Basics configuration of router and switch

Routers can be configured using either Graphical User Interface (GUI) or Command Line Interface (CLI). Most of the router manufacturers provide SDM (Security Device Manager) software along with the router to enable users configure the router graphically.

SDM Express uses eight configuration steps to assist in creating a basic router configuration: Overview Cisco, Basic Configuration, LAN IP Address, DHCP, Internet (WAN), Firewall, Security Settings and Summary.

The SDM Express windows provide step-by-step guidance to create the initial configuration of the router. After the initial configuration is completed, the router is available on the LAN. The router can also have a WAN connection, a firewall and up to 30 security enhancements configured. CLI is used throughout this course.

2.1.1 Cisco IOS Modes of Operation

The Cisco IOS software provides access to several different command modes. Each command mode provides a different group of related commands. For security purposes, the Cisco IOS software provides two levels of access to commands: user and privileged. The unprivileged user mode is called user EXEC mode. The privileged mode is called privileged EXEC mode and requires a password. The commands available in user EXEC mode are a subset of the commands available in privileged EXEC mode.

Note:

- ✓ ***User EXEC*** mode Limited to basic monitoring commands.
- ✓ ***Privileged EXEC*** mode Provides access to all other router commands.
- ✓ ***Global configuration mode*** Commands that affect the entire system.
- ✓ ***Specific configuration*** modes Commands that affect interfaces/processes only.

The following table describes some of the most commonly used modes, how to enter the modes, and the resulting prompts. The prompt helps you identify which mode you are in and, therefore, which commands are available to you.

Mode of operation	**Usage**	**How to Enter the Mode?**	**Prompt**
User EXEC	Change terminal settings on a temporary basis, perform basic tests, and list system information.	First level accessed.	Router>
Privileged EXEC	System administration, set operating parameters.	Router>**enable**	Router#

Global Config	Modify configuration that affect the system as a whole.	Router#**configure terminal**	Router(config)#
Interface Config	Modify the operation of an interface.	Router(config)#**interface fastethernet 0/0**	Router(configif)#

<u>User EXEC Mode:</u>

When you are connected to the router, you are started in user EXEC mode. The user EXEC commands are a subset of the privileged EXEC commands.

<u>Privileged EXEC Mode:</u>

Privileged commands include the following:

- Configure – Changes the software configuration.
- Debug – Display process and hardware event messages.
- Setup – Enter configuration information at the prompts.

Enter the command disable to exit from the privileged EXEC mode and return to user EXEC mode.

Configuration Mode

Configuration mode has a set of sub modes that you use for modifying interface settings, routing protocol settings, line settings, and so forth. Use caution with configuration mode because all changes you enter take effect immediately. To enter configuration mode, enter the command **configure terminal** and exit by pressing **Ctrl-Z**.

2.1.2 Basic Router/Switch Configuration

Use the following topology for the whole basic router and switch configuration.

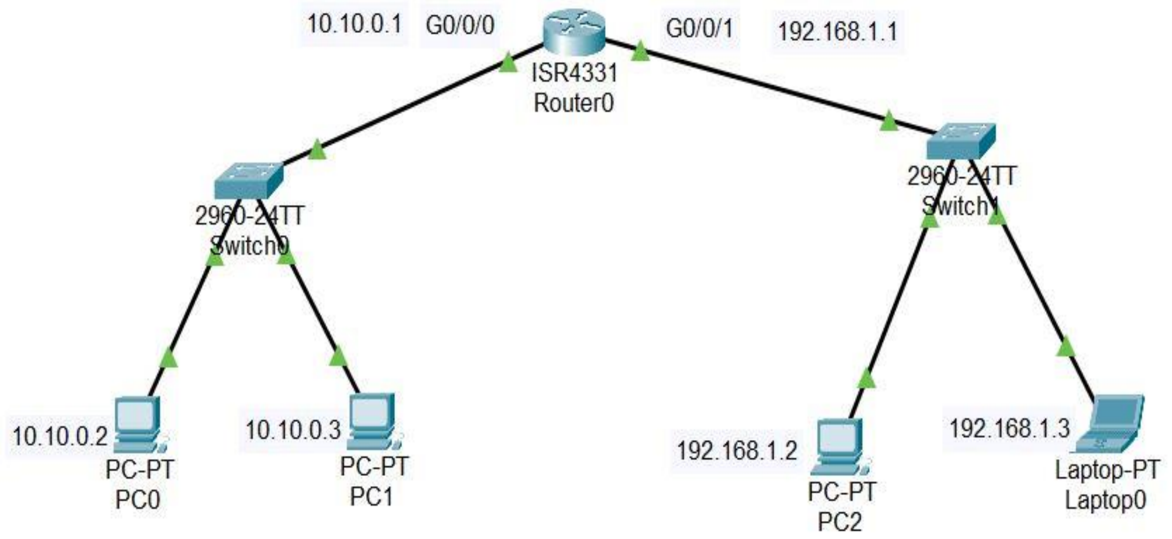


Fig 2.3 network topology

Lab section

1. 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**.

2. Disabling DNS lookup

DNS lookup can sometime take your time looking for the name translations even if you did not configure any host name but we can disable the DNS lookup from your cisco device.

Example:

```
Router>enable
Router#configure terminal
Router(config)#no ip domain-lookup
Router(config)#exit
```

3. Rename the Router

To specify or modify the host name for the router, global configuration command HOSTNAME is used. Hostname is case sensitive. The host name is used in prompts and default configuration filenames. For instance, the first router R1 can be renamed as MTUR1 as follow.

```
Router (config) # hostname MTUR1

MTUR1 (config) #
```

The factory-assigned default host name is *router but we can change by the above configuration command.*

4. Setting the System Clock

The system clock runs from the moment the system starts up and keeps track of the current date and time based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). The system clock can be set from a number of sources, and in turn can be used to distribute the current time through various mechanisms to other systems. To manually set the system clock, use one of the formats of the clock set EXEC command.

Clock set *hh:mm:ss day month yyyy*

clock set *hh:mm:ss month day yyyy*

In the following example, the system clock is manually set to 1:32 p.m. on May 12, 2001:

```
MTUR1 # clock set 13:32:00 12 DEC 2015
```

Show System Time

To display the system clock, use the **show clock** EXEC command. If time has not been set by the clock set command, then this command will show the time elapsed since router is up.

```
MTUR1 # show clock
```

5. Setting the Banner

To specify a message-of-the-day (MOTD) banner, use the **banner motd** global configuration command. The ***no*** form of this command deletes the MOTD banner. When someone connects to the router, the MOTD banner appears before the login prompt.

```
MTUR1 (config)# banner motd # message #
```

Example. MTUR1 (config)# banner motd # well come to It fourth year practical class #

If we want to delete or remove the message, use the following configuration

```
MTUR1 (config)# no banner motd
```

Here (#) sign is used as delaminating character. You can use any character.

6. Setting Passwords

To specify a password on a line, use the **password** line configuration command. Use the **no** form of this command to remove the password. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters.

a. Console Password

Console password is needed when logging into router at user EXEC mode from console.

```
MTUR1 (config)# line console 0
MTUR1 (config-line)# password console Password
MTUR1 (config-line)#login
```

b. Vty lines password

Virtual terminal lines (vty) are used to allow remote access to the router (by telneting through its interfaces). The router has five virtual terminal lines by default.

```
MTUR1 (config)# line vty 0 4
MTUR1 (config-line)# password vtyPassword
MTUR1 (config-line)#login
```

c. Privileged Access Password

To set a local password to control access to various privilege levels, use the **enable password** global configuration command. Use the **no** form of this command to remove the password requirement.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Must not have a number as the first character.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.

```
MTUR1 (config)# enable password WeakPrivilegePassword
```

Setting Secret (Encrypted) Password

To set an encrypted local password to control access to various privilege levels, use the **enable secret** global configuration command. Use the **no** form of this command to remove the password requirement.

```
MTUR1 (config)# enable secret StrongPrivilegePassword
```

7. Bring up an interface

On cisco routers all interfaces by default are in shut down mode means administratively down

You can check the status of these interfaces by using the command *show ip interface brief* at the user privilege mode on cisco routers. To bring up the status of an interface we use the *no shutdown* command.

Example:

```
MTUR1 >enable
MTUR1 #configure terminal
MTUR1 (config)#interface serial2/0
MTUR1 (config-if)#no shutdown
MTUR1 (config-if)#exit
MTUR1 (config)#interface fastethernet0/0
MTUR1 (config-if)#no shutdown
MTUR1 (config-if)#exit
```

8. Clock rate on serial interfaces

Serial interface with DCE ends of a router need to be configured with the clock rate and following example describe the commands used to set the clock rate on serial interfaces.

Example:

```
MTUR1 >enable
MTUR1 #configure terminal
MTUR1 (config)#interface serial2/0
MTUR1 (config-if)#no shutdown
MTUR1 (config-if)#clock  rate 4800
MTUR1 (config-if)#exit
```

The clock rate can be set from some specific values.

9. Setting the Description for an Interface

To add a description to an interface configuration, use the **description** interface configuration command. Use the **no** form of this command to remove the description.

The **description** command is meant solely as a comment to be put in the configuration to help you remember what certain interfaces are used for.

The following example shows how to add a description for a T1 interface:

```
Router(config)# interface serial 2/0
MTUR1 (config-if)# description T1 line to MTUR1 - 128 Kb/s
```

The description "T1 line to MTUR1- 128 Kb/s" appears in the output of the following EXEC commands: **show startup-config**, **show interfaces**, and **show running-config**

MTUR1 # **show startup-config** MTUR1 # **show interfaces** MTUR1 # **show running-config**

10. IP addressing

Every interface need to be configured with an IP address on the router to communicate over the network. Consider an example in which we will assign the ip address 192.168.10.1 with subnet mask 255.255.255.0 on FastEthernet interface of router and ip address 192.168.20.1 with subnet mask 255.255.255.0 on the serial interface of router.

```
MTUR1 >enable
MTUR1 #configer terminal
MTUR1 (config)#interface fastethernet0/0
MTUR1 (config-if)#ip address 10.10.10.1 255.255.255.0
MTUR1 (config-if)#no shutdown
MTUR1 (config-if)#exit
MTUR1 (config)#interface serial2/0
MTUR1 (config-if)#ip add 192.168.20.1 255.255.255.252
MTUR1 (config-if)#no shutdown
MTUR1 (config-if)#exit
```

11. DHCP (Dynamic Host Configuration Protocol)

In IP environment, before a computer can communicate to another one, they need to have their own IP addresses. There are two ways of configuring an IP address on a device: + Statically assign an IP address. This means we manually type an IP address for computers + Use a protocol so that the computer can obtain its IP address automatically (dynamically) from a DHCP server.

How DHCP works

1. When a client boots up for the first time (or try to join a new network), it needs to obtain an IP address to communicate. So it first transmits a **DHCP DISCOVER** message on its local subnet. Because the client has no way of knowing the subnet to which it belongs, the DHCP DISCOVER is an all-subnets broadcast (destination IP address of 255.255.255.255, which is a layer 3 broadcast addresses) and a destination MAC address of FF-FF-FF-FF-FF-FF (which is a layer 2 broadcast address). The client does not have a configured IP address, so the source IP address of 0.0.0.0 is used. The purpose of DHCP DISCOVER message is to try to find out a DHCP Server (a server that can assign IP addresses).

2. After receiving the discover message, the DHCP Server will dynamically pick up an unassigned IP address from its IP pool and broadcast a **DHCP OFFER** message to the client. DHCP OFFER message could contain other information such as subnet mask, default gateway, IP address lease time, and domain name server (DNS).

Note: In fact, the DHCP OFFER is a layer 3 broadcast message (the IP destination is 255.255.255.255) but a layer 2 unicast message (the MAC destination is the MAC of the DHCP Client, not FF-FF-FF-FF-FF-FF). So in some books they may say it is a broadcast or unicast message.

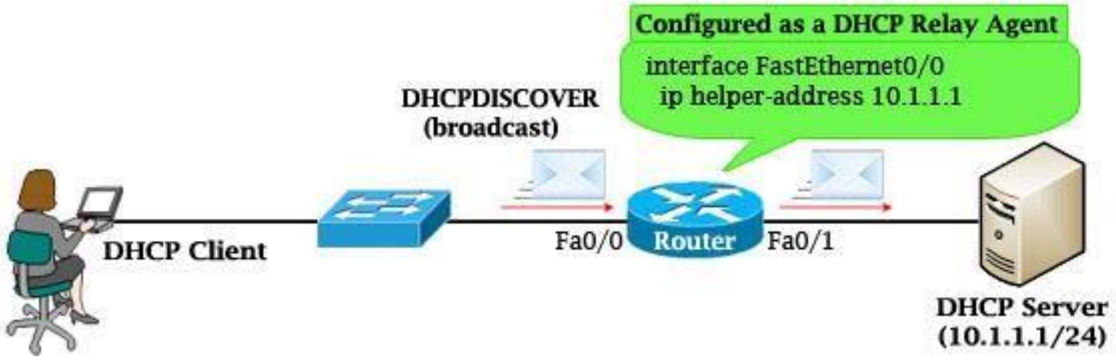
3. If the client accepts the offer, it then broadcasts a **DHCP REQUEST** message saying it will take this IP address. It is called request message because the client might deny the offer by requesting another IP address. Notice that DHCPREQUEST message is still a broadcast message because the DHCP client has still not received an acknowledged IP. Also a DHCP Client can receive DHCPOFFER messages from other DHCP Servers so sending broadcast DHCPREQUEST message is also a way to inform other offers have been rejected.

4. When the DHCP Server receives the DHCPREQUEST message from the client, the DHCP Server accepts the request by sending the client a unicast **DHCP ACKNOWLEDGEMENT** message (DHCPACK).

In conclusion there are four messages sent between the DHCP Client and DHCP Server: DHCP **D**ISCOVER, DHCP **O**FFER, DHCP **R**EQUEST and DHCP **A**CKNOWLEDGEMENT. This process is often abbreviated as **DORA** (for Discover, Offer, Request, and Acknowledgement).

After receiving DHCP ACKNOWLEDGEMENT, the IP address is leased to the DHCP Client. A client will usually keep the same address by periodically contacting the DHCP server to renew the lease before the lease expires.

If the DHCP Server is not on the same subnet with the DHCP Client, we need to configure the router on the DHCP client side to act as a DHCP Relay Agent so that it can forward DHCP messages between the DHCP Client & DHCP Server. To make a router a DHCP Relay Agent, simply put the “ip helper-address <*IP-address-of-DHCP-Server*>” command under the interface that receives the DHCP messages from the DHCP Client.


Configured as a DHCP Relay Agent
interface FastEthernet0/0
ip helper-address 10.1.1.1
DHCPDISCOVER (broadcast)
DHCP Client
Fa0/0
Router
Fa0/1
DHCP Server (10.1.1.1/24)

As we know, router does not forward broadcast packets (it drops them instead) so DHCP messages like DHCPDISCOVER message will be dropped. But with the “ip helper-address …” command, the router will accept that broadcast message and cover it into a unicast packet and forward it to the DHCP Server. The destination IP address of the unicast packet is taken from the “ip helper address …” command.

When a DHCP address conflict occurs

During the IP assignment process, the DHCP Server uses ping to test the availability of an IP before issuing it to the client. If no one replies, then the DHCP Server believes that IP has not been allocated and it can safely assign that IP to a client. If someone answers the ping, the DHCP Server records a conflict, the address is then removed from the DHCP pool and it will not be assigned to a client until the administrator resolves the conflict manually.

Configure a DHCP Server on Cisco router

Instead of using a separate computer/server as a DHCP Server, we can save the cost and configure a Cisco router (even a Layer 3 Cisco switch) to work as a DHCP Server. The following example configuration will complete this task:

Configuration	**Description**
Router(config)#ip dhcp pool CLIENTS	Create a DHCP Pool named CLIENTS
Router(dhcp-config)#network 10.1.1.0 /24	Specifies the subnet and mask of the DHCP address pool
Router(dhcp-config)#default-router 10.1.1.1	Set the default gateway of the DHCP Clients
Router(dhcp-config)#dns-server 10.1.1.1	Configure a Domain Name Server (DNS)
Router(dhcp-config)#domain-name mtu.com	Configure a domain-name

Router(dhcp-config)#lease 0 12	Duration of the lease (the time during which a client computer can use an assigned IP address). The syntax is "**lease**{days[hours] [minutes] | infinite}". In this case the lease is 12 hours. The default is a one-day lease. Before the lease expires, the client typically needs to renew its address lease assignment with the server
Router(dhcp-config)#exit	
Router(config)# ip dhcp excluded-address 10.1.1.1 10.1.1.10	The IP range that a DHCP Server should not assign to DHCP Clients. Notice this command is configured under global configuration mode

12. Handling 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.

Viewing, saving and erasing configurations

After you are done with your router's configurations you can view save and erase the configurations of your router. Example:

Viewing

```
MTUR1>enable
MTUR1#show running-config
```

Saving

```
MTUR1>enable
MTUR1#copy running-config starup-config or MTUR1#write
```

Erasing startup configurations MTUR1>enable

```
MTUR1#erase startup-config
```

13. no and **do** commands

Almost every configuration command also has a no form. In general, use the no form to disable a feature or function. Use the command without the keyword **no** to re-enable a disabled feature or to enable a feature that is disabled by default. For example, IP routing is enabled by default. To disable IP routing, enter the **no ip routing** command and enter **ip routing** to re-enable it. For instance, to remove previously configured IP address in MTUR1 router fast Ethernet 0/0 you can type the following.

```
MTUR1 (config)#int fa0/0
MTUR1 (config-if)#no ip address
```

14. Disabling Logging synchronous messages

When configuring routers and switches sometime some interrupting messages may disturb you.

To stop this kind of messages, use the following command

```
MTUR1 (config)#line console 0
MTUR1 (config-line)#logging synchronous
```

15. Remote Device Management (telnet & SSH)

SSH i.e. Secure Shell and Telnet are the network protocols that serves the same purpose that is to provide remote access to the system in order to establish some sort of communication between the systems for ex. Communication between the Server and the Client. However, the main difference between these protocols is the security of the data being transferred between the systems.

Following are the points that differentiates SSH and Telnet.

SSH (Secure Shell):-

- ✓ SSH **encrypts** the data/packets being transferred between the systems so it cannot be **Decoded by the Hackers**. For ex. the user-name, password etc.
- ✓ In **Public network** mostly SSH is used for remote connection due to it's security mechanism.
- ✓ SSH uses **authentication** which ensures that the source of the data is still the same system and not another. Without the authentication, any other person can intercept and perform some undesired tasks.
- ✓ SSH uses public and private keys, to identify hosts and users (authentication).
- ✓ By default, SSH runs on port **22**.

Telnet: -

- ✓ The data transferred between the systems is in **Plain text** (ASCII form) and not in encrypted format which is the major security concern. So the data can be easily read by anybody in the network and can **hack** the system.
- ✓ Telnet is mostly used in **Private network** as it's highly insecure to use in Public network.

✓ Telnet does not use Authentication which is again a security issue.
✓ Telnet runs on port **23**.

Configuring Telnet:

Virtual terminal lines are used to allow remote access to a router. A virtual terminal line is not associated with either the auxiliary or console port; instead, it is a "virtual port" on the router. The router has five virtual terminal lines, by default. You will configure the five vty lines (vty 0 through 4) for Telnet access and set a password of **mtuvty123** on these lines. In addition, you want to ensure that, after 15 minutes of inactivity on the vty lines, the connection times out. To configure the vty lines, you will do the following from global configuration mode:

Step 1. Enter line configuration mode.

Step 2. Enable login on the vty lines.

Step 3. Set a password for Telnet access.

Step 4. Set the **exec-timeout** interval.

```
Router>enable
Router#configure terminal
Router(config)#banner motd #Welcome to MTU Router#
Router(config)#enable password mtu123
Router(config)#interface fastethernet0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#line vty 0 4
Router(config-line)#password mtuvty123
Router(config-line)#login
Router(config-line)#logging synchronous
Router(config-line)#exec-timeout 30
Router(config-line)#motd-banner
```

In order to remotely control a router, we must set a password so “**enable password mtu123”** sets a password to the router.

The “**line vty**” command enable the telnet and the “**0 4″** is just to let more lines or sessions simultaneously to the router. If you need a single session, you must type “**line vty 0**“. The “**password**” command set the “**mtuvty123**” as password for telnet. You can set your own password.

The “**login**” command authenticate and ask you the password of telnet. If you type “**no login**” command, the telnet never authenticate for password, which is not a good practice in real network environment.

The “**logging synchronous**” command stops any message output from splitting your typing. The “**exec-timeout”** command just sets the time-out limit on the line from the default to “**30″** minutes.

The **motd-banner** forces a banner message to appear when logging in. OK, the Telnet services enabled successfully.

Testing Telnet Connectivity

Now from a client PC test the telnet connectivity and to insure that it works fine or not yet. If it is not work, try to troubleshoot telnet errors.

Let's test telnet from the admin PC. Type **telnet 192.168.0.1** and press enter, then enter the telnet password. Next type **enable** command and press enter, then type the router password.

```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.0.1
Trying 192.168.0.1 …Open Welcome to MTU
Router User Access Verification Password:
Router>enable  Password:
Router#
```

Now you are remotely connected to router Router and you can execute all router commands through telnet command line interface. If you need to disconnect the logged in remote connection type "**logout"** and press enter**.** If you need more information about Telnet commands and options, from the **config-line** mode type "? ", the question mark will display all telnet commands.

Configuring SSH:

1. Open the router Router console line and create domain and user name.

```
Router(config)#ip domain-name mtu.com
Router(config)#username mtu Password mtussh123 Router(config)#
```

Then "**ip domain-name**" command create a domain and named **mtu.com**. The "**username mtu Password mtussh123**" command just create a user name "**mtu**" with "**mtussh123**" password.

2. If you don't, just follow and generate the encryption keys for securing the ssh session.

```
Router(config)#crypto key generate rsa
The name for the keys will be: Router.mtu.com
Choose the size of the key modulus in the range of 360 to 2048 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] Router(config)#
```

Type "**crypto key generate rsa**" command and press enter, when ask you "**How many bits in the modulus [512]:**" just type "**1024″** and press enter. The system will generate**1024** bits keys to secure session lines. You can choose modulus in the range of 360 to 2048.

3. Now enable SSH version 2, set time out duration and login attempt time on the router. Remember this message if you going to use ssh version 2 "**Please create RSA keys (of at least 768 bits size) to enable SSH v2.**"

```
Router(config)#ip ssh version 2
Router(config)#ip ssh time-out 50
Router(config)#ip ssh authentication-retries 4
```

4. Enable vty lines and configure access protocols.

```
Router(config)#line vty 0
Router(config-line)#transport input ssh
Router(config-line)#password mtu123
Router(config-line)#login
Router(config-line)#motd-banner
Router(config-line)#exit
Router(config)#
```

The configuration is the same as telnet, just the **transport input ssh** command change the line to **Secure Shell.** Configuration has completed, next test ssh from a client PC.

Testing SSH Connectivity

From a client PC, open the command line and type "**ssh -l mtu 192.168.0.1**" then press enter.

```
Packet Tracer PC Command Line 1.0
PC>ssh -l mtu 192.168.0.1
Open Password:
Router>enable
Password:
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z. Router(config)#
```

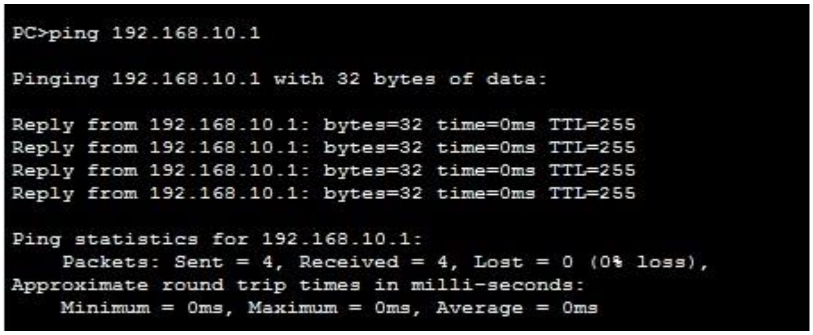
Connection established successfully and the connection is secured with Secure Shell.

2.2 <u>Troubleshooting</u>: ***<u>TCP/IP Utilities</u>***

TCP/IP also provides a number of command-line utilities that can be useful when troubleshooting networks. You can use any of these utilities at the DOS command prompt in Windows.

1. **Ping**

To test if your network connection is complete between two computers, you can use the *Packet Internet Groper*, better known as *ping*. The ping utility works by sending a message to a remote computer. If the remote computer receives the message, it responds with a reply message (see Figure 2.4). The reply consists of the remote workstation's IP address, the number of bytes in the message, how long it took to reply - given in milliseconds (ms) - and the time-to-live (TTL) in seconds. If you receive back the message "***Request timed out,"*** this means that the remote workstation did not respond before the TTL time expired. This might be the result of heavy network traffic or it might indicate a physical disconnection in the path to the remote workstation.



```
PC>ping 192.168.10.1

Pinging 192.168.10.1 with 32 bytes of data:

Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255
Reply from 192.168.10.1: bytes=32 time=0ms TTL=255

Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

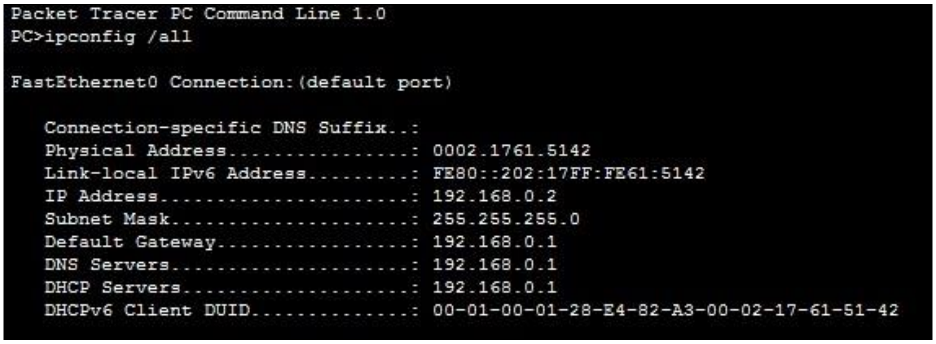
Fig 2.5 ping

2. Tracert

Another utility that documents network performance is called *tracert*. While the *ping* utility merely lets us know that the connection from A to B is complete, tracert informs us of the route and number of hops the packet of data took to arrive at its destination.

3. Ipconfig /all

Another useful software troubleshooting tool is *ipconfig*. This diagnostic command displays all current TCP/IP network-configuration values. This command is useful on systems running DHCP, allowing users to determine which TCP/IP configuration values have been configured by DHCP. An example of using the ipconfig utility is shown in Figure 2.6. The output lists the current IP address of the computer, the subnet mask, and the default gateway. The subnet mask indicates which class of network the computer is a part of. Because the first three numbers in the subnet mask are 255 this means that the computer is on a class C network (i.e. the first 24 bits of the IP address are fixed). If this computer needs to send a packet of data to a computer outside of this subnet, it must first send it to the *default gateway*. The default gateway is a computer or router on the subnet that is responsible for forwarding packets to addresses outside the subnet.



```
Packet Tracer PC Command Line 1.0
PC>ipconfig /all

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Physical Address................: 0002.1761.5142
   Link-local IPv6 Address.........: FE80::202:17FF:FE61:5142
   IP Address......................: 192.168.0.2
   Subnet Mask.....................: 255.255.255.0
   Default Gateway.................: 192.168.0.1
   DNS Servers.....................: 192.168.0.1
   DHCP Servers....................: 192.168.0.1
   DHCPv6 Client DUID..............: 00-01-00-01-28-E4-82-A3-00-02-17-61-51-42
```

Fig 2.6. ipconfig /all

4.Nslookup

Nslookup is a utility that can be used to manually query the DNS database. It can be a useful troubleshooting tool if the DNS server is not working correctly.

5. Netstat

The *netstat* command can be used to display the currently active TCP connections on a computer.

6. Route

Every computer and network routing device stores a *routing table* in its RAM. A routing table stores information about which routers to send network packets to. The *route* command can be used to display and modify the routing table of a computer.

7. Syslog

As an administrator of a network, you have just completed all the configuration and they are working nicely. Now maybe the next thing you want to do is to set up something that can alert you when something goes wrong or down in your network. Syslog is an excellent tool for system monitoring and is almost always included in your distribution.

Places to store and display syslog messages

There are some places we can send syslog messages to:

Place to store syslog messages	**Command to use**
Internal buffer (inside a switch or router)	logging buffered [size]
Syslog server	Logging
Flash memory	logging file flash:filename
Nonconsole terminal (VTY connection…)	terminal monitor
Console line	logging console

Note: If sent to a syslog server, messages are sent on UDP port 514.

By default, Cisco routers and switches send log messages to the console. We should use a syslog server to contain our logging messages with the **logging** command. Syslog server is the most popular place to store logging messages and administrators can easily monitor the wealth of their networks based on the received information.

Syslog syntax

A syslog message has the following format:

seq no:timestamp%FACILTY-SEVERITY-MNEMONIC: message text

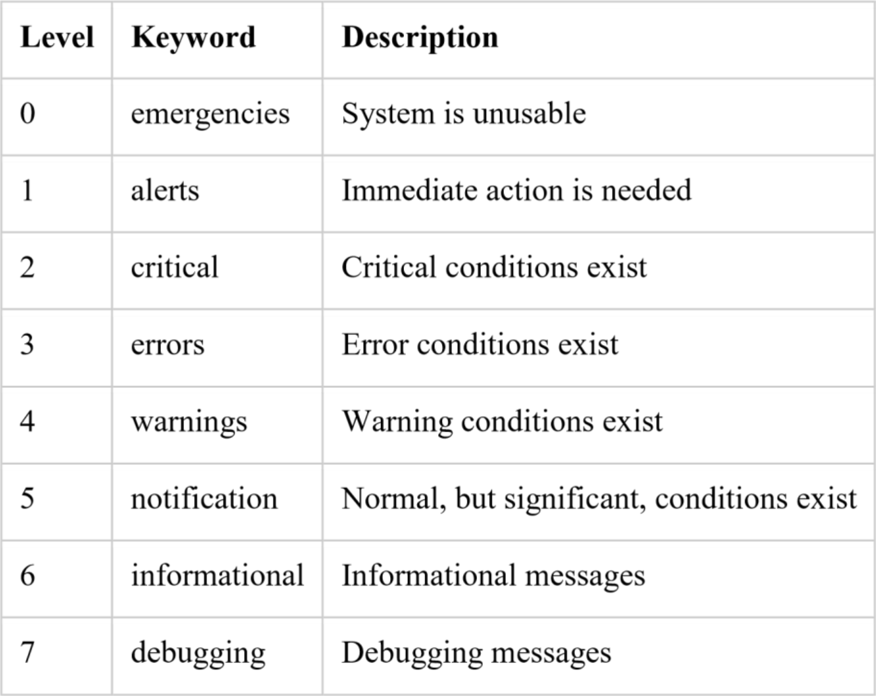
Each portion of a syslog message has a specific meaning:

+ **Seq no**: a sequence number only if the **service sequence-numbers** global configuration command is configured

+ **Timestamp**: Date and time of the message or event. This information appears only if the **service timestamps** global configuration command is configured.

+ **FACILITY**: This tells the protocol, module, or process that generated the message. Some examples are SYS for the operating system, IF for an interface…

+ **SEVERITY**: A number from 0 to 7 designating the importance of the action reported. The levels are:



Level	Keyword	Description
0	emergencies	System is unusable
1	alerts	Immediate action is needed
2	critical	Critical conditions exist
3	errors	Error conditions exist
4	warnings	Warning conditions exist
5	notification	Normal, but significant, conditions exist
6	informational	Informational messages
7	debugging	Debugging messages

Note: You can remember the order above with the sentence: "**E**ventually **A**ll **Critical Errors W**ill **N**ot **I**nvolve **D**amage".

The highest level is level 0 (emergencies). The lowest level is level 7. To change the minimum severity level that is sent to syslog, use the **logging trap *level*** configuration command. If you specify a level, that level and all the higher levels will be displayed. For example, by using the **logging console warnings** command, all the logging of emergencies, alerts, critical, errors, warnings will be displayed. Levels 0 through 4 are for events that could seriously impact the device, whereas levels 5 through 7 are for less-important events. By default, syslog servers receive informational messages (level 6).

+ **MNEMONIC**: A code that identifies the action reported.

+ **message text**: A plain-text description of the event that triggered the syslog message.

Let's see an example of the syslog message:

```
39345: May 22 13:56:35.811: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to down
```

+ **seq no**: 39345

+ **Timestamp**: May 22 13:56:35.811
+ **FACILTY**: LINEPROTO
+ **SEVERITY level**: 5 (notification)
+ **MNEMONIC**: UPDOWN
+ **message text**: Line protocol on Interface Serial0/0/1, changed state to down

Syslog Configuration

The following example tells the device to store syslog messages to a server on 10.10.10.150 and limit the messages for levels 4 and higher (0 through 4):

```
Router(config)#logging 10.10.10.150
Router(config)#logging trap 4
```

Of course on the server 10.10.10.150 we have to use a syslog software to capture the syslog messages sent to this server.

Exercise:

Use the topology given above at fig 2.3

1. Configure Router R2 (Follow the configuration done on MTUR1)
2. Configure the Switch (rename, set passwords, disable DNS lookup etc.)
3. Assign static IP addresses to router interfaces which have connection with other devices and allow the other hosts to obtain IP addresses to automatically from DHCP server by configuring a DHCP on the routers
4. Remotely configure R2 from PC A (use telnet and SSH)
5. Check all network troubleshooting commands discussed in the material on both a Physical machine and PCs used in Packet Tracer for the above topology
6. What is the function of a Clock rate command? Clock rate Vs bandwidth commands