INTRODUZIONE ALLE RETI

DTE = data terminal equipment, Sono dispositivi come Computer e stampanti considerati componenti terminali della rete.
Le schede di rete sono interfacce poiché sono parte dell' apparato elaborativo.

DCE = data communication eqipment. Ha la funzione di stabilire, mantenere e terminare una connessione per la trasmissione dati. Un esempio è il modem.

COMMUTAZIONE = tecniche elettroniche e metodologie utilizzate per far dialogare tra loro calcolatori connessi in rete (termine importato dall'area delle reti telefoniche).Si divide in commutazione di circuito e di pacchetto.

- **di circuito** = tramite apertura e chiusura di interruttori si crea un circuito riservato alla comunicazione attiva.
- **di pacchetto a datagramma** = i pacchetti seguono percorsi diversi e tra i pacchetti non c'è un ordine quindi tutti i pacchetti contengono l' indirizzo del destinatario.
- **di pacchetto a circuito virtuale** = tutti i pacchetti seguono lo stesso percorso. I pacchetti sono ordinati e sulla linea di comunicazione possono viaggiare contemporaneamente più conversazioni.

CLASSIFICAZIONE SECONDO LA GESTIONE DELLE RISORSE
Dalla teoria dei sistemi operativi, il controllo di una risorsa si articola in varie attività: verifica dei diritti d'accesso, sequenziamento, esecuzione delle operazioni disponibili, per ogni risorsa ci sono 1 o più gestori.

- gestione autocratica -ogni risorsa ha 1 unico gestore (1 a 1)
- gestione multilaterale –c'è più di un gestore per la stessa risorsa (1 a n)
    - gestione partizionata: ogni attività di gestione è effettuata da un solo processo
    - gestione successiva: tutte le attività sono effettuate a turno da più processi
    - gestione replicata: tutti i gestori partecipano a ciascuna attività (la gestione replicata è detta democratica quando ogni attività ha luogo tramite una cooperazione "alla pari" tra i gestori: ogni decisione è negoziata attraverso un esplicito consenso)
- **CONSENZIENZA** = alta se è alto il numero di gestori che partecipano ad ogni istanza di una certa attività.
- **EQUIPOLLENZA** = grado di uguaglianza nella responsabilità di gestione.

MODELLO ISO OSI

n-pdu = n-pci + n-sdu

N-pdu (protocol data unit): insieme dei dati piu tutte le intestazioni aggiunte dai livelli precedenti.
N-pci (protocol control information): header aggiunto dal livello n.
N-sdu (service data unit): o payload è il dato vero e proprio.
N-sap: punto logico di incontro tra n-utente e n-servizio.

LIVELLO FISICO:
●Si interfaccia direttamente con i mezzi fisici di trasmissione
●offre allo strato superiore una comunicazione *indipendente dal particolare mezzo trasmissivo.*
●servizi forniti allo strato di collegamento:
●– gestione della connessione fisica, identificazione della con. fisica, trasmissione delle unità dati, consegna in sequenza delle unità dati, notificazione di malfunzionamenti
●qualità dei servizi:
●– tasso d'errore, disponibilità, frequenza di cifra, ritardo di trasferimento.

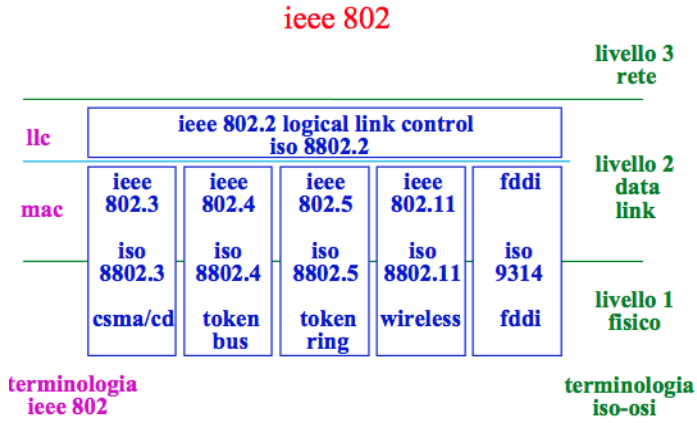
LIVELLO DATA-LINK:
●Obiettivo:
● fronteggiare i malfunzionamenti dello strato fisico (rilevazione e correzione degli errori)
●servizi offerti allo strato di rete:
●– trasferimento di informazioni senza vincoli di formato, codice o contenuto
●– selezione di una certa qualità di servizio
●utilizzo di due code, nelle due direzioni.

●LIVELLO DI RETE
●• conoscelatopologiadellarete
●instradamento
●• se connesso, instaura, mantiene e rilascia le connessioni di rete
●• il3-servizioconsentedi:
●– trasferire informazioni da estremo a estremo
●– selezionare una certa qualità (tempo di attraversamento, disponibilità) - non sempre
●• commutazione:
●– circuito, pacchetto datagramma, circuito virtuale

LIVELLO DI TRASPORTO:
●Colma deficienze e fluttuazioni del grado di servizio delle connessioni di rete e ottimizza l'uso della rete dal punto di vista dei costi
●è il primo strato estremo-estremo *(risiede solo nei nodi terminali)*
●Servizi offerti allo strato 5:
● instaurazione di una connessione – trasferimento dati e gestione della connessione – rilascio
●sincronizzazione tra i due sistemi per mezzo di conferma.

PROTOCOLLO 802 (FISICO - DATA LINK)

Standardizza i livelli 1 e 2 del modello ISO-OSI.



Campi presenti in ogni un pacchetto di livello MAC:

MAC-DSAP (indirizzo MAC del destinatario 6 byte)	MAC-SSAP (indirizzo MAC del mittente 6 byte)	LLC-PDU (dati)				FCS (Frame control system)
		LLC-DSAP (1 Byte)	LLC-SSAP (1 Byte)	CONTROL (1 o 2 Byte)	PDU L3 (n Byte) Livello di rete.	

Se gli LLC-SAP (mittente e destinatario) contengono il Byte “AA” allora il protocollo di livello 3 è non standard.

MAC-DSAP (indirizzo MAC del destinatario 6 byte)	MAC-SSAP (indirizzo MAC del mittente 6 byte)	LLC-PDU (dati)					FCS (Frame control system)
		LLC-DSAP (1 Byte) “AA”	LLC-SSAP (1 Byte) “AA”	CONTROL (1 o 2 Byte)	***Protocoll Identifier (Solo se gli LLC-SAP valgono “AA”) 5 Byte***	PDU L3 (n Byte) Livello di rete.	

I SAP di LLC servono a dentoare i protocolli di livello superiore a cui sono destinati i pacchetti.

Consentono la convivenza di protocolli diversi di livello 3 sulla stessa LAN e sulla stessa macchina!

CSMA/CD protocollo di livello 2 (MAC) per reti ethernet 802.3.

Carrier Sense Multiple Access With Collision Detection

●*Carrier Sense = Prima di trasmettere viene ascoltato il canale per verificare che sia libero.*
●*Multiple Access =Si possono verificare Collisioni.*
●*Collision Detection = Rilevazione di una collisione.*

A seguito di una collisione la stazione trasmittente invia una sequenza di jamming e la stazione ricevente riceve un pezzetto di pacchetto e la sequenza di jamming e scarta tutto.

La stazione trasmittente riprova dopo un tempo random multiplo di 51.2 microS su eth a 10 Mb/s per un massimo di 16 tentativi.

• **round trip delay 2t** e' il tempo necessario per un bit per propagarsi da un estremo all'altro della rete e "tornare indietro"
•**osservazione**: una stazione trasmittente riesce a capire che il pacchetto che ha trasmesso e' entrato in collisione solo mentre trasmette.

Pacchetto piu piccolo: 512 Bit.
In eth a 10 Mbps quanto tempo occupano il canale trasmissivo 512 bit?
512 Bit / 10*10^6 = 51.2 microS = Round Trip Delay (2t)
Quanto spazio occupano sul mezzo trasmissivo?
51.2 microS / 2 * 2/3 Vluce = 5 Km

Algoritmo di Backoff

Se tentativo=1 (primo tentativo di ritrasmissione del frame)

allora
    max:=2
altrimenti
    se tentativo < limite_di_backoff
        allora max:=max x 2
aspetta(2t x random(0,max-1))

ESERCIZIO
Considera due stazioni A e B su un dominio di collisione ethernet, entrambe con infiniti pacchetti da trasmettere. I pacchetti di A sono numerati A1, A2, ecc. I pacchetti di B sono numerati B1, B2, ecc.
La rete e' inizialmente priva di traffico e ad un certo istante A e B tentano di trasmettere contemporaneamente A1 e B1. Le stazioni rilevano entrambe una collisione.
Nel corrispondente backoff, A estrae il numero 0 mentre B estrae il numero 1. In questo caso A trasmette A1 e B deve aspettare.Nel momento in cui A smette di trasmettere entrambe le stazioni hanno un pacchetto da trasmettere (A2 e B1). Quindi si verifica sicuramente una nuova collisione.
Quali sono le probabilita' che dopo la collisione:
a) si verifichi una nuova collisione b) B trasmetta e A debba aspettare c) A trasmetta e B debba aspettare

PRIMA COLLISIONE tentativoA=1 maxA=2 randA=0 scelto in (0,1) wA=0
tentativoB=1 maxB=2 randB=1 scelto in (0,1) wB=2t
TRASMETTE A1

tentativoA=1 maxA=2 randA è scelto in (0,1)
tentativoB=2 maxB=4 randB è scelto in (0,3)
POSSIBILI EVENTI:

Collisione se ho randA=randB 0,0 oppure 1,1 prCol = ¼
Trasmette A se randA<RandB 0,1 ; 0,2 ; 0,3 ; 1,2 ; 1,3 p r A = 5/8
Trasmette B se rand A>RandB prB =1/8

ETHERNET 802.3

*(**64-1518** byte <u>senza</u> preambolo ed sfd)*

- Coassiali, doppini telefonici, f. ottiche.
- Bus e stella
- Codifica: Manchester

LIV MAC IN 802.3

- SOURCE / DESTINATION ADDRESS (48 bit +48 bit)
- DATA: contiene l' LLC-PDU di eth 802.3
- FCS contiene il valore di crc calcolato (32 bit).
- PREAMBOLO: Sincronizzazione **(56 bit)** è una sequenza alternata di 0 e 1 a 5 Mhz con codifica Manchester a 10 Mbit/s consente alla stazione ricevente di "agganciare" in frequenza e fase il pacchetto, il preambolo non viene passato allo strato superiore.

- START FRAME DELIMITER Inizio pacchetto che viola la codifica Manchester **(8 bit)**
- LENGTH numero di byte del campo data (16 bit)
- PAD riempimento per ottenere che DATA+PAD = da 46 a 1500 byte;

MAC DSAP	MAC SSAP	DATA (LLC-PDU)	FCS	PREAMBOLO	SFD	LENGTH	PAD

1500 byte è la dimensione massima per tutti i pacchetti che girano in rete, implica che le altre stazioni dovranno attendere per carrier sense.
Non c'è il delimitatore di fine pacchetto ma un tempo di 9.6 microS
Lunghezza del jam: 32 bit. E 96 per i repeater.

RIPETITORI

- il ripetitore è situato al livello fisico
- ha, in generale, varie porte
- ripete il segnale ricevuto su una porta a tutte le altre porte
  i bit sono inoltrati immediatamente sulle altre porte
- non è una macchina *store and forward*
- rigenera il preambolo e ritemporizza tutti i bit
- se una collisione viene rilevata su una porta trasmette jam su tutte le porte
  - transmit collision: collisione rilevata sulla porta su cui si sta trasmettendo; trasmissione di jam su tutte le porte
  - receive collision: collisione rilevata sulla porta su cui si sta ricevendo; trasmissione di jam su tutte le altre porte
- può escludere una porta quando sul suo segmento si verificano troppe collisioni.

ETHERNET 2.0: Liv3 incapsulato direttamente dentro MAC

MAC DSAP	MAC SSAP	DATA ***<u>Livello 3</u>*** ***<u>NON HA LLC!!!!!</u>***	FCS	PREAMBOLO	SFD	**TYPE** (Svolge funzioni di multiplexing di LLC che non è presente.)	PAD

TOKEN RING 802.5 ed FDDI

Il token è un particolare pacchetto che circola sull'anello e che ne indica la disponibilità:
Il token gira continuamente anche se nessuno deve trasmettere
Una stazione che vuole trasmettere attende il token, lo cattura e quindi trasmette
Catturato il token, la stazione trasmette uno o più pacchetti, entro il tempo tht (token holding time).

L**' active monitor** è la stazione responsabile del token ed è incaricata di:

- immetterlo
- verificarne l' esistenza
- immetterlo nuovamente in caso di malfunzionamenti

Per l' elezione dell' Active Monitor tutte le macchine iniziano a trasmettere un proprio valore "CLAIM" alla stazione successiva (ad esempio il MAC addres); se il claim ricevuto è maggiore del proprio allora la macchina smetterà di inviare il proprio claim ed invierà quello ricevuto. La macchina che ha il claim maggiore è eletta come active monitor.

Rilascio del token: **attendere che il pacchetto ritorni davanti alla stazione che ha immesso il pacchetto per essere rimosso e rilasciare il token** (in realtà aspetta i Source Address) è inefficiente poiché anche se il pacchetto non occupa tutto l' anello la stazione lo riempie con bit di riempimento occupando il canale senza motivo.
Il rilascio anticipato del token avviene **rilasciando il token alla fine dell' immissione del pacchetto prima che il SA ripassi davanti alla macchina che l' ha inviato**. Quando il pacchetto ripassa davanti alla stazione che l' ha generato allora lo rimuove lasciano il frammento da SD a SA.

Formato del Token:

SD (Start Delimiter)	AC (Access Controll) **1 bit specifica se è un pacchetto o un token.**	ED (Ending delimiter) Un bit detto Intermediate BIT specifica se il pacchetto è seguito da altri o si tratta dell' ultimo.

trasmissione con mittente A e destinatario C (sul ring B e D) ÿ A attende il token, quando arriva lo "cattura"; ciò avviene portando ad **1 il bit opportuno dell'access control** . ÿ la parte di token già ritrasmessa viene quindi trasformata nella parte iniziale del pacchetto dati. **(Mozzicone di Token)** ÿ A inibisce il circuito di ripetizione tra ring-in e ring-out ÿ **A trasmette il pacchetto** (comprensivo di indirizzi mac destinazione e sorgente, dati, ecc) ÿ se A ha altri dati da trasmettere e **non** ha ancora **superato** il **tht**, allora mette ad **1 l'intermediate bit dell'end delimiter** e trasmette il pacchetto successivo	quando A ha **trasmesso l'ultimo pacchetto pone a 0 l'intermediate bit** ÿ se A termina la trasmissione di un pacchetto prima di aver iniziato a riceverlo indietro, trasmette **bit di riempimento** fino a quando può rigenerare il token. ÿ quando A riceve il source address del pacchetto trasmesso, se la trasmissione è terminata, toglie il pacchetto e genera il token. ÿ tutte le altre stazioni (qui B e D) ripetono i bit alla stazione successiva ÿ ogni stazione verifica l'indirizzo di destinazione, se il pacchetto le è destinato lo copia ÿ alla fine della ricezione dei propri pacchetti A riabilita il circuito di ripetizione -Quando la stazione ha terminato di inviare pacchetti rilascia il token per consentire l'utilizzo della rete alle altre stazioni

SD (1 byte)	**AC (1 Byte)**	Frame Controll	Dest Address	Source Address	Routing Info	INFO	FCS	**ED (1 Byte)**	Frame Status (1 Byte)

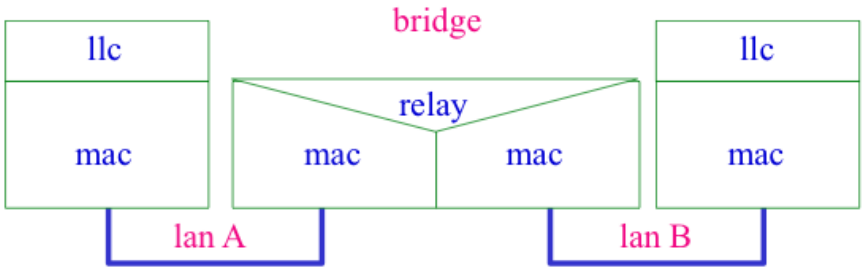
BRIDGE/SWITCH (LIV 2)

SI OCCUPA DELLE COLLISIONI

E' una soluzione a problemi di carico sopportabile, numero di sistemi interconnessi e distanza massima che può ricoprire una LAN.

ARCHITETTURA

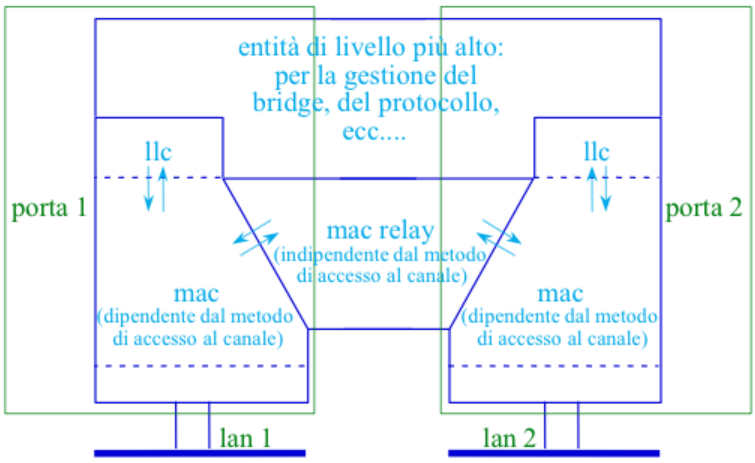
Un bridge può interconnettere **LAN anche con MAC differenti.** Nel caso di MAC differenti occorre effettuare una traduzione di formato del pacchetto, compreso il ricalcolo dell' FCS, se la LAN non è conforme a 802 allora è necessario ricostruire anche LLC.
Nell 'interconnettere reti con MAC differenti si ha il problema di pacchetti di lunghezza massima diversa (es: wi-fi, fddi, ethernet) c'è quindi la necessità di frammentare il pacchetto ma ***la frammentazione non compete al livello 2*** quindi sarà fatta da altri apparati specializzati.



I MAC sulla stessa LAN (es LAN A o LAN B) devono necessariamente essere uguali, mentre potranno essere diversi tra loro i due MAC del bridge.

SPANNING TREE

I Bridge si occupano inoltre dello **spanning tree,** un meccanismo che evita la possibilità di creare un loop in seguito all' errato cablaggio della rete disattivando automaticamente le porte che formano il loop e formando così un albero ricoprente; le porte vengono riattivate nel caso in cui ci dovessero essere problemi sulle altre.



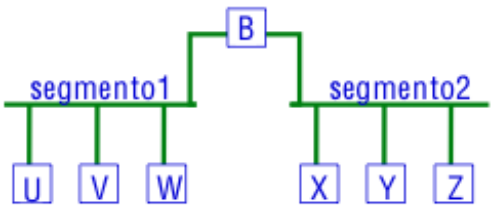
Se una porta è attiva può trovarsi in stato di:
LISTENING: la porta partecipa alla lettura dei pacchetti e il processo di learning aggiunge nuove informazioni alla tabella di instradamento.
FORWARDING: La porta partecipa alla ritrasmissione dei pacchetti. Allo scadere del forwarding delay time la porta torna in stato di learning.

INSTRADAMENTO (LEARNING)

Un bridge trasmette su una LAN solo i pacchetti che hanno come destinatario un PC di quella LAN altrimenti i traffici locali restano separati.(Filtering)
Ci sono due tipi di bridge:
-Transparent Bridge: conformi a 801.1d con tabelle di instradamento a bordo.

-Sourece Routing Bridge: Utilizzati nelle Token-Ring con tabelle nei sistemi e specifica completa del percorso del pacchetto.

Il processo di learning funziona solo se la tipologia della rete è ad albero.



evento	lista segmento1	lista segmento2
bootstrap di B		
U -> V	U	
V -> U	U,V	
Z broadcast	U,V	Z
Y -> V	U,V	Z,Y
Y -> X	U,V	Z,Y
X -> W	U,V	Z,Y,X
W -> Z	U,V,W	Z,Y,X

La tabella di instradamento contiene entry statiche e dinamiche, il tempo massimo di sopravivenza per entry dinamiche è di 5 minuti di inattività.

Mentre un malfunzionamento del learning può essere superato inviando su tutte le porte il pacchetto, un malfunzionamento dello spanning tree rende la rete inutilizzabile a causa dei cicli.

FUNZIONAMENTO CUT-THROUGH

- Evita lo store and forward e diminuisce la latenza
- Inizia a trasmettere subito il primo bit ricevuto alla porta di destinazione se è libera.
- Non ricalcola FCS quindi ritrasmette anche gli errori
- **Non è possibile se: ci sono diversi protocolli, diverse velocità o la porta è occupata.**

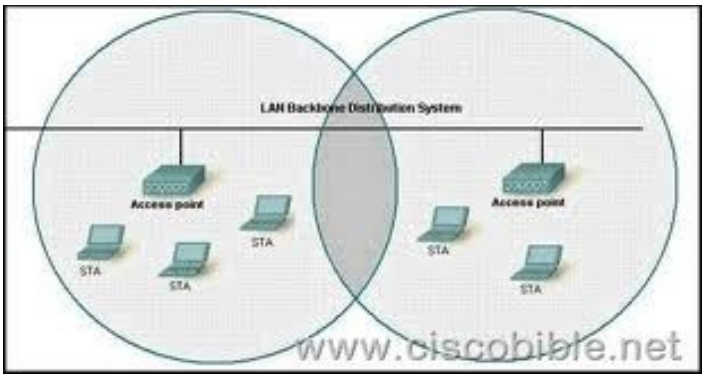
FUNZIONAMENTO SOURECE ROUTING

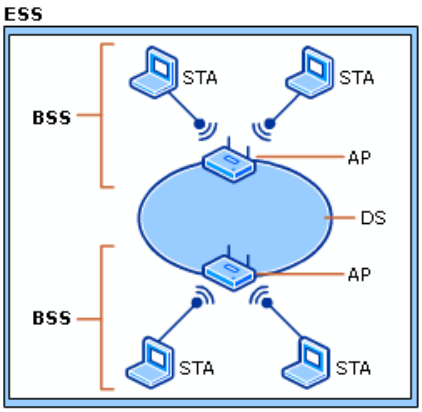
- Utilizza un campo RI (routing information) per la posizione del destinatario.
- Un pacchetto senza RI ha destinatario locale.
- Utilizza le tabelle di instradamento.
- Le tabelle si calcolano tramite l' uso dei pacchetti (all routers explorer) ARE nel processo di route discovery.

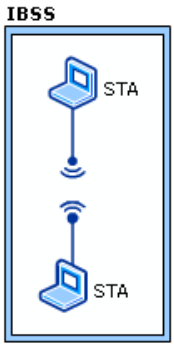
Quando un pacchetto parte per la prima esplorazione arriva a destinazione più volte (tante quante le strade possibili) ogni bridge che lo ha fatto passare ha scritto nell' ARE il suo ID.
Viene rispedito indietro dalla destinazione solo il primo ARE arrivato cioè quello che percorre la strada più breve. La tabella è quindi aggiornata con il percorso ottimo.

WIRELESS LAN

BSS: Basic Service Set, Insieme delle macchine connesse all' AP
AP: Access Point, si comporta come un bridge.
Ogni BSS ha un identificatore BSSID, tipicamente l' indirizzo MAC della scheda wireless dell' access point.
ESS: Extended service Set, unione di tutti i BSS della rete.
DS: rete wired di backbone.







E' previsto l' utilizzo in cui gli AP dialoghino via wireless e non tramite infrastuttura wired.

LIVELLO 2 nelle reti WI-FI

LLC: Standard 802.2 come per le altre tecnologie.
MAC: Handshaking, indirizzamento, accesso al mezzo trasmissivo, ***frammentazione***, gestione della potenza, roaming.

Handshaking: Se un calcolatore vuole accedere a una BSS deve scambiarsi (presentare) l' indirizzo MAC all' AP che fornirà il suo.
O l'AP invia dei pacchetti broadcast per informare della sua presenza (pacchetti beacon) oppure la stazione che vuole connettersi esplora l'esterno con pacchetti di probe-request in attesa di un probe-response.

Indirizzamento: Nel pacchetto MAC ci sono ben 4 indirizzi oltre a 2 bit: fromDS e toDS.
ToDS vale 1 se il pacchetto è spedito sull' AP per essere smistato sul DS.
FromDS vale 1 se il pacchetto è stato ricevuto dal DS.

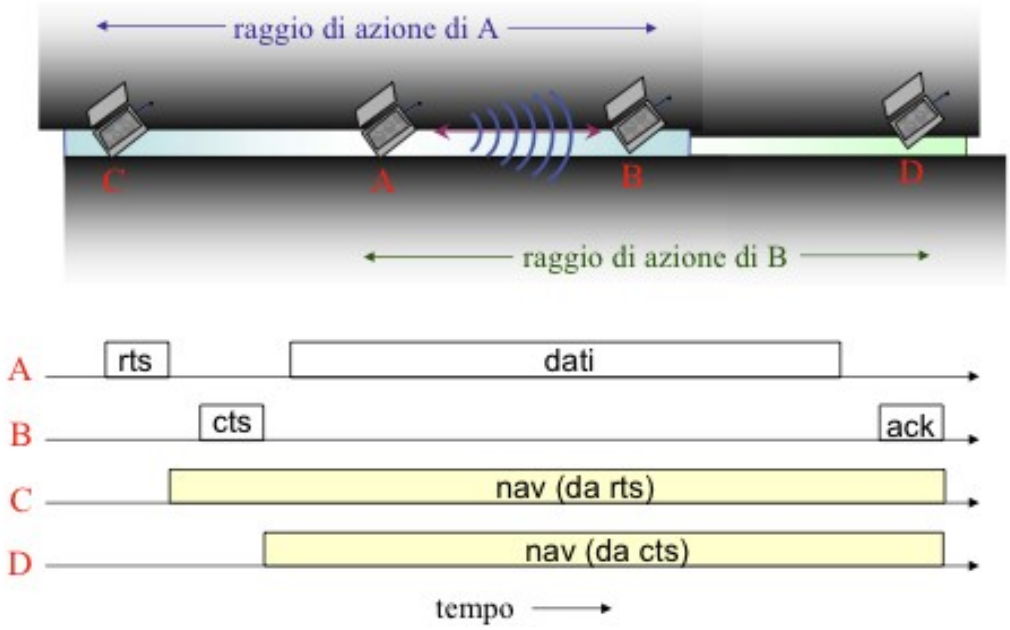
RA=recipient address (scheda ricevente),
TA=transmitter address (scheda trasmittente),
DA=destination address (destinatario finale),
SA=sender address (sorgente del pacchetto).

	ToDs	FromDS	Add1 Destinatario	Add2 Mittente	Add3	Add4
Da pc a pc	0	0	DA	SA	BSSID	
Da ap a pc	0	1	DA	BSSID	SA	
Da pc ad ap	1	0	BSSID	SA	DA	
Da ap ad ap	1	1	RA	TA	DA	SA

ADD1: è sempre il mac della scheda cui è destinato il pacchetto (guardando la BSS).
ADD2: è sempre il mac della scheda che trasmette il pacchetto (guardando la BSS).
ADD3: se FromDS = 1 contiene SA se ToDS=1 contiene DA
ADD4: è utilizzato solo per comunicazioni wireless nel DS. Contiene SA.

ACCESSO AL MEZZO TRASMISSIVO.

Per accedere al mezzo tasmissivo è previsto l' uso di CSMA/CA (collision avoidance)
Non si usa CSMA/CD a causa del problema della stazione nascosta.
Cioè: A pensa di poter trasmettere dati a B perchè non vede che C gia dialoga con B.
Prenotazione: Quando una stazione vuole trasmettere spedisce un breve frame al destinatario chiedendo l'autorizzazione alla trasmissione.
Se il destinatario è libero invia un frame di conferma e alle stazioni connesse è chiede di non interferire per tutto il tempo della comunicazione che sta per avvenire.
La durata residua della connessione è scritta nel campo duration dei pacchetti wireless.
Tutte le stazioni che ricevono un rts (request to send) o un cts (clear to send) sanno che le 2 stazioni stanno dialogando e che lo faranno per il tempo indicato nel campo duration del pacchetto.
La durata viene memorizzata da ogni stazione nel suo NAV che viene man mano decrementato, quando è pari a 0 allora si puo inviare un RTS.
ACK: riscontro di fine trasmissione da parte del ricevente.



Si rileva una collisione se la stazione trasmittente non riceve il CTS del destinatario.

BACKOFF 802.11

- Viene lanciato da chi rileva la collisione
- Il numero di slot time che la stazione deve attendere è scelta a caso all' interno di una Contention Window (CW)
- A ogni nuova collisione l' intervallo di CW raddoppia (0 – 15) diventa (0 – 31) diventa (0 – 63)
- Per ogni intervallo che il canale è libero il contatore viene decrementato (cioè se il NAV è pari a 0) a differenza di csma/cd, il valore del contatore viene decrementato solamente se il canale è libero (cioè se il nav della stazione è pari a zero).

FRAMMENTAZIONE perchè
- Le wlan hanno pacchetti di dimensione inferiore a quelli delle reti wired
- Per ridurre l' overhead in caso di ritrasmissione del pacchetto.
- Per diminuire la probabilità di errore nella trasmissione.

VERSIONI

• **802.11b** opera nella banda 2,4 Ghz – velocità max di trasmissione 11 Mbs – copertura Indoor 150 Mt. Outdoor 500 Mt.(?) – utilizzo della modulazione HR-DSSS.

• **802.11g** opera nella banda 2,4 Ghz – velocità max di trasmissione 54 Mbs – copertura indoor 30 Mt. outdoor 150 Mt. – utilizzo della modulazione CCK/OFDM.

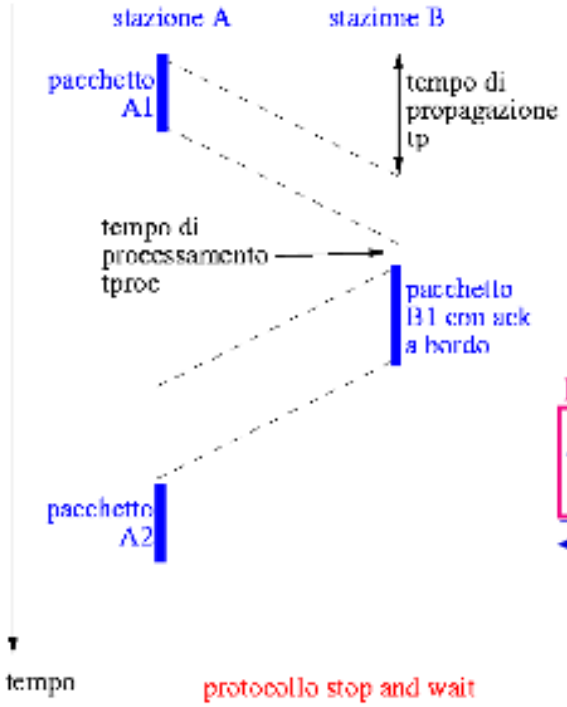
LIVELLO 2 NELLE RETI WAN

L' interfaccia di una rete locale verso la rete geografica è il router o gateway, apparecchiatura di livello 3.
Protocolli di livello 2 per WAN:
sdlc, hdlc, **ppp** (variante bilanciata di hdlc) e lapb.

GESTIONE DEGLI ACKNOLEDGEMENTS

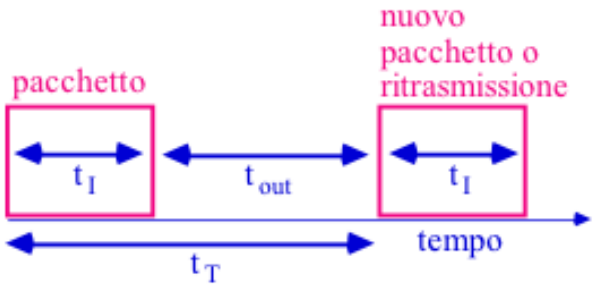
STOP AND WAIT

Dopo la trasmissione di un pacchetto la stazione trasmittente aspetta un ACK (o NACK) se non arrivano ne un ACK ne un NACK entro un certo tempo il pacchetto viene ritrasmesso.

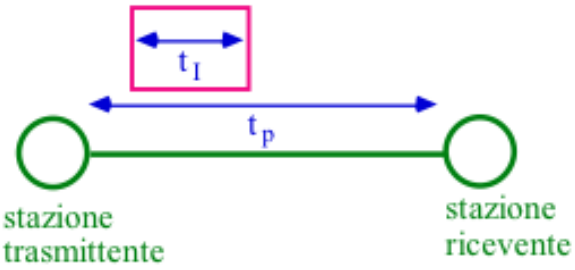


protocollo stop and wait

Ti= tempo di immissione
Tout=tempo di intervallo tra 2 pacchetti
Tp=tempo di propagazione da estremo a estremo della rete.
Tproc=processamento del pacchetto
Ts=tempo per trasmettere ack o nack
tout > 2Tp + Tproc + Ts
per semplicità uniamo Tproc in Tp,
Tt=Ti+Tout (tempo tra inizi di due pacchetti diversi)



A <u>non può trasmettere più di 1/Tt</u> pacchetti al secondo, il throughput è però inferiore a causa di errori di trasmissione.

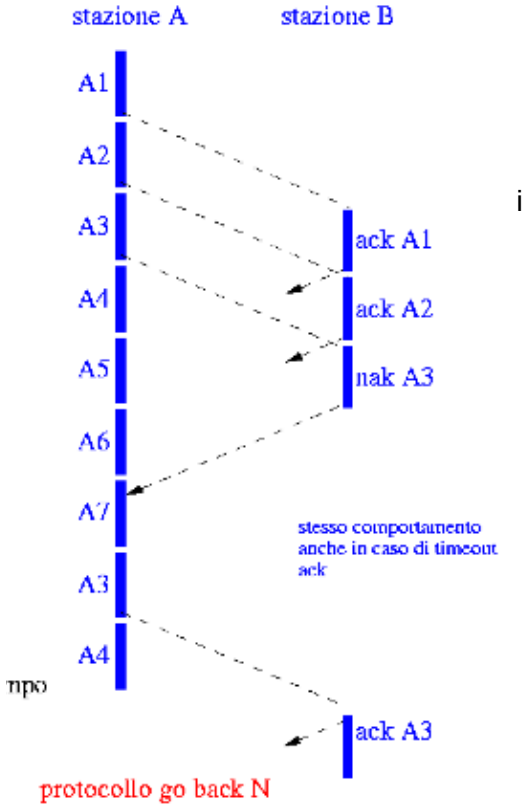


GO BACK N

A invia in sequenza i pacchetti in coda senza preoccuparsi se ancora non ha ricevuto ack o nack
da B.
B inizierà ad inviare le notifiche ma se un pacchetto non dovesse arrivare allora B o non risponde o manda un nack e scarta i successivi.
A, rilevato il Tame Out o il NACK, reinvia il pacchetto corrotto e pacchetti successivi.

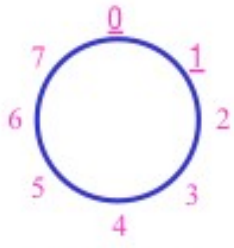
Avrei avuto lo stesso comportamento se non
avessi ricevuto il NACK da B. (Time Out).

Schema di numerazione dei pacchetti:
Ogni pacchetto è numerato con un frammento finito di bit di Bit con una numerazione mod M, con 0 <= N <= M-1
AL PIU POSSO AVERE M-1 PACCHETTI IN ATTESA DI RISCONTRO!!!

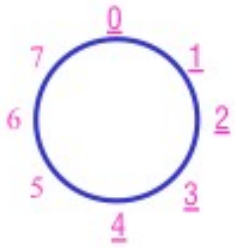


i

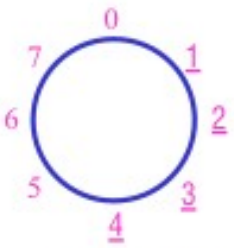
npo



due pacchetti non ancora riscontrati

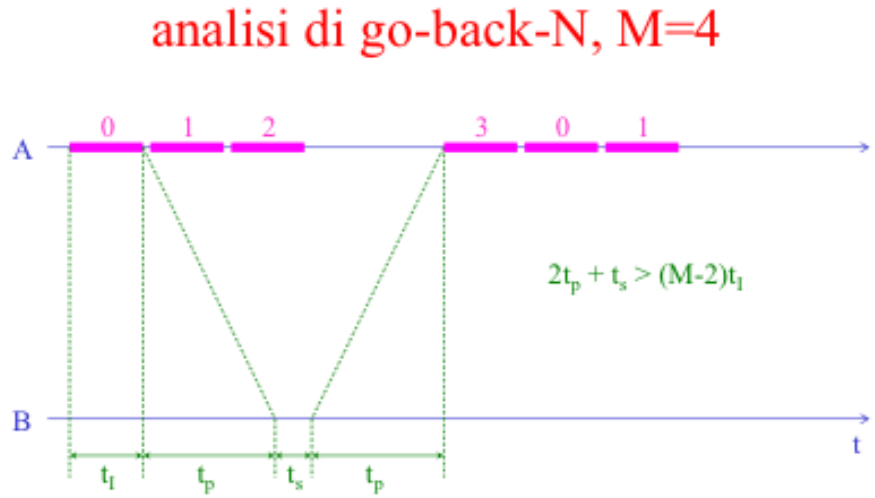


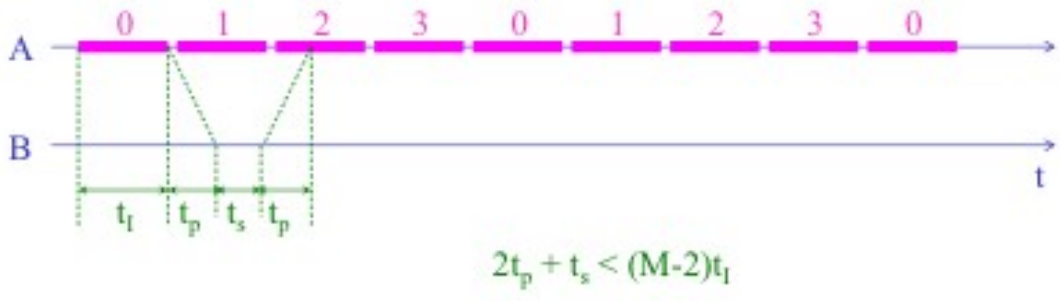
invio di tre ulteriori pacchetti



viene ricevuto il riscontro del pacchetto 0

Non posso mandare il terzo pacchetto perchè ho gia M-1 pacchetti in attesa di riscontro!
Appena arriva l' ACK mando anche il pacchetto 3.





IL LIVELLO DI RETE (Liv 3)

Il livello di rete sceglie una strada per i pacchetti e quindi conosce la topologia della rete, fornisce inoltre servizi al livello di trasporto (liv 4) il quale non vuole conoscere ne il numero e la topologia delle varie sottoreti che vengono attraversate per raggiungere una destinazione ne la tecnologia usata per realizzare le varie sottoreti.

I servizi possono essere CONNESSI e NON CONNESSI: ad esempio il protocollo di liv 3 più utilizzato, IP, offre servizi NON CONNESSI; un liv 3 connesso generalmente usa una commutazione a circuito virtuale, mentre un liv 3 non connesso utilizza una connessione a datagramma.

Il liv 4 vuole conoscere le macchine attraverso indirizzi univoci distribuiti in modo consistente su tutta la rete. Un esempio di primitiva di invio a liv4 può essere:

spedisci_pacchetto(ind_liv3, payload_liv3);

ROUTER / GATEWAY

Gli IS che lavorano a livello 3 ma contengono anche i livelli 1 e 2 sono detti Router o Gateway, talvolta però contengono anche strati superiori dell' architettura ISO OSI.
NB: L' instradamento è di norma effettuato a liv3 però alcuni episodi elementari di instradamento si riscontrano anche a liv2 con i bridge e gli switch!

La differenza tra i due instradamenti è nel fatto che un indirizzo di liv2 (MAC) identifica il destinatario di una LAN mentre un indirizzo di liv3 (IP) identifica il destinatario nell' ambito dell' intera rete.

Un Router necessita di tanti MAC quante sono le schede di rete (le porte del router) ma di un solo indirizzo IP!

Gli IS possono effettiare instradamento con 3 principali metodi:

routing by network address • nel pacchetto c"è l"indirizzo del sistema destinatario • la commutazione è a datagramma in base a tale indirizzo

label swapping • nel pacchetto c"è una label che identifica la connessione • la commutazione è a circuito virtuale in base alla label

source routing • nel pacchetto è specificata la successione di is da attraversare • es: bridge token ring.

ROUTING BY NETWORK ADDRESS
Nel pacchetto c'è l' indirizzo del sistema destinatario, l' IS utilizza l' indirizzo come chiave di ricerca in una tabella locale e determina il cammino di trasmissione, la commutazione è a datagramma.

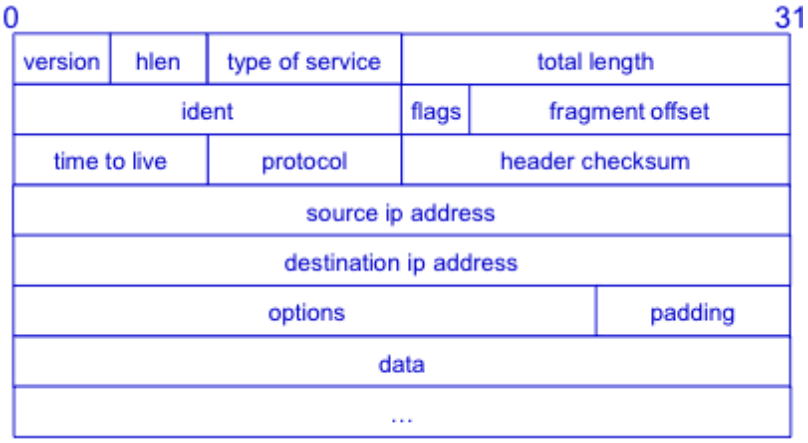
LABEL SWAPPING
Nel pacchetto c'è una label che identifica la connessione e viene usata come chiave di ricerca in una tabella piccola e viene deciso il cammino di ritrasmissione. La commutazione è a circuito virtuale.
Per evitare di dover verificare nell' intera rete che una label non sia gia stata utilizzata per un altra connessione, ad ogni tratto del circuito è assegnata una label diversa ed assegnata localmente.

SOURCE ROUTING
Nel pacchetto c'è tutta la strada da fare per arrivare a destinazione.

IL PROTOCOLLO IP e la suite TCP

Esempi di possibili protocolli accoppiati: telnet, tcp, ip, 802.3 oppure ftp, tcp, ip, 802.3

Commutazione a datagramma, non connesso, funzioni di instradamento, frammentazione, riassemblaggio e rilevazione di errori.
Riceve messaggi dai protocolli di liv4 TCP e UDP.
Preleva il pacchetto, eventualmente lo frammenta e provvede al loro instradamento.
La grandezza del pacchetto dipende dai vincoli di livello 2, se dovesse essere troppo grande allora lo frammenta, successivamente provvede al routing (è semplice nel caso di una LAN, più complesso nel caso di host remoti.
Un router non può riassemblare i pacchetti!!!



VERSION (4 bit): è il numero di versione del protocollo ip che ha generato il pacchetto, attualmente vale 4.

HLEN (4 bit): è la lunghezza dell' header espressa in parole di 32 bit, vale al minimo 5.

TYPE OF SERVICE: specifica la priorità di un pacchetto rispetto ad un altro, non sempre utilizzato.

IDENT (16 bit): intero che identifica un pacchetto, serve all' IP dell' host ricevente nel momento del riassemblaggio; due pacchetti di liv3 con lo stesso IDENT vengono assemblati nello stesso pacchetto a liv2.

FRAGSEGMENT OFFSET (13 bit): Serve ad unire i frammenti nel giusto ordine, indica lo scostamento dal primo pacchetto a cui va collegato. (Es: se vale 4 vuol dire che contiene i dati a partire dal 32esimo byte (4 x 8))

FLAGS (3 bit): il primo deve essere sempre 0, il secondo specifica se ilk pacchetto può essere frammentato, il terzo specifica se è l' ultimo frammento del pacchetto.

TOTAL LENGHT (16 bit): lunghezza totale del pacchetto (HEADER+DATA)

TIME TO LIVE (8 bit): specifica il tempo di vita del pacchetto, viene decrementato ad ogni hop, se vale 0 viene scartato dal router di passaggio che invia al mittente la segnalazione dell' errore.

PROTOCOL (8 bit): identifica il protocollo di livello4 che è nel payload del pacchetto. (Es: 1=ICMP, 6=TCP , 17=UDP)

HEADER CHECKSUM (16 bit): riguarda solo l'header e va ricalcolato ad ogni hop e confrontato con il valore di questo campo: se non c'è corrispondenza il pacchetto viene scartato. È da notare che non viene effettuato alcun controllo sulla presenza di errori nel campo *Data* deputandolo ai livelli superiori.

INDIRIZZO IP CLASSFUL

Class A (da 0.0.0.0 a 127.255.255.255)
- poche reti di dimensioni notevoli, 7 bit per la net e 24 per l'host, max 126 net e circa 16 milioni di host per net, il primo campo ha valore compreso tra 1 e 127
- NETMASK 255.0.0.0

Class B (da 128.0.0.0 a 191.255.255.255)
- numero medio di reti di dimensioni medio-grandi, 14 bit per la net e 16 per l'host, max 16382 net e circa 64000 host per net, il primo campo ha valore compreso tra 128 e 191
- NETMASK 255.255.0.0

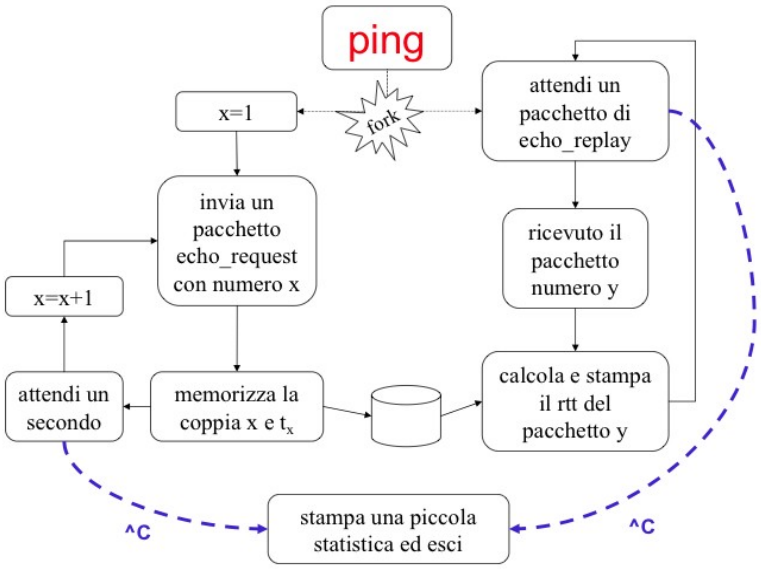
Class C (da 192.0.0.0 a 223.255.255.255)
- molte net di dimensioni piccole, 22 bit per la net e 8 per l'host, max 2milioni di net e 256 di host per net, il primo campo ha valore compreso tra 192 e 223
- NETMASK 255.255.255.0

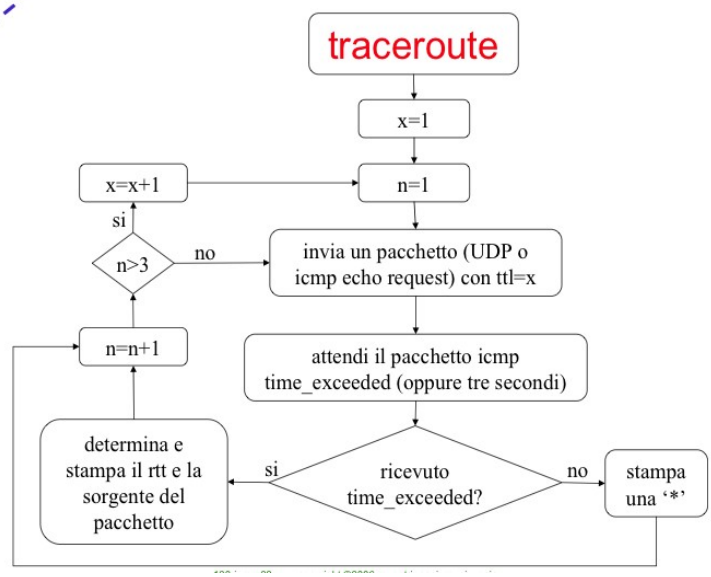
Class D (da 224.0.0.0 a 239.255.255.255) – riservati per uso multicast

Class E riservati per usi futuri

PROTOCOLLI DI SUPPORTO DEL LIVELLO 3

PROTOCOLLO ICMP: **LIVELLO 4**
- Non esistono messaggi di errore come risposte a malfunzionamenti su ICMP
- Se viene frammentato, solo il primo frammento può generare un messaggio di errore.
- Non è contenuto in messaggi broadcast e multicast.
- Contenuto nel campo data del pacchetto di livello 3.
- Utilizzato per Ping e Traceroute





LO STRATO DI TRASPORTO (LIV4)

- Il servizio offerto dallo strato di trasporto deve essere affidabile ed è normalmente **connesso**.
- I processi che utilizzano le primitive di trasporto assumono che esse siano affidabili.

ESEMPI DI PRIMITIVE:

- **Listen**: in attesa di connessione
- **Connect**: tentativo di instaurare una connessione
- **Send**: invio di dati
- **Receive**: in attesa di dati
- **Disconnect**: rilascio connessione.

INSTAURAZIONE DI UNA CONNESSIONE: Metodo ***Three-way hanshake***

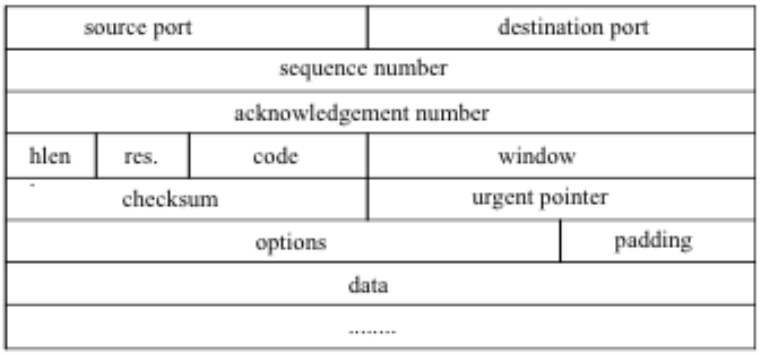
- A sceglie il numero di sequenza iniziale x per i propri pacchetti
- A invia la richiesta di connessione con il numero x a B
- B riceve la richiesta con x
- B sceglie il proprio numero di sequenza y
- B accetta la connesisone e invia l'accettazione con i numeri x e y
- A riceve la conferma
- A riscontra y a B

Per quanto riguarda il rilascio avviene in modo indipendente dall' altra stazione e quando uno dei due rilascia la connessione continua comunque a ricevere dati dall' altro.

PORT: I port permettono di distinguere più destinazioni su una stessa macchina, costituiscono i TCP SAP
Il numero dei port ha 2 byte e i port minori di 256 sono riservati per servizi standard.

TCP (connesso)

- Servizio fullduplex pto pto, non supporta broadcasting e multicasting,
- Garantisce l'affidabilità della trasmissione tramite l' utilizzo dei riscontri
- Basa la comunicazione su due processi, indirizzo ip e numero di port per entrambi i punti.

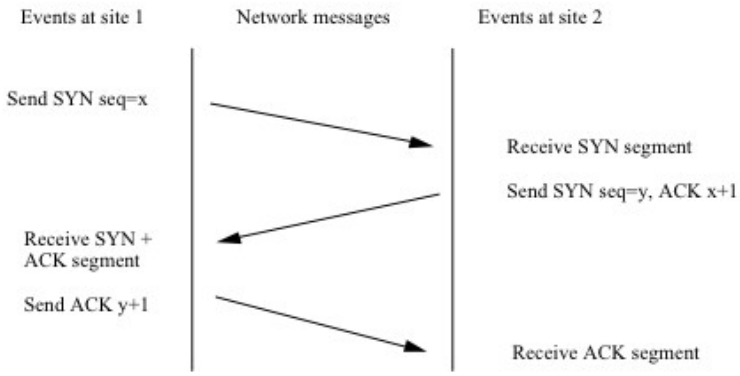


I numeri x e y (sequence number e acknoledgement number) vengono utilizzati per gestire il meccanismo di reinvio di pacchetti e riscontri; si utilizza in particolare un sistema di riscontri Go-Back-N orientato al byte.

HELN: numero di parole di 32 bit dell' intestazione
CODE: determina il tipo di messaggio nel segmento

é formato da URG: urgent pointer field, ACK: acknoledgement, PSH: push, RST: reset connection, SYN: sincronizzare i numeri di sequenza, FIN: fine invio dati.

<u>*OPTIONS*</u>: specifica l' ampiezza del campo dati negoziando durante l' instaurazione della connessione. (min 536 byte di dati)



RILASCIO DELLA CONNESSIONE UDP:

- Uno dei due pti manda un segment con FIN=1ficmp
- Quando il punto riceve il riscontro ACK del FIN inviato considera chiuso il flusso
- I dati possono continuare a fluire in direzione opposta
- La connessione è rilasciata se entrambi i flussi sono chiusi
- Può essere chiusa per time out se ACK non arriva.
  Il primo ACK e il secondo fin possono essere a bordo dello stesso pacchetto!

UDP (non connesso)

Fornisce un servizio di trasmissione non affidabile, il mittente cioè non ha informazione sull' esito della ricezione, viene utilizzato infatti per Trivial file transfer protocol e streaming.
Nell' Header ci sono 4 campi di 16 bit che specificano il port da cui viene mandato il messaggio, il port destinazione, la lunghezza e il checksum.

DNS Domain Name System

Anzichè usare l'indirizzamento ip numerico a 32 bit, si possono utilizzare il namespace, che permette di tradurre gli indirizzi ip in nomi o, viceversa, il mapping (nomi - ip).
L'accesso al mapping (mappatura della rete) avviene con tecniche client-server; sviluppi del mapping: sono stati decentralizzati il sistema di assegnazione dei nomi e la responsabilità, è stato introdotto un database distribuito di corrispondenze nome - indirizzo, il namespace è stato partizionato per migliorare l'efficienza ed è stato dato un controllo autonomo delle assegnazioni.
I nomi sono sequenze di caratteri separate da punti (es: paperino.paperopoli.waltdisney); il punto determina la gerarchia.
Più si va verso destra e più il nome è utilizzato (top level); il nome più a sinistra è unico (host).
Gerarchie del namespace: il livello più alto (top level) della gerarchia partiziona lo spazio dei nomi e delega la gestione dei nomi delle singole partizioni ad autorità locali.
L'autorità top level non deve occuparsi dei cambiamenti interni alle partizioni, se ne occuperanno le autorità locali (o sottoautorità).
La gerarchia viene definita in base alla struttura dell'organizzazione a cui appartengono gli host (Esempio: top level = stato, autorità locali = regioni, host = comuni).
Un dominio è un sottoalbero del namespace (potrebbe essere anche un singolo host), che ha per nome quello della radice (ossia sottoautorità.toplevel). Ci sono pochi domini top level (net, org, com) e nazionali (it, uk, ru). **L'organizzazione dei nomi di internet è detta domain name system (dns);** i **sistemi che realizzano mapping tra nomi e indirizzi sono detti name server (ns),** possono dialogare tra loro e **alcuni di essi hanno una delega per un particolare sottoalbero del namespace (dominio)**.
Un name server ha informazioni su una parte del namespace detta zona, è l'autorità per quella zona e può esserlo anche per altre. Un dominio è più grande rispetto a una zona perché la zona non è composta da tutti i rami del dominio; gli altri sottodomini vengono delegati ad altri name server (namespace > dominio > zona).
Name server: relativamente a una zona un name server può essere primary (unico per la zona dove traduce i nomi) o secondary (più di uno per zona, interpellato se primary non è disponibile), ma anche master (possiede la versione corretta del mapping della zona) e slave (richiede informazioni sul mapping della zona). Generalmente, una zona ha un name server primary master, con altri secondary slave. Un name server può essere contemporaneamente primary master per una zona e secondary slave per altre.
Resolver: **i client che usano i name server si chiamano resolver e sono a bordo degli host**. Un resolver sa interrogare un name server (chiedere l'indirizzo), interpretare le risposte, inviare le informazioni ricavate (ilnumero ip) ai programmi a cui servono. Un resolver non è detto che sia un processo autonomo e **quando serve, per sapere l'indirizzo attraverso il nome, si rivolge al name server.**

Risoluzione: se le informazioni richieste da un resolver sono possedute dal name server, quest'ultimo le fornisce direttamente, altrimenti si rivolge all'autorità radice (top level) del dominio. La radice del dominio a sua volta indicherà al name server un name server più specifico; per questo motivo i name server alle radici hanno migliaia di query ogni ora. La risoluzione può essere ricorsiva o iterativa:

- **Ricorsiva**: il client chiede a quale indirizzo corrisponde il nome n; se il name server non possiede l'indirizzo n, il medesimo deve contattare gli altri server per averlo.
- **Iterativa**: il client chiede a quale indirizzo corrisponde il nome n; se il server non ce l'ha, il client chiede indicazione di un altro server a cui rivolgersi.

Cache: durante le query, un name server apprende molte informazioni sui nomi e sui server che svolgono il ruolo di autorità per molte zone; le informazioni ricavate vengono depositate all'interno di una cache. Bisogna far attenzione al tempo di vita delle informazioni, altrimenti c'è il rischio di memorizzare informazioni obsolete.
Bisogna avere il giusto compromesso tra consistenza ed efficienza.
Resource record: le informazioni dns sono memorizzate in record; ogni dominio è memorizzato in un resource record. I record contengono l'indirizzo ip e altre informazioni. Quando un resolver fa una query relativa a un nome, come risposta ottiene i record associati al nome. U**n resource record è composto dal nome del dominio, dal tempo di vita, dalla classe (in internet è sempre IN), dal tipo (SOA start of authority, è il nome della fonte primaria di informazioni sulla zona, e-mail dell'amministratore**;

A indirizzo ip di un host;
MX specifica il nome dell'host che accetta le mail indirizzate al dominio record;
NS name server per questo dominio) e dal valore (dipendente dal tipo).

Hyper Text Transfer Protocol.

Una connessione è composta dalle seguenti fasi:

1. Apertura della connessione tra client e server **da parte del client**
2. Richiesta del client al server (tramite un pacchetto di richiesta con la specifica desiderata)
3. Risposta del server al client (tramite il pacchetto di risposta)
4. Chiusura della connessione da parte del server.

Avviene **una sola transazione per ogni connessione**; la connessione è senza stati.

Metodi di richiesta:

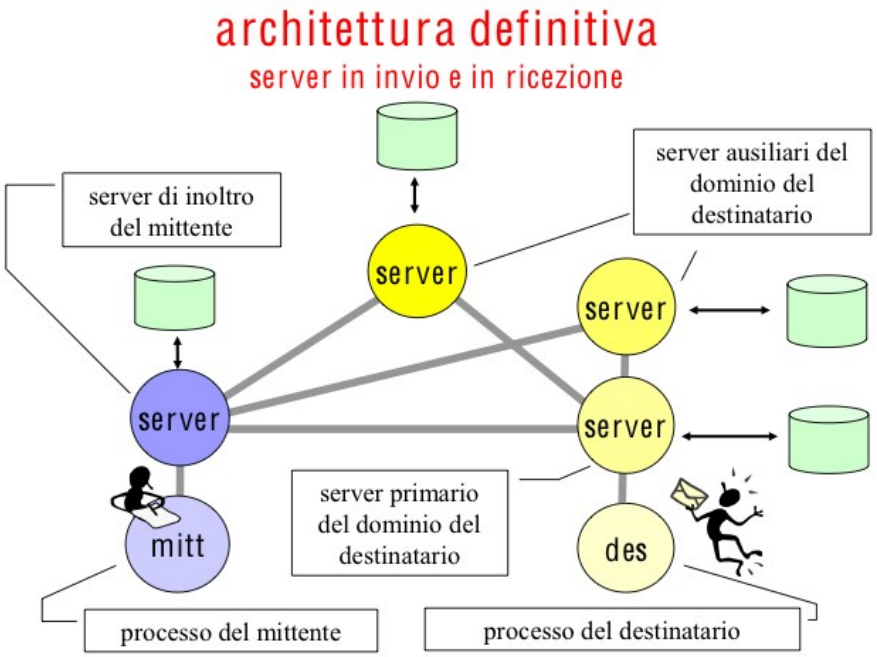
GET: richiede la risorsa indicata;
POST: invia dati alla risorsa indicata;
HEAD: chiede informazioni sulla risorsa indicata;
PUT: ricopia i dati inviati sulla risposta indicata, sostituendo il file presente;
DELETE: richiede la cancellazione di una risorsa;
OPTIONS: richiede di conoscere le opzioni disponibili per il trasferimento della risorsa indicata.

Formato del pacchetto di richiesta
HEADER: con metodo (di richiesta),
RISORSA: (il nome del file richiesto),
VERSIONE (del protocollo http) e informazioni opzionali;
BODY: contiene i dati (inviati dal client al server).

Formato del pacchetto di risposta
HEADER: con versione (del protocollo http),
CODICE (di stato), spiegazione (sul codice di stato) e informazioni opzionali;
BODY: contiene i dati (inviati dal server al client).

Codici di stato: con **200** si indica che il server riesce a esaudire la richiesta del client,
con **400** si indica la richiesta errata,
con **500** si indica una richiesta legittima che non può essere soddisfatta.

La Posta Elettronica



Nel servizio di posta sono coinvolte due componenti fondamentali:

MUA (Mail User Agent) detto anche mailer, consiste in un interfaccia utente utilizzata per accedere al servizio di posta.

MTA (Mail Transmission Agent) è un applicazione che fa da intermediaria nel processo di trasmissione del messaggio dalla sorgente alla destinazione. L' MTA è presente su: Outgoing Mail Server, Mail Exchanger e Incoming Mail Server.

Outgoing Mail Server: è la macchina il cui MTA è quello a cui fa riferimento il MUA per l' inoltro della posta.

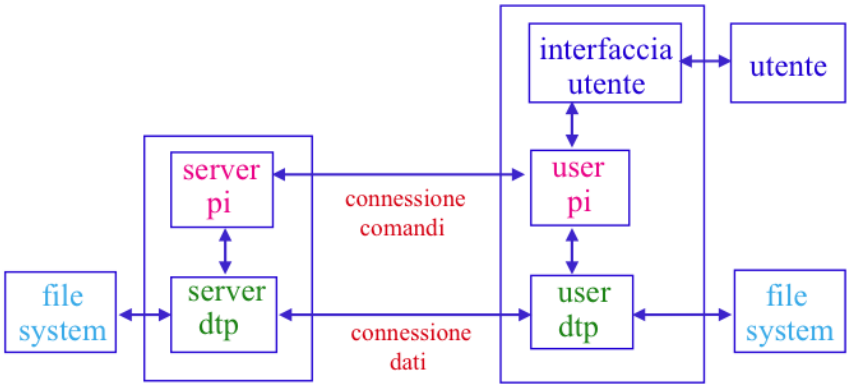
Incoming Mail Server: è la macchina che ospita l'MTA da cui il MUA ritira la posta, generalmente coincide con il Mail eXchanger primario del dominio.

Mail eXchanger: Ogni dominio definisce nel suo DNS una lista di host che ospitano gli MTA che sono incaricati di ricevere posta per il dominio.

SMTP: protocollo relativo al trasferimento del messaggio fino al server del dominio di destinazione.

POP3: protocollo relativo al trasporto dal server del dominio di destinazione al MUA del destinatario.

FTP



Architettura client server a due livelli che ospitano rispettivamente una connessione comandi e una connessione dati.

La connessione comandi resta attiva fino a quando non si decide di chiuderla mentre la connessione dati viene aperta per lo scambio di un file e richiusa al termine del trasferimento.

Sulla connessione comandi transitano le richieste ftp dell' utente e i riscontri FTP del server.

I comandi FTP specificano: data port, transfer mode, reppresentation type, structure.

Comandi: Store, retrieve, append, delete.

INSTAURAZIONE DI UNA CONNESSIONE (IN ACTIVE MODE):

- L' USER-PI attraverso una porta qualunque si connette alla porta 21 del SERVER-PI per la connessione dati.
- <---------(comandi)--------
- Il Client FTP richiede al SO una porta dinamica sulla quale mettere su la connessione dati.
- L' USER-DTP si mette in ascolto su quella porta.
- Il Client comunica al server la coppia <INDIRIZZO_IP, NUMERO PORTA> tramite il comando PORT.
- <----IP, PORT--(comandi)----
- Il server DTP si connette al client.
- -----------(dati)---------->

La connessione la chiude chi invia il file!

In questo caso il user-DTP si comporta come un server poiché attende che sia il server-DTP a richiedere la connessione dati! **Il SERVER** utilizza la porta 21 per essere raggiunto dall' esterno e la 20 la usa come fosse un client per mettere su la connessione dati.

Il CLIENT utilizza una porta dinamica per la connessione comandi e una porta per ricevere la connessione dati (come fosse un server).

In ACTIVE MODE sarebbe possibile evitare il comando PORT del CLIENT verso il SERVER se il server si connettesse direttamente dalla sua porta 20 alla porta dinamica del CLIENT. Il server utilizzando due porte differenti 20 e 21, non creerebbe equivoci tra le due connessioni.

In questo modo però durante la chiusura della connessione DATI alla fine di un trasferimento il TCP lato server entrerebbe in time out per attendere la chiusura rendendo inutilizzabili le porte 20–*porta_dinamica*

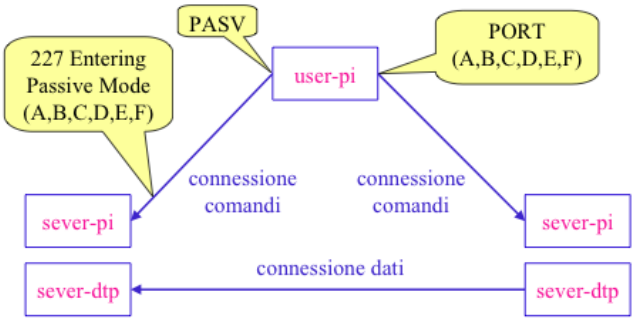
INSTAURAZIONE DI UNA CONNESSIONE (IN PASSIVE MODE)

- In PASSIVE MODE il server è sempre in ascolto anche nel caso della connessione dati.
- Da una porta dinamica l' USER-PI richiede una connessione dati al SERVER-PI con il comando PASV
- <-----(comandi)-----PASV------
- Il SERVER-PI richiede una porta dinamica al suo S.O.
- Il SERVER-DTP si mette in ascolto sulla porta assegnatagli.
- Il SERVER-PI comunica al CLIENT-PI la coppia <indirizzoIP, porta>
- -----(comandi)------IP, PORT-----|
- Il CLIENT DTP si connette al SERVER-DTP
- <----(dati)------------------
-

Il SERVER utilizza la porta 21 su cui riceve la connessione comandi e una porta dinamica assegnatagli dal prorpio S.O.

Il CLIENT utilizza una porta dinamica per la connessione comandi e una per la connessione dati.

TRIANGOLAZIONE IN PASSIVE MODE



La triangolazione in Passive Mode consiste in una doppia connessione FTP PASSIVA tra un client e due server.

Il Client instaura la connessione comandi con i due Server su porta 21 specificando che intende instaurare una connessione PASV.

I due server comunicano le coppie <indirizzoIP, Porta> a questo punto il client connette un server all' altro grazie agli indirizzi ottenuti formando così tra loro una connessione DATI.