LAB Program - 9

Share the folder in a system, and access the files of that folder from other system using IP address

Windows to Windows sharing

Step 1: Enable file sharing

1. Open Control Panel - Network & sharing Center
2. Click on Change advanced sharing settings
3. Under Private, ensure the following are enabled:
   - Turn on network discovery
   - Turn on file and printer sharing
   - Turn off password-protected sharing (optional if you want access without needing credentials)

Step 2: Share the folder

1. Right-click the folder you want to share
2. select properties → sharing tab
3. Click Advanced sharing
4. Check Share this folder, then Click Permissions and configure the access premissions (e.g. Read, Write).
5. Click OK and close the window

Step 3: Obtain the IP address

1. Open Command prompt
2. Type ipconfig and press Enter
3. Look for the IPv4 Address (eg. 192.168.1.x)

Step 4: Access the folder from Another System

1. On the second system, open file Explorer.
2. In the address bar, type \\[IP Address] (eg. \\192.168.1.x) and press Enter
3. You should now see the shared folder. You may need to enter credentials if password protection is enabled.

OR

1. On the second system, open RUN /windows+R
2. Type \\[IP Address] (eg. \\ 192.168.1.x) and press OK
3. You should now see the shared folder. You may need to enter credentials if password protection is enabled.

Lap Prg - 7

Configure and connect the computer in lan

1. Launch cisco Packet Tracer:
   Open the cisco packet application of your computer
2. Create a simple Network Topology
   - select End devices from the device types
   - Drag & drop PC's (end devices) onto the workspace, place as many PC's as you want to connect
   - Drag & drop a switch onto the workspace, use the 2960 switch (which is common for lan)

3. Connecting Devices
   - select the connections tab
   - choose the copper straight: Through cable (represented by a solid line)
   - click on the first pc, then select Fast Ethernet0 (network interface) as the port
   - Next, click on the switch and select any Fast Ethernet port (e.g, Fast Ethernet 0/1) to connect the pc to the switch
   - Repeat this process to connect all other PC's to the switch via different ports

(4) Configure IP addresses:

Assign each computer a unique IP address within the same network

* click on the first PC
* Go to the desktop tab and select IP configuration
* Enter the IP address & subnet mask, Example
  - IP address: 192.168.1.1
  - Subnet mask: 255.255.255.0
* Repeat the process for each PC, assigning them different IP's (e.g. 192.168.1.3, 192.168.1.4, etc) but use the same subnet mask

5. Verify Connections

* Use the command Prompt on one of the pc's to verify connectivity
* Open command prompt on one PC by selecting the desktop tab → Command prompt
* Type the following command to ping another PC IP address: ping 192.168.1.3

* If you recieve replies, the connection is succesfull, Meaning the computer are properly connected in a lan.

lab program - 4

Study of network IP address configuration (classification of address, static & dynamic address)

What is an IP Address?

An IP address (internet protocol address) is a unique no. assigned to every device connected to an network whether it's a computer, smartphone, printer or router

Static IP Address

A static IP address is manually assigned to a device and does not change unless manually modified. It's like assigning a permanent home address to a device

Features

- Manual Assignment: Requires an administrator to configure it.
- Doesn't change: Once assigned, the device keeps the same IP address
- Common Uses:
  - Servers that need to be consistently reachable (e.g. web servers, file servers)
  - Devices that need to maintain a fixed identity in the network such as printers or security cameras.

Dynamic IP Address

A dynamic IP address is automatically assigned by a DHCP server (Dynamic Host Configuration Protocol) whenever a device connects to the network, most home networks and small offices use dynamic IP address

Features

- Automatic Assignment: Devices automatically receive an IP address from the DHCP server
- Can change: The IP address may change after the device disconnects or if the DHCP lease expires
- Common Uses:
  - Home and office devices like laptops, smartphones, & tablets that don't require a fixed IP address
  - Any devices that doesn't need to be consistently reachable at the same address

lab program - 5

Study of network IP address configuration (IPv4 & IPv6, Subnet, Supernet)

IPv4 (Internet Protocol version 4): IPv4 is the most commonly used version of the internet protocol and has been the foundation of network communication for decades.

Key Characteristics of IPv4:

- Address format: IPv4 address are 32-bit numbers, represented as four octets (8-bit blocks) separated by dots (also called dotted decimal notation)
  - Example: 192.168.1.1
- Address Space: IPv4 supports around 4.3 billion unique address (2^32).
- Depletion of addresses: Due to the rapid growth of devices connected to the internet, IPv4 addresses have become scare. Techniques like NAT (Network Address Translation) and private IP addressing have been implemented to extend the life of IPv4
- Common Use: Despite the development of IPv4, is still widely used in most networks todays. especially in private networks.
- Example of IPv4 Address:

  192.168.0.1: A typical home router IP

  Subnet mask: Common subnet mask 255.255.255.0

IPv6 (Internet protocol version 6):

IPv6 was developed to overcome the limitations of IPv4, particularly the exhaustion of address

Key characteristics of IPv6:

- Address format: IPv6 address are 128-bit numbers, represented in hexadecimal format & separated by colons
  - Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334
- Address space: IPv6 supports an enormous number of addresses (approximately 340 undecillion addresses, or 2^128), making it virtually impossible to run out of address
- No NAT Needed: Since there are plenty of addresses, IPv6 doesn't rely on NAT (Network Address Translation) as IPv4 does

What is Subnetting?

Subnetting is the process of dividing a large network into smaller, more manageable subnetworks, or subnets. This helps improve network efficiency, security, & address management

Efficient IP Address Usage:

Subnetting allows better allocation of IP addresses. for example, instead of wasting addresses in a large network, you can divide it into subnets based on the

actual number of devices (hosts) needed).

Example

* Original Network: You have the IP address block 192.168.1.0/24. This means:
  - Total Address: 256 (from 192.168.1.0 to 192.168.1.255)
  - Usable Address: 254 (after subtracting 2 for network and broadcast address)

* Subnetting:

You decide to divide this network into smaller subnets to keep things organized & manage traffic better. You want to create 2 subnets:

- Subnet 1:
  - Network Address: 192.168.1.0/26
  - Usable Address: 62 (from 192.168.1.1 to 192.168.1.62)
  - Broadcast Address: 192.168.1.63

- Subnet 2:
  - Network Address: 192.168.1.64/26
  - Usable Addresses: 62 (from 192.168.1.65 to 192.168.1.126)
  - Broadcast Address: 192.168.1.127

What is supernetting?

Supernetting is the opposite of subnetting. Instead of dividing a network into smaller subnets, supernetting combines multiple networks (subnets) into a larger network. This is also known as CIDR (Classless Inter-Domain Routing)

Scenario: You manage multiple small networks for different departments in a company Each department has its own network

- Department A: 192.168.2.0/26 (64 addresses)
- Department B: 192.168.2.64/26 (64 addresses)
- Department C: 192.168.2.128/26 (64 addresses)
- Department D: 192.168.2.192/26 (64 addresses)

Total: You have 4 small network that you want to combine to simplify management

1. Supernetting: You decide to aggregate these four network into a single larger network:

- Combined Network:
  - Network address: 192.168.2.0/24
  - Total addresses: 256 (from 192.168.2.0 to 192.168.2.255)
  - Usable Address: 254 (after subtracting 2 for network & broadcast addresses)

lab program-12

Configuration of switch:

1. Configure password (for login to switch)
Enable for switch configuration steps

step1: Switch > Enable (en)
step2: Switch # Config t / configuration
step3: Switch (config) # line console 0/con 0
step4: Switch (config-line) # password 1234
step5: Switch (config-line) # login
step6: Switch (config-line) # Exit
step7: Switch (config) # Exit
step8: Switch # Exit

2. Configure password for configuration switch

Step1: Switch En or Enable
Step2: Switch # Config t / Configuration terminal
step3: Switch (config) # enable secret 123456
step4: Switch (config) # Exit
step5: Switch # Exit

To check for configuration password (ie. login to switch)
first need to enter console password.
User Access Verification

password: (login password)
switch > En /enable
password: (configoration password i.e secret password)

switch #

3. Configure switch hostname as st. Francis

step 1: Switch # configure t
step 2: Switch (config) # hostname st. francis
step 3: St. francis (config) #

4. Configure the messag of the day as "Welcome to st. francis college".

Step 1: st. francis (config) # banner motd #
" Welcome to st. francis college"

step 2: st. francis (config) # Exit (To check the message exit from the configoration)

step 3: st. francis # Exit

Lab program 10

Share the printer in network and take print from other PC

Step 1: Set up the devices

a. Add devices to the workspace:
* Drag and drop a printer (e.g. a generic printer) & two PC's onto the workspace
* Add a switch to the workspace to connect the devices

b. Connect the devices
* Use copper straight - Through cables to connect each PC & the printer to the switch

Step 2: Assign IP address.

a. Configure IP address on each PC:
* Click on PC0 > Desktop > IP configuration
  - Assign an IP address, such as 192.168.1.2
  - set the subnet mask be 255.255.255.0
* Repeat for PC1 with an IP address e.g. 192.168.1.3

b. Assign IP address to the printer
* Click on the printer > Config > settings
  - Assign an IP address such as 192.168.1.2
  - set the subnet mask to 255.255.255.0

Step 3: Set up printer on PC0 and PC1

a. Test the printer connection on PC0 & PC1

- Go to PC0 > Desktop > Command prompt
- Ping the printer using Command ping 192.168.1.10
- Ensure the printer is reachable
- Follow the same steps on PC1 also

Lab program 11

Configuration of wifi-hotspot, and connect other devices (mobile / laptop)

Step 1: Set up a wireless Router

a. Add a wireless Router:

- In cisco packet tracer, go to the network devices section & drag a wireless Route (e.g. WRT 300N) onto the workspace

b. Configure the wireless Router:

- click on the router go to the config (or) GUI tab
- Under the wireless settings:
  - set the SSID (e.g. "SFCwifi")
  - choose a security mode (eg. WPA-2 PSK for stronger security)
  - set a Pre-shared key (123 456 789)
- Configure other parameters a needed (e.g DHCP settings to provide IP address automatically to devices)

Step2:- Setup a Device to connect to wifi (e.g laptop or smartphone)

a. Add a laptop or smartphone

- Go to the End Devices section & drag a laptop or smartphone onto the workspace

b. Connect the devices to wifi:
- Click on the device & go to the desktop tab (for laptops) or Config tab (for smartphone)

- select the pc wireless or smartphone Wireless configuration
- Search for avaiable networks select the SSID you configured (e.g. 'SFC wifi') & enter the pre-shared key to connect

Step 3: Test the connection

a. Verify Connectivity

- Once connected, try pinging the router's IP address from the devices to confirm it's connected to the wifi network.

lab program 15

Configuration of VLAN using packet Tracer / GNS3

A VLAN (Virtual Local Area Network) is a way to divide a network into smaller, isolated sections, even though they all share the same physical hardware. It allows you to create separate "networks" within a single switch or network infrastructure.

In the example below:

- we created two separate groups of devices: PCs on the 192.12.1.x network and PCs on the 192.12.20.x network

- VLAN 20 was setup to logically separate PCs (PC2 & PC3) from the rest of the network

- Devices on VLAN 20 can only communicate with other devices within the same VLAN unless a router allows traffic b/w VLANS.

Step 1 :- Set up the hardware

- Deploy four PC's, one router (cisco 1841 model), & one switch (cisco 2960) in the simulation environment

Step 2: Connect PC's to the switch

- Use copper straight-through cables to connect each PC to the switch
- steps:-
  - * Select the cable
  - * Click on PC0, select FastEthernet 0.
  - * Connect it to switch on Fast Ethernet 0/7
  - * Repeat this process for the other PC's connecting each to a different FastEthernet port on the switch

Step 3: Connect the Router to the switch

- Connect the router to the switch using a copper straight through cable
- steps:
  - * click on the switch, select FastEthernet 0/5
  - * Connect it to the router's Fast Ethernet - 0/0

Step 4: Configure the Router interface

- set up the IP address on the router
- steps:
  - * Click on the router go to the Config tab, select Fast Ethernet 0/0
  - * set the IP address to 192.12.1.1
  - * Enable the port status (turn it ON)

Step 5: Configure PC0

- set IP configuration on PC0
- steps:
  - * Go to the config tab, select Fast Ethernet 0

* Set the IP address to 192.12.1.2
* In the settings tab, set the default gateway to 192.12.1.1 (router IP)

Step6: Configure PC1
- set IP configuration on PC1
- steps:
  * set the IP address to 192.12.1.3
  * set the default gateway to 192.12.1 (router IP)

Step7: Configure PC2
- set IP configuration on PC2
- steps:
  * set the IP address to 192.12.20.2
  * set the default gateway to 192.12.20.1

Step 8: Configure PC3
- set IP configuration on PC3
- steps:
  * set the IP address to 192.12.20.3
  * Set the default gateway to 192.12.20.1

Step 9: Create VLAN 20 on the Router
- Set up VLAN 20 in the router's VLAN database
- steps:
  * Click on the router go to the switching menu & select VLAN database
  * Set VLAN number to 20 & VLAN name to LAN-1
  * Click Add to create the VLAN

Step 10: Configure a subinterface to VLAN 20 on the Router

- Enable subinterface routing on the router for VLAN 20
- Commands

```
Router # Config t
Router (config) # int f0/0.1
Router (config-subif) # encapsulation dot1q 20
Router (config-subif) # ip address 192.12.20.1 255.255.255.0
Router (config-subif) # Exit
Router (config) # Exit
```

- Explanation
  - Int F0/0.1: Creates a subinterface for VLAN-20 on FastEthernet 0/0
  - Encapsulation: dot1q 20: Tags the subinterface for VLAN 20
  - Ip address: 192.12.20.1 255.255.255.0: Assigns an IP to the subinterface

Step 11: Assign VLAN20 to switch Port FastEthernet 0/3

- Go to the switch's configuration, set FastEthernet 0/3 to VLAN 20
- Steps
  * click on the switch go to the config tab
  * select FastEthernet 0/3, set VLAN to 20 & Click Add

Step 12: Assign VLAN 20 to switchport fastEthernet 0/4

- Repeat step 11 for fast Ethernet 0/4

Step 13: Test Connectivity with ping

- Verify that devices on the same VLAN (VLAN 20) can communicate (PC2 & PC3)

- Example from PC2, ping 192.12.20.3 (PC3 IP)