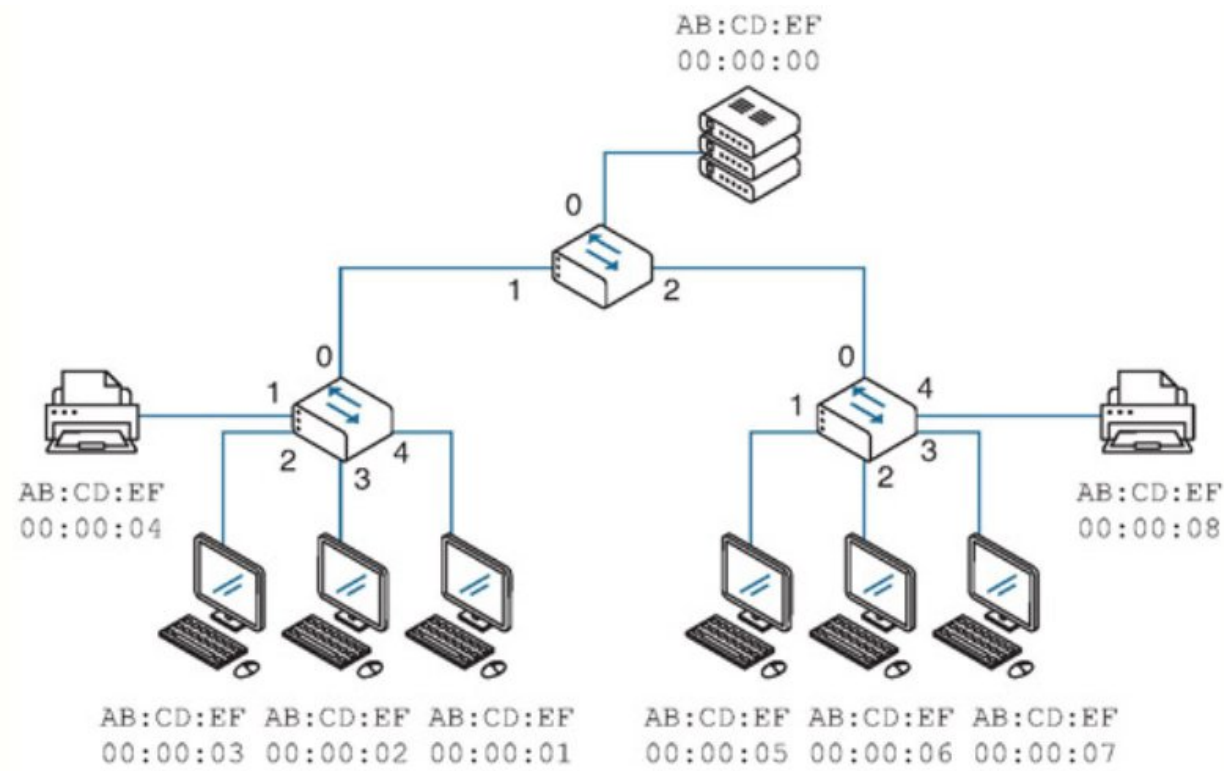


Esercizi svolti – SWITCH



Nell'ipotesi che gli switch siano stati appena accesi, se il PC con indirizzo MAC AB:CD:EF:00:00:01 invia una richiesta alla stampante connessa allo stesso switch, avente indirizzo MAC AB:CD:EF:00:00:04, il relativo frame avrà il seguente contenuto

Preambolo	SOF	Indirizzo destinazione	Indirizzo origine	Lunghezza dati	Dati	FCS
...	...	AB:CD:EF 00:00:04	AB:CD:EF 00:00:01

e la tabella MAC dello switch, inizialmente vuota, diverrà la seguente in quanto il frame viene ricevuto dalla porta 4 a cui è connesso il PC

Porta	Dispositivi
0	
1	
2	
3	
4	AB:CD:EF:00:00:01

Lo switch non ha nella propria tabella MAC l'indirizzo di destinazione per cui effettua il flooding inviando il frame su tutte le porte che risultano connesse a un altro dispositivo (0, 1, 2, 3), esclusa la porta di provenienza (4). Il frame sarà ricevuto non solo dagli end device del laboratorio, ma – attraversando gli altri switch – anche dal server e da tutti gli end device dell'altro laboratorio se questi sono accesi: solo la stampante che ha l'indirizzo MAC di destinazione del frame lo elaborerà, tutti gli altri dispositivi lo scarteranno.

Com'è tipico nel modello client/server, la stampante risponderà al PC di origine della richiesta ricevuta, costruendo il seguente frame

Preambolo	SOF	Indirizzo destinazione	Indirizzo origine	Lunghezza dati	Dati	FCS
...	...	AB:CD:EF 00:00:01	AB:CD:EF 00:00:04

Quando lo switch del laboratorio lo riceve (dalla porta 1 a cui è connessa la stampante) aggiorna la propria tabella MAC che diviene la seguente

Porta	Dispositivi
0	
1	AB:CD:EF:00:00:04
2	
3	
4	AB:CD:EF:00:00:01

e, trovando l'indirizzo MAC di destinazione nella tabella associato alla porta 4, inoltra il frame esclusivamente su questa porta: il frame viene ricevuto solo dal PC che ha lo stesso indirizzo MAC indicato nella destinazione.

Si noti che lo switch ha associato alle porte a cui sono connessi sia il PC sia la stampante i relativi indirizzi MAC: altri frame che in futuro avranno questi indirizzi come destinazione saranno inoltrati sulla porta corretta, evitando il flooding che viene effettuato esclusivamente in caso di mancanza di informazioni.

Se il PC con indirizzo MAC AB:CD:EF:00:00:03 invia una richiesta al server, che ha indirizzo MAC AB:CD:EF:00:00:00, il relativo frame avrà il seguente contenuto

Preambolo	SOF	Indirizzo destinazione	Indirizzo origine	Lunghezza dati	Dati	FCS
...	...	AB:CD:EF 00:00:00	AB:CD:EF 00:00:03

e la tabella MAC dello switch del laboratorio diverrà la seguente in quanto il frame viene ricevuto dalla porta 2 a cui è connesso il PC

Porta	Dispositivi
0	
1	AB:CD:EF:00:00:04
2	AB:CD:EF:00:00:03
3	
4	AB:CD:EF:00:00:01

Lo switch non ha nella propria tabella MAC l'indirizzo di destinazione per cui effettua il flooding inviando il frame su tutte le porte che risultano connesse a un altro dispositivo (0, 1, 2, 3), esclusa la porta di provenienza (2). Il frame sarà quindi ricevuto dallo switch a cui è connesso il server dalla porta 1, dalla quale aveva in precedenza ricevuto per effetto del flooding il frame proveniente dal PC con indirizzo MAC AB:CD:EF:00:00:00 e la sua tabella MAC avrà a questo punto il seguente contenuto

Porta	Dispositivi
0	
1	AB:CD:EF:00:00:01 AB:CD:EF:00:00:03
2	

Nella tabella non è presente l'indirizzo MAC di destinazione per cui lo switch effettua il flooding inviando il frame su tutte le porte che risultano connesse a un altro dispositivo (0, 2), esclusa la porta di provenienza (1). Il frame sarà quindi ricevuto non solo dal server, ma – attraverso l'altro switch della rete – anche da tutti gli end device dell'altro laboratorio se questi sono accesi: solo il server che ha l'indirizzo MAC di destinazione del frame lo elaborerà, tutti gli altri dispositivi lo scarteranno.

Il server risponderà al PC trasmettendo un frame con il seguente contenuto

Preambolo	SOF	Indirizzo destinazione	Indirizzo origine	Lunghezza dati	Dati	FCS
---	---	AB:CD:EF 00:00:03	AB:CD:EF 00:00:00	---	---	---

Lo switch lo riceve dalla porta 0 e aggiorna di conseguenza la propria tabella MAC

Porta	Dispositivi
0	AB:CD:EF:00:00:00
1	AB:CD:EF:00:00:01 AB:CD:EF:00:00:03
2	

nella quale trova, associato alla porta 1, l'indirizzo di destinazione: il frame viene di conseguenza inoltrato esclusivamente su questa porta dalla quale raggiunge lo switch del laboratorio nella cui tabella MAC si trova l'indirizzo di destinazione associato alla porta 2, sulla quale viene inoltrato per essere ricevuto dal PC che ha l'indirizzo MAC di destinazione.

Si noti che, con l'attuale contenuto delle tabelle MAC degli switch coinvolti, eventuali altre richieste inoltrate al server dagli end device dello stesso laboratorio non saranno inoltrate in flooding, ma raggiungeranno esclusivamente l'end device designato

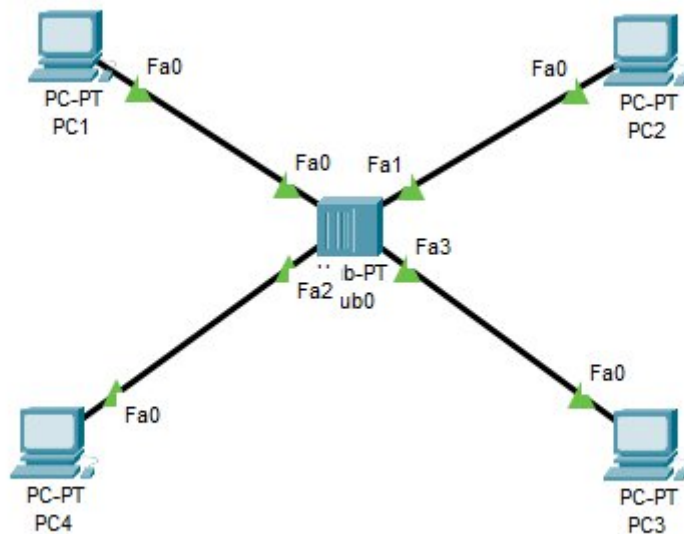
Esercizio rete peer to peer con hub (peer-to-peer con hub.pkt)

Configurare una piccola rete formata da 4 computer connessi tra loro tramite un hub seguendo la tabella seguente per l'indirizzamento IP:

PC1		PC2		PC3		PC4	
IP address	192.168.1.1	IP address	192.168.1.2	IP address	192.168.1.3	IP address	192.168.1.4
subnet mask	255.255.255.0	subnet mask	255.255.255.0	subnet mask	255.255.255.0	subnet mask	255.255.255.0

SVOLGIMENTO

1. Aprire il programma Packet Tracer e inserire 1 hub e 4 PC nel workspace.
2. Collegare all'hub le schede di rete (FastEthernet) di ciascun PC con il cavo UTP "Copper Straight-through". La comparsa dei due triangolini verdi all'estremità di ciascun cavo indica che la connessione a livello Physical è funzionante



3. Configurare ogni PC in modalità statica, inserendo nei campi IPv4 Address e Subnet Mask i valori indicati nella tabella.

Test di connettività

Restando in modalità Realtime, eseguire il test di connettività con il comando ping.

Simulare il comportamento della rete

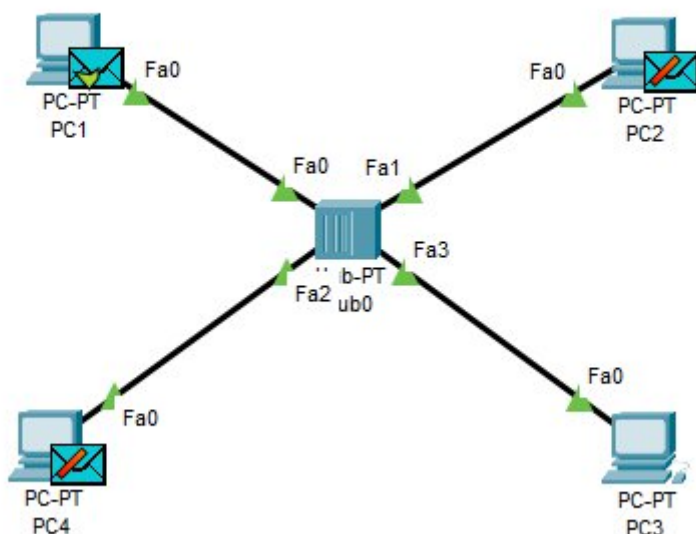
Aprire l'ambiente di simulazione selezionando la modalità Simulation. Usare un filtro così da visualizzare nella Event List le PDU di interesse. È importante sottolineare che il filtro agisce solo sulla visualizzazione, rendendo più veloce la simulazione, che non deve mostrare tutti gli eventi. Le PDU che sono state filtrate, però, continuano a essere presenti nella rete e a influenzarne il traffico.

Nel nostro scenario vogliamo simulare il comportamento della rete quando PC1 invia un ping a PC3, quindi:

1. nel Simulation Panel cliccare su Edit Filters e selezionare solo ICMP, togliendo l'eventuale spunta a tutte le altre PDU;
2. nella toolbar secondaria selezionare "Add Simple PDU" e cliccare prima su PC1 e poi su PC3;
3. clic su Play per avviare la simulazione; i pulsanti "Play Controls" sono presenti sia nella toolbar inferiore sia nel Simulation Panel; in questo pannello è anche disponibile uno slider che permette di variare la velocità con cui avviene l'animazione.

Il pacchetto inviato da PC1 è ricevuto da PC2, PC3 e PC4, ma solo PC3 accetta il pacchetto, gli altri dispositivi lo cestinano. Analogamente il pacchetto di risposta che PC3 invia a PC1, viene ricevuto anche da PC2 e PC4, che, però, lo scartano.

Nella figura seguente è mostrata la ricezione della risposta inviata da PC3, che termina il flusso di dati transitati in rete a seguito dell'invio del ping (Simple PDU) da parte di PC1



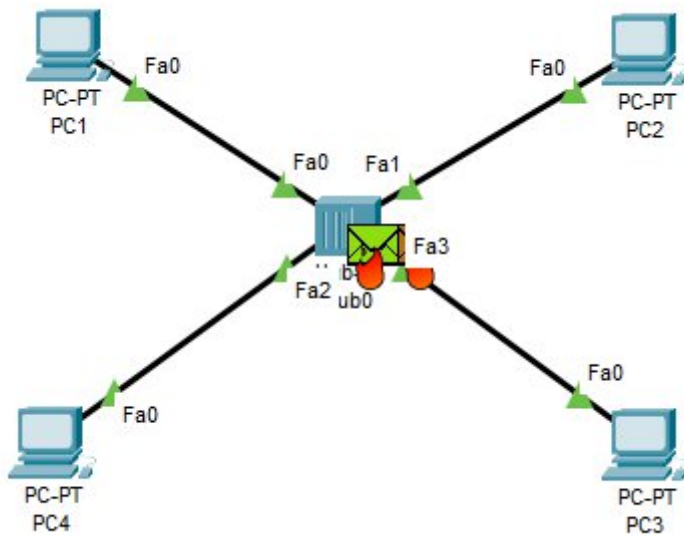
Per ogni PDU catturata, in Event List sono visualizzate le seguenti informazioni:

- **Visible:** la presenza dell'icona di un occhio indica che un evento sta accadendo in quel momento e l'icona sarà presente per tutti i pacchetti che sono visibili nell'animazione in quel dato istante;
- **Time:** il tempo, in secondi, in cui si è verificato l'evento è calcolato in modo relativo, a partire dall'ultimo restart della simulazione; inoltre, il tempo avanza solo quando ci sono eventi da catturare, in caso contrario si ferma e riparte quando si verifica il prossimo evento;
- **Last Device:** indica il dispositivo che aveva il pacchetto prima dell'attuale;
- **At Device:** indica il dispositivo dove si trova il pacchetto in quel momento;
- **Type:** visualizza il tipo di pacchetto catturato, ossia la PDU relativa al protocollo coinvolto (ICMP, HTTP, ecc.), è presente anche un riquadro colorato: a ogni protocollo corrisponde un colore diverso.

Per cancellare gli eventi presenti nella Event List e riportare lo scenario allo stato iniziale, si usa il pulsante **Reset Simulation**. Se, invece, si vuol eliminare la simulazione della PDU in esame, il ping nel nostro caso, si usa il pulsante **Delete** presente nella toolbar inferiore.

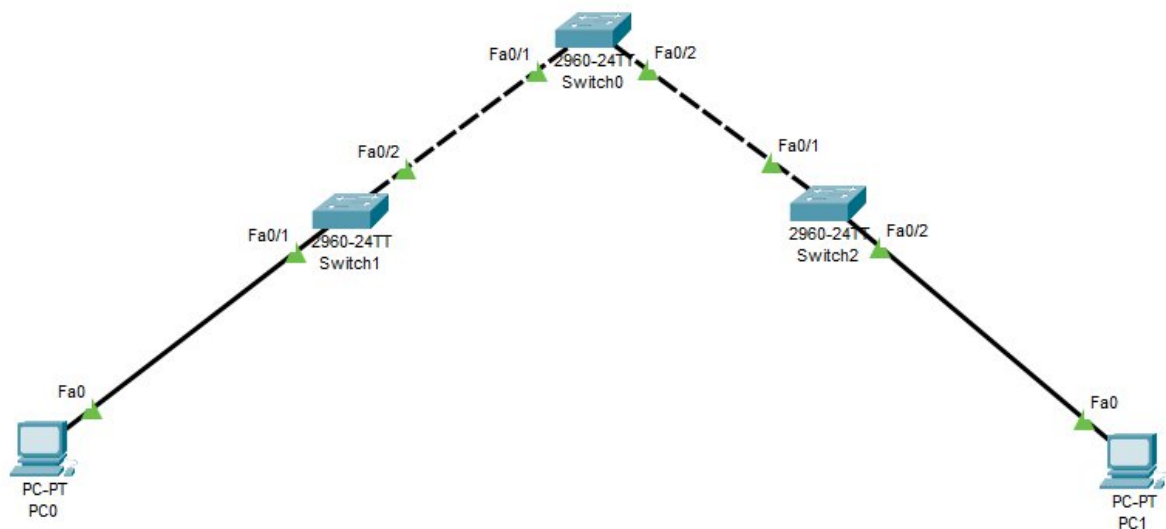
Simulare una collisione

Si provi contemporaneamente a fare due ping, uno da PC1 a PC3 e l'altro da PC2 a PC4: avviene una collisione nell'hub che è segnalata graficamente dalle due fiamme rosse sui pacchetti



Esercizio visualizzazione MAC Table

Realizzare la rete di figura:



PC0: 192.168.1.1 — 255.255.255.0

PC1: 192.168.1.2 — 255.255.255.0

Verificare il funzionamento dello switching attraverso l'osservazione delle MAC Table appena realizzata la connessione fisica (triangolino verde) e dopo aver inviato una PDU tra i due PC posti alle due estremità della rete

SVOLGIMENTO

Dopo aver inserito i dispositivi sul workspace e dopo averli opportunamente collegati configuriamo gli indirizzi dei PC.

Svuotiamo la MAC Table di tutti gli switch con il comando:

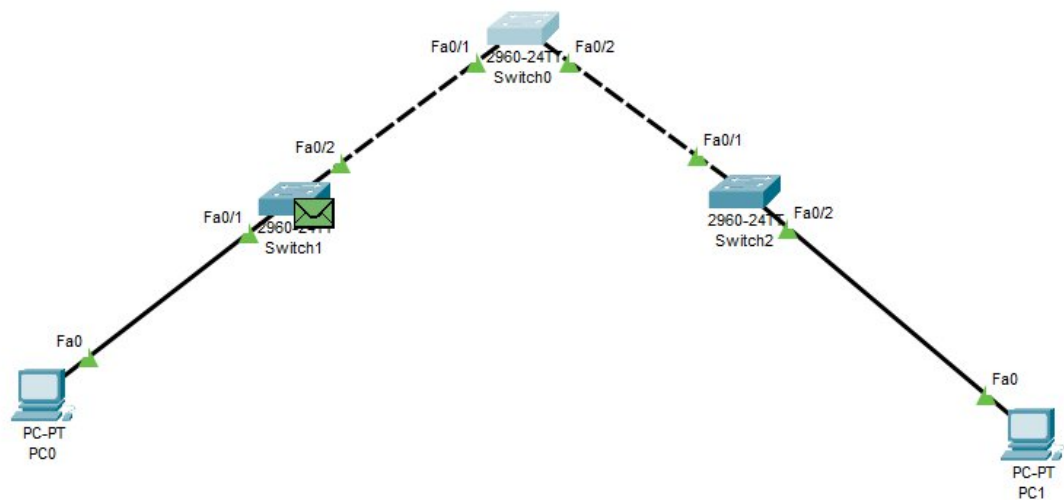
```
Switch#clear mac-address-table dynamic
```

Ora visualizziamo la MAC Table dello Switch0 con il comando:

```
Switch#show mac-address-table dynamic
```

```
Switch#show mac-address-table dynamic
Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       0000.0c71.0101   DYNAMIC     Fa0/2
1       0002.17c0.2402   DYNAMIC     Fa0/1
```

In modalità simulazione inviamo un pacchetto da PC0 a PC1, avviamo la simulazione e con la lente di ingrandimento, cliccando sullo switch e scegliendo MAC Table visualizziamo:



MAC Table for Switch0

VLAN	Mac Address	Port
1	0000.0C71.0101	FastEthernet0/2
1	0002.17C0.2402	FastEthernet0/1
1	0005.5E10.9057	FastEthernet0/1
1	0050.0F2E.C9...	FastEthernet0/2

La figura mostra l'istante in cui la PDU di ritorno sta giungendo a PC0, quindi la penultima entry in tabella indica il MAC Address del PC0 collegato alla Fa0/1 dello switch mentre l'ultima rappresenta il MAC Address del PC1 collegato alla Fa0/2