CYT 145 - Ethical and Legal Issues

Project option A - Network Design and Configuration Infrastructure

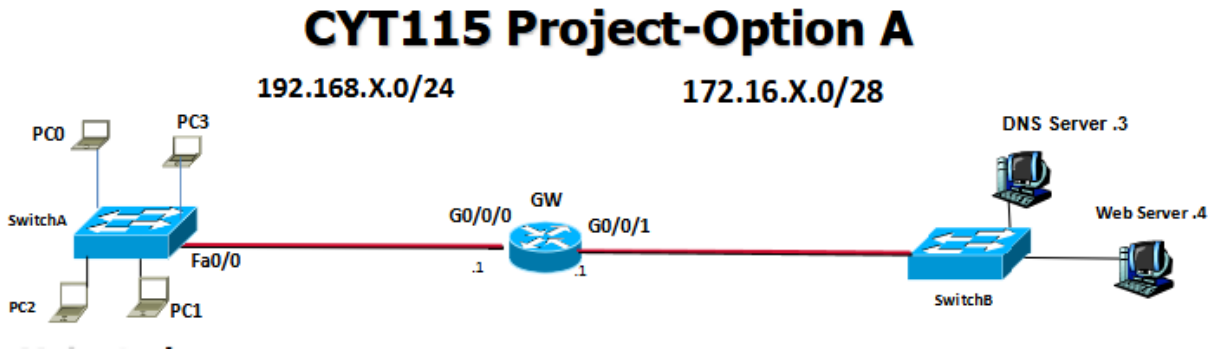
Instructor

Professor Lisa Li

Student (Individual work)

Khang Le 119039253

Introduction



This project involves designing and configuring a dual-LAN network in Cisco Packet Tracer using a Cisco 2911 router, 2960 switches, Cisco PCs, and two Server-PT devices for DNS and web hosting. The network uses static IP addressing, provides DNS and HTTP/HTTPS services, and implements port security and ACLs to control access between the user LAN and server LAN. The project demonstrates essential skills in routing, switching, service configuration, and basic network security.

Project Objectives

- Design a dual-LAN network topology using a Cisco 2911 router, Cisco 2960 switches, PCs, and server devices.
- Assign static IPv4 addressing to all network devices for consistent and reliable connectivity.
- Configure essential network services, including DNS and a web server hosting HTTP/HTTPS.
- Implement router configuration to enable communication between the user LAN and server LAN.
- Apply switch port security to restrict unauthorized device connections on access ports.
- Deploy Access Control Lists (ACLs) to control traffic flow, limit access to server resources, and secure remote management.
- Verify network functionality through testing of connectivity, DNS resolution, web access, and ACL enforcement.

Devices List

- 1 Router: Cisco 2911 router.
- 2 Switches, Switch A (left) and Switch B (right): 2960 switches.
- 4 Pcs: Cisco PCs.
- 1 DNS Server: Cisco Server-PT.
- 1 Web Server: Cisco Server-PT.

Connections

Copper straight-through cables will be used across all connections for connecting different kinds of network devices. The setup includes left network of client side with 4 client PCs connected to a switch under 192.168.10.0/24 network and right network under 172.16.20.0/28 network consists of DNS and webserver connect to a switch.

Left side network (192.168.10.0/24):

PC should be connected to switch through fast internet port since switch supports 100 Mbps Fast Ethernet ports.

PC (FastEthernet0) → Switch (FastEthernet0/1-4)

Enterprise switches reserve the highest numbered port for uplinks to routers.

FastEthernet0/24 → GigabitEthernet0/0

Right side network (172.16.20.0/28):

Connected through straight-through cable with Ethernet.

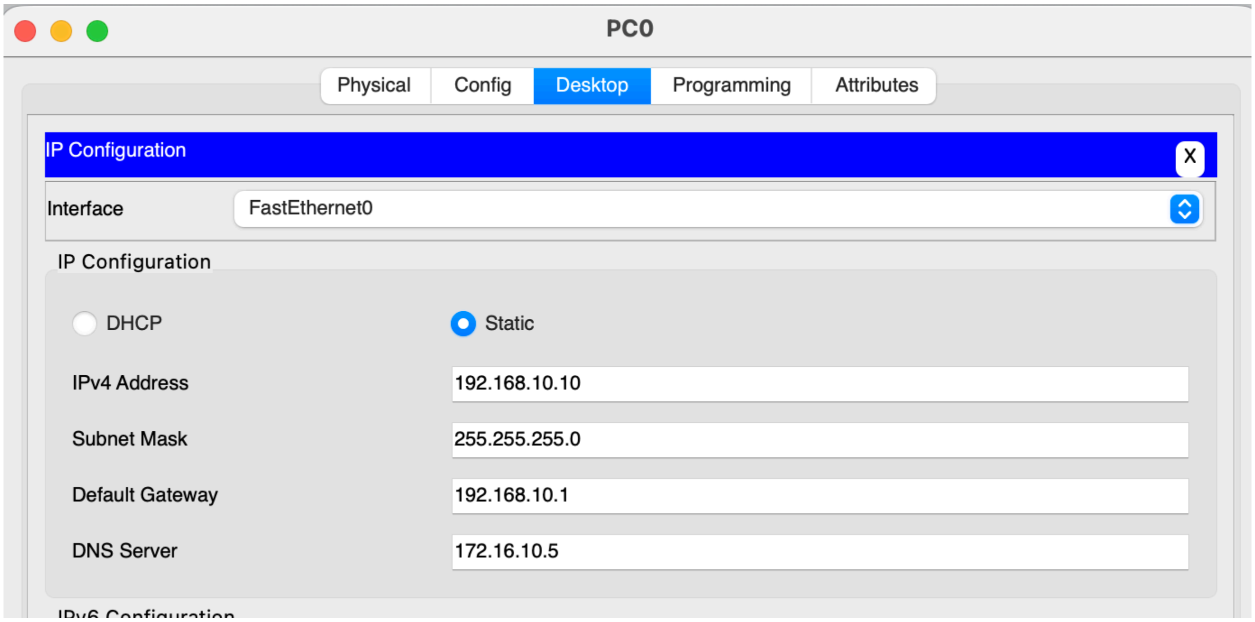
Server (FastEthernet0) → Switch (FastEthernet0/1-2)

Enterprise switches reserve the highest numbered port for uplinks to routers.

FastEthernet0/24 → GigabitEthernet0/1

Assigned IP Table

IP addresses are assigned through device's Desktop tab:



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.10.10

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.10.1

DNS Server: 172.16.10.5

IPv6 Configuration

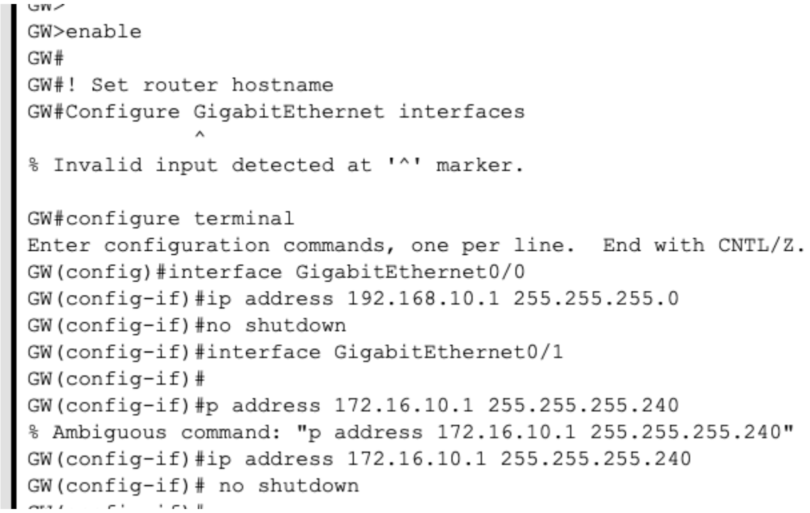
IPv4, subnet mask and gateway of each device are configured as following table:

Devices	IPv4 Address	Subnet Mask	Gateway
PC0	192.168.10.10	255.255.255.0	192.168.10.1
PC1	192.168.10.11	255.255.255.0	192.168.10.1
PC0	192.168.10.10	255.255.255.0	192.168.10.1
PC0	192.168.10.10	255.255.255.0	192.168.10.1
Router G0/0	192.168.10.1	255.255.255.0	192.168.10.1
Router G0/1	172.16.20.1	255.255.255.240	172.16.10.1
DNS server	172.16.20.5	255.255.255.240	172.16.10.1
Web Server	172.16.20.6	255.255.255.240	172.16.10.1

Configure the Router

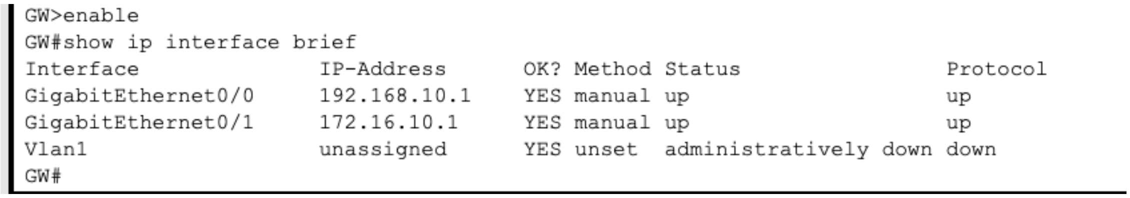
sets up two router interfaces with IP addresses, enables them, and saves the configuration. left interface (192.168.10.1/24), and the right interface (172.16.20.1/28). The router can be configured through following commands:

Appendix A: Router Configuration



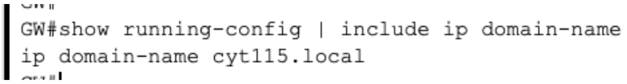
```
GW>
GW>enable
GW#
GW#! Set router hostname
GW#Configure GigabitEthernet interfaces
             ^
% Invalid input detected at '^' marker.

GW#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
GW(config)#interface GigabitEthernet0/0
GW(config-if)#ip address 192.168.10.1 255.255.255.0
GW(config-if)#no shutdown
GW(config-if)#interface GigabitEthernet0/1
GW(config-if)#
GW(config-if)#p address 172.16.10.1 255.255.255.240
% Ambiguous command: "p address 172.16.10.1 255.255.255.240"
GW(config-if)#ip address 172.16.10.1 255.255.255.240
GW(config-if)# no shutdown
GW(config-if)#
```

The desired setting after configuring:



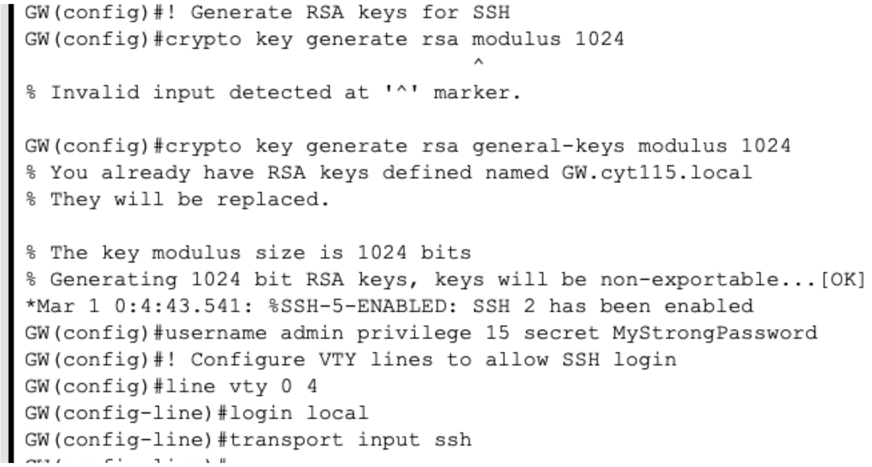
```
GW>enable
GW#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0     192.168.10.1    YES manual up                    up
GigabitEthernet0/1     172.16.10.1     YES manual up                    up
Vlan1                  unassigned      YES unset  administratively down down
GW#
```

And set cyt115.local as a domain-name:



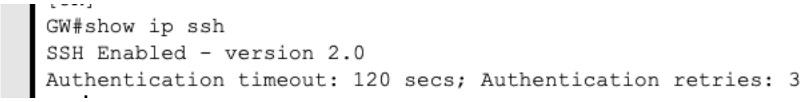
```
GW#
GW#show running-config | include ip domain-name
ip domain-name cyt115.local
GW#!
```

Configure router to allow SSH with encrypted password:

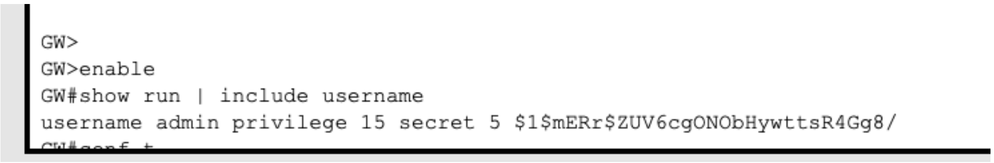


```
GW(config)#! Generate RSA keys for SSH
GW(config)#crypto key generate rsa modulus 1024
                                   ^
% Invalid input detected at '^' marker.

GW(config)#crypto key generate rsa general-keys modulus 1024
% You already have RSA keys defined named GW.cyt115.local
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
*Mar 1 0:4:43.541: %SSH-5-ENABLED: SSH 2 has been enabled
GW(config)#username admin privilege 15 secret MyStrongPassword
GW(config)#! Configure VTY lines to allow SSH login
GW(config)#line vty 0 4
GW(config-line)#login local
GW(config-line)#transport input ssh
```

The result account uses for ssh:



```
GW#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```



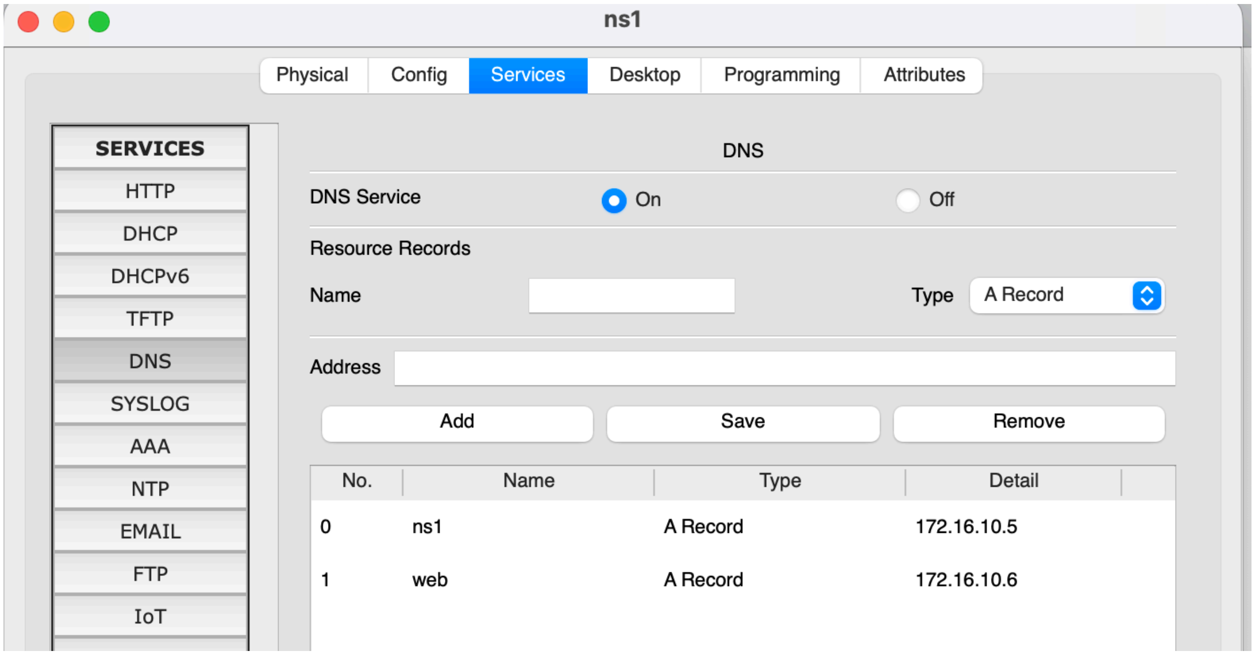
```
GW>
GW>enable
GW#show run | include username
username admin privilege 15 secret 5 $1$mERr$ZUV6cgONObHywttsR4Gg8/
```

Configure DNS SERVER

DNS server serves as address translation, allows to lookup devices by defined name rather than IPv4. It should have A records for itself and for the web server.

I can be configured through the services tab:

Appendix B: DNS server Configuration



DNS

DNS Service ● On ○ Off

Resource Records

Name

Type A Record

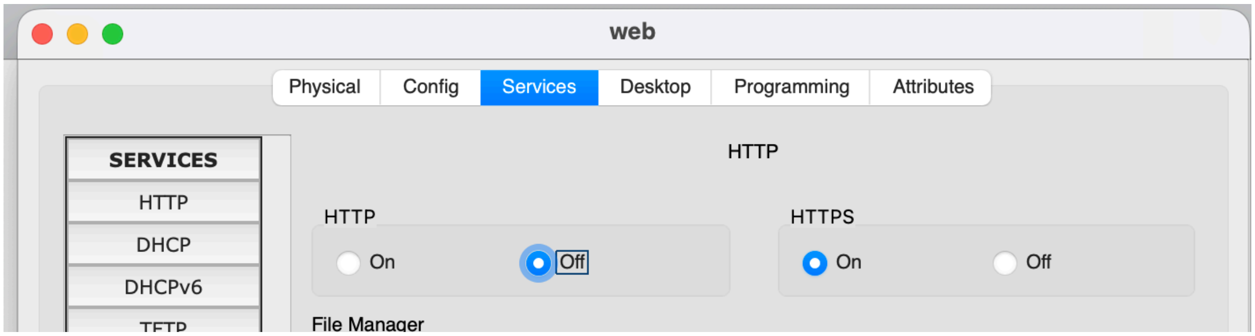
Address

No.	Name	Type	Detail
0	ns1	A Record	172.16.10.5
1	web	A Record	172.16.10.6

Configure WEB SERVER

Web server allows device to lookup web page through typing IPv4 address in web browser. It can be configured through HTTP tab under device services, for this setting, only HTTPS connection is allowed for its security capacity.

Appendix C: Web server Configuration



HTTP

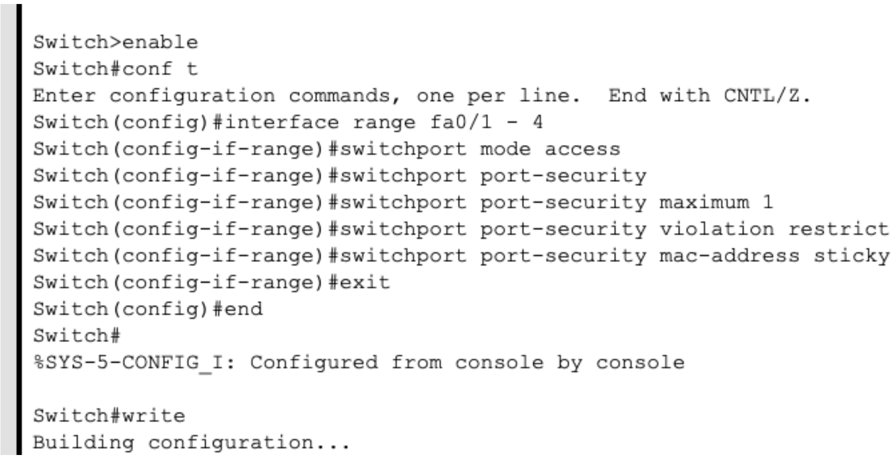
HTTP ○ On ● Off

HTTPS ● On ○ Off

Configuring Switch Port Security

I configured switch ports fa0/1 to fa0/4 as access ports with port security, allowing only one device per port and using sticky MAC addresses to remember connected devices; this ensures that unauthorized devices are blocked while legitimate devices maintain network access. Switch on the right side should follow similar setting.

Appendix D: Switch Configuration



```
Switch>enable
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#interface range fa0/1 - 4
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security maximum 1
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#switchport port-security mac-address sticky
Switch(config-if-range)#exit
Switch(config)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#write
Building configuration...
```

Configure the ACL

ACL is lists of rules that control incoming and exiting traffic through the network, for this project, ACL allows all PCs to have access to DNS and web server, while only PC0 can ping DNS and webserver. Furthermore, PC1/2 can SSH login to GW router, and all rest type of IP packet from left network to right network should be blocked. It can be configured through the router through these commands:

Router> enable

Router# configure terminal

! Define ACL

Router(config)# access-list 10 permit 192.168.10.1

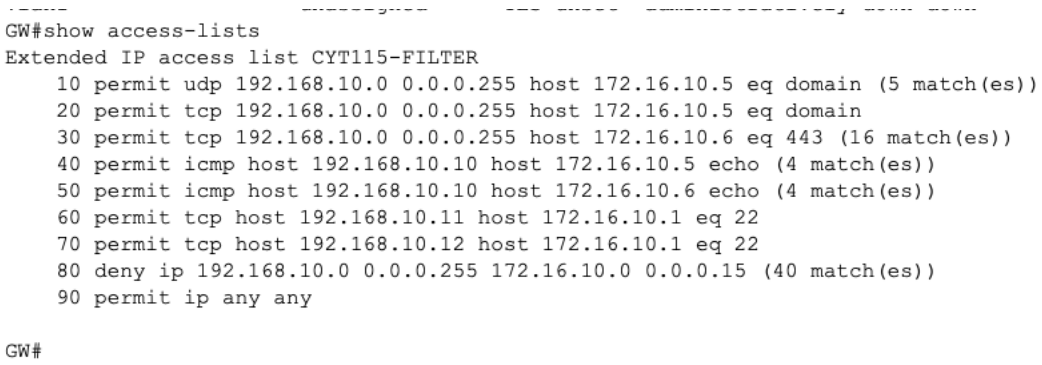
! Apply to an interface (inbound traffic)

Router(config)# interface GigabitEthernet0/0

Router(config-if)# permit udp 192.168.10.0 0.0.0.255 host 172.16.10.3 eq 53

The ACL after configuring is as follow:

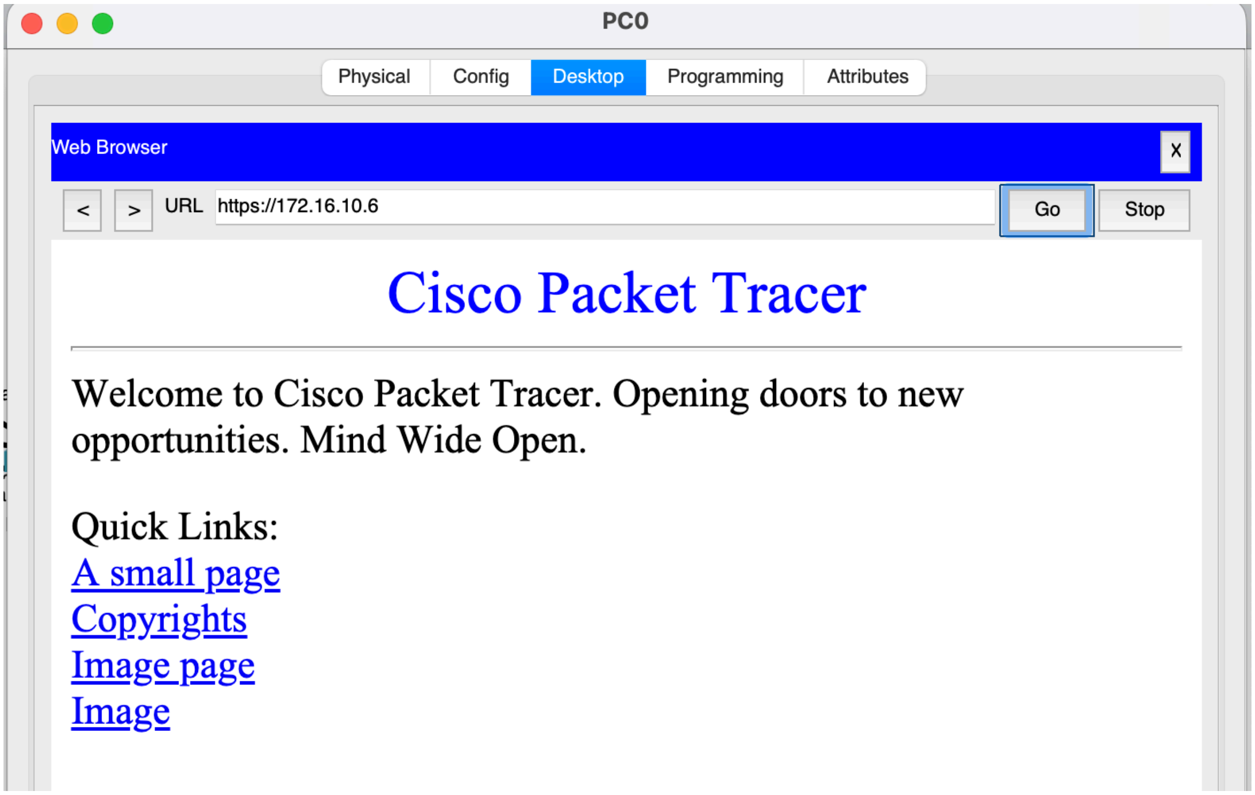
Appendix E: ACL Configuration



```
GW#show access-lists
Extended IP access list CYT115-FILTER
    10 permit udp 192.168.10.0 0.0.0.255 host 172.16.10.5 eq domain (5 match(es))
    20 permit tcp 192.168.10.0 0.0.0.255 host 172.16.10.5 eq domain
    30 permit tcp 192.168.10.0 0.0.0.255 host 172.16.10.6 eq 443 (16 match(es))
    40 permit icmp host 192.168.10.10 host 172.16.10.5 echo (4 match(es))
    50 permit icmp host 192.168.10.10 host 172.16.10.6 echo (4 match(es))
    60 permit tcp host 192.168.10.11 host 172.16.10.1 eq 22
    70 permit tcp host 192.168.10.12 host 172.16.10.1 eq 22
    80 deny ip 192.168.10.0 0.0.0.255 172.16.10.0 0.0.0.15 (40 match(es))
    90 permit ip any any

GW#
```

Connectivity check

Connect to web server all PC should be all to access the web server through HTTPS and connect through HTTP is not allowed since its less secure

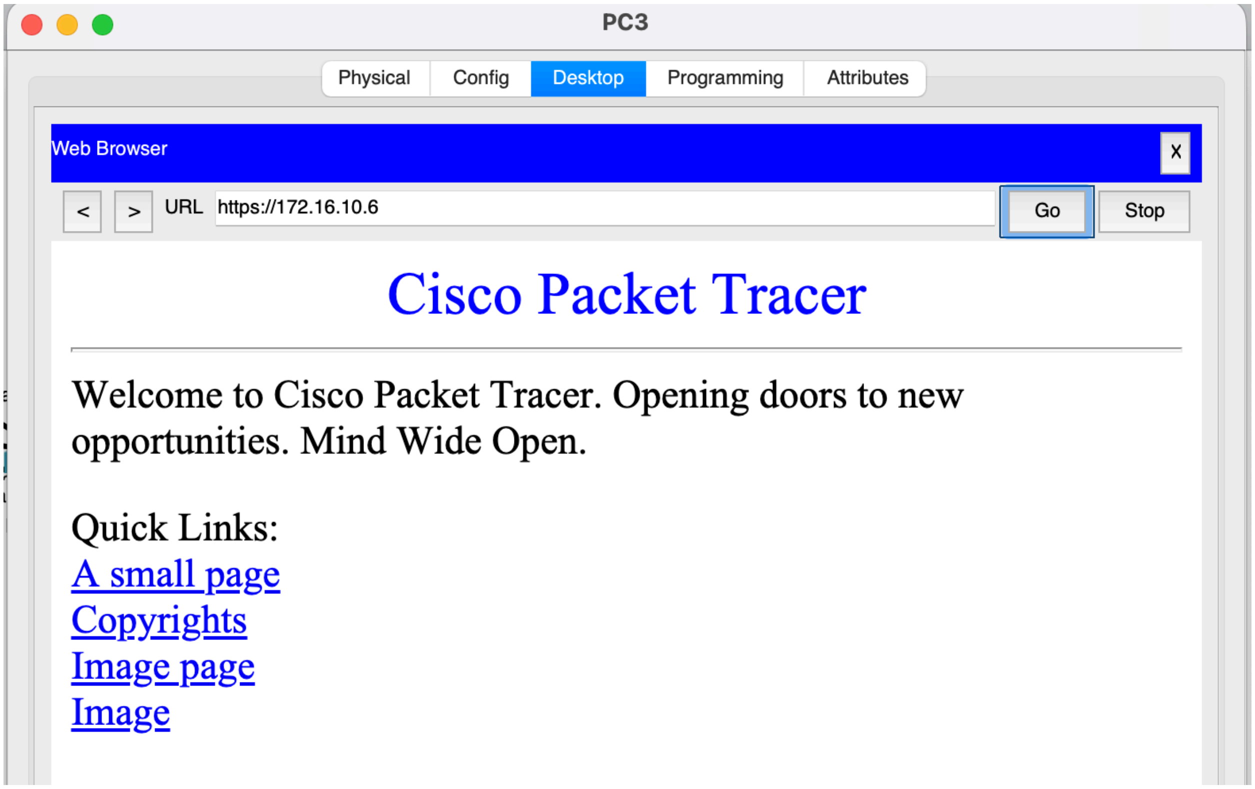


URL https://172.16.10.6

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

Quick Links:
A small page
Copyrights
Image page
Image



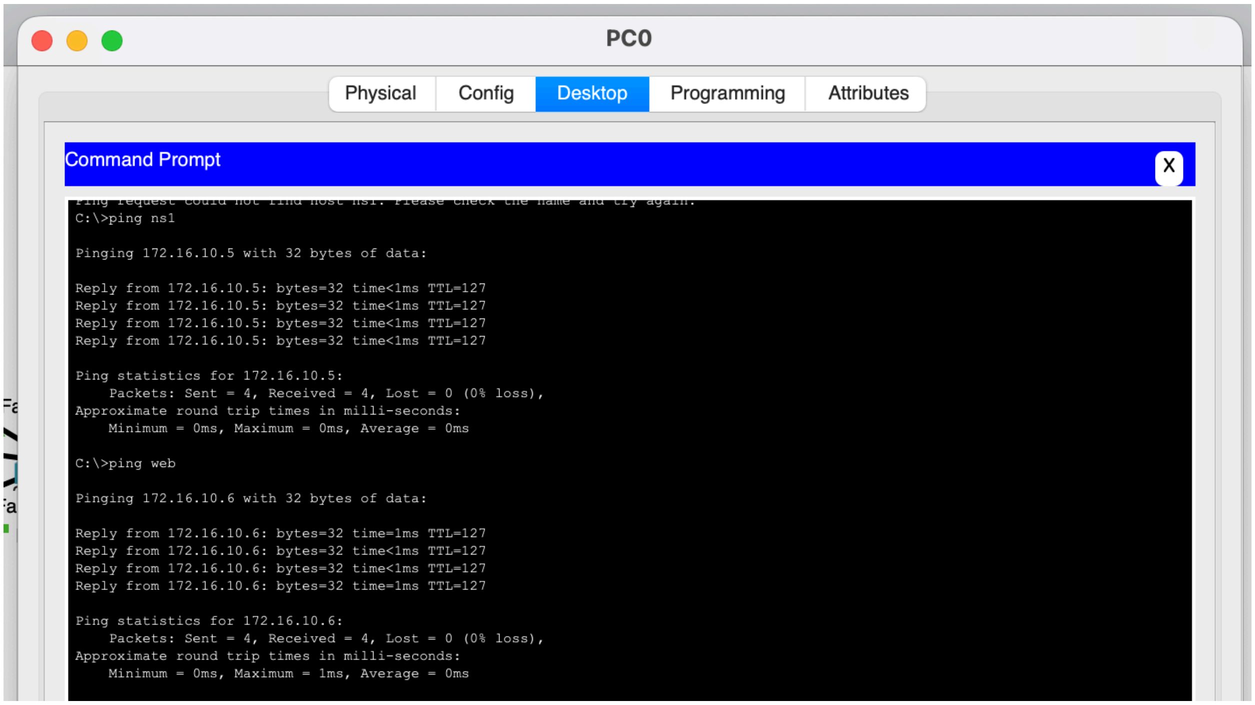
URL https://172.16.10.6

Cisco Packet Tracer

Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.

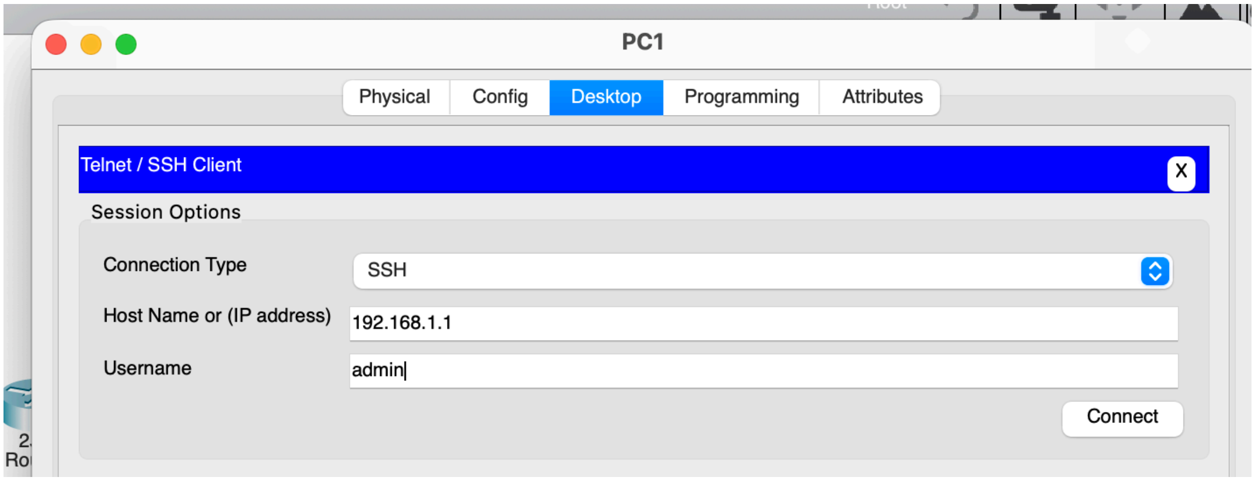
Quick Links:
A small page
Copyrights
Image page
Image

PC0 can ping web server and web server:



```
Ping request could not find host ns1. Please check the name and try again.
C:\>ping ns1

Pinging 172.16.10.5 with 32 bytes of data:

Reply from 172.16.10.5: bytes=32 time<1ms TTL=127
Reply from 172.16.10.5: bytes=32 time<1ms TTL=127
Reply from 172.16.10.5: bytes=32 time<1ms TTL=127
Reply from 172.16.10.5: bytes=32 time<1ms TTL=127

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping web

Pinging 172.16.10.6 with 32 bytes of data:

Reply from 172.16.10.6: bytes=32 time=1ms TTL=127
Reply from 172.16.10.6: bytes=32 time<1ms TTL=127
Reply from 172.16.10.6: bytes=32 time<1ms TTL=127
Reply from 172.16.10.6: bytes=32 time=1ms TTL=127

Ping statistics for 172.16.10.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pc1/2 can ssh into router securely with encrypted password, the ssh connection is established for the router with the following credential:

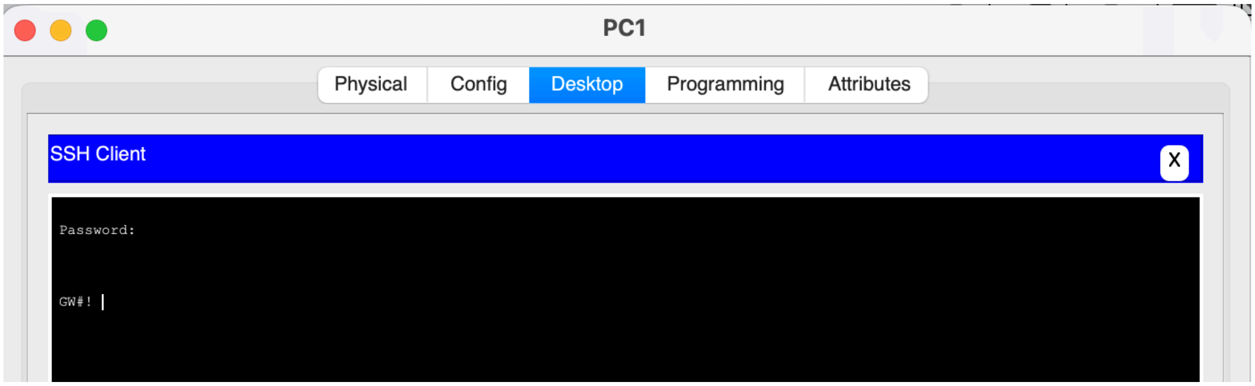


Session Options

Connection Type: SSH

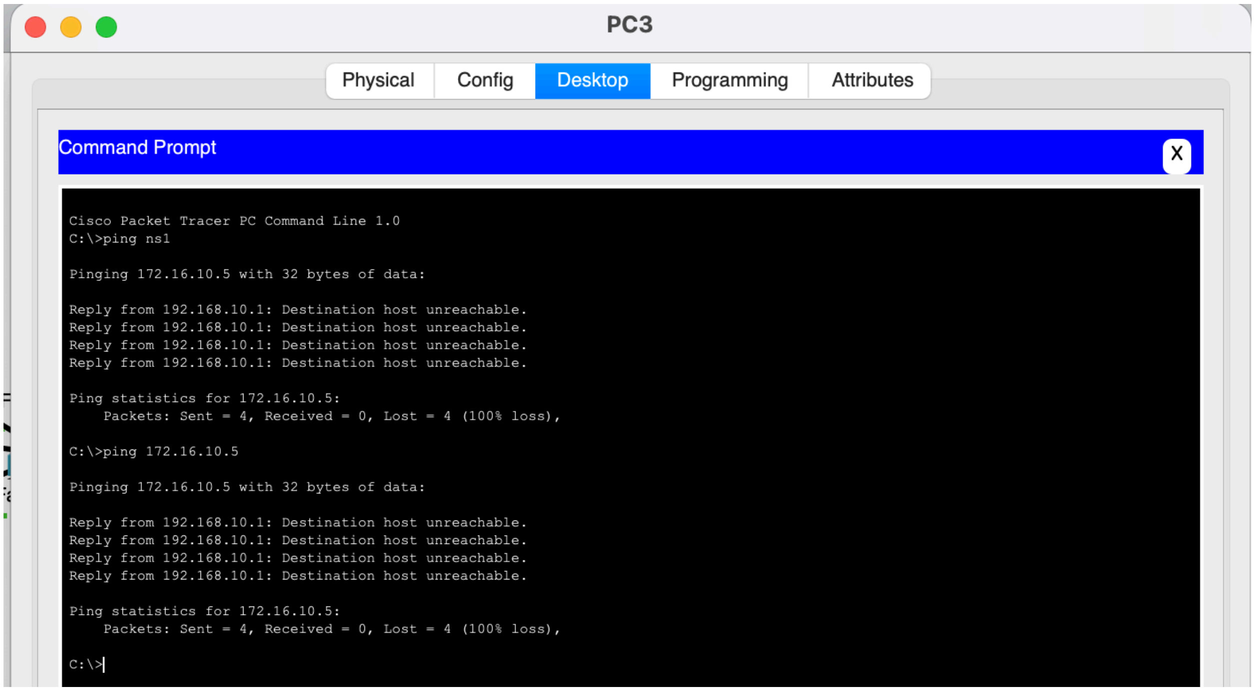
Host Name or (IP address): 192.168.1.1

Username: admin



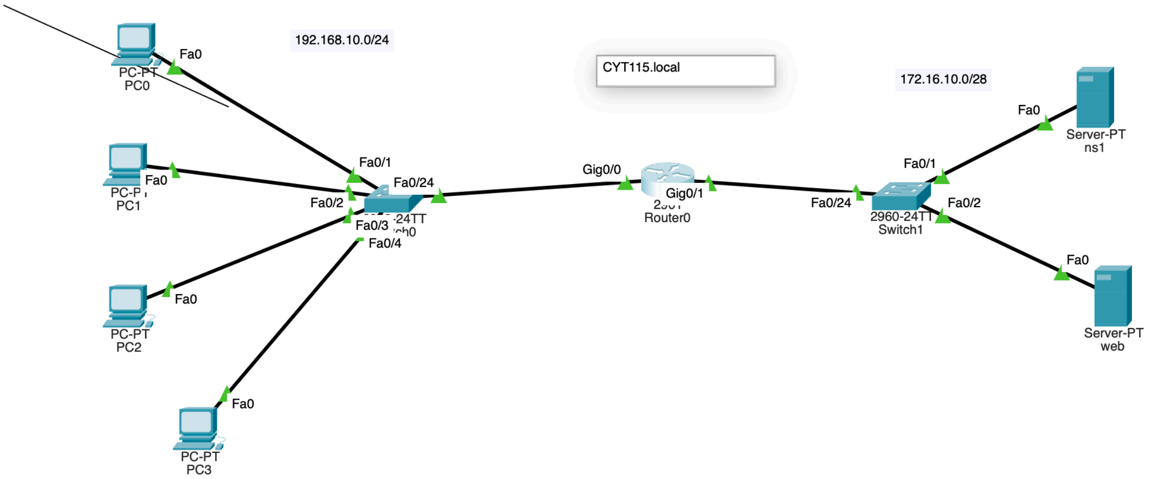
```
Password:


GW#!
```

Connection that are not permitted on the ACL should be blocked:



```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping ns1

Pinging 172.16.10.5 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.10.5

Pinging 172.16.10.5 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 172.16.10.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

Physical layout of the final project:



Summary:

The CYT 115 Project focused on designing and securing a small network infrastructure using Cisco Packet Tracer. Key tasks included configuring router interfaces, setting up SSH with encrypted passwords, and implementing ACLs to control traffic and restrict access to critical resources. Switch port security was applied to harden access to servers, ensuring only authorized devices could connect. The project emphasized practical skills in network configuration, security enforcement, and traffic management, providing hands-on experience with industry-standard networking practices.

Appendix:

Appendix A: Router Configuration

Appendix B: DNS server Configuration

Appendix C: Web server Configuration

Appendix D: Switch Configuration

Appendix E: ACL Configuration

References

Seneca College – CYT115 Course Materials

Seneca College. (2025). *CYT115 Lab 10,11,12: VLANs and Inter-VLAN Routing*. School of Information Technology Administration & Security.

Seneca College. (2025). *CYT115 Lecture 11: Firewalls.pdf*. School of Information Technology Administration & Security.