

Deepraj Bhosale - 181105016

Experiment No 5

Aim

Study of basic network commands and Network configuration commands.

Apparatus (Software)

Command Prompt and Packet Tracer.

Procedure

In this experiment - students have to understand basic networking commands eg ping, tracer etc. All commands related to network configuration which includes how to switch to privileged mode and normal mode and how to configure router interface and how to save this configuration to flash memory or permanent memory.

This command includes:

- Configuring the router commands
- General Commands to configure the network
- Privileged Mode commands of router
- Router process and statistics
- IP commands

ping:

ping(8) sends an ICMP ECHO REQUEST packet to the specified host. If the host responds, you get an ICMP packet back. Sound strange? Well, you can “ping” an IP address to see if a machine is alive. If there is no response, you know something is wrong.



```
Physical  Config  Desktop  Programming  Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.3

Pinging 192.168.1.3 with 32 bytes of data:

Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128
Reply from 192.168.1.3: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

tracert:

Tracert is a command which can show you the path a packet of information takes from your computer to one you specify. It will list all the routers it passes through until it reaches its destination, or fails to and is discarded. In addition to this, it will tell you how long each 'hop' from router to router takes.

```
C:\>tracert 192.168.1.3

Tracing route to 192.168.1.3 over a maximum of 30 hops:

  0  0 ms  0 ms  0 ms  192.168.1.3

Trace complete.

C:\>
```

nslookup:

Displays information from Domain Name System (DNS) name servers. NOTE :If you write the command as above it shows as default your pc's server name firstly.

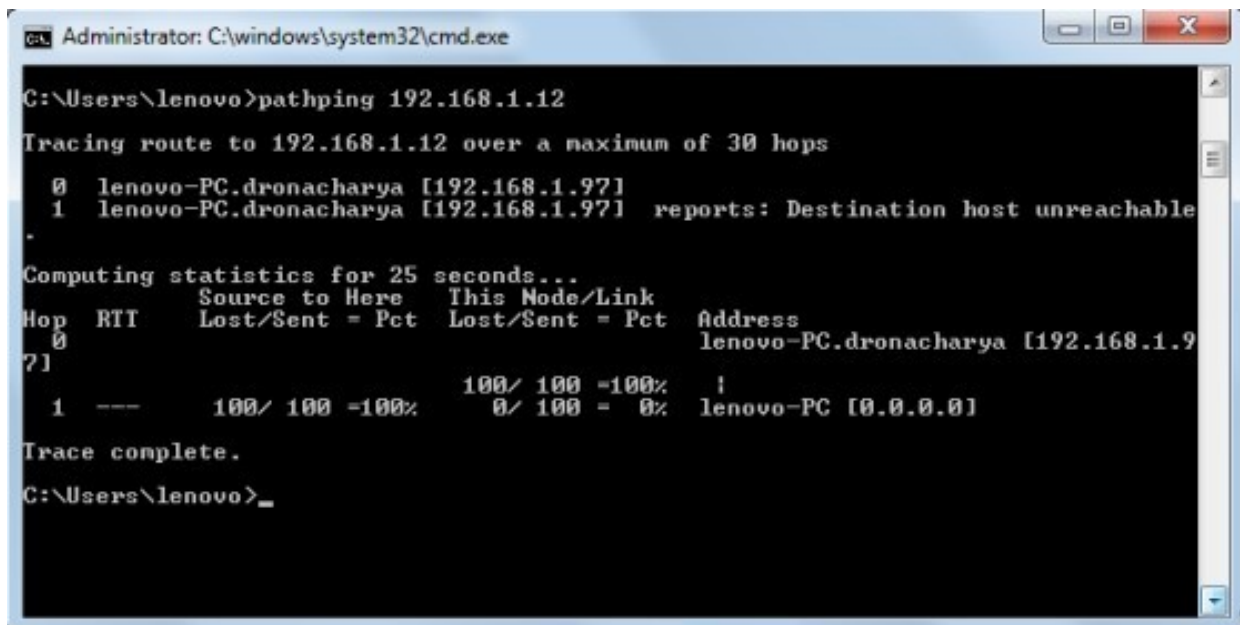
```
C:\>nslookup

Server: [255.255.255.255]
Address: 255.255.255.255

>
```

pathping:

A better version of tracert that gives you statistics about packet lost and latency.



```
Administrator: C:\windows\system32\cmd.exe

C:\Users\lenovo>pathping 192.168.1.12

Tracing route to 192.168.1.12 over a maximum of 30 hops

  0  lenovo-PC.dronacharya [192.168.1.97]
  1  lenovo-PC.dronacharya [192.168.1.97] reports: Destination host unreachable
.

Computing statistics for 25 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0  ---      Lost/Sent = Pct  Lost/Sent = Pct  lenovo-PC.dronacharya [192.168.1.97]
 1  ---      100/ 100 =100%   0/ 100 = 0%     lenovo-PC [0.0.0.0]

Trace complete.

C:\Users\lenovo>
```

Getting Help

In any command mode, you can get a list of available commands by entering a question mark (?).

Router>?

To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?).

Router#co?

configure connect copy To list keywords or arguments, enter a question mark in place of a keyword or argument. Include a space before the question mark.

Router#configure ?

memory Configure from NV memory network Configure from a TFTP network host terminal
Configure from the terminal You can also abbreviate commands and keywords by entering just enough characters to make the command unique from other commands. For example, you can abbreviate the show command to sh.

Configuration Files

Any time you make changes to the router configuration, you must save the changes to memory because if you do not they will be lost if there is a system reload or power outage. There are two types of configuration files: the running (current operating) configuration and the startup configuration. Use the following privileged mode commands to work with configuration files

- configure terminal – modify the running configuration manually from the terminal.
- show running-config – display the running configuration.
- show startup-config – display the startup configuration.
- copy running-config startup-config – copy the running configuration to the startup configuration.
- copy startup-config running-config – copy the startup configuration to the running configuration.
- erase startup-config – erase the startup-configuration in NVRAM.
- copy tftp running-config – load a configuration file stored on a Trivial File Transfer Protocol (TFTP) server into the running configuration.
- copy running-config tftp – store the running configuration on a TFTP server.

IP Address Configuration

Take the following steps to configure the IP address of an interface.

Step 1:

Enter privileged EXEC mode:

Router>enable password

Step 2:

Enter the configure terminal command to enter global configuration mode.

Router#config terminal

Step 3:

Enter the interface type slot/port (for Cisco 7000 series) or interface type port (for Cisco 2500 series) to enter the interface configuration mode. Example:

Router (config)#interface ethernet 0/1

Step 4:

Enter the IP address and subnet mask of the interface using the ip address ipaddress sub- netmask command. Example:

Router (config-if)#ip address 192.168.10.1 255.255.255.0

Step 5:

Exit the configuration mode by pressing Ctrl

Router(config-if)#[Ctrl-Z]

Conclusion

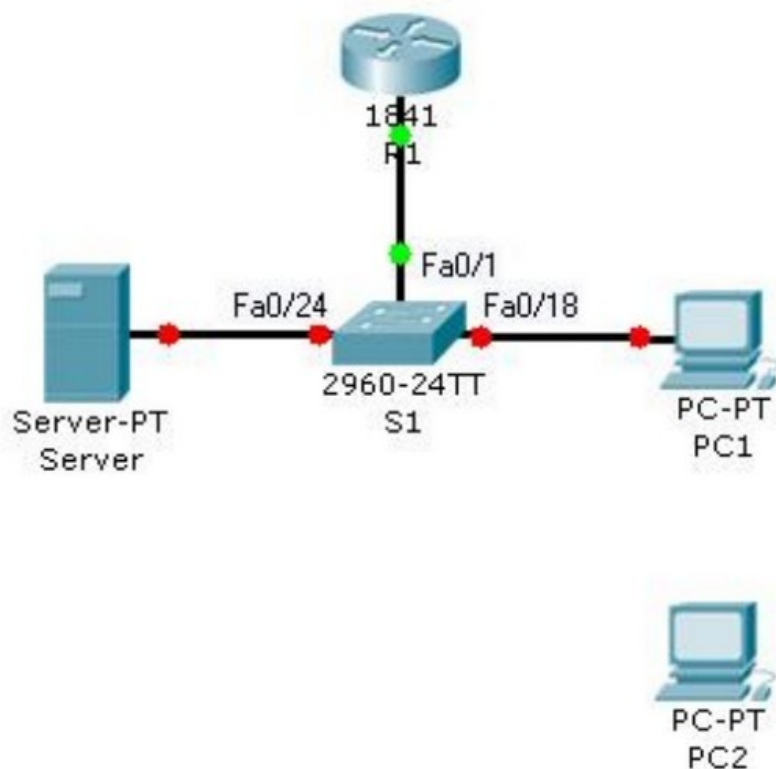
Studied the basic network commands and network configuration commands.

Experiment No 8

Aim

Configure and troubleshoot a switched network.

Topology Diagram



Objectives

- Establish console connection to the switch.
- Configure the host name and VLAN1.
- Use the help feature to configure the clock.
- Configure passwords and console/Telnet access.
- Configure login banners.
- Configure the router.
- Solve duplex and speed mismatch problems.
- Configure port security.
- Secure unused ports.
- Manage the switch configuration file.

Background / Preparation

In this Packet Tracer Skills Integration Challenge activity, you will configure basic switch management, including general maintenance commands, passwords, and port security. This activity provides you an opportunity to review previously acquired skills.

Addressing Table

Device	Interface	IP Address	Subnet Mask
R1	Fa0/0	172.17.99.1	255.255.255.0
S1	Fa0/1	172.17.99.11	255.255.255.0
PC1	NIC	172.17.99.21	255.255.255.0
PC2	NIC	172.17.99.22	255.255.255.0
Server	NIC	172.17.99.31	255.255.255.0

Step 1: Establish a console connection to a switch

For this activity, direct access to the S1 Config and CLI tabs is disabled. You must establish a console session through PC1.

1. Connect a console cable from PC1 to S1.
2. From PC1, open a terminal window and use the default terminal configuration. You should now have access to the CLI for S1.
3. Check results.

Your completion percentage should be 8%. If not, click Check Results to see which required components are not yet completed.

Step 2: Configure the host name and VLAN 1

1. Configure the switch host name as S1.
2. Configure port Fa0/1. Set the mode on Fast Ethernet 0/1 to access mode.
 - (a) S1(config)#interface fastethernet 0/1
 - (b) S1(config-if)#switchport mode access
3. Configure IP connectivity on S1 using VLAN 1.
 - (a) S1(config)#interface vlan 1
 - (b) S1(config-if)#ip address 172.17.99.11 255.255.255.0
 - (c) S1(config-if)#no shutdown
4. Configure the default gateway for S1 and then test connectivity. S1 should be able to ping R1.
5. Check results.

Your completion percentage should be 31%. If not, click Check Results to see which required components are not yet completed. Also, make sure that interface VLAN 1 is active.

Step 3: Configure the current time using Help

1. Configure the clock to the current time. At the privileged EXEC prompt, enter clock
?.
2. Use Help to discover the steps required to set the current time.
3. Use the show clock command to verify that the clock is now set to the current time. Packet Tracer may not correctly simulate the time you entered.

Packet Tracer does not grade this command, so the completion percentage does not change.

Step 4: Configure passwords

1. Use the encrypted form of the privileged EXEC mode password and set the password to class.
2. Configure the passwords for console and Telnet. Set both the console and vty password to cisco and require users to log in.
3. View the current configuration on S1. Notice that the line passwords are shown in clear text. Enter the command to encrypt these passwords.
4. Check results.

Your completion percentage should be 42%. If not, click Check Results to see which required components are not yet completed.

Step 5: Configure the login banner

If you do not enter the banner text exactly as specified, Packet Tracer does not grade your command correctly. These commands are case-sensitive. Also make sure that you do not include any spaces before or after the text.

1. Configure the message-of-the-day banner on S1 to display as Authorized Access Only. (Do not include the period.)
2. Check results.

Your completion percentage should be 46%. If not, click Check Results to see which required components are not yet completed.

Step 6: Configure the router

Routers and switches share many of the same commands. Configure the router with the same basic commands you used on S1.

1. Access the CLI for R1 by clicking the device.
2. Do the following on R1:
 - Configure the hostname of the router as R1.
 - Configure the encrypted form of the privileged EXEC mode password and set the password to class.
 - Set the console and vty password to cisco and require users to log in.
 - Encrypt the console and vty passwords.
 - Configure the message-of-the-day as Authorized Access Only. (Do not include the period.)
3. Check results

Your completion percentage should be 65%. If not, click Check Results to see which required components are not yet completed.

Step 7: Solve a mismatch between duplex and speed

1. PC1 and Server currently do not have access through S1 because the duplex and speed are mismatched. Enter commands on S1 to solve this problem.
2. Verify connectivity.
3. Both PC1 and Server should now be able to ping S1, R1, and each other.
4. Check results.

Your completion percentage should be 73%. If not, click Check Results to see which required components are not yet completed.

Step 8: Configure port security

1. Use the following policy to establish port security on the port used by PC1:

- Enable port security
- Allow only one MAC address
- Configure the first learned MAC address to "stick" to the configuration

Note: Only enabling port security is graded by Packet Tracer and counted toward the completion percentage. However, all the port security tasks listed above are required to complete this activity successfully.

2. Verify that port security is enabled for Fa0/18. Your output should look like the following output. Notice that S1 has not yet learned a MAC address for this interface. What command generated this output?

S1#

Port Security : Enabled Port Status : Secure-up Violation Mode : Shutdown Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1

Total MAC Addresses : 0 Configured MAC Addresses : 0 Sticky MAC Addresses : 0

Last Source Address:Vlan : 0000.0000.0000:0 Security Violation Count : 0

3. Force S1 to learn the MAC address for PC1. Send a ping from PC1 to S1. Then verify that S1 added the MAC address for PC1 to the running configuration.

!

interface FastEthernet0/18

<output omitted>

switchport port-security mac-address sticky 0060.3EE6.1659

<output omitted>

!

4. Test port security. Remove the FastEthernet connection between S1 and PC1. Connect PC2 to Fa0/18. Wait for the link lights to turn green. If necessary, send a ping from PC2 to S1 to cause the port to shut down. Port security should show the following results: (the Last Source Address may be different)

Port Security : Enabled

Port Status : Secure-shutdown Violation Mode : Shutdown Aging Time : 0 mins

Aging Type : Absolute

SecureStatic Address Aging : Disabled Maximum MAC Addresses : 1

Total MAC Addresses : 1 Configured MAC Addresses : 1 Sticky MAC Addresses : 0

Last Source Address:Vlan : 00D0.BAD6.5193:99 Security Violation Count : 1

5. Viewing the Fa0/18 interface shows that line protocol is down (err-disabled), which also indicates a security violation.

S1#show interface fa0/18

FastEthernet0/18 is down, line protocol is down (err-disabled)

<output omitted>

6. Reconnect PC1 and re-enable the port. To re-enable the port, disconnect PC2 from Fa0/18 and reconnect PC1. Interface Fa0/18 must be manually reenabled with the no shutdown command before returning to the active state.

7. Check results.

Your completion percentage should be 77%. If not, click Check Results to see which required components are not yet completed.

Step 9: Secure unused ports

1. Disable all ports that are currently not used on S1. Packet Tracer grades the status of the following ports: Fa0/2, Fa0/3, Fa0/4, Gig 1/1, and Gig 1/2.
2. Check results.

Your completion percentage should be 96%. If not, click Check Results to see which required components are not yet completed.

Step 10: Manage the switch configuration file

1. Save the current configuration for S1 and R1 to NVRAM.
2. Back up the startup configuration file on S1 and R1 by uploading them to Server. Verify that Server has the R1-config and S1-config files.
3. Check results.

Your completion percentage should be 100%. If not, click Check Results to see which required components are not yet completed.

Conclusion

Configured and troubleshooted a switched network.