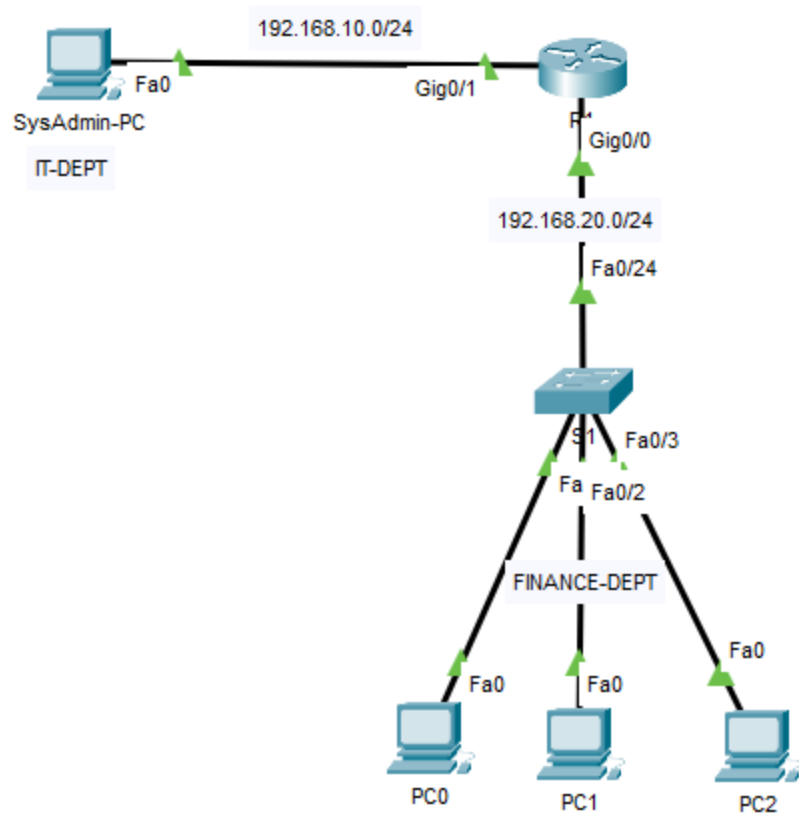


Virtual Terminal (VTY) Lines with Access Control List

ACL CONFIGURATION ON VTY LINES

INACIO ANDRE



SysAdmin-PC

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.10.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

PC0

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.5
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

PC1

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.6
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

PC2

IP Configuration	
<input type="radio"/> DHCP	<input checked="" type="radio"/> Static
IPv4 Address	192.168.20.7
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.1
DNS Server	0.0.0.0

R1

```
Router>en
Router#config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname R1
R1(config)#int g0/0
R1(config-if)#ip add 192.168.20.1 255.255.255.0
R1(config-if)#no shut

R1(config)#int g0/1
R1(config-if)#ip add 192.168.10.1 255.255.255.0
R1(config-if)#no shut
```

S1

```
Switch>en
Switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#int vlan 1
S1(config-if)#ip add 192.168.20.254 255.255.255.0
S1(config-if)#no shut

S1(config)#ip default-gateway 192.168.20.1
S1(config)#enable secret cisco
S1(config)#ip domain-name cisco.com
S1(config)#username cisco secret cisco
S1(config)#banner motd #Unauthorized Access is Prohibited#
S1(config)#crypto key generate rsa
The name for the keys will be: S1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
S1(config)#ip ssh version 2

S1(config)#access-list 10 permit host 192.168.10.5
S1(config)#access-list 10 deny any
S1(config)#line vty 0 15
S1(config-line)#access-class 10 in
S1(config-line)#exit

S1#show run | section line vty
line vty 0 4
    access-class 10 in
    login local
    transport input ssh
line vty 5 15
    access-class 10 in
    login local
    transport input ssh
```

Physical Config Desktop Programming Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l cisco 192.168.20.254

Password:

Unauthorized Access is Prohibited

S1>
```

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ssh -l cisco 192.168.20.254

% Connection refused by remote host
C:\>
```

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ssh -l cisco 192.168.20.254

% Connection refused by remote host
C:\>
```

Physical Config Desktop Programming Attributes

Command Prompt

```
C:\>ssh -l cisco 192.168.20.254

% Connection refused by remote host
C:\>
```