**LAB MANUAL**

***COMPUTER NETWORKS***

**Faculty of Computing and Emerging Technologies**

**Preface**

This lab manual has been prepared to facilitate the students of software engineering in studying and implementing the layered approach in data communications, switching technologies, and protocols of networking. It will assist students in designing via simulation of various routing protocols and services, like DNS, WWW, DHCP, FTP, etc., using Cisco’s packet tracer. These labs would also be helpful to develop expertise, such as the designing, optimization, and maintenance of various types of networks. As part of the course, the labs will help learn about the planning aspect of the networks by implementing IPv4 addresses, and understanding the addressing schemes will guide students to learn about LAN (private) and WAN (public) addressing and subnetting and super-netting concepts. Similarly, students will learn about different types of LAN cables, troubleshooting a network, network devices, security implementation, and technologies to assist in the smooth running of networks and related issues.

**Tools/ Technologies**

* Crimping tool, wire stripper, Cable tester.
* Gen 8 or above PC or laptop.
* Windows 10 or higher OS.
* Cisco Packet Tracer latest ver.

Note: Students may register him/herself on the Cisco web site using a link <https://id.cisco.com/>. Similarly, it is recommended that a student download the latest version from the site too.

# About Packet Tracer

Packet Tracer is a simulation, visualization, collaboration, and assessment tool for teaching networking. It allows students to construct their model or virtual networks, obtain access to important graphical representations of those networks, animate those networks by adding their own data packets, ask questions about those networks, and finally annotate and save their creations.

**TABLE OF CONTENTS**

[Preface i](#_bookmark33)

[Tools/ Technologies i](#_bookmark34)

[About Packet Tracer i](#_bookmark35)

[LAB 1: Preparing Ethernet Cables 1](#_bookmark36)

[LAB 2: Understanding Network Commands 10](#_bookmark37)

[LAB 3: IP Addressing and Subnetting 20](#_bookmark38)

[LAB 4: Configuring Basic Switch and Router 27](#_bookmark39)

[LAB 5: Securing the Switch and Router 37](#_bookmark40)

[LAB 6: Virtual LAN (VLANs) 44](#_bookmark41)

[LAB 7: Cisco Discovery Protocol (CDP) and Servers 54](#_bookmark42)

[LAB 8: Switch Redundant connections and Loops (STP) 66](#_bookmark43)

[LAB 9: Configuring Static Routing 68](#_bookmark44)

[LAB 10: Configuring WAN Connection and Default Routes 70](#_bookmark45)

[LAB 11: Setting up Dynamic Routing Protocol RIP ver.1 74](#_bookmark46)

[LAB 12: Implementing Router Information Protocol (RIP) ver. 2 78](#_bookmark47)

[LAB 13: Open-Ended Lab 80](#_bookmark48)

[LAB 14: Lab Project 81](#_bookmark49)

[Appendix ‘A’ Writing a Lab Report 82](#_bookmark50)

[Appendix ‘B’ Evaluation Rubrics 86](#_bookmark51)

# LAB 1: Preparing Ethernet Cables

**Objectives**

* Understand different types of communication cables for LAN.
* How to wire Ethernet cables and connect them to RJ45 jacks.
* Understand the color combinations of UTP cables.
* Understand the limitations of the UTP cables.
* How to use the tools to prepare the Ethernet cables.

**Tools required: -**

* Cable - bulk Category 5e, 6 and 6e
* Wire Cutters - to cut the cable if necessary.
* Wire Stripper - to strip the cable if necessary.

**For Patch Cables (connect switches):**

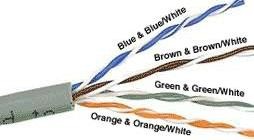
* RJ45 Plugs
* RJ45 Crimper

**For Fixed Wiring:**

* RJ45 Jacks

**Recommended:**

* Wire Stripper
* Cable Tester
  + 1. **Introduction: About the Cable**

You can find bulk supplies of the cable at many computer stores or most electrical or home centers. UTP (Unshielded Twisted Pair) Category 5e cables are used for basic 10/100 Mbps functionality and CAT 5e and 6 for gigabit also called 1000BaseT operation, and CAT 7 gives you a measure of future-proofing with 10

gigabits per second transmission.

Bulk cable comes in many types, and there are two basic categories, solid and braided cable. Braided cable tends to work better in patch applications for desktop use. It is more flexible and resilient than solid cable and easier to work with but meant for shorter lengths. Solid cable is meant for longer runs in a fixed position.

The plenum-rated cable must be used whenever the cable travels through an air circulation space, for example, above a false ceiling or below a raised floor. It may be difficult or impossible to tell from the package what type of cable it is, so peal out an end and investigate and look inside the cable. Usually, there are eight color-coded wires. These wires are twisted into four pairs of wires, and each pair has a common color theme. Plenum-rated (CMP) cable has an outer jacket made of fire-resistant material like Teflon to prevent fire from

spreading. When a fire happens, plenum-rated cable is designed to: Restrict flame propagation to no more than five feet. Limit the amount of harmful smoke released

One wire in the pair is a solid or primarily solid-colored wire, and the other is a primarily white wire with a colored stripe. Examples of the naming schemes used are Orange (alternatively Orange/White) for the solid-colored wire and White/Orange for the striped cable. The twists are extremely important. Twisting is there to counteract noise and interference.

* + - 1. **Preparing a cable**

It is important to wire according to a standard to get proper performance from the cable. The TIA/EIA-568-A specifies two wiring standards for an 8 or 4-position modular connector such as RJ45 also known as 8P4C (100Mbps) or 8P8C (1000Mbps). The two wiring standards, T568A and T568B vary only in the arrangement of the colored pairs.

Your choice might be determined by the need to match existing wiring, jacks, or personal preference, but you should maintain consistency. I've shown connections of 568B standard in Figures 1.4 and 1.5 for straight-through and crossover cabling. But before we jump into standards, the next section will focus on some important details first.

* + - 1. **Cable pairs by color coding**

Each twisted pair of cabling in the UTP cable is color-coded for easy identification. In North America, each wire in a twisted pair is identified by one of 5 colors: blue, orange, green, brown, or slate (gray). Then this copper wire is paired with a different wire from the other color group made up of white, red, black, yellow, or violet. Usually, one copper wire in a twisted pair is solid-colored, and the second one is striped with the color of its mate. Ex: A solid blue- colored copper cable is paired with a white and blue striped copper cable. It will make it easy to identify and match them. Alexander Graham Bell invented this twisted pair of cabling in 1881.

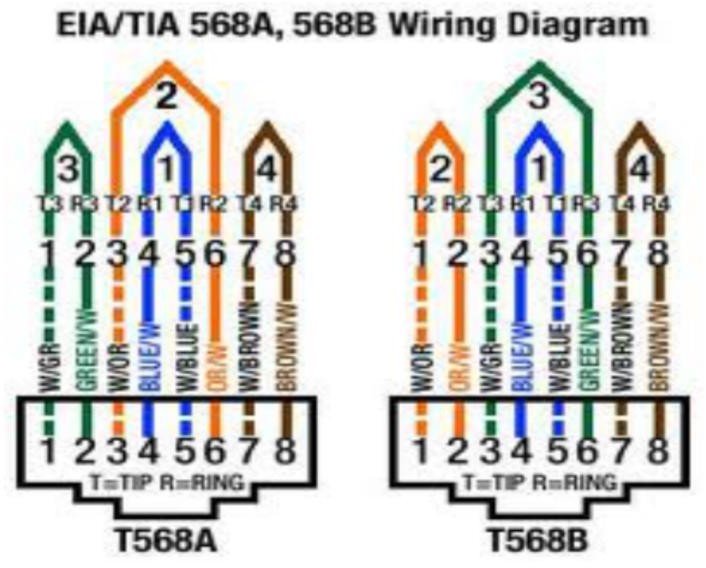


Fig 1.0 UTP color pairs and 568A and 568B standards

* + 1. **Introduction to RJ45 Plugs or Jacks:**

An 8-pin/8-position plug or jack is commonly used to connect computers to Ethernet-based local area networks (LAN), as shown in Figure 1.1. There are a couple of variations available. The primary variation students need to pay attention to is whether the connector is intended for braided or solid wire.

For braided/stranded wires, the connector has sharp pointed contacts that pierce the wire.

For solid wires, the connector has fingers that cut through the insulation and contact the wire by grasping it from both sides.

The connector is the **weak point** in an ethernet cable; choosing the wrong one will often cause grief later. If you just walk into a computer store, it's nearly impossible to tell what type of plug it is. You may be able to determine what type it is by crimping one without a cable.

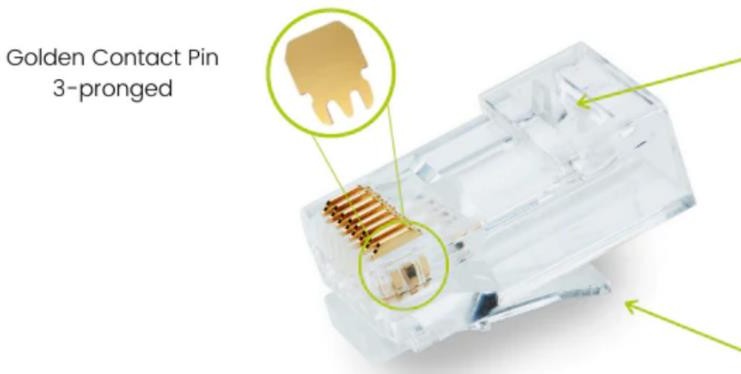


Figure 1.1 RJ45 Plug or Jack

RJ45 jacks come in a variety of styles intended for several different mounting options. The choice is one of the requirements and preferences. RJ45 jacks are designed to work only with solid cable. Most jacks come labeled with color codes for either T568A, T568B, or both.

* + 1. **Forms of Ethernet Cables - Crossed and Straight cables: When to use them**

The following diagram shows the Normal use of Crossed and Straight cables (see figure 1.2).

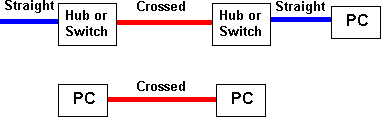


Figure 1.2 Type of ethernet cables

Notes:

1. We show Straight cables as **BLUE** and Crossed as **RED**. That is our convention; the cable color can be anything you choose or, more likely, the vendor decides.
2. To avoid the need for Crossed cables, many vendors provide **UPLINK** ports on Hubs or Switches - these are specially designed to allow the use of a STRAIGHT cable when connecting back-to-back Hubs or Switches. Read the manufacturer's documentation carefully.
   * 1. **Ethernet Cable Pin Outs and Connections**

There are two basic cable pinouts. A straight-through cable is used to connect to a hub or Switch, and a crossover cable is used to operate in a peer-to-peer fashion without a hub/switch. Generally, all fixed wiring should be run straight through. Some ethernet interfaces can cross and un-cross a cable automatically as needed, a handy feature.

*NOTE: Standard, Straight-Through Wiring (both ends are the same):*

Let's first learn how to find the PIN No. of the Connector. Make sure you identify and start with the correct Pin.

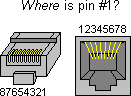


Figure 1.3 Pinout of connector

* + 1. **What Is Straight Through Cable?**

A straight-through cable is a type of twisted pair cable that is used in local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straight-through cable uses one wiring standard: both ends use the T568A wiring standard, or both ends use the T568B wiring standard. The following figure shows a straight-through cable of which both ends are wired as the T568B standard.

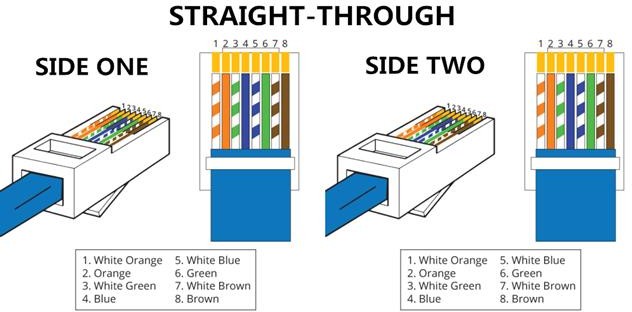


Figure 1.4 Straight-Through cable connections

* + 1. **What Is Crossover Cable?**

A crossover Ethernet cable is a type of Ethernet cable used to connect computing devices directly. Unlike straight-through cable, the RJ45 crossover cable uses two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g., two computers (via network interface controller) or two switches to each other.

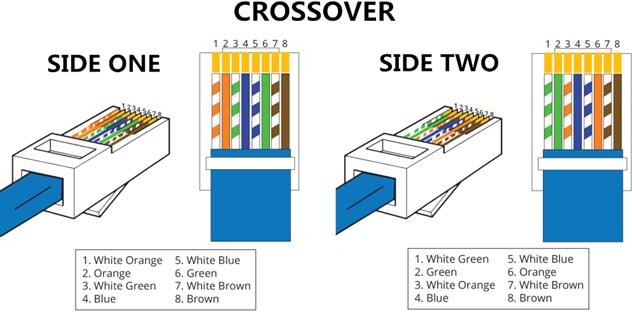
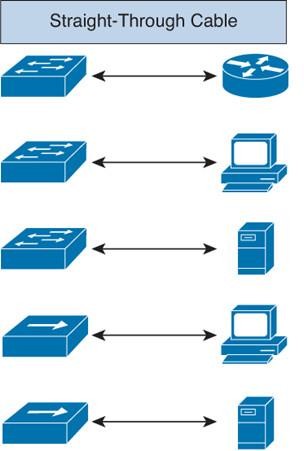
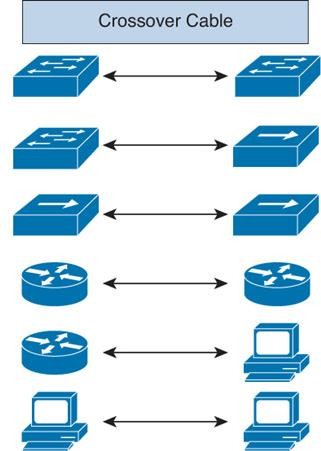


Figure 1.5 Crossover Cable

* + 1. **Straight Through vs. Crossover Cable, which to choose?**

Straight through vs. crossover cable, which one should I choose? Usually, straight-through cables are primarily used for connecting, unlike devices. And crossover cables are used for connecting like devices.

Use **straight-through** Ethernet cable for the following cabling:

* Switch to Router
* Switch to PC or server
* Hub to PC or server

Use **crossover** cables for the following cabling:

* Switch to switch
* Switch to Hub
* Hub to Hub
* Router to Router
* Router Ethernet port to PC NIC
* PC to PC
  + 1. **Pin Out Tables for ethernet and fast ethernet connection**

**s**

**Straight-Through Cable Pin Out for T568A (8P8C)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RJ45 Pin # | Wire Color (T568A) | Wire Diagram (T568A) | 10Base-T Signal 100Base-TX Signal | 1000Base-T Signal |
| 1 | White/Green | white/green | Transmit+ | BI\_DA+ |
| 2 | Green | green | Transmit- | BI\_DA- |
| 3 | White/Orange | white/orange | Receive+ | BI\_DB+ |
| 4 | Blue | blue | Unused | BI\_DC+ |
| 5 | White/Blue | white/blue | Unused | BI\_DC- |
| 6 | Orange | orange | Receive- | BI\_DB- |
| 7 | White/Brown | white/brown | Unused | BI\_DD+ |
| 8 | Brown | brown | Unused | BI\_DD- |

**Straight-Through Cable Pin Out for T568B (8P8C)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RJ45 Pin # | Wire Color (T568B) | Wire Diagram (T568B) | 10Base-T Signal 100Base-TX Signal | 1000Base-T Signal |
| 1 | White/Orange | white/orange | Transmit+ | BI\_DA+ |
| 2 | Orange | orange | Transmit- | BI\_DA- |
| 3 | White/Green | white/green | Receive+ | BI\_DB+ |
| 4 | Blue | blue | Unused | BI\_DC+ |
| 5 | White/Blue | white/blue | Unused | BI\_DC- |
| 6 | Green | green | Receive- | BI\_DB- |
| 7 | White/Brown | white/brown | Unused | BI\_DD+ |
| 8 | Brown | brown | Unused | BI\_DD- |

**Cross Over Cable (T568B):**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| RJ45  Pin # (END 1) | Wire Color | Diagram End #1 | RJ45  Pin # (END 2) | Wire Color | Diagram End #2 |
| 1 | White/Orange | white/orange | 1 | White/Green | white/green |
| 2 | Orange | orange | 2 | Green | green |
| 3 | White/Green | white/green | 3 | White/Orange | white/orange |
| 4 | Blue | blue | 4 | White/Brown | white/brown |
| 5 | White/Blue | white/blue | 5 | Brown | brown |
| 6 | Green | green | 6 | Orange | orange |
| 7 | White/Brown | white/brown | 7 | Blue | blue |
| 8 | Brown | brown | 8 | White/Blue | white/blue |

**Note:** The crossover cable layout is suitable for 1000Base-T operation; all four pairs are crossed.

* + 1. **How to wire Ethernet Patch Cables:**

1. Strip off about 2 inches of the cable sheath.
2. Untwist the pairs - don't untwist them beyond what you have exposed; the more untwisted cable you have, the worse the problems you can run into.
3. Align the colored wires according to the diagrams above.
4. Trim all the wires to the same length, about 1/2" to 3/4" left exposed from the sheath.
5. Insert the wires into the RJ45 plug - make sure each wire is fully inserted into the front of the RJ45 plug and in the correct order. The sheath of the cable should extend into the RJ45 plug by about 1/2" and will be held in place by the crimp.
6. Crimp the RJ45 plug with the crimper tool.
7. Verify the wires ended up in the right order and that the wires extend to the front of the RJ45 plug and make good contact with the metal contacts in the RJ45 plug
8. Cut the cable to length - make sure it is more than long enough for your needs.
9. Repeat the above steps for the second RJ45 plug.
   * 1. **How to wire fixed Ethernet Cables:**
10. Run the full length (Max 100 meters) of cable in place, from endpoint to endpoint, making sure to leave excess.
11. At one end, cut the wire to length, leaving enough length to work but not too much excess.
12. Strip off about 2 inches of the cable sheath.
13. Align each of the colored wires according to the layout of the jack.
14. Use the punch-down tool to insert each wire into the jack.
15. Repeat the above steps for the second RJ45 jack.
    * 1. **Precautions While Preparing Cable**

If a cable tester is available, use it to verify the proper connectivity of the cable. That should be it; if your cable doesn't turn out, look closely at each end and see if you can find the problem. Often a wire ends up in the wrong place, or one of the wires is making no contact or poor contact.

Also, double-check the color coding to verify it is correct. If you see a mistake or problem, cut the end off and start again. A cable tester is invaluable at identifying and highlighting these issues.

When sizing cables, remember that an end-to-end connection should not extend more than 100m (~328ft). Try to minimize the cable length; the longer the cable becomes, the more it may affect performance. This is usually noticeable as a gradual decrease in speed and increase in latency.

* + 1. **Ethernet Technologies**

In computer networking, Fast Ethernet physical layers communicate at the nominal rate of 100 Mbps, whereas, its successor Ethernet speed was originally 10 Mbit/s.

* + - 1. **Ethernet over Twisted pair cables**

An Ethernet cable is a common type of network cable used with wired networks. Ethernet cables connect devices such as PCs, routers, and switches within a local area network.

These physical cables are limited by length and durability. If a network cable is too long or of poor quality, it won't carry a good network signal. These limits are one reason different types of Ethernet cables are optimized to perform certain tasks in specific situations.

**100BASE-TX** and **100BASE-T4,** are the technical name of Fast Ethernet over twisted pair cables. It is a predominant form of Fast Ethernet carrying data traffic at 100 Mbps (Mega bits per second) in local area networks (LAN). 100 Mbps, BASE denoted the use of baseband transmission, and TX and T4 denote the use of twisted pair cables in Fast Ethernet.100 Mbps, where T4 denotes the use of four twisted pair cables in Fast Ethernet.

**Ethernet over Fiber optic cables**

**100BASE-FX** is the technical name of Fast Ethernet over fiber optic cables. 100 Mbps, BASE denoted the use of baseband transmission, and FX denotes the use of optical fibers in Fast Ethernet.

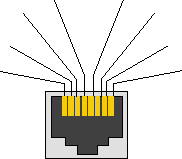
All the above standards of Ethernet are launched as the IEEE 802.3u standard in 1995. Here, 100 is the maximum throughput, i.e.

**Lab Task (Part A)**

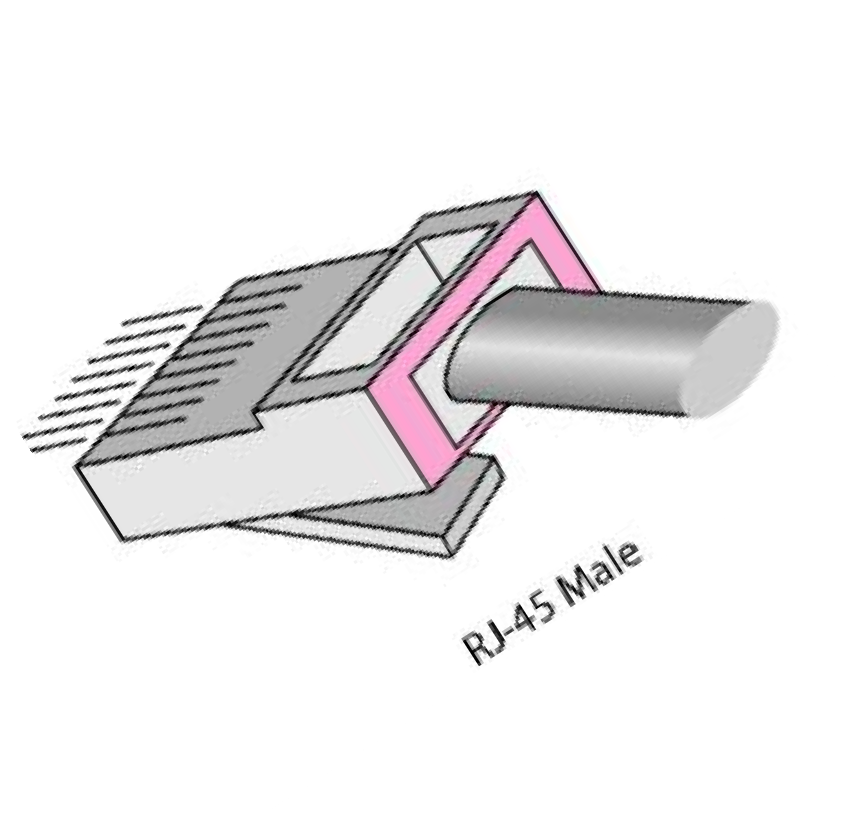
During the lab, a student has to take pictures of the tools they are using and the procedure of preparing the cable and preparing the report task.

**Lab Task (Part B)**

1. Prepare the ethernet cable during the lab. Explain the steps and attach the pictures of the equipment and steps performed with the Lab 1 report.
2. Perform the Lab task and attach it along with the lab report while submitting.
3. Identifying the pins on the RJ45 male connector, which are used for transmission of 100 Mbps.

**Identify The Color Pairs**

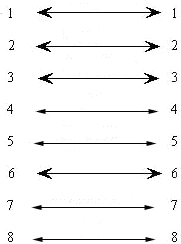
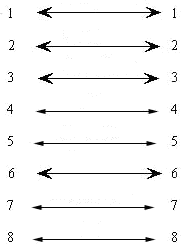
PAIR NO 1 PAIR NO 2 PAIR NO 3 PAIR NO 4

1. Correctly number the pins of the jack
2. Label the pins according to

the color coding schemes

1. Provide a correct color code of the connector for 568b standard.

Straight Cable Cross Cable



# LAB 2: Understanding Network Commands

**Objectives**

* + Gather information including connection, hostname, Layer 2 MAC address, and Layer 3 TCP/IP network address information.
  + Compare network information to other PCs on the network.
  + Learn to use the TCP/IP Packet Internet Groper (ping) command from a workstation.
  + Learn to use the Trace Route (tracert) command from a workstation.
  + Observe name resolution occurrences using WINS and/or DNS servers.

1. **Introduction**

This lab assumes the use of command prompt Windows 10 and above. This is a non-destructive lab and can be done on any machine without concern about changing the system configuration. Ideally, this lab is performed in a Computer Lab or other LAN environment that connects to the internet.

The commands help us to diagnose the LAN environment and troubleshoot the network. The following command will be used to practice during the lab, Ensuring the computer has an IP address:

1. **Ping**
2. **Trace Route**
3. **ARP**

NOTE: The command prompt (CMD) is displayed in black color. Students are advised **not** to use the black background diagrams in reports, instead change the color and then paste figures.

**How to change the color of COMMAND PROMPT**

1. COLOR**XY** - Specifies color attribute of console output
2. Color attributes are specified by TWO hex digits -- the first corresponds **X** to the background; the second **Y** is the foreground.
3. Each digit can be any of the following values:



To change the color of the CMD use the following command

*C:\Users\Hasan Shah>COLOR F0*

1. **Understanding the computer’s Local area connections**

**Step 1 Connect to the Network**

Establish and verify connectivity to the internet using a network device like a switch or router. This ensures the computer has an IP address.

**Step 2 Gather TCP/IP configuration information**

Use the Start menu to open the Command Prompt, an MS-DOS-like window.

**Press** Windows + R **Key, Then type cmd.**

**Task 1 IPCONFIG**

Type ipconfig and press the Enter key. The spelling of **ipconfig** is critical, while the case is not. It is short for IP Configuration.

This first screen shows the IP address, subnet mask, and default gateway. The IP address and the default gateway should be in the same network or subnet. Otherwise, this host would not be able to communicate outside the network. In figure 2.1, the subnet mask tells us that the first three octets must be the same to be in the same network. Further understanding of IP addresses shall be taught in Lab 3.

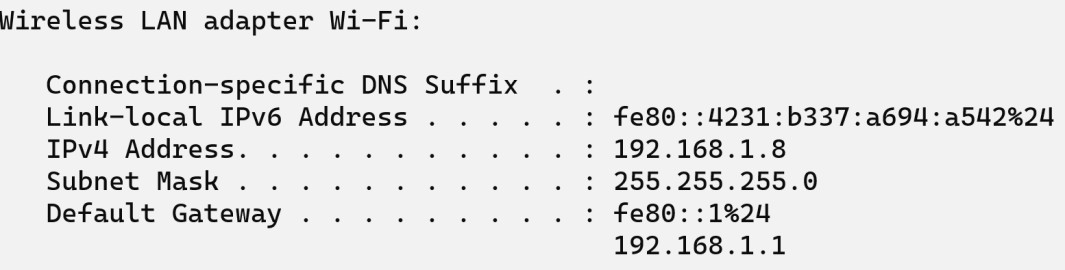


Figure 2.1 IPconfig command

**Note**: If this computer is on a LAN, the default gateway might not be seen, if it is running behind a Proxy Server. Record the following information for this computer.

**Record the following TCP/IP information for this computer**

IP address:

Subnet Mask:

Default Gateway:

Record a couple of the IP Addresses:

**Task 2 Check additional TCP/IP configuration information**

To see detailed information, type **ipconfig /all** and press **Enter**.

Figure 2.2 shows the detailed IP configuration screen of multiple Ethernet adaptors connected to the Computer. Choose an adaptor accordingly.

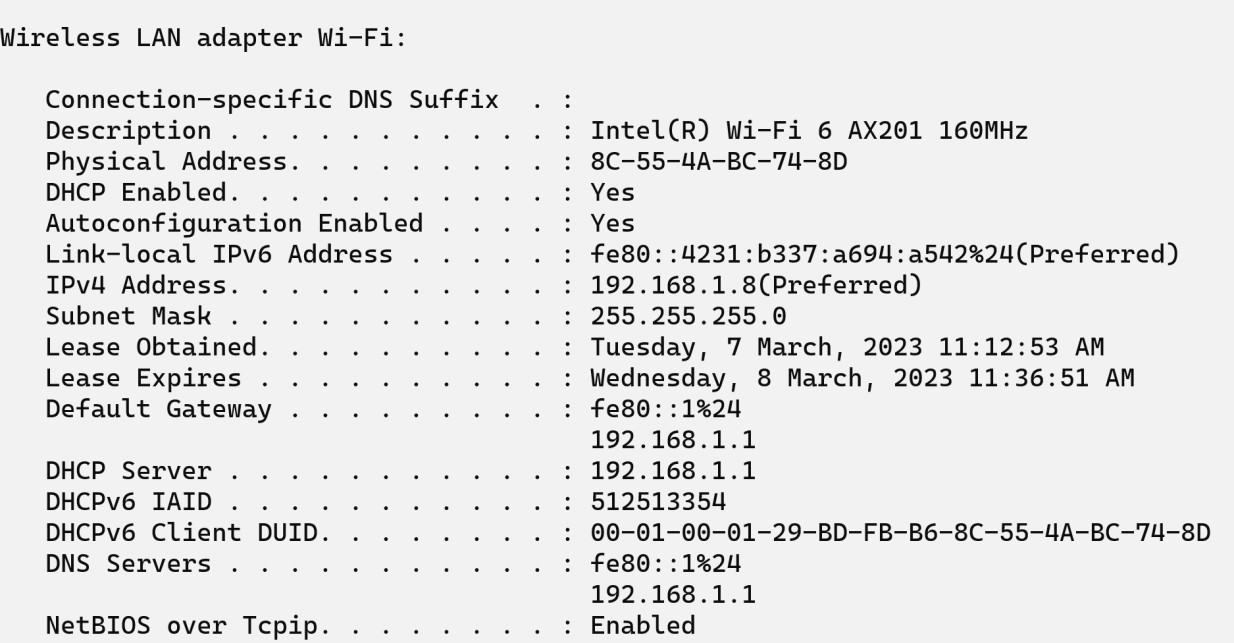


Figure 2.2 Ipconfig /all

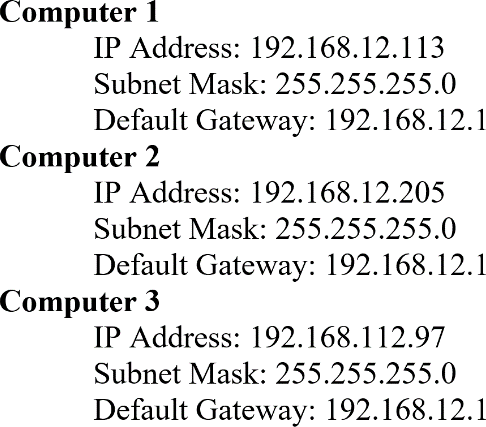
Figure 2.2 shows WiFi adaptor information. It shows the IP address of the machine, its subnet mask, its MAC address (Physical addresses) including the DHCP server address, and the date the IP lease starts and ends should be displayed. Looking over the information we can see the Default gateway entry to connect to the internet.

**Close the screen**

Close the screen when finished examining network settings. Repeat the previous steps as necessary.

**Reflection**

Based on the above observations, what can be deduced about the following results taken from three computers connected to one Switch?

Should they be able to talk to each other? Are they all on the same network?

Why or why not? If something is wrong, what is most likely the problem

1. ICMP commands "ping" and "tracert "

**Objective**

* Learn to use the TCP/IP Packet Internet Groper (ping) command.
* Learn to use the Trace Route (tracert) command.

**PING Background**

This lab assumes the use of any Windows 10 and above version. This is a non-destructive lab and can be done on any machine without concern about changing the system configuration. Ideally, this lab is performed in a LAN environment that connects to the internet. It can be done from a single remote connection via a modem or DSL-type connection. The student will need the IP addresses that were recorded in the previous part of the lab.

**Step 1 Establish and verify connectivity to the internet**

This ensures the computer has an IP address.

**Step 2 Access the command prompt**

As accessed in the previous part of the lab. Press the windows button and type **cmd**

**Task 1**

**Ping the IP address of another computer**

In the CMD window, type **ping**, a space, and the IP address of a computer recorded in the previous lab. The following figure shows the successful results of **ping** to this IP address.

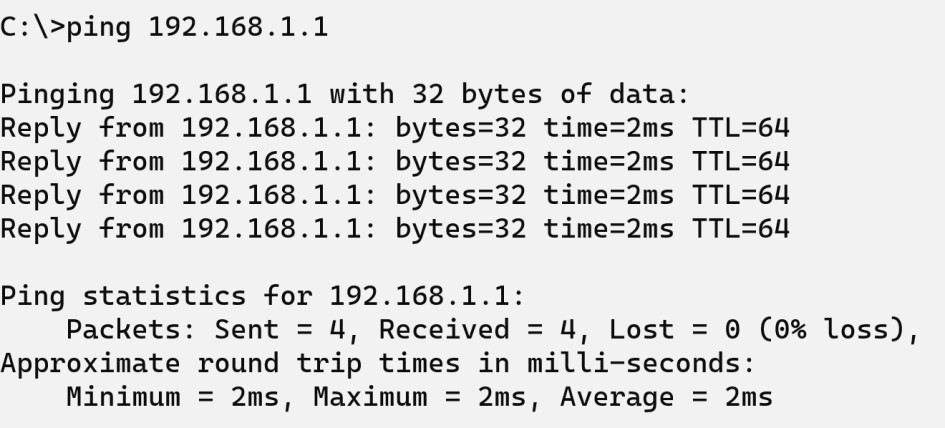


Figure 2.3 Ping Command reply

**ping** uses the ICMP echo and reply feature to test physical connectivity. Since the **ping** reports four attempts, it indicates the reliability of the connection. Look over the results and verify that the **ping** was successful.

Is the **ping** successful?

**Step 4 ping the IP address of the default gateway**

Try to ping the IP address of the default gateway if one was listed in the last exercise. If the ping is successful, it means there is physical connectivity to the Router on the local network and probably the rest of the world.

**Step 5 ping the IP address of a DHCP or DNS servers**

Try to **ping** the IP address of any DHCP and/or DNS servers listed in the last exercise. If this works for either server, and they are not in the network,

What does this indicate?

Was the ping successful?

**Step 6 ping the Loopback IP address of this computer**

Loopback address helps to identify if the NIC of the computer is working fine or if it is faulty. Type the following command: ping 127.0.0.1

The 127.0.0.0 network is reserved for loopback testing. If the ping is successful, then TCP/IP is properly installed and functioning on this computer.

Was the ping successful?

**Step 7 ping the hostname of another computer**

Try to **ping** the hostname of the computer that was recorded in the previous lab. The figure shows the successful result of the **ping** of the hostname.

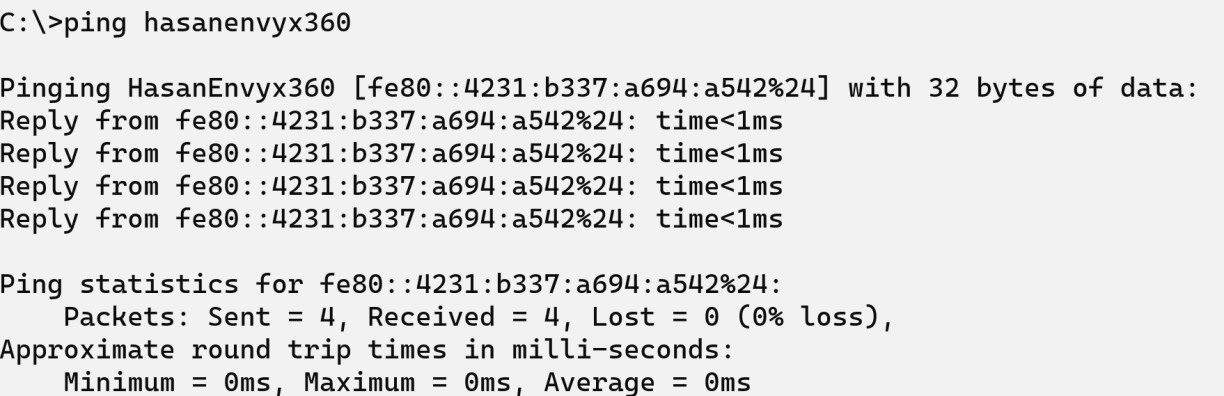


Figure 2.4 Pinging hostname

Look over the results. Notice that the first line of output shows the hostname, m450, in the example, followed by the IP address. This means the computer was able to resolve the hostname to an IP address. Without name resolution, the **ping** would have failed because TCP/IP only understands valid IP addresses, not names.

If the **ping** was successful, it means that connectivity and discovery of IP addresses can be made with only a hostname. This is how many early networks communicated. If successful, then **ping** a hostname also shows that there is probably a WINS server working on the network.

**Step 8 ping the Cisco website** Type the following command: **ping** [**www.cisco.com**](http://www.cisco.com/)

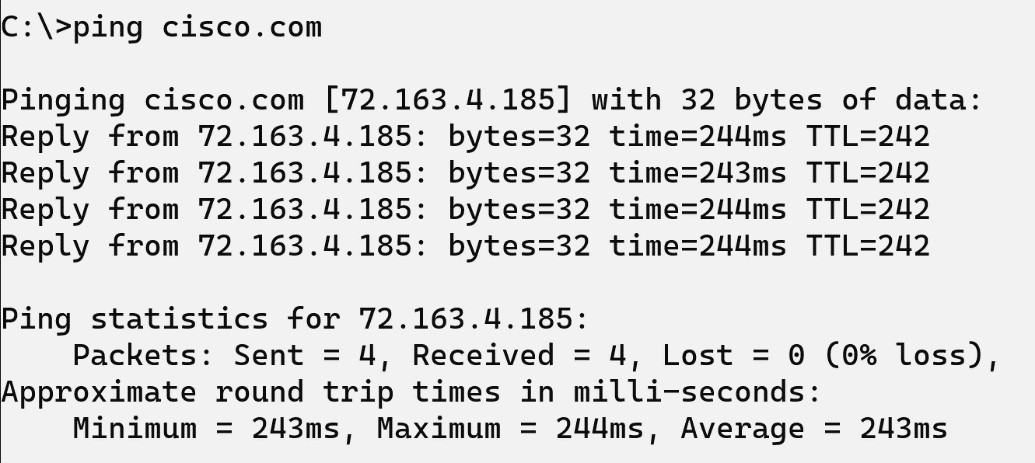


Figure 2.5 Ping Cisco.com

The first output line shows the Fully Qualified Domain Name (FQDN) followed by the IP address. A Domain Name Service (DNS) server somewhere in the network was able to resolve the name to an IP address. DNS servers resolve domain names, not hostnames, to IP addresses. Without this name resolution, the ping would have failed because TCP/IP only understands valid IP addresses. It would not be possible to use the web browser without this name resolution.

With DNS, connectivity to computers on the internet can be verified using a familiar web address, or domain name, without having to know the actual IP address. If the nearest DNS server does not know the IP address, the server asks for a DNS server higher in the Internet structure.

**Step 9 ping the Microsoft website**

Type the following command: ping [www.microsoft.com](http://www.microsoft.com/)

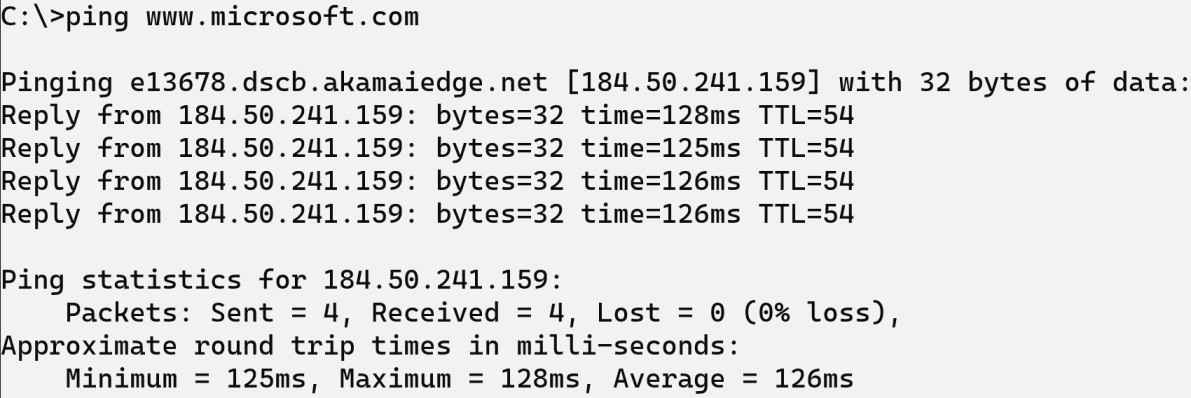


Figure 2.6 Ping [www.Microsoft.com](http://www.Microsoft.com/)

Notice that the DNS server was able to resolve the name to an IP address, but there is no response.

Some Microsoft routers are configured to ignore ping requests. This is a frequently implemented security measure.

**Ping** some other domain names and record the results. For example, **ping** [**www.msn.de**](http://www.msn.de/)

Trace the route to the Cisco website

**Step 1:** Type tracert [**www.cisco.com**](http://www.cisco.com/)and press **Enter**.

**Tracert** is TCP/IP abbreviation for traceroute. The preceding figure shows the successful result when running a **tracert** from Bavaria in Germany. The first output line shows the FQDN followed by the IP address. Therefore, a DNS server was able to resolve the name to an IP address. Then there are listings of all routers the **tracert** requests had to pass through to get to the destination.

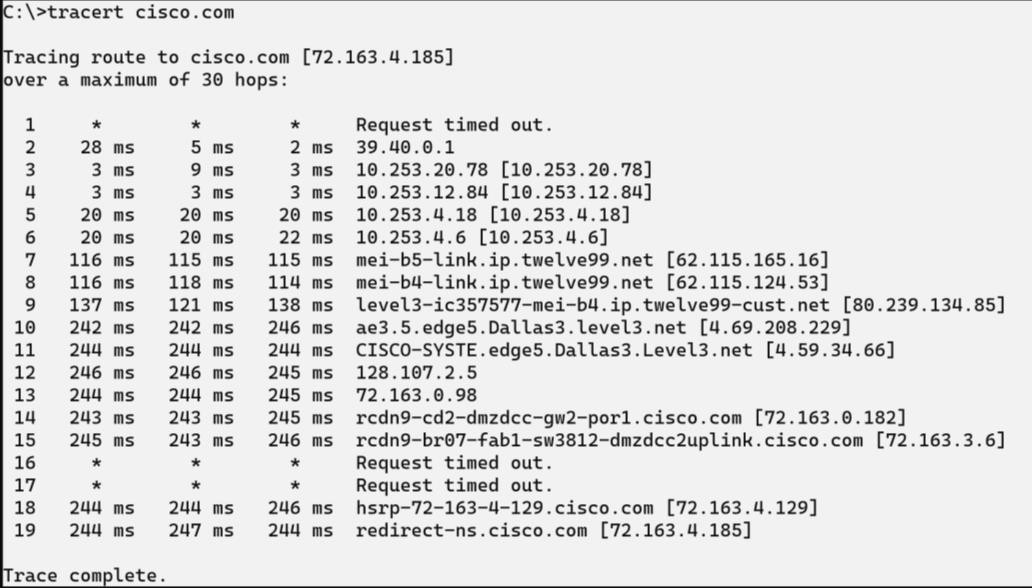
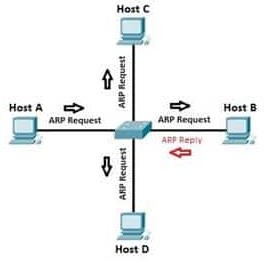


Figure 2.6 Tracert to Cisco.com

Tracert uses the same echo requests and replies as the ping command but in a slightly different way. Observe that tracert contacted each Router three times. Compare the results to determine the consistency of the route. Notice in the above example that there were relatively long delays after routers 11 and 13, possibly due to congestion. The main thing is that there seems to be a relatively consistent connection.

1. What is the ARP command?

**ARP** stands for “Address Resolution Protocol” and is a protocol for mapping an IP address to a physical MAC address on a local area network.

ARP is a program used by a computer system to find another computer’s MAC address based on its IP address. Now you have a question “why do we need MAC address?”

The reason is simple, any local communications would use a MAC address, not an IP address.

When a computer wants to communicate with another computer on a different network, the IP address would be used. The IP address is like your mailing address while the MAC address is like your name. On a TCP/IP network, every computer is assigned an IP address, and some local server’ IP addresses are also given to a network client. Now you’re probably wondering – “How often does your computer use ARP?”.

**To demonstrate how ARP works let’s take an example.**

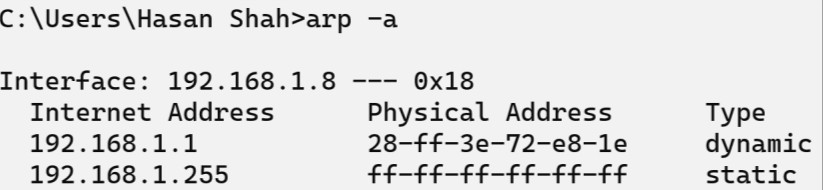
On a local area network, a client computer tries to contact a server. Here we are talking about communication between two computers on the same broadcast domain means a local area network. First, the client checks its ARP cache.

ARP cache is a table of IP addresses with their corresponding MAC addresses.

To view a Windows computer’s ARP table, open a command prompt and enter the following command:

*C:\Users\Hasan Shah>arp -a*

You can see your computers ARP table in the following output:



The first column is the IP address, and the second column is corresponding to the MAC address.

The ARP entry is either static or dynamic. **Static ARP** entry is manually added to the ARP cache table. **Dynamic entries** are what the ARP program gets. They stay there until the ARP cache timeout has expired. Suppose no entry has been found for the server, the client computer will use ARP to send a message through the whole network.

This is a broadcast message to the local network that says who has the IP address so and so, and whats your MAC address. When a server hears the broadcast message, they respond “yes” I have that IP address, and here is my MAC address.

Now, let’s Break down the ARP Process Step by Step:

* 1. The client sends a broadcast message because the destination MAC address is a broadcast address. Simply saying hello! anyone has an IP address 192.168.1.8 if you hear me would you please give me your MAC address?, and here are my IP address and MAC address. Other devices hear the broadcast message and discard the ARP packet silently.
  2. When a server hears the message, it sends a unicast message to the client because the destination MAC address and IP address belong to the client.
  3. The client cache the server's MAC address. At the same time, the client updates its cache table for future reference.

**ARP Summary**

It is a layer 2 protocol that uses a layer 3 IP address to find the layer 2 MAC address.

It operates on a LAN or the same broadcast domain because ARP relies on broadcasting. It uses the ARP table.

**ARP Announcements**

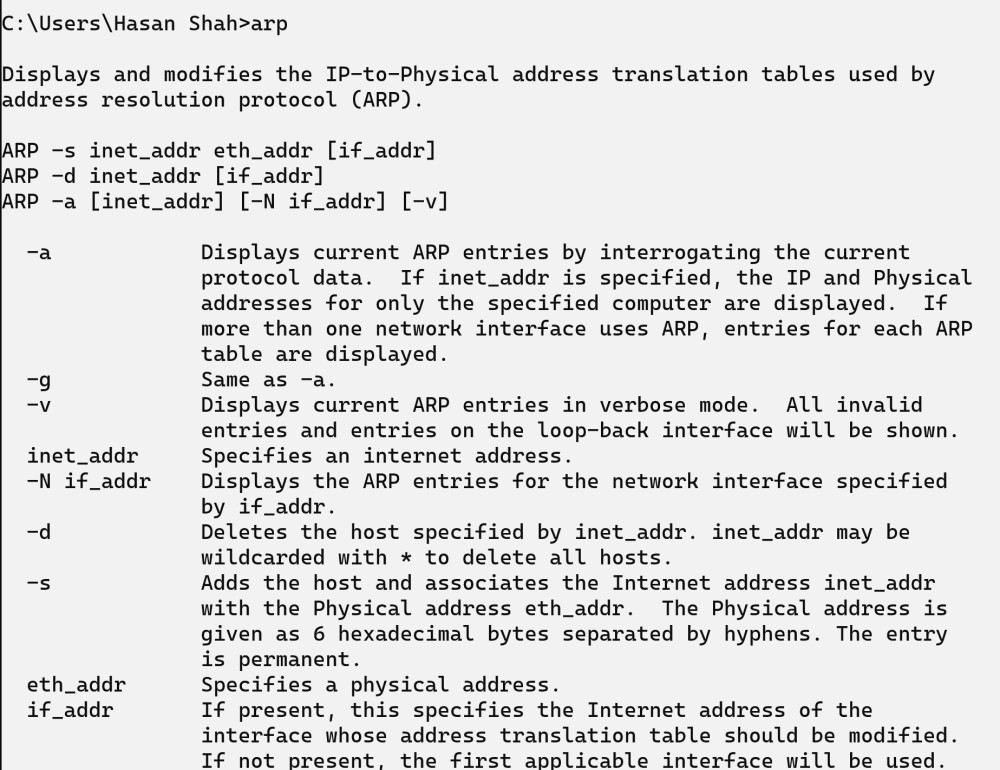
ARP Announcements are a way to officially “claim” the IP address on the network.

ARP announcement to update other hosts' ARP tables without the need for an ARP request. It helps update the network faster when there was a recent change to a host's IP address.

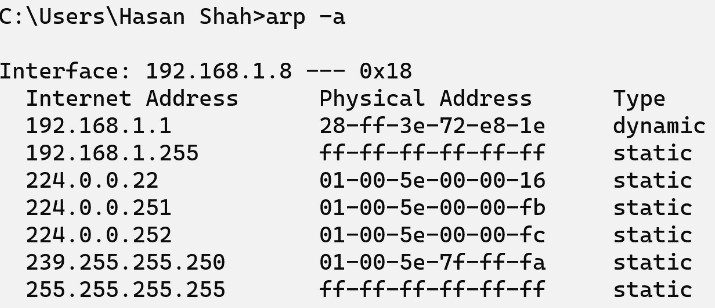
**How to Use ARP**

ARP Command is a TCP/IP utility used for viewing and modifying the local Address Resolution Protocol (ARP) cache.

ARP Cache contains recently resolved MAC addresses of Internet Protocol (IP) hosts on the network. Run ARP command without any arguments will display a list of the command’s parameters.

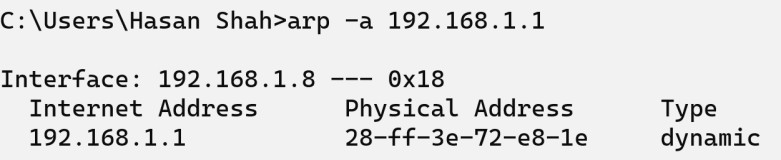


You can display the complete ARP cache by running the following command:

*arp -a*

You should see the following output:

You can also find the ARP cache entry for a specific IP address by specifying the IP address with the arp command:



**Lab Task**

1. Test the NIC of the PC - Ping 127.0.0.1 called (Loopback address)
2. Ping the default gateway.
3. Ping your hostname.
4. Ping the DNS server(s)

Do you get a positive reachability result?

1. How to obtain the following network configuration on your computer.

Host Name: MAC Address: IP Address: Subnet Mask: Default Gateway:

DHCP Servers:

1. Open a web browser and visit the following website: <http://whatismyipaddress.com/> Is the reported IP address consistent with that obtained by ipconfig? If not, why?
2. Perform ARP and report dynamic addresses
3. Identify the computer names of the dynamic addresses and perform ARP using computer names.

# LAB 3: IP Addressing and Subnetting

**Objectives**

* + To undersrtand IP ver 4.
  + Learning the concept of subnetting.
  + Study fixed length and variable length subnetting in IPV4.
  + Learn about local, global, default route, loopback, and APIPA addresses.

**Tools required**

Advance IP subnet calculator for windows

* 1. **Introduction to IP**

The specifications of the Internet Protocol (IP) were set up by RFC791 in 1982. Some contents of the specifications stipulate the structure of IP addresses. The structure provides each host and router interface with 32-bit binary logical addresses, including the **N**etwork part and the **H**ost part, sometimes written as N.N.N.H or represented by Subnet Mask.

For easy writing and remembering, one IP address is usually expressed by 4 decimal digits within 0~255, with a period separating each adjacent two digits. Each of these decimal digits represents 8 bits of the 32-bit address, namely the so-called octet. This is called dotted decimal notation, as shown in Figure 3.1.

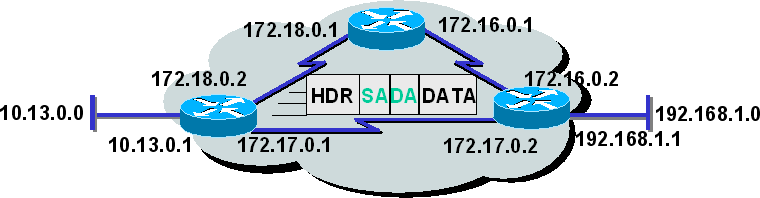


Fig. 3.1 IP Addresses

* 1. **Classification of IP Addresses**

The address types are classified according to network scale, shown as following allows:

Class A: super-large networks

Class B: medium-size networks of the limited number Class C: a small-size network of a large number

Class D Special class: (for multi-point transmission) and Class E, usually for test and research purposes

Types of IP addresses can be determined by way of checking the first octet in the address (the most important). The highest bit value determines the type of address. The bit format also defines the decimal value range of the octet related to each address type.

**Class A:**

For class A addresses, 8 bits are assigned to the network address, and the other 24 bits are assigned to the host address, represented as N.H.H.H. If the most significant bit of the first octet is 0, the address is a class A address.

This corresponds to the possible octet of 0~127. Among these addresses, 0 and 127 are reserved, so the actual value range is 1~126. Among type A addresses, only 126 networks can be used. Since only 8 bits are reserved for the network address, the first bit must be 0. However, the digits for a host can be 24 bits, so, each network can support up to 16,777,214 hosts.

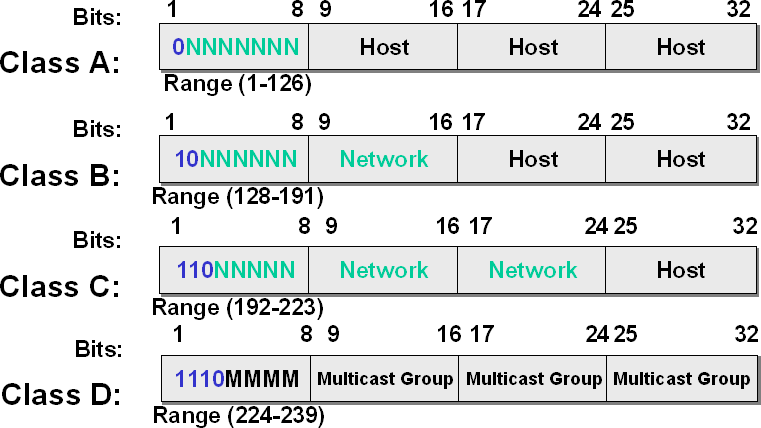


Fig. 3.2 IP Address Types

**Class B:**

Of class B addresses, 16 bits are assigned to the network address, and the other 16 bits are assigned to the host address. A type B address can be identified using the first two bits (set to 10) of the first octet represented as N.N.H.H. This corresponds to values of 128~191. Since the first two bits have been pre-defined, actually 14 bits are reserved for the network address. Therefore, the possible combination generates 16,384 networks, whereas each network supports 65,534 hosts.

**Class C:**

Of class C addresses, 24 bits are assigned to the network address, and the other 8 bits are reserved for the host address represented as N.N.N.H. In class C address, the first three bits of the first octet are 110. This corresponds to decimal digits 192~223. Among class C addresses, only the last octet is used for the host addresses. This imposes a limit that each network can have 254 hosts at the maximum. Now that 21 bits can be used as a network number (3 bits have been preset as 110), there can be 2,097,152 possible networks.

**Class D:**

A class D address starts at 1110. This means that the octet is within 224~239. These addresses are not used as standard IP addresses. On the contrary, class D addresses refer to a group of hosts, which are registered as multi-point transmission group members. The assignment list of the multi-point transmission group is similar to that of emails. You can use names in an assignment list to send a message to a user group. You are also able to send data to some hosts by way of multi-point transmission addresses. Multi-point transmission needs to be configured with special routes. It will not be transferred by default.

**Class E:**

If the first four bits of the first octet are set as 1111, the address is a class E address. These addresses are within the range of 240~254; addresses of this type are not used as common IP addresses. Addresses of this type are sometimes used in laboratories or for research.

We focus on types A, B, and C in our discussion, for they are used for conventional IP addressing.

* 1. **Reserved IP Address**

An IP address is used to identify a unique network device. However, not all IP addresses can be used. Some special IP addresses are used for various purposes, instead of identifying network devices.

An IP address with “0” exclusively for the whole host bits is called a network address. A **network address** is used for identifying a network segment. For example, class A address 1.0.0.0, private addresses 10.0.0.0, and 192.168.1.0 are network addresses.

An IP address with all 1’s exclusively for the whole host bits is called a network segment **broadcast address.** A network segment broadcast address is used to identify all the hosts of a network, for example, 10.255.255.255, 192.168.1.255, and so on. A router can transfer broadcast packets on network segments as 10.0.0.0 or 192.168.1.0. A broadcast address is used for transmitting packets to all nodes of the local network segment.

An IP address with “127” for the network part, such as 127.0.0.1, is usually for **loopback tests.**

it is usually used to test the NIC of the system is working or not.

An IP address with the value “0” configured for all bits, such as 0.0.0.0, represents all the hosts. On a router, address 0.0.0.0 is used for designating the **default route**.

An IP address with the value “1” configured for al bits, such as 255.255.255.255, is also a **broadcast address**. The address 255.255.255.255 represents all the hosts, which are used for transmitting packets to all nodes of the network. A Broadcast like this cannot be transferred by a router.

**Automatic Private IP Addressing (APIPA)** is a feature in operating systems (such as Windows) that enables computers to automatically self-configure an IP address and subnet mask when their DHCP server isn’t reachable. The IP address range for APIPA is **169.254.0.1- 169.254.255.254**, with the subnet mask of **255.255.0.0**.

When a DHCP client boots up, it looks for a DHCP server to obtain network parameters. If the client can’t communicate with the DHCP server, it uses APIPA to configure itself with an IP address from the APIPA range. This way, the host will still be able to communicate with other hosts on the local network segment that is also configured for APIPA.

* 1. **Calculation of Usable Host Addresses**

As mentioned above, there may be some IP addresses in each network segment that cannot be used as IP addresses for hosts. Now, let’s calculate the available IP addresses.

In class B network segment 172.16.0.0, there are 16 host bits, so there can be 216 IP addresses accordingly. With one network address 172.16.0.0 and one broadcast address 172.16.255.255 deducted (they cannot identify a host), there will be 216-2 addresses available for hosts.

In type C network segment 1192.168.1.0, there are 8 host bits, so there can be 28(256) IP addresses; with one network address 192.168.1.0 and one broadcast address 192.168.1.255 deducted, there will be 254 addresses available for hosts. We can calculate the addresses available for hosts in each network segment with the following method: If there are n bits for hosts in the network segment, the number of addresses available for hosts will be: 2n-2.

A network layer device (such as a router) uses a network address to represent the hosts in the network segment, thus greatly reducing entries of the routing table of the router.

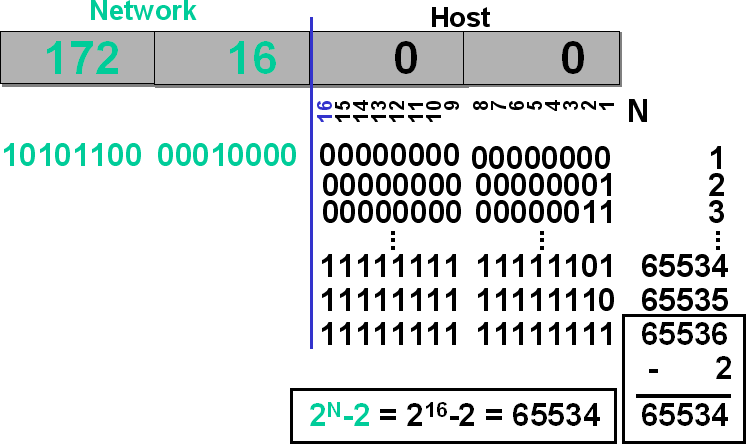


Fig. 3.3 Calculation of Number of Available Host Addresses

* 1. **Addresses with Subnet Division**

Any IP address organization without a subnet will be considered a single network. It is not necessary to know its internal architecture. For instance, all routes to address 172.16.X.X are considered as in the same direction, so the third and fourth octets of the address will not be taken into consideration. A plan like this can have fewer entries in the routing table.

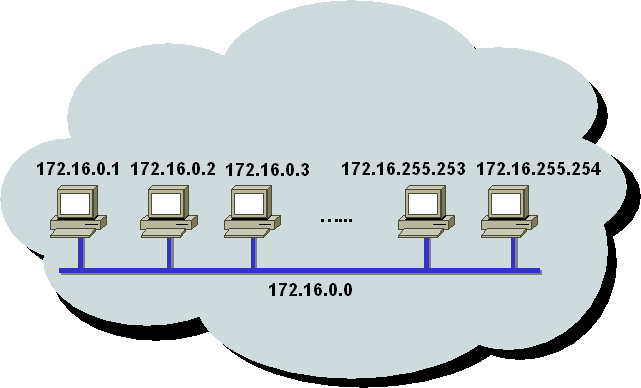


Fig. 3.4 Addressing without Subnet

However, this plan is unable to distinguish different subnet segments in a large network. In this case, all the hosts in the network receive the broadcast in the large network. Therefore, it will reduce the network performance, and hinder network management.

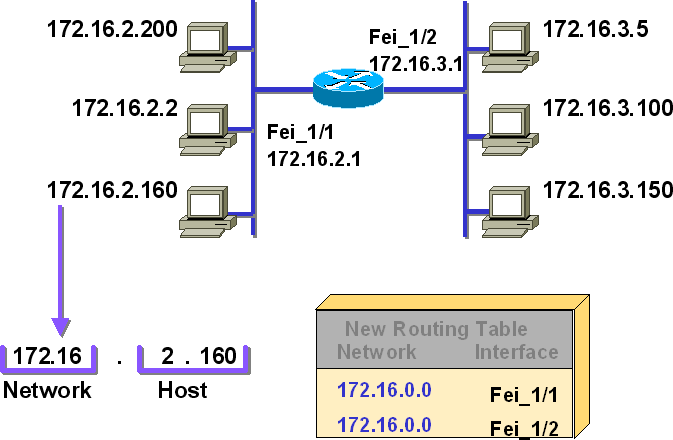
For example, a class B network can accommodate 65000 hosts, but it is too difficult to manage so many hosts simultaneously. So we need to divide such a network into different segments. In this way, we can manage the subnet according to network segments. Usually, host bits can be divided into subnet bits and host bits.

Fig. 3.5 Addressing with Subnets

In this example, the subnet bits occupy the 8 bits of the third segment. Compared with the previous example, the original class B network is divided into 256 subnets, and the number of hosts each subnet can accommodate is reduced to 254.

When different subnets are divided, different logical networks are created accordingly. The routers are responsible for communication between these different networks. That is, an original large broadcast domain is divided into multiple smaller broadcast domains.

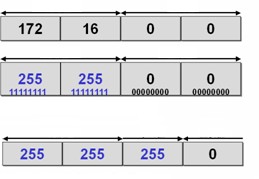
A network device uses a subnet mask to identify network bits, subnet bits, and host bits. The network device can distinguish the destination address of an IP packet, according to the IP address and subnet mask configured. The network device can distinguish whether the destination address of an IP packet and its address are located in the same subnet, in a network of the same type but in different subnets, or in networks of different types.

* 1. **Subnet Mask**

An IP address without the related subnet mask is of no significance.

A subnet mask defines how many bits from the 32 bits of an IP address are used as the network bits, or as bits for the network and its related subnet bits.

IP address



Network bits

Host bits

Network bits

Host bits

It can also be "/16", where 16 is the digits for the mask

Network bits Subnet bits Host bits

It can also be "/24", where 24 is the bits for the mask

Default mask

8-bit subnet mask

Fig. 3.6 Subnet Mask

The binary bits in the subnet mask can be used as a filter, which calculates the network address by identifying the part of the IP address of the network address. The process of this task is called “Bitwise AND”.

“Bitwise AND” is a logical operation, which performs the calculation of each bit of the address and the corresponding mask bit.

To divide a subnet is actually to borrow the host bits in the original address to be used as the subnet bits. It is currently stipulated that bits shall be borrowed from the left to the right in succession, that is, the 1 and 0 in the subnet mask shall be consecutive.

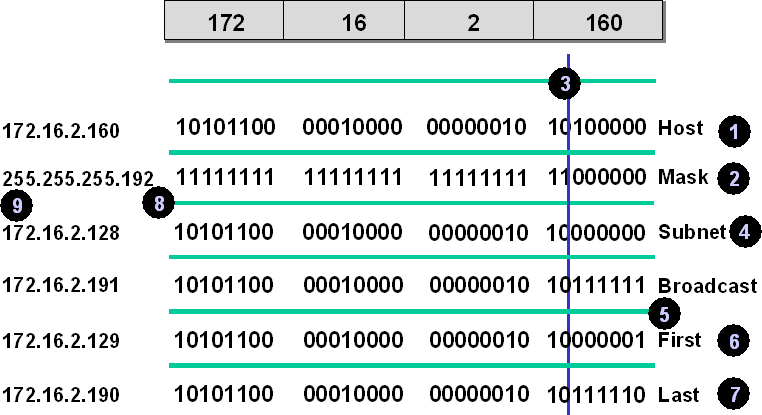
* 1. **Examples of Address Calculation**

Fig. 3.7 Examples of Address Calculation Above are examples of address calculation:

For a given IP address and subnet mask, the address calculation involves the address, the broadcast address, and the available IP address range of the subnet where the IP address is located.

* + - Convert the IP address to one presented in the binary system.
    - Also convert the subnet mask to one presented in the binary system.
    - Draw a vertical line between 1’s and 0’s of the subnet mask. Bits on the left side of the line are for the network (including the subnet), and bits on the right are for the host.
    - Set all the host bits as 0. The network bits are the network address of the subnet.
    - Set all the host bits as 1. The network bits are the broadcast address of the subnet.
    - The available IP addresses range from the network address to the broadcast address of the subnet.
    - Complete the above three network addresses.
    - Finally, convert them to decimal numbers.

IP Addressing & Network Planning

**Subnet Mask Task (Rough work at the back of the Page)**

IP Address Subnet Mask Class Network address Of given IP Broadcast address of given IP

203.200.10.60 255.255.255.248 C 203.200.10.56 203.200.10.63

First Subnet \_203.200.10.0\_\_\_ No. of Hosts per subnet \_\_\_\_6\_\_\_\_

Solved Example

|  |  |  |
| --- | --- | --- |
|  |  |  |

Class 1st subnet of Network 1st subnet Broadcast address

|  |  |  |
| --- | --- | --- |
|  |  |  |

13.14.193.6 255.255.248.0

This IP Subnet

No. of Hosts per subnet

128.17.35.13/30

. . .

Class Network address Of given IP Broadcast address of given IP

First Subnet No. of Hosts per subnet

|  |  |  |
| --- | --- | --- |
|  |  |  |

2nd subnet address

Class Network address Of given IP Broadcast address of given IP

|  |  |  |
| --- | --- | --- |
|  |  |  |

145.60.6.27/25

. . .

First Subnet No. of Hosts per subnet

last Subnet address

Network address = keeping all the bits of a host as “0”, Broadcast address = one address before next subnet & No. of Hosts = 2n-2 (n= No. of bits)

# LAB 4: Configuring Basic Switch and Router

**Objectives**

* + - * Perform basic switch configuration on zero configured Switch in Cisco packet tracer to enable the Switch for the basic functionality.
      * Complete walk-through of 100 MB full duplex configuration in Cisco Switch step by step.

1. **Introduction**

There are a lot of devices that fall into the “network switch” category. Since we’re talking about configuration, we’ll be referring specifically to managed switches in this article. It’s worth noting how you configure a Layer 2 vs Layer 3 switch will be different, as will small office/home office (SOHO) vs. enterprise switches. And don’t forget there are always going to be small differences between vendors and software versions.

Because Cisco is so common, and its IOS-style CLI is used on more than just Cisco switches, we’ll focus on the command-line configuration of Cisco switches running IOS as our prime example. But you’ll be able to use what we cover here in lots of different environments. Because many of the commands and concepts apply to routing devices too, this can also be a good reference for basic router and switch configuration.

From a network perspective, we’ll focus on features related to Layer 2 switching.

A good thing about the **Cisco IOS** is that it works quite similarly on both the routers as well as switches, However, there is a difference in the commands that we use for each one of them. For example, some specific commands are meant only for the switches while others are for routers as per the device's functionality.

In this lab, we will assign an IP address to the VLan1 interface and we will configure the default gateway on the Switch. We will also perform some basic configurations which will prepare the Router for the functional network.

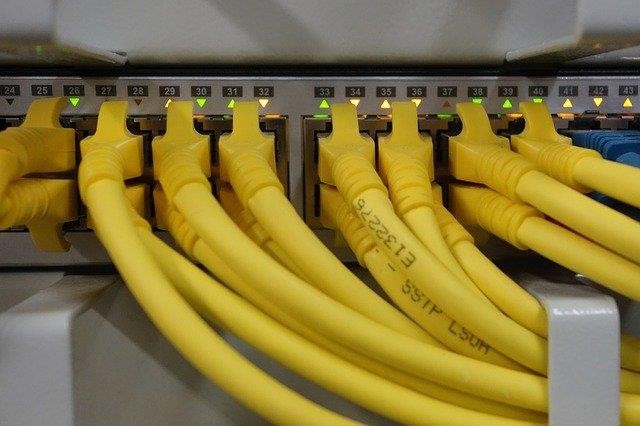


Figure 4. 1 Ethernet cables connected to the Switch

1. **Basic Switch configuration:**

Basic switch configuration can be thought of as the minimum network, port, and security provisioning required for the production deployment of a switch. In practice, your exact needs

will vary from environment to environment. And overall, [effective switch management](https://auvikstage.wpengine.com/franklyit/blog/effective-switch-management/) is a detailed topic in its own right.

Our goal here is to cover some switch and router configurations basics that apply to most production use cases. These include configuring device management settings and hardening the switch and router.

All switches come with default VLAN1, To assign an IP address to the VLAN1 interface, we have to enter interface configuration mode. While configuring the Switch for basic functionality, we should also assign a default gateway to the Switch.

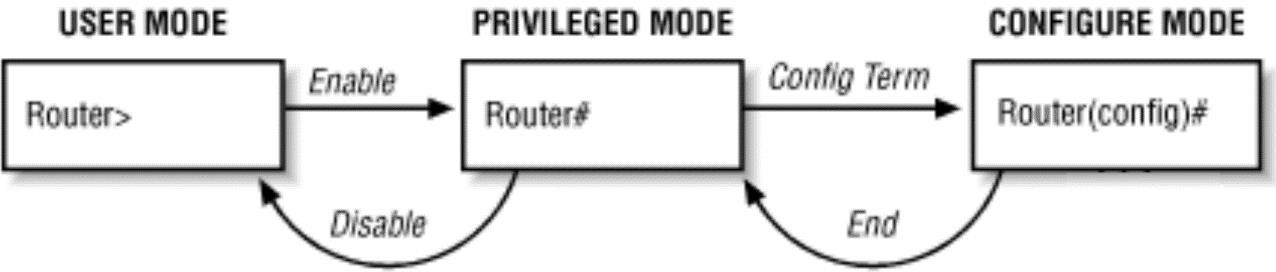


Figure 4.2 modes of switch and Router

***It is important to remember that the VLAN1 interface and default gateway IP address must be on the same network.*** This enables the Switch to redirect traffic to other networks.

Routers however are considered gateways and do not support VLANS. Routers have limited interfaces and each interface requires a different Network address.

* 1. **important Commands To Remember**

Before we proceed some commands require your attention. They are helpful while you perform actions on the switches.

* + 1. **Saving the configurations on Switch**

Vlan1 interface allows us to connect with the Switch remotely via telnet, we can use the telnet client to remotely manage and configure the Switch. If you are unable to save the changes made to the Switch, all the hard work will do down the drain. Therefore, if the changes made to the Switch is worth-a-while and nothing unexpected has occurred, the user may save configuration on Cisco devices by typing the command **'write'**. It copies the running-config to the startup- config alternatively we can also use the command **'copy running-config startup config'** to save the running configuration of the device.

* + 1. **No IP Domain Lookup**

While configuring Cisco devices, it's common to make typing mistakes. If we mistype a command then the Cisco device will try to resolve the name to the IP address. This makes Cisco devices freeze for about 60 seconds as it resolves IP addresses in the background. One minute is the maximum time taken by the device. Now, we have to wait until the device allows us to type something again. This can be very annoying. It happens because the domain name lookup is enabled by default in Cisco devices. Hence, to solve this problem we can disable

domain lookup by entering the command **'No IP Domain Lookup'** in the switch command line.

* + 1. **Logging synchronous**

Now, let us talk about the status of messages received on Cisco devices. When we receive status messages on Cisco devices the message kind of mixes with the text that we type on the CLI. This can also be very confusing sometimes.

So, to solve this problem we can type the command **'logging synchronous**'. This command synchronizes the status messages. Hence, the message does not interfere with our typing.

* 1. **Getting started**

There are a lot of nuances related to the configuration of a switch that isn’t obvious to beginners. Here are some basic tips to be aware of before you start.

Command line completion, Use the tab key, and up/down arrows are time savers

Typos are a pain, and typing out long commands is tedious. Fortunately, Cisco’s IOS has features that can help you avoid typos and work faster:

1. **Command Line completion.** Once you type enough of a command that is unique, you can just hit enter. For example, instead of typing “configure terminal”, you can use the command “config t” like this:

Switch#config t

1. **Tab completion.** Hitting the tab key once you have enough unique text on the screen will auto-complete a command. For example, hitting tab after “conf” auto-completes to “configure”:

[](https://auvikstage.wpengine.com/wp-content/uploads/2021/07/tab_complete.gif)

1. **Command scrolling with up/down keys.** Need to rerun a command? You can scroll through your command history with the up/down arrows on your keyboard.

[](https://auvikstage.wpengine.com/wp-content/uploads/2021/07/scroll_complete.gif)

1. **Bonus! Use “?” for added help.** Hitting “?” at the beginning of a command prompt will show you all the commands that are available in the current context. Hitting “?” after a command will show you all the parameters that are available in that context.
   * 1. **Access levels and modes**

There are several Cisco access levels and modes that allow you to run different commands. You can learn more about each mode in the [Cisco IOS command hierarchy](https://www.cisco.com/E-Learning/bulk/public/tac/cim/cib/using_cisco_ios_software/02_cisco_ios_hierarchy.htm), but the table below is a reference for our examples.

|  |  |  |  |
| --- | --- | --- | --- |
| Cisco Mode | What the prompt looks like for switch and router | Command to enter from upper-level mode | Command to exit  to upper-level mode |
| User EXEC mode | Switch>, **Router>** | Default mode | logout or exit |
| Privileged EXEC (access from EXEC) | Switch#, **Router#** | enable | disable |
| Global configuration  (access from  Privileged EXEC) | Switch(Config)#,  **Router(Config)#** | config t | CTRL/Z |
| Interface configuration (access from global configuration) | Switch(config-if)#  **Router(config-if)#** | interface  <interface name> | Exit |
| Routing engine level within configuration mode | **Router(config- router)#** | Router <protocol> RIP | exit |
| Line level configuration (access from global configuration) | Switch(config- line)# **Router(config- line)#** | line <line name/ number>  vty, tty, aux, console | Exit |

* + 1. **Console ports and cables**

When you’re connecting to a switch for the first time, you’re often doing it through the console port. Usually, this is done by connecting a serial cable to the switch. You can also use a USB to serial adapter to make the connection.

Once the physical connections are made, how can you access the CLI? By using a terminal emulator. For Windows, there are several popular emulator options, like **Putty, RealTerm, and TerraTerm**.

* + 1. **Startup config vs. running-config**

Your switch has two “config” types and locations. A switch’s *running-config* is stored in RAM. Its *startup-config* is stored in nonvolatile memory (harddisk).

Why is this important? Take it from someone who has made the mistake too many times: if your configuration changes aren’t saved to the startup-config, you’ll lose them, when the **switch reboots**. As you make changes to the running config, you’ll see them take effect in real- time. However, you need to explicitly save those changes to the running config for them to persist. Save yourself some pain and double-check before moving on.

**Duplexing and Link Speed**

Most of the time **Cisco auto-negotiation** for duplex selection works perfectly. However, in some instances, a Cisco device is unable to detect the duplex mode and it may result in a duplex

mismatch. This could result in collisions in the network. Therefore, to fully utilize the bandwidth and the capacity of the Switch, it is a good practice to hard-code the speed and duplex on the Cisco devices.

In this lab, we will learn how to configure a basic switch and how can we connect it with LAN to communicate between the terminals. First, we will learn how to enter the command line of the switch using the console cable to configure the basic settings, once that set we will perform further settings like giving it an IP address, gateway address, duplex, and speed to links, we will have to go into the specific interface on which we want to hard-code the speed and duplex setting.

Please note that full-duplex configuration must be configured on each interface on which we want to hardcode the full-duplex mode.

Full duplex

**Show Commands For Switch Configurations**

The following example shows how to list the show commands available in privileged mode:

Switch> enable

Switch# **show** <command>

Frequently used command are highlighted

**Show commands:**

show arp Show ARP table

show cdp Show Cisco Discovery Protocol Information show running-config Show system configuration

show flash Show system flash information show interface Show network interfaces

└status Duplex/speed

└Vlan <No.> VLan information

└switchport all vlan ports information

└trunk trunk information show ip Show IP Information

show logging Show system logging information show mac-address-t Show MAC table information show port-security Show port information

show spantree Show spantree information show trunk Show trunk ports

show users Show active Admin sessions

show version show vlan

Show version information Show Virtual LAN information

show vtp Show VTP Information

Console> (enable)

**Lab Task: Configure A Network Switch**

Now that you know the basics, we can move on to the commands. Here, we’ll walk through some of the most important basic network switch configuration tasks.

While any particular production deployment will likely require specific additional steps (e.g. for additional hardening and user management), these commands will help you hit the ground running.

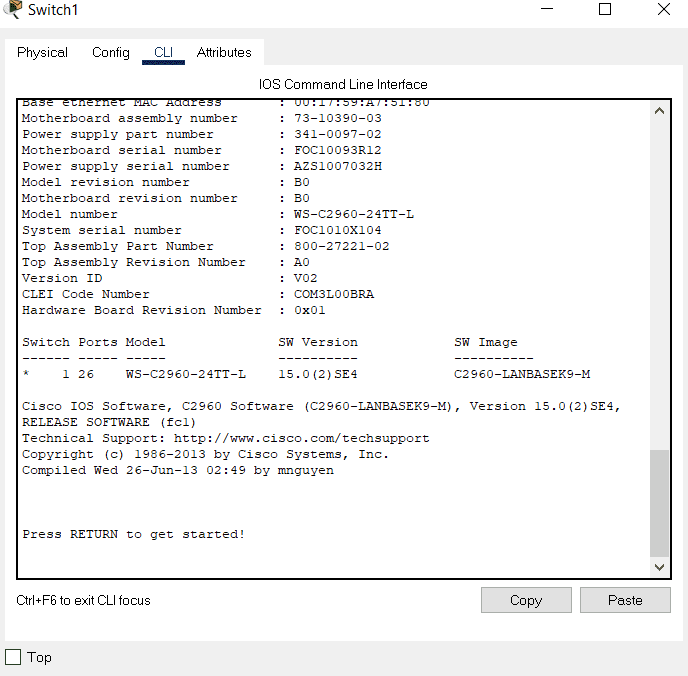
[](https://auvikstage.wpengine.com/wp-content/uploads/2021/07/switch-CLI_1.png)

Fig 4.1 shows the start-up of a typical CISCO Switch

**Task 1: Connect to the console**

You need to start with a connection to the console port. That means configuring your terminal emulator software and connecting your rollover cable between your switch’s console port and your PC.



Figure 4.2 connecting a switch using a console cable Many Cisco switches use these serial settings shown in Figure 4.3.

1. Double-click on PC0, click on the “Desktop” tab, and then click on “Terminal”. (Note: In real life, you can use HyperTerminal or PuTTY for Windows XP.)

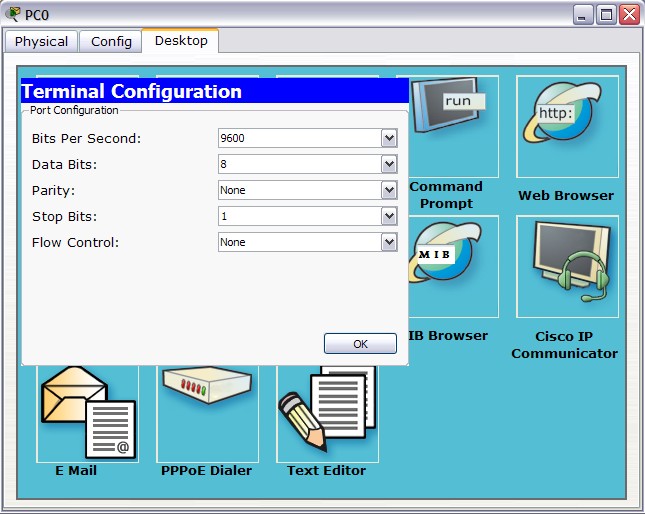


Figure 4.3 setting up the serial connection to switch

1. Set the parameters according to the above screen, and click “ok” to continue.
2. From now on, use the “Terminal” of PC0 to configure the router instead of using the CLI in the router.

(Note: “Terminal” is how a router is configured in the real world. “CLI” shown in Figure 4.4 is just a “convenience” in Packet Tracer. “CLI” does not exist in the real world”.)



Figure 4.4 The “CLI” of the Router does not exist in the real world.

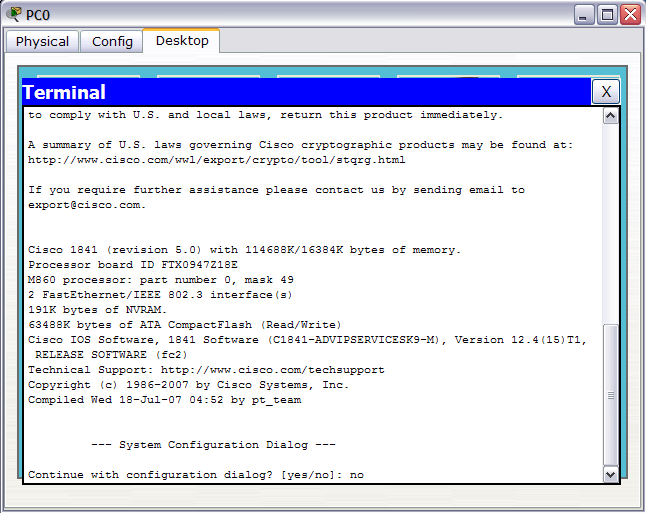


Figure 4.5 shows router configuration in the real world, with a rollover cable and a Terminal program.

3. Wait for the booting up of the switch and router.

NOTE: During booting the router will ask you if you want to setup using dialog.

**Type “no” (as shown in the above screen).**

5. Hit enters key to get the first router prompt.

Router> **OR** Switch>

**Task 2: Set a management IP and default gateway**

The management IP address is where you can log in to the switch for future administrative tasks. Once your management IP is set up, you can use it to SSH into the switch and configure it over the network.

First, we access Privileged EXEC mode with the “enable” switch configuration command:

*Switch>enable Switch#*

*And*

*Router> enable Router#*

**Assign Ip To A Switch To Use In the LAN**

From there, we enter Global Configuration mode with “config t” (or “configure terminal”):

*Switch#config t*

*[Enter configuration commands, one per line. End with “CNTL/Z”.] Switch(config)#*

Next, we access the switch VLAN interface:

*Switch(config)#interface vlan 1 Switch(config-if)#*

Now, we can assign the management IP and subnet.

In this example, I’ll assign a 192.168.1.0 network address with a 255.255.255.0 subnet.

**Be sure to replace that with the correct values for your switch!**

*Switch(config-if)#ip address 192.168.1.10 255.255.255.0 Switch(config-if)#*

We can exit interface configuration mode and assign a default gateway for the switch from global configuration mode.

*Switch(config-if)#exit*

*Switch(config)#ip default-gateway 192.168.1.1 Switch(config)#*

**Tasks For Router**

**Unlike the switch, we assign an IP address to each interface on a router.**

**For the router select an appropriate interface to assign IP, as the example shows IP address is assigned to an interface.**

*Router(config)# interface FastEthernet 0/1 Router(config-if)# ip address 192.168.1.1 255.255.255.0*

*Router(config-if)# no shutdown (as the interfaces are shut, use the command to turn them on Router(config-if)# exit*

**Task 3: Set hostname**

In addition to setting the IP address of the switch, you should give it a logical hostname. To do that, we enter global configuration mode and use the hostname command:

*Switch(config)#hostname PepperAndEggSwitch PepperAndEggSwitch(config)#*

**Task 4: Setting Duplex of Individual Port** *Switch(config)#interface FastEthernet 0/1 Switch(config)#duplex full*

**Task 5: Setting speed of individual port** *Switch(config)#interface fastethernet 0/1 Switch(config)#speed 100*

**Task 6: For multiple ports assignment (only for Switch)**

Apply the above on all ports of Switch, How Use range command

*switch(config)#interface range fastethernet 1/24 switch(config-if-range)#*

*OR*

*switch(config)#interf r f1/1-24 switch(config-if-range)#*

**Task 7:Save Configuration**

When our configuration is complete, we can save our changes to the startup configuration. Don’t forget this step, or all your work will be gone come the next switch reboot!

*Switch(config-if)#exit Switch(config)#exit Switch#*

*%SYS-5-CONFIG\_I: Configured from console by console*

*Switch#copy running-config startup-config Destination filename [startup-config]?*

*Building configuration... [OK]*

*Switch#*

**OR**

*Switch#write*

**Task 8:**

*Switch(config)#no ip domain lookup Router(config)#no ip domain lookup*

**Task 9:**

*Switch(config)#line con 0*

*Switch(config-line)#logging synchronous*

*Router(config)#line con 0*

*Router(config-line)#logging synchronous*

**Task 10: Show running-config**

*Switch# show run*

# LAB 5: Securing the Switch and Router

**Objectives**

* Configuring MOTD banner and Telnet in packet tracer.
* Learn about telnet configuration in Cisco packet tracer.
* We will encrypt various passwords configured on the Cisco device using commands.
* we will be configuring switch port security in the packet tracer to secure the Switch from unauthorized access.
* We will also learn how to limit the MAC address to connect to the switch port.

1. **Introduction**

This lab exercise entails the basic setup of the Switch or a router. In this lab, we will configure the IP address on a fast Ethernet port of the Router. We will name the interface the 'Branch Office Interface.' Naming the interface is an excellent and very essential practice because it will let us know, to which location the port is connected.

As a Network Admin, when we log into a router, the description of the interfaces is very helpful. It makes management of the interfaces a wee bit easier, especially in big networks where there are many different devices. The user has to go into the interface configuration mode to set up the IP Address and description.

* 1. **MOTD banner and Telnet**

You will also learn to configure MOTD [Message of the Day in this lab. When the user is logged into the device then a message appears on the screen. That message is known as the Message of the Day (MOTD). Usually, the MOTD banner is set up as a warning against unauthorized access.

Some people show ASCII art and huge messages like terms and conditions as a message of the day however best practice is to use short and precise MOTD banners as big messages put extra load on the device which results in unnecessary processor cycles.

It's all up to the admin to choose whatever message of the day should show up when we log in to the Cisco device.

* **The message of the Day (MOTD):** This type of login message has been around for a long time on Unix and mainframe systems. The idea of the message is to display a temporary notice to users, such as issues with system availability.

However, because the message displays when a user connects to the device before login, most network administrators are now using it to display legal notices regarding access to the switch, such as *unauthorized access to this device is prohibited and violators will be prosecuted to the full extent of the law* and other such cheery endearments.

* **Login:** This banner is displayed before login to the system, but after the MOTD banner is displayed. Typically, this banner is used to display a permanent message to the users.
* **Exec:** This banner displays after the login is complete when the connecting user enters User EXEC mode. Whereas all users who attempt to connect to the switch see the other banners, only users who successfully log on to the switch see this banner, which can be used to post reminders to your network administrators.
  1. **Telnet connection and Testing**

Configuring the Telnet Connection on the Router allows the user to manage the Router remotely with the help of a Telnet Protocol. Setting up a Telnet Connection also requires a Telnet Password to be configured. We will configure that password in this lab. Also, we will have to get into the Telnet lines to configure the telnet. We can do this by typing the line VTY command.

Configuration of the telnet helps a lot when we have to manage the device from a remote location or we are not available onsite. Configuration of the devices remotely has become common practice now a day and especially due to the Coronavirus outbreak, most IT individuals are working from home using the internet.

Using the internet is not to connect to an office network is not safe and secure so to overcome this issue we should use a VPN connection or we should use SSH instead of telnet as it encrypts the data which prevents the network from attacks from hackers.

MOTD banner and telnet lab in packet tracer

Fig 5.1 Telnet configuration in Cisco packet tracer.

* + 1. **Description:**

Telnet -Protocol developed in 1969, allow us to connect to the remote device using the command line interface, telnet protocol is part of the TCP/IP suite. To use the telnet, the device should have a telnet client installed and the remote device should be configured to accept telnet connection so most of the devices like servers, routers, switches, firewalls, etc are configured to allow telnet connection.

We can use any telnet client to establish the connection; one of the famous free telnet clients is putty. **Putty** is used by many organizations as it is open source and it also works for SSH connection.

In this packet tracer lab, we will set up a router for telnet access. And then use the command prompt on the computer to test our telnet connection. To telnet the Router from our PC we will have to assign an IP address to our PC. After that, we will assign the IP address to the router interface which is connected to that PC.

For establishing a successful telnet connection, our PC and Router should be on the same network as the PC and Router are connected directly.

Telnet in cisco devices

After assigning the IP addresses to both our devices, we have to enable the Router for a telnet connection by configuring the VTY lines. We will configure telnet lines 0-15 on the Router, which will allow 16 simultaneous telnet connections to the Router, this feature is helpful if more than one person wants to log in to the device at the same time, this type of practice is common if we have many administrators to look after the device.

Once we have configured both devices properly, we can try pinging the Router from our PC to check the connectivity. If the Router is responding to the ping command then we can establish a telnet connection from our PC's command prompt. Once the telnet connection is initiated successfully, we will be prompted with the password to access the Router via a telnet connection.

An important thing, we have to configure the privileged mode password. That's because it is not possible to access the privileged mode through a telnet connection if the password for our privileged mode is not configured. if we will try to access privileged mode without the configuration of the password then we will see an error message saying 'no password set'.

* 1. **Cisco Password Encryption.**

Configuring passwords and securing devices is very important and we must configure the password on different layers to prevent unauthorized access to the device.

Due to the increased number of cyber-attacks, networks now a day are more prone to online attacks rather than physical damage to the devices and hackers continuously try to find out the loophole in the network to compromise the security. Every year organizations lose thousands of dollars due to cyber-attacks and sometimes important data is lost permanently. Most of these attacks can be prevented if security is properly implemented at every layer.

There are various types of devices available in the market to stop these attacks like advance firewalls, intrusion prevention systems, antivirus, etc however we should not ignore the basic security parameters like setting up a good password on the device. Organizations spend a large amount of money on expensive hardware to secure the networks however that can be of no use if security is not implemented at every layer.

In this lab, we will encrypt all the passwords on the device with one command. When we configure passwords like Privileged Mode password, VTY line password, Console line password, etc. on our Cisco devices, these passwords are visible as clear text in the running- config. This is a security vulnerability since anyone can view them just by looking at the running-config or start-up config. Even when you are checking the Cisco device configuration, someone could be watching over your shoulder. To fix this problem, we could use a command known as the 'service password-encryption. This command encrypts all passwords and

converts them into alphanumeric numbers. Hence, we can use this command to store and display the passwords in encrypted form for added security.

Service password-encryption command encrypts the password so just by looking at the password, no one will be able to figure out or steal it however it does not provide complete protection as someone can easily copy that encrypted password from the running or startup- config and can find the used password by decrypting that, there are some sites available online that easily decrypt the password with just one click so we must use enable secret that use MD5 hash to encrypt the password which is a very powerful encryption and it is not easy to reverse engineer the hash.

Although password encryption should be enabled by default it is not so we have to manually encrypt the passwords.

* 1. **Cisco Port Security:** *Configuring switch port security in packet tracer.*

Cisco has implemented some security measures to safeguard its devices from unauthorized access. Therefore, to be able to secure the physical ports on a Cisco Switch, we have to enable Port Security.

There are a few options available to the user while configuring the Port Security. One such option is to limit the number of MAC Addresses that the port can connect with. This security feature does not provide complete security however it makes it extremely difficult for the attacker to break into the network. The only way a hacker can beat this security parameter is by finding out the attached mac-address and giving the same mac-address to the device which attackers want to connect to the particular switch port.

Many times, some employees in the organization connect their devices to the switch port available in their cubicles just for the fun or sometimes for experimental purposes, and if security is not implemented then that device can jeopardize the whole network and hackers can also this vulnerability to hack into the network.

In this lab, we will allow only one MAC Address to be able to access the interface fast Ethernet 0/2. If some other device is attached to the interface the port will go to a shutdown state. Also, when the port will be shut down then the light on the Switch will turn amber on that switch port so the admin can find out the issue just by looking at the physical indicator on the Switch.

To enable Port Security on a Cisco switch, we have to change the switch port mode from dynamic to access. By default, the switch port mode is set to dynamic. Once the switch port mode is changed, we can then enable the switch port security on that port. There are a couple of ways in which we can restrict devices with random mac-address to connect with the switch port. One way is to hardcode the mac address on the switch interface with the command "switchport port-security mac-address [mac-address number]"

Another command that we can use is "switchport port-security mac-address sticky", this command will stick the already attached mac-address to the interface and other mac-address will be rejected so if devices with other mac-address will try to connect with the interface then the interface will simply reject the connection and we can also configure how the interface should react when the security violation takes place.

**Lab Task (Switch)**

**Task 1**

Click on pc2 > click desktop tab > click on terminal > click ok (you should be able to access a switch or a Router)



**Task 2: MOTD**

A banner is a message presented to a user who is using the Cisco switch. Based on the type of banner you configured for use, the message will be shown to users of the Cisco switch. Banners are a very powerful tool to alert the intruder to stay away from the device.

To configure each of these banners and set them up on your switch, follow these commands:

*SW1#enable SW1#configure terminal*

*Enter configuration commands, one per line. End with CNTL/Z. SW1(config)#banner motd #Admin Access only!#*

*SW1(config)#*

**Task 3: Set logins on VTY lines and console port (telnet connections)**

Strong passwords are an important part of hardening a managed switch, so next, we’ll add a password to all virtual terminal (VTY) lines. Our switch has 16 VTY lines which are used for remote access, so we’ll configure the entire range from 0-15:

*Switch(config)#line vty 0 15 Switch(config-line)#password cisco Switch(config-line)#*

Next, we’ll exit the VTY configuration, access console line 0, and assign it a separate password:

*Switch(config-line)#exit Switch(config)#line console 0 Switch(config-line)#password cisco Switch(config-line)#*

**Task 4: Set Privileged EXEC password**

In addition to password-protecting the VTY and console lines, we can and should protect Privileged EXEC mode with a password.

We can do that from the global configuration mode:

*Switch(config-line)#exit Switch(config)#enable secret cisco Switch(config)#*

*Note: Because switch security is a complex topic, and we’re focused on the basics, we won’t go into* [user management](https://lp.auvik.com/manage-network-switch-ebook/) *here. However, be sure to properly configure users or remote authentication servers before production deployment.*

**Task 5: Enable SSH**

At some point, you’ll find yourself in need of access to your network devices, and you’re not physically in the same room as them. To access a switch’s CLI over the network, you’ll need to use Telnet or SSH. From a security perspective, Telnet is usually a non-starter because data is transmitted in plaintext. That leaves us with SSH.

The first step to enabling SSH is generating the RSA keys:

*Switch(config)#crypto key generate rsa*

The name for the keys will be: numlselab1

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 are in the modulus [2048]:

% Generating 2048-bit RSA keys, keys will be non-exportable...[OK]

*Switch(config)#*

**Task 6 Setting SSH version to 2:**

*Switch(config)#ip ssh version 2*

*\*Mar 4 7:4:9.374: %SSH-5-ENABLED: SSH 1.99 has been enabled Switch(config)#*

Now, we can set SSH up on specific VTY lines. I’ll use the first 6 lines here:

*Switch(config)#line vty 0 5 Switch(config-line)#transport input ssh*

Finally, we’ll tell the switch to check the local users’ database to authenticate users:

*Switch(config-line)#login local Switch(config-line)#*

**Task 7 Switch Port Access**

Switch(config)#interface fastethernet 0/2

Switch(config-if)#switchport mode access Switch(config-if)#switchport port-security Switch(config-if)#switchport port-security maximum 1

**Task 8 Switch Port Security**

Switch(config-if)#switchport port-security violation shutdown

**(Router)**

**Task 1: connect to the Router using the console cable.**

**Task 2 MOTD**

*Router(config)#banner motd #*

*Enter TEXT message. End with the character '#'. Authorized users only, violaters will be shot on sight!*

**Task 3** Specifies a virtual terminal for remote console access Router(config)#line vty 0 15

Router(config-line)#password cisco Router(config-line)#login

*Router(config)# line console 0 Router(config)# password cisco1 Router(config-line)# login*

**Task 4**

Sets the interval that the EXEC command interpreter waits until user input is detected. The default is 10 minutes. You can also optionally add seconds to the interval value.

*Router(config-line)# exec-timeout 5 30*

**Task 5**

Router(config)#interface fastEthernet 0/0

Router(config-if)#description BRANCH OFFICE INTERFACE

**Task 6**

*Click on pc0 > click on command prompt PC0> type telnet 192.168.1.1*

*PC0> type privileged mode password Router(config)#enable secret cisco Router(config)#service password encryption*

# LAB 6: Virtual LAN (VLANs)

**Objectives**

* Create and configure VLANs in Cisco packet tracer.
* Study the Router on a Stick Configuration.
* Learn to Configure native VLAN in Cisco packet tracer and Fix native VLAN mismatch.

1. **Introduction to VLANs**

Technically, VLAN (virtual local area network) is also known as a virtual LAN. This technology can logically partition and isolate one or more physical LANs into multiple broadcast domains. And each broadcast domain is regarded as one VLAN. Generally, only devices under the same VLAN can communicate with each other. Why VLAN is used? Before VLAN, there was a single broadcast domain over the specified network, which is called LAN (local area work). Just like the following LAN application topology showed, to communicate with host B, host A will broadcast its ARP (address resolution protocol) request to all the switches and other hosts over the same local area network.

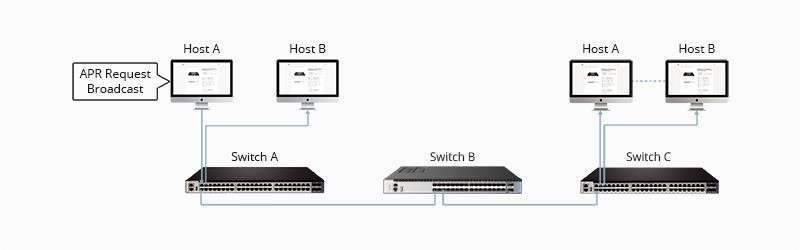


Figure 6.1 LAN overheads

1. **How VLAN works**

Here is step by step details of how VLAN works:

1. VLANs in networking are identified by a number.
2. A Valid range is 1-4094. On a VLAN switch, you assign ports with the proper VLAN number.
3. The switch then allows data that needs to be sent between various ports having the same VLAN.
4. Since almost all networks are larger than a single switch, there should be a way to send traffic between two switches.
5. One simple and easy way to do this is to assign a port on each network switch with a VLAN and run a cable between them.
6. **VLAN Ranges**

Here are the important ranges of VLAN:

|  |  |
| --- | --- |
| **Range** | **Description** |
| VLAN 0-4095 | Reserved VLAN, which cannot be seen or used. |
| VLAN 1: | This is a default VLAN of switches. You cannot delete or edit this VLAN, but it can be used. |
| VLAN 2-1001: | It is a normal VLAN range. You can create, edit, and delete it. |
| VLAN 1002-1005: | These ranges are CISCO defaults for token rings and FDDI. You cannot delete this VLAN. |
| VLAN 1006-4094: | It is an extended range of VLANs. |

1. **Characteristics of VLAN**

Here are the important characteristics of VLAN:

1. Virtual LANs offer a structure for making groups of devices, even if their networks are different.
2. It increases the broadcast domains possible in a LAN.
3. Implementing VLANs reduces the security risks as the number of hosts which are connected to the broadcast domain decreases.
4. This is performed by configuring a separate virtual LAN for only the hosts having sensitive information.
5. It has a flexible networking model that groups users depending on their departments instead of network location.
6. Changing hosts/users on a VLAN is relatively easy. It just needs a new port-level configuration.
7. It can reduce congestion by sharing traffic as individual VLANs work as separate LANs.
8. A workstation can be used with full bandwidth at each port.
9. Terminal reallocations become easy.
10. A VLAN can span multiple switches.
11. The link of the trunk can carry traffic for multiple LANs.
12. **Types of VLANs**

Here are the important types of VLANs

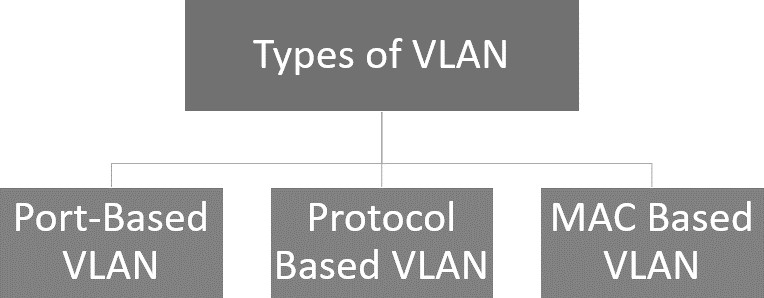


Figure 6.2 Types of VLAN

* 1. **Port-Based VLAN**

Port-based VLANs group virtual local area networks by port. In this type of virtual LAN, a switch port can be configured manually to a member of the VLAN.

Devices that are connected to this port will belong to the same broadcast domain that is because all other ports are configured with a similar VLAN number.

The challenge of this type of network is to know which ports are appropriate to each VLAN. The VLAN membership can’t be known just by looking at the physical port of a switch. You can determine it by checking the configuration information.

* 1. **Protocol Based VLAN**

This type of VLAN processes traffic based on a protocol that can be used to define filtering criteria for tags, which are untagged packets.

In this Virtual Local Area Network, the layer-3 protocol is carried by the frame to determine VLAN membership. It works in multi-protocol environments. This method is not practical in a predominately IP-based network.

* 1. **MAC Based VLAN**

MAC Based VLAN allows incoming untagged packets to be assigned virtual LAN and, thereby, classify traffic depending on the packet source address. You define a Mac address to VLAN mapping by configuring mapping the entry in MAC to the VLAN table.

This entry is specified using the source [Mac address](https://www.guru99.com/what-is-mac-address.html) proper VLAN ID. The configurations of tables are shared among all device ports.

1. **Difference between LAN and VLAN**

Here is an important difference between LAN and VLAN:

|  |  |
| --- | --- |
| **LAN** | **VLAN** |
| LAN can be defined as a group of computer and peripheral devices that are connected in a limited area. | A VLAN can be defined as a custom network that is created from one or more local area networks. |
| The full form of LAN is Local Area Network | The full form of VLAN is Virtual Local Area Network. |
| The latency of the LAN is high. | The latency of VLAN is less. |
| The cost of LAN is high. | The cost of a VLAN is less. |
| In LAN, the network packet is advertised to each and every device. | In VLAN, the network packet is sent to only a specific broadcast domain. |
| It uses a ring, and FDDI (Fiber Distributed Data Interface) is a protocol. | It uses ISP and VTP as a protocol. |

1. **Advantages of VLAN**

Here are the important pros/benefits of VLAN:

1. It solves a broadcast problem.
2. VLAN reduces the size of broadcast domains.
3. VLAN allows you to add a layer of security.
4. It can make device management simple and easier.
5. You can make a logical grouping of devices by function rather than location.
6. It allows the creation of groups of logically connected devices that act like they are on their network.
7. You can logically segment networks based on departments, project teams, or functions.
8. VLAN helps to geographically structure your network to support growing companies.
9. Higher performance and reduced latency.
10. VLANs provide increased performance.
11. Users may work on sensitive information that must not be viewed by other users.
12. VLAN removes the physical boundary.
13. It lets you easily segment your network.
14. It helps you to enhance network security.
15. You can keep hosts separated by VLAN.
16. You do not require additional hardware and cabling, which helps you to save costs.
17. It has operational advantages because of changing the IP subnet of the user in software.
18. It reduces the number of devices for a particular network topology.
19. VLAN makes managing physical devices less complex.
20. **Disadvantages of VLAN**

Here are the important cons/ drawbacks of VLAN:

1. A packet can leak from one VLAN to another.
2. An injected packet may lead to a cyber-attack.
3. Threats in a single system may spread a virus through a whole logical network.
4. You require an additional router to control the workload in large networks.
5. You can face problems in interoperability.
6. A VLAN cannot forward network traffic to other VLANs.
7. **Application/Purpose of VLAN**

Here are the important uses of VLAN:

1. VLAN is used when you have 200+ devices on your LAN.
2. It is helpful when you have a lot of traffic on a LAN.
3. VLAN is ideal when a group of users needs more security or is being slowed down by many broadcasts.
4. It is used when users are not on one broadcast domain.
5. Make a single switch into multiple switches.
6. **Working with VLANs**

We will create VLAN 10 and VLAN 20 in this lab. It is always a good practice to give names to the VLANs as this makes it easier for the admins to manage the configured VLANs. The best way to give a name is according to their role in the network e.g. if there is a VLAN that handles traffic for the voice of IP then we can give the name 'voice' to the VLAN and another way of assigning a name is according to the departments in the organization like Sales, marketing, etc.

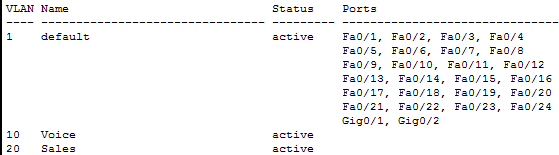
In a case of a network outage or any issue with the VLANs, admins can easily identify the VLANs with names, which makes their work easier.

We can use the following command to create VLAN 10 and 20 and give them a name. Switch(config)#vlan 10

Switch(config-vlan)#name Voice Switch(config-vlan)#no shutdown

Switch(config)#vlan 20 Switch(config-vlan)#name Sales Switch(config-vlan)#no shutdown

Once we are done creating the VLANs, we can check the created VLANs with the command Switch#*show VLAN brief*



* 1. **Assigning ports to VLANs:**

You can see in the image above that although we have created the VLANs however to use those VLANs, we have to assign ports to VLAN. By default, all ports are assigned to VLAN 1 We will assign 1 port to VLAN 10 and 5 ports to VLAN 20

If we want to assign multiple ports to a single VLAN then we can use the interface range command and include the range of ports that we want to add to any VLAN

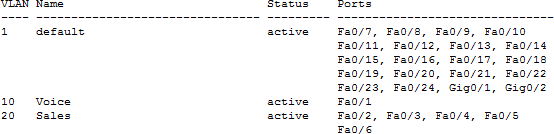
*Switch(config)#interface fastEthernet 0/1 Switch(config-if)#switchport mode access Switch(config-if)#switchport access vlan 10*

**RANGE**

*Switch(config)#interface range fastEthernet 0/2 – 6*

*Switch(config-if-range)#switchport mode access Switch(config-if-range)#switchport access vlan 20*

Now, we can see in the image below that assigned ports are appearing in front of VLAN 10 and 20



* 1. **Inter VLAN routing in packet tracer**

Each VLAN represents a separate network so to enable routing from one VLAN to another VLAN; we have to either use a layer 3 switch or Router.

On a single router interface, we can create sub-interfaces and configure those interfaces to accept traffic from specific VLANs so we can use only one interface that is connected to the Switch for routing purposes.

After configuring the sub-interfaces, we have to assign a default gateway on the end device so the default gateway would be the IP address of the sub-interface specified for the same VLAN of the end device.

Now the traffic will travel within Switch when communicating with the end device in the same VLAN and traffic will travel through the Router when communicating with devices on other VLANs.

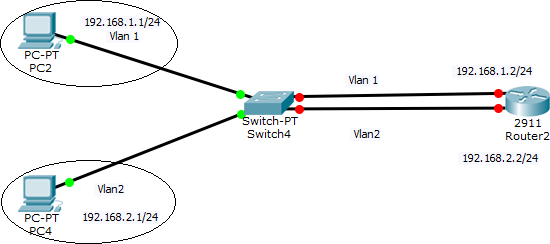
Please check section 2 ‘[router on a stick](https://www.packettracerlab.com/router-on-a-stick-configuration/)’ part to properly configure inter-VLAN routing.

1. **Router on A Stick:**

'Router on a Stick' allows routing between VLANs with only one interface. Each VLAN represents a different Subnet. In general, routers can take traffic from only one subnet and transfer it to another subnet. And we can assign only one IP Address to a router interface. 'Router on a stick' allows us to create sub-interfaces, and assign IP Addresses to those sub- interfaces. To make it work, we have to create a truck connection between the Switch and a router so that traffic from multiple VLANs can be sent to the Router.

If we create a route between VLANs without the 'Router on a Stick' method, then we have to waste interfaces on the switches and routers. And if we enable routing between multiple VLANs then it will become practically inefficient as the switches and the routers will use those multiple interfaces.

The image below is an alternative method for allowing routing between VLANs. As you can see, we are using two interfaces on both the Router and a switch to allow routing between VLANs. We have not created a sub-interface in the below figure.

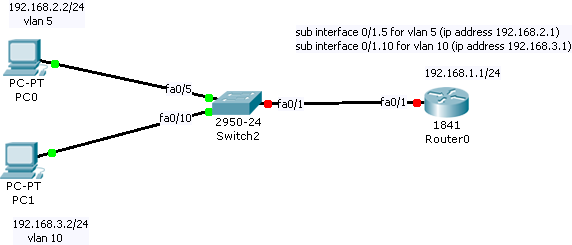


You can see that we have to use extra interfaces for each VLAN. So, it becomes practically non-efficient if we have multiple VLANs. Hence, 'Router on a Stick' is a perfect solution for routing between VLANs with just one router interface.

The simpler way to do routing between VLANs is by using a Layer 3 Switch. We just have to create virtual interfaces for each VLAN and assign them IP Addresses from the same network. A Layer 3 Switch will then enable routing between VLANs as it has routing capabilities as well. However, Layer 3 Switch is quite expensive so it might not be an affordable option for small office networks.

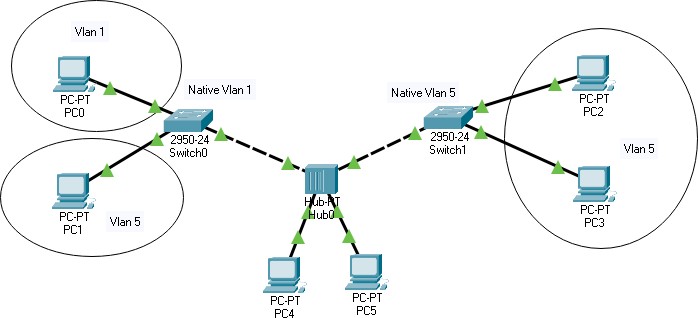
In the below lab, we will configure a 'Router on a Stick' that would allow routing between the VLANs. Some of the important concepts in this lab are – creating sub-interfaces, using the encapsulation dot1Q command to encapsulate the traffic, and mentioning the VLAN number to ascertain for which VLAN the sub-interface should respond.

Draw the figure on the Packet tracer, as shown below to start configuring Router on a stick configuration in the packet tracer.



1. **Native VLAN and Mismatch:**

Native VLAN – Native VLAN allows untagged traffic to be part of one particular VLAN. Native VLAN functionality is used when untagged traffic is received on the trunk connection of the Switch.



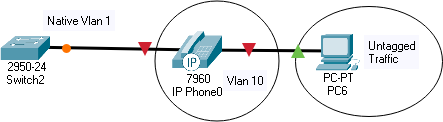
In the above image, you can see that the Hub is connected to the Switch. VLAN and tagging are switching technology and as Hub is unable to tag the traffic then what will happen if PC 4 and PC 5 which are connected to the Hub send the traffic? In that case, we have to specify native VLAN on both of the switch interfaces that are connected to Hub, and that will help when the Switch will receive the untagged traffic on those interfaces then it will be part of the specified VLAN which we have configured as Native VLAN.

Although Hubs are not in use now a day's however in a small organization where the budget is low and organizations cannot afford to spend money on new network equipment and they want to use the old network devices then network admin may have to work with such topologies.

In small networks, speed is not the priority for the company so using the device as a hub does not harm the network.

Another network scenario, in which native VLAN is used commonly, is shown below. IP phones are used commonly in companies these days, they allow daisy-chaining of end devices like PC which saves the interfaces and saves the extra cost of the telecom.

Daisy-chaining the PC is an efficient solution as an organization does not have to buy extra switches to implement IP phones.



PC 6 cannot tag the traffic so we have to configure Native VLAN to route the traffic generated by the PC on the desired VLAN. However, the Cisco IP phone can tag the traffic so native VLAN will only be used by the PC.

By default, native VLAN is configured as 1 on all the interfaces however, in case we want to route traffic to another VLAN then we have to change the native VLAN accordingly.

To check the native VLAN that is configured, we can use the command *'show interfaces trunk*'

https://www.packettracerlab.com/wp-content/uploads/2022/02/Native-Vlan-number.png

To configure the native VLAN or to change the default native VLAN, we have to use the following command.

*Switch(config)#interface FastEthernet 0/24 Switch(config-if)#switchport trunk native vlan 5*

We have to enter into interface configuration mode and then use the command shown above; we have to specify the VLAN number where we want to redirect untagged traffic. In the above example, traffic will be routed to VLAN 5.

* 1. **Native VLAN mismatch**

Native VLAN mismatch happens when interfaces of the Switch are configured with different native VLANs and in that case, traffic generated by the PC will be routed to both VLANs which will cause issues in the network.

The good thing about the Switch is that it detects the native VLAN itself and the following message is displayed on the Command-line interface of the device.

*— %CDP-4-NATIVE\_VLAN\_MISMATCH: Native VLAN mismatch*

discovered on FastEthernet0/24 (5), with Switch FastEthernet0/24 (1) —

To fix the Native VLAN mismatch, we have to configure the same native VLAN on all interfaces that are connected to the Hub so that the traffic generated will only be redirected to one VLAN.

In this lab, we have intentionally created a native VLAN mismatch so you can learn and practice fixing the mismatch by assigning the same Native VLAN on both switches.

You will be able to see the mismatch message on the CLIs of both of the switches.

**Lab Task**

**Task 1**

Click on pc0 > click on desktop tab > click on IP configuration > set IP address and default gateway

**Task 2**

Switch(config)#interface fa0/5

*Try Range command for allocating multiple ports to a Vlan*

Switch(config-if)#switchport access vlan 5 Switch(config-if)#in fa0/10

Switch(config-if)#switchport access vlan 10

**Task3**

Switch(config)#in fastethernet 0/1 Switch(config-if)#switchport mode trunk

**Task 4**

Router(config)#in fa 0/1 Router(config-if)#no shutdown

Router(config)#interface fastethernet 0/1.10 Router(config-subif)#encapsulation dot1Q 10

Router(config-subif)#ip address 192.168.10.1 255.255.255.0

Router(config-subif)#in fastethernet 0/1.20 Router(config-subif)#encapsulation dot1Q 20

Router(config-subif)#ip add 192.168.20.1 255.255.255.0

**For Routing the data Over Router**

Router(config)# ip route 192.168.10.0 255.255.255.0 GigabitEthernet0/0.10

Router(config)# ip route 192.168.20.0 255.255.255.0 GigabitEthernet0/0.20

Note: Check the router ports by using the command show run the ports may differ router to router, respectively.

# LAB 7: Cisco Discovery Protocol (CDP) and Servers

**Objectives**

* Using CDP protocol to find out neighbor information in Cisco packet tracer.
* Setting up a DHCP server in Cisco packet tracer.
* Configure a WEB server in the Cisco packet tracer and access the internet.
* Configuring DNS server.

1. **Introduction: CDP Protocol:**

CDP is a handy protocol. It is a fantastic tool for searching the details about directly connected devices. However, being Cisco propriety, it only works if the connected device is a Cisco device. It sends messages to the directly connected devices, these messages contain details about the host, devices, network, IOS, ports, etc. It is enabled by default on all Cisco devices.

CDP protocol generates messages every 60 seconds, these messages are received by the neighbor device and then the information is stored in the database.

CDP provides us with information that is quite useful if we do not have a complete diagram or incomplete documentation about the network.

By using CDP we can find out the following information:

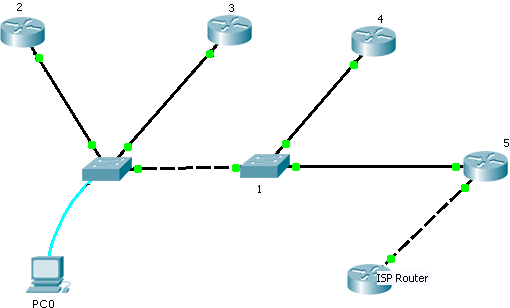
1. The hostname of the remote devices
2. Local and remote interfaces on which the devices are connected
3. Type of device and the platform
4. The IP address of the connected devices
5. The version of IOS running

Although CDP provides good information about the directly connected devices however it can also pose a security threat to the network as hackers can identify and gather information very easily if any device in the network is compromised so it is the best practice to use this protocol very carefully and disable this protocol on highly secure devices. For e.g, we should not send CDP messages on the interface that is connecting outside of our network.

If we do not have the Cisco device on the other end then the CDP protocol will not work. However, we can use the LLDP (Link Layer Discovery Protocol) as an alternative since it is a non-proprietary protocol so most of the vendors support this protocol. It is an industry-standard protocol with the same functionality.

In this lab, you will be required to find information about directly connected devices. To find complete information and details of all the devices, you have to use telnet because CDP can only provide information about directly connected devices. In the below lab, 'device0' does not have a direct link to all Cisco devices. And finally, we have to disable the CDP on the fast Ethernet 0/5 interface of router 5 – which is connected with the ISP router – because we do not want to pass our internal network information to the internet service provider (ISP).

**Draw the diagram as shown below and perform CDP in the packet tracer.**



**Command to see CDP information**

show cdp

Use the **show cdp** command to display Cisco Discovery Protocol (CDP) information.

**show cdp neighbors** [*mod\_num*[*/port\_num*]] [**detail] show cdp port** [*mod\_num*[*/port\_num*]]

***Syntax Description***

|  |  |
| --- | --- |
| **neighbors** | Keyword used to show CDP information for all Cisco products connected to the switch. |
| *mod\_num* | (Optional) Number of the module for which CDP information is displayed. If no module number is specified, CDP information for the entire switch is displayed. |
| *port\_num* | (Optional) Number of the port for which CDP information is displayed. |
| **detail** | (Optional) Keyword used to show detailed information about neighboring Cisco products. |
| **port** | Keyword used to show CDP port settings. |

The following **example** shows how to display CDP information about neighboring systems:

Console> (enable) **show cdp neighbor 4**

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge S - Switch, H - Host, I - IGMP, r - Repeater

Port Device-ID Port-ID Platform Capability

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4/1 | 001905905 | 4/1 | WS-C5000 | T S |
| 4/1 | 062000101(CAT3) | 9 | WS-C1201 | S I |
| 4/1 | 069000022 | 8/1 | WS-C5500 | T S |
| 4/1 | 069000040 | 4/2 | WS-C5500 | T S |

Console> (enable)

The following example shows how to display detailed CDP information:

Console> (enable) **show cdp neighbor 4 detail**

Device-ID: 001905905

Device Addresses:

IP Address: 172.16.25.140

Holdtime: 168 sec

Capabilities: TRANSPARENT\_BRIDGE SWITCH Version:

WS-C5000 Software, Version McpSW: 2.2(4) NmpSW: 2.3(103-Eng) Copyright (c) 1995,1996 by Cisco Systems

Platform: WS-C5000

Port-ID (Port on Device): 4/1 Port (Our Port): 4/1

Device-ID: 062000101(CAT3)

Device Addresses:

IP Address: 172.16.25.212

Holdtime: 175 sec Capabilities: SWITCH IGMP Version:

WS-C1201 Software, Version DmpSW: 4.26 NmpSW: 4.26 Copyright (c) 1994,1995 by Cisco Systems

DMP S/W compiled on Apr 18 1997 15:03:03

NMP S/W compiled on Apr 18 1997 14:52:51 System Bootstrap Version: 1.1

Hardware Version: 3.0 Model: WS-C1201 Serial #: 062000101 1 FDDI interface

8 10BaseT interfaces

4096K bytes of DRAM memory. 1024K bytes of NMP FLASH memory.

32K bytes of non-volatile configuration memory. Uptime is 8 days, 22 hours, 25 minutes

Platform: WS-C1201

Port-ID (Port on Device): 9 Port (Our Port): 4/1 Console> (enable)

The following example shows how to display CDP information for a particular port:

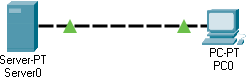
Console> (enable) **show cdp port 2/1**

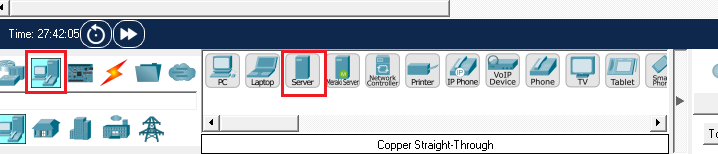
Port CDP Status Message-Interval

2/1 enabled 60 Console> (enable)

1. **DHCP Server:**

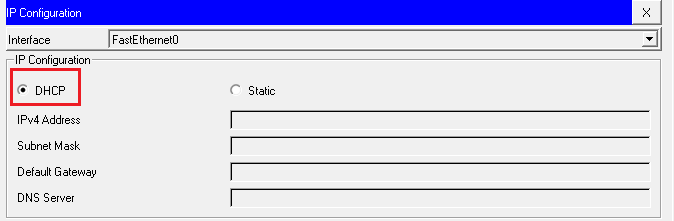
Setting up a DHCP server and configuring the Router as a DHCP server in the Cisco packet tracer.

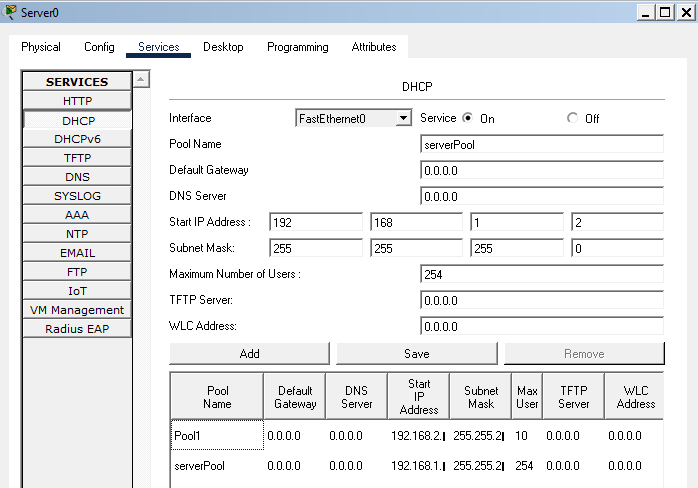




In the Cisco packet tracer, various endpoints are given that we can use to create networks and one of them is the server. This single server provides lots of services like HTTP, FTP, email, DHCP, etc.

Before enabling the DHCP service on the server, we must assign the static IP address to the server to establish connectivity.





PC should be configured to accept IPs from the DHCP server so we will change the IP configuration from static to DHCP. To configure the DHCP service, we have to click on the DHCP tab and turn on the DHCP service.

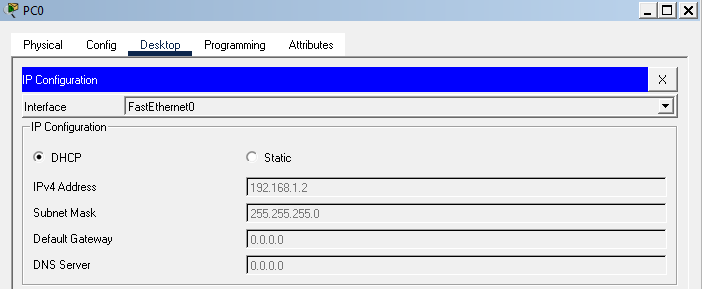
We can change the default name of the pool which is server pool.

We can set up the default gateway and DNS if required as per our network design.

Define the start IP address so the server will issue the IP address according to our scope mentioned.

We now have to define the maximum number of users so the server will not lease IP addresses to the devices if the limit is reached. In this example, the defined limit is 10 in pool1, now the server will only release 10 IP addresses even if the mentioned IP range scope has a high number of IP addresses. Multiple pools can be added to the server and if any pool is not required then it can be removed easily.

One extra pool name as pool1 has been added to the server with a different IP range so now the server has a lot more IPs to assign.



We can see in the image above that PC has been assigned an IP address successfully by the DHCP server. An assigned IP address is from the configured scope on the server.

Now, as we are done configuring the DHCP on the server. We will configure the Router as a DHCP server in the following [packet tracer lab](https://www.packettracerlab.com/).

https://www.packettracerlab.com/wp-content/uploads/2022/05/router-as-dhcp.png

We have to configure the same parameters on the Router as well however we have to use the Router's command-line interface to set up the routers with DHCP capabilities.

We will configure DHCP on the Cisco router with 4 easy steps.

Creating a pool and naming the pool. In this lab, we have given the name 'dynamic' to the

* 1. **DHCP pool.**

*Command : Router(config)#ip dhcp pool Dynamic*

Defining the ranges of the addresses that the Router will lease to the clients.

*Command: Router(dhcp-config)#network 192.168.1.0 255.255.255.0*

Excluding the range of IP addresses that we do not want the Router to lease, this comes in handy when we want to keep some IPs that can be assigned to the devices statically whenever required in our network. In this example, we have assigned IP 192.168.1.1 to the Router so we should exclude this IP to prevent any IP address conflict.

Command: Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.5

Finally, we will enable the DHCP service on the Router using the following command. Command: Router(config)#service dhcp

Additionally, the time limit can be defined for the lease. For e.g, if we want the Router to lease IP for a certain period then we can configure the same using the following command.

*Command: Router(config)#lease 10 10 10*

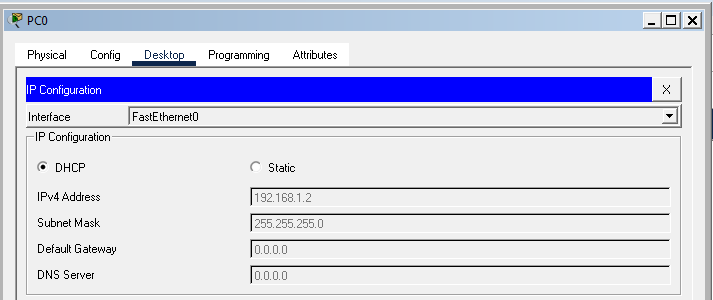
This would mean that Router will lease the IP for 10 days 10 hours and 10 mins. After the defined period, the client will be given a new IP address.

OR

Use the following command to lease the IP for an indefinite time.

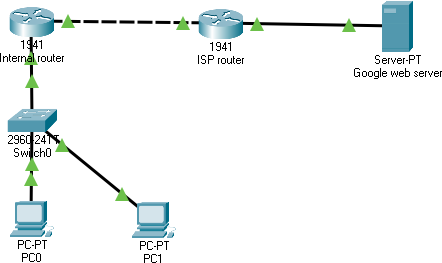
*Command: Router(config)#lease infinite.*

In the image, we can see that the PC has received the IP address from the Router so now the Router is acting as a DHCP server.



1. **Web Server and Internet:**

To simulate the internet, we have to configure the server endpoint given. The server can provide web service.

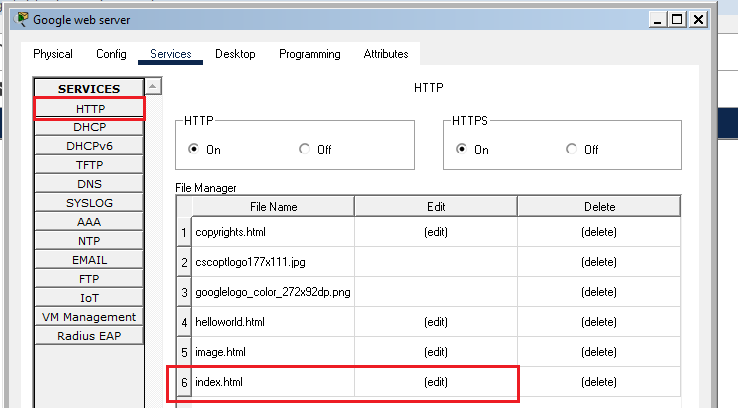


We have two hosts that will be able to access the internet via an ISP router. Our internal network is connected to the ISP router. The interface of the internal Router which is connected to the ISP router has been given public IP address. This is static IP that has been configured on the interface.

ISP router is further connected to the Google web server so after the successful configuration of our network, we should be able to access the google.com

* 1. **How to configure the web server.**

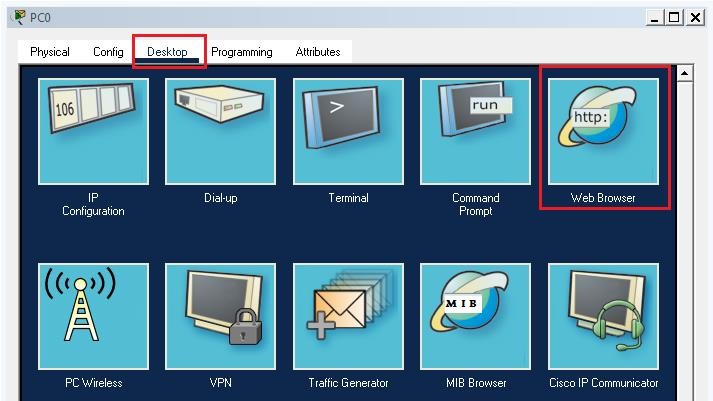
We have to open services and click on HTTP service. This service is enabled by default and we can see that server is hosting some files already. These files are present by default and when we point the web browser to this server, this server will serve the web page to our browser.



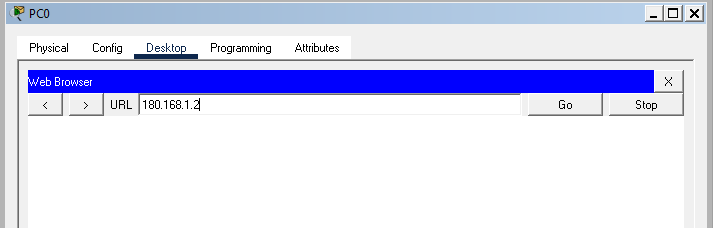
We have configured this server as a Google web server and it is serving a Google web page. To change the content of the webpage, we have to edit the index file present in the web server.

For testing purposes, we can copy the source code of any side that you want the webserver to show and paste it into the index file. After saving the file, the web server will show sites according to the source code.

Now, we can test the web server by opening the browser on the PC and pointing it to the server.



We have to enter the IP address of the web server in the URL and press enter. If everything is configured properly then we should see the browser loading the webpage successfully.



Before opening the browser, we must make sure that the connectivity of the server is fine. Download the lab and test the Google web server and if you want the server to host any other site then change the index file present on the server.

This lab is the smaller presentation of a big network like the Internet. This is the way how the internet works however there are thousands of routers and servers connected forming a huge network.

You can try adding more servers with different sites and accessing those sites on the browser on the PC.

1. **DNS in Cisco packet tracer and how to configure DNS on Cisco router**

There are a couple of ways in which we can configure DNS in packet tracers. We will configure DNS on the Cisco router and endpoint server.

DNS means domain name server, and DNS contains a database of domain names and IP mapping. DNS servers are very helpful as we don't have to remember the IP address and we can use the domain name instead. Names are much easier to type and learn so DNS plays an important role in every network.

When we enter google.com in the web browser the DNS server finds out the mapped IP of that domain and the HTTP request is forwarded to that IP address.

* 1. **Configure DNS on the Cisco router**

To configure the Cisco router as DNS, we have to enable the DNS service on the Router using the following command.

Router(config)#ip dns server

Now, we have to map the names with the IP address using the following command. Router(config)#ip host PC1 192.168.1.5

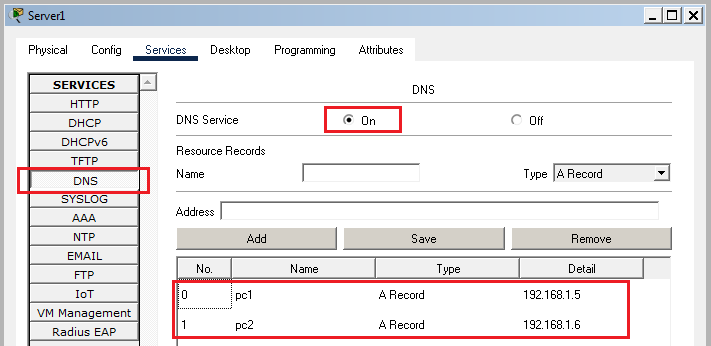
Router(config)#ip host PC2 192.168.1.6

Finally, we need to configure the DNS server IP in the PC setting. In this case, as the Router is configured as a DNS server, we will use the Router's IP.

Now, we can ping one PC from another PC with their names.

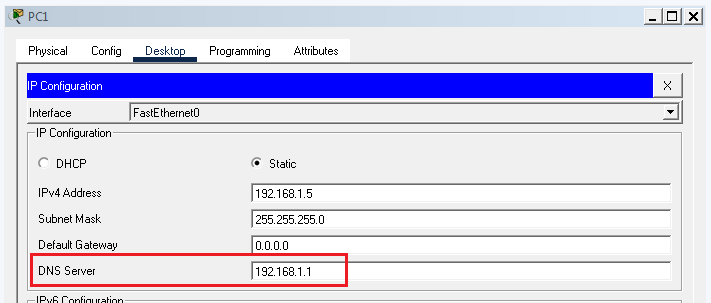
Please note that Configuring the Cisco router as a DNS server is not possible in packet tracer as it does not provide this functionality however If you want to try this lab then you can use GNS3 as it has all the commands.

**Configuring DNS in Cisco packet tracer with the available server endpoint**



To configure the DNS server, we have to enable the DNS service in the server which is disabled by default.

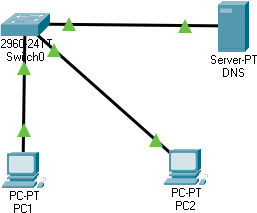
Now, we have to add an A record or create a name for IP mapping in the server. Finally, PCs should be configured with the IP address of the server in the DNS settings.

That is all required to successfully enable the DNS server in packet tracer. Now, we should be able to ping the PCs with the names.

C:\>ping PC2

Pinging 192.168.1.6 with 32 bytes of data:

Reply from 192.168.1.6: bytes=32 time=35ms TTL=128 Reply from 192.168.1.6: bytes=32 time<1ms TTL=128 Reply from 192.168.1.6: bytes=32 time<1ms TTL=128 Reply from 192.168.1.6: bytes=32 time<1ms TTL=128

As expected, we can ping one PC from another with the names. Perform this lab and ping the PC with names,

and you will see the successful ping replies.

Activity for you: Create a mapping for the Switch in the server so that PCs can ping the Switch with the name 'Switch'

**Lab Task CDP**

**Task 1**

Router#show cdp neighbors Router#show cdp neighbors detail

**Task 2**

From Switch 0

local interface – Remote interface and IP address

1. FastEthernet 0/1 FastEthernet 0/1- 192.168.1.100
2. FastEthernet 0/2 FastEthernet 0/0- 192.168.1.3
3. FastEthernet 0/3 FastEthernet 0/0- 192.168.1.4

From Switch 1

1. FastEthernet 0/2 FastEthernet 0/0- 192.168.1.45/24
2. FastEthernet 0/3 FastEthernet 0/0- 192.168.1.43/24

**Task 3**

Router(config)#interface FastEthernet 0/1 Router(config-if)#no cdp enable

**Task 4**

Switch>show CDP

**DHCP**

**Task 5**

Configure the router for DHCP on the given IP addresses and connect a switch and three PCs. To obtain IP addresses from DHCP, open the IP configuration on the PC. Attach a screenshot of the PCs receiving IP addresses through DHCP.

**WEB SERVER**

**Task 6**

Add different servers to other sites and access those sites on the PC browser. Attach a screenshot of the PCs accessing these sites.

**DNS**

**Task 7**

Create a mapping for the switch in the server so that PCs can ping the switch with the name ‘switch’.

# LAB 8: Switch Redundant connections and Loops (STP)

**Objectives**

* Using CDP protocol to find out neighbor information in Cisco packet tracer.
* Setting up a DHCP server in Cisco packet tracer.
* Configure a web server in the Cisco packet tracer and access the internet in the packet tracer.

1. **Introduction to Spanning tree protocol**

In typical network topology, we have redundant connections between switches. Redundant connections play a very crucial role as it eliminates the single point of failure in the network. However, redundant connections create a loop in the network. And to prevent those loops in networks the Spanning Tree Protocol chooses the best link while blocking the redundant links.

Root Bridge is the most important Switch in a Spanning Tree Network. And all the other switches choose the best way to reach a Root Bridge and block the redundant links. Therefore, it is very important to choose the best Switch in the network as a Root Bridge.

The root is selected based on a Bridge ID. So, whichever Switch will have the lowest Bridge ID, that very Switch will be selected as a Root Bridge. Bridge ID is made up of a priority number and the MAC address. And by default, all switches have the same priority number – 32768 to be precise – so the Spanning Tree relies on a MAC address for the selection of Root Bridge. But the problem is that by default any switch which has the lowest Bridge ID can be automatically selected as a Root Bridge. And if that Switch is slow then it will slow down the entire network because its network traffic will pass through that Switch. Hence, every Spanning Tree Network must have the best Switch as a root.

By default, the Spanning Tree is enabled on the switches so if we create a redundant connection on switches then the Spanning Tree Protocol will automatically come into action to prevent a loop in the network. Therefore, for maximum optimization, it is very important to select the right Switch as a Root Bridge.

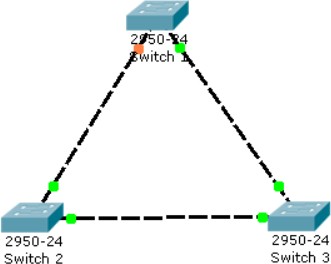


Fig 8.1 switches STP configuration

We cannot, however, change the MAC address of a switch so we will have to change the priority number of switches to influence the selection of a Root Bridge.

The highest priority is considered as the lowest No. i.e. 0. However, the priority is a multiple of 4096.

In this lab, we will try changing the priority of a switch to be able to select the Switch of our choice as a **Root Bridge**. Root Bridge is selected as per the VLAN number so we have to mention for which VLAN, the Switch is a root. We will also enable a newer version of the Spanning Tree which is a Rapid Spanning Tree.

The RSTP protocol is the new enhanced version of the original STP protocol. It uses an enhanced negotiation mechanism to directly synchronize topology changes between switches, it no longer uses timers as in the original STP protocol, which results in a much faster reconvergence time. The maximum allowed network diameter for the RSTP protocol is 40 switches.

Perform Spanning tree protocol configuration in packet tracer.

**Lab Task**

1. Select switch 1 as a root bridge
2. Enable rapid spanning tree protocol

**Lab Configuration**

**Task 1 making a Switch root bridge** Switch(config)#spanning-tree vlan 1 priority 0 or

Switch(config)#spanning-tree vlan 1 root primary

*Switch the priority of the Switches to see the changes and report.*

**Subtask** – switchport should be configured as Trunk (like 0/1-5)

* Speed 100
* duplex full
* VLAN 1 all switches should on the same network 192.168.1.0

-Vlan no shutdown

**Task 2**

All Switches

Switch(config)#spanning-tree mode rapid-pvs

# LAB 9: Configuring Static Routing

**Objectives**

* Configure the Router for static routing.

**A. Static Route**

Static routes – Static routes are those routes that are configured manually on the Router. Static routes are useful when we have a very small network with a small number of routers. We do not require routing protocols in a small network where routes are not constantly changing and we do not have new routers added often in the network.

A static route is easy to configure however it takes time to build manual routes so dynamic routing with routing protocol is the only choice we have when working with big networks.

In big networks, we have thousands of routes are they are constantly changing so in that situation, we have to use the advanced routing protocol which helps us to easily handle all the routes, and routing protocol also provides us with many features like load balancing, auto alternative route selection, etc

In this example, you will learn to perform the basic configuration of the static route. First of all, we have to assign the IP Addresses to the router interfaces that are connecting different routers. After assigning the IP Addresses, you should easily be able to ping the devices that are directly connected. However, to reach out to the routers that are not directly connected, or to reach the other networks, routers should have their routes specified in the routing table.

Routers can learn their routes with the help of a routing protocol, or else we can specify the static route on those routers so that they can reach other networks that they don't yet recognize.

And to create a static route, we have to make the Router aware of the other networks so that it can reach out to them. And for that, it has to go out to its interface.

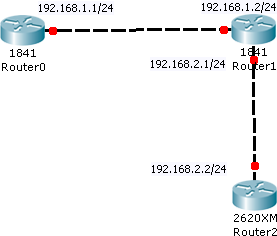
For example, in the following scenario we have to tell Router 0 that to reach the 192.168.1.0 network, it has to go out to its interface using the IP Address 192.168.1.2

Now, we don't have to configure the static route on router 1 as it already knows about the networks 192.168.1.0 and 192.168.2.0 being directly connected to these networks. However, we have to configure the static route on router 2 as it does not know about the 192.168.1.0 network.

Once we have configured the static routes, you will be able to see those static routes in your routing table. Using command

Router# show ip route static

And finally, to confirm, you can try pinging router 2 from router 0 and check if they have been configured correctly.

**Lab Task**

**Task 1**

**Router 0**

Router(config)#interface FastEthernet 0/0 Router(config-if)#ip address 192.168.1.1

255.255.255.0

Router(config-if)#no shutdown

**Router 1**

Router(config)#interface FastEthernet 0/0 Router(config-if)#ip address 192.168.1.2

Fig 10.1 shows the IP address to configure Static Route

255.255.255.0

Router(config-if)#no shutdown

Router(config)#interface fastethernet 0/1

Router(config-if)#ip address 192.168.2.1 255.255.255.0 Router(config-if)#no shutdown

**Router 2**

Router(config)#interface FastEthernet 0/0

Router(config-if)# ip address 192.168.2.2 255.255.255.0 Router(config-if)#no shutdown

**Task 2**

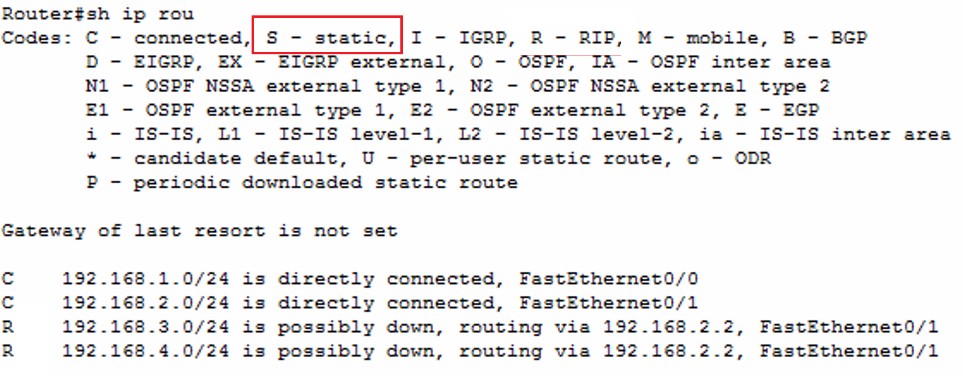
**Router 0**

Router(config)#ip route 192.168.2.0 255.255.255.0 192.168.1.2

**Task 3**

**Router 2**

Router(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.1

**Task 4**

**Any Router**

Router#show IP Route

# LAB 10: Configuring WAN Connection and Default Routes

**Objectives**

* Serial connection explanation and configuration in packet tracer.
* Configuring router for default routes.

1. **Configuring Serial Connections**

The Serial connection is used to create a WAN connection with the help of a service provider who offers a dedicated leased line to its customers.

Business organizations buy leased lines to establish a WAN connection to connect with different offices and business sites that could physically be thousands of miles apart. Businesses have to pay for these leased lines according to the service availed. And accordingly, the service providers charge for this service i.e. based on the bandwidth they offer to their client organizations.

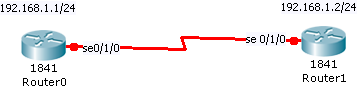
One of the connections used for a leased line is the Serial Connection in Cisco-based networks. If we have Cisco routers on both sides of the network then the default encapsulation known as HDLC will be used by the Cisco routers. However, this will not work with other brands' routers (i.e. with the non-Cisco routers) because this protocol is solely a Cisco proprietary.

If we want to establish a successful connection with a router of other vendors then we must configure the same data link protocol on both routers. If there will be a mismatch then a connection cannot be established and we will see the status of the interface as down under the data link.

If we are configuring a new Cisco router then by default the data link protocol would be HDLC however if we are configuring an old device then we should check the configuration and if there is a mismatch then we have to configure the same protocol on both routers.

Although HDLC works out of the box on all Cisco routers however it is not widely used because of its proprietary nature and it does not provide many features so PPP protocol is used by most organizations. Even on Cisco routers, organizations prefer the PPP protocol over the HDLC protocol due to its advanced features and benefits.

In this lab, we will configure a Serial Connection between the routers. We will set up a clock rate at 56000, which will provide a speed of 56 Kbps. In the real world, the DCE side of the cable is configured by the service provider. Generally, the clock speed is configured according to the availability of the bandwidth speed that the service provider is offering. The following lab uses a serial cable that will simulate a service provider. We will configure the clock speed on the Router that has the DCE side connected.



**Lab Task of serial connections**

**Task 1**

**Router 0**

Router(config)#interface serial 0/1/0

Router(config-if)# ip address 192.168.1.1 255.255.255.0 Router(config-if)# no shut

**Task 2**

**Router 1**

Router(config)#interface serial 0/1/0

Router(config-if)# ip address 192.168.1.2 255.255.255.0 Router(config-if)# no shut

**Task 3**

**Router 0**

Router(config-if)# clock rate 56000

1. **Setting up Default Routes Objectives**

* Configuring default static route in Cisco packet tracer and discussing the role of the static route in networking.

**Theoretical Description**

A Default Static Route is configured on the routers so the traffic can be transferred to a default route if there is no entry in the routing table for a specific network.

Before sending packets to the other networks, routers check their routing table. The Router drops the packets if it is unable to find a specific route on which traffic should be sent. And when a router does not find the route in its routing table it sends the traffic to a default route, if that default route is configured. So basically, the traffic is sent out of the interface mentioned in the default route in the absence of an entry in the routing table for the traffic.

The default route is most useful when sending traffic to a public network like the Internet because it is not possible to have the routing table for the entire Internet. Hence, the default route helps the routers to send the packets going out to the internet.

In the local area network, when the destination address is not available in the local network then the data is sent out of the default gateway which is then routed to the other networks by routers; similarly, the default route helps to find the destination which is not available in the routing table.

In the below lab, we will create a default route on the Router to enable routing between different subnets.

The below network scenario is not common in the real world, we have just created this lab to show how the default route can route the traffic without the routing table however we can test the real default route in action if we configure the default route on the Router which is connected to the internet. In the packet tracer lab, we cannot emulate the internet so we are testing the default route in a simple network.

Note: we will only create a default route on the Router. After that, the Router should be able to route traffic. You can ping router 4 from router 0 to check the routing in action.

Command explanation – IP route 0.0.0.0 0.0.0.0 192.168.1.2

In the above command, 0.0.0.0 means that any IP address with any subnet mark should be sent out of interface 192.168.1.2 if a route is not present in the routing table.

Once we configure the default route, we can see the default route in the routing table with the S\* symbol while static routes are shown with just the S symbol.

Before configuring the default route, you will see that the gateway of last resort is not set however once the default route is configured, the gateway of last resort is the Router's interface from which traffic will be sent out.

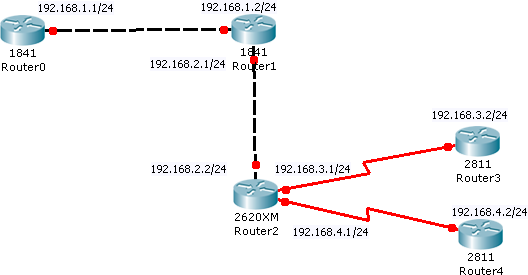


Fig 10.2 Default routes setup using serial connections

**-**

**Lab Task of Default Routes**

**Task 1**

**Router 0**

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.2

**Task 2**

**Router 1**

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.2

**Task 3**

**Router 2**

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.2.1

**Task 4**

**Router 3**

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.3.1

**Router 5**

Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.4.1

**Task 6**

**Router 0**

Router#ping 192.168.4.2

**LAB 11: Setting up Dynamic Routing Protocol RIP ver.1 Objectives**

* Configure the hostname of a router.
* Configure the password for a router.
* We will configure three Cisco routers.
* We will enable these routers for dynamic routing using the RIP protocol.

**Theoretical Description**

Setting up router names and passwords

By default, the Cisco router is configured with the hostname 'router' and Switch is configured with the default hostname of 'switch' so we must change the default names of all the devices to make it relevant to the network diagram and this also makes it easy to understand and help us recognize the device when we are configuring the device.

It is the best practice to give hostnames to the devices according to the location for example if the Router is situated in the network then we can give the hostname as network followed by the model number [Network 1700] or we can give the hostname as per the role of the device for example If a router is connecting to the ISP then a good hostname can be ISP router.

Once a password is configured, users will be prompted to type in that password whenever they enter the Privileged Exec Mode. And if both the 'Enable Password' and 'Secret' are configured, then the users will have to access the Privileged Mode with 'Enable Secret' as enable secret is considered a superior password.

In this lab, we will also configure the Console line password and Auxiliary line password. To set up the Console line and Auxiliary line passwords we have to get under the line configuration mode of both lines.

We will also edit the hostname of our device. The device's name will instantly change when we enter the command – 'hostname *device-name* on the Command-line Interface. And to check the configured password for the privileged mode you have to exit back to the User Exec mode by simply typing Exit while on the Privileged mode. Then, you will have to type the password every time you enter into the Privileged mode.

You can check the password by initiating a Console connection once again. However, the Auxiliary line password cannot be simulated in the Packet Tracer.

Basic router configuration in packet tracer

Configuration of RIP protocol is very easy as compared to some of the link-state routing protocols like OSPF or EIGRP however RIP protocol does not offer that many features and RIP has a very simple working mechanism. RIP protocol uses hop counts when directing the traffic in the network.

RIP protocol is still widely used due to its simplicity and it is favored in small company networks where there is a fewer number of routers used small networks do not even need advanced routing protocols as they rarely use features that are provided by the advanced routing protocols while big companies with hundreds of Router and complex networks use advance routing protocols as they provide more features that are required for the stability and the functioning of the big networks so at the end it comes up to the requirement of the network.

To set up routers, we will assign an IP address to the router interfaces. It's the best practice to give a unique name to the Router, as well as describe the interfaces of the routers.

To enable the routing between routers we will use a basic routing protocol called Rip. After implementing the Rip protocol on all routers, we can look into the routing table of every Router to check if it has learned the routes with the help of the Rip protocol. We can check the routing table using the command 'show IP route'.

After the successful configuration of the routing protocol, we must see the routes in the routing table learned with the help of RIP and if we are unable to see the routes then we have to check the configuration and troubleshoot the issue with the configuration.

In Figure 9.1, check out the routes that are learned using RIP protocol by the Router, you should also make sure that Router should learn the routes of all the networks as shown.

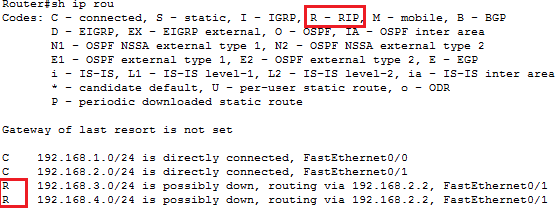


Fig 9.1 Router with IP routes connected and RIP implemented

**R** is representing the RIP protocol so all the routes having R in the front are learned by the Router via RIP protocol. By default, the RIP protocol auto-summarizes the routes so we have to disable the summarization on each Router.

We will also disable auto summarization of the routes in the routing table by using the command 'no auto-summary. Also, we will set up a MOTD banner on all the routers.

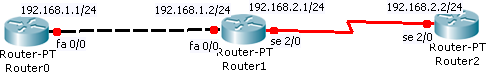


Fig 9.2 Routers connected with other Routers using RIP protocol

**Use debug command to get the details :**

**# debug ip rip**

>> Use this command to show all routes configured in router, say for router R1 :

**R1# show ip route**

>> Use this command to show all protocols configured in router, say for router R1 :

**R1# show ip protocols**

**Lab Task**

**Task 1** Router(config)#hostname R1 R1(config)#

**Task 2**

R1(config)#enable password cisco

**Task 3**

R1(config)#enable secret cisco

**Task 4**

R1(config)#line con 0 R1(config-line)#password lab R1(config-line)#login

**Task 5**

R1(config)#line aux 0

R1(config-line)#password ciscolab R1(config-line)#login

**Task 6 hostname**

|  |  |  |
| --- | --- | --- |
| **Router 0** | **Router 1** | **Router 2** |
| Router(config)#hostname Islamabad | Router(config)#hostname Lahore | Router(config)#hostname Karachi |

**Task 7 IP address to router interfaces**

|  |  |  |
| --- | --- | --- |
| **Router 0** | **Router 1** | **Router 2** |
| Router(config)#in fa 0/0 Router(config-if)#ip add 192.168.1.1 255.255.255.0  Router(config-if)#no sh | Router(config)#in fa 0/0 Router(config-if)#ip add 192.168.1.2 255.255.255.0  Router(config-if)#no sh  Router(config-if)#in se 2/0 Router(config-if)#ip add 192.168.2.1 255.255.255.0  Router(config-if)#no sh Router(config-if)#clock rate 56000 | Router(config)#in se 2/0 Router(config-if)#ip add 192.168.2.2 255.255.255.0  Router(config-if)# no sh |

**Task 8**

|  |  |  |
| --- | --- | --- |
| **Router 0** | **Router 1** | **Router 2** |
| Router(config)#router rip Router(config-router)#ver 1 Router(config-router)#network 192.168.1.0  Router(config-router)#no auto- summary | Router(config)#router rip Router(config-router)#ver 1 Router(config- router)#network 192.168.1.0 Router(config- router)#network 192.168.2.0 Router(config-router)#no auto-summary | Router(config)#router rip Router(config-router)#ver 1 Router(config-router)#network 192.168.2.0  Router(config-router)#no auto- summary  Router(config)#interface fastEthernet 0/0 Router(config-if)#ip address 192.168.1.1 255.255.255.0  Router(config-if)#no shutdown |

**Task 9**

|  |  |  |
| --- | --- | --- |
| **Router 0** | **Router 1** | **Router 2** |
| Router(config)#in fa 0/0  Router(config-if)#description connection to headquarter | Router(config)#in fa 0/0 Router(config-if)#description connection to branch 1 Router(config)#in se 2/0 Router(config-if)#description connection to branch 2 | Router(config)#in se 2/0 Router(config-if)#description connection to headquarter |

**Task 10** On all routers set MOTD

Router(config)#banner motd / —- UNAUTHORIZED ACCESS IS NT ALLOWED —- /

# LAB 12: Implementing Router Information Protocol (RIP) ver. 2

**Objectives**

* Configure the RIP protocol on all the routers.

**Introduction to Routing Protocols**

Static routing is not feasible in a large network. Hence, to implement routing in an easier way we can use dynamic routing protocols.

Routing information protocol (RIP) is one of the dynamic protocols that can be used for routing. The best part is that the Rip protocol is very easy to configure.

We will configure Rip version 2 in this lab.

RIP version 1 was introduced in 1988 when networks were comparatively simple that did not require complex routing. An earlier version of RIP had some limitations hence RIP version 2 was introduced in 1993 which improved some of the features of the RIP protocol. RIP is a distance-vector routing protocol and hops count to determine the route in the network. The RIP protocol only works till 15 hops and it does not work if the network is more than 15 hops away so this prevents RIP to work properly in a big network.

Major differences between versions 1 and 2

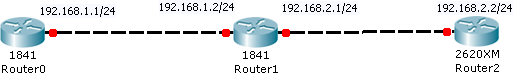
1. RIP V2 supports classless networks, which means we can use VLSM [Variable length subnet mask] in our network while RIP V1 does not support subnetted networks.
2. RIP V2 supports authentication while RIP V1 does not support authentication which makes RIP v1 prone to hacking attacks while Rip v2 provides added security while configuring the networks.
3. RIP V2 uses multicast packets for routing updates while RIP V1 uses broadcast packets which increases unnecessary traffic in the network.

To configure RIP Ver2 on a router, we just have to type the "version 2" command after the "router rip" command to enable version 2 on any router. After configuring RIP version 2, we have to advertise the directly connected networks by using the command **'network *id*** ' after enabling the RIP protocol on all the routers. Once the Rip protocol is configured properly you will be able to see the routes in the routing table, learned with the help of Rip protocol by the routers.

Below is an example of a route that is learned after configuring the RIP protocol:

*R 192.168.2.0/24 [120/1] via 192.168.1.2, 00:00:28, FastEthernet0/0*

You can verify and check routes in the routing table by using the command 'show IP route'. We will also disable auto summarization by the Rip protocol.



**Lab Task**

**Task 1**

**Router 0**

Router(config)#router rip Router(config-router)#version 2

Router(config-router)#network 192.168.1.0 Router(config-router)#no auto-summary

**Router 1**

Router(config)#router rip Router(config-router)#version 2

Router(config-router)#network 192.168.1.0

Router(config-router)#network 192.168.2.0 Router(config-router)#no auto-summary

**Router 2**

Router(config)#router rip Router(config-router)#version 2

Router(config-router)#network 192.168.2.0 Router(config-router)#no auto-summary

# LAB 13: Open-Ended Lab

**Objectives**

1. Apply the concepts of computer networks to design the network topology.

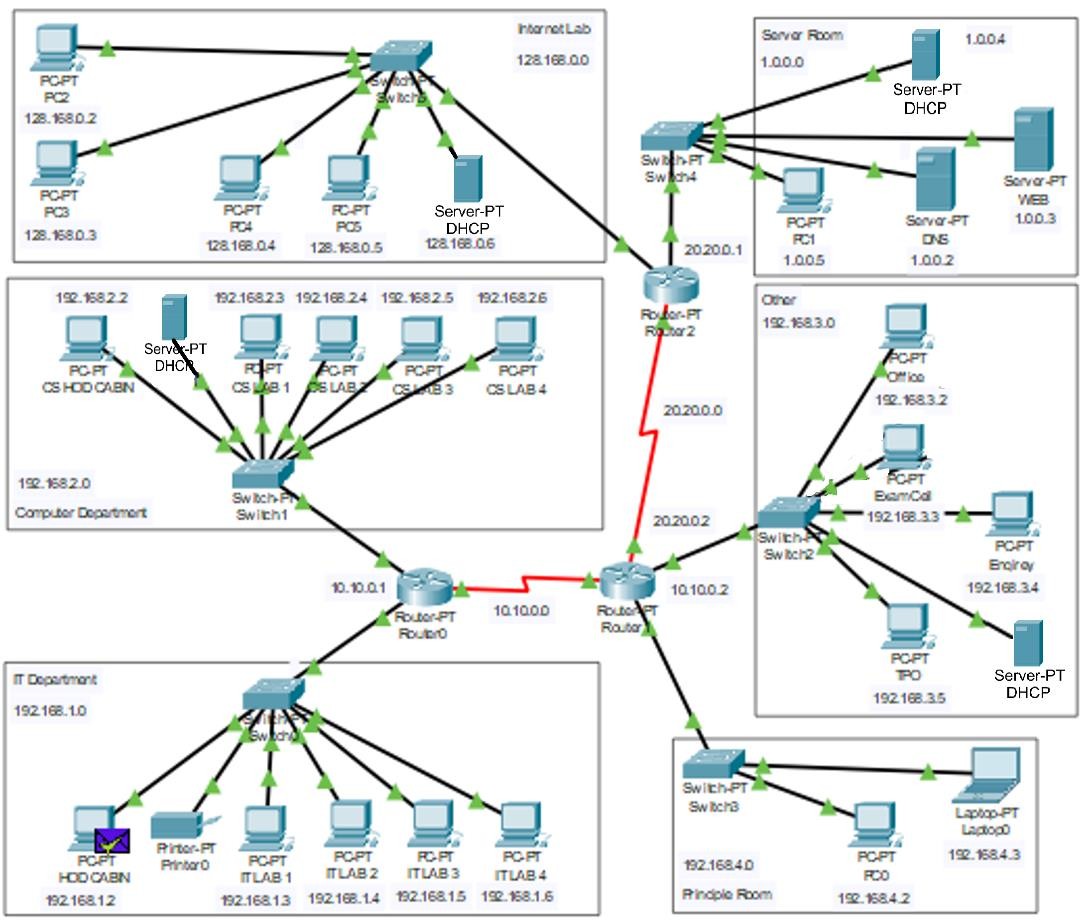
Students have to set up an enterprise-level network and test the connectivity. The network address i.e., the first octet of the IP addresses is the last two digits of your roll number (the last three octets can be of your choice).

**Note: If the last two digits of your roll number are 00, then take 100 as the first octet.**

* 1. Design the topology in the Cisco packet tracer for enterprise-level and configure the network as shown in the figure below (Minimum 2 sites and 3 routers).
  2. Change the name of routers and switches to your name, e.g., <your name>\_SW1,

<yourname>\_SW2, <yourname>\_R1.

* 1. Configure the router using RIPv2, check the connectivity across each end device (PC/Laptop), and attach the screenshots.



**Tasks:**

**Figure 13.1 Enterprise-level network**

1. **Apply** the concepts of computer networks to design the network topology.
2. **Demonstrate** the output at each step.
3. **Express** the outputs and results of the assigned task with greater clarity in a document and complete it in the given time frame.

**Objective**

# LAB 14: Lab Project

To sum up, the work learned during the labs, students have to create a network and implement the technologies necessary for a working network.

Students need to prepare an enterprise-level network. With the following requirements.

1. LAN requirements
   1. 4 sights with multiple switches and routers.
   2. DHCP server, Web server.
   3. VLAN min 3 for each site.
   4. STP setup.
2. WAN requirements
   1. 5 routers (name them city-wise accordingly).
   2. RIP ver. 2 implementation.
   3. DNS setup (Name routers city-wise and Switches campus/business-wise).
   4. Serials connections between the routers and Fast Ethernet connection with its designated LAN.
   5. PPP encapsulation.
3. **Apply** the concepts of computer networks to design the network topology.
4. **Demonstrate** the output at each step.
5. **Express** the outputs and results of the assigned task with greater clarity in a document and complete it in the given time frame.

# Appendix ‘A’ Writing a Lab Report

* 1. **Overview**

This document describes a general format for lab reports that a student should adopt and is recommended. This document may describe the labs of computer networks but this is only a helpful document and explains about writing a lab report.

Lab reports are the most frequent kind of document written in any domain and can count for as much as 20% of lab marks. Yet, if little time or attention is devoted to how to write them will help the student to attain the above-mentioned marks. Worse yet, each teacher wants something a little different.

Regardless of variations, however, the goal of lab reports remains the same: document your findings and communicate their significance. With that in mind, we can describe the report's format and basic components. Knowing the pieces and purpose, you can adapt to the particular needs of a course or a teacher.

A good lab report does more than present results or tasks; it demonstrates the writer's comprehension of the concepts behind the Lab work. Merely recording the expected and observed work is not suffice; you should also identify how and why differences occurred, explain how they affected your task, and shows your understanding of the task at hand.

Bear in mind that a format, however helpful, cannot replace clear thinking and organized writing. You still need to organize your ideas carefully and express them coherently.

* 1. Typical Components
     1. **Font and Size**

The report should be written in Times New Roman, font size 10, whereas, the headings should be in **BOLD** with proper numbering bullets e.g. 1.0, 2.0, 3.0 with a subheading level 2 as 1.1, 1.2,

2.1, 2.2. Whereas, level 3 headings as 1.1.1, 1.1.2, 2.1.1, and so on.

* + 1. **Header and Footer**

Lab Report header should contain; Roll No. XXXXX (Left), (Spring XX) (Mid), Lab X (Right)

Lab Report Footer should contain; Computer Networks (Left), Software Engineering Department (Mid), Page No. X out of Total (Right) e.g, Page 9 | 12

***NOTE: Remember to add “Different first page” from Layout > Page setup, if the first page is desired by an instructor.***

* + 1. **Main Document Body**
       1. Lab Title Heading
       2. Abstract of the Lab
       3. Equipment required for the Lab
       4. Introduction to the Lab
       5. Lab Task
          1. Tasks chronology
          2. Transcribing task results
          3. Discussion on tasks
       6. Conclusion
       7. Appendices

1. **The Title Heading** needs to contain **Lab No. X** top Center, **BOLD**, Name of the Lab. The title should be as mentioned in the lab manual (i.e. "**Lab No.1: Preparing Ethernet Cables**".
2. **The Abstract** summarizes four essential aspects of the report: **the purpose/Objective** of the lab, what did you learn from the lab, and the major conclusion. The abstract often also includes a brief reference to the theory behind the learning or methodology. The information should enable readers to decide whether they need to read your whole report. The abstract should be one paragraph of 100-200 words.

Quick Abstract

**Must have:**

1. Purpose
2. Leaning aspect
3. Major conclusion

**May include:**

* 1. Brief method
  2. Brief theory

**Restrictions:**

ONE page 200 words MAX

1. **Equipment required for Lab**

Mention hardware and software as subheadings

Equipment can usually be a simple list, but make sure it is accurate and complete. In some cases, you can simply direct the reader to a lab No, of manual or standard procedure:

"Equipment was set up as in Lab manual."

***Quick Intro***

**Must Have:**

1. Purpose of the Lab
2. Important background and/or theory

**May include:**

* 1. Description of specialized equipment
  2. Justification of experiment's importance

1. **The Introduction** is more narrowly focused than the abstract meaning it elaborates on each aspect covered during a specific lab. It states the objective of the lab and provides the reader with background on why this lab is important. State the topic of your lab clearly and concisely, in one or two sentences:

**Note on Verb Tense**

Introductions often create difficulties for students who struggle with keeping verb tenses straight. These two points should help you navigate the introduction:

* + The experiment is already finished. Use the *past* tense when talking about the experiment.

"The objective of the lab **was**..."

* + - The lab, the theory, and the equipment used still exist; therefore, these get the present tense:

"The purpose of this lab **is**..."

"The results of the ping command enlist..." "The command executed on router1 displays...

1. **Lab Tasks** describe the process in chronological order. Using a clear paragraph structure, explain and attach all steps in the order as happened. If the instructor asks, you can simply state that you followed the procedure mentioned in some X or Y lab of the manual or labs earlier performed. For example, the router was configured as mentioned in lab 7 or the switch was configured as per lab No. X.

Be sure you still document occasions when you did not follow the instructions exactly. If you've done it right, another student should be able to duplicate your experiment.

A student should at least write a minimum of two **precautions** while documenting performed tasks, in the task section.

**Transcribing Task Results** are usually dominated by tables, and figures; however, you still need to state all performed tasks explicitly in verbal form.

Graphics need to be clear, easily read, and well labeled (e.g. Figure 1: router on the stick). An important strategy for making your lab work effective is to draw the reader's attention to them with a sentence or two, so the reader has a focus when reading the graph.

In most cases, providing a sample figure is sufficient in the report. Leave the remainder in an appendix. Likewise, if you have raw data it can be placed in an appendix. Refer to appendices as necessary, pointing out trends and identifying special features.

**Discuss** is the most important part of your Lab, you show that you understand the lab beyond the simple level of completing it. Explain tasks, some people like to think of this as the "subjective" part of the report. By that, they mean this is what is not readily observable. This part of the lab focuses on the question of understanding "What is the significance of the task, what have you learned, and why it is important to learn?" To answer this question explain it in the discussion:

More particularly, focus your discussion with strategies like these:

**1. Analysis**

What do the lab task indicate clearly? What have you found?

Explain what you know with certainty based on your results and draw conclusions:

**2. Interpretation**

What is the significance of the lab? What ambiguities exist?

What questions might we raise?

Find logical explanations for problems in the data:

1. Conclusion can be very short in most undergraduate labs. Simply state what you know now for sure, after performing the lab:
2. **Appendices typically** include such elements as raw data, calculations, graphs pictures, or tables that have not been included in the report itself. Each kind of item should be contained in a separate appendix.

Make sure students refer to each Appendix at least once in your report. For example, the task section of lab 1 might state during the discussion: “the categories of the UTP and STP cables are contained in Appendix A.