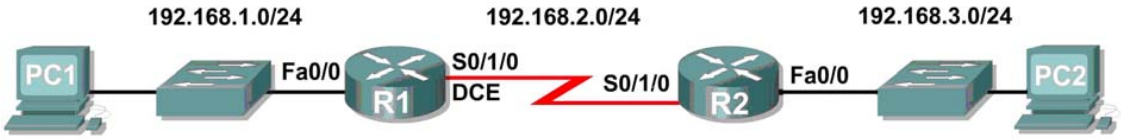
Introductory Lab: Cabling a Network and Basic Device Configuration

Topology Diagram



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	**Fa0/0**	192.168.1.1	255.255.255.0	N/A
	S0/1/0	192.168.2.1	255.255.255.0	N/A
R2	**Fa0/0**	192.168.3.1	255.255.255.0	N/A
	S0/1/0	192.168.2.2	255.255.255.0	N/A
S1	**VLAN99**	192.168.1.99	255.255.255.0	192.168.1.1
S2	**VLAN99**	192.168.3.99	255.255.255.0	192.168.3.1
PC1	**NIC**	192.168.1.10	255.255.255.0	192.168.1.1
PC2	**NIC**	192.168.3.10	255.255.255.0	192.168.3.1

Learning Objectives

Upon completion of this lab, you will be able to:

- Cable devices and establish console connections.
- Configure a terminal emulation program.
- Erase configuration files and reload the network device.
- Perform basic IOS command line interface operations.
- Perform basic router configuration.
- Perform basic switch configuration.
- Verify and test configurations using show commands, ping and traceroute.
- Create and reload a startup configuration file.

Background/Scenario

In this lab activity, you will review previously learned skills in the first CCNA RoS course (Introduction to Networks), including cabling devices, establishing a console connection, and basic IOS command line interface operation and configuration commands. You will also learn to save configuration files and capture your configurations to a text file. The skills presented in this lab are essential to completing the rest of the labs in the second course CCNA RoS (Routing and Switching Essentials).

During this lab you are going to work in a team of 4 students that comprises two lab groups (Group 1 and Group 2) which are corresponding to the routers R1 and R2. You have two work places per team in the laboratory. One group of two students will take care of configuring one router, one switch and host computers belonging to a work place. One student may work using the console of the device. The other student may use a host computer to establish a telnet session to access the device terminal if it is properly configured.

Important Note: The routers that are available for you in the laboratory are Cisco routers of the series 2800 or 2900. These routers have different platforms, hardware capabilities, **IOS** versions and network interfaces. However, all the labs will be performed on these routers in a similar way but with small differences. The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4) M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches, and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. However you may use any current router in your lab as long as it has the required interfaces as shown in the topology.

Task 1: Cable the Ethernet part of the network.

Learn how your work place is cabled to the **main rack** of the lab room. Cables are already drawn from the **front side of the desk** to the **patch panels** on the rack. Your task is to complete the cabling of the Ethernet links for a network that is similar to the one in the Topology Diagram. Be sure to use the appropriate type and length of Ethernet cables to connect from host to switch, switch to router.

Which of the devices in the Topology Diagram require an Ethernet cable between them?

.....

Group 1

Step 1: Connect the R1 router to the S1 switch.

Use a straight-through Ethernet cable to connect the FastEthernet 0/0 interface of the R1 router to the FastEthernet 0/12 interface on the S1 switch.

Observe the color of the link status light next to the FastEthernet 0/0 interface on R1 and the one next to the FastEthernet 0/12 interface on S1.

Step 2: Connect PC1 to the S1 Switch.

Connect the network interface card (NIC) of PC1 by using a straight-through Ethernet patch cable from the **patch panel** to the FastEthernet 0/1 Interface of the S1 switch.

What color is the link status light next to the FastEthernet 0/1 interface on S1? ……

If the link status lights are not green, wait a few moments for the link between the two devices to become established. If the lights do not turn green after a few moments, check that you are using a straight-through Ethernet cable and that the power is on for the S1 switch and PC1.

Group 2

Connect R2 and PC2 to the S2 Switch.

Repeat the Group 1's steps 1 and 2 to connect the PC2 and R2 to S2.

What color is the link status light next to the FastEthernet 0/0 interface on R2? ……

Task 2: Cable the Serial Link between the R1 and R2 Routers.

In a real-world WAN connection, the customer premises equipment (CPE), which is often a router, is the data terminal equipment (DTE). This equipment is connected to the service provider through serial cable to a data circuit-terminating equipment (DCE) device, which is commonly a modem or channel service unit (CSU)/ data service unit (DSU). This device is used to convert the data from the DTE into a form acceptable to the WAN service provider.

The serial cables in the real world are not connected back to back as in the case of the cables used in the academy laboratory. In a real-world situation, one router might be in a customer's main building, while another router might be in a remote office. An administrator located in **main building** would have to connect to the router in **remote office** through the WAN cloud in order to troubleshoot that router.

In the academy labs, devices that make up the WAN cloud are simulated by the connection between the back-to-back DTE-DCE cables. The connection from one router serial interface to another router serial interface simulates the whole network cloud.

Step 1: Create a null serial cable to connect the R1 router to the R2 router.

In the academy labs, the WAN connection between routers uses one DCE cable and one DTE cable. The DCE-DTE connection between routers is referred to as a null serial cable. The labs will use one V.35 DCE cable and one V.35 DTE cable to simulate the WAN connection. The V.35 DCE connector is usually a **female** V.35 (34-pin) connector. The DTE cable has a **male** V.35 connector. The cables are also labeled as DCE or DTE on the router end of the cable.

The DTE and DCE V.35 cables must be joined together. Holding one of the V.35 ends in each hand; examine the pins and sockets as well as the threaded connectors. Note that there is only one proper way for the cables to fit together. Align the **pins** on the male cable with the **sockets** on the female cable and gently couple them. Very little effort should be required to accomplish this. When they are joined, turn the thumbscrews clockwise and secure the connectors.

Step 2: Connect the DCE end of the null serial cable to the Serial 0/1/0 interface of the R1 router, and the DTE end of the null serial cable to the Serial 0/1/0 interface of the R2 router.

Review the information provided below before making these connections.

Before making the connection to one of the routers, examine the connector on the router and the cable. Note that the connectors are tapered to help prevent improper connection. Holding the connector in one hand, try to orient the cable and router connecter so that the tapers match. Now push the cable connector partially into the router connector. It probably will not go in all the way because the threaded connectors need to be tightened in order for the cable to be inserted completely. While holding the cable in one hand and gently pushing the cable toward the router, turn one of the thumb screws clockwise, 3 or 4 rounds, to start the screws. Now turn the other thumbscrew clockwise, 3 or 4 rounds, to get it started. At this point the cable should be attached sufficiently to free both hands to advance each thumbscrew at the same rate until the cable is fully inserted. Do not **over-tighten** these connectors.

Task 3: Establish a Console connection to the device (Router and Switch).

The console port is a management port used to provide out-of-band access to a device. It is used to set up the initial configuration of the device and to monitor it.

A **rollover** cable and an RJ-45 to DB-9 adapter are used to connect a PC to the console port. A terminal emulation software is used to configure the router over the console connection. For this purpose one may use either Tera Term or **HyperTerminal** in Windows and **Minicom** in Linux. HyperTerminal is installed in the Windows operating system and you will configure it for use in this lab.

At the end of this lab manual, the following three appendices are available for your reference concerning these terminal emulation programs:

- Appendix 1: Installing and Configuring Tera Term for use on Windows
- Appendix 2: Configuring Minicom to establish a Console Session with the Router
- Appendix 3: Accessing and Configuring HyperTerminal

- **Member 1 of the group will work with the Router (R1 or R2).**

- **Member 2 of the group will work with the switch (S1 or S2).**

Step 1: Examine the device and locate the RJ-45 connector labeled Console.

Step 2: Examine PC and locate a 9-pin male connector of the serial port.

It may—or may not—be labeled as COM1.

Step 3: Locate the console cable.

Locate a console cable with a built-in RJ-45 to DB-9 adapter attached to one end.

Step 4: Connect the console cable to the device and PC.

First, examine the cable connected to the device console port, and find the RJ-45 connector labeled "Console" on the **front side of the desk**. Next, connect the DB-9 end of the console cable to the serial port of PC.

Step 5: Test device connection.

1. Open your terminal emulation software (HyperTerminal, or Minicom if you prefer using Linux).
2. Configure the software parameters specific to your applications (see appendices for help).
3. Once the terminal window is open, press the **Enter** key. There should be a response from the device. If there is, then the connection has been successfully completed. If there is no connection, troubleshoot as necessary. For example, verify that the device has power. Check the connection to the serial port on the PC and the console port on the device.

Task 4: Erase and Reload the Device.

- **Member 1 of the group will work with the Router (R1 or R2).**

- **Member 2 of the group will work with the switch (S1 or S2).**

Router:

Step 1: Using the HyperTerminal session established in Task 3

Prior to this lab, the router should have no substantial configuration. If there is some configuration then you will erase it in step 2 of this task. If you are required to enter a password, please consult your instructor.

Enter privileged EXEC mode on the router:

```
Router>enable
Router#
```

Step 2: Erase existing configuration (the startup configuration file from NVRAM).

To clear the configuration, issue the **erase startup-config** command to remove the startup configuration from nonvolatile random-access memory (NVRAM). Confirm the objective when prompted, and answer **no** if asked to save changes. The result should look something like this:

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete
Router#
```

Step 3: Reload the router.

When the prompt returns, issue the **reload** command. When prompted to Proceed with reload, press Enter to confirm the reload. Pressing any other key will abort the reload.

```
Router# reload
Proceed with reload? [confirm]


*Nov 29 18:28:09.923: %SYS-5-RELOAD: Reload requested by console. Reload
Reason: Reload Command.
```

Note: You may receive a prompt to save the running configuration prior to reloading the router. Respond by typing **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

After the router finishes the boot process, choose **not** to use the initial configuration and confirm terminating the AutoInstall facility, as shown:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

```
Would you like to terminate autoinstall? [yes]: (Press Enter to accept
default.)

Press RETURN to get started!
```

Switch:

Step 1: Connect to the switch.

Console into the switch and enter privileged EXEC mode.

```
Switch> enable
Switch#
```

Step 2: Determine if there have been any virtual local-area networks (VLANs) created.

Use the **show flash** command to determine if any VLANs have been created on the switch.

```
Switch# show flash

Directory of flash:/

    2  -rwx        1919   Mar 1 1993 00:06:33 +00:00  private-config.text
    3  -rwx        1632   Mar 1 1993 00:06:33 +00:00  config.text
    4  -rwx       13336   Mar 1 1993 00:06:33 +00:00  multiple-fs
    5  -rwx    11607161   Mar 1 1993 02:37:06 +00:00  c2960-lanbasek9-
mz.150-2.SE.bin
    6  -rwx         616   Mar 1 1993 00:07:13 +00:00  vlan.dat

32514048 bytes total (20886528 bytes free)
Switch#
```

Step 3: Delete the VLAN file.

a. If the **vlan.dat** file was found in flash, then delete this file.

```
Switch# delete vlan.dat
Delete filename [vlan.dat]?
```

You will be prompted to verify the file name. At this point, you can change the file name or just press Enter if you have entered the name correctly.

b. When you are prompted to delete this file, press Enter to confirm the deletion. (Pressing any other key will abort the deletion.)

```
Delete flash:/vlan.dat? [confirm]
Switch#
```

Step 4: Erase the startup configuration file.

Use the **erase startup-config** command to erase the startup configuration file from NVRAM. When you are prompted to remove the configuration file, press Enter to confirm the erase. (Pressing any other key will abort the operation.)

```
Switch# erase startup-config
Erasing the nvram filesystem will remove all configuration files! Continue?
[confirm]
[OK]
Erase of nvram: complete
Switch#
```

Step 5: Reload the switch.

Reload the switch to remove any old configuration information from memory. When you are prompted to reload the switch, press Enter to proceed with the reload. (Pressing any other key will abort the reload.)

```
Switch# reload
Proceed with reload? [confirm]
```

Note: You may receive a prompt to save the running configuration prior to reloading the switch. Type **no** and press Enter.

```
System configuration has been modified. Save? [yes/no]: no
```

Step 6: Bypass the initial configuration dialog.

After the switch reloads, you should see a prompt to enter the initial configuration dialog. Type **no** at the prompt and press Enter.

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Switch>
```

Task 5: Understand Command Line Basics.

- **Member 1 of the group will work with the Router (R1 or R2).**

- **Member 2 of the group will work with the switch (S1 or S2).**

Router:

Step 1: Enter privileged EXEC mode.

```
Router>enable
Router#
```

Step 2: Enter an incorrect command and observe the router response.

```
Router#configure herminal
                  ^
% Invalid input detected at '^' marker.
```

Command line errors occur primarily from typing mistakes. If a command **keyword** is incorrectly typed, the user interface uses the caret symbol (^) to identify and isolate the error. The ^ appears at or near the point in the command string where an incorrect command, keyword, or argument was entered.

Step 3: Correct the previous command.

If a command is entered incorrectly, and the **Enter** key is pressed, the **Up Arrow** key on the keyboard can be pressed to repeat the last command. Use the **Right Arrow** and **Left Arrow** keys to move the cursor to the location where the mistake was made. Then make the correction. If something needs to be deleted, use the **Backspace** key. Use the directional keys and the **Backspace** key to correct the command to **`configure terminal`**, and then press **Enter**.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Step 4: Return to privileged EXEC mode with the `exit` command.

```
Router(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Router#
```

Step 5: Examine the commands that are available for privileged EXEC mode.

A question mark "**?**" can be entered at the prompt to display a list of available commands.

```
Router#?
Exec commands:
  <1-99>      Session number to resume
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
 --More--
```

Notice the `--More--` at the bottom of the command output. The `--More--` prompt indicates that there are multiple screens of output. When a `--More--` prompt appears, press the **Spacebar** to view the next available screen. To display only the next line, press the **Enter** key. Press any other key to return to the prompt.

Step 6: View output.

View the rest of the command output by pressing the **Spacebar**. The remainder of the output will appear where the `--More--` prompt appeared previously.

```
  telnet      Open a telnet connection
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  vlan        Configure VLAN parameters
  write       Write running configuration to memory, network, or terminal
```

Step 7: Exit privileged EXEC mode with the `exit` command.

```
Router#exit
```

The following output should be displayed:

```
Router con0 is now available

Press RETURN to get started.
```

Step 8: Press the Enter key to enter user EXEC mode.

The `Router>` prompt should be visible.

Step 9: Type an abbreviated IOS command.

IOS commands can be abbreviated, as long as enough characters are typed for the IOS to recognize the unique command.

Enter only the character **`e`** at the command prompt and observe the results.

```
Router>e
% Ambiguous command: "e"
```

```
Router>
```

Enter **en** at the command prompt and observe the results.

```
Router>en
Router#
```

The abbreviated command **en** contains enough characters for the IOS to distinguish the **enable** command from the **exit** command.

Step 10: Press the Tab key after an abbreviated command to use auto-complete.

Typing an abbreviated command, such as **conf**, followed by the **Tab** key completes a partial command name. This functionality of the IOS is called auto-complete. Type the abbreviated command **conf**, press the **Tab** key, and observe the results.

```
Router#conf
Router#configure
```

This auto-complete feature can be used as long as enough characters are typed for the IOS to recognize the unique command.

Step 11: Enter IOS commands in the correct mode.

IOS commands must be entered in the correct mode. For example, configuration changes cannot be made while in privileged EXEC mode. Attempt to enter the command **hostname R1** (or **R2**) at the privileged EXEC prompt and observe the results.

```
Router#hostname R1
               ^
% Invalid input detected at '^' marker.
Router#
```

Switch:

Step 1: Enter privileged EXEC mode.

Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode. Enter **enable** if the prompt has changed back to Switch>.

```
Switch>enable
Switch#
```

Step 2: Enter an incorrect command and observe the router response.

```
Switch#configure herminal
               ^
% Invalid input detected at '^' marker.
```

Command line errors occur primarily from typing mistakes. If a command **keyword** is incorrectly typed, the user interface uses the caret symbol (^) to identify and isolate the error. The ^ appears at or near the point in the command string where an incorrect command, keyword, or argument was entered.

Step 3: Correct the previous command.

If a command is entered incorrectly, and the **Enter** key is pressed, the **Up Arrow** key on the keyboard can be pressed to repeat the last command. Use the **Right Arrow** and **Left Arrow** keys to move the cursor to the location where the mistake was made. Then make the correction. If something needs to be deleted, use the **Backspace** key. Use the directional keys and the **Backspace** key to correct the command to **configure terminal**, and then press **Enter**.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config#

The prompt changed again to reflect global configuration mode.
```

Step 4: Return to privileged EXEC mode with the `exit` command.

```
Switch(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
Switch#
```

Step 5: Examine the commands that are available for privileged EXEC mode.

A question mark "**?**" can be entered at the prompt to display a list of available commands.

```
Switch#?
Exec commands:
  <1-99>      Session number to resume
  clear       Reset functions
  clock       Manage the system clock
  configure   Enter configuration mode
  connect     Open a terminal connection
  copy        Copy from one file to another
  debug       Debugging functions (see also 'undebug')
  delete      Delete a file
  dir         List files on a filesystem
  disable     Turn off privileged commands
  disconnect  Disconnect an existing network connection
  enable      Turn on privileged commands
  erase       Erase a filesystem
  exit        Exit from the EXEC
  logout      Exit from the EXEC
  no          Disable debugging informations
  ping        Send echo messages
  reload      Halt and perform a cold restart
  resume      Resume an active network connection
  setup       Run the SETUP command facility
  show        Show running system information
 --More--
```

Notice the `--More--` at the bottom of the command output. The `--More--` prompt indicates that there are multiple screens of output. When a `--More--` prompt appears, press the **Spacebar** to view the next available screen. To display only the next line, press the **Enter** key. Press any other key to return to the prompt.

Step 6: View output.

View the rest of the command output by pressing the **Spacebar**. The remainder of the output will appear where the `--More--` prompt appeared previously.

```
  telnet      Open a telnet connection
  traceroute  Trace route to destination
  undebug     Disable debugging functions (see also 'debug')
  vlan        Configure VLAN parameters
  write       Write running configuration to memory, network, or terminal
```

Step 7: Exit privileged EXEC mode with the `exit` command.

```
Switch#exit
```

The following output should be displayed:

```
Switch con0 is now available

Press RETURN to get started.
```

Step 8: Press the Enter key to enter user EXEC mode.

The `Switch>` prompt should be visible.

Step 9: Type an abbreviated IOS command.

IOS commands can be abbreviated, as long as enough characters are typed for the IOS to recognize the unique command.

Enter only the character **e** at the command prompt and observe the results.

```
Switch>e
% Ambiguous command: "e"
Switch>
```

Enter **en** at the command prompt and observe the results.

```
Switch>en
Switch#
```

The abbreviated command **en** contains enough characters for the IOS to distinguish the **enable** command from the **exit** command.

Step 10: Press the Tab key after an abbreviated command to use auto-complete.

Typing an abbreviated command, such as **conf**, followed by the **Tab** key completes a partial command name. This functionality of the IOS is called auto-complete. Type the abbreviated command **conf**, press the **Tab** key, and observe the results.

```
Switch#conf
Switch#configure
```

This auto-complete feature can be used as long as enough characters are typed for the IOS to recognize the unique command.

Step 11: Enter IOS commands in the correct mode.

IOS commands must be entered in the correct mode. For example, configuration changes cannot be made while in privileged EXEC mode. Attempt to enter the command **hostname R1** (or **R2**) at the privileged EXEC prompt and observe the results.

```
Switch#hostname S1
                ^
% Invalid input detected at '^' marker.

Switch#
```

Task 6: Perform Basic Configuration of Network Device

- **Member 1 of the group will work with the Router (R1 or R2).**

- **Member 2 of the group will work with the switch (S1 or S2).**

Router:

Note: The following steps are for R1 (For R2, perform the same Steps 1 up to 9).

Step 1: Enter privileged EXEC mode (if you are not already there**).**

```
Router>en
Router#
```

Step 2: Enter global configuration mode.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
```

Step 3: For the router R1, configure the router name as R1.

Enter the command **hostname R1** at the prompt.

```
Router(config)#hostname R1
R1(config)#
```

Step 4: Disable DNS lookup with the `no ip domain-lookup` command.

```
R1(config)#no ip domain-lookup
R1(config)#
```

Why would you want to disable DNS lookup in a lab environment?

What would happen if you disabled DNS lookup in a production environment?

Step 5: Configure an EXEC mode password.

Configure an EXEC mode password using the **enable secret** *password* command. Use **class** for the *password*.

```
R1(config)#enable secret class
R1(config)#
```

The **enable secret** command is used to provide an additional layer of security over the **enable password** command. The **enable secret** command provides better security by storing the **enable secret** password using a non-reversible cryptographic function. The added layer of security encryption is useful in environments where the password crosses the network or is stored on a TFTP server. When both the **enable password** and **enable secret** passwords are configured, the router expects the password as defined in the **enable secret** command. In this case, the router ignores the password defined in the **enable password** command.

Step 6: Remove the `enable password`.

Because the **enable secret** is configured, the **enable password** is no longer necessary. IOS commands can be removed from the configuration using the **no** form of the command.

```
R1(config)#no enable password
R1(config)#
```

Step 7: Configure a message-of-the-day banner using the `banner motd` command.

```
R1(config)#banner motd &
Enter TEXT message.  End with the character '&'.
********************************
  !!!AUTHORIZED ACCESS ONLY!!!
********************************
&
R1(config)#
```

When does this banner display?

Why should every router have a message-of-the-day banner?

Step 8: Configure the console password on the router.

Use **cisco** as the password. When you are finished, exit from line configuration mode.

```
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Step 9: Configure the password for the virtual terminal lines.

Use **cisco** as the password. When you are finished, exit from line configuration mode.

```
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#login
R1(config-line)#exit
R1(config)#
```

Switch:

Note: The following steps are for S1 (For S2, perform the same Steps 1 up to 13).

In this task, you will configure the basic switch settings, such as hostname and an IP address for the switch management SVI. Assigning an IP address on the switch is only the first step. As the network administrator, you must specify how the switch is managed. Telnet and SSH are the two most common management methods. However, Telnet is not a secure protocol. All information flowing between the two devices is sent in plain text. Passwords and other sensitive information can be easily looked at if captured by a packet sniffer.

Step 1: Enter privileged EXEC mode (if you are not already there**).**

Assuming the switch had no configuration file stored in NVRAM, verify you are at privileged EXEC mode. Enter **enable** if the prompt has changed back to Switch>.

```
Switch> enable
Switch#
```

Step 2: Enter global configuration mode.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#
```

The prompt changed again to reflect global configuration mode.

Step 3: For the switch 1, configure the hostname as S1.

```
Switch(config)# hostname S1
S1(config)#
```

Step 4: configure password encryption

```
S1(config)# service password-encryption
S1(config)#
```

Step 5: Assign class **as the secret password for privileged EXEC mode access.**

```
S1(config)# enable secret class
S1(config)#
```

Step 6: Prevent unwanted DNS lookups.

```
S1(config)# no ip domain-lookup
S1(config)#
```

Step 6: Configure a MOTD banner.

```
S1(config)# banner motd #
Enter Text message.  End with the character '#'.
Unauthorized access is strictly prohibited. #
```

Step 7: Verify your access settings by moving between modes.

```
S1(config)# exit
S1#
*Mar  1 00:19:19.490: %SYS-5-CONFIG_I: Configured from console by console
S1# exit
S1 con0 is now available

Press RETURN to get started.

Unauthorized access is strictly prohibited.
S1>
```

Step 8: Go back to privileged EXEC mode from user EXEC mode. Enter class as the password when prompted.

```
S1> enable
Password:
S1#
```

Note: The password does not display when entering.

Step 9: Enter global configuration mode to set the SVI IP address of the switch. This allows remote management of the switch.

Before you can manage S1 remotely from PC-A, you must assign the switch an IP address. The default configuration on the switch is to have the management of the switch controlled through VLAN 1. However, a best practice for basic switch configuration is to change the management VLAN to a VLAN other than VLAN 1.

For management purposes, use VLAN 99. The selection of VLAN 99 is arbitrary and in no way implies that you should always use VLAN 99.

First, create the new VLAN 99 on the switch. Then set the IP address of the switch to 192.168.1.2 with a subnet mask of 255.255.255.0 on the internal virtual interface VLAN 99.

```
S1# configure terminal
S1(config)# vlan 99
S1(config-vlan)# exit
S1(config)# interface vlan99
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to
down
S1(config-if)# ip address 192.168.1.99 255.255.255.0
S1(config-if)# no shutdown
S1(config-if)# exit
S1(config)#
```

Notice that the VLAN 99 interface is in the down state even though you entered the **no shutdown** command. The interface is currently down because no switch ports are assigned to VLAN 99.

Step 10: Assign all user ports to VLAN 99.

```
S1(config)# interface range f0/1 – 24,g0/1 - 2
S1(config-if-range)# switchport access vlan 99
S1(config-if-range)# exit
```

```
S1(config)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed state to up
```

To establish connectivity between the host and the switch, the ports used by the host must be in the same VLAN as the switch. Notice in the above output that the VLAN 1 interface goes down because none of the ports are assigned to VLAN 1. After a few seconds, VLAN 99 comes up because at least one active port (F0/6 with PC-A attached) is now assigned to VLAN 99.

Step 11: Configure the IP default gateway for S1.

If no default gateway is set, the switch cannot be managed from a remote network that is more than one router away. It does respond to pings from a remote network. Although this activity does not include an external IP gateway, assume that you will eventually connect the LAN to a router for external access. Assuming that the LAN interface on the router is 192.168.1.1, set the default gateway for the switch.

```
S1(config)# ip default-gateway 192.168.1.1
S1(config)#
```

Step 12: Configure the console password on the switch.

Console port access should also be restricted. The default configuration is to allow all console connections with no password needed. To prevent console messages from interrupting commands, use the **logging synchronous** option.

```
S1(config)# line con 0
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# logging synchronous
S1(config-line)# exit
S1(config)#
```

Step 13: Configure the password for the virtual terminal lines.

Configure the virtual terminal (vty) lines for the switch to allow Telnet access. If you do not configure a vty password, you are unable to telnet to the switch.

```
S1(config)# line vty 0 15
S1(config-line)# password cisco
S1(config-line)# login
S1(config-line)# end
S1#
*Mar  1 00:06:11.590: %SYS-5-CONFIG_I: Configured from console by console
```

Task 7: Configure the active interfaces of each router.

Group 1: For the router R1

Step 1: Configure the FastEthernet 0/0 interface with the IP address 192.168.1.1/24.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R1(config-if)#
```

Step 2: Use the `description` command to provide a description for this interface.

```
R1(config-if)#description R1 LAN
R1(config-if)#
```

Step 3: Configure the Serial0/1/0 interface with the IP address 192.168.2.1/24.

Set the clock rate to 64000.

Note: Because the routers in the labs will not be connected to a live leased line, one of the routers will need to provide the clocking for the circuit. This is normally provided to each of the routers by the service provider. To provide this clocking signal in the lab, one of the routers will need to act as the DCE on the connection. This function is achieved by applying the command **clock rate 64000** on the serial 0/1/0 interface, where the DCE end of the null modem cable has been connected. The purpose of the **clock rate** command is discussed further in Chapter 2, "Static Routes."

```
R1(config-if)#interface serial 0/1/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#clock rate 64000
R1(config-if)#no shutdown
R1(config-if)#
```

Note: The interface will not be activated until the serial interface on R2 is configured and activated.

Step 4: Use the description command to provide a description for this interface.

```
R1(config-if)#description Link to R2
R1(config-if)#
```

Step 5: Use the end command to return to privileged EXEC mode.

```
R1(config-if)#end
R1#
```

Step 6: Save the R1 configuration.

Save the R1 configuration using the **copy running-config startup-config** command.

```
R1#copy running-config startup-config
Building configuration...
[OK]
R1#
```

Group 2: For the router R2

Step 1: Configure the Serial 0/1/0 interface with the IP address 192.168.2.2/24.

```
R2(config)#interface serial 0/1/0
R2(config-if)#ip address 192.168.2.2 255.255.255.0
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface Serial0/1/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/1/0, changed
state to up
R2(config-if)#
```

Step 2: Use the description command to provide a description for this interface.

```
R2(config-if)#description Link to R1
R2(config-if)#
```

Step 3: Configure the FastEthernet 0/0 interface with the IP address 192.168.3.1/24.

```
R2(config-if)#interface fastethernet 0/0
R2(config-if)#ip address 192.168.3.1 255.255.255.0
R2(config-if)#no shutdown

%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed
state to up
R2(config-if)#
```

Step 4: Use the `description` command to provide a description for this interface.

```
R2(config-if)#description R2 LAN
R2(config-if)#
```

Step 5: Use the `end` command to return to privileged EXEC mode.

```
R2(config-if)#end
```

Step 6: Save the R2 configuration.

Save the R2 configuration using the **`copy running-config startup-config`** command,

```
R2#copy running-config startup-config
Building configuration...
[OK]
```

Task 8: Configure IP Addressing on the Host PCs.

Group 1: Configure the host PC1.

Configure the host PC1 that is attached to S1 with an IP address of 192.168.1.10/24 and a default gateway of 192.168.1.1.

Group 2: Configure the host PC2.

Configure the host PC2 that is attached to S2 with an IP address of 192.168.3.10/24 and a default gateway of 192.168.3.1.

Task 9: Using `ping`.

The **`ping`** command is a useful tool for troubleshooting Layers 1 though 3 of the OSI model and diagnosing basic network connectivity. Pings can be sent from a router or a host PC. This operation can be performed on **the router** at either the user or privileged EXEC modes. Using **`ping`** sends an Internet Control Message Protocol (ICMP) packet to the specified device and then waits for a reply.

Note: The steps that will be performed in this task are only examples of the router **R1**; however the same steps should be achieved on the router **R2** in a similar way with the corresponding addresses.

Step 1: Use the `ping` command to test connectivity between the R1 router and PC1.

```
R1#ping 192.168.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 72/79/91 ms
```

Each exclamation point (!) indicates a successful echo reply. Each period (.) on the display indicates that the application on the router timed out while it has waited for a successful ping. The first ping packet is failed because the router may not have an ARP table entry for the destination address of the IP packet. Because there is no ARP table entry, then the router sends an ARP request, receives a response, and adds the MAC address to the ARP table. When the next ping packet arrives, it will be forwarded and be successful.

Step 2: Repeat the ping from R1 to PC1.

```
R1#ping 192.168.1.10
```

What is the result from ping now?

.....

.....

.....

Step 3: Send an extended ping from R1 to PC1.

To accomplish this, type **ping** at the privileged EXEC prompt and press **Enter**. Fill out the rest of the prompts as shown:

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.10
Repeat count [5]: 10
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 100-byte ICMP Echos to 192.168.1.10, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 53/77/94
ms

R1#
```

Step 4: Send a ping from PC1 to R1.

From Windows go to **Start > All Programs > Accessories > Command Prompt**. In the Command Prompt window that opens, ping **R1** by issuing the following command:

```
C:\> ping 192.168.1.1
```

The ping should respond with successful results. What is the difference in the operation compared with step 2?

.....

.....

Step 5: Send an extended ping from PC1 to R1.

To accomplish this, enter the following command at the Windows command prompt:

```
C:\>ping 192.168.1.1 –n 10
```

There should be 10 successful responses from the command. How can you change the default size of the ping packet?

.....

.....

Is it possible to ping from **PC1** to **PC2**? Why or why not? Explain.

.....

.....

.....

Step 6: Send a ping from PC1 to S1.

```
C:\> ping 192.168.1.99
```

The ping should respond with successful results. Which host (or interface) has replied to the ping?

.....

.....

Task 10: Using `traceroute`.

The **`traceroute`** command is an excellent utility for troubleshooting the path that a packet takes through an internetwork of routers. It can help to isolate problem links and routers along the way. The **`traceroute`** command uses ICMP packets and the error message generated by routers when the packet exceeds its Time-To-Live (TTL). This operation can be performed at either the user or privileged EXEC modes. The Windows version of this command is **tracert**.

Note: The steps that will be performed in this task are only examples of the router **R1** and **PC1**; however the same steps should be achieved on the router **R2** and **PC2** in a similar way.

Step 1: Use the `traceroute` command at the R1 privileged EXEC prompt to discover the path that a packet will take from the R1 router to PC1.

```
R1#traceroute 192.168.1.10
Type escape sequence to abort.
Tracing the route to 192.168.1.10

     1   192.168.1.10    103 msec  81 msec   70 msec
R1#
```

Step 2: Use the `tracert` command at the Windows command prompt to discover the path that a packet will take from PC1 to the R1 router.

```
C:\>tracert 192.168.1.1

Tracing route to 192.168.1.1 over a maximum of 30 hops:

  1   71 ms 70 ms 73 ms 192.168.1.1

Trace complete.
```

Task 11: Examine `show` Commands.

There are many **`show`** commands that can be used to examine the operation of the router (or switch). In both privileged EXEC and user EXEC modes, the command **`show ?`** provides a list of available **`show`** commands. The list is considerably longer in privileged EXEC mode than it is in user EXEC mode.

Note: The outputs that will be shown in the rest of this task are only examples of the router **R1** and the switch **S1**; however the same steps should be achieved on the router **R2** and the switch **S2** in a similar way.

Step 1: Examine the `show running-config` command.

The **`show running-config`** command is used to display the contents of the currently running configuration file. From privileged EXEC mode on the R1 router, examine the output of the **`show running-config`** command. If the `--More--` prompt appears, press the **Spacebar** to view the remainder of the command output.

```
R1(or S1)#show running-config
```

Which configuration commands that you entered before and now appear in the output?

.....

.....

.....

.....

.....

.....

Step 2: Examine the `show startup-config` command.

The **`show startup-config`** command displays the startup configuration file contained in NVRAM. From privileged EXEC mode on the R1 router, examine the output of the **`show startup-config`** command. If the `--More--` prompt appears, press the **Spacebar** to view the remainder of the command output.

```
R1(or S1)#show startup-config
```

Is the output identical with the previous one? Why or why not?

.....

.....

Step 3: Examine the `show interfaces` command.

The **`show interfaces`** command displays statistics for all interfaces configured on the router. A specific interface can be added to the end of this command to display the statistics for only that interface. From privileged EXEC mode on the R1 router, examine the output of the **`show interfaces fastEthernet0/0`** command. If the `--More--` prompt appears, press the **Spacebar** to view the remainder of the command output.

```
R1#show interfaces fastEthernet 0/0
```

Which parts of information are relevant in the output? Can you explain the meaning of each of them?

.....

.....

.....

.....

.....

.....

```
S1# show interface vlan99
```

Which parts of information are relevant in the output?

.....

.....

.....

```
S1# show vlan brief
```

Which user ports are in VLAN 99?

.....

.....

.....

Step 4: Examine the `show version` command.

The **`show version`** command displays information about the currently loaded software version along with hardware and device information. From privileged EXEC mode on the **R1** router or the Switch **S1**,

examine the output of the **show version** command. If the --More-- prompt appears, press the **Spacebar** to view the remainder of the command output.

```
R1(or S1)#show version
```

What does the output tell you about your device? Give details of some important parts of the shown information, for example; platform, interfaces, memory, IOS etc.

.....

.....

.....

.....

.....

.....

Step 5: Examine the show ip interface brief (or show vlan brief) command.

The **show ip interface brief** command displays a summary of the usability status information for each interface. From privileged EXEC mode on the R1 router, examine the output of the **show ip interface brief** command. If the --More-- prompt appears, press the **Spacebar** to view the remainder of the command output.

```
R1#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.1.1     YES manual up                    up
FastEthernet0/1        unassigned      YES manual administratively down down
Serial0/1/0            192.168.2.1     YES manual up                    up
Serial0/1/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual administratively down down
```

Issue **show vlan brief** command to verify that all the user ports are in VLAN 99.

```
S1# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active
99   VLAN0099                         active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

Task 12: Create a start.txt File.

Router (or switch) configurations can be captured to a text (.txt) file and saved for later use. The configuration can be copied back to the device so that the commands do not have to be entered one at a time.

Note: The steps that will be performed in this task are only examples of the router **R1** (or the switch **S1**); however the same steps should be achieved on the router **R2** (or the switch **S2**) in a similar way.

Step 1: View the running configuration of the device using the `show running-config` command.

```
R1(or S1)#show running-config
```

Step 2: Copy the command output.

Select the command output. From the HyperTerminal Edit menu, choose the copy command.

Step 3: Paste output in Notepad.

Open Notepad. Notepad is typically found on the **Start** menu under All **Programs > Accessories**. From the Notepad Edit menu, click **Paste**.

Step 4: Edit commands.

Some commands will have to be edited or added before the startup script can be applied. Some of these changes are:

- Adding a **`no shutdown`** command to FastEthernet and serial interfaces that are being used on the router and the interface vlan 99 on the switch.
- Replacing the encrypted text in the **`enable secret`** command with the appropriate password.
- Removing unused interfaces.
- Removing any characters that are not part of the commands.

Edit the text in the Notepad file as necessary.

Step 5: Save the open file in Notepad to start.txt.

Task 13: Load the start.txt File onto the device.

Note: The steps that will be performed in this task are only examples of the router **R1** (or the switch **S1**); however the same steps should be achieved on the router **R2** (or the switch **S2**) in a similar way.

Step 1: Erase the current startup configuration of the device.

Confirm the objective when prompted, and answer **no** if asked to save changes. The result should look something like this:

```
R1(or S1)#erase startup-config
Erasing the nvram filesystem will remove all files! Continue? [confirm]
[OK]
Erase of nvram: complete

R1(or S1)#
```

Step 2: When the prompt returns, issue the `reload` command.

Confirm the objective when prompted. After the router finishes the boot process, choose not to use the AutoInstall facility, as shown:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
Would you like to terminate autoinstall? [yes]:
Press Enter to accept default.
Press RETURN to get started!
```

Step 3: Enter global configuration mode.

```
Router(or Switch)##configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)#
```

Step 4: Copy the commands.

In the start.txt file that was created in Notepad, select all the lines, and then choose **Edit > Copy**.

Step 5: From the HyperTerminal Edit menu, choose "Paste to Host".

Step 6: Verify the running configuration.

After all of the pasted commands have been applied, use the **show running-config** command to verify that the running configuration appears as expected.

Step 7: Save the running configuration,

Save the running configuration to NVRAM using the **copy running-config startup-config** command.

```
R1(or S1)#copy running-config startup-config
Building configuration...
[OK]
R1(or S1)#
```

Now view the **startup-config** file and verify that your current configuration is properly saved.

Reflection

1. Why should you configure the vty lines for the router (or the switch)?

2. Why change the default management VLAN 1 to a different VLAN number?

3. How can you prevent passwords from being sent in plain text?

Appendix 1: Installing and Configuring Tera Term for use on Windows XP

Tera Term is a free terminal emulation program for Windows. It can be used in the lab environment in place of Windows HyperTerminal. Tera Term can be obtained at the following URL:

http://hp.vector.co.jp/authors/VA002416/teraterm.html

Download the “ttermp23.zip”, unzip it, and install Tera Term.

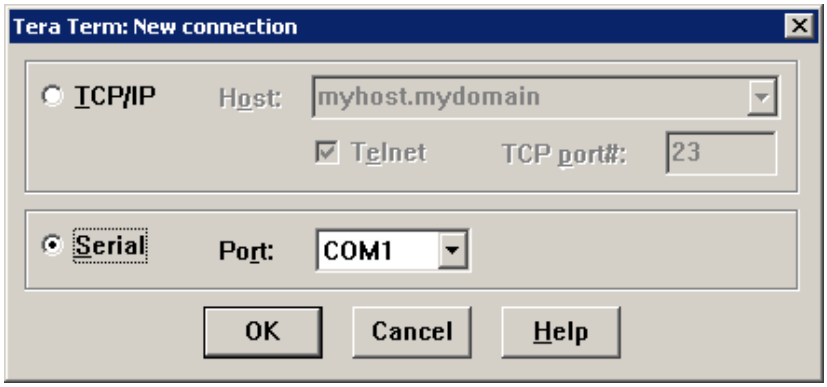
Step 1: Open the Tera Terminal program.

Step 2: Assign Serial port.

To use Terra Term to connect to the router console, open the **New connection** dialog box and select the **Serial** port.

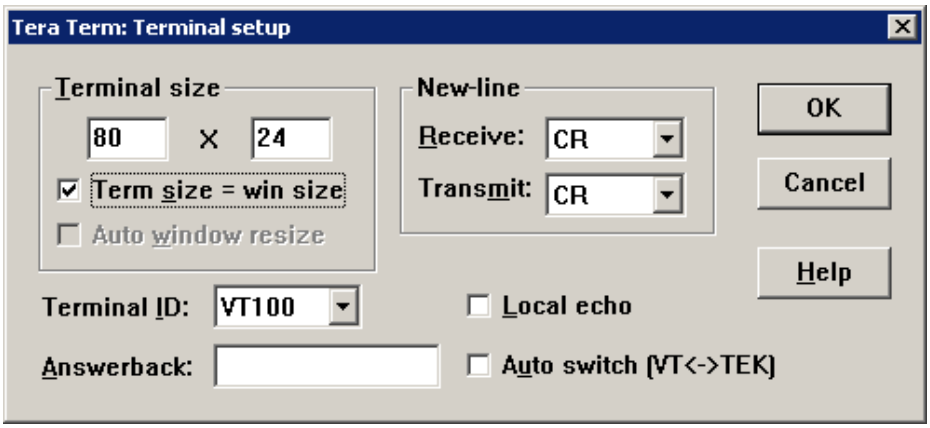
Step 3: Set Serial port parameters.

Set appropriate parameters for Port in the Serial section of the **Tera Term:New Connection** dialog box. Normally, your connection is through COM1. If you are unsure what port to use, ask your instructor for assistance.



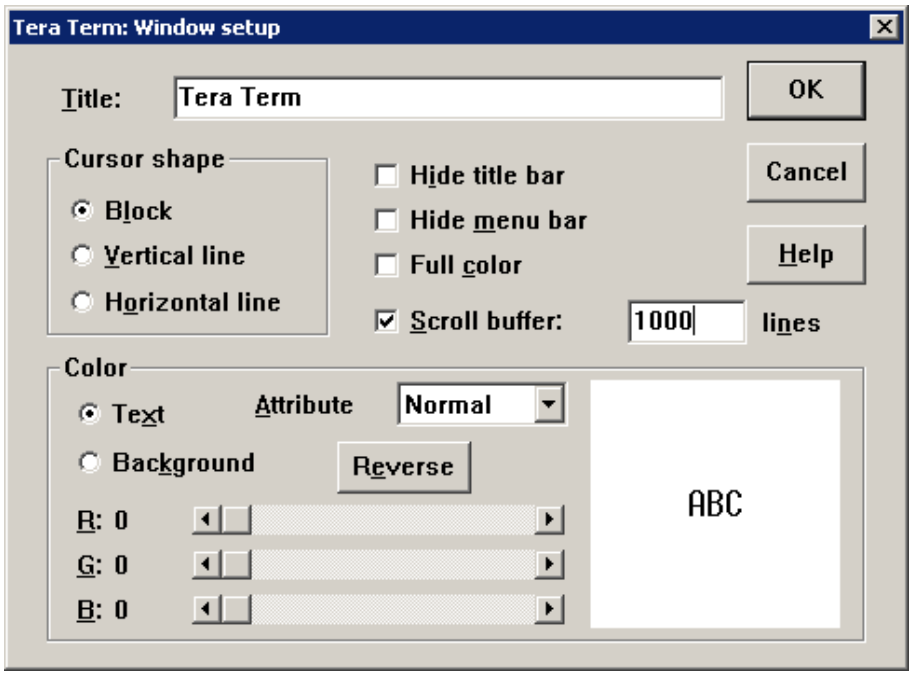
Step 4: Configure settings.

Terra Term has some settings that can be changed to make it more convenient to use. From the **Setup > Terminal** menu, check the **Term size = win size** checkbox. This setting allows command output to remain visible when the Terra Term window is resized.



Step 5: Change scroll buffer number.

From the **Setup > Window** menu, change the scroll buffer number to a number higher than 100. This setting allows you to scroll up and view previous commands and outputs. If there are only 100 lines available in the buffer, only the last 100 lines of output are visible. In the example below, the scroll buffer has been changed to 1000 lines.



Appendix 2: Configuring Minicom to establish a Console Session

Step 1: Start Minicom application in configuration mode.

Note: To configure Minicom, root access is required. From the Linux command prompt, start **minicom** with the **–s** option. This starts Minicom in the configuration mode:

```
[root]# minicom –s <ENTER>
```

Step 2: Configure Minicom for serial communications.

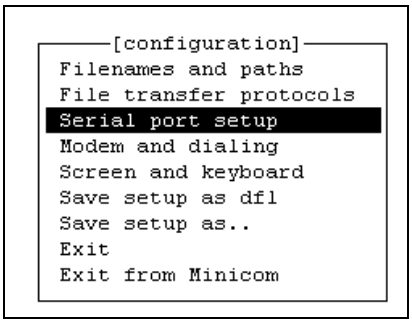


Figure 1. Main Configuration Window

Refer to Figure 1. To configure the serial port, scroll down the configuration list and select **Serial port setup**. Press **Enter**.

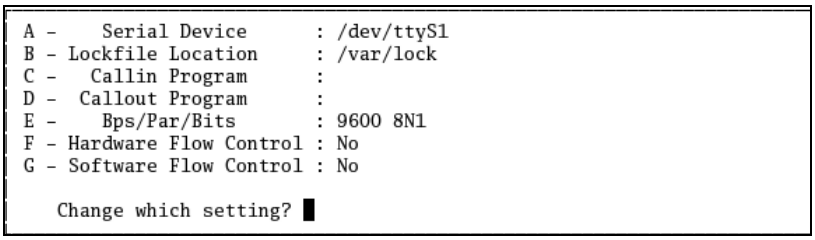


Figure 2. Serial Port Configuration Window

Refer to Figure 2. Use the letter by the field to change a setting. Refer to Table 1 for the correct values.

Option	Field	Value
A	Serial Device	/dev/ttyS0 for COM1 /dev/ttyS1 for COM2
E	Bps/Par/Bits	Bps- 9600 Par- None Bits- 8 Stop bits- 1 (or, select option 'Q')
F	**Hardware Flow Control**	Toggle- No
G	**Software Flow Control**	Toggle- No

Table 1. Serial Port Settings

Return to the Configuration menu by pressing **Enter** or **Esc**. Refer to Figure 3. Select **Save setup as dfl** (default file). When Minicom is restarted, the default values will be reloaded.

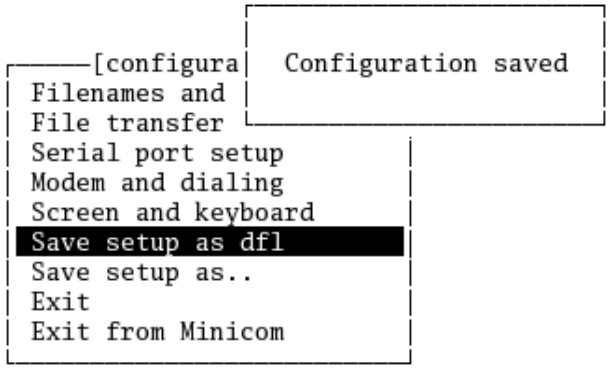


Figure 3. Serial Port Configuration Window

Step 3: Close Minicom.

When finished, close the Minicom session. Select **`Exit from Minicom`**.

Step 4: Restart the Minicom session.

```
[root]# minicom <ENTER>
```

When the session window starts, press the **Enter** key. There should be a response from the router. This indicates that connection has been successfully completed. If there is no connection, troubleshoot as necessary. For example, verify that the router has power. Check the connection to the correct COM1 port on the PC and the console port on the router. If there is still no connection, ask the instructor for assistance.

Step 5: Perform Basic Commands.

Minicom is a text-based, menu-driven, serial communication utility. Basic commands are not intuitive. For example, users communicate with remote devices within the terminal window. However, to control the utility, use **`<CTRL> A`**. To get help, press **`<CTRL> A`**, followed by **`Z`**.

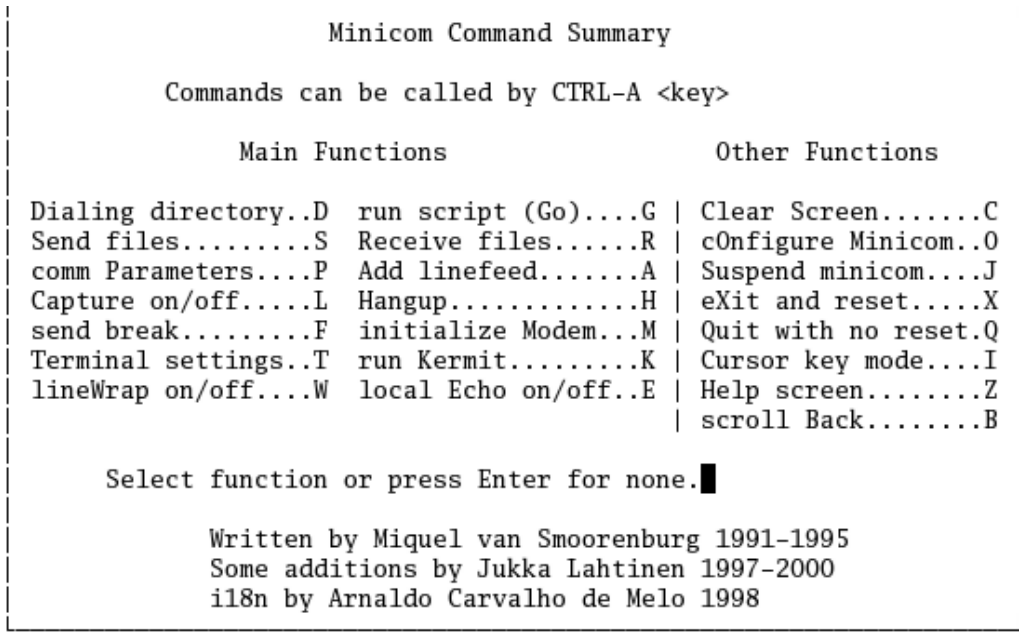


Figure 4. Minicom Command Summary Screen

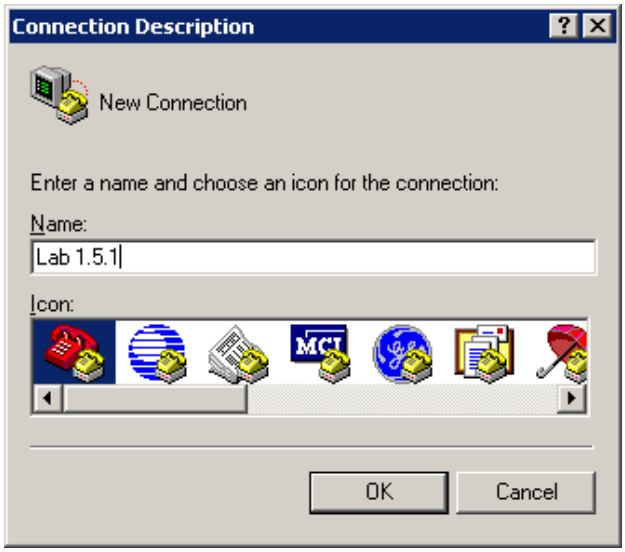
Refer to Figure 4 for a list of functions and corresponding keys. To quit Minicom, press **`<CTRL> A`**, followed by either **`Q`** or **`X`**.

Appendix 3: Accessing and Configuring HyperTerminal

In most versions of Windows, HyperTerminal can be found by navigating to **Start > Programs > Accessories > Communications > HyperTerminal**.

Step 1: Create a new connection.

Open HyperTerminal to create a new connection to the router. Enter an appropriate description in the **Connection Description** dialog box and then click **OK**.

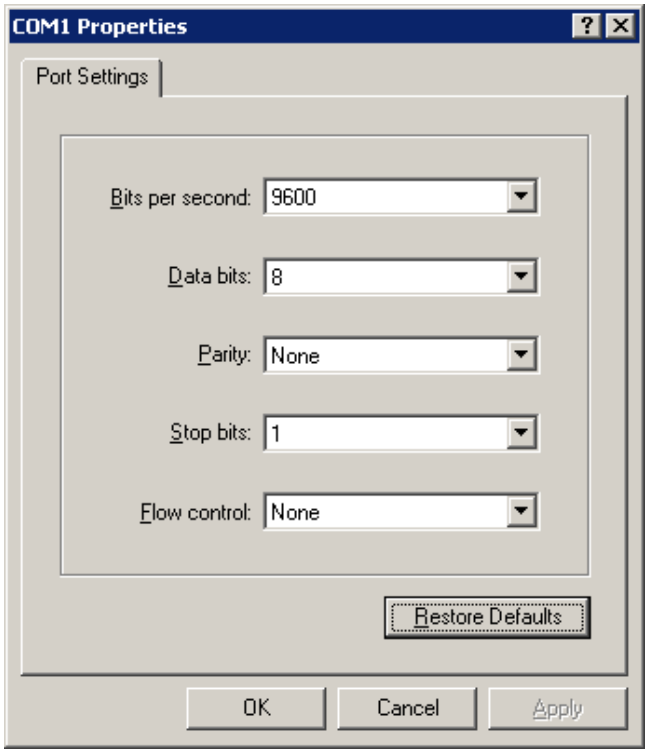


Step 2: Assign COM1 port.

On the **Connect To** dialog box, make sure the correct serial port is selected in the **Connect using** field. Some PCs have more than one COM port. Click **OK**.

Step 3: Set COM1 properties.

In the **COM1 Properties** dialog box under Port Setting, clicking **Restore Defaults** normally sets the correct properties. If not, set the properties to the values show in the following graphic, and then click OK.



Step 4: Verify connection.

You should now have a console connection to the router. Press **Enter** to get a router prompt.