FREE CCNA Lab 001: Basic Router Security Configuration 1

Link to YouTube video

Overview – An enable password secures the privileged mode (conf t/configure terminal), which is required for all commands that change the router's configuration.

Setup script:

```
en
conf t
hostname R1
enable password cisco
exit
sh run
```

Teardown script:

```
no service password-encryption
```

Setup script:

```
en
conf t
hostname R2
enable password networking
exit
sh run
```

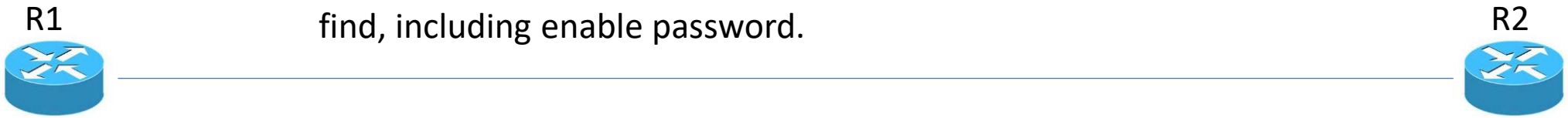
Teardown script:

```
no service password-encryption
```

FREE CCNA Lab 002: Basic Router Security Configuration 2

Link to YouTube video

Overview – An **enable password** secures the **privileged mode** (conf t/configure terminal), which is required for all commands that change the router's configuration. The **service-password encryption** will encrypt all the passwords in running-config it can find, including enable password.



Setup script:

```
en
conf t
hostname R1
enable password cisco
enable secret ccna
service password-encryption
exit
sh run
```

Teardown script:

```
no service password-encryption
```

Setup script:

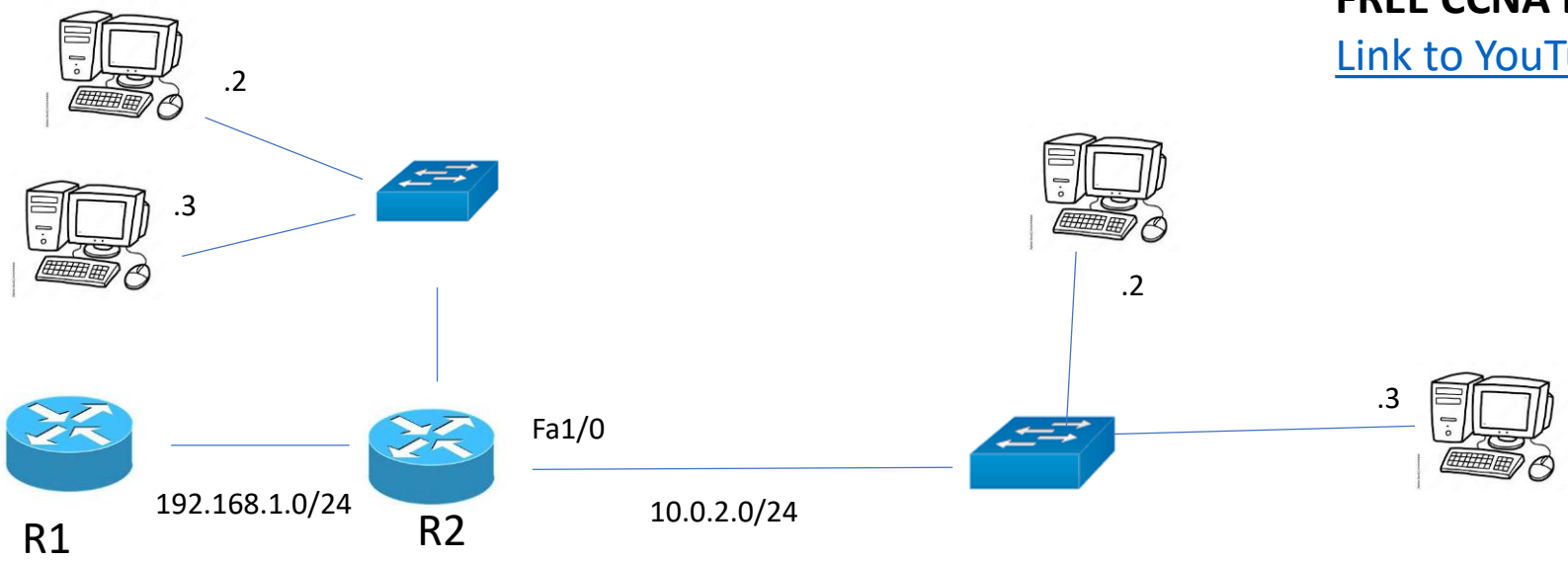
```
en
conf t
hostname R2
enable password cisco
enable secret ccnp
service password-encryption
exit
sh run
```

Teardown script:

```
no service password-encryption
```

FREE CCNA Lab 027: RIP (Part 1)

[Link to YouTube video]



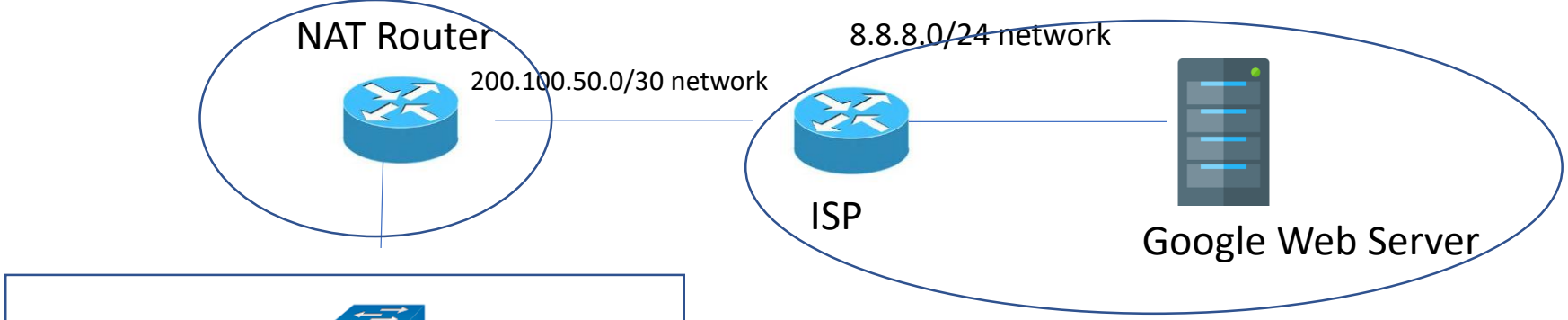
Overview

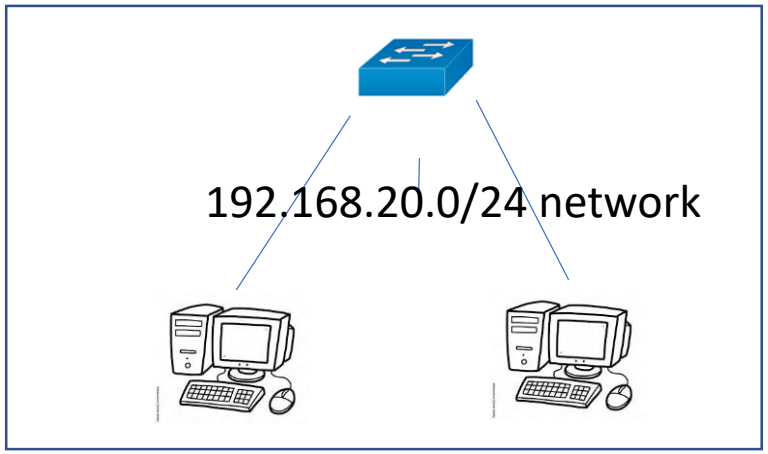
Setup script:

en
conf t
Router rip
Network 192.168.1.0
Network 10.0.0.0
Version 2
No auto-summary
do sh ip route

Setup script:

en
conf t
Router rip
Network 192.168.1.0
Version 2
No auto-summary
do sh ip route





Static NAT

[Link to YouTube video]

Setup script for NAT router:

```
en
conf t
router ospf 30
Router-id 1.1.1.1
Network 192.168.20.0 0.0.0.0.255 area 0
Network 200.100.50.0 0.0.0.0.3 area 0
Ip nat inside source static 192.168.20.10 200.100.50.1
Int g0/1
Ip add 192.168.20.1 255.255.255.0
No shut
Int g0/0
Ip add 200.100.50.1 255.255.255.252
No shut
Ip nat inside
Int g0/0
Ip nat outside
```

Setup script for ISP router:

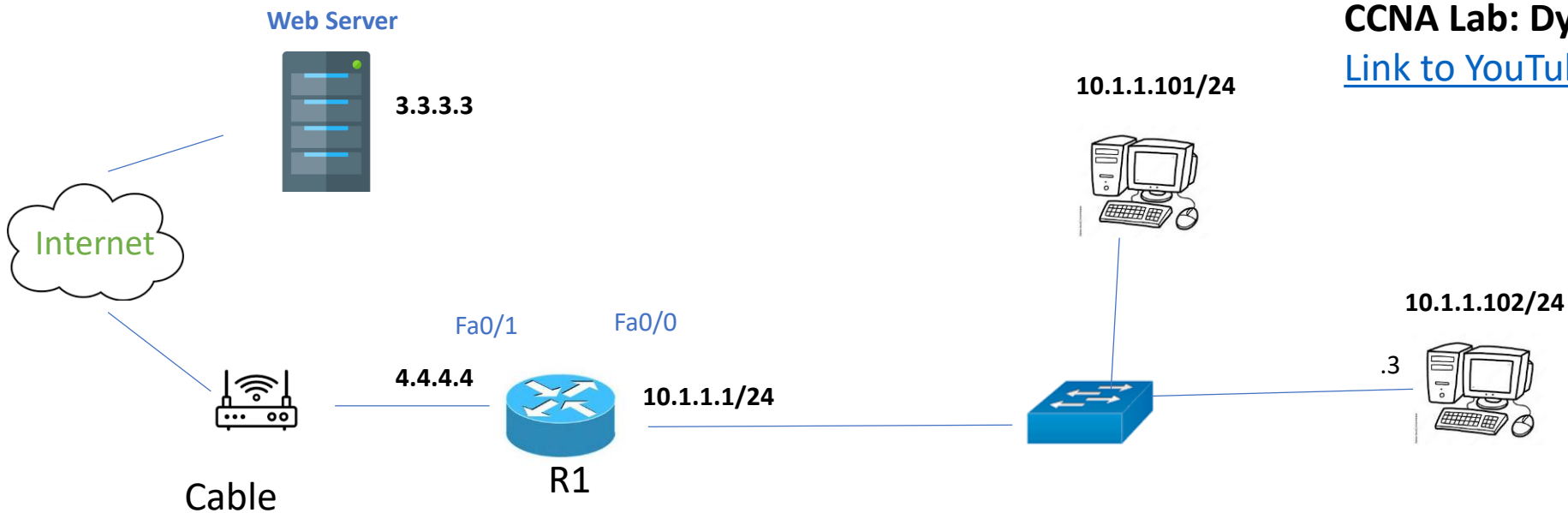
```
en
conf t
router ospf 30
Router-id 2.2.2.2
Network 8.8.8.0 0.0.0.255 area 0
Network 200.100.50.0 0.0.0.0.3 area 0
```

Static (map) network address translation (NAT) provides a one-to-one mapping of private IP addresses to public IP addresses. It allows you to map an IP address on your internal network to an IP address that you want to make public.

CCNA Lab: Dynamic NAT

[Link to YouTube video]

Overview



Setup script:

```
en
conf t
int fa0/0
ip add 10.1.1.1 255.255.255.0
no shut
ip nat inside
int fa0/1
ip add 4.4.4.4 255.0.0.0
no shut
ip nat outside
exit
access-list 1 permit 10.1.1.0 0.0.0.255
ip nat pool POOL 4.4.4.2 4.4.4.3 netmask 255.255.255.0
ip nat inside source list 1 pool POOL
```

Check for IP NAT translations:

Ping 3.3.3.3 from computer

Go to router and type:

show ip nat translations

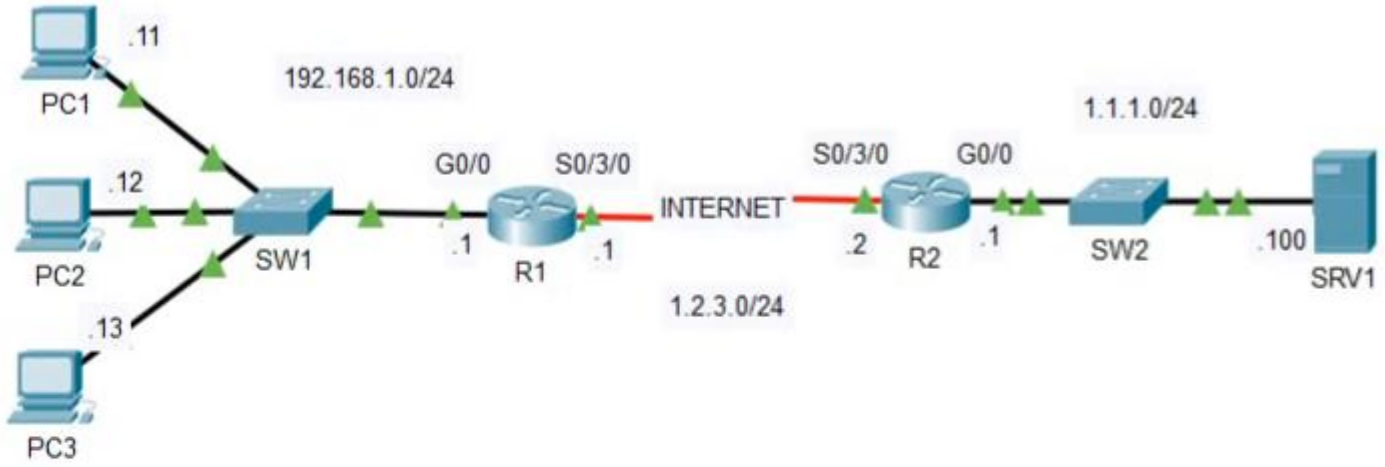
Source Address: 4.4.4.3

Destination Address: 3.3.3.3

Inside Local Address	Inside Global Address	Outside Global Address
10.1.1.101	4.4.4.2	3.3.3.3
10.1.1.102	4.4.4.3	3.3.3.3

CCNA Lab: PAT

[Link to YouTube video]



1. RIP has been configured so that R1 and R2 can reach their inside networks.
   Why can't PC1, PC2, and PC3 successfully ping SRV1?
   (Hint: The serial connection between R1 and R2 is simulating the Internet with ACLs)

2. Configure PAT on R1 to translate addresses in the 192.168.1.0/24 network to R1's S0/3/0 interface.
   (make sure to 'overload' the interface!)

3. Ping from each PC to SRV1, then use a show command on R1 to check the translations.

R1 Setup script:

```
en
conf t
int g0/0
ip nat inside
Int s0/3/0
ip nat outside
exit
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface s0/3/0 overload
```

Check for IP NAT translations:

Ping 1.1.1.00 from computer

Go to router and type

show ip nat translations

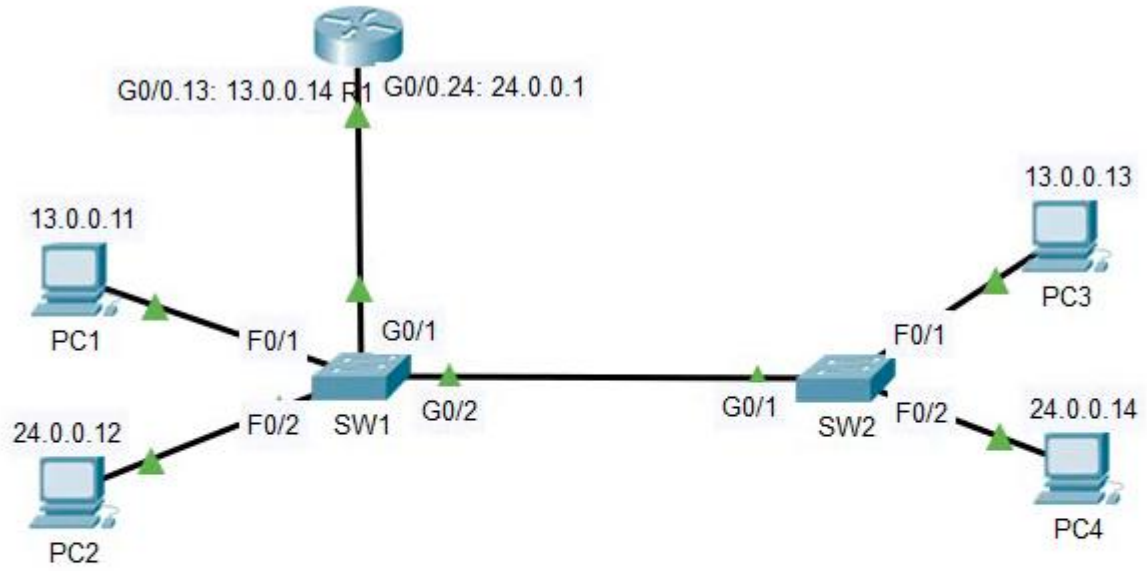
```
R1#sh ip nat trans
Pro  Inside global     Inside local       Outside local      Outside global
icmp 1.2.3.1:1024      192.168.1.13:1     1.1.1.100:1        1.1.1.100:1024
icmp 1.2.3.1:1025      192.168.1.13:2     1.1.1.100:2        1.1.1.100:1025
icmp 1.2.3.1:1026      192.168.1.13:3     1.1.1.100:3        1.1.1.100:1026
icmp 1.2.3.1:1027      192.168.1.13:4     1.1.1.100:4        1.1.1.100:1027
icmp 1.2.3.1:1         192.168.1.12:1     1.1.1.100:1        1.1.1.100:1
icmp 1.2.3.1:2         192.168.1.12:2     1.1.1.100:2        1.1.1.100:2
icmp 1.2.3.1:3         192.168.1.12:3     1.1.1.100:3        1.1.1.100:3
icmp 1.2.3.1:4         192.168.1.12:4     1.1.1.100:4        1.1.1.100:4
icmp 1.2.3.1:5         192.168.1.11:5     1.1.1.100:5        1.1.1.100:5
icmp 1.2.3.1:6         192.168.1.11:6     1.1.1.100:6        1.1.1.100:6
icmp 1.2.3.1:7         192.168.1.11:7     1.1.1.100:7        1.1.1.100:7
icmp 1.2.3.1:8         192.168.1.11:8     1.1.1.100:8        1.1.1.100:8
```

```
auto        Set trunking mode dynamic negotiation parameter to AUTO
desirable   Set trunking mode dynamic negotiation parameter to DESIRABLE
```

CCNA Lab: DTP

Link to YouTube video

DTP is used to negotiate if an interface becomes an access or trunk port. It should be disabled for security purposes. DTP link



VLAN 13: PC1, PC3
VLAN 24: PC2, PC4

1. Disable negotiation of trunk ports. Manually configure the mode of each switchport in use.

2. Assign PCs to the correct VLANs.

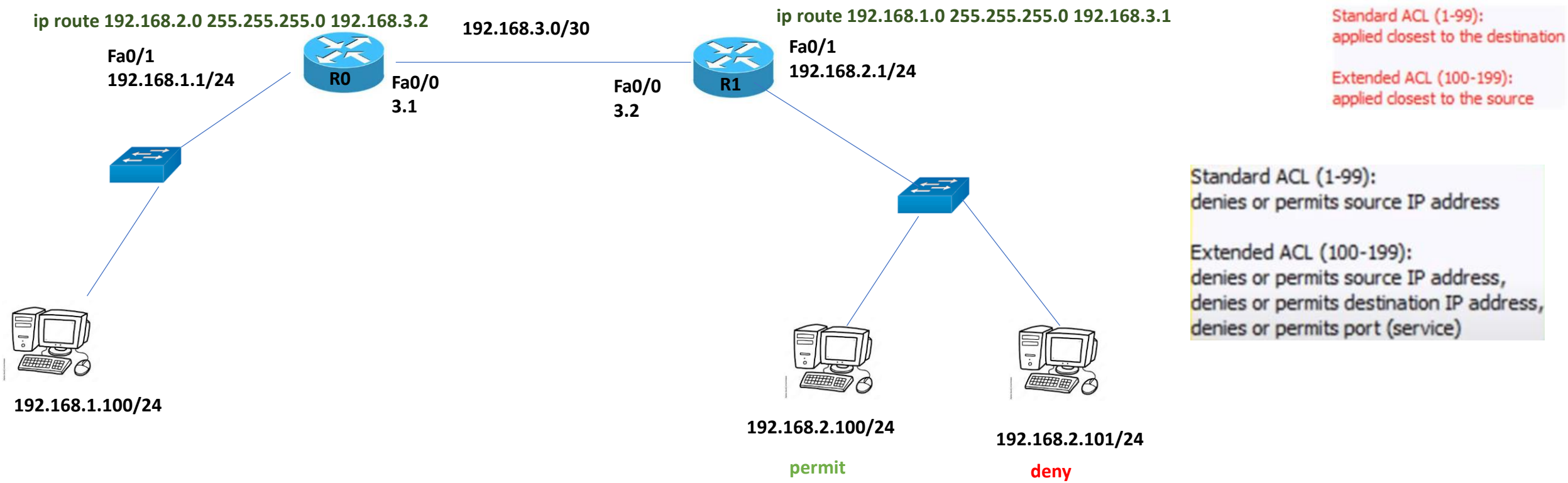
You have successfully completed the lab when DTP is disabled and there is full connectivity throughout the network.

SW1 script:

```
En
Sh int g0/2 sw
Conf t
Switchport nonegotiate
Switchport mode trunk
Intrange fa0/1 – 2
Switchport mode access
Switchport nonegotiate
Exit
Int fa0/1
Swtichport access vlan 13
Int fa0/2
Switchport access vlan 24
```

SW2 script:

```
En
Conf t
Int g0/1
Switchport mode trunk
Switchport nonegotiate
Int range fa0/1 -2
Switchport mode access
Switchport nonegotiate
Exit
Int fa0/1
Switchport access vlan 13
Int fa0/2
Switchport access vlan 24
```



Standard ACL (1-99):
applied closest to the destination

Extended ACL (100-199):
applied closest to the source

Standard ACL (1-99):
denies or permits source IP address

Extended ACL (100-199):
denies or permits source IP address,
denies or permits destination IP address,
denies or permits port (service)

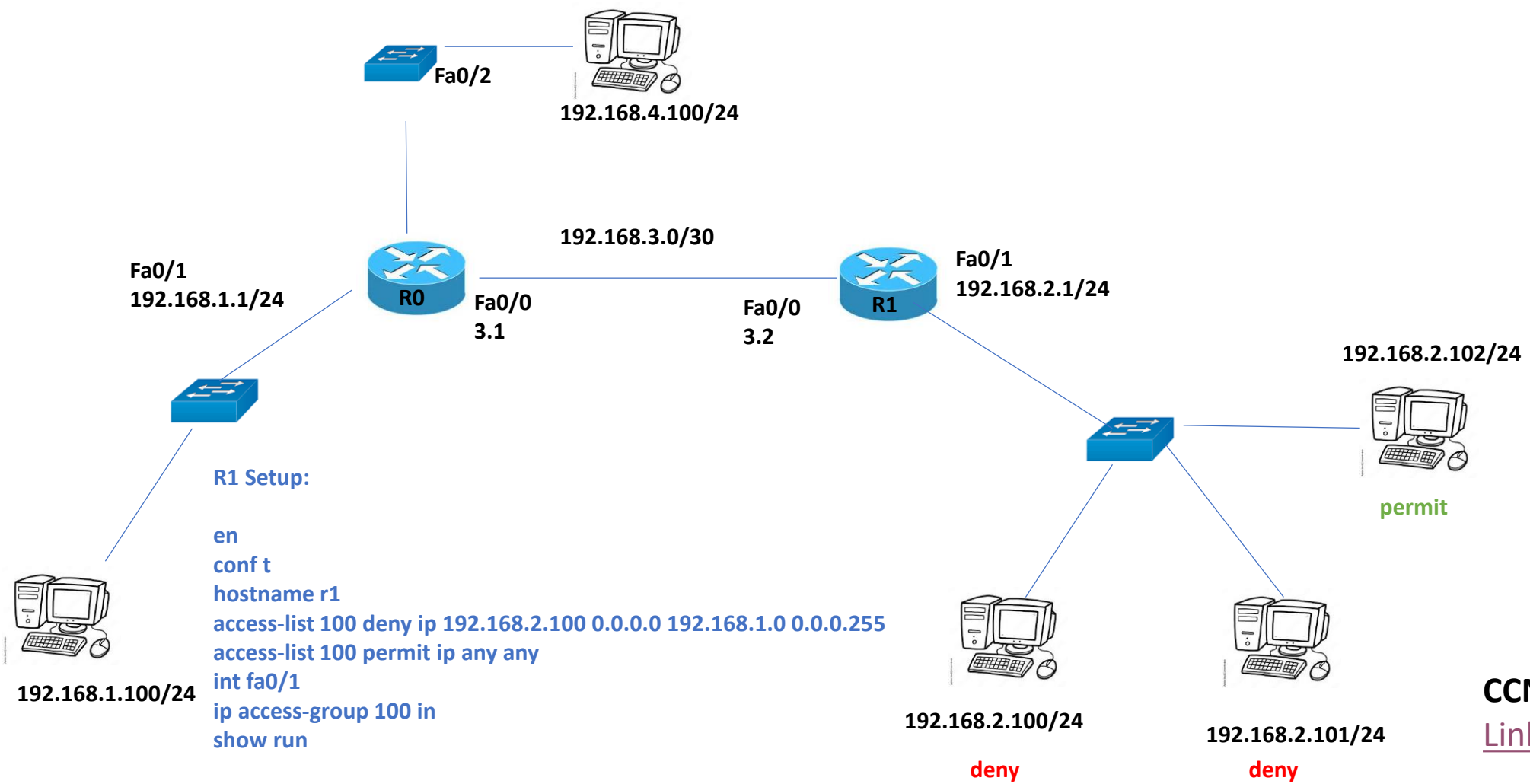
R1 Setup:

```
en
conf t
hostname r0
access-list 1 deny 192.168.2.101 0.0.0.0
access-list 1 permit any
show run

----------------------------------------------------
en
conf t
int fa0/1
ip access-group 1 out
```

CCNA Lab: Standard ACLs

Link to YouTube video



Standard ACL (1-99):
applied closest to the destination

Extended ACL (100-199):
applied closest to the source

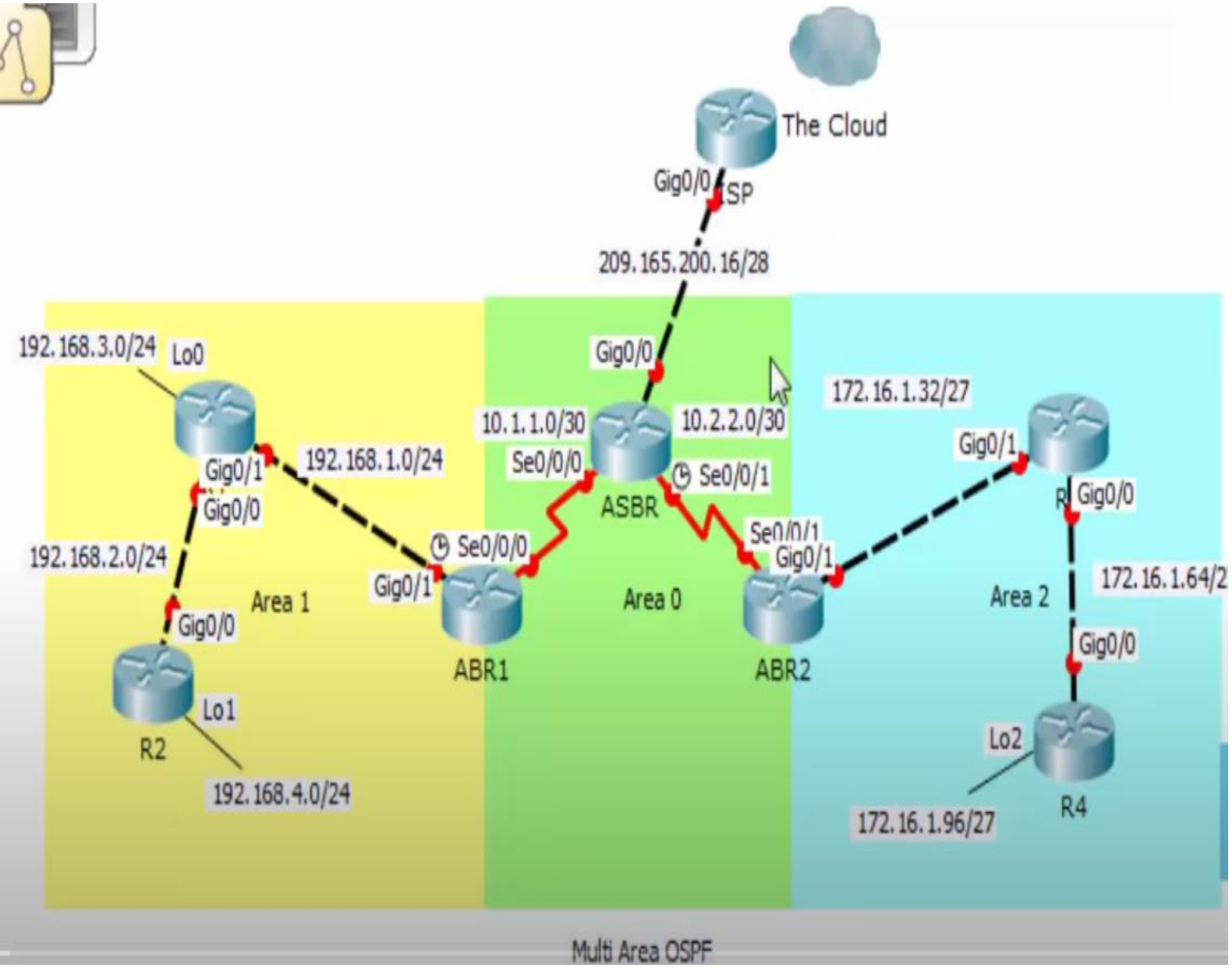
Standard ACL (1-99):
denies or permits source IP address

Extended ACL (100-199):
denies or permits source IP address,
denies or permits destination IP address,
denies or permits port (service)

CCNA Lab: Extended ACLs

Link to YouTube video

ip route 192.168.2.0 255.255.255.0 192.168.3.2
ip route 192.168.1.0 255.255.255.0 192.168.3.1
ip route 192.168.4.0 255.255.255.0 192.168.3.1



ISP router
En
Conf t
Hostname ISP
Int g0/0
Ip add 209.165.200.17 255.255.255.240
No shut
Ip route 0.0.0.0 0.0.0.0 g0.0
Do wr

ASBR router
En
Conf t
Hostname asbr
Int g0/0
Ip add 209.165.200.18 255.255.255.240
No shut
Int s0/0/0
Ip add 10.1.1.2 255.255.255.252
Int s0/0/1
Ip add 10.2.2.2 255.255.255.252
Clock rate 128000
No shut
Ip route 0.0.0.0 0.0.0.0 g0/0
Router ospf 1
Router-id 7.7.7.7
Network 10.1.1.0 0.0.0.3 area 0
Network 10.2.2.0 0.0.0.3 area 0
Default-information originate

ABR1 router
En
Conf t
Hostname ABR1
Int0/0/0
Ip 10.1.1.1 255.255.255.252
Clock rate