

## Modulo 8 – Ethernet Switching

Upon completion of this module, the student will be able to perform tasks related to the following:

8.1	Ethernet Switching
8.2	Collision Domains and Broadcast Domains

### 8.1 Ethernet Switching

#### 8.1.1 Bridging a livello 2

Aumentando il numero di nodi su un singolo segmento aumenta la probabilità di avere collisioni e quindi ritrasmissioni. Una soluzione è spezzare segmenti grandi in parti più piccole e separate creando domini di collisioni isolati. Per far questo un bridge mantiene una tabella di indirizzi MAC e delle porte ad essi associati. Il bridge decide di inoltrare un frame o buttarlo in base a questa tabella.

- All'avvio la tabella del bridge è vuota, si mette in ascolto e quando arriva un frame lo processa.
- Il bridge aggiunge l'indirizzo MAC della sorgente del frame e la porta su cui è arrivato alla tabella e non sapendo su quale porta sia l'indirizzo del destinatario lo invia sulla porta opposta a quella dove il frame è arrivato, come farebbe un repeater.
- Quando il destinatario risponde viene memorizzato nella tabella anche il suo indirizzo MAC e la porta su cui è.
- Da questo momento il traffico tra questi 2 PC avviene solo sulle porte interessate, per cui se i 2 PC sono sulla stessa porta il frame non viene passato sull'altra porta.

#### 8.1.2 Switching a livello 2

Solitamente un bridge ha solo 2 porte e divide il dominio di collisione in 2 parti. Poiché agisce a livello 2 (sugli indirizzi MAC) e non a livello 3 (sugli indirizzi IP) un bridge divide un dominio di collisione ma non un dominio broadcast, che può essere diviso solo da un router.

Uno switch è un bridge multiporta veloce, ogni porta crea il proprio dominio di collisione. Lo switch crea una tabella detta CAM (Content Addressable Memory) che contiene gli indirizzi MAC e la porta corrispondente all'indirizzo MAC.

#### 8.1.3 Operazione dello Switch

Nel caso più semplice una porta dello switch è collegata ad un solo host. Questo piccolo segmento fisico è detto microsegmento. Un cavo UTP usa una coppia di fili per la trasmissione ed un'altra per la ricezione, è possibile quindi che i segnali passino contemporaneamente nelle 2 direzioni, questa possibilità di comunicazione è detta full duplex. Molti switch e molte NIC funzionano in full duplex, per cui non si devono contendere il mezzo e non esiste più il dominio di collisione. Teoricamente si raddoppia la banda in full duplex.

La CAM è un tipo di memoria che sostituisce quella convenzionale che permette ad uno switch di trovare la porta associata ad un indirizzo MAC senza usare algoritmi di ricerca.

ASIC (Application Specific Integrated Circuit) è un circuito integrato programmabile che svolge funzioni logiche ad alta velocità che viene usato per passare i frame da una porta all'altra velocemente. Le operazioni che prima venivano fatte software ora sono fatte hardware con l'ASIC e quindi si riducono i tempi.

### 8.1.4 Latenza

La latenza è il ritardo tra il tempo in cui il frame lascia la sorgente ed il tempo in cui arriva a destinazione. Molte condizioni possono causare ritardi:

- I segnali lungo i media hanno una velocità finita, per cui più lungo è il cavo e maggiore sarà il ritardo
- I ritardi dei circuiti elettronici posti lungo il percorso che devono analizzare il segnale
- I ritardi software causati dalle decisioni sullo switching e sui protocolli
- I ritardi causati dal contenuto del frame e da quando vengono prese le decisioni di switching, ad esempio un frame non può essere inviato da uno switch almeno finché non viene letto l'indirizzo MAC di destinazione.

### 8.1.5 Modi dello Switch

Uno switch può privilegiare o la latenza o l'affidabilità.

Uno switch può iniziare il trasferimento del frame sulla porta di destinazione non appena riceve l'indirizzo MAC di destinazione, tale metodo è detto *cut through* e dà la minore latenza tuttavia non viene fatto nessun controllo di errore.

All'opposto lo switch può aspettare la ricezione dell'intero frame prima di inviarlo sulla porta di destinazione, questo metodo detto *store and forward* permette di valutare l'FCS (Frame Check Sum) e quindi garantire che il frame sia corretto. Se il frame è difettoso viene buttato.

Un compromesso tra i 2 precedenti è il metodo *fragment free*, che legge solo i primi 64 bytes, che includono l'header del frame, prima di iniziare la trasmissione. Questo modo verifica l'affidabilità degli indirizzi e delle informazioni del protocollo LLC per assicurare che la destinazione ed il trattamento dei dati siano corretti.

Quando si usa il metodo cut through le porte sorgente e destinazione devono operare alla stessa velocità per tenere il frame intatto, questo è detto switching sincrono. Se le velocità sono diverse, occorre memorizzare l'intero frame prima di iniziare la trasmissione, questo è detto switching asincrono e si può usare nel metodo store and forward. Lo switching asincrono permette la connessione tra porte con bande diverse, ad esempio 100 Mbps e 1000 Mbps, si usa ad esempio per le connessioni client server, dove il server richiede più banda.

### 8.1.6 Spanning-Tree Protocol

Spesso le reti con switch sono progettate con percorsi ridondanti che forniscono affidabilità e tolleranza agli errori. I percorsi ridondanti sono desiderabili ma possono creare effetti indesiderati come i switching loop, che creano broadcast storm ed in breve intasano una rete. Per evitare questi loop gli switch hanno un protocollo di base chiamato Spanning-Tree. Ogni switch della Lan usando questo protocollo manda dei messaggi detti BPDU (Bridge Protocol Data Units) fuori da tutte le porte per conoscere l'esistenza di altri switch e per eleggere un root bridge nella rete. Gli switch usano l'algoritmo Spanning-Tree (STA) per bloccare i percorsi ridondanti.

Ogni porta dello switch nel protocollo Spanning-Tree può avere 5 stati:

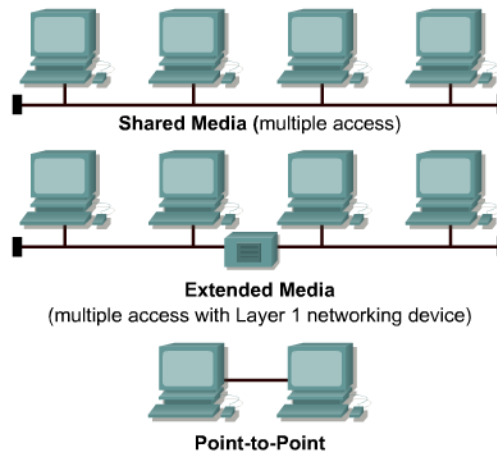
States	Purpose
Blocking	Receives BPDUs only
Listening	Building "active" topology
Learning	Building bridging table
Forwarding	Sending and receiving user data
Disabled	Administratively down

Il risultato dell'eliminazione dei loop è quello di creare un albero logico gerarchico, tuttavia i percorsi alternativi sono ancora disponibili per quando sarà necessario.

## 8.2 Domini di collisione e broadcast

### 8.2.1 Ambiente di mezzo condiviso

Ci possono essere vari tipi di reti:



- Mezzo condiviso: si ha quando più host hanno l'accesso allo stesso mezzo.
- Mezzo condiviso esteso: in questo caso ci sono dispositivi di rete che possono estendere la lunghezza del mezzo.
- Punto a punto: è molto usato nelle connessioni di rete dialup (tramite modem) ed è il più usato per gli utenti a casa. Un dispositivo è collegato solo ad un altro dispositivo.

Le collisioni possono avvenire solo in un mezzo condiviso. Ci sono regole per determinare chi può accedere al mezzo, ma a volte si hanno le stesse collisioni.

### 8.2.2 Domini di collisioni

I domini di collisione sono i segmenti fisici di rete dove si possono verificare collisioni.

Le collisioni fanno sì che reti diventino inefficienti, ogni volta che avviene una collisione tutte le trasmissioni si bloccano per un periodo di tempo variabile determinato da un algoritmo di backoff per ogni dispositivo di rete.

I tipi di dispositivi che interconnettono i segmenti definiscono i domini di collisioni:

- I dispositivi di livello 1 (hub e repeater) estendono il dominio di collisione
- I dispositivi di livello 2 (bridge e switch) spezzano il dominio di collisione
- I dispositivi di livello 3 (router) spezzano il dominio di collisione

Lo spezzare il dominio di collisione incrementa il numero di domini di collisione ed è chiamato segmentazione.

Più dispositivi ci sono in un dominio di collisione e maggiore è la probabilità di avere collisioni.

La regola dei 4 repeater stabilisce che non si possano mettere più di 4 repeater tra 2 computer qualsiasi della rete. Se non si rispetta questa regola si può violare il limite massimo di ritardo consentito e questo incrementa drammaticamente le collisioni.

Una late collision si ha quando una collisione avviene dopo i primi 64 bytes. Le NIC sono progettate per non ritrasmettere automaticamente dopo una late collision e questo aggiunge del ritardo detto *consumption delay*.

La regola 5-4-3-2-1 richiede che si abbiano:

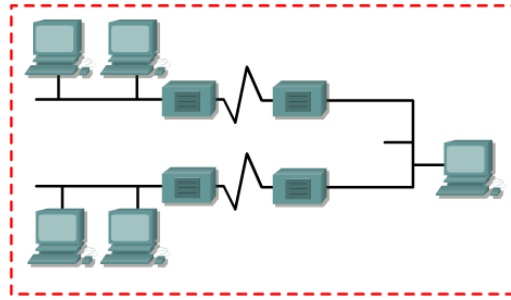
5 segmenti

4 repeater o hub

3 segmenti con host

2 sezioni senza host

1 largo dominio di collisione

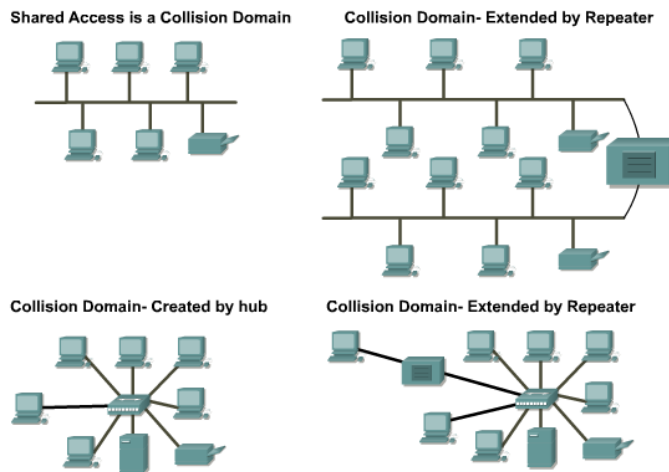


- - - - - = Collision Domain

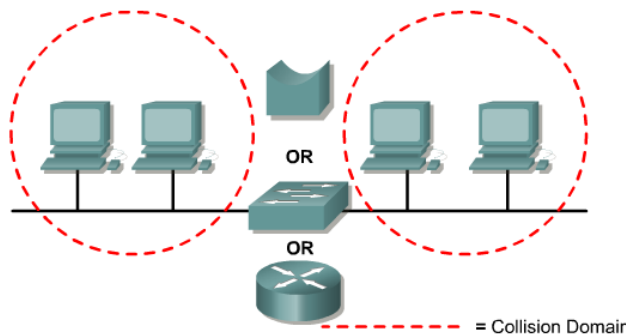
### 8.2.3 Segmentazione

La storia di come la tecnologia Ethernet tratta le collisioni ed i domini di collisione proviene dagli studi fatti dall'Università delle Hawaii nel 1970, che sviluppò un protocollo detto Aloha per la comunicazione wireless tra le isole. Il protocollo Ethernet si basa sul protocollo Aloha.

Una importante abilità per il progettista di reti è individuare i domini di collisione. I dispositivi di livello 1 allungano ma non controllano i domini di collisione.



I dispositivi di livello 2 segmentano i domini di collisione.



- - - - - = Collision Domain

Questo rende più efficiente la trasmissione su segmenti diversi perché evita le collisioni.

A causa dei ritardi però i dispositivi di livello 2 possono diventare anche dei colli di bottiglia e rallentare le comunicazioni.

Anche i dispositivi di livello 3 spezzano i domini di collisione.

### 8.2.4 Broadcast di livello 2

Per comunicare con tutti i domini di collisione i protocolli usano frame di tipo broadcast o multicast a livello 2 del modello OSI. Quando un host vuole comunicare con tutti gli altri usa un frame broadcast con indirizzo di destinazione FF-FF-FF-FF-FF-FF, questo è un indirizzo a cui tutte le NIC devono rispondere.

I dispositivi di livello 2 propagano i frame broadcast e multicast su tutte le porte. In alcuni casi i messaggi broadcast possono saturare la banda e non concedere spazio per i dati, questa situazione è detta *broadcast storm*.

Le 3 sorgenti di messaggi broadcast e multicast sono le workstation, i router e le applicazioni multicast.

Le workstation usano i broadcast quando fanno una ARP request, cioè per trovare un indirizzo MAC noto l'indirizzo IP.

I protocolli di routing come ad esempio il RIP che invia gli update ogni 30 sec incrementano di molto i messaggi broadcast.

Le applicazioni multicast possono peggiorare le performance di reti grandi.

### 8.2.5 Domini broadcast

Un dominio broadcast è un insieme di domini di collisione collegati da dispositivi di livello 2. Spezzare una LAN in più domini di collisione fa aumentare la probabilità che un host riesca ad accedere al mezzo. I domini broadcast sono controllati a livello 3, perché i router non propagano i frame broadcast. Un router agisce a livelli 1, 2, 3 e inoltra un pacchetto se l'indirizzo di rete di destinazione è diverso dall'indirizzo di rete sorgente.

### 8.2.6 Introduzione al flusso dei dati

I dati a livello 3 vengono incapsulati aggiungendo gli indirizzi IP sorgente e destinazione e a livello 2 vengono aggiunti gli indirizzi MAC sorgente e destinazione.

I dispositivi di livello 1 non fanno filtraggio, lasciano sempre passare i frame sugli altri segmenti di rete, essi rigenerano e risincronizzano solamente i segnali portandoli alla stessa qualità di trasmissione originale. Ogni segmento collegato a dispositivi di livello 1 è parte degli stessi domini di collisione e broadcast.

I dispositivi di livello 2 filtrano i dati in base all'indirizzo MAC di destinazione. I frame sono lasciati passare a meno che la destinazione non sia sullo stesso segmento della sorgente. I dispositivi di livello 2 spezzano i domini di collisione ma mantengono un solo dominio broadcast.

I dispositivi di livello 3 filtrano i pacchetti in base all'indirizzo IP di destinazione. Un frame è inviato solo se l'indirizzo di rete di destinazione è diverso da quello della sorgente. I dispositivi di livello 3 spezza sia i domini di collisione che broadcast.

### 8.2.7 Cosa è un segmento?

La definizione dipende dal contesto: a livello hardware un segmento è una sezione di una rete collegata da bridge, switch o router.

Nel protocollo TCP i dati sono suddivisi in piccole unità chiamate segmenti della dimensione massima di 1500 bytes.