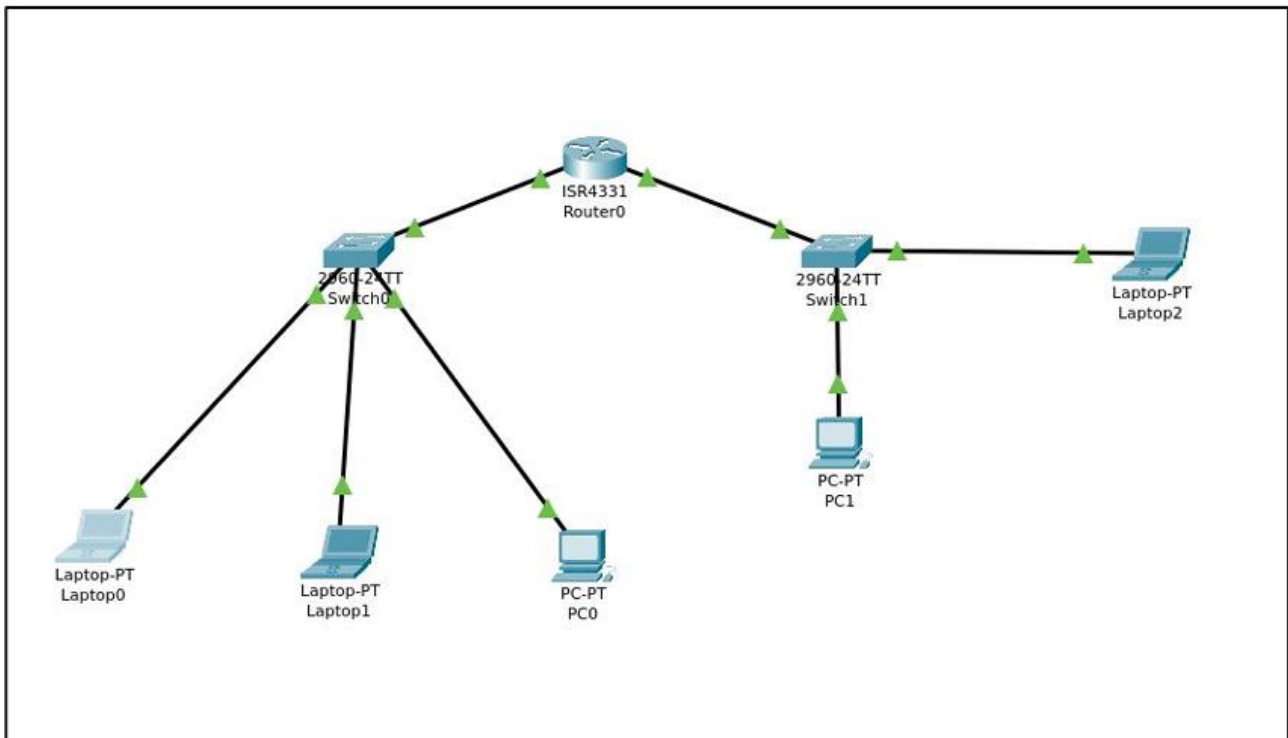


Task:

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



- Come richiesto da traccia, ho iniziato a inserire i vari indirizzi IP nei vari dispositivi, quindi nel PC-PT-PC0 avremo i seguenti dati. *(N.B. Vedremo solo i dati di un dispositivo, ma la procedura è uguale per tutti i dispositivi richiesti dalla traccia)*

Physical Config Desktop Programming Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IPv4 Address: 192.168.100.103

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.100.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ Automatic ☒ Static

IPv6 Address:

Link Local Address: FE80::201:64FF:FE87:EA1B

Default Gateway:

DNS Server:

802.1X

☐ Use 802.1X Security

Authentication: RADIUS

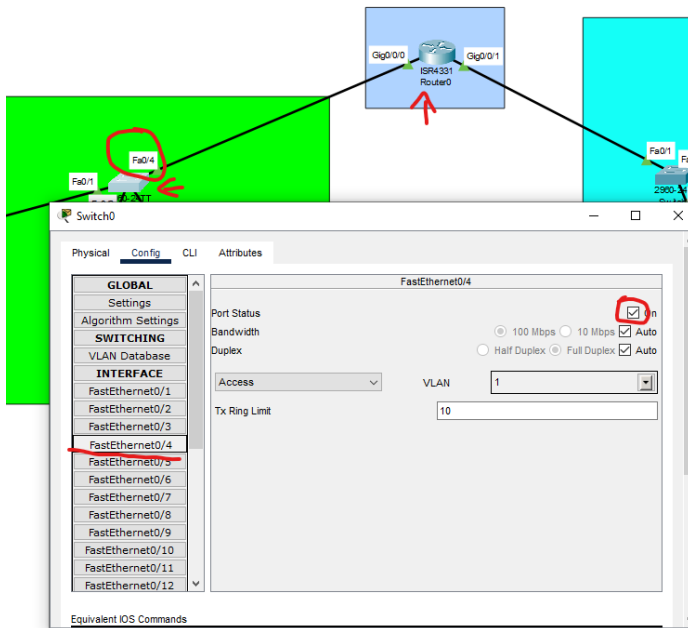
Username:

Password:

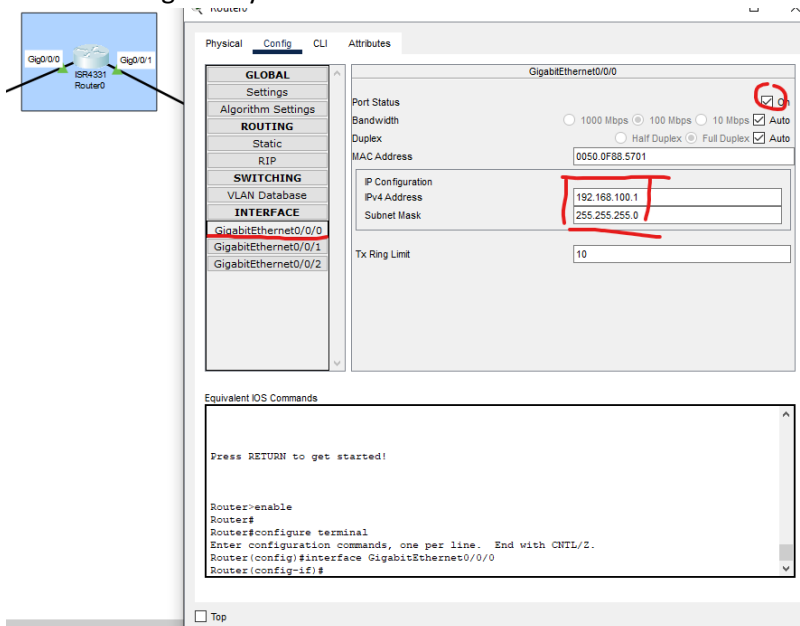
☐ Top

Noterai che insieme all'indirizzo IP e la subnet Mask, abbiamo inserito il Gateway. Questo ci permetterà di comunicare con il router.

Per permettere ciò, però, c'è ancora un passaggio molto importante da fare, ovvero assegnare l'interfaccia: Come vediamo in figura, lo Switch ha interfaccia Fa0/4, quindi attiveremo quella porta spuntando ON.



Stessa cosa vale per il nostro Router. Sappiamo che la sua interfaccia è 0/0/0 in questo caso, quindi inseriremo il gateway nel IPv4 Address del nostro Router e la subnet mask, spuntando ON.



Adesso il nostro switch e il nostro router possono comunicare.

Non ci resta altro che iniziare a fare un piccolo test tramite il prompt dei comandi, pingando i dispositivi come richiesto dalla nostra task, così da capire se tutto funziona correttamente.

Come fare? Apriamo il prompt del nostro Laptop PT0 una volta aperto, scriveremo il seguente prompt: “ping 192.168.100.103 che sarebbe l’IP del dispositivo con il quale vogliamo comunicare.

```
C:\>ping 192.168.100.103

Pinging 192.168.100.103 with 32 bytes of data:

Reply from 192.168.100.103: bytes=32 time<1ms TTL=128
Reply from 192.168.100.103: bytes=32 time<1ms TTL=128
Reply from 192.168.100.103: bytes=32 time<1ms TTL=128
Reply from 192.168.100.103: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.100.103:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Il nostro Laptop è riuscito a comunicare con il *PC-PT-PC0*.

Adesso dobbiamo controllare che questo laptop riesca a comunicare anche con il *LAPTOP-PT2* che ha come IP 192.168.200.100

```
C:\>ping 192.168.200.100

Pinging 192.168.200.100 with 32 bytes of data:

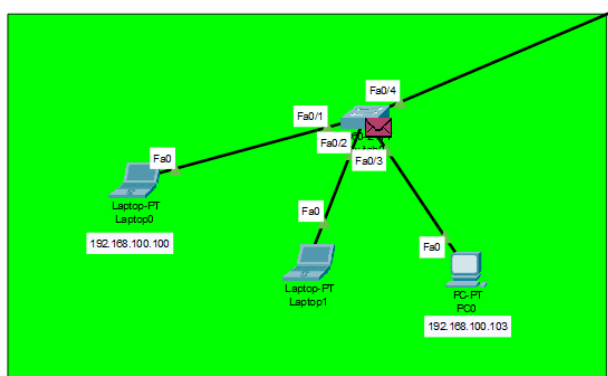
Reply from 192.168.200.100: bytes=32 time=6ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time<1ms TTL=127
Reply from 192.168.200.100: bytes=32 time=4ms TTL=127

Ping statistics for 192.168.200.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 6ms, Average = 2ms
```

Come vedi, anche qui, i dispositivi riescono a comunicare correttamente.

Tutto funziona correttamente.

Per capire più dettagliatamente cosa succede ad ogni dispositivo quando viene mandato il ping, possiamo, tramite Cisco Packet Tracer, fare il test della “letterina”, che non è altro che un frame, ma in questo caso ci permette di fare una simulazione e di capire cosa succede nelle macchine.



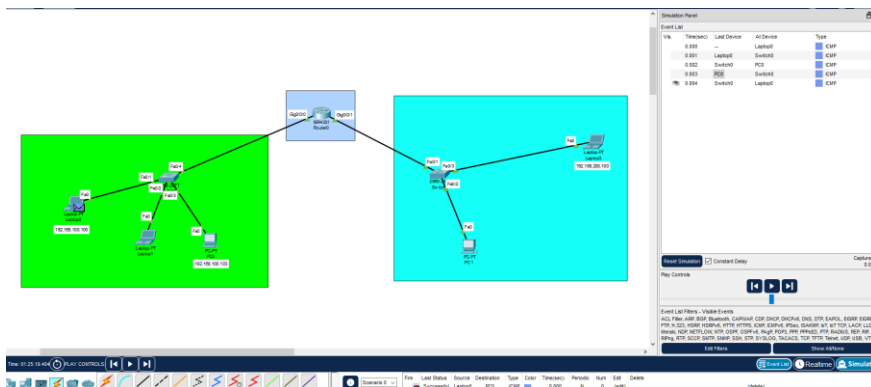
Abbiamo detto che tramite il Laptop PT0 avremmo mandato un ping al PC-PT PC0, cosa succede però?

Dal momento in cui scegliamo di mandare il frame, il nostro software ci simula tutti gli eventi (vedi immagine) e possiamo comodamente visionarli per capire cosa succede nell'effettivo nei vari layer cliccando gli eventi.

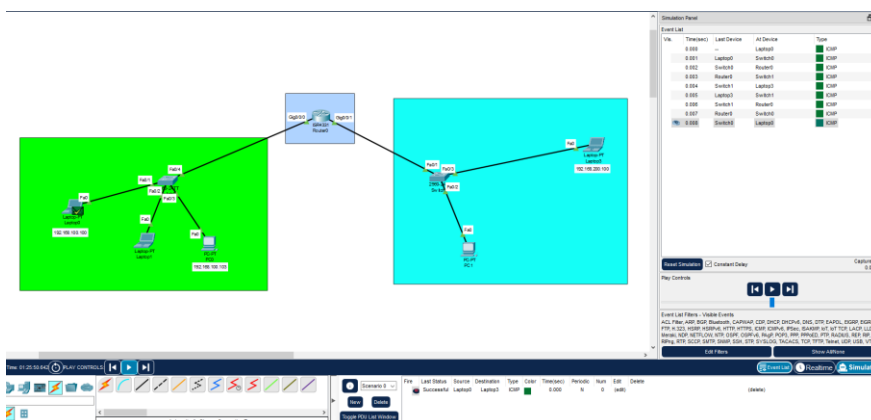
Simulation Panel			
Event List			
Via	Time(sec)	Last Device	Type
0.000	—	Laptop0	ICMP
0.001	Laptop0	Switch0	ICMP
0.002	Switch0	PC0	ICMP
0.003	PC0	Switch0	ICMP
0.004	Switch0	Laptop0	ICMP

☒ Constant Delay
 Captured to 0.004 s

Event List Filters - Visible Events
 ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPsec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoE, PTP, RADIUS, REP, RIP, RIPv2, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP



Come possiamo vedere in basso, sappiamo che il nostro frame è arrivato a destinazione.



Tramite questa simulazione, è possibile osservare tutti i vari step che fa il frame attraverso i layer in modo dettagliato e comprendere meglio il funzionamento dei layer, ricordando però che quest'ultimi hanno un ordine da seguire. La sorgente segue l'ordine a partire da applicazione a fisico e il ricevente ha l'ordine inverso da fisico ad applicazione.

