host va configurata al valore 255.255.255.224
non può utilizzare per l'interfaccia di un host l'indirizzo IP 137.204.57.159

La completa configurazione dell'interfaccia IP di un host richiede di specificare:

numero IP, netmask, default gateway e server DNS.

Nell'elaborazione del routing table lookup:

si fa uso del campo IP DESTINATION nonché' del contenuto dei campi NETMASK e DESTINATION della tabella di instradamento

Un router riceve un datagramma IP di 1100 byte, di cui 20 di header, con FRAGMENT OFFSET = 3000 e che deve essere inviato su di una rete che accetta datagrammi di lunghezza massima pari a 400 byte:

se il flag DONT FRAGMENT vale 1 non invia il datagramma e ritorna un messaggio di errore all'host sorgente.

Un datagramma con il flag DONT FRAGMENT = 1:

qualora dovesse essere frammentato, viene scartato producendo un messaggio di errore.

Il messaggio DHCP OFFER:

viene inviato dal server DHCP e serve al client per identificare a quale server rivolgersi per la configurazione dell'interfaccia.

Un router riceve un datagramma IP di 1500 byte con FRAME OFFSET = 0. IL datagramma deve essere inviato su di una rete che accetta datagrammi di lunghezza massima pari a 20 byte di header e 512 byte di dati (payload). Ne consegue che:

se il flag DON'T FRAGMENT vale 1, il router non invia il datagramma e ritorna un messaggio di errore all'host sorgente.

se il campo FRAGMENT OFFSET vale 0 frammenta il datagramma in 3 parti con FRAGMENT OFFSET rispettivamente 0, 64, 128.

L'interfaccia di rete di un host ha configurato il numero IP a 192.168.20.12 ed il parametro NETMASK al valore 255.255.255.224; ne consegue che:

l'indirizzo della rete a cui appartiene l'host è 192.168.20.0

la network IP può contenere al più 30 host (oppure 29 host ed un gateway)

la network IP a cui appartiene l'host utilizza 5 bit per indirizzare i singoli host

Con il termine "Direct Forwarding" si intende:

la capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router

Quale fra i seguenti è un indirizzo valido per un host in una rete IP con numerazione privata:

192.168.1.1
10.0.0.100

La tabella ARP in un host:

contiene corrispondenze fra numeri IP e indirizzi MAC.

L'indirizzo IP 190.240.20.254:

è un indirizzo di classe B.

Tra due router viene configurata la rete 10.0.0.4/30. Ne consegue che:

I router avranno indirizzi 10.0.0.5 e 10.0.0.6

L'applicazione Traceroute:

serve per comprendere quale sia il percorso seguito da un datagramma fra una sorgente ed una destinazione.

utilizza il campo TTL del datagramma IP ed i messaggi di errore ICMP per svolgere le sue funzioni.

La modalità di instradamento dei datagrammi nella rete Internet:

viene fatta sulla base dell'indirizzo IP di destinazione

Applicare la netmask 255.255.255.224 alla rete IP 192.168.1.0 significa:

suddividere la rete in 8 sottoreti.

che l'indirizzo IP 192.168.1.31 è indirizzo broadcast per una subnet.

Nell'intestazione (header) del datagramma IP il campo FRAGMENT OFFSET:

Indica la distanza del frammento dall'inizio del datagramma in blocchi di 8 byte.

La consegna di un datagramma con instradamento indiretto:

implica il coinvolgimento di almeno un router.

non avviene se i due host appartengono alla medesima network IP.

Il protocollo ARP

viene utilizzato ogni volta che si deve inviare un datagramma ad un host il cui indirizzo IP non compare nella tabella ARP.

Un host connesso in rete utilizzando il protocollo IP:

può avere una o più interfacce e ad ognuna deve essere assegnato un numero IP

I messaggi del protocollo ICMP

vengono trasportati direttamente su IP senza utilizzare un protocollo di trasporto

Quali di questi sono compiti tipici dello strato di linea (DL layer)

Rivelazione di errore

Controllo di flusso

L'Internet checksum:

viene utilizzato nei vari protocolli della rete Internet dove necessario
utilizza l'operazione di somma binaria modulo 1

Il messaggio DHCPACK:

viene inviato dal server DHCP e termina la fase di configurazione dell'interfaccia IP del client

Nell'intestazione (header) del datagramma IP il campo MORE FRAGMENTS (MF):

Occupava 1 bit

Nell'intestazione (header) del datagramma IP il campo Header checksum:

Deve essere ricalcolato ad ogni hop, ossia ogni volta che il datagramma attraversa un router

Verifica la correttezza della sola intestazione del pacchetto e pertanto viene calcolato sui soli byte delle PCI del datagramma

Un host appartenente ad una rete connessa ad Internet tramite un NAT ha attribuito all'interfaccia di rete l'indirizzo 192.168.0.1 ed ha attiva una connessione sulla porta TCP 51321:

nei datagrammi che riceve da trasmettere su Internet per la connessione il NAT deve necessariamente modificare il numero IP sorgente e, in funzione del tipo di configurazione e delle connessioni esistenti, potrebbe modificare il numero di porta sorgente

Nell'intestazione (header) del datagramma IP il campo Versione (Version):

Occupava 4 bit

Una rete IP di classe C:

Usa 3 byte per l'indirizzo della rete e 1 byte per l'indirizzo dell'Host

Nell'intestazione (header) del datagramma IP il campo Time to live:

Limita il tempo di permanenza di un pacchetto in Internet

Nell'intestazione (header) del datagramma IP è presente il campo IDENTIFICATION, che contiene un numero che identifica il datagramma. Quale delle seguenti affermazioni sono vere al riguardo.

Occupava 2 byte

Serve per consentire la eventuale frammentazione e riassemblaggio dei datagrammi

Il concetto di distanza nel routing in Internet:

Può essere un qualunque valore numerico il cui significato viene convenzionalmente definito

Il protocollo BGP:

È un protocollo di tipo Path Vector

Garantisce l'assenza di cicli nella determinazione delle rotte

Un algoritmo di routing si dice statico quando:

Il router fa uso di una tabella di routing definita a priori in fase di configurazione

Quali di questi protocolli di Routing sono stati usati in Internet:

BGP

I termini protocollo e algoritmo di instradamento

indicano rispettivamente i metodi di scambio delle informazioni sulla topologia della rete e di calcolo delle tabelle di instradamento

I protocolli della famiglia Link State

Sono protocolli dinamici, Prevedono che ogni router trasmetta a tutti i nodi della rete la propria distanza dai vicini

Il flooding:

È il modo più semplice per spedire un pacchetto a tutti gli host di una rete

Viene usato come algoritmo ausiliario in alcuni protocolli di routing standardizzati da IETF

Qualora si utilizzi in una rete un protocollo di routing di tipo flooding:

tutte le possibili destinazioni vengono sicuramente raggiunte dai pacchetti

L'algoritmo di Dijkstra:

Richiede la conoscenza della topologia della rete

Permette di ricavare i percorsi di lunghezza minima fra una qualunque coppia di nodi di rete

Per l'organizzazione di Internet un Autonomous System:

È un dominio di routing che comunica con l'esterno utilizzando un Exterior Gateway Protocol quale il BGP.

Il protocollo OSPF

Viene usato come Interior Gateway Protocol.

I protocolli della famiglia Distance Vector:

Prevedono che ogni router trasmetta ai propri vicini la propria distanza da tutti i nodi della rete

Richiedono che ogni router conosca a priori la distanza dai suoi vicini

I protocolli di routing:

servono per creare e manutenere le tabelle di routing nei nodi

logicamente sono protocolli di livello applicativo che fanno parte del piano di controllo della rete

Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si può dire che:

I Link State richiedono più memoria nel router

Quali fra i protocolli elencati in seguito sono protocolli di Routing utilizzati in Internet:

RIP

I messaggi del protocollo OSPF:

hanno tutti un'intestazione comune, seguita da informazioni specifiche che dipendono dal tipo di pacchetto
vengono utilizzati per l'implementazione del protocollo di HELLO che permette ai router di scoprire i propri vicini

Quali di questi campi sono contenuti nei pacchetti di tipo Link State prodotti dal protocollo OSPF

Età del pacchetto

Indirizzo del mittente

Numero di sequenza

Confrontando i protocolli della famiglia Distance Vector (DV) con quelli della famiglia Link State (LS) si può dire che

In generale i protocolli LS garantiscono un funzionamento migliore di quelli DV

Quali delle seguenti descrizioni può essere ritenuta corretta per le funzioni delle tabelle di routing utilizzate nei nodi a commutazione di pacchetto

Associare ad ogni indirizzo di destinazione una porta di uscita

Associare ad ogni indirizzo di destinazione e ad ogni porta di uscita un costo convenzionalmente definito

Il routing nella rete Internet

Viene implementato in modo dinamico e distribuito da tutti i nodi di rete, utilizzando sia scambio di informazioni sia opportuni algoritmi, secondo diverse modalità per diverse sezioni della rete

In un collegamento IPSec tunnel mode

viene cifrato sia il contenuto sia l'intestazione dei datagrammi IP

Quali fra questi campi sono contenuti nella trama MAC dello standard IEEE 802.3

Starting delimiter

Padding

In una LAN IEEE 802.11 implementata con più Access Point operanti con WDS la trama diretta all'access point a cui è connessa la stazione di destinazione

ha come primo indirizzo MAC quello dell'access point di destinazione

Quali sono le principali differenze fra RIP versione 1 e versione 2:

il RIP v2 supporta il CIDR mentre il RIP v1 interpreta gli indirizzi IP solamente con la logica classfull

il RIP v2 supporta l'autenticazione dei router mentre il RIP v1 no

In un LAN wireless del tipo IEEE 802.11 (Wi-Fi) il canale radio

viene suddiviso in due canali a diverse frequenze, uno dei quali è utilizzato dalla stazione base (downlink) e l'altro dalle stazioni di utente (uplink)

Il progetto IEEE 802

Definisce, per le reti locali di calcolatori, gli standard relativi ai mezzi trasmissivi e agli strati 1 e 2 del modello OSI

Si dice bridge

un dispositivo per l'interconnessione di reti locali operante a livello 2

Su uno switch a 8 porte configuro due VLAN. La VLAN 1 sulle porte 1, 2, 3, 7 e la VLAN 2 sulle porte 4, 5, 6, 8. Ciò significa che

un calcolatore connesso alla porta 1 può comunicare con un calcolatore connesso alla porta 2 senza la necessità di ulteriori apparati

un calcolatore connesso alla porta 1 non può comunicare con un calcolatore connesso alla porta 4 a meno che non utilizzi ulteriori apparati

Stazioni Ethernet che appartengono al medesimo dominio di collisione

sono tipicamente collegate tramite un hub

se tramattono contemporaneamente danno luogo a collisione

Con il nome di rete Ethernet si indica un atecnologie che corrisponde a:

uno standard della IEEE

Una rete 802.11 infrastrutturata

prevede che le stazioni comunichino fra loro tramite una stazione base che riceve il segnale su un canale di uplink e lo ripete su di un canale di downlink

La consegna di un datagramma con instradamento indiretto

implica il coinvolgimento di almeno un router

non avviene se i due host appartengono alla medesima network IP

Un datagramma viene inviato con TTL=1 nell'intestazione

verrà bloccato nel primo router che incontra generando un messaggio di errore ICMP

potrebbe essere generato dall'applicazione TRACEROUTE

Fra i mezzi trasmissivi usati nelle le reti in area locale (LAN) ci sono

Canale radio

Coppie bifilari avvitate (Twisted Pairs)

Fibre ottiche

Secondo la terminologia Wi-Fi un ESS

è un sistema di più access point funzionanti come un'unica LAN

In base all'evoluzione dei sistemi di cablaggio, una rete LAN in un edificio aziendale si può dire che tipicamente è realizzata con

Cablaggio orizzontale di piano con cavo UTP e interconnessione fra piani con cavo UTP o fibra ottica.

Secondo la terminologia dello standard IEEE 802.11 un BSS è

un'area in cui una serie di stazioni mobili possono colloquiare grazie ad un access point se si parla di Infrastructure BSS

un'area dove viene implementata una rete ad hoc se si parla di Independent BSS

Un Ethernet switch a 4 porte 100baseT

redirige i pacchetti sulle uscite in base all'indirizzo MAC destinazione

fornisce prestazioni superiori rispetto ad un hub

Una rete Ethernet 1000baseT

prevede una velocità di trasmissione pari a 1 Gbit/s

prevede come mezzo trasmissivo il doppino incrociato non schermato (UTP) di categoria 5E o superiore

Le dimensioni di una LAN sono tipicamente
dell'ordine delle centinaia di metri

Un protocollo di accesso si definisce a contesa quando la procedura di accesso
È distribuita e non garantisce l'assenza di collisioni

In una VPN funzionante in modalità roadwarrior un utente della VPN

può collegarsi alla VPN da un qualunque punto di Internet tramite un'opportuna procedura di autenticazione (username e password tipicamente)

Secondo gli standard IEEE 802 gli indirizzi MAC sono tali che

Sono associati in modo univoco alle schede di rete
Permettono di individuare il costruttore della scheda

Un'azienda ha quattro reti LAN in quattro capannoni contigui, realizzate con quattro switch Ethernet, uno per capannone. Si vuole interconnettere le LAN realizzando un'unica rete che corrisponderà ad un'unica network IP:

È preferibile connettere i quattro switch delle LAN tramite uno switch

Il dispositivo denominato HUB

È ormai in disuso in quanto fornisce prestazioni inferiori rispetto agli switch
Può essere utile se si vuole monitorare il traffico sulla LAN

Quali delle seguenti affermazioni sono pertinenti se si considera un Internet Service Provider
è un soggetto economico che fornisce a pagamento l'accesso alla rete Internet agli utenti finali,
ha un'infrastruttura presente sul territorio in particolari punti detti Point of Presence o PoP

In un LAN implementata secondo le moderne tecnologie di cablaggio qual è il ruolo dei path cord
collegare i punti di arrivo delle prese a muro nei patch panel con le corrette porte degli apparati attivi presenti nell'armadio di rete

Nella terminologia OSPF un ABR è

un router che ha almeno un'interfaccia connessa alla propria area ed un'interfaccia connessa all'area di backbone o ad un'altra area

un router che annuncia verso il resto dell'AS gli indirizzi IP delle reti facenti parte della propria area

Il protocollo BGP viene utilizzato per gestire il routing fra gli AS. Viene detto di tipo path vector. Questo significa che

i messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la lista degli AS che vanno attraversati per raggiungerli, Il protocollo BGP

i router quando vedono un'informazione di router in cui compare il loro AS la ignorano onde evitare cicli

Un canale su cui viene utilizzato un protocollo ARQ di tipo STP-AND-WAIT (finestra W=1) è caratterizzato da una probabilità di perdita, indipendente da bit a bit e costante pari a Pb=0.1 % (1 bit su mille). L'overhead dovuto alle PCI e al tempo di propagazione delle trame sul canale ammonta in prima approssimazione a O=20 bit. Ne consegue che la dimensione ottimale della trama (trascurando le PCI) risulta essere:

circa 140 bit.

Un protocollo ARQ opera su di un canale di capacità C=512 Kbit/s e ritardo di propagazione di R=0.8 ms. In prima approssimazione si ipotizza che il protocollo utilizzi trame di dimensione fissa pari a F=8 byte. Ne consegue che il protocollo ha massima efficienza nell'uso del canale se la finestra W ha dimensione almeno uguale a:

6.

In un codice polinomiale il polinomio generatore:

deve essere noto a priori a ricevitore e trasmettitore determina il numero minimo di bit da dedicare al controllo dell'errore nelle PCI determina le capacità di rilevazione dell'errore (TUTTE).

Secondo il modello ISO OSI un protocollo di livello N:

stabilisce le regole di dialogo fra due entità di livello N.

Per realizzare collegamenti su lunghe distanze è preferibile:

utilizzare le fibre ottiche in virtù della loro bassa attenuazione

Un protocollo Stop-and-wait:

generalmente risulta poco efficiente se velocità di trasmissione (C) e ritardo di propagazione (I) sono molto elevati, è un protocollo a finestra scorrevole in cui la finestra ha valore W=1

In una LAN IEEE 802.11 implementata come BSS, la trama diretta all'access point:

ha come primo indirizzo MAC quello dell'access point

Le due network IP 137.204.6.0/24 e 137.204.7.0/24 potrebbero essere aggregate nella network:

137.204.6.0/23

Quali delle seguenti affermazioni sono corrette con riferimento all'applicazione PING:

viene implementata utilizzato il protocollo ICMP

permette di avere una stima del Round Trip Time fra de nodi della rete Internet

Un host appartenente ad una rete connessa ad Internet tramite un NAT ha attribuito all'interfaccia di rete l'indirizzo 192.168.10.200 ed ha attiva una connessione sulla porta TCP 63520. Ne consegue che:

Il NAT riceve datagrammi da trasmettere su Internet con indirizzo IP sorgente 192.168.10.200

Il campo TTL nell'intestazione del dagramma IP ha dimensione pari a:

8 bit.

Il routing si dice dinamico quando:

Il router costruisce la tabella di routing sulla base delle informazioni che ottiene dagli altri router della rete.

Un certo numero di calcolatori connessi tutti allo stesso switch, in assenza di VLAN, si dice che appartengono tutte la medesimo dominio di broadcast. Questo significa che:

se uno di loro invia un messaggio di ARP request, tutti lo ricevono

se due di loro trasmettono contemporaneamente un messaggio di ARP request avviene una collisione

Nelle reti Wi-Fi le trame portano 4 indirizzi MAC. Il secondo di questi è l'indirizzo sorgente che:

in un BSS contiene l'indirizzo MAC del calcolatore da cui la trama è partita nella tratta di uplink

Un router IP riceve un datagramma. Analizzando l'indirizzo di destinazione del datagramma non trova corrispondenza in alcuna riga della sua tabella di routing. Di conseguenza:

se presente in tabella manda il pacchetto sulla destinazione di default

se non è presente una destinazione di default scarta il datagramma ed invia un messaggio di controllo ICMP tipicamente di Destination Unreachable alla sorgente del datagramma

I pacchetti di LINK STATE ADVERTISEMENT in un protocollo di routing link state vengono numerati poiche':

i router comprendono se un pacchetto arriva duplicato e lo trascurano
i router devono poter capire se un pacchetto che arriva e' meno recente di uno gia' ricevuto in modo da trascurarlo.

Con riferimento allo split horizon quali delle seguenti affermazioni sono vere:

è una tecnica che si applica ai protocolli di routing Distance Vector.
migliora le prestazioni del protocollo.

La tecnologia utilizzata per lo sviluppo della rete pubblica a larga banda detta FTTH prevede che la fibra ottica raggiunga:

la casa dell'utente.

Servizi quali la posta elettronica, whatts, telegram ecc. secondo la tassonomia dei servizi ITU sono classificabili come:

interattivi con scambio dell'informazione in tempo differito con memorizzazione

Un protocollo ARQ per il recupero dell'errore può utilizzare il metodo cosiddetto Selective Repeat. Qualora sia identificata come perduta la trama numero N, in questo caso:

viene ritrasmessa la sola trama numero N

vengono ritrasmessi meno dati rispetto alla politica Go Back N

DOMANDE APERTE

Il "table lookup" è essenziale al corretto funzionamento di ogni nodo IP. Nell'ipotesi di considerare un moderno router che supporta il CIDR, spiegare:

1. quale sia in termini generali lo scopo di tale funzione
2. cosa si intenda con i termini "tabella di instradamento" e "rotta" o "route"
3. quali informazioni vengano utilizzate dal router IP per svolgere questa funzione e dove si trovano (tabella di instradamento o pacchetto IP);
4. se vi sia un ordine preciso nell'uso delle informazioni presenti nella tabella di instradamento
5. se sia possibile che l'operazione di table lookup non dia alcun risultato e, se si, cosa accada di conseguenza

Risposte:

- 1) Il table lookup cerca l'indirizzo ip di destinazione nella tabella di routing

2) Con tabella di instradamento si intende la tabella in cui sono riportati in ogni riga l'indirizzo ip della rete di destinazione con la relativa subnet mask, Gateway, Metrica e l'interfaccia di rete associata

Per singola rotta si intende una singola riga della tabella

3) Destination, Netmask, Gateway, Interface, Metric (si trovano all'interno della tabella di instradamento)

4) L'ordinamento in funzione della Netmask decrescente garantisce di considerare in ordine

- singoli host

- reti piccole

- reti grandi

5) Se il route non esiste genera un messaggio di errore

- Tipicamente notificato all'indirizzo sorgente (ICMP - Destination Unreachable)
-

Con riferimento all'applicazione PING spiegare:

1.a quale scopo viene usata,

2.quali protocollo viene utilizzato per la sua implementazione,

3.quali messaggi utilizza di tale protocollo,

4.quali informazioni sia possibile ottenere eseguendo l'applicazione;

5.per quale motivo su molti sistemi server moderni tale applicazione sia disabilitata.

Risposte:

1) Permette di controllare se l'host DEST è raggiungibile o meno da SORG

2) SORG invia a DEST un pacchetto ICMP di tipo "echo"

3) Echo ed Echo reply (rispettivamente sorgente e destinazione)

4) Indirizzo IP di destinazione, dimensione del pacchetto, TTL (time to live), il "round-trip time" (RTT), numero pacchetti persi, min, max e media del RTT

5) Per evitare la banda venga saturata da troppe richieste PING

Con riferimento all'applicazione TRACEROUTE spiegare:

1.a quale scopo viene usata,

2.quali protocollo viene utilizzato per la sua implementazione,

3.quali messaggi utilizza di tale protocollo,

4.se e quali campi dell'intestazione IP vengono utilizzati per il suo funzionamento;

5.quale sia il principio di tale funzionamento.

Risposte:

- 1) Permette di conoscere il percorso seguito dai pacchetti inviati da SORG e diretti verso DEST
 - 2) Viene utilizzato il protocollo ICMP
 - 3) Echo e TIME EXCEEDED
 - 4) TIME-TO-LIVE (TTL) progressivo da 1 a 30 (per default)
 - 5) primo pacchetto TTL=0, al primo router il pacchetto viene scartato, Risposta con ICMP (TIME EXCEEDED)
secondo pacchetto TTL=1.... arrivo a destinazione
-

I codici polinomiali per l'implementazione della rivelazione di errore si basano sulla divisione di polinomi e sulla definizione di un polinomio generatore. Si chiede di spiegare quanto segue:

1. quanti siano i bit di controllo aggiunti dal codice se il polinomio generatore è di grado 7
2. cosa significhi che questi codici sono di tipo sistematico
3. come venga costruita la parola di codice complessiva (il messaggio) che viene inviata da trasmettitore a ricevitore
4. cosa avviene quando tale messaggio viene ricevuto dal ricevitore
5. quale sia il massimo numero di bit errati consecutivi che vengono sicuramente rilevati dal polinomio generatore di grado 7 di cui sopra

Risposte:

1. 7
2. Significa che i primi n bit che corrispondono al messaggio, mentre in fondo avrà m bit che corrispondono al controllo d'errore.
3. Data la sequenza di bit da inviare la si trasforma in un polinomio nella variabile x $P(x)$, quindi dato il polinomio generatore $G(x)$ si ha il suo grado r e si calcola il prodotto $P(x) \cdot G(x)$ che chiamo $T(x)$. Eseguo il calcolo $T(x) \div G(x)$ ottenendo polinomio $Q(x)$ e resto R . La trama da inviare quindi è $T'(x) = Q(x) + R$, (l'operazione di somma sarebbe un xor).
4. Vengono estratti i bit di ridondanza dalla parola codice, poi viene estratto il messaggio da cui saranno calcolati i bit di ridondanza da confrontare con quelli ottenuti inizialmente, se sono uguali allora la trasmissione è avvenuta correttamente, altrimenti no.
5. Boh

Iniziato Wednesday, 16 December 2020, 09:33

Stato Completato

Terminato Wednesday, 16 December 2020, 10:47

Tempo impiegato 1 ora 14 min.

Valutazione 30,00 su un massimo di 30,00 (100%)

Domanda 1

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Il protocollo RIP esiste in due versioni, la versione 1 (o v1) e la versione 2 (v2).

Paragonando le due versioni quali delle seguenti affermazioni sono vere:

Scegli una o più alternative:

- a. il RIP V1 permette di comunicare anche la destinazione di reti IP conformi al CIDR mentre il RIP v2 no
- b. il RIP v2 prevede un formato dei messaggi completamente diverso da quello del RIP v1 senza alcuna parte in comune
- c. il RIP v2 permette l'autenticazione dei messaggi di REspone, mentre il RIP v1 no



Your answer is correct.

La risposta corretta è: il RIP v2 permette l'autenticazione dei messaggi di REspone, mentre il RIP v1 no



Domanda 2

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Le dimensioni di una LAN sono tipicamente

Scegli un'alternativa:

- a. dell'ordine delle centinaia di metri
- b. dell'ordine dei chilometri
- c. dell'ordine del metro
- d. Non so



Risposta corretta.

La risposta corretta è: dell'ordine delle centinaia di metri

Domanda 3

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si puo' dire che

Scegli una o più alternative:

- a. I Distance Vector richiedono maggior potenza di elaborazione
- b. I Distance Vector si adattano piu' velocemente ai cambiamenti della rete
- c. I Link State richiedono piu' memoria nel router



Risposta corretta.

La risposta corretta è: I Link State richiedono piu' memoria nel router



Domanda 4

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

La tabella ARP in un host:**Scegli una o più alternative:**

- a. Viene configurata all'attivazione dell'host e non puo' essere piu' modificata.
- b. Viene aggiornata dal DNS
- c. contiene corrispondenze fra numeri IP e indirizzi MAC



Risposta corretta.

La risposta corretta è: contiene corrispondenze fra numeri IP e indirizzi MAC

Domanda 5

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Nel cablaggio strutturato l'armadio di rete**Scegli una o più alternative:**

- a. e' il punto di arrivo del cablaggio orizzontale
- b. serve per alloggiare gli apparati attivi della LAN (switch, hub ecc.)
- c. serve per contenere tutte le prese a cui collegare direttamente i vari calcolatori della LAN



Your answer is correct.

Le risposte corrette sono: e' il punto di arrivo del cablaggio orizzontale, serve per alloggiare gli apparati attivi della LAN (switch, hub ecc.)



Domanda 6

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Quale destinazione viene scelta per un datagramma indirizzato a 192.168.200.130 da un router la cui tabella di instradamento si presenta come segue (si faccia attenzione, le righe sono presentate in ordine casuale, va quindi considerato quale sarebbe l'ordinamento corretto per rispondere alla domanda):

Scegli un'alternativa:

- a. 0.0.0.0 0.0.0.0 192.168.200.1 en0
- b. 192.168.1.0 255.255.255.0 192.168.0.254 en0
- c. 192.168.200.0 255.255.255.0 192.168.10.254 en1



Your answer is correct.

La risposta corretta è: 192.168.200.0 255.255.255.0 192.168.10.254 en1

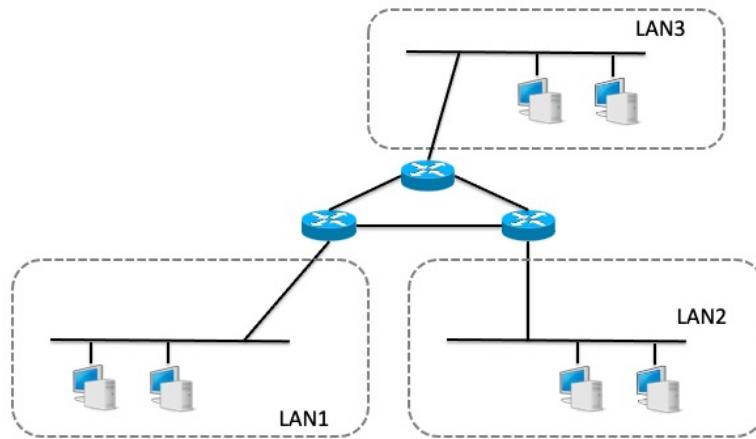


Domanda 7

Completo

Punteggio ottenuto 10,00 su 10,00

Si faccia riferimento alla topologia di rete in figura, che comprende tre LAN (LAN1, LAN2, LAN3). Le LAN devono poter connettere fino a 50 calcolatori ciascuna, mentre i tre router sono connessi con collegamenti punto-punto.



L'azienda proprietaria dell'infrastruttura deve pianificare la numerazione della rete, avendo a disposizione l'insieme di indirizzi pubblici 137.200.190.0/24

Si chiede pertanto di:

1. attribuire un opportuno insieme di numeri IP alle LAN creando delle network IP separate;
2. attribuire un opportuno insieme di numeri IP alle reti di interconnessione fra i router creando anche in questo caso opportune network IP;
3. scegliere gli indirizzi delle varie interfacce dei router;
4. scrivere la configurazione dell'interfaccia IP del calcolatore che su ciascuna LAN ha attribuito il numero di valore minore, indicando nome e valore dei parametri che verranno configurati (manualmente o automaticamente);
5. dire se rimangano a disposizione indirizzi per un'eventuale espansione della rete ed eventualmente quanti.

1) LAN 1 -> 137.200.190.0/26

LAN 2 -> 137.200.190.64/26

LAN 3 -> 137.200.190.128/26



2) LAN 1 a LAN 2 -> 137.200.190.192/30

LAN 1 a LAN 3 -> 137.200.190.196/30

LAN 2 a LAN 3 -> 137.200.190.200/30

3) Router da LAN 1 a LAN 2 -> 137.200.190.193/30

Router da LAN 2 a LAN 1 -> 137.200.190.194/30

Router da LAN 1 a LAN 3 -> 137.200.190.197/30

Router da LAN 3 a LAN 1 -> 137.200.190.198/30

Router da LAN 2 a LAN 3 -> 137.200.190.201/30

Router da LAN 3 a LAN 2 -> 137.200.190.202/30

Router su LAN 1 -> 137.200.190.62/26

Router su LAN 2 -> 137.200.190.126/26

Router su LAN 3 -> 137.200.190.190/26

4) LAN 1

IP: 137.200.190.1 NETMASK: 255.255.255.192 GATEWAY: 137.200.190.62/26

LAN 2

IP: 137.200.190.65 NETMASK: 255.255.255.192 GATEWAY: 137.200.190.126/26

LAN 3

IP: 137.200.190.129 NETMASK: 255.255.255.192 GATEWAY: 137.200.190.190/26

IP, NETMASK e GATEWAY possono venire configurati sia manualmente che automaticamente con un protocollo tipo DHCP, va inoltre specificato un server DNS di default tipo 8.8.8.8 di google

5) In ogni rete LAN con i calcolatori rimangono a disposizione 11 indirizzi inutilizzati (64 - 50 - indirizzo di rete - indirizzo broadcast - gateway) e inoltre rimangono inutilizzate tutte le reti /30 che rimangono dalla divisione dell'ultima sottorete /26 effettuata per ottenere le reti fra i router

Commento:



Domanda 8

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

I termini protocollo e algoritmo di instradamento

Scegli un'alternativa:

- a. sono equivalenti
- b. indicano rispettivamente i metodi di calcolo delle tabelle di instradamento e di scambio delle informazioni sulla topologia della rete
- c. indicano rispettivamente i metodi di scambio delle informazioni sulla topologia della rete e di calcolo delle tabelle di instradamento ✓

Risposta corretta.

La risposta corretta è: indicano rispettivamente i metodi di scambio delle informazioni sulla topologia della rete e di calcolo delle tabelle di instradamento

Domanda 9

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Secondo la terminologia dello standard IEEE 802.11 un BSS e'

Scegli una o più alternative:

- a. un'area dove piu' access point mettono in comunicazione stazioni nascoste le une dalle altre
- b. un'area dove viene implementata una rete ad hoc se si parla di Independent BSS ✓
- c. un'area in cui una serie di stazioni mobili possono colloquiare grazie ad un access point se si parla di Infrastructure BSS ✓

Risposta corretta.

Le risposte corrette sono: un'area in cui una serie di stazioni mobili possono colloquiare grazie ad un access point se si parla di Infrastructure BSS, un'area dove viene implementata una rete ad hoc se si parla di Independent BSS



Domanda 10

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Il routing nella rete Internet

Scegli un'alternativa:

- a. Viene implementato in modo dinamico e distribuito da tutti i nodi di rete utilizzando un unico algoritmo senza scambio di informazioni
- b. Viene implementato in modo statico da un nodo speciale che calcola per le tabelle di instradamento per tutti gli altri nodi della rete
- c. Viene implementato in modo dinamico e distribuito da tutti i nodi di rete, utilizzando sia scambio di informazioni sia opportuni algoritmi, secondo diverse modalità per diverse sezioni della rete



Risposta corretta.

La risposta corretta è: Viene implementato in modo dinamico e distribuito da tutti i nodi di rete, utilizzando sia scambio di informazioni sia opportuni algoritmi, secondo diverse modalità per diverse sezioni della rete

Domanda 11

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

L'applicazione Traceroute

Scegli una o più alternative:

- a. permette di verificare l'efficienza dei protocolli e degli algoritmi di routing
- b. utilizza il campo TTL del datagramma IP ed i messaggi di errore ICMP per svolgere le sue funzioni
- c. serve per comprendere quale sia il percorso seguito da un datagramma fra una sorgente ed una destinazione



Risposta corretta.

Le risposte corrette sono: serve per comprendere quale sia il percorso seguito da un datagramma fra una sorgente ed una destinazione, utilizza il campo TTL del datagramma IP ed i messaggi di errore ICMP per svolgere le sue funzioni



Domanda 12

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Una rete utilizza un sistema di multiplazione a divisione di tempo con allocazione statica della banda. Ne consegue che la rete è tendenzialmente adatta:

Scegli un'alternativa:

- a. non so
- b. per fornire servizi diffusivi perché permette di implementare facilmente canali di tipo broadcast
- c. per fornire servizi in tempo differito poiché non garantisce una buona trasparenza temporale
- d. per fornire servizi di tipo real time conversazionali poiché garantisce una buona trasparenza temporale



Your answer is correct.

La risposta corretta è: per fornire servizi di tipo real time conversazionali poiché garantisce una buona trasparenza temporale

Domanda 13

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Con il termine "Direct Forwarding" si intende

Scegli un'alternativa:

- a. la capacità di un host di consegnare datagrammi interagendo direttamente con un gateway
- b. la capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router
- c. la capacità di un host di inviare datagrammi che i router tratteranno in modo prioritario



Risposta corretta.

La risposta corretta è: la capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router



Domanda 14

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Il protocollo ARP

Scegli un'alternativa:

- a. viene utilizzato ogni volta che si deve inviare un datagramma ad un host il cui indirizzo IP non compare nella tabella ARP ✓
- b. viene utilizzato solamente per raggiungere il router di default
- c. viene utilizzato solamente quando si debbano inviare datagrammi ad host raggiungibili tramite instradamento diretto

Risposta corretta.

La risposta corretta è: viene utilizzato ogni volta che si deve inviare un datagramma ad un host il cui indirizzo IP non compare nella tabella ARP

Domanda 15

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

I messaggi del protocollo OSPF

Scegli una o più alternative:

- a. vengono utilizzati per l'implementazione del protocollo di HELLO che permette ai router di scoprire i propri vicini ✓
- b. hanno tutti un'intestazione comune, seguita da informazioni specifiche che dipendono dal tipo di pacchetto ✓
- c. sono di due soli tipi REQUEST e RESPONSE

Risposta corretta.

Le risposte corrette sono: hanno tutti un'intestazione comune, seguita da informazioni specifiche che dipendono dal tipo di pacchetto, vengono utilizzati per l'implementazione del protocollo di HELLO che permette ai router di scoprire i propri vicini



Domanda 16

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

L'Internet checksum:**Scegli una o più alternative:**

- a. viene utilizzato nei vari protocolli della rete Internet quando sia necessario controllare l'errore di trasmissione ✓
- b. utilizza l'operazione di somma binaria modulo 1 ✓
- c. viene calcolato suddividendo i dati in parole di 32 bit

Le risposte corrette sono: utilizza l'operazione di somma binaria modulo 1, viene utilizzato nei vari protocolli della rete Internet quando sia necessario controllare l'errore di trasmissione

Domanda 17

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

La massima efficienza di un protocollo ARQ che trasporta trame di lunghezza $F=500$ byte di cui $H=10$ di intestazione

Scegli un'alternativa:

- a. risulta pari al 95% qualunque sia il valore della finestra
- b. Non so
- c. risulta pari al 98% qualunque sia la dimensione della finestra
- d. risulta pari al 98% solo se la finestra viene correttamente dimensionata ✓

La risposta corretta è: risulta pari al 98% solo se la finestra viene correttamente dimensionata



Domanda 18

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Secondo la logica di Internet una "network IP" e':

Scegli un'alternativa:

- a. un insieme di calcolatori che hanno interfacce di rete utilizzanti tutte il medesimo indirizzo
- b. un insieme di calcolatori che hanno interfacce di rete a cui sono attribuiti numeri IP con prefisso comune ✓
- c. un insieme di calcolatori che hanno interfacce di rete a cui sono attribuiti numeri IP con una parte dei bit avente valore "1"

Your answer is correct.

La risposta corretta è: un insieme di calcolatori che hanno interfacce di rete a cui sono attribuiti numeri IP con prefisso comune

Domanda 19

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Quali fra i protocolli elencati in seguito sono protocolli di Routing utilizzati in Internet

Scegli una o più alternative:

- a. RIP ✓
- b. BGP ✓
- c. TCP

Risposta corretta.

Le risposte corrette sono: RIP, BGP



Domanda 20

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Il Dipartimento di un ente ottiene per l'indirizzamento IP la rete 137.204.57.128/26. Ne consegue che

Scegli una o più alternative:

- a. la netmask dei relativi host va configurata al valore 255.255.255.224
- b. potrebbe scegliere come indirizzo IP del gateway di default il numero 137.204.57.129 ✓
- c. non puo' utilizzare per l'interfaccia di un host l'indirizzo IP 137.204.57.159

Risposta corretta.

La risposta corretta è: potrebbe scegliere come indirizzo IP del gateway di default il numero 137.204.57.129

Domanda 21

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

La tecnologia utilizzata per lo sviluppo della rete pubblica a larga banda detta FTTH prevede che la fibra ottica raggiunga

Scegli un'alternativa:

- a. la centrale di rete pubblica piu' vicina all'utente
- b. no so
- c. la casa dell'utente ✓
- d. gli armadi di interconnessione presenti in strada che raccolgono collegamenti da numerose unità abitative (isolati)

Your answer is correct.

La risposta corretta è: la casa dell'utente









Vai a...

[Prova punteggio ►](#)



[DASHBOARD](#) / [I MIEI CORSI](#) / [APPELLI DI FRANCO CALLEGATI](#) / [SEZIONI](#) / [RETI DI TELECOMUNICAZIONI](#) / [ESAME DEL 16/06/2021](#)

Domanda

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Iniziato Wednesday, 16 June 2021, 09:26**Stato** Completato**Terminato** Wednesday, 16 June 2021, 10:32**Tempo impiegato** 1 ora 5 min.**Valutazione** 25,50 su un massimo di 30,00 (85%)Domanda **1**

Risposta non data

Punteggio max.: 1,00

Se si vuole implementare un codice a rilevazione di errori che sia in grado di rilevare errori su un singolo bit e su due bit per trame , si può:

Se si vuole implementare un codice a rivelazione di errori che sia in grado di rilevare errori su un singolo bit e su due bit per trame, si puo':

Scegli un'alternativa:

- a. utilizzare un codice polinomiale con il polinomio generatore suggerito dall'ITU $x^{16}+x^{12}+x^5+1$
- b. utilizzare il bit di parita' dispari poiche' il bit di parita' pari non rileva errori su numeri pari di bit
- c. utilizzare un codice polinomiale con polinomio generatore $x+1$

La risposta corretta è: utilizzare un codice polinomiale con il polinomio generatore suggerito dall'ITU $x^{16}+x^{12}+x^5+1$

Domanda **2**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

La dimensione dell'indirizzo MAC utilizzato nelle LAN Ethernet ha dimensione pari a:

La dimensione dell'indirizzo MAC utilizzato nelle LAN Ethernet ha dimensione pari a

Scegli un'alternativa:

- a. 6 byte
- b. 4 byte
- c. 8 byte



La risposta corretta è: 6 byte

Domanda 3

Risposta non data

Punteggio mass.: 1,00

Con il termine "Direct Forwarding" si intende:

Con il termine "Direct Forwarding" si intende

Scegli un'alternativa:

- a. la capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router ✓
- b. la capacità di un host di inviare datagrammi che i router tratteranno in modo prioritario
- c. la capacità di un host di consegnare datagrammi interagendo direttamente con un gateway

La risposta corretta è: la capacità di un host di inviare datagrammi ad altri host della sua network senza bisogno di ricorrere ad un router

Domanda 4

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Nelle PCI del protocollo IP compaiono 16 bit dedicati al controllo dell'errore calcolati utilizzando l'Internet checksum:

Nelle PCI del protocollo IP compaiono 16 bit dedicati al controllo dell'errore calcolati utilizzando l'Internet checksum:

- a. sui soli bit dell'header (PCI) del datagramma suddivisi in parole di 16 bit ✓
- b. su tutti i bit che compongono il datagramma suddivisi in parole di 16 bit
- c. sui soli bit di dati (escludendo le PCI) che compongono il datagramma suddivisi in parole di 16 bit

La risposta corretta è:

sui soli bit dell'header (PCI) del datagramma suddivisi in parole di 16 bit

Tra due router viene configurata la rete 10.0.0.4/30. Ne consegue che:

Tra due router viene configurata la rete 10.0.0.4/30. Ne consegue che

- a. I router avranno indirizzi 10.0.0.5 e 10.0.0.6
- b. I router avranno indirizzi 10.0.0.0 e 10.0.0.4
- c. I router avranno indirizzi 10.0.0.4 e 10.0.0.5

Domanda

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

La risposta corretta è:

I router avranno indirizzi 10.0.0.5 e 10.0.0.6

Domanda **6**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Il protocollo DHCP viene utilizzato per:

Il protocollo DHCP viene utilizzato per

Scegli un'alternativa:

- a. configurare i parametri dell'interfaccia di rete di un calcolatore su una certa network IP
- b. configurare le credenziali di accesso alla rete Wi-Fi
- c. configurare il sistema operativo del calcolatore all'avvio



La risposta corretta è: configurare i parametri dell'interfaccia di rete di un calcolatore su una certa network IP

Il campo TTL nell'intestazione del datagramma IP ha dimensione pari a:

Il campo TTL nell'intestazione del dagramma IP ha dimensione pari a

Scegli un'alternativa:

- a. 16 bit
- b. 4 bit
- c. 8 bit



La risposta corretta è: 8 bit

Domanda **8**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Domanda

Rispo

Punt

Con riferimento agli Autonomous System (AS) quando si parla di peering si intende:

Con riferimento agli Autonomous System (AS) quando si parla di peering si intende

Scegli un'alternativa:

- a. un'interconnessione per scambiarsi traffico direttamente
- b. un accordo per scambiarsi informazioni di routing con opportune regole di import ed export
- c. una modalita' specifica per l'interconnessione dei router interni agli AS



La risposta corretta è: un'interconnessione per scambiarsi traffico direttamente

Domanda

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

9

or

tot

Un router SOHO è concepito per essere utilizzato:

Un router SOHO è concepito per essere utilizzato:

- a. in ambienti domestici o piccolo uffici
- b. nella rete di trasporto degli operatori
- c. nella rete di accesso degli operatori



La risposta corretta è:

in ambienti domestici o piccolo uffici

Domanda **10**

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

In una VPN funzionante in modalità roadwarrior un utente della VPN:

In una VPN funzionante in modalità roadwarrior un utente della VPN

Scegli un'alternativa:

- a. puo' collegarsi alla VPN solamente dall'interno della rete aziendale
- b. necessita di un router specifico per poter raggiungere la VPN
- c. puo' collegarsi alla VPN da un qualunque punto di Internet tramite un'opportuna procedura di autenticazione (username e password tipicamente)



La risposta corretta è: puo' collegarsi alla VPN da un qualunque punto di Internet tramite un'opportuna procedura di autenticazione (username e password tipicamente)

Domanda 1

Risposta corretta

Punteggio

Secondo la terminologia OSI una Protocol Data Unit (PDU) di livello N è composta da:

re
tt

Secondo la terminologia OSI una Protocol Data Unit (PDU) di livello N è composta da

- a. dai soli dati d'utente
- b. dal SA e dai dati d'utente
- c. Due parti denominate PCI e SDU



La risposta corretta è:

Due parti denominate PCI e SDU

Domanda 12

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Un servizio di tipo broadcast:

Un servizio di tipo broadcast

Scegli una o più alternative:

- a. se realizzato utilizzando un canale di tipo broadcast che "copre" una certa area geografica, permette la fruizione del servizio in mobilità nell'area ✓
- b. puo' essere realizzato con qualunque tipologia di canale, anche se risulta piu' efficiente utilizzare un canale broadcast ✓
- c. deve necessariamente essere realizzato con un canale punto-multipunto

Le risposte corrette sono: puo' essere realizzato con qualunque tipologia di canale, anche se risulta piu' efficiente utilizzare un canale broadcast, se realizzato utilizzando un canale di tipo broadcast che "copre" una certa area geografica, permette la fruizione del servizio in mobilità nell'area

Domanda 1

Risposta corretta

Punteggio

L'interfaccia di rete di un host ha configurato il numero IP a 192.168.20.12 ed il parametro NETMASK al valore 255.255.255.224; ne consegue che:

L'interfaccia di rete di un host ha configurato il numero IP a 192.168.20.12 ed il parametro NETMASK al valore 255.255.255.224; ne consegue che

Scegli una o più alternative:

- a. La network IP può contenere al più 30 host (oppure 29 host ed un gateway) ✓
- b. La network IP a cui appartiene l'host utilizza 5 bit per indirizzare i singoli host ✓
- c. L'indirizzo della rete a cui appartiene l'host è 192.168.20.0 ✓

Le risposte corrette sono: l'indirizzo della rete a cui appartiene l'host è 192.168.20.0, la network IP a cui appartiene l'host utilizza 5 bit per indirizzare i singoli host, la network IP può contenere al più 30 host (oppure 29 host ed un gateway)

Domanda 14

Parzialmente corretta

Punteggio ottenuto 0,50 su 1,00

Quali delle seguenti affermazioni sono corrette con riferimento all'applicazione PING:

Quali delle seguenti affermazioni sono corrette con riferimento all'applicazione PING:

Scegli una o più alternative:

- a. permette di avere una stima del Round Trip Time fra due nodi della rete Internet ✓
- b. viene implementata utilizzando il protocollo ICMP
- c. permette di misurare la distanza geografica fra due nodi della rete Internet

Le risposte corrette sono: viene implementata utilizzando il protocollo ICMP, permette di avere una stima del Round Trip Time fra due nodi della rete Internet

Domanda 1

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

5

re

0t u 0,00

Un datagramma viene inviato con TTL = 1 nell'intestazione:

Un datagramma viene inviato con TTL=1 nell'intestazione

Scegli una o più alternative:

- a. ptrebbe essere generato dall'applicazione TRACEROUTE ✓
- b. verra' bloccato nel primo router che incontra generando un messaggio di errore ICMP ✓
- c. verra' instradato dal primo router che incontra

Le risposte corrette sono: verra' bloccato nel primo router che incontra generando un messaggio di errore ICMP, ptrebbe essere generato dall'applicazione TRACEROUTE

Domanda 16

Parzialmente corretta

Punteggio ottenuto 0,50 su 1,00

In un protocollo ARQ quando il ricevitore riceve una trama:

In un protocollo ARQ quando il ricevitore riceve una trama:

- a. controlla che sia corretta verificando le PCI per la rivelazione di errore ✓
- b. qualora la trama risulti errata la scarta e può inviare al trasmettitore un messaggio di Acknowledge negativo
- c. qualora la trama risulti errata la scarta e può non fare null'altro

Le risposte corrette sono:

controlla che sia corretta verificando le PCI per la rivelazione di errore,

qualora la trama risulti errata la scarta e può non fare null'altro

7

Completo

Punteggio sicurato

Domanda 1

Il RIP è uno dei protocolli utilizzati per il routing in Internet:

Il RIP è uno dei protocolli utilizzati per il routing in Internet. Si chiede di:

1. indicare se si tratti di un protocollo di tipo Distance Vector o Link State e spiegare cosa questo significhi
2. indicare se sia un protocollo di tipo IGP o EGP spiegando cosa questo significhi
3. spiegare quale metrica venga normalmente utilizzata per il routing e se sia definito un valore massimo della distanza fra due nodi
4. dire se ne esistano più versioni oppure una sola
5. spiegare come sia strutturato un tipico messaggio RIP e se esistano diversi tipi di messaggi o meno.

RIP risulta essere la denominazione di Routing Information Protocol, è un protocollo distance vector, relativamente "vecchio" 1988. È utilizzato quasi ed esclusivamente su Reti TCP/IP.

- 1) RIP è un protocollo Distance Vector, per cui avviene una comunicazione ai nodi vicini in cui viene esplicitata la propria distanza rispetto a tutti gli altri nodi della rete.
- 2) RIP è un protocollo Interior Gateway Protocol (IGP), quindi impiegato all'interno delle AS per implementare il routing.
- 3) Il valore massimo della distanza fra due nodi è 15 "hop", essendo un protocollo distance vector, la metrica utilizzata è quella del numero di hop.
- 4) esistono più versioni di RIP, infatti all'interno del pacchetto RIP è presente un campo version in cui viene indicata appunto la versione.
- 5) I messaggi RIP sono di due tipi: REQUEST e RESPONSE. REQUEST serve per chiedere esplicitamente informazioni ai nodi vicini, RESPONSE invece viene impiegato per trasmettere informazioni di Routing come ad esempio i distance Vector. Questi messaggi sono trasportati da UDP ed utilizzano la porta 520. La struttura tipica dei messaggi racchiude i seguenti campi: command: (REQUEST o RESPONSE), version: la versione del RIP, address family identifier: tipo di indirizzo rete utilizzato, address: destinazione per la quale viene data la distanza, metrica: è la distanza dalla destinazione indicata.

8

Risposte a e rata

Punteggio ottenuto 0

Domanda 1

Il protocollo BGP viene utilizzato per gestire il routing fra gli AS. Viene detto tipo path vector. Questo significa che:

Il protocollo BGP viene utilizzato per gestire il routing fra gli AS. Viene detto di tipo path vector. Questo significa che

- a. i router quando vedono un'informazione di router in cui compare il loro AS la ignorano onde evitare cicli ✓
- b. i messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la lista degli AS che vanno attraversati per raggiungerli ✓
- c. i messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la distanza da tutti gli AS noti ✗

Le risposte corrette sono: i messaggi che si scambiano i router che utilizzano questo protocollo riportano la lista delle reti di un AS e la lista degli AS che vanno attraversati per raggiungerli,
i router quando vedono un'informazione di router in cui compare il loro AS la ignorano onde evitare cicli

Domanda 19

Risposta corretta

Punteggio ottenuto 1,00 su 1,00

Quando si parla dei soggetti coinvolti nella realizzazione dell'architettura della rete Internet si parla fra gli altri di ISP e IXP. Quale delle seguenti affermazioni sono corrette al riguardo.

Quando si parla dei soggetti coinvolti nella realizzazione dell'architettura della rete Internet si parla fra gli altri di ISP e IXP. Quale delle seguenti affermazioni sono corrette al riguardo:

Scegli una o più alternative:

- a. IXP e' acronimo di Internet Exchange Point ✓
- b. gli ISP sono le amministrazioni statali che decidono sulle politiche da applicare alla rete Internet in una nazione
- c. ISP e IXP sono di fatto acronimi diversi per identificare i medesimi soggetti.

La risposta corretta è: IXP e' acronimo di Internet Exchange Point

20

Risposta corretta

Punteggio ottenuto 1 su ,00

Quali di questi campi sono contenuti nei pacchetti di tipo Link State prodotti dal protocollo OSPF:

Quali di questi campi sono contenuti nei pacchetti di tipo Link State prodotti dal protocollo OSPF

Scegli una o più alternative:

- a. Età del pacchetto ✓
- b. Numero di sequenza ✓
- c. Indirizzo del destinatario

Le risposte corrette sono: Età del pacchetto, Numero di sequenza

Domanda 21

Parzialmente corretta

Punteggio ottenuto 0,50 su 1,00

Nella terminologia OSPF un ABR è:

Nella terminologia OSPF un ABR è'

Scegli una o più alternative:

- a. un router che ha almeno un'interfaccia connessa alla propria area ed un'interfaccia connessa all'area di backbone o ad un'altra area ✓
- b. un router che interconnette fra loro tutte le aree dell'AS
- c. un router che annuncia verso il resto dell'AS gli indirizzi IP delle reti facenti parte della propria area

Le risposte corrette sono: un router che ha almeno un'interfaccia connessa alla propria area ed un'interfaccia connessa all'area di backbone o ad un'altra area, un router che annuncia verso il resto dell'AS gli indirizzi IP delle reti facenti parte della propria area

◀ Esame del 28/01/2021 Turno 1

Vai a...

Prova punteggio ►

Domanda 1

Risposta non ancora data

Punteggio max.: 1,00

▼ Contrassegna domanda

Qualora si utilizzi in una rete un protocollo di routing di tipo flooding
Qualora si utilizzi in una rete un protocollo di routing di tipo flooding

Scegli una o più alternative:

- a. ciascun nodo di commutazione deve assolutamente ritrasmettere un pacchetto sul collegamento da cui lo ha ricevuto
- b. tutte le possibili destinazioni vengono sicuramente raggiunte dai pacchetti
- c. si ottiene il corretto instradamento dei pacchetti con l'utilizzazione minima possibile delle risorse di rete

Domanda 2

Risposta non ancora data

Punteggio max.: 1,00

▼ Contrassegna domanda

Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si puo' dire che
Confrontando i protocolli Distance Vector (DV) con quelli Link State (LS) si puo' dire che

Scegli una o più alternative:

- a. I Distance Vector si adattano piu' velocemente ai cambiamenti della rete
- b. I Distance Vector richiedono maggior potenza di elaborazione
- c. I Link State richiedono piu' memoria nel router

Domanda 3

Risposta non ancora data

Punteggio max.: 1,00

▼ Contrassegna domanda

Secondo la terminologia Wi-Fi un ESS
Secondo la terminologia Wi-Fi un ESS

Scegli un'alternativa:

- a. Non so
- b. e' un sistema di piu' access point funzionanti come un'unica LAN
- c. e' la stazione base di una LAN infrastrutturata
- d. e' una particolare tipologia di stazione wireless con caratteristiche estese rispetto alle altre della LAN

Domanda 4

Risposta non ancora data

Punteggio max.: 1,00

▼ Contrassegna domanda

Stazioni Ethernet che appartengono al medesimo dominio di collisione
Stazioni Ethernet che appartengono al medesimo dominio di collisione

Scegli una o più alternative:

- a. sono tipicamente collegate tramite uno switch
- b. se tramattono contemporaneamente danno luogo a collisione
- c. sono tipicamente collegate tramite un hub

Domanda 5

Risposta non ancora data

Punteggio max.: 1,00

▼ Contrassegna domanda

Un host appartenente ad una rete connessa

Un host appartenente ad una rete connessa ad Internet tramite un NAT ha attribuito all'interfaccia di rete l'indirizzo 192.168.0.1 ed ha attiva una connessione sulla porta TCP 51321

Scegli un'alternativa:

- a. nei datagrammi che riceve da trasmettere su Internet per la connessione il NAT deve necessariamente modificare il numero IP sorgente e, in funzione del tipo di configurazione e delle connessioni esistenti, potrebbe modificare il numero di porta sorgente

Risposta non ancora data
Punteggio max.: 1,00

▼ Contrassegna domanda

Le grandi reti di telecomunicazioni geografiche hanno tipicamente una topologia

- a. di tipo gerarchico in cui si può distinguere una sezione cosiddetta di accesso tipicamente con topologia a stella ed una sezione cosiddetta di trasporto con topologia a maglia
- b. Non so
- c. di tipo a stella
- d. di tipo gerarchico in cui si può distinguere una sezione cosiddetta di accesso tipicamente con topologia a maglia ed una sezione cosiddetta di trasporto con topologia a stella

Le grandi reti di telecomunicazioni geografiche hanno tipicamente una topologia

Domanda 7
Risposta non ancora data

Punteggio max.: 1,00
▼ Contrassegna domanda

In un collegamento IPSec tunnel mode
In un collegamento IPSec tunnel mode

Scegli un'alternativa:

- a. viene cifrato solamente il contenuto dei datagrammi IP
- b. viene cifrata solamente l'intestazione dei datagrammi IP
- c. Non so

d. viene cifrato sia il contenuto sia l'intestazione dei datagrammi IP

Domanda 8
Risposta non ancora data
Punteggio max.: 30,00
▼ Contrassegna domanda

Al fine di poter inviare e ricevere dati su Internet un calcolatore (host) deve avere almeno una interfaccia di rete configurata per utilizzare il protocollo IP. La configurazione e' determinante per il corretto funzionamento della connessione di rete. A tale proposito si chiede di dire:

1. quali siano i parametri dell'interfaccia che devono assolutamente essere configurati e quale sia lo loro funzione
2. quale tipo di connettività sia disponibile all'host qualora questi siano gli unici parametri configurati
3. quale o quali altri parametri sia possibile configurare e a quale fine
4. se tale configurazione sia necessariamente da impostare a mano oppure se esista un metodo automatico per impostarla, nel caso specificando come sia implementato
5. se la configurazione di una scheda possa essere automaticamente applicata anche ad altre schede di rete dell'host.



Domanda 9
Risposta non ancora data
Punteggio max.: 1,00
▼ Contrassegna domanda

Quale fra i seguenti e' un indirizzo valido per un host in una rete IP con numerazione privata
Quale fra i seguenti e' un indirizzo valido per un host in una rete IP con numerazione privata

Scegli un'alternativa:

- a. 137.256.121.0
- b. 0.1.220.198

c. 192.168.1.1

Domanda 10
Risposta non ancora data
Punteggio max.: 1,00
▼ Contrassegna domanda

Servizi quali la posta elettronica, whatts, telegram

Servizi quali la posta elettronica, whatts, telegram ecc. secondo la tassonomia dei servizi ITU sono classificabili come:

- a. interattivi con scambio dell'informazione in tempo differito con memorizzazione
- b. distributivi con controllo di presentazione
 - c. Non so
 - d. interattivi con scambio dell'informazione in tempo reale

Domanda 11
Risposta non ancora data
Punteggio max.: 1,00
▼ Contrassegna domanda

In un codice polinomiale il polinomio generatore

In un codice polinomiale il polinomio generatore

Scegli una o più alternative:

- a. determina il numero minimo di bit da dedicare al controllo dell'errore nelle PCI
 - b. determina le capacita' di rilevazione dell'errore
- c. deve essere noto a priori a ricevitore e trasmettitore

Domanda 12
Risposta non ancora data
Punteggio max.: 1,00
▼ Contrassegna domanda

L'applicazione PING:
L'applicazione PING:

Scegli una o più alternative:

- a. Serve per controllare se un host IP e' raggiungibile su Internet.
 - b. Serve per misurare le dimensioni di una rete
- NO** c. Serve per riconoscere il percorso fra una rete e l'altra

Domanda 13
Risposta non ancora data
Punteggio max.: 1,00
▼ Contrassegna domanda

Se consideriamo la network IP 192.168.1.0/27 possiamo dire che:

Se consideriamo la network IP 192.168.1.0/27 possiamo dire che:

Scegli una o più alternative:

- a. un host della rete puo' avere indirizzo 192.168.1.10
- b. potrei attribuire al default gateway della rete il numero IP 192.168.1.30

FORSE C

Punteggio max:
1,00
▼ Contrassegna
domanda

della rete Internet si parla fra gli altri di ISP e IXP. Quale delle seguenti affermazioni sono corrette al riguardo:

Scegli una o più alternative:

- a. IXP e' acronimo di Internet Exchange Point
- b. ISP e IXP sono di fatto acronimi diversi per identificare i medesimi soggetti.
- c. gli ISP sono le amministrazioni statali che decidono sulle politiche da applicare alla rete Internet in una nazione

Domanda 15

Risposta non
ancora data

Punteggio max:
1,00

▼ Contrassegna
domanda

Quali delle seguenti affermazioni sono pertinenti se si considera un Internet Service Provider
Quali delle seguenti affermazioni sono pertinenti se si considera un Internet Service Provider

- a. e' un soggetto economico che fornisce a pagamento interconnessioni intercontinentali ad altri gestori di rete
- b. e' un soggetto economico che fornisce a pagamento l'accesso alla rete Internet agli utenti finali
- c. ha un'infrastruttura presente sul territorio in particolari punti detti Point of Presence o PoP

Domanda 16

Risposta non
ancora data

Punteggio max:
1,00

▼ Contrassegna
domanda

All'interfaccia di rete di un calcolatore

All'interfaccia di rete di un calcolatore e' attribuito un certo numero IP. Per determinare il Network ID corrispondente, secondo le regole dell'indirizzamento CLASSFULL (precedente al CIDR)

Scegli un'alternativa:

- a. e' sufficiente interpretare correttamente i primi bit dell'indirizzo
- b. e' necessario utilizzare la NETMASK
- c. e' necessario utilizzare il DEFAULT GATEWAY

Domanda 17

Risposta non
ancora data

Punteggio max:
1,00

▼ Contrassegna
domanda

I protocolli della famiglia Link State

I protocolli della famiglia Link State

Scegli un'alternativa:

- a. Richiedono che ogni router conosca a priori la distanza dai suoi vicini
- b. Non so
- c. Prevedono che ogni router trasmetta ai propri vicini la propria distanza da tutti i nodi della rete
- d. Prevedono che ogni router trasmetta a tutti i nodi della rete la propria distanza dai vicini

Domanda 18

Risposta non
ancora data

Punteggio max:
1,00

▼ Contrassegna
domanda

Un protocollo ARQ a finestra scorrevole che trasmette su di un collegamento di capacità C, trame di dimensione pari a F bit di cui D di dati di utente e H di PCI

Scegli un'alternativa:

Domanda 19

Risposta non ancora data

Punteggio max:
1,00

▼ Contrassegna domanda

La dimensione dell'indirizzo MAC utilizzato nelle LAN Ethernet ha dimensione pari a
La dimensione dell'indirizzo MAC utilizzato nelle LAN Ethernet ha dimensione pari a

Scegli un'alternativa:

a. 6 byte

b. non so

c. 4 byte

d. 8 byte

Domanda 20

Risposta non ancora data

Punteggio max:
1,00

▼ Contrassegna domanda

Il protocollo BGP

Il protocollo BGP

Scegli una o più alternative:

a. E' usato come Interior Gateway Protocol

b. Garantisce l'assenza di cicli nella determinazione delle rotte

c. E' un protocollo di tipo Path Vector

Termina il tentativo...

prova

Vai a...



©Copyright 2020 - ALMA MATER STUDIORUM - Università di Bologna - Via Zamboni, 33 - 40126 Bologna - Partita IVA: 01131710376

[Informativa sulla Privacy](#) [Informativa per l'uso dei cookie](#)

[CALL-30946-2019](#)