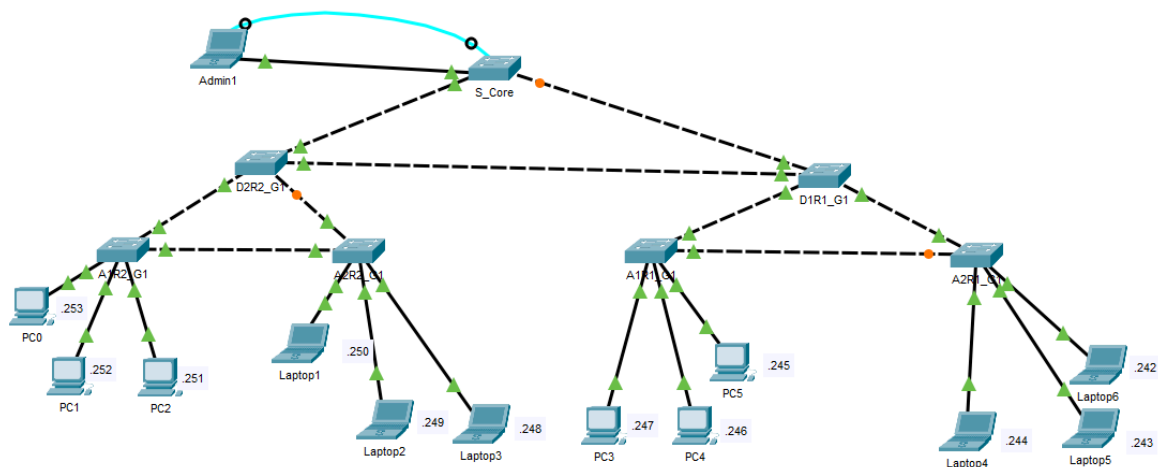



Experience 1 - Switching



Part 1 - Cabling and basic configurations

Name	Management	Interface	Connect to	Mode	Port Security
S_Core	SVI Number: 1	Fa0/8	Admin1	Dynamic A.	N
	IP Add: 192.168.1.2/24	Fa0/23	D1R1_G1	Dynamic A.	N
	Def. GW: -	Fa0/24	D2R2_G1	Dynamic A.	N
	Telnet/SSH: telnet				

Le tabelle di configurazione dei rimanenti switch:

 Tab_exp1_p1

Configurazioni degli switch:

- banner MOTD “*Authorized Acces Only!*”,
- password *cisco* per accesso utente,
- password *class* per accesso privilegiato,
- password *cisco* per VTY 0-14,
- password *mgmt* per VTY 15

Le seguenti immagini mostrano il risultato del comando ping tra *Admin1* e *Laptop 6* ed il risultato della connessione da *Admin1* ad *A2R1_G1* tramite telnet:

```
C:\>ping 192.168.1.242

Pinging 192.168.1.242 with 32 bytes of data:

Reply from 192.168.1.242: bytes=32 time<1ms TTL=128
Reply from 192.168.1.242: bytes=32 time<1ms TTL=128
Reply from 192.168.1.242: bytes=32 time<1ms TTL=128
Reply from 192.168.1.242: bytes=32 time=13ms TTL=128

Ping statistics for 192.168.1.242:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 3ms

C:\>telnet 192.168.1.8
Trying 192.168.1.8 ...Open Authorized Acces Only!

User Access Verification

Password:
A2R1_G1>
```

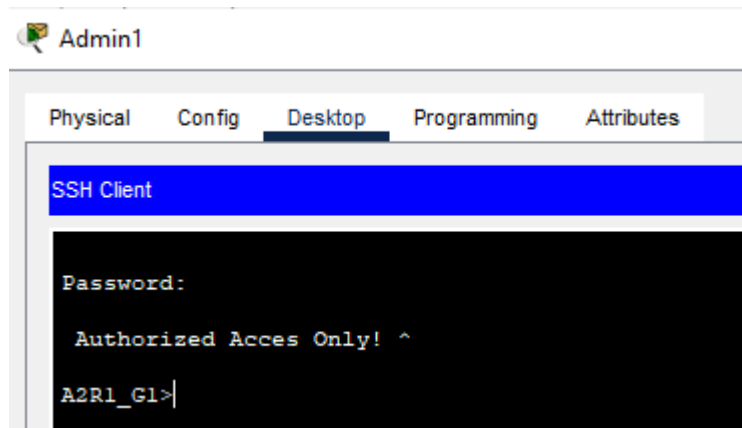
Le prove di connettività appena mostrate sono state eseguite con successo anche nei seguenti casi:

- ogni host è in grado di raggiungere tutti gli altri host e ogni switch è in grado di raggiungere tutti gli altri switch,
- gli host e gli switch sono in grado di raggiungersi tra loro,
- gli host e gli switch sono in grado di accedere tramite telnet agli altri switch.

Part 2 - SSH and port security

SSH

La figura dimostra la connessione tramite SSH tra *Admin1* e *A2R1_G1*:



Anche se non mostrato, tutti i PC/Laptop della rete hanno stabilito con successo connessioni SSH verso tutti gli switch.

Configurazioni SSH:

- domain name: labtlc.com,
- RSA 1024 bit keys,
- username *admin*, secret *ccna*,
- accesso telnet disabilitato,
- SSH v.2

Port Security

Port Security: dynamic(default)-static-sticky

PC	PC mac-addr	int. A1R2_G1
PC0	0001.43EE.3A4D	fa 0/1
PC1	0009.7CD6.4498	fa 0/2
PC2	00D0.BAA1.C25E	fa 0/3

Risultato test con configurazione porte *dynamic(default)*:

```
AlR2_G1(config-if)#do ping 192.168.1.251

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.251, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/11 ms

AlR2_G1(config-if)#do show port-security int fa0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 3
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 0
Last Source Address:Vlan : 0001.43EE.3A4D:1
Security Violation Count : 0

AlR2_G1(config-if)#do show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                        Ports    Remaining Age
-----  -
1        0001.43EE.3A4D    DynamicConfigured          FastEthernet0/1
1        0009.7CD6.4498    DynamicConfigured          FastEthernet0/2
1        00D0.BAA1.C25E    DynamicConfigured          FastEthernet0/3
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Per l'esecuzione del test sono stati eseguiti dei ping da e verso i PC in modo da poter visualizzare in tabella i MAC address dei dispositivi.

Successivamente, sullo switch *A1R2_G1* è stato effettuato il comando *reload* in modo da verificare che i MAC address non vengano salvati permanentemente:

```
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE
SOFTWARE (fcl)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

Press RETURN to get started!

Authorized Acces Only!

User Access Verification

Password:

AlR2_G1>en
Password:
AlR2_G1#show po
AlR2_G1#show port-security add
AlR2_G1#show port-security address
Secure Mac Address Table
-----
Vlan    Mac Address      Type                        Ports    Remaining Age
-----  -
1        0001.43EE.3A4D    DynamicConfigured          FastEthernet0/1
1        0009.7CD6.4498    DynamicConfigured          FastEthernet0/2
1        00D0.BAA1.C25E    DynamicConfigured          FastEthernet0/3
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
AlR2_G1#
```

Risultato test con configurazione porte *static*:

```
Port Security      : Enabled
Port Status       : Secure-up
Violation Mode     : Shutdown
Aging Time        : 0 mins
Aging Type        : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 3
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

A1R2_G1#show port
A1R2_G1#show port-security add
A1R2_G1#show port-security address
      Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
1       0001.43EE.3A4D    SecureConfigured    Fa0/1    -
1       0009.7CD6.4498    SecureConfigured    Fa0/2    -
1       00D0.BAa1.C25E    SecureConfigured    Fa0/3    -
-----

Total Addresses in System (excluding one mac per port) : 0
Max Addresses limit in System (excluding one mac per port) : 1024
A1R2_G1#show mac-add
      Mac Address Table
-----
Vlan    Mac Address      Type                Ports
-----
1       0001.43ee.3a4d    STATIC              Fa0/1
1       0002.4a02.e818    DYNAMIC              Fa0/23
1       0009.7cd6.4498    STATIC              Fa0/2
1       0030.f278.2318    DYNAMIC              Fa0/24
1       00d0.baal.c25e    STATIC              Fa0/3
```

Per l'inserimento statico dei MAC address è stato eseguito per le porte fa0/1,fa0/2 ed fa0/3 (access port), il comando:

A1R2_G1 (conf-if) # **switchport port-security mac-address** *mac-address*

Dopo il comando *reload*, effettuando dei ping da, o verso, i PC/switch si nota che la modalità statica persiste:

```
AlR2_G1#ping 192.168.1.253

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.253, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/0 ms

AlR2_G1#show mac-add
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.43ee.3a4d   STATIC    Fa0/1
1       0002.4a02.e818   DYNAMIC   Fa0/23
1       0030.f278.2318   DYNAMIC   Fa0/24
AlR2_G1#ping 192.168.1.252

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.252, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms

AlR2_G1#show mac-add
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.43ee.3a4d   STATIC    Fa0/1
1       0002.4a02.e818   DYNAMIC   Fa0/23
1       0009.7cd6.4498   STATIC    Fa0/2
1       0030.f278.2318   DYNAMIC   Fa0/24
AlR2_G1#
```

Risultato test con configurazione porte *sticky*:

```
A1R2_G1(config)#do show port-security add
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
1       0001.43EE.3A4D   SecureSticky        Fa0/1    -
1       0009.7CD6.4498   SecureSticky        Fa0/2    -
1       00D0.BAAd.C25E   SecureSticky        Fa0/3    -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
A1R2_G1(config)#do show port-security int fa0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 3
Total MAC Addresses    : 1
Configured MAC Addresses : 0
Sticky MAC Addresses   : 1
Last Source Address:Vlan : 0001.43EE.3A4D:1
Security Violation Count : 0

A1R2_G1(config)#do show port-security add
Secure Mac Address Table
-----
Vlan    Mac Address      Type                Ports    Remaining Age
-----
1       0001.43EE.3A4D   SecureSticky        Fa0/1    -
1       0009.7CD6.4498   SecureSticky        Fa0/2    -
1       00D0.BAAd.C25E   SecureSticky        Fa0/3    -
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

La protezione della porta, configurata con il metodo *sticky*, passa automaticamente alla modalità dinamica qualora la configurazione corrente non venga salvata in quella di avvio, o se il comando *no switchport port-security mac-address sticky* viene esplicitamente eseguito.

Per cui, affinché la configurazione *sticky* sia permanente, dopo un riavvio, comando *reload* o quant'altro, è necessario copiare il *running-config* nello *startup-config* tramite il comando:

A1R2_G1 # copy running-config startup-config

```

!
interface FastEthernet0/1
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0001.43EE.3A4D
!
interface FastEthernet0/2
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0009.7CD6.4498
!
interface FastEthernet0/3
 switchport mode access
 switchport port-security
 switchport port-security maximum 3
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 00D0.BAa1.C25E
!

```

* screenshot parziale *startup-config*

Violation Modes: shutdown(default)-protect-restrict

(le modalità di violazione sono state testate sull'interfaccia fa 0/1 dello switch A1R2_G1)

Il test in modalità *shutdown* è stato condotto modificando l'indirizzo MAC del PC0 per simulare il superamento del numero massimo di dispositivi consentiti. Il sistema ha reagito correttamente, attivando la modalità shutdown come mostrato di seguito:

The screenshot displays a network simulation environment. On the left, a physical topology shows a switch (A1R2_G1) connected to three PCs (PC0, PC1, PC2). PC0 is connected to Fa0/1, PC1 to Fa0/2, and PC2 to Fa0/3. The switch configuration is shown in the center, with the CLI tab selected. The configuration includes port security on all three interfaces, with a maximum of 3 MAC addresses and sticky learning. The MAC address table is also displayed, showing the learned MAC addresses for each interface. On the right, a command prompt window shows the results of a ping test from PC0 to 192.168.1.2. The first ping is successful, but the second ping fails with a 'Request timed out' message, indicating a port security violation. The switch status bar at the bottom shows the link state as 'LINK-S-CHANGED: Interface FastEthernet0/1, changed state to administratively down' and the line protocol as 'LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down'.

Vlan	Mac Address	Type	Ports
1	0001.43ee.3a4a	STATIC	Fa0/1
1	0001.43ee.3a4c	STATIC	Fa0/1
1	0001.43ee.3a4d	STATIC	Fa0/1
1	0002.4a02.e818	DYNAMIC	Fa0/23
1	0009.7cd6.4498	STATIC	Fa0/2
1	0030.f278.2318	DYNAMIC	Fa0/24
1	00d0.baal.c25e	STATIC	Fa0/3
1	00d0.ff9e.94b1	DYNAMIC	Fa0/23

```

A1R2_G1#show port-security interface fa0/1
Port Security          : Enabled
Port Status            : Secure-up
Violation Mode         : Shutdown
Aging Time             : 0 mins
Aging Type             : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses  : 3
Total MAC Addresses    : 3
Configured MAC Addresses : 0
Sticky MAC Addresses   : 3
Last Source Address:Vlan : 0001.43EE.3A4C:1
Security Violation Count : 0

```

```

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255
Reply from 192.168.1.2: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.2
Pinging 192.168.1.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

```

In caso di violazione della sicurezza, il "Security Violation Count" viene incrementato e l'interfaccia interessata viene disabilitata. Per ripristinarla, è necessario eseguire in sequenza i comandi *shutdown* e *no shutdown*.

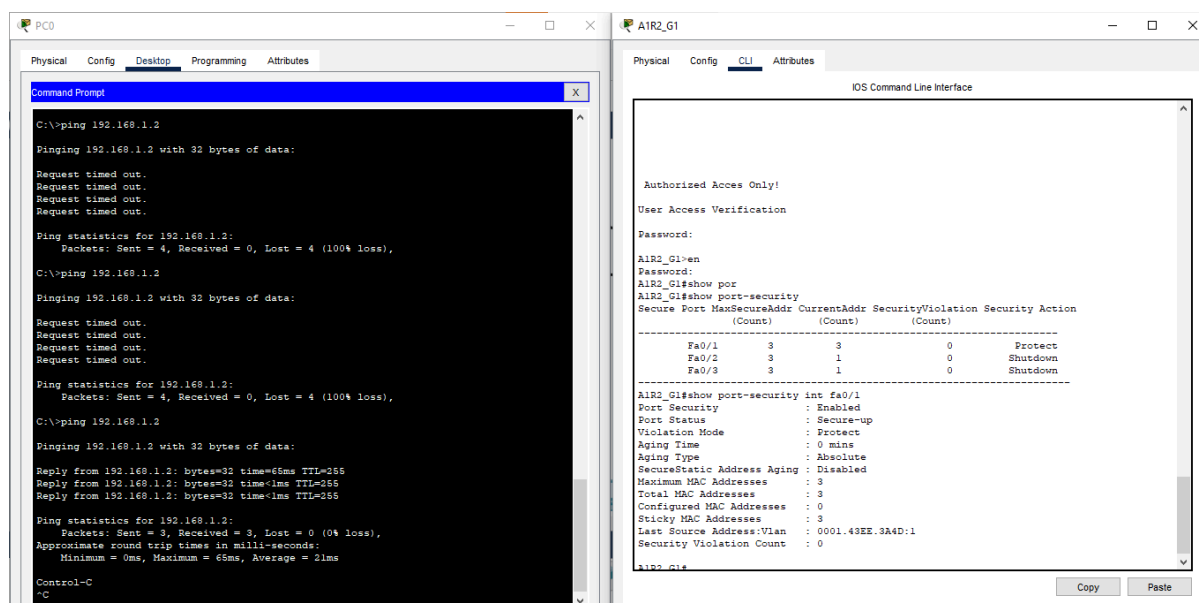
Dopo aver eseguito il comando :

A1R2_G1 (conf-if) # **switchport port-security violation protect**

sono stati eseguiti test di ping dal PC0 allo switch S_Core, prima con un indirizzo MAC non autorizzato e successivamente con un indirizzo MAC autorizzato.

L'immagine mostra che il traffico proveniente da un indirizzo MAC non autorizzato viene scartato senza che il "Security Violation Count" venga incrementato.

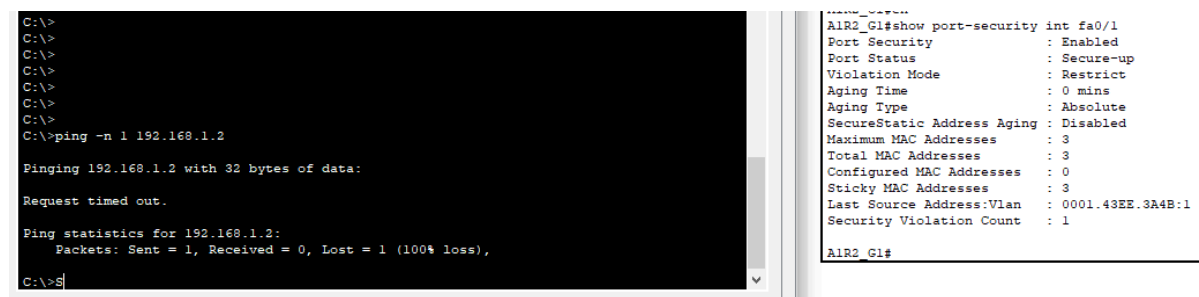
Diversamente, con un indirizzo MAC autorizzato, il sistema opera normalmente:



Ultima modalità di violazione testata è la *restrict*:

A1R2_G1 (conf-if) # **switchport port-security violation restrict**

A differenza della modalità *protect*, si ha un incremento del "Security Violation Count":



In conclusione, la modalità *shutdown* richiede un intervento manuale per il ripristino della porta, a differenza delle modalità *restrict* e *protect*.

Part 3 - VLANs

La rete è stata così suddivisa:

VLAN	NETWORK	NETMASK	FIRST ADDRESS	LAST ADDRESS	BCAST ADDRESS
Vlan 10 (Student)	192.168.1.0/26	255.255.255.192	192.168.1.1	192.168.1.62	192.168.1.63
Vlan 20 (Faculty)	192.168.1.64/26	255.255.255.192	192.168.1.65	192.168.1.126	192.168.1.127
Vlan 30 (Guest)	192.168.1.128/28	255.255.255.240	192.168.1.129	192.168.1.142	192.168.1.143
Vlan 99 (Mgmt)	192.168.1.144/28	255.255.255.240	192.168.1.145	192.168.1.158	192.168.1.159

Sugli access switch sono state effettuate le configurazioni riportate in tabella:

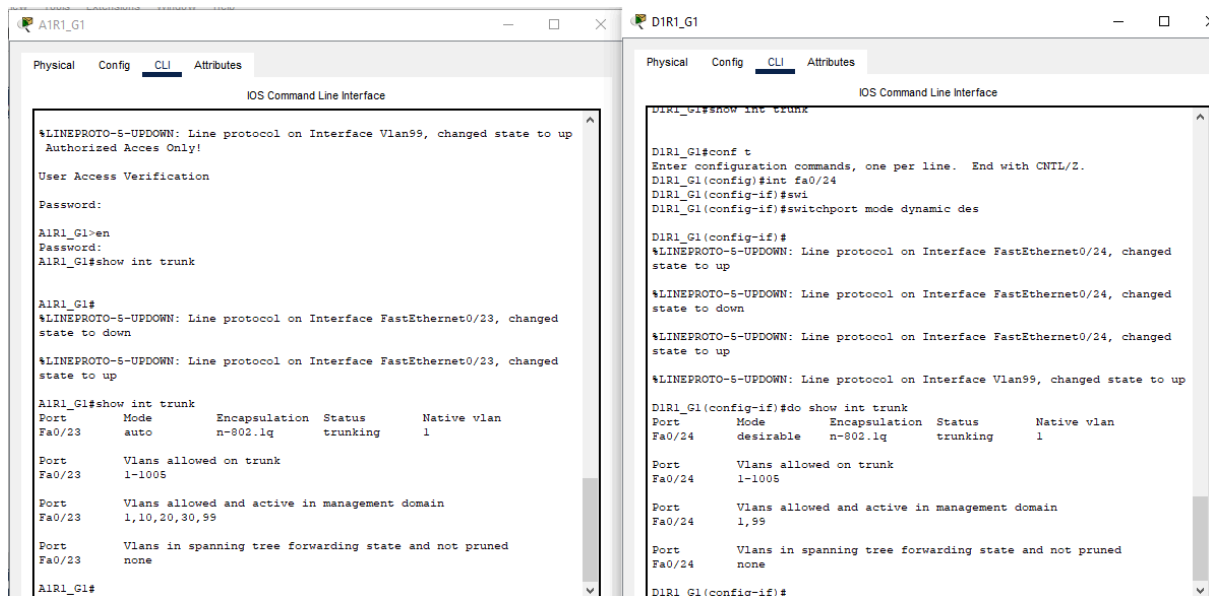
Name	Management	Interface	VLAN	Mode	Connects to	IP Host
A1R2_G1	SVI Number: 99	Fa0/1 - Fa0/6	Student - Vlan 10	Access	PC 0 (Fa0/1)	192.168.1.1/26
	IP Add: 192.168.1.158/28	Fa0/7 - Fa0/12	Faculty - Vlan 20	Access	PC 1 (Fa0/7)	192.168.1.65/26
	Def. GW: -	Fa0/13 - Fa0/16	Guest - Vlan 30	Access	PC 2 (Fa0/13)	192.168.1.129/28
	Telnet/SSH: SSH	Fa0/17 - Fa0/18	Mgmt - Vlan 99	Access	Admin 2 (Fa0/17)	192.168.1.145/28
		Fa0/23	-	Dyn. Auto	D2R2_G1	-
		Fa0/24	-	Dyn. Auto	A2R2_G1	-

 exp1_p3

Le configurazioni per testare le varie modalità sono:

Modes	Device	Port	Connected to	Port	Result
Dyn. Auto - Dyn. Auto	D1R1_G1	Fa.0/23	A2R1_G1	Fa.0/23	Access
Dyn. Auto - Dyn. Des.	D1R1_G1	Fa.0/24	A1R1_G1	Fa.0/23	Trunk
Dyn. Auto - Trunk	D2R2_G1	Fa.0/23	A2R2_G1	Fa.0/23	Trunk
Dyn. Des - Dyn. Des.	D1R1_G1	Fa.0/22	S_Core	Fa.0/23	Trunk
Dyn. Des - Trunk	D2R2_G1	Fa.0/22	S_Core	Fa.0/24	Trunk
Trunk - Trunk	D2R2_G1	Fa.0/21	D1R1_G1	Fa.0/21	Trunk

Risultato CLI modalità *Dynamic Auto* - *Dynamic Desirable*:



Dai test effettuati si evince che:

- solo in modalità *Dyn. Auto* - *Dyn. Auto* non viene instaurato un link trunk tra le rispettive interfacce degli switch
- la negoziazione del trunk viene disattivata quando le porte sono configurate come *access*
- le configurazioni in modalità *Dyn. Auto/Dyn.Des.* - *Trunk* instaurano un link trunk solo se la negoziazione del trunk è attiva

Per poter impostare come nativa la vlan 200 è stato eseguito il comando:

switchport trunk native vlan 200

Per consentire le sole vlan 10,20,30 e 99 sui link trunk:

int range fa0/x-y

switchport trunk allowed vlan 10,20,30,99

I comandi appena mostrati sono stati eseguiti su tutti gli switch.