**PART 1 – Subnet**

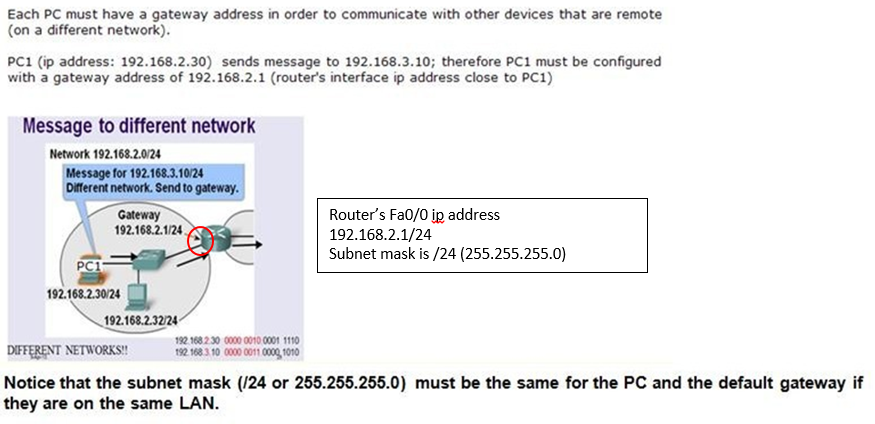
Be sure to read chapter 11, complete the PT activity files, and Lab documents found in the online curriculum **BEFORE** attempting Part 2 Task 4.

**Summary:**

The default gateway address (refer to curriculum topic: 2.3.1) is the address of the router’s interface connected to the same local network as the source host. All hosts on the local network use the default gateway address to send messages to the router. Once the host knows the default gateway IP address, it can use ARP to determine the MAC address. The MAC address of the router is then placed in the frame, destined for another network.

It is important that the correct default gateway be configured on each host on the local network. It can use any ip address within your subnet but it is common practice to use the first or last ip address.

If no default gateway is configured in the host TCP/IP settings, or if the wrong default gateway is specified, messages addressed to hosts on remote networks cannot be delivered. Example shown below:



**VIDEOS**

Default Gateway - http://www.youtube.com/watch?v=sAKgfi0tZZM

Subnetting & Calculating the range (9:59min) - <http://www.youtube.com/watch?v=ZTJIkjgyuZE&list=PLBBA99EC3925F5FC0>

Subnetting- <http://www.youtube.com/watch?v=pbU80DJ5XRQ>    
Setup SSH on Cisco IOS (7 MIN.) <https://www.youtube.com/watch?v=zXj37jAeer8>

## Learning Objectives

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

* Complete subnetting
* Identify the Default Gateway
* Configure the physical lab topology.
* Configure the logical LAN topology.
* Verify LAN connectivity.

Task 1: Subnet

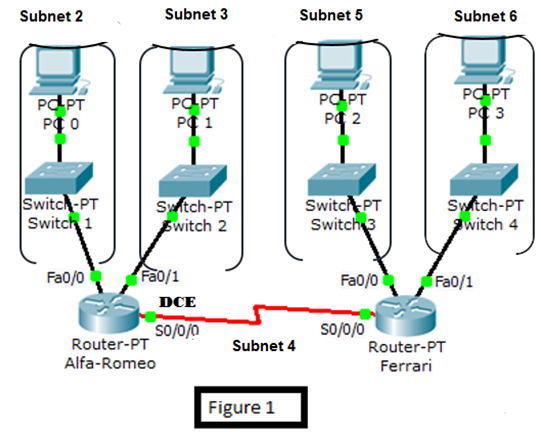
A logical topology of a network is given below. We need Five (5) subnets.

**Q1. Complete the table below by typing the missing number(s). DO NOT TYPE THE PERIOD.**

*IPv4 Address (Layer 3) Information Table*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network/Subnet Address** | **Subnet Mask – Dotted Decimal** | **First Host Address** | **Last Host Address** | **Subnet Broadcast Address** |
| #1 192.168.2.0 | 255.255.255.\_\_\_ | 192.168.2. ­­\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |
| #2 192.168.2. \_\_\_\_ | 255.255.255.\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |
| #3 192.168.2. \_\_\_\_ | 255.255.255.\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |
| #4 192.168.2. \_\_\_\_ | 255.255.255.\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |
| #5 192.168.2. \_\_\_\_ | 255.255.255.\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |
| #6 192.168.2. \_\_\_\_ | 255.255.255.\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ | 192.168.2. \_\_\_\_\_ |

Task 2: Configure the Logical Topology.



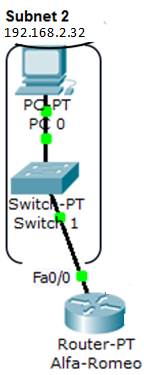
Step 1: Document logical network settings.

The host computer gateway’s IP address is used to send IP packets to other networks. Therefore, the Gateway address is the IP address assigned to the router interface for that subnet. **READ CAREFULLY!**

Using Figure 1 and the IPv4 Address information table recorded on page 2, complete the tables on page 4 and page 5 by typing the missing information for each computer, switch & router.

* The router’s LANs’ Fast Ethernet (Fa) interfaces will use the first host available IP address in the network address block.
* The host computers from each subnet will use the second host available IP address in the network address block.
* Alfa-Romeo’s S0/0/0 ip address will be 192.168.2.97.
* Ferrari’s S0/0/0 ip address will be 192.168.2.98.
* The switches’ VLAN1 will use the last host address in their network address block.

Below PC0 is shown as an example.



PC0 *belongs to subnet #2 which is 192.168.2.32 as shown above*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Network/Subnet Address** | **Subnet Mask** | **First Host Address** | **Last Host Address** | **Broadcast Address** |
| #2 192.168.2.32 | 255.255.255.224 | 192.168.2.33 | 192.168.2.62 | 192.168.2.63 |

|  |  |
| --- | --- |
| **PC0** | |
| IPv4 Address | 192.168.2.**34** {*2nd host address*} |
| Subnet Mask | 255.255.255.224 {*subnet mask determine in the Addressing table on page 2*} |
| Gateway Address | 192.168.2.**33** {*Alfa-Romeo’s Fa0/0 port ip address is the gateway for subnet #2 -* use the first host address} |

Complete the tables below by typing the missing information (do not type the period): IP address, subnet mask & gateway.

|  |  |
| --- | --- |
| **PC1** | |
| IP v4 Address | 192.168.2.\_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ |
| Gateway Address | 192.168.2.\_\_\_ |

|  |  |
| --- | --- |
| **PC2** | |
| IP v4 Address | 192.168.2.\_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ |
| Gateway Address | 192.168.2.\_\_\_ |

|  |  |
| --- | --- |
| **PC3** | |
| IP v4 Address | 192.168.2.\_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ |
| Gateway Address | 192.168.2.\_\_\_ |

|  |  |  |  |
| --- | --- | --- | --- |
| Switch1 | | Switch2 | |
| VLAN1 IP Address | 192.168.2. \_\_\_ | VLAN1 IP Address | 192.168.2. \_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ | Subnet Mask | 255.255.255.\_\_\_\_ |
| Default Gateway | 192.168.2. \_\_\_ | Default Gateway | 192.168.2. \_\_\_ |
| Switch3 | | Switch4 | |
| VLAN1 IP Address | 192.168.2. \_\_\_ | VLAN1 IP Address | 192.168.2. \_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ | Subnet Mask | 255.255.255.\_\_\_\_ |
| Default Gateway | 192.168.2. \_\_\_ | Default Gateway | 192.168.2. \_\_\_ |

|  |  |  |  |
| --- | --- | --- | --- |
| Alfa-Romeo | | Ferrari | |
| Fa0/0 IP Address | 192.168.2. \_\_\_ | Fa0/0 IP Address | 192.168.2. \_\_\_ |
| Fa0/1 IP Address | 192.168.2. \_\_\_ | Fa0/1 IP Address | 192.168.2. \_\_\_ |
| S0/0/0 IP Address | 192.168.2. \_\_\_ | S0/0/0 IP Address | 192.168.2. \_\_\_ |
| Subnet Mask | 255.255.255.\_\_\_\_ | Subnet Mask | 255.255.255.\_\_\_\_ |

STOP! Submit your answers for Part 1 now!

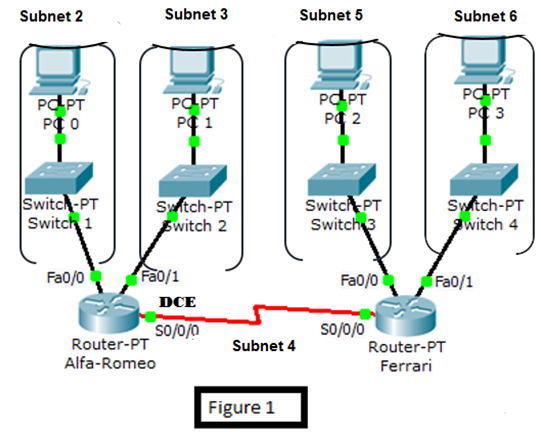
* 1. Before moving to the next part of the lab, you will submit your answer for Part 1 to ensure that your solutions are correct.
  2. Review the correct answers in Canvas for Part2. Then, proceed to the next page (Page 6).

Before going to the next page, please review the “correct” answers in Canvas (after submitting your answers, the feedback will be available)

1. Complete the User Profile BEFORE attempting the activity otherwise, you may accidently “reset” your activity.

PART 2 \*\*\* Did you verify your answers in Canvas? \*\*\*

Be sure to read chapter 11, complete the PT activity files, and Lab documents found in the online curriculum BEFORE attempting Part 2 Task 4.

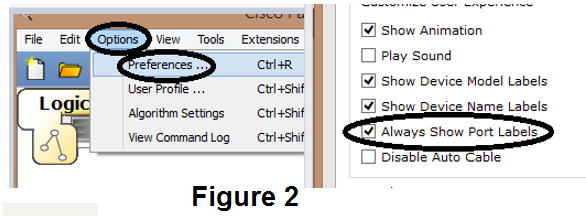


Task 1: Configure the Physical Lab Topology.

**Step 1: Physically connect devices**.

a. Cable the network devices as shown in Figure 1. Be sure to use the right cables (crossover, straight, console, etc.) and connect to the right ports, i.e.: Switch1 connected to Alfa-Romeo’s Fa0/0 port.

Figure 2 displays how to enable Port Label viewing.



b. Connect the Serial DCE cable to the S0/0/0 interface on the Alfa-Romeo router and attach the other end to Ferrari’s S0/0/0 interface. The clock rate of 56000 has been added for you.

Step 2: Visually inspect network connections

After cabling the network devices, take a moment to verify the connections. Attention to detail now will minimize the time required to troubleshoot network connectivity issues later.

Task 2: Configure the Logical Topology.

Step 1: Configure host computers. Add the IP configuration for each PC.

Step 2: Configure Switches and Routers. Use the CLI tab or console into the routers/switches. Review chapter 2 if needed. NOTE: To remove a command, place the word “no” before the command

For example to remove a hostname:  
(config)# no hostname *name*

1. Configure VLAN1 and the gateway **only on** the switches.
2. On all switches and routers, configure the hostname, the console and telnet password, the enable secret password, and create a MOTD.

**NOTE:** Alfa-Romeo’s console and telnet password will be different than the other devices. See configuration tasks below.

Configure tasks include the following:

|  |  |
| --- | --- |
| **Task** | **Specification** |
| Device hostname | (Switch1, Switch2, Switch3, Switch4, Alfa-Romeo, Ferrari) |
| Encrypted privileged exec password | class |
| **Alfa-Romeo’s Console and Telnet (0-4) password** | **cisco12345** |
| Console access password | cisco |
| Telnet access password (0-4) | cisco |
| Configure the MOTD banner. | Configured by a dedicated Cisco student! |
| Router’s interface Fa0/0 | set the Layer 3 ip address  (config)# interface fa0/0  (config-if)# ip address *{ip address} {subnet mask}*  (config-if)# no shutdown |
| Router’s interface Fa0/1 | set the Layer 3 ip address |
| Router’s interface S0/0/0 | set the Layer 3 ip address |
| All Switches’ VLAN1 | set the Layer 3 ip address |
| All Switches’ gateway ip address | set the Layer 3 ip address |

Note: At this time the Packet Tracer (PT) wizard will not grade:

* Alfa-Romeo “Encrypted privileged exec password”.
* The vty lines basic “login” command for both Switch1 and Alfa-Romeo.

Step 3: Configure both Routers.

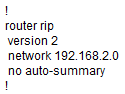
Only on both Routers, add the network address 192.168.2.0 under the RIPv2 (this will be discuss in a forthcoming chapter) routing protocol, as shown below:

Alfa-Romeo (config)# router rip

Alfa-Romeo (config-router)#version 2

Alfa-Romeo (config-router)#network 192.168.2.0

Alfa-Romeo (config-router)#no auto-summary

Verify that the RIPv2 is enable on the routers by typing the command *show run* at the privilege prompt. Hit the space bar until you see this output:  If not redo Step 3 again.

Task 3: Verify Network Connectivity.

Verify that the switches and routers are configured correctly by typing the commands *show run, show ip int brief*. Otherwise, connectivity will be broken between LANs. Network connectivity can be verified with the Windows **ping** command (PC’s Desktop – Command Prompt).

**Q2. From the command prompt, what command will display the complete IP configuration for PC0?**

Use the following table to methodically verify and record connectivity (ping) with each network device. Take corrective action to establish connectivity if a test fails:

| **From** | **To** | **IP Address** | **Ping Results** |
| --- | --- | --- | --- |
| PC0 | Gateway (Alfa-Romeo, Fa0/0) | 192.168.2.33 | successful |
| PC0 | Alfa-Romeo, Fa0/1 |  |  |
| PC0 | Switch1 VLAN1 |  |  |
| PC0 | PC1 |  |  |
| PC0 | Switch2 VLAN1 |  |  |
| PC0 | Alfa-Romeo, S0/0/0 |  |  |
| PC0 | Ferrari, S0/0/0 |  |  |
| PC0 | PC2 |  |  |
| PC0 | Switch3 VLAN1 |  |  |
| PC0 | PC3 |  |  |
| PC0 | Switch4 VLAN1 |  |  |

Note any break in connectivity. When troubleshooting connectivity issues, the topology diagram can be extremely helpful.

#### Task 4: Configure Basic Security Measures on Switch1

**Step 1: Configure SSH access on Switch1.**

Secure Shell (SSH) is a network protocol that establishes a secure terminal emulation connection to a router or other networking device. SSH encrypts all information that passes over the network link and provides authentication of the remote computer. SSH is rapidly replacing Telnet as the remote login tool of choice for network professionals. SSH is most often used to log in to a remote device and execute commands; however, it can also transfer files using the associated Secure FTP (SFTP) or Secure Copy (SCP) protocols. The network devices that are communicating must be configured to support SSH in order for SSH to function. In this lab, you will enable the SSH server on a router and then connect to that router using a PC with an SSH client installed. On a local network, the connection is normally made using Ethernet and IP.

a. Enable SSH on Switch1. Create a domain name of **CCNA-Lab.com**.

b. Create a local user database entry for use when connecting to the switch via SSH. Create a standard user account with the username **smithr** and the password **sshadmin**. By default the password will not be encrypted. You will use this username and password to SSH into the switch.

c. Configure the transport input for the vty lines 0-4 to allow SSH connections only, and to use the local database for authentication.

d. Generate an RSA crypto key using a modulus of 1024 bits.

OPTIONAL COMMANDS:

Use the command ***show crypto key mypubkey rsa***, to view the keys generated.

If you made a mistake and need to remove the keys, use the command ***crypto key zeroize rsa***

(config)#crypto key zeroize rsa

% All RSA keys will be removed.

% All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no]: yes

**Step 2: Verify the SSH configuration on Switch1.**

Using SSH client software on PC0 open an SSH connection to Switch1. On Linux or MAC OS you can use

the *ssh* command. On Windows you can use Teraterm or Putty. Since we are using Packet Tracer, use

the following command to log in with **smithr** for the username and **sshadmin** for the password.

**Note**: The option after ssh is the letter “el” not the number one.

PC0> **ssh –l smithr 192.168.2.62**

Password: **sshadmin**

*Switch1>*

Was the connection successful? Yes. If, not troubleshoot.



Go into privilege exec mode and examine the running-config.

Type **exit** to end the SSH session on Switch1.

Task 5: Configure Basic Security Measures on the *Alfa-Romeo router*

* 1. Strengthen passwords.

An administrator should ensure that passwords meet the standard guidelines for strong passwords. These guidelines could include mixing letters, numbers, and special characters in the password and setting a minimum length. The current console and vty password is cisco; the current enable secret password is class.

* + 1. Change the privileged EXEC encrypted password to: **Enablep@55**
    2. Require that a minimum of 10 characters be used for all passwords.
  1. Enable SSH connections.
     1. Assign the domain name as **CCNA-lab.com**.
     2. Create a local user database entry to use when connecting to the router via SSH. The password should meet strong password standards, and the user should have administrator-level 15 access.

**username: admin**

**password: Admin15p@55**

* + 1. Configure the transport input for the vty lines so that they accept SSH connections, but do not allow Telnet connections. The vty lines should use the local user database for authentication.
    2. Generate a RSA crypto key using a modulus of 1024 bits.
  1. Secure the console and VTY lines.
     1. You can set the router to log out of a connection that has been idle for a specified time. If a network administrator was logged into a networking device and was suddenly called away, this command automatically logs the user out after the specified time.

Configure the router to log out a line that has been idle for 5 minutes.

* + 1. Another way hackers learn passwords is simply by brute-force attacks, trying multiple passwords until one works. It is possible to prevent this type of attack by blocking login attempts to the device if a set number of failures occur within a specific amount of time

Block anyone for three minutes who fails to log in after two attempts within a two-minute period.

* 1. Verify that your security measures have been implemented correctly.
     1. From the command prompt of PC0, telnet to *Alfa-Romeo using the ip address of 192.168.2.33*.



**Q3. Critical Thinking question: Does *Alfa-Romeo* accept the Telnet connection? No. Why not? Be specific.**

* + 1. From the PC0, SSH to Alfa-Romeo: *ssh -l admin 192.168.2.33*

Does *Alfa-Romeo* accept the SSH connection? Yes. If not, troubleshoot.

Type **exit** to end the SSH session on Alfa-Romeo.

* + 1. Intentionally mistype the user and password information to see if login access is blocked after two attempts.

**Q4. What happened after you failed to login the second time?**

* + 1. From your console session **on the router**, issue the **show login** command to view the login status. In the example below, the **show login** command was issued within the 180 second login blocking period and shows that the router is in Quiet-Mode. The router will not accept any login attempts for 14 more seconds.

*Alfa-Romeo* # **show login**

A default login delay of 1 second is applied.

No Quiet-Mode access list has been configured.

Router enabled to watch for login Attacks.

If more than 2 login failures occur in 120 seconds or less,

logins will be disabled for 180 seconds.

Router presently in Quiet-Mode.

Will remain in Quiet-Mode for 14 seconds.

Denying logins from all sources.

*Alfa-Romeo* #

* + 1. After the 180 seconds has expired, SSH to *Alfa-Romeo* again and login using the **admin** username and **Admin15p@55** for the password.

**Q9. After you successfully logged in, what was displayed?**

* + 1. Enter privileged EXEC mode and use **Enablep@55** for the password.
    2. Issue the **show running-config** command at the privileged EXEC prompt to view the security settings you have applied.

For Part 2 - You will attach your PT file and the answers for Q2, Q3 and Q4.