Appunti di Sistemi Operativi e Reti

Domande e risposte – Parte di Reti (Network)

Capitolo 4 – Livello di rete: Piano dei Dati

1) Cosa si intende per router?

Si definisce router un dispositivo hardware che si occupa di inoltrare ed instradare i pacchetti tra reti diverse, gestendo il traffico di dati tra computer, dispositivi e reti.

2) Quali sono le funzionalità del network layer?

Le funzionalità del livello di rete sono:

→ forwarding: sposta i pacchetti dal collegamento di input di un router al collegamento di output appropriato del router;

→ routing: determina il percorso intrapreso dai pacchetti dalla sorgente alla destinazione.

3) Differenza tra piano dei dati e piano di controllo

Il piano dei dati determina come il datagramma in arrivo sulla porta di input del router viene inoltrato alla porta di output del router, mentre il piano di controllo determina come il datagramma viene instradato tra i router lungo il percorso end-to-end dall'host di origine all'host di destinazione.

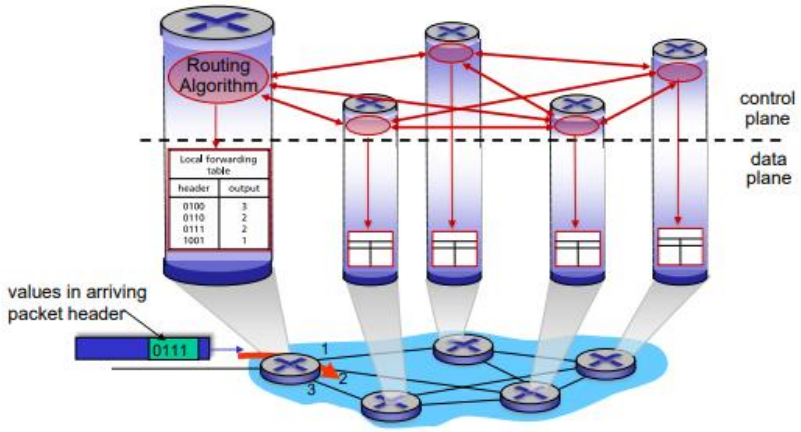
Vengono utilizzati due approcci:

→ algoritmi di routing tradizionali: implementati nel router;

→ software – defined networking (SDN): implementato in un server remoto.

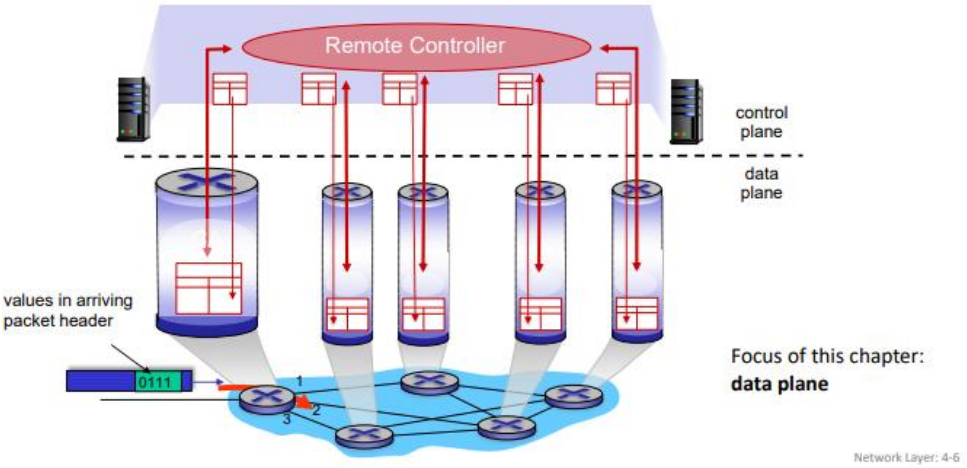
4) Caratteristiche del piano di controllo per router

I singoli componenti dell'algoritmo di routing in ogni singolo router interagiscono nel piano di controllo.



5) Caratteristiche del Software – Defined Networking (SDN)

Il controller remoto computa e installa tabelle di forwarding nei routers.



6) Cosa è e quali sono le caratteristiche del Network Service Model?

Il Network Service Model è un concetto fondamentale nella progettazione e nell'implementazione delle reti di telecomunicazioni che si riferisce alla struttura e alle funzionalità che il servizio di rete offre agli utenti e alle applicazioni. Essa ha le seguenti caratteristiche:

→ Trasparenza: il modello di servizio di rete deve essere trasparente agli utenti finali, il che significa che questi non devono preoccuparsi dei dettagli tecnici su come i dati vengono trasportati attraverso la rete (esempio sistemi distribuiti).

→ Affidabilità: un buon modello di servizio di rete deve garantire che i dati vengano consegnati in modo affidabile. Questo implica la capacità di rilevare e correggere gli errori durante la trasmissione e di gestire eventuali perdite di pacchetti.

→ Scalabilità: il modello deve essere scalabile, ossia deve poter crescere e adattarsi all'aumento del numero di utenti e del volume di dati senza compromettere le prestazioni.

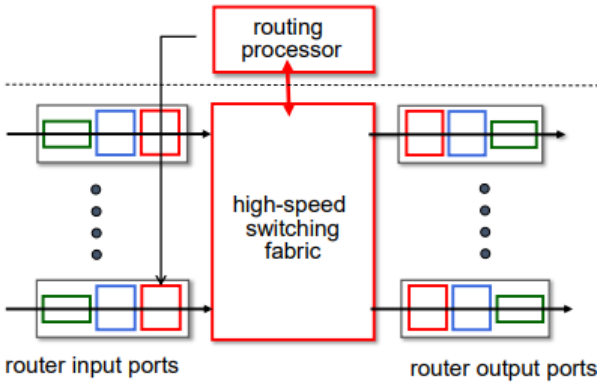
→ Efficienza: il modello deve essere efficiente nell'utilizzo delle risorse di rete, come la larghezza di banda e la capacità di elaborazione. Questo implica l'ottimizzazione dei protocolli di comunicazione e la gestione delle risorse in modo da minimizzare i ritardi e massimizzare il throughput.

→ Sicurezza: la sicurezza è un aspetto critico del modello di servizio di rete. Questo include la protezione dei dati durante la trasmissione attraverso tecniche di crittografia, l'autenticazione degli utenti e il controllo degli accessi per prevenire usi non autorizzati della rete.

→ Qualità del Servizio (QoS): la rete deve essere in grado di fornire diversi livelli di qualità del servizio, a seconda delle esigenze delle diverse applicazioni. Ad esempio, le applicazioni in tempo reale come la voce e il video richiedono una bassa latenza e una minima variazione del ritardo (jitter), mentre le applicazioni di trasferimento file possono tollerare ritardi maggiori.
→ Indipendenza dal Supporto Fisico: il modello di servizio deve essere indipendente dal supporto fisico utilizzato per la trasmissione dei dati. Che si tratti di fibra ottica, cavi di rame, o comunicazioni wireless, il servizio di rete deve poter operare su diversi tipi di infrastrutture fisiche senza modifiche significative.
→ Flessibilità: il modello deve essere flessibile per adattarsi alle diverse tecnologie e protocolli di rete. Deve supportare una vasta gamma di servizi e applicazioni, nonché consentire l'integrazione di nuove tecnologie man mano che diventano disponibili.
→ Manutenibilità: il modello deve essere progettato in modo da facilitare la manutenzione e l'aggiornamento della rete.
→ Interoperabilità: la rete deve essere interoperabile, il che significa che deve essere in grado di funzionare con altre reti e sistemi di comunicazione.

7) Illustrare l'architettura di un router

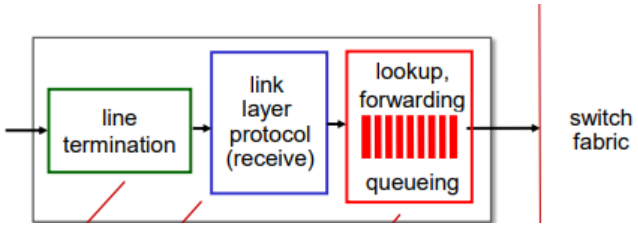
Ecco una rappresentazione ad alto livello di un router



8) Quali sono le funzioni delle porte in input del router?

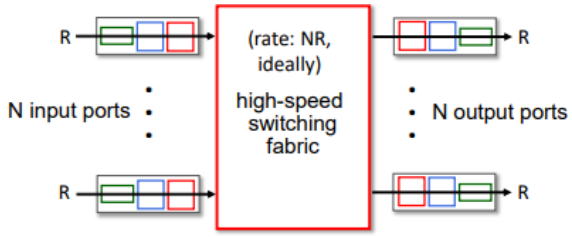
Le funzioni sono:
→ layer fisico: ricezione del bit – level;
→ link layer: come Ethernet;
→ switching decentralizzato: utilizza i valori negli header, trova la porta di output in base alla tabella di forwarding e se i datagrammi arrivano troppo velocemente, allora vengono accodati in una input port queuing. Viene

effettuato il forward destination based in base al solo indirizzo IP di destinazione.



9) Che ruolo possiede lo switching fabrics?

Lo switching fabrics trasferisce i pacchetti da un input link verso l'appropriato output link.

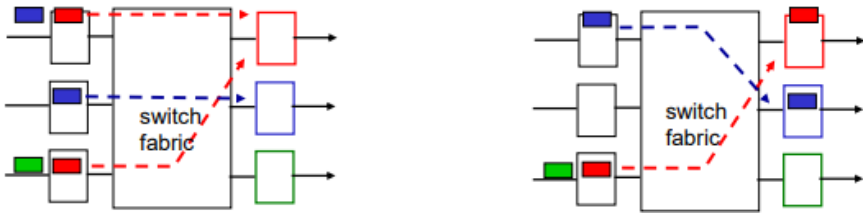


10) Cosa si inttende per switching rate?

Si definisce switching rate la frequenza con la quale i pacchetti sono trasferiti.

11) Descrivere le caratteristiche dell'input port queuing e definire HOL blocking

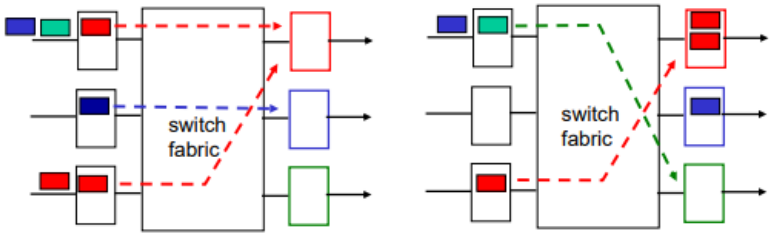
Nell'input port queuing i pacchetti in arrivo vengono accodati presso la porta di ingresso prima di essere elaborati e instradati verso la destinazione appropriata ed offre semplicità di implementazione e riduzione del buffering alle porte di uscita, ma presenta il rischio di HOL blocking e può limitare la scalabilità del sistema. Il HOL (Head-of-Line) blocking è un fenomeno che può verificarsi in una coda di pacchetti in una rete di computer, dove un pacchetto in testa alla coda (head-of-line) impedisce agli altri pacchetti dietro di esso di essere processati o trasmessi, anche se questi potrebbero essere instradati immediatamente.



12) Descrivere le caratteristiche dell'output port queuing

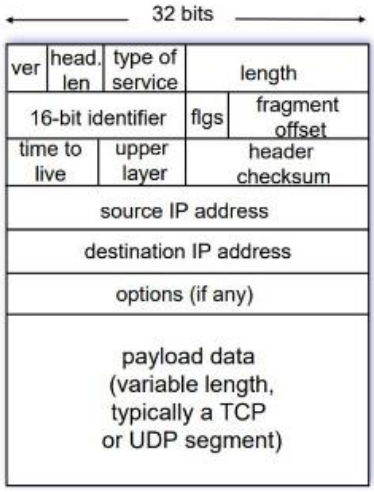
L'output port queuing rappresenta una coda di output che può essere geestita mediante:

→ buffering: usata quando i datagrammi arrivano dal fabric più velocemente del link transmission rate e i datagrammi possono essere persi (drop policy);
→ scheduling discipline: viene scelto un datagramma da trasmettere (priority scheduling).



13) Quali sono i componenti di un datagramma IP

I componenti sono:
→ ver: la versione (IPv4 o IPv6);
→ head len: lunghezza header;
→ length: lunghezza del datagramma totale;
→ type of service: qualità del servizio;
→ TTL (time to live): un valore intero che viene decrementato di uno al passaggio di ogni router e viene inizialmente impostato a 255;
→ upper layer: effettua l'operazione di multiplexing e demultiplexing verso il livello di trasporto e indirizza il datagramma verso il protocollo corretto TCP o UDP;
→ header checksum: intestazione dedicata al checksum (non per il payload);
→ indirizzo IP sorgente: l'indirizzo IP della sorgente;
→ indirizzo IP destinazione: l'indirizzo IP della destinazione;
→ opzioni: se non si considerno le opzioni si avrà una introduzione di overhead con 20 Bytes di TCP, 20 Bytes IP e application layer TCP + IP.



14) Cosa si intende per indirizzo IP (Internet Protocol)?

Si definisce indirizzo IP (Internet Protocol) un identificatore numerico assegnato a ciascun dispositivo (host, router e anche switch per scopi di configurazione o accesso remoto) collegato a una rete informatica che utilizza il protocollo Internet per la comunicazione. La versione 4 (IPv4) utilizza la notazione decimale puntata e consistono in quattro ottetti (4 byte o 32 bit), ciascuno separato da un punto e ogni ottetto può avere un valore compreso tra 0 e 255.

Esempio:

```
Indirizzo IPv4. . . . . . . . . . . . : 192.168.1.42
Subnet mask . . . . . . . . . . . . . : 255.255.255.0
Gateway predefinito . . . . . . . . . : 192.168.1.1
```

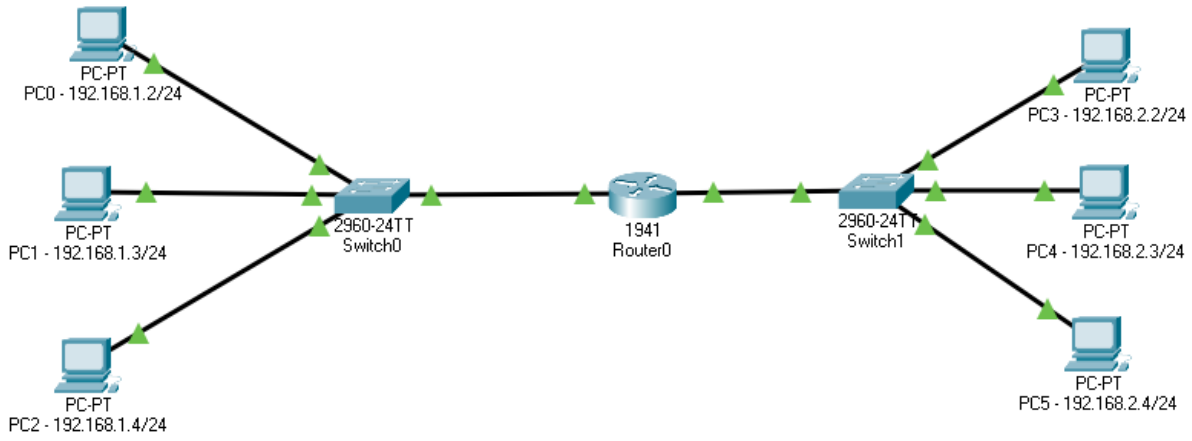
192.168.1.41 = 11000000.10101000.00000001.00101001
255.255.255.0 = 11111111.11111111.11111111.00000000
192.168.1.1 = 11000000.10101000.00000001.00000001

15) Cosa si intende per interfaccia di rete?

Un'interfaccia di rete è un componente hardware o software che permette a un dispositivo, come un computer o un router, di connettersi a una rete e comunicare con altri dispositivi. Le interfacce di rete sono essenziali per il funzionamento delle reti di computer, poiché gestiscono la trasmissione e la ricezione dei dati tra i dispositivi.

16) Cosa si intende per sottorete?

Si definisce sottorete (o subnet) na porzione logica di una rete IP più grande. Le sottoreti consentono di organizzare e ottimizzare la rete in segmenti più piccoli, migliorando la gestione del traffico, la sicurezza e l'efficienza dell'uso degli indirizzi IP.



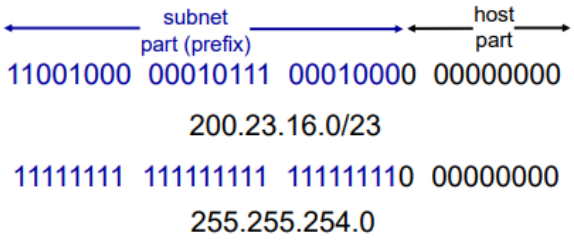
Le carattteristiche e il funzionamento delle sottoreti è dovuto a:
→ Indirizzo IP: indirizzo univoco assegnato ad un dispositivo host connesso in rete.

```
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:47FF:FE61:7E1C
   IPv6 Address.....: ::
   IPv4 Address.....: 192.168.1.2
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                                 192.168.1.1
```

→ Subnet Mask: determina quale parte dell'indirizzo IP identifica la rete e quale parte identifica il dispositivo all'interno della rete. L'indirizzo IP infatti è formato da: Subnet Part + Host Part.

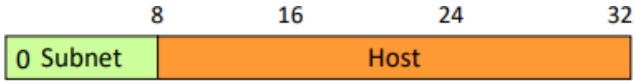
17) Cosa significa CIDR (Classless Inter Domain Router)?

Si definisce CIDR (Classless Inter Domain Router) un metodo utilizato per allocare e specificare indirizzi IP e instradamenti IP in modo più flessibile rispetto al sistema di classi di rete tradizionale (Classful Networking). Esso è stato introdotto per affrontare il problema dell'esaurimento degli indirizzi IPv4 e per migliorare l'efficienza del routing su Internet. Esso ha il formato a.b.c.d/x dove x indica il numero di bit utilizzati dalla Subnet Part.



18) Quali sono le classi degli indirizzi IP?

Le classi degli indirizzi IP sono:
→ Classe A: indirizzi da 0.0.0.0 a 127.255.255.255



→ Classe B: indirizzi da 128.0.0.0 a 191.255.255.255

→ Classe C: indirizzi da 192.0.0.0 a 223.255.255.255

19) Quali sono le categorie degli indirizzi IP speciali?

Le categorie degli indirizzi IP speciali sono:
→ Subnet address: indirizzi IP con host part pari a 0 (esempio 193.17.31.0/24).

→ Direct broadcast address: indirizzi IP che identificano tutti gli host (esempio 193.17.31.255/24).
→ Limited broadcast address: indirizzi IP che identificano il broadcast nella stessa rete, che non viene inoltrato (esempio 255.255.255.255).

20) Come può un host ottenere un indirizzo IP?

Un indirizzo IP può essere ottenuto mediante:
→ configurazione statica: l'indirizzo IP viene impostato manualmente dall'utente o dall'amministratore di rete;
→ DHCP (Dynamic Host Configuration Protocol): gli host ottengono dinamicamente l'indirizzo IP da un server quando accedono alla rete.
I passaggi per ottenere un indirizzo IP tramite DHCP sono:
→ DHCP DISCOVER: cerca un server DHCP;
→ DHCP OFFER: il server risponde con un indirizzo IP;
→ DHCP REQUEST: l'host accetta l'indirizzo IP;
→ DHCP ACK: il server conferma l'assegnazione.

21) Cosa si intende per NAT? Come avviene la sua implementazione?

Si definisce NAT (Network Address Translation) una tecnologia utilizzata nei router e nei firewall per modificare le informazioni sugli indirizzi IP nei pacchetti di rete mentre questi attraversano un dispositivo di rete. Viene utilizzata principalmente per conservare gli indirizzi IP pubblici per migliorare la sicurezza della rete. L'implementazione avviene come segue:
→ ai datagrammi in uscita viene cambiato il source IP e la porta con il NAT IP e nuova porta;
→ viene utilizzata la NAT translation table per salvarne la traduzione;
→ ai datagrammi in entrata viene applicato il processo inverso (sempre grazie alla tabella di traduzione).

Capitolo 5 – Livello di rete: Piano di Controllo

22) Qual è lo scopo dell'algoritmo di routing?

Lo scopo dell'algoritmo di routing è quello di determinare i path o i cammini da una sorgente a una destinazione attraverso una rete.

23) Cosa si intende per cammino (o path)?

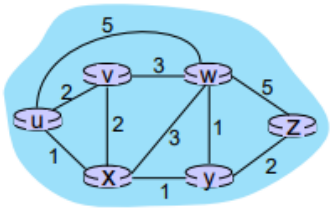
Si definisce cammino (o percorso) una sequenza di router che il pacchetto deve attraversare da una sorgente a una destinazione.

24) Che ruolo ha un protocollo di routing?

Il protocollo di routing ha lo scopo di determinare la modalità con la quale le informazioni devono essere condivise tra i router per l'esecuzione degli algoritmi di routing.

25) Caratteristiche del grafo di astrazione relativo ad una rete

Una rete può essere rappresentata mediante un grafo, in cui ogni link diretto ha un costo (viene utilizzato ∞ per indicare l'inesistenza del link).



Sia N l'insieme dei router e sia E l'insieme dei link con

N = {u, v, w, x, y, z}

E = {(u,v), (u,x), (v,x), (v,w), (x,w), (x,y), (w,y), (w,z), (y,z)}

Esempio:

$c_{w,z} = 5$

$c_{u,z} = \infty$

26) Come vengono classificati gli algoritmi di routing?

Gli algoritmi di routing vengono classificati in:

→ globali: tutti i router conoscono la rete e i costi dei link (link state);

→ decentralizzati: iterativo e viene effettuato lo scambio di informazioni solo con i vicini (distance vector);

→ statici: in cui risulta rara la modifica delle route nel tempo;

→ dinamici: in cui la modifica delle route risulta essere periodica.

27) Descrivere l'algoritmo distance vector

L'algoritmo distance vector si basa sull'implementazione dell'equazione di Bellman – Ford:

$dist(A, X) = \min \{dist(V, X) + c(A, V)\}$

Le caratteristiche dell'algoritmo sono:

→ di volta in volta, ogni nodo invia la sua stima del distance vector ai vicini;

→ quando un router riceve una stima distance vector, aggiorna anche la propria;

→ la distanza stimata converge al costo minore.

L'algoritmo distance vector è:

→ iterativo: viene applicato in ogni nodo;

→ asincrono: non ci deve essere sincronizzazione;

→ distribuito: è presente in ogni router;
→ terminante: se non ci sono aggiornamenti, nessuno fa nulla.

28) Descrivere l'algoritmo link state

L'algoritmo link state è stato implementato in modo tale che ogni router deve comunicare in broadcast il proprio link state agli altri router. Esso ha le seguenti caratteristiche:
→ distribuzione in "selective flooding" delle informazioni relative alla topologia di rete;
→ utilizza l'algoritmo di Dijkastra;
→ centralizzato, ossia tutti i nodi hanno le informazioni;
→ si basa su una forwarding table;
→ iterativo: dopo k iterazioni, conosce il costo minore per k destinazioni.

29) Differenze tra distance vector e link state

Distance Vector	Link State
Semplice e intuitivo	Selective flooding
Pochi messaggi scambiati	Molti messaggi scambiati
Lenta convergenza	Robusto e convergenza
Protocollo BGP	Protocollo OSPF, IS – IS

30) Descrivere la scalabilità della rete

La scalabilità della rete a livello di rete (piano di controllo) riguarda la capacità della rete di crescere e gestire un aumento del carico di lavoro senza compromettere le prestazioni o la stabilità. Per permettere ciò è possibile aggregare la rete in regioni chiamate "sistemi autonomi" o domini, in due tipi:
→ intra – AS routing nella stessa AS: esiste un gateway router per comunicare con altri sistemi autonomi;
→ inter – AS routing tra AS: comunicazione tra gateway router.

31) Cosa si intende per Inter – AS routing?

Si definisce Inter – AS routing, un tipo di aggregazione in cui il router propaga agli altri le informazioni sulle reti raggiungibili.

32) Cosa si intende per Intra – AS routing?

Si definisce Intra – AS routing, un tipo di aggregazione in cui vengono utilizzati i protocolli detti IGP (Interior Gateway Protocol), e possono essere:
→ RIP (Routing Information Protocol): di tipo distance – vector ed è uno dei protocolli più antichi e semplici utilizzati per la gestione delle informazioni di

routing nelle reti IP.
→ EIGRP (Enhanced Interior Gateway Routing Protocol): protocollo di routing avanzato sviluppato da Cisco, noto per le sue caratteristiche che combinano i vantaggi dei protocolli di routing distance vector e link state.
→ OSPF (Open Shortest Path First): protocollo di tipo link – state in cui ogni router propaga il proprio link state agli altri router e conosce lo stato della rete.

33) OSPF gerarchico: definizione

Si definisce OSPF gerarchico, l'approccio OSPF basato su due livelli local area e backbone, in cui ogni nodo conosce la direzione per raggiungere altre destinazioni.

34) Definire il BGP (Border Gateway Protocol)

Si definisce BGP (Border Gateway Protocol) un protocollo che consente alle subnet difare conoscere la propria esistenza e le destinazioni raggiungibili al resto della rete. Si hanno due tipi di protocolli BGP:
→ eBGP: ottiene le informazioni dalle vicine AS;
→ iBGP: propaga le informazioni ottenute ai router interni alla AS.

35) Quali sono le differenze di protocollo intra e inter?

I protocolli usati nelle intra e nelle inter sono differenti sulla base di:
→ Privacy: in cui
a) inter: l'admin ha il controllo sul traffico e su chi lo genera;
b) intra: policy più "leggere".
→ Scale: che riducono il traffico di upaate e la grandezza delle tabelle.
→ Performance: in cui
a) inter: la policy ha ha meglio sulle performance;
b) intra: si pwò concentrare solle performance.

36) Cosa si intende per ICMP?

Il protocollo ICMP (Internet Control Message Protocol) è un protocollo di rete utilizzato per diagnosticare problemi di comunicazione in reti IP e per generare messaggi di errore quando i pacchetti IP non riescono a raggiungere la loro destinazione.

Esempio:

```
gianl@DESKTOP-BU3868V MINGW64 ~
$ ping 142.251.209.4

Esecuzione di Ping 142.251.209.4 con 32 byte di dati:
Risposta da 142.251.209.4: byte=32 durata=12ms TTL=115
Risposta da 142.251.209.4: byte=32 durata=12ms TTL=115
Risposta da 142.251.209.4: byte=32 durata=13ms TTL=115
Risposta da 142.251.209.4: byte=32 durata=13ms TTL=115

Statistiche Ping per 142.251.209.4:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 12ms, Massimo =  13ms, Medio =  12ms
```

37) Cosa si intende per traceroute?

Traceroute è un comando di diagnostica di rete utilizzato per determinare il percorso che i pacchetti di dati seguono attraverso una rete IP per raggiungere una destinazione specifica. Le operazioni eseguite per computare il comando sono le seguenti:

→ la source invia un set di segmenti UDP alla destinazione e ogni router incontrato sul percorso elimina il datagramma e risponde con un ICMP 11, code 0;

→ la destinazione raggiunta risponde con un ICMP type 3, code 3 – "port unreachable";

→ la source registra il RTT di ogni pacchetto;

→ le risposte possono contenere informazioni come il nome del router che risponde e il suo indirizzo IP.

```
gianl@DESKTOP-BU3868V MINGW64 ~
$ tracert 142.251.209.4

Traccia instradamento verso mil04s50-in-f4.1e100.net [142.251.209.4]
su un massimo di 30 punti di passaggio:

  1     3 ms     3 ms     3 ms  modemtim.homenet.telecomitalia.it [192.168.1.1]
  2     *        *        *     Richiesta scaduta.
  3     9 ms     9 ms     9 ms  172.17.184.228
  4    10 ms     9 ms     9 ms  172.17.185.26
  5    12 ms    13 ms    12 ms  172.19.184.82
  6    26 ms    12 ms    61 ms  172.19.177.60
  7    11 ms    10 ms    11 ms  195.22.205.116
  8    14 ms    12 ms    12 ms  74.125.146.168
  9    12 ms    12 ms    11 ms  72.14.238.234
 10    13 ms    13 ms    13 ms  142.251.235.173
 11    13 ms    13 ms    13 ms  mil04s50-in-f4.1e100.net [142.251.209.4]

Traccia completata.
```

Capitolo 6 – Livello di Collegamento e Reti Locali

38) Cosa si intende per collegamento?

Si definisce collegamento un canale di comunicazione che connette le interfacce di endpoint adiacenti di una rete che può essere di tre tipologie:

→ via cavo (straight through o cross over);

→ wireless (onde radio o Wi-Fi);

→ optical fiber.

39) Come vengono denominati i pacchetti a livello 2 (collegamento)?

I pacchetti a livello di collegamento vengono denominati frame o trame (che incapsulano datagrammi).

40) Quali sono i servizi del livello di collegamento?

I servizi del livello di collegamento sono:
→ incapsula i datagrammi in frame, aggiungendo l'header (detto framing);
→ controlla l'accesso ai canali (nel caso in cui il mezzo fisico è condiviso tra diversi host);
→ consegna affidabile tra nodi vicini (link wireless hano un rate di errore maggiore);
→ controlla di flusso;
→ controllo e correzione degli errori (effettuata mediante EDC);
→ comunicazione half duplex o full duplex.

41) Quali sono le due tipologie di collegamento fisico?

Si hanno due tipologie di collegamento fisico:
→ point to point: collegamento diretto che connette ad esempio l'interfaccia di un end device all'interfaccia di uno switch;
→ broadcast: canale condiviso tra diversi host, come canale radio (Wi – Fi) o 4G e 5G oppure reti Ethernet.

42) Descrivere il Multiple Access Protocols

Un protocollo di accesso multiplo è un insieme di regole e procedure che gestisce l'uso condiviso di un mezzo di comunicazione da parte di più dispositivi o nodi in una rete. Questi protocolli sono essenziali per evitare collisioni e garantire che i dati siano trasmessi in modo efficiente e senza interferenze.

43) Quali sono le tre categorie diverse di protocolli ad accesso multiplo?

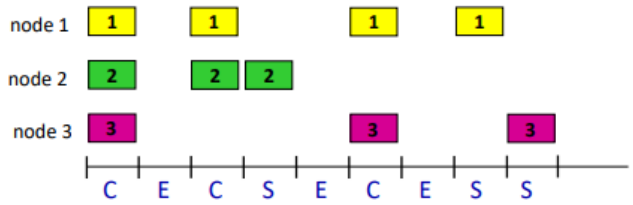
Le tre categorie di protocolli ad accesso multiplo sono:
→ partizionamento del canale: partizione del canale ad uso esclusivo di un singolo nodo;
→ random access protocol: nesson controllo, le collisioni vengono risolte e tali protocolli sfruttano questo meccanismo: slotted ALOHA, ALOHA puro, CSMA (Carrier Sense Multiple Access), CSMA/CD (Carrier Sense Multiple Access/Collision Detection);
→ a turni: ogni nodo attende il proprio turno per poter comunicare e i protocolli polling e token passing sfruttano questo meccanismo.

44) Caratteristiche del protocollo slotted ALOHA

Nello slotted ALOHA ogni nodo ha un uguale di time slice nel quale può trasmettere ed è sincronizzato agli altri nodi. Se si presenta una collisione, il frame viene ritrasmesso fino al successo (probabilità p). Esso ha le seguenti caratteristiche:

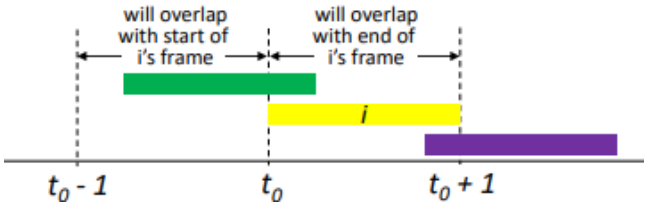
→ trasmissione continua (vantaggio);
→ decentralizzato (vantaggio);
→ collisioni fanno perdere slot (svantaggio);
→ slot in stallo (svantaggio);
→ clock di sincronizzazione (svantaggio).

L'efficienza è del 37%.



45) Caratteristiche di ALOHA puro

Nell'ALOHA puro non si ha slot e sincronizzazione e aumentano le collisioni. Risulta essere più semplice e l'efficienza è del 18%.



46) Caratteristiche di Carrier Sense Multiple Access

Nel protocollo CSMA un nodo ascolta prima di trasmettere e se il canale è occupato, allora avvia una trasmissione differita, altrimenti invia l'intero frame.

47) Caratteristiche di Carrier Sense Multiple Access/Collision Detection

Nel protocollo CSMA/CD il nodo ascolta il canale per verificare se è libero e in caso positivo trasmette. Se durante la trasmissione rileva una collisione, interrompe la trasmissione e attende un intervallo di tempo casuale prima di ritentare. L'algoritmo è come segue:

1 – controllo dello stato del canale e inizio della trasmissione;
2 – se tutto viene trasmesso, l'operazione risulta terminata;
3 – se collide, abortisce e invia un Jam signal;
4 – arretra nella trasmissione (backoff).

Risulta essere migliore del protocollo ALOHA.

$$efficiency = \frac{1}{1 + 5t_{prop}/t_{trans}}$$

48) Cosa si intende per indirizzo MAC (Medium Access Protocol)?

Si definisce indirizzo MAC (Medium Access Protocol) un identificatore univoco lungo 48 bit (6 byte) assegnato ad una scheda di rete (NIC, Network Interface Card) per l'uso nelle comunicazioni all'interno di una rete segmentata. Gli indirizzi MAC sono utilizzati nelle reti Ethernet e nelle reti wireless IEEE 802.11.

Esempio: 00:1A:2B:3C:4D:5E

49) Cosa si intende per ARP (Address Resolution Protocol)?

Si definisce ARP (Address Resolution Protocol) un protocollo che traduce un indirizzo IP in indirizzo MAC grazie alle ARP Table, rinnovata circa ogni 20 minuti e propria di ogni dispositivo di rete.

Esempio:

Indirizzo IP	Indirizzo MAC
137.196.7.14	58-23-D7-FA-20-B0

50) Cosa si intende per Ethernet?

Ethernet è una tecnologia di rete utilizzata per connettere dispositivi all'interno di una rete locale (LAN, Local Area Network). È il metodo più comune per le connessioni cablate in una rete, ed è standardizzato dall'IEEE sotto la famiglia di standard 802.3.

51) Quali sono le caratteristiche di Ethernet?

Le caratteristiche di Ethernet sono:

→ semplicità ed economicità;

→ connectionless, in quanto non c'è un handshake;

→ unreliable, in quanto non ci sono segnali di ack.

52) Quali sono le topologie di rete più diffuse?

Le topologie di rete sono:

→ bus: tutti i nodi comunicano su un unico collegamento, con collisioni;

→ switched: la rete è governata dagli switch.

53) Cosa si intende per polling?

Si definisce polling un approccio in cui un nodo master gestisce la comunicazione di nodi dumb e ha le seguenti caratteristiche:

→ overhead;
→ latenza;
→ punto singolo di fallimento sul server.

54) Quali sono le caratteristiche del token passing?

Un token è passato tra i nodi per consentire l'uso del canale ed ha le seguenti caratteristiche:

→ overhead;
→ latenza;
→ punto singolo di fallimento sul token.

55) Indicare i componenti di un frame Ethernet

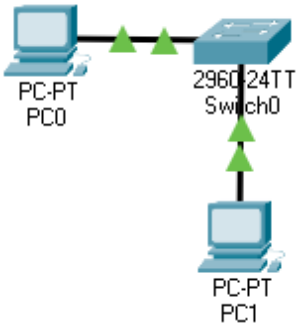
I componenti di un frame Ethernet sono:

→ preambolo: usato per sincronizzare mittente, destinatario e clock;
→ indirizzi MAC mittente e destinatario;
→ tipo: indica il protocollo di livello superiore (IP);
→ CRC: che effettua il controllo ciclico delle ridondanze;
→ payload data.

56) Cosa si intende per switch Ethernet?

Si definisce switch Ethernet un dispositivo del livello di collegamento che permette la comunicazione tra host situati nella stessa rete locale (LAN) e svolge un ruolo attivo:

→ store and forward dei frame;
→ inoltra i pacchetti in base all'indirizzo MAC;
→ trasparente agli host;
→ non ha bisogno di configurazione (plug and play) e possono comunicare tra loro;
→ grazie allo switch, gli host possono comunicare simultaneamente senza collisioni in full duplex.



57) Cosa si intende per switch table?

Si definisce switch table una tabella contenuta nello switch Ethernet che associa un'interfaccia di un host all'indirizzo MAC corrispondente. Viene costruita dallo switch leggendo il MAC di orgine dei pacchetti che gestisce.

58) Cosa si intende per switching?

Lo switching è un algoritmo costituito dai seguenti passaggi:

→ registra il MAC;

→ interroga la switch table;

→ se trova l'indirizzo inoltra il frame (drop se corrisponde al mittente);

→ altrimenti lo inoltra a tutti i collegamenti.