Switch

Le prime reti degli anni '80 erano in grado di connettere solo pochi elaboratori, e la loro evoluzione, sollecitata dalle esigenze sempre più diffuse di connessione, è stata possibile grazie ai miglioramenti tecnologici dei mezzi trasmissivi e dei dispositivi di rete a vari livelli.
Tra tutti i dispositivi assume notevole importanza lo **switch,** dispositivo di **livello 2** ,che ha di fatto sostituito gli hub e i bridge, e che consente di segmentare una rete e creare domini di collisione separati per ogni segmento.
Infatti, gli hub consentivano di estendere la rete, ma aumentavano il dominio di collisione.
Per **dominio di collisione** si intende l'insieme di segmenti fisici di rete un cui possono verificarsi collisioni, cioè situazioni in cui più nodi tentano di accedere allo stesso mezzo trasmissivo per trasmettere. L'eccesso di collisioni porta naturalmente al decadimento della velocità di trasmissione all'interno del dominio.
Lo **switch** invece **spezza il dominio di collisione**, permettendo la comunicazione dedicata fra due nodi, che possono trasmettere senza disturbare le trasmissioni fra gli altri nodi, e limitando i casi di collisione alla situazione in cui una stazione debba ricevere contemporaneamente da più emittenti. In tal caso la collisione viene gestita con un buffer di transito che sequenzia i flussi che insistono sulla medesima porta
.
Uno switch è caratterizzato da:

- **numero di interfacce** notevolmente più **elevato** rispetto al bridge
- **capacità di smistare il frame sulla porta** richiesta dall'emittente grazie all'utilizzo di memorie CAM ad accesso veloce
- **trasmissione full duplex**
- **banda garantita** per ogni stazione collegata

I frame vegnono smistati grazie alla **filtering table**. All'interno dello switch è infatti presente una memoria dinamica, la **CAM** (Content Addressable Memory) che mantiene aggiornata una tabella in cui sono memorizzati tutti gli indirizzi MAC mittente dei pacchetti che transitano per le sue porte. La riga della tabella, detta **filtering database** contiene tre valori: il MAC Address, la porta da cui il pacchetto è passato e da quanto tempo è presente in tabella (ageing time). Quando un pacchetto si presenta ad una porta avviene il **learning,** cioè l'aggiornamento del filtering database, poi si analizza il pacchetto e si cerca nella filtering table il MAC destinatario. Se esso è presente si invia il pacchetto alla sola porta interessata, qualora questo non sia presente nella tabella avviene il **flooding**, cioè il pacchetto viene smistato su tutte le porte tranne quella di provenienza. Mentre all'accensione la CAM è vuota e quindi lo switch si comporta come un hub, il filtraggio aumenta man mano che la tabella si riempie,
Il mezzo trasmissivo più utilizzato per associare una porta dello switch ad un host, il cosiddetto microsegmento, è il cavo **UTP** 5 che, usando una coppia di fili per la trasmissione e una per la ricezione, consente la comunicazione full duplex e consente quindi un raddoppio della banda di trasmissione. Gli switch full duplex sono stati introdotti nel 1997 con lo standard IEEE802.3x e evitano le collisioni prevedendo due canali fisici separati per ricezione e trasmissione e regolando i flussi contemporanei con appositi buffer di memorizzazione: Essi utilizzano il protocollo MAC control per mettere in pausa temporanea i nodi trasmittenti, evitando le collisioni, ma dando comunque origine a un rallentamento dovuto appunto a questi pacchetti di PAUSE.

I router

I **router**, detti anche **IS** (Intermediate System) sono dei dispositivi del livello di Network o Rete (**livello 3** di ISO/OSI) che permettono di "scegliere" il percorso che i datagrammi prenderanno per arrivare a destinazione.
I compiti più importanti che un router svolge sono il **routing,** cioè l' **individuazione del miglior percorso,** l' aggiornamento della tabella di instradamento e l'**inoltro** cioè passaggio del pacchetto al nodo successivo.
Quindi il **routing** , in una rete a commutazione di pacchetti , è **il processo di selezione del percorso** sul quale spedire un pacchetto, mentre **il router è il dispositivo** che svolge questa operazione.
Quando gli indirizzi di sorgente e destinazione hanno lo **stesso identificatore di rete**, il r**outing è diretto,** l'indirizzo è recuperato a livello di datalink tramite ARP e nessun router è coinvolto nella trasmissione.
Se gli indirizzi di sorgente e destinazione hanno identificatori di rete diversi , l'istradamento avviene tra reti fisiche distinte: il **routing è indiretto(indirect delivery).** L'host non è in grado di comunicare direttamente con il destinatario e delega ad un altro host (router) il compito di trasmettere il pacchetto. Ogni rete fisica appartenente ad un internet deve includere almeno un router.
Gli elementi necessari al funzionamento del livello 3 sono:

- il **router** e le sue **porte** di inoltro
- gli **indirizzi** contenuti nei pacchetti da inoltrare
- la tabella di instradamento, TdI**,** o **tabella di routing**, che contiene i dettagli dei cammini
- l'**algoritmo** di TdI, che fornisce le regole di compilazione della TdI.

Di fatto il livello 3 è l'ultimo che interagisce con l'hardware, i livelli superiori al 3 sono esclusivamente software.
L'indirizzo a cui spedire un datagram è individuato con la consultazione delle tabelle o tavole di routing IP. La tavola di routing è una lista di percorsi (rotte) che possono essere create staticamente (comando route) o dinamicamente (ICMP redirect)
La tabella di routing è una tabella che contiene delle righe con le regole che consentono al router di decidere su che porta un pacchetto deve essere inoltrato.
Ogni riga contiene varie informazioni:
destinazione: indirizzo di host o network (**Destination net address**)
netmask: netmask della destinazione
interfaccia: **porta** locale da usare per la rotta (**Interface)**
gateway: Ip del next hop, cioè identificatore della porta fisica del router successivo verso la destinazione
flag: informazioni riguardanti la rotta
•Metric: peso assegnato al cammino

La coppia dest_net_addr + subnet_mask serve per identificare la possibile sottorete di destinazione
La coppia next_hop + interface serve per determinare univocamente dove instradare il datagramma

Quando riceve un pacchetto di livello 3 , trasmesso al livello IP, il router guarda l'intestazione del datagramma ed estrae l'indirizzo di destinazione.
Se l'indirizzo IP di destinazione appartiene a uno degli indirizzi cui una delle interfacce del router è collegata, l'informazione può essere inviata al livello 4 dopo che l'intestazione IP sia stata disincapsulata (tolta).
Se invece l'indirizzo IP di destinazione fa parte di una rete diversa, il router consulta le righe della propria tabella di routing, che definisce il percorso da prendere per un indirizzo dato, e consulta il campo **Porta** della riga per inoltrarlo. E' sufficiente conoscere il prossimo router a cui inviare il datagram (next hop).

Il messaggio è così mandato da router in router per salti successivi, fino a che il destinatario appartenga ad una rete direttamente connessa ad un router. Quest'ultimo trasmetterà allora direttamente il messaggio al terminale scelto.
Questo meccanismo consistente nel riconoscere solo l'indirizzo del prossimo passaggio che porta a destinazione viene detto routing per salti successivi (**next-hop routing)**
Quando il destinatario appartiene a una rete non referenziata nella tabella di routing., il router usa un router di default (detto anche **Gateway predefinito**).

La dimensione della tabella influisce fortemente sui tempi di trasmissione, quindi bisogna costruire tabelle di piccole dimensioni. Le tecniche per controllare la dimensione delle tabelle sono basate sul principio del mascheramento dell'informazione: divisione dell'indirizzo IP in indirizzo di rete ed indirizzo di host, una sola rotta per tutti gli host di una rete,utilizzo di un solo indirizzo di rete per più reti fisiche (subnetting e supernetting), proxy ARP, rotte di default

In caso di indirect delivery, il ruolo del router, soprattutto quello della tabella di routing, è molto importante. Quindi il funzionamento di un router è determinato dal modo in cui questa tabella di routing è creata.

- Se la tabella di routing è inserita manualmente dall'amministratore, si parla di **routing non adattativo o statico** (utilizzabile per piccole reti)
- Se il router costruisce da solo la tabella di routing in funzione delle informazioni ricevute (attraverso i protocolli di routing), si parla di **routing adattativo o dinamico**

In caso di router statico, è l'amministratore che aggiorna la tabella di routing.
In caso di router dinamico, invece, un protocollo detto **protocollo di routing** permette l'aggiornamento automatico della tabella affinché contenga in ogni momento il percorso ottimale.

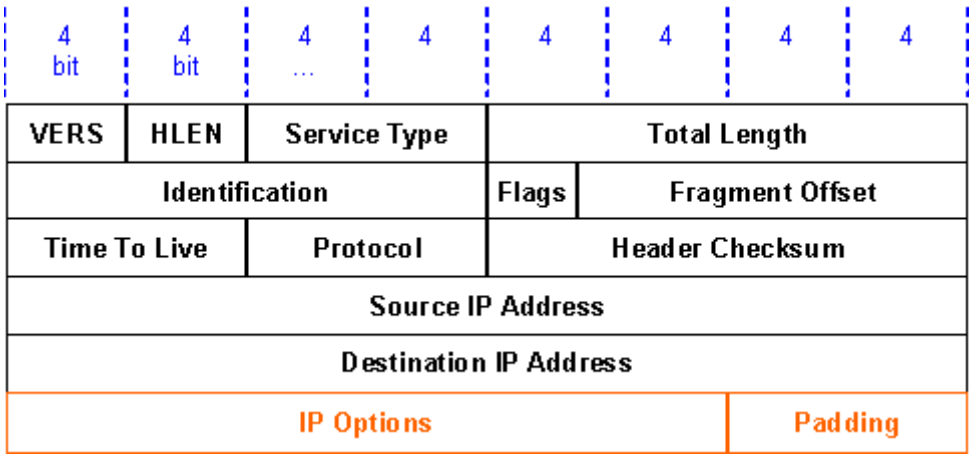
Il pacchetto IP

Il compito fondamentale del protocollo IP è dunque quello di instradare e inoltrare messaggi sulla rete nella modalità best-effort delivery (miglior sforzo per spedire a destinazione) pur senza effettuare correzione di errori. Ma è un suo compito anche frammentare e riassemblare i messaggi.
Quando un host invia dei dati, questi seguono un percorso dall'alto verso il basso e, secondo il principio dell'incapsulamento, ogni livello agiunge un header con una serie di informazioni di controllo, fino al livello di rete dove avviene fisicamente la trasmissione.
Al livello di rete , il dato assume il nome di **datagramma (IP datagram)**, avrà già incapsulato l'header del livello applicativo e del livello trasporto secondo questo schema:

IP	TCP head	APP head	Dati

Ogni singolo pacchetto IP ,detto datagramma **,** viene frammentato in pacchetti di 1500 byte.

L'intestazione o header del datagram IP è descritta da RFC 791 è costituita da alcuni gruppi di 4 byte, 20 byte fissi e da una parte opzionale di lunghezza variabile secondo questo schema:



I campi del formato datagram hanno le seguenti funzioni:

- **VERS**, indica la versione del protocollo IP del pacchetto, quindi IPv4
- **HLEN o IHL** (Internet header length) indica la lunghezza dell'header del datagram IP (numero di parole da 32 bit)
- **Service Type**, specifica come un protocollo di livello inferiore deve trattare il pacchetto in riferimento al routing (priorità, ritardo, affidabilità,...)
- **Total length,** indica la lunghezza del datagram indicata in byte, comprensiva dell'intestazione e dei dati. Non può superare 64K.

I tre campi identification, flag, offset servono a controllare frammentazione e riassemblaggio dei datagram

- **Identification,** valore intero che serve all'host ricevente per individuare a quale datagram appartiene il frammento che arriva a destinazione
- **Flags :** indica se è possibile o meno frammentarlo, se è l'ultimo frammento o un frammento intermedio ecc.
- **Fragment Offset,** indica la posizione del frammento nel datagram originale
- **Time to live, (TTL)** indica il tempo in secondi (a partire da 255 fino a 0) che il datagram può rimanere nella rete Internet prima di essere scartato, viene decrementato da ogni router e viene scartato quando arriva a 0.
- **Protocol,** specifica il protocollo di livello superiore cui appartengono i dati del datagram
- **Header Checksum,** controlla se l'header del datagram contiene errori, nel qual caso il datagram viene scartato
- **Source IP address,** contiene l'indirizzo IP dell'unità che ha generato il datagram
- **Destination IP address**, contiene l'indirizzo IP del destinatario
- **Option**, di lunghezza variabile, può fornire opzioni sulla sicurezza e sul routing (sui router attraversati e/o da attraversare, grado di segretezza del pacchetto, ecc.)
- **Padding,** di lunghezza variabile, serve a rendere l'header un multiplo di 32 bit