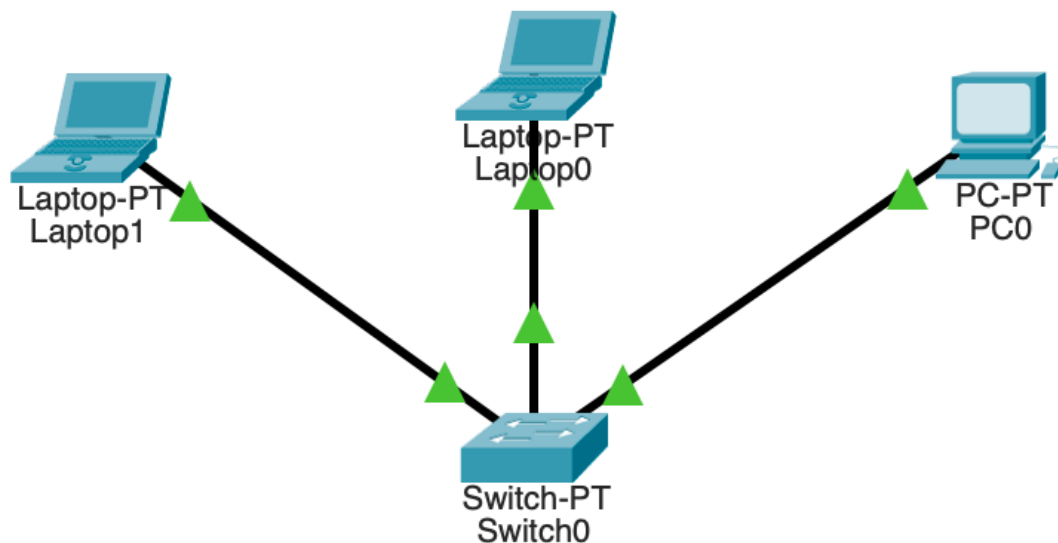


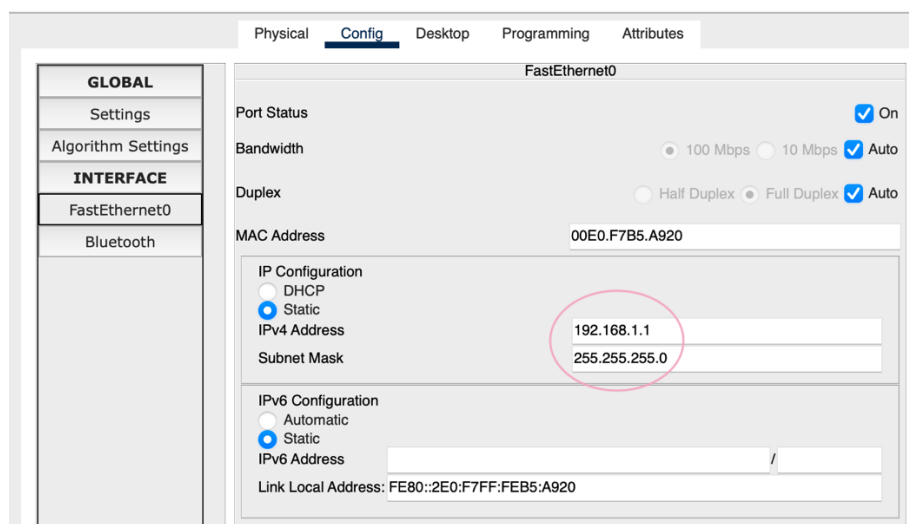
CISCO PACKET TRACER

Il compito di oggi riguarda la creazione di una rete di calcolatori attraverso l'utilizzo del software Packet Tracer.

Il primo passo è stato quello di creare la rete a livello fisico con 2 laptop (Laptop0, Laptop1), 1 pc (PC0) e collegarli ad uno switch come nella seguente figura.

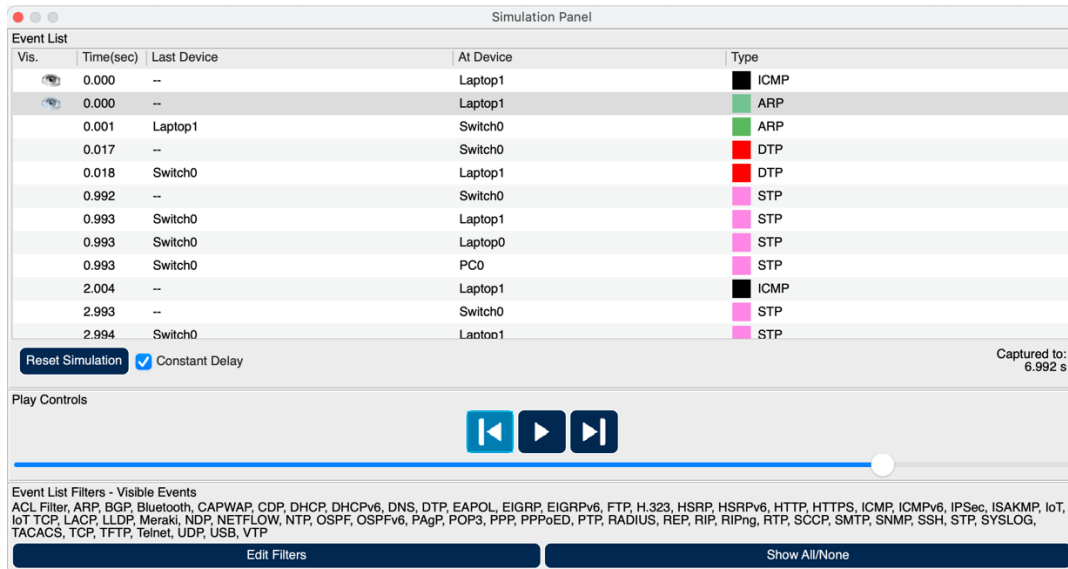


Successivamente ho impostato l'indirizzo IP e la Subnet Mask per i tre dispositivi fisici parlanti (Laptop0, Laptop1 e PC0) rispettivamente (192.168.1.1/ 255.255.255.0 - 192.168.1.2/ 255.255.255.0 - 192.168.1.3/ 255.255.255.0) come nell'esempio successivo.



Raul Pastor

Dopodichè ho utilizzato la modalità simulazione lanciando dal primo computer (con IP 192.168.1.1) il comando “ping 192.168.1.1” nel command prompt per verificare step-by-step cosa succedesse nel simulation panel tra i dispositivi a livello protocollare e a livello di layer intaccati.



The screenshot shows the 'Simulation Panel' window. At the top is the 'Event List' table. Below it are 'Reset Simulation' and 'Constant Delay' (checked) buttons. Further down are 'Play Controls' with back, play, and forward buttons, and a progress bar. At the bottom are 'Event List Filters - Visible Events' and buttons for 'Edit Filters' and 'Show All/None'.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop1	ICMP
	0.000	--	Laptop1	ARP
	0.001	Laptop1	Switch0	ARP
	0.017	--	Switch0	DTP
	0.018	Switch0	Laptop1	DTP
	0.992	--	Switch0	STP
	0.993	Switch0	Laptop1	STP
	0.993	Switch0	Laptop0	STP
	0.993	Switch0	PC0	STP
	2.004	--	Laptop1	ICMP
	2.993	--	Switch0	STP
	2.994	Switch0	Laptop1	STP

Reset Simulation ☒ Constant Delay Captured to: 6.992 s

Play Controls

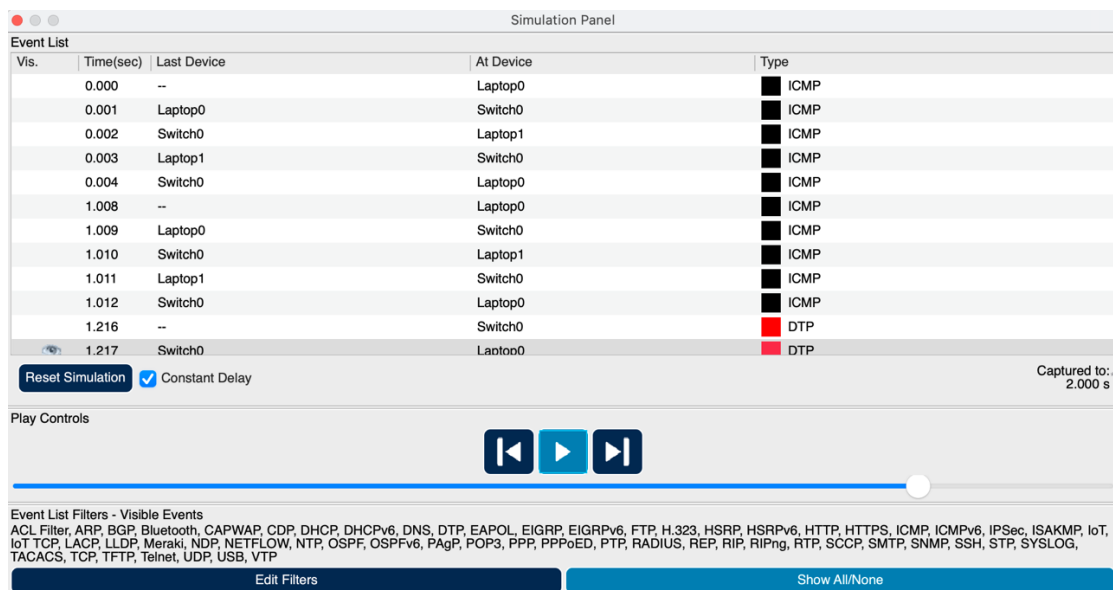
Event List Filters - Visible Events
ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, Meraki, NDP, NETFLOW, NTP, OSPF, OSPFv6, PaGP, POP3, PPP, PPPoE, PTP, RADIUS,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

Edit Filters Show All/None

Principalmente il protocollo ICMP lancia il comando verso lo switch che non risponde direttamente dato che non conosce gli indirizzi MAC dei dispositivi quindi lancia il protocollo ARP che individua l'indirizzo MAC del dispositivo associato all'indirizzo IP del destinatario.

una volta individuato lo rispedisce al mittente che riesegue il ping (Dopo una serie di protocolli DTP e STP per “chiacchiere di gestione LAN”) per 4 volte di seguito e riceve risposte per altrettante volte.

Ho rieseguito il comando una volta terminato il precedente e ho notato che i protocolli sono cambiati, come se lo switch avesse “imparato” quali sono i MAC associati a quei dispositivi:



The screenshot shows the 'Simulation Panel' window. At the top is the 'Event List' table. Below it are 'Reset Simulation' and 'Constant Delay' (checked) buttons. Further down are 'Play Controls' with back, play, and forward buttons, and a progress bar. At the bottom are 'Event List Filters - Visible Events' and buttons for 'Edit Filters' and 'Show All/None'.

Vis.	Time(sec)	Last Device	At Device	Type
	0.000	--	Laptop0	ICMP
	0.001	Laptop0	Switch0	ICMP
	0.002	Switch0	Laptop1	ICMP
	0.003	Laptop1	Switch0	ICMP
	0.004	Switch0	Laptop0	ICMP
	1.008	--	Laptop0	ICMP
	1.009	Laptop0	Switch0	ICMP
	1.010	Switch0	Laptop1	ICMP
	1.011	Laptop1	Switch0	ICMP
	1.012	Switch0	Laptop0	ICMP
	1.216	--	Switch0	DTP
	1.217	Switch0	Laptop0	DTP

Reset Simulation ☒ Constant Delay Captured to: 2.000 s

Play Controls

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, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Edit Filters Show All/None

I protocolli utilizzati nel Data layer del modello ISO/OSI utilizzati sono:

- ARP: protocollo che serve per mappare il dispositivo ed associare un MAC ad un IP.
- STP: protocollo utilizzato per evitare che si presentino loop in presenza di piu switch collegati tra loro.
- DTP: protocollo utilizzato per verificare se una porta dev'essere Access (per singolo host) o Trunk (per piu VLAN tra Switch).