PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

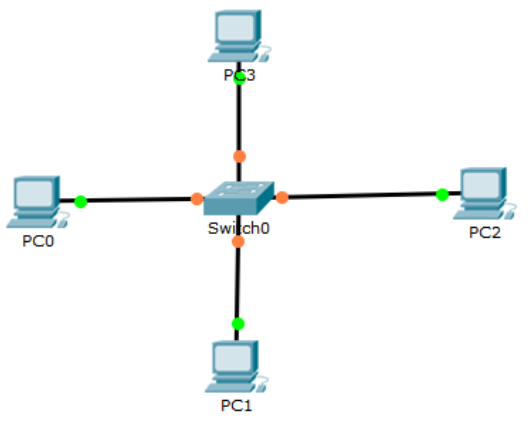
Wales Institute of Science and Art (WISA)

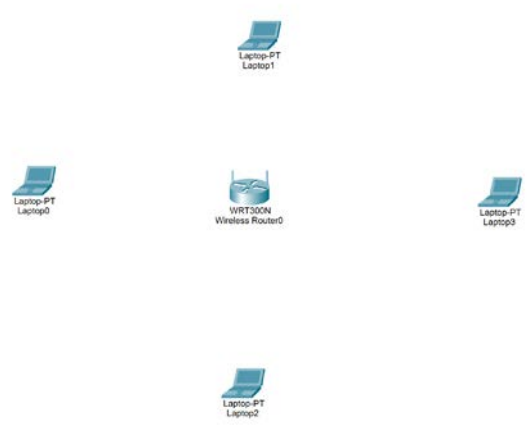
Networks and Cybersecurity Essentials (ACCA4024)

Lab 4: Design and Implement Home Network.

Cisco | Networking Academy®
Mind Wide Open™

Topology:





Topology 1 **Topology 2**

LAB Objectives

After designing the above home network, we have to configure the network and make a successful network.

Topology 1:

1. Using Windows Calculator to determine the IP address of the hosts in the network.
2. Configure the Intermediate L2 device to the network and test the network. Troubleshoot if required.

Topology 2:

1. Configure wireless network and enhance security.

Requirements

- Use Packet Tracer to create the above recommended topology

Use for reading

Intermediate Devices: *(Switch, Routers)*

The two most common methods to access the command line interface of any intermediate devices are console and SSH. For a console, a PC/ Laptop needs to be directly connected to the console port of the network device to configure. For SSH, a pre-configuration is required to access.

Switch: Layer 2 Device

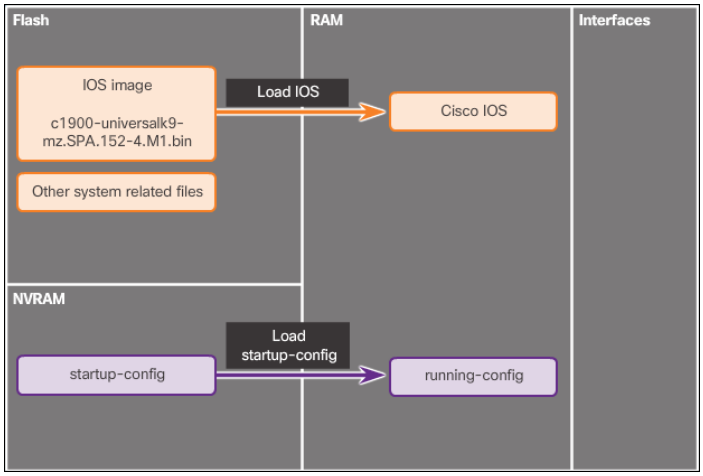
When the switch is on, the power-on self-test (POST) begins.

During POST, the LEDs blink while a series of tests determine that the switch is functioning properly.

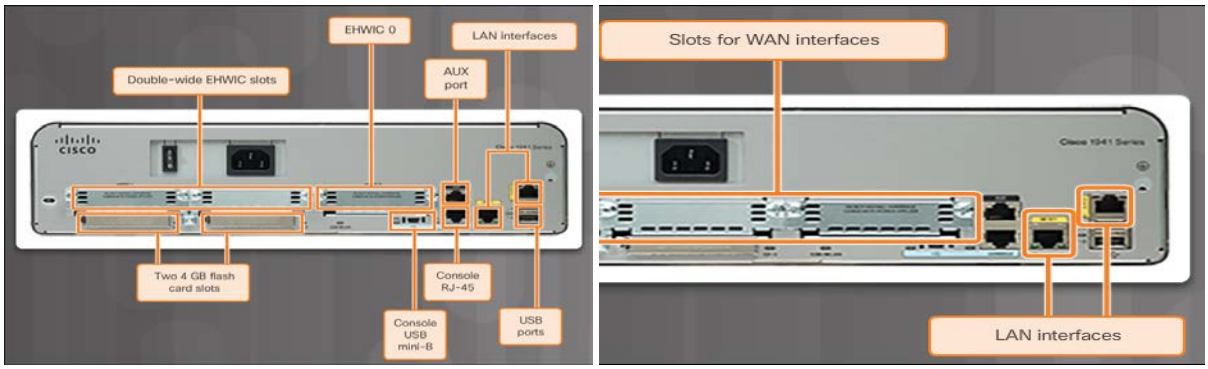
POST is completed when the SYST LED rapidly blinks green.

If the switch fails POST, the SYST LED turns amber.

Memory



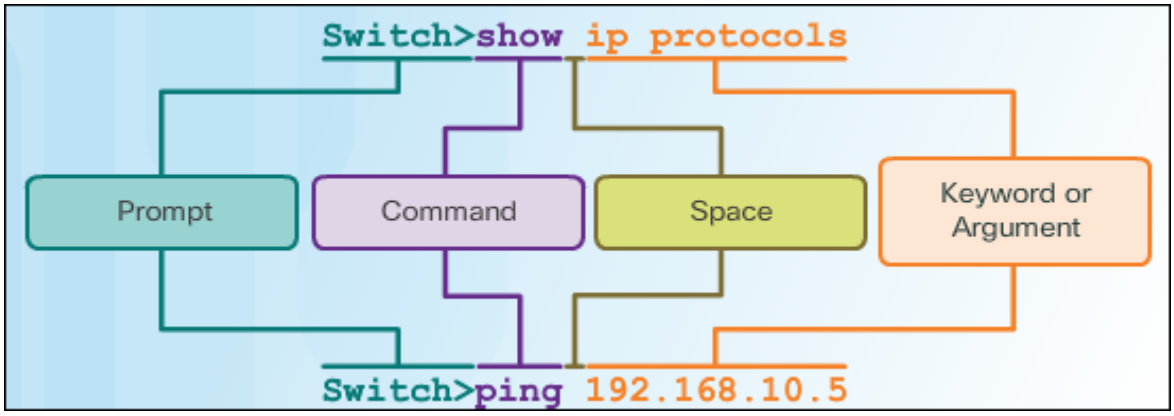
Router



All routers are essentially computers. Just like computers, routers also require operating systems (OS), central processing units (CPU), random-access memory (RAM), read-only memory (ROM), and nonvolatile random-access memory (NVRAM).

Every Cisco router has the same general hardware components, and these connections: console ports, 2 LAN interfaces, and enhanced high-speed WAN interface card (EHWIC) slots.

Command Mode	Description	Default Device Prompt
User Exec Mode	• Mode allows access to only a limited number of basic monitoring commands. • It is often referred to as "view-only" mode.	`Switch>` `Router>`
Privileged EXEC Mode	• Mode allows access to all commands and features. • The user can use any monitoring commands and execute configuration and management commands.	`Switch#` `Router#`




```
Switch>enable
Switch#show ru
Switch#show running-config
Building configuration...

Current configuration : 1080 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Switch
!
```

Task 1: Switch Configurations (Use Topology 1)

Create the Topology as given in Packet Tracer.

Configure IP Address and Subnet Mask for PC0, 1, 2, 3

Device	Interface	IP Address	Subnet Mask
PC0	NIC	11000000.10101000.01001000.00011110	/24
PC1	NIC	11000000.10101000.01001000.00101000	/24
PC3	NIC	11000000.10101000.01001000.00110010	/24
PC4	NIC	11000000.10101000.01001000.01000110	/24

Basic Switch Configurations

1. **User Mode, Privilege Mode, Global Configuration Mode:**
2. **Give a Host Name: SwTMyFirstSwitch**

```
Swt1(config)#hostname SwTMyFirstSwitch
```

The NO Command

To remove a command, use ***"no"*** *before the executing command Eg: no hostname*

3. **Passwords (Basic Security)**

Configure console password: cisco123

```
>enable
# Config t
Line console 0
password cisco123
login
Exit
#
```

Configure vty password: 1CiSc3

```
>enable
# Config t
Line vty 0 15
password 1CiSc3
login
Exit
#
```

Enable Privileged Password: Password

```
>enable
# Config t
Enable password cisco
```

Observe the running configuration of your switch and note the configuration

hostname SwTMyFirstSwitch
enable password cisco
line con 0 - password cisco123
line vty 0 4 - password 1CiSc3
line vty 5 15 - password 1CiSc3

Is your privileged password shown in running-configuration? (Yes/No)
If Yes, how is it displayed?

Yes. It is encrypted. It says: "enable password cisco".

Now, remove the privileged password. To do that, go to config mode (Privileged Executive mode)

Config t
No enable password cisco
And Type
enable secret cisco

Observe the running configuration of your switch again and note the difference between password and secret

hostname SwTMyFirstSwitch
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
line con 0 - password cisco123
line vty 0 4 - password 1CiSc3
line vty 5 15 - password 1CiSc3

How are the other passwords?

Other passwords are not encrypted and are displayed as plain text.

Now, go to config mode (Privileged Executive mode) again

Config t
Service password-encryption

Observe the running configuration of your switch again and note the difference now

hostname SwTMyFirstSwitch
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
line con 0 - password 7 0822455D0A16544541
line vty 0 4 - password 7 08706F473A1A56
line vty 5 15 - password 7 08706F473A1A56

The DO Command

Allows you to execute any EXEC mode command from within any configuration mode Eg:

Config t

Do show running-configuration

4. IP Address

```
SwTMyFirstSwitch > en
SwTMyFirstSwitch # config t
SwTMyFirstSwitch (config)#interface vlan 1
SwTMyFirstSwitch (config-if)#
ip address 192.168.72.254 255.255.255.0
SwTMyFirstSwitch(config-if)#no shut
SwTMyFirstSwitch(config-if)#exit
```

5. Show Commands

Show running-config

show interfaces

show arp

show version

Erase startup-config

Reload

The BANNER Display your banner

banner motd "

Enter TEXT message. End with the character ""
Welcome to Switch GF "

6. Save the Configurations

copy run startup
write memory

Try out!!!

Add a router to your network and do the same configurations and record your reflections

Before password changes:
hostname SwTMyFirstRouter
enable password cisco
line con 0 - password cisco123
line vty 0 4 - password 1CiSc3
line vty 5 15 - password 1CiSc3

After password encryptions:
hostname SwTMyFirstRouter
enable secret 5 1mERr$hx5rVt7rPNoS4wqbXKX7m0
line con 0 - password 7 0822455D0A16544541
line vty 0 4 - password 7 08706F473A1A56
line vty 5 15 - password 7 08706F473A1A56

References:

Ipconfig - ipconfig /all - ipconfig /release and ipconfig /renew

ping

netstat

tracert

nslookup

Understand:

If pings to both the name and IP address are successful, but the user is still unable to access the application, then the problem most likely resides in the application on the destination host

If neither ping is successful, then network connectivity along the path to the destination is most likely the problem

If the ping to the default gateway is successful, the problem is not local. If the ping to the default gateway fails, the problem resides on the local network.

A ping may fail due to the firewall on the sending or receiving device, or a router along the path blocking the pings.

Task 2: Wireless Configurations (Use Topology 2)

Create the topology using Cisco packet Tracer.

In your wireless router (WRT 300N), do the following configurations

- Set up Router IP Address 192.168.10.1
- Enable DHCP
- Set Start IP as 192.168.10.20
- Maximum No. of users: 3
- Save the configuration.
- Set the Network mode: Mixed
- Name your network: MyNetwork
- Enable Broadcast
- WPA2 Personal Security
- Encryption AES
- Passpharse: 123456789
- Router Password: Cisco
- Enable Remote Management

Connect all the end devices as per the topology to the Wireless router.

Did all the laptops successfully connected to the wireless router?

No.

If NO, Troubleshoot until all the hosts successfully connects and record your troubleshooting methods here.

I had to replace all of the laptops modules so they supported a wireless connection.

Did all the laptops gain DHCP IP address?

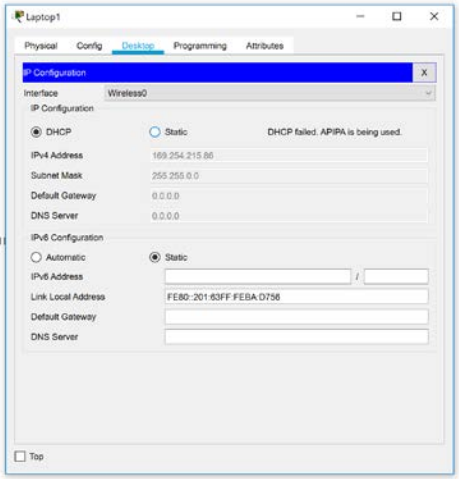
No.

Record your understanding, why all the laptops could not get IP address assigned from the DHCP.

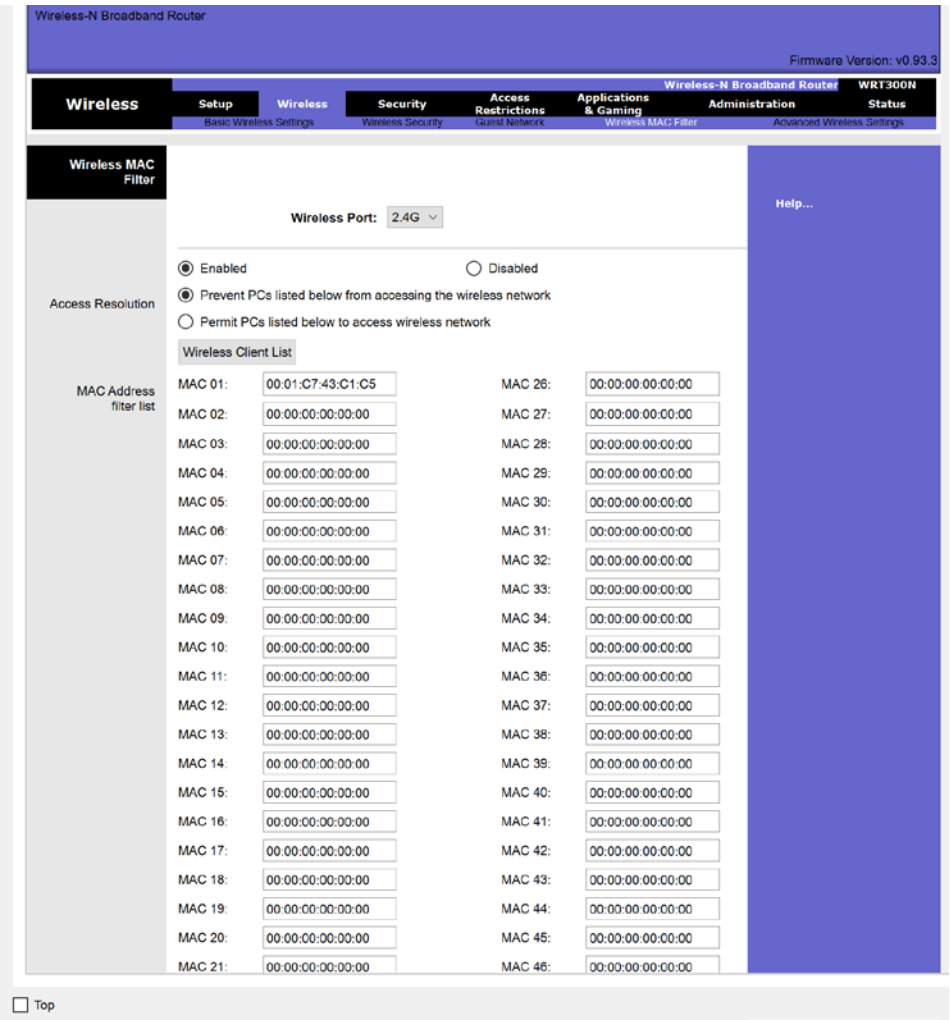
Only 3 laptops were able to get an IP assigned from DHCP because I limited the amount of users on the network to 3. Therefore, one laptop does not have an approprite IP address.

Disable and enable the DHCP IP Configurations in the Laptop and check the status.

DHCP failed therefore APIPA is being used.



Collect the MAC address of any two laptops and go to wireless mac filter option in the wireless router and set MAC Addressing FILTERING to prevent them to connect the network.



Observe the changes in the network and record your reflections about MAC Filtering and enhancing the security in Wireless Networks.

Since I configured the router's settings to prevent laptop1 and laptop 2 from connecting to the network, they are no longer able to do so. I can therefore use MAC filtering to prevent malicious users from connecting to the network and causing it harm, whilst allowing other users to connect without an issue.

Learnings from this lab:

- ✓ ***Build a home Network***
- ✓ ***Understand and configure IP Address***
- ✓ ***Use Ping/ Trace route Utility to check the connection status***
- ✓ ***Use ipconfig /all command to determine the MAC address of a Windows computer on an Ethernet network.***
- ✓ ***Analyze a MAC address to determine the manufacturer.***
- ✓ ***Analyze the Wired and Wireless Network connection.***
- ✓ ***Analyze Address Resolution Protocol (ARP).***
- ✓ ***Connect to a Wireless Router and configure the basic settings in a wireless router and add security features.***
- ✓ ***Use nslookup command to understand the url to ip conversion.***
- ✓ ***Configure basic connectivity settings in Intermediate devices (Switch/ Router).***