

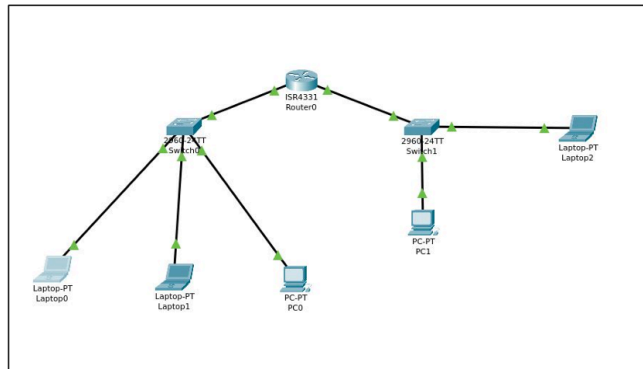
W1S1L4

Il laboratorio di oggi consiste nella creazione e configurazione di una rete di calcolatori con il tool Cisco Packet Tracer, come in figura. Lo scopo è capire come funzionano le comunicazioni a livello 2 e 3 del modello ISO / OSI con i rispettivi device di rete.

Esercizio:

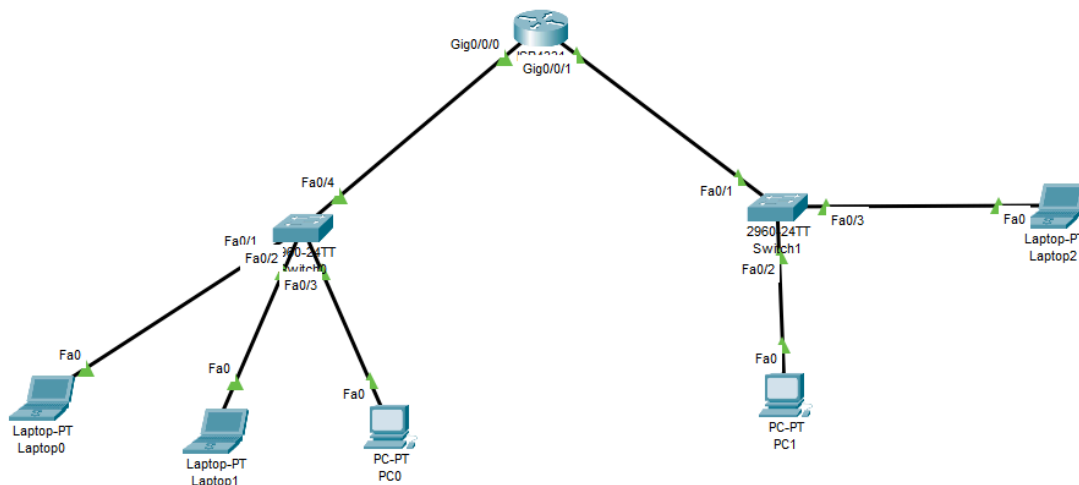
- Mettere in comunicazione il laptop-PT0 con IP 192.168.100.100 con il PC-PT-PC0 con IP 192.168.100.103
- Mettere in comunicazione il laptop-PT0 con IP 192.168.100.100 con il laptop-PT2 con IP 192.168.200.100
- Spiegare, con una relazione, cosa succede quando un dispositivo invia un pacchetto ad un altro dispositivo di un'altra rete.

Architettura target:



Topologia Logica

La topologia logica che abbiamo creato è costituita da due reti LAN (Local Area Network) che possono comunicare tra di loro attraverso l'utilizzo di un router che le mette in contatto.



Configurazione del Router Centrale

In questa sezione viene mostrata la configurazione del router utilizzato per mettere in comunicazione le due LAN. Il router ha due interfacce, ognuna collegata a una rete diversa, e tramite la configurazione viene reso capace di gestire il traffico tra di esse. Di seguito sono riportati gli step principali eseguiti per configurare il dispositivo, con uno screenshot per ogni fase importante.

Configurazione dell'hostname

Iniziamo configurando l'hostname del router da interfaccia di comando per poterlo riconoscere.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#
```

Nel momento esatto in cui entriamo in un router, ci troviamo nella **user EXEC mode**, che viene indicata dal simbolo `>` dopo il nome del router (hostname). Questa modalità ci permette solamente di visualizzare alcuni dati sul router, ma non consente di fare alcuna modifica. Utilizziamo il comando `enable` per accedere alla **privileged EXEC mode**, una modalità più avanzata che consente più libertà di comando. In seguito, usiamo il comando `configure terminal` per accedere alla **configuration mode**, che ci permette di modificare diverse impostazioni del nostro router. Da questa modalità, lanciamo il comando `hostname R1` e cambiamo il nome del nostro router.

La seconda cosa da fare è attivare le interfacce, perché di default le interfacce di un router sono in modalità "shutdown", cioè disattivate.

```
R1(config)#interface g0/0/0
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0, changed state to up


R1(config-if)#interface g0/0/1
R1(config-if)#no shutdown

R1(config-if)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/1, changed state to up

R1(config-if)#
```

Sempre dalla **configuration mode**, entriamo nelle singole interfacce (g0/0/0 e g0/0/1) e lanciamo il comando `no shutdown` per attivarle.

 **Nota:** In questi casi si può utilizzare anche il comando `interface range` per accedere a più interfacce contemporaneamente, ma in questo esercizio ho preferito seguire una procedura step by step per maggiore chiarezza.

Dopo aver attivato le interfacce, che ora possono comunicare con i dispositivi collegati, dobbiamo configurare un indirizzo IP per ogni interfaccia attiva. Questo indirizzo funzionerà da **gateway predefinito** per tutti i dispositivi che vorranno raggiungere il router per comunicare con il mondo esterno o con altre reti.

```
R1(config)#interface GigabitEthernet0/0/0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface G0/0/1
R1(config-if)#ip address 192.168.200.1 255.255.255.0
R1(config-if)#
```

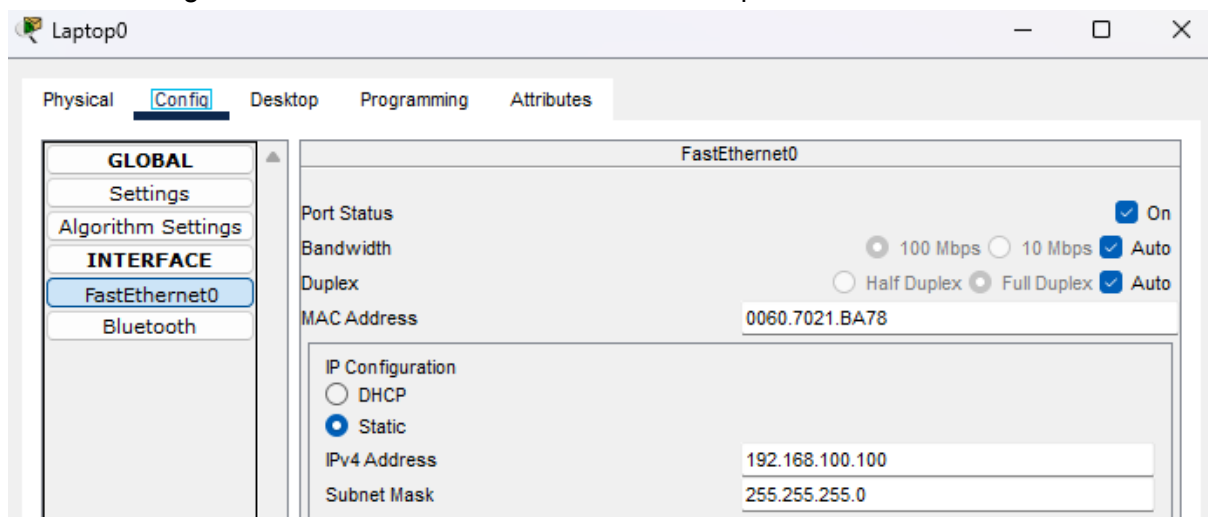
Entriamo nelle singole interfacce utilizzando il comando `interface interface-id` e, con il comando `ip address`, assegniamo un indirizzo IP ad ogni interfaccia attiva.

La configurazione del router è ora completata con successo e il dispositivo è pronto per mettere in comunicazione due reti LAN diverse.

Configurazione degli End Hosts

Dopo aver configurato il router, è arrivato il momento di configurare gli end hosts, che in questo caso sono solo dei PC o laptop. Per questa esercitazione andremo a configurare solamente i dispositivi che dovranno comunicare tra loro, ma la procedura è valida per qualsiasi dispositivo collegato alla rete.

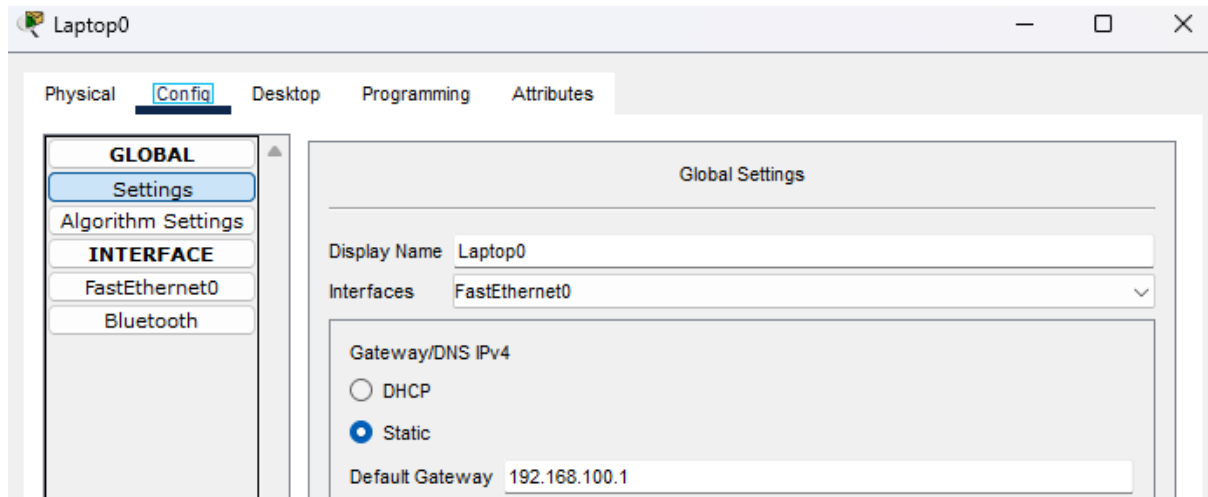
Iniziamo configurando un indirizzo IP insieme alla sua rispettiva subnet mask.



In questo caso utilizziamo la GUI (Graphic User Interface) per configurare i dispositivi. Inseriamo l'indirizzo IP fornito dalla traccia dell'esercizio e impostiamo la subnet mask. In questo caso, la subnet mask `255.255.255.0` indica che i primi tre byte (24 bit) vengono

usati per identificare la parte di rete, mentre l'ultimo byte (8 bit) serve a identificare la parte host, cioè il singolo dispositivo all'interno della rete.

Dopo aver configurato l'indirizzo IP e la subnet mask, possiamo procedere con l'impostazione del **default gateway**, che permetterà al PC o laptop di raggiungere il router.



Seguiamo lo stesso procedimento per tutti i dispositivi interessati e, una volta completata la configurazione, saremo finalmente pronti per far comunicare tra loro le nostre due reti LAN.

Comunicazione intra-LAN (Local Area Network)

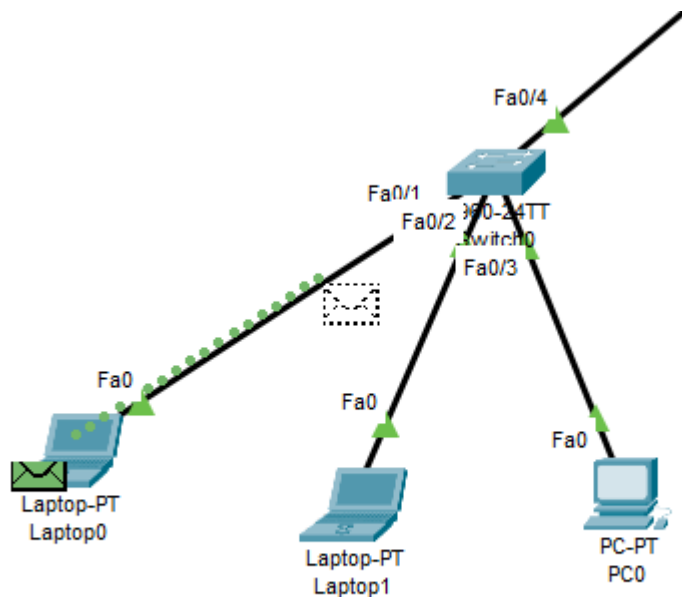
Dopo aver configurato tutti i dispositivi interessati, siamo pronti per farli comunicare tra di loro. Come primo esempio faremo comunicare due dispositivi collegati alla stessa rete locale, nello specifico Laptop0 e PC0.

```
Pinging 192.168.100.103 with 32 bytes of data:

Reply from 192.168.100.103: bytes=32 time=8ms TTL=128
Reply from 192.168.100.103: bytes=32 time=4ms TTL=128
Reply from 192.168.100.103: bytes=32 time=4ms TTL=128
Reply from 192.168.100.103: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.100.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

In questo momento ci troviamo nel command prompt di Laptop0 e utilizziamo il comando **ping** con l'indirizzo IP di PC0 per inviare una serie di messaggi e verificare se è attivo e correttamente connesso alla rete.



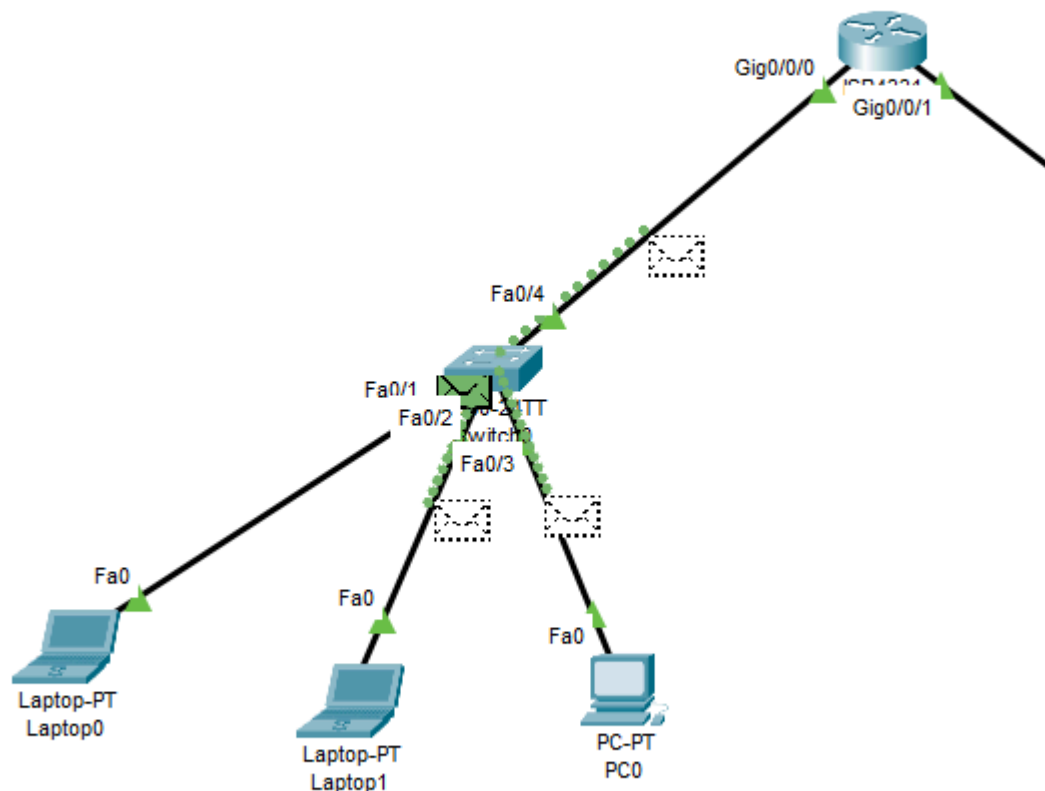
Laptop0 vuole comunicare con PC0. Prima di farlo, deve sapere se PC0 è attivo e raggiungibile, quindi decide di inviare un ping al suo indirizzo IP. Tuttavia, a questo punto c'è un piccolo problema: Laptop0 conosce l'indirizzo IP di PC0, ma non il suo indirizzo MAC, necessario per poter inviare i pacchetti sulla rete locale.

A livello 2 del modello OSI (Data Link), le comunicazioni all'interno della rete funzionano tramite indirizzi MAC (Media Access Control), che sono univoci per ogni scheda di rete e vengono utilizzati dagli switch per indirizzare correttamente i pacchetti. Quando Laptop0 vuole comunicare con PC0 ma non conosce il suo MAC, entra in gioco il protocollo ARP (Address Resolution Protocol).

Il funzionamento è il seguente: Laptop0 invia una ARP Request in broadcast all'interno della LAN, chiedendo "Chi ha l'indirizzo IP 192.168.100.103?" (l'IP di PC0). Essendo un messaggio broadcast, viene ricevuto da tutti i dispositivi connessi allo switch, ma solo PC0, riconoscendo il proprio indirizzo IP nella richiesta, risponderà con una ARP Reply. Questa risposta, inviata in unicast, contiene il suo indirizzo MAC.

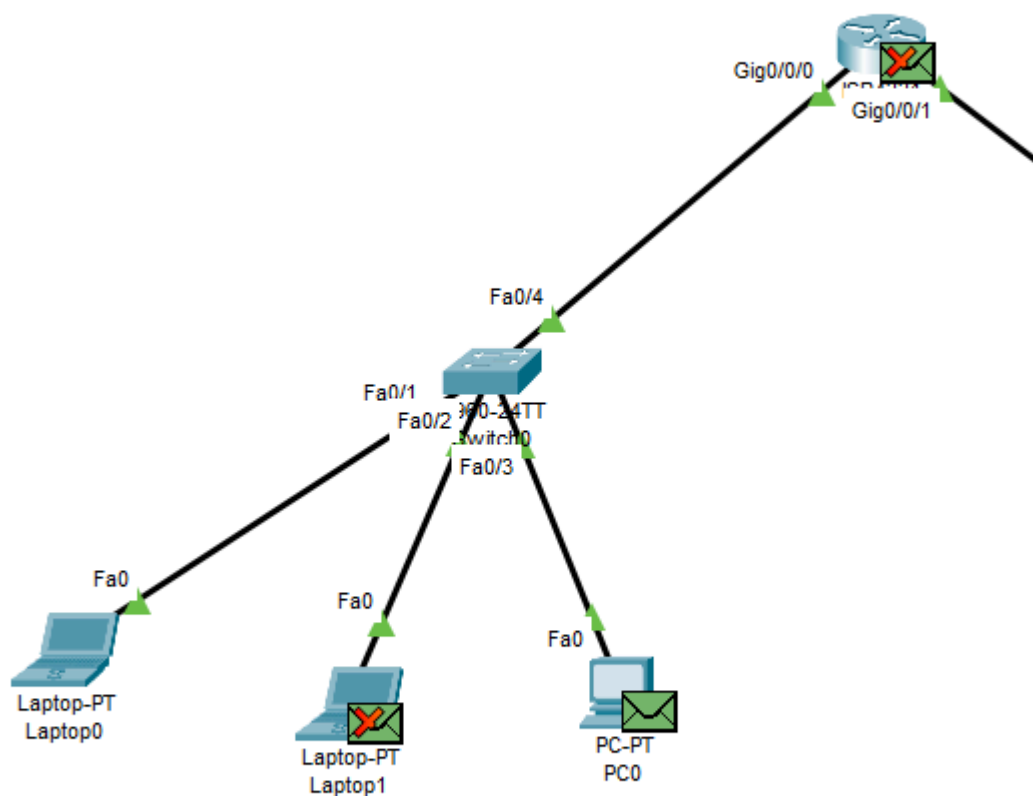
Grazie a questo scambio, Laptop0 ottiene il MAC di PC0 e può finalmente inviare i pacchetti ICMP (ping) direttamente al destinatario. Da questo momento, la comunicazione continua in unicast: i pacchetti viaggiano tra i due dispositivi attraverso lo switch, che nel frattempo ha popolato la sua MAC address table associando ogni indirizzo MAC alla porta da cui l'ha visto arrivare.

Tutto questo processo dimostra come, prima ancora di poter testare la connettività a livello IP con **ping**, sia necessario un meccanismo di risoluzione degli indirizzi a livello inferiore per permettere il corretto inoltro dei pacchetti.

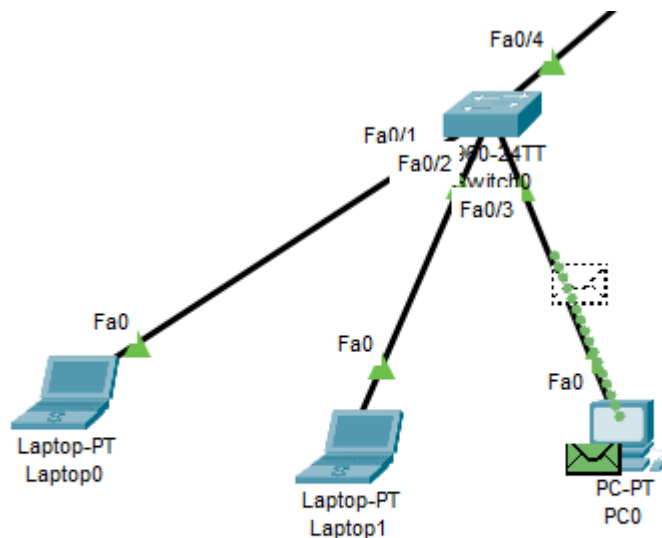


Switch0 riceve la richiesta ARP inviata da Laptop0 e, non avendo ancora appreso l'indirizzo MAC del destinatario, inoltra il messaggio su tutte le sue porte, tranne quella da cui l'ha ricevuto. Questo comportamento è tipico degli switch quando devono gestire un pacchetto con destinazione sconosciuta.

Poiché lo switch è un dispositivo di **livello 2** del modello OSI, non è in grado di interpretare gli indirizzi IP, ma si basa esclusivamente sugli **indirizzi MAC** per instradare i frame. Non conoscendo ancora a quale porta è collegato il MAC di PC0, lo switch si comporta come un "ripetitore intelligente", trasmettendo il frame ARP a tutti i dispositivi collegati, sperando che il destinatario corretto risponda.

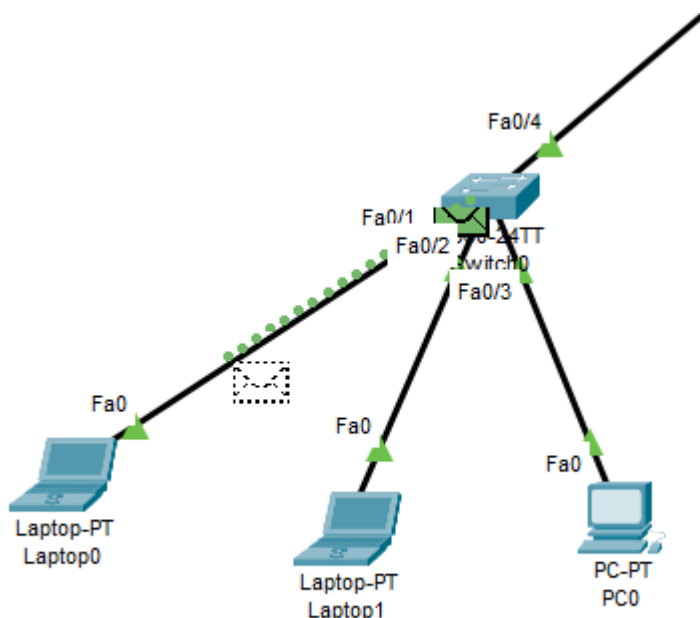


Il pacchetto ARP inviato in broadcast dallo switch raggiunge tutti i dispositivi collegati alla rete. Ogni dispositivo controlla il contenuto del pacchetto, in particolare l'indirizzo IP di destinazione. Solo il dispositivo con un indirizzo IP corrispondente a quello indicato nella richiesta – in questo caso PC0 – riconosce il pacchetto come destinato a sé e lo accetta. Tutti gli altri dispositivi, non essendo i destinatari, **ignorano** il pacchetto.



PC0, dopo aver ricevuto il pacchetto ARP Request, invia una risposta chiamata **ARP Reply**. A differenza della richiesta iniziale, che era un messaggio **broadcast** inviato a tutti i dispositivi della rete, la risposta è invece un messaggio **unicast**: viene cioè spedito solo al mittente, in questo caso Laptop0.

Il pacchetto ARP Reply contiene l'indirizzo MAC di PC0 e viene inviato direttamente al MAC di Laptop0, che aveva originato la richiesta. Grazie a questa risposta, Laptop0 può ora completare il processo di risoluzione ARP e salvare l'associazione IP-MAC nella sua cache.

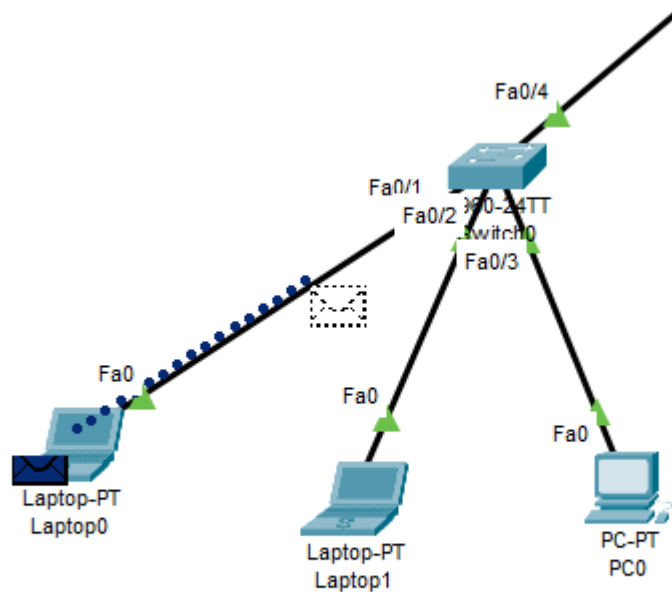


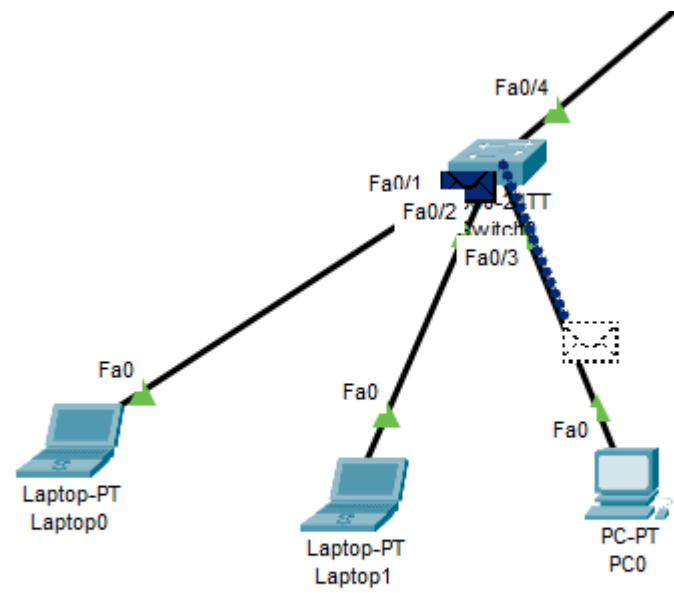
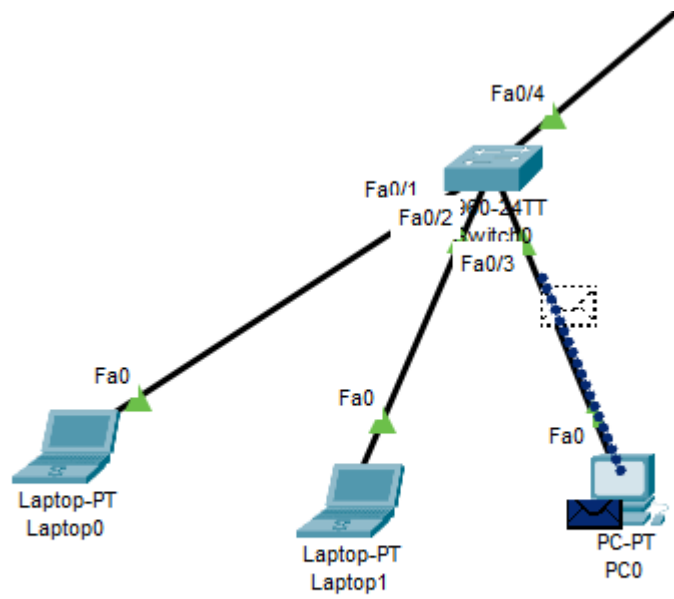
Lo switch riceve il pacchetto ARP Reply da PC0 e lo inoltra direttamente a Laptop0, senza doverlo inviare su tutte le sue porte. Questo è possibile grazie a una tabella interna chiamata **MAC address table**, che lo switch utilizza per memorizzare l'associazione tra indirizzi MAC e le porte fisiche su cui si trovano.

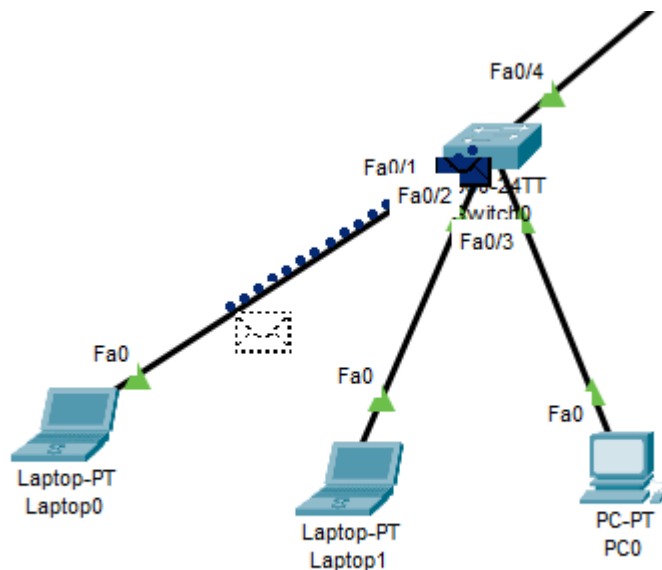
Durante lo scambio iniziale (ARP Request), lo switch ha imparato il MAC di Laptop0 e lo ha associato alla porta da cui è arrivato. Quando poi riceve l'ARP Reply da PC0, aggiorna la tabella salvando anche il MAC di PC0 con la relativa porta.

A questo punto entrambi i dispositivi sono nella tabella MAC e lo switch può gestire i futuri scambi di dati in modalità **unicast**, cioè inoltrando i pacchetti solo alla porta corretta, senza doverli più diffondere su tutta la rete.

Dopo questo scambio di ARP Request e ARP Reply, Laptop0 ha tutte le informazioni necessarie per iniziare una vera comunicazione IP con PC0. Può quindi finalmente inviare il ping, che raggiungerà PC0 seguendo il percorso giusto all'interno della LAN.







Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop0	ICMP
	0.000	--	Laptop0	ARP
	0.001	Laptop0	Switch0	ARP
	0.002	Switch0	Laptop1	ARP
	0.002	Switch0	PC0	ARP
	0.002	Switch0	R1	ARP
	0.003	PC0	Switch0	ARP
	0.004	Switch0	Laptop0	ARP
	0.004	--	Laptop0	ICMP
	0.005	Laptop0	Switch0	ICMP
	0.006	Switch0	PC0	ICMP
	0.007	PC0	Switch0	ICMP
👁	0.008	Switch0	Laptop0	ICMP

Infine, utilizzando la modalità **Simulation** del tool Packet Tracer, possiamo osservare in dettaglio lo scambio dei pacchetti che abbiamo descritto nei passaggi precedenti. Ogni messaggio ARP e ICMP viene visualizzato in ordine cronologico, permettendoci di comprendere meglio come avviene la comunicazione all'interno della rete locale.

Comunicazione Inter-LAN (Local Area Network)

In questa parte dell'esercitazione, mettiamo in comunicazione due LAN differenti passando attraverso il router. Il dispositivo Laptop0 invierà un ping a Laptop2, che si trova su un'altra rete.

Il processo è molto simile a quello visto per la comunicazione intra-LAN: prima viene eseguita una richiesta ARP (ARP Request) per conoscere l'indirizzo MAC del gateway, poi una risposta (ARP Reply), e solo dopo inizia il vero scambio di pacchetti ICMP per il ping.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop0	ICMP
	0.000	--	Laptop0	ARP
	0.001	Laptop0	Switch0	ARP
	0.002	Switch0	Laptop1	ARP
	0.002	Switch0	PC0	ARP
	0.002	Switch0	R1	ARP
	0.003	R1	Switch0	ARP
	0.004	Switch0	Laptop0	ARP

Nella prima fase, Laptop0 invia una ARP Request per scoprire il MAC del router, che funge da gateway. Dopo aver ricevuto l'ARP Reply, invia il pacchetto ICMP verso il router.

0.004	--	Laptop0	ICMP
0.005	Laptop0	Switch0	ICMP
0.006	Switch0	R1	ICMP
0.006	--	R1	ARP
0.007	R1	Switch1	ARP
0.008	Switch1	PC1	ARP
0.008	Switch1	Laptop2	ARP
0.009	Laptop2	Switch1	ARP
0.010	Switch1	R1	ARP

Il router, ricevuto il pacchetto, lo instrada verso la seconda rete. Se non conosce ancora il MAC di Laptop2, effettua una nuova ARP Request e riceve l'ARP Reply. Dopo aver appreso il MAC, inoltra il ping verso Laptop2.

6.004	--	Laptop0	ICMP
6.005	Laptop0	Switch0	ICMP
6.006	Switch0	R1	ICMP
6.007	R1	Switch1	ICMP
6.008	Switch1	Laptop2	ICMP
6.009	Laptop2	Switch1	ICMP
6.010	Switch1	R1	ICMP
6.011	R1	Switch0	ICMP
6.012	Switch0	Laptop0	ICMP

Laptop2 riceve il pacchetto ICMP e risponde correttamente. Il ping di Laptop0 verso Laptop2 è completato con successo, confermando che la comunicazione tra le due LAN funziona.