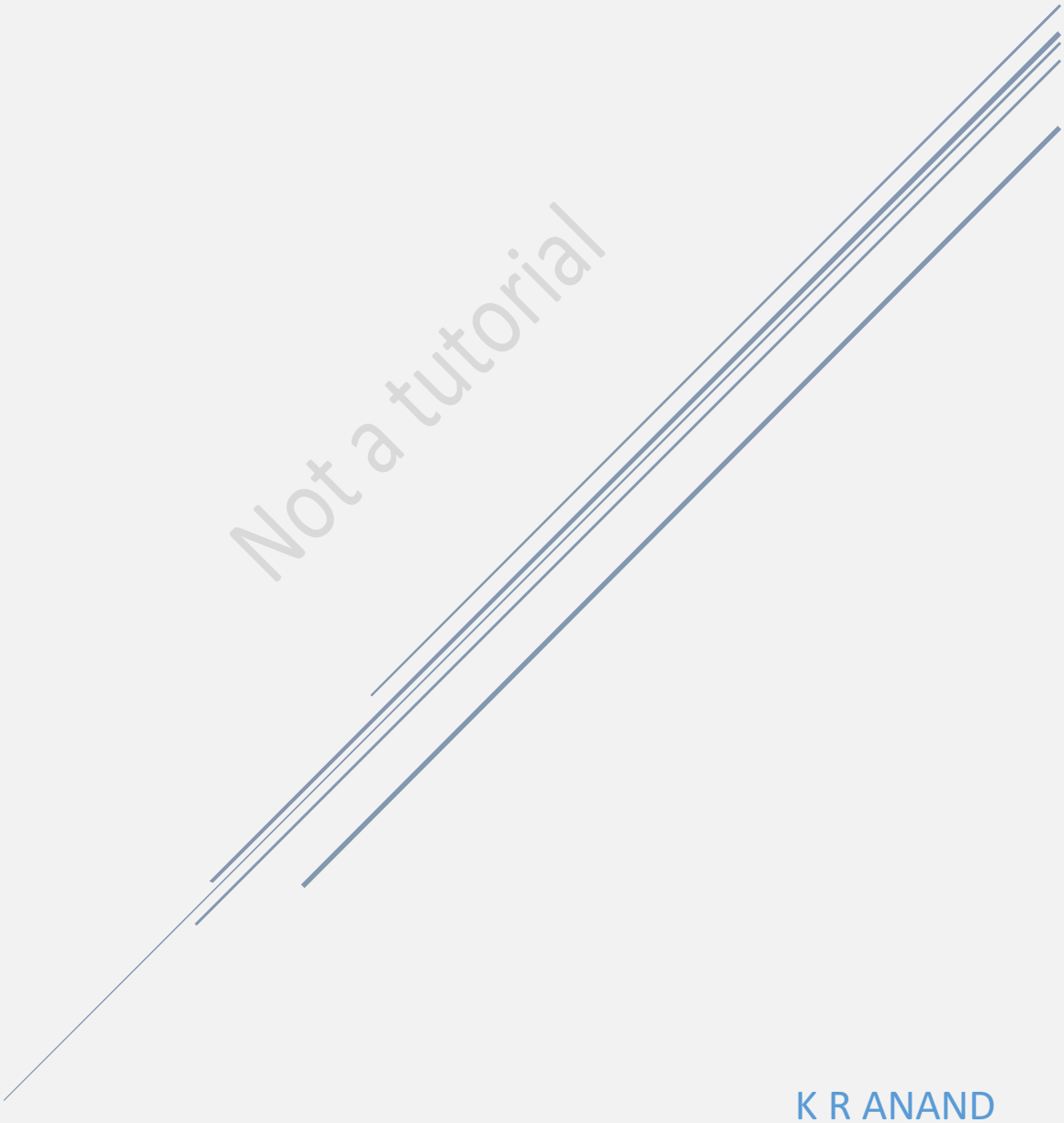
# MY CCNA

## Not a tutorial




K R ANAND
My CCNA

# Table of Contents

# TABLE OF TABLES ;-)



# TABLE OF FIGURES

NOTE

This is my journey into CCNA.

blank

page

# Networking Basics Overview

## What is a network?

A network is interconnection between devices so that the devices can communicate and share resources with each other. This is mainly achieved by the devices (~~geeky~~ technical people call it as *nodes* or *hops*) and a *transmission medium*.

Physically this may be achieved in two ways with respect to the *transmission medium*:

1. Wired medium
2. Wireless medium

## Network types

On the basis of size networks can be sub divided into:

- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WAN: Wide Area Network
- PAN: Personal Area Network
- CAN: Campus Area Network



We will be focusing on some network types below:

### LAN

A Local Area Network (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone's home or office. In general, LAN will be used as one type of transmission medium.

#### Characteristics of LAN

Here are important characteristics of a LAN network:

- It is a private network, so an outside regulatory body never controls it.
- LAN operates at a relatively higher speed compared to other WAN systems.

- There are various kinds of media access control methods like token ring and Ethernet.

Advantages of LAN

Here are pros/benefits of using LAN:

- Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
- You can use the same software over the network instead of purchasing the licensed software for each client in the network.
- Data of all network users can be stored on a single hard disk of the server computer.
- You can easily transfer data and messages over networked computers.
- It will be easy to manage data at only one place, which makes data more secure.
- Local Area Network offers the facility to share a single internet connection among all the LAN users.

Disadvantages of LAN

Here are the important cons/ drawbacks of LAN:

- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
- Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

## MAN

A Metropolitan Area Network or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.

Characteristics of MAN

Here are important characteristics of the MAN network:

- It mostly covers towns and cities in a maximum 50 km range
- Mostly used medium is optical fibers, cables
- Data rates adequate for distributed computing applications.

Advantages of MAN

Here are pros/benefits of using MAN system:

- It offers fast communication using high-speed carriers, like fiber optic cables.
- It provides excellent support for an extensive size network and greater access to WANs.
- The dual bus in MAN network provides support to transmit data in both directions concurrently.
- A MAN network mostly includes some areas of a city or an entire city.

Disadvantages of MAN

Here are drawbacks/ cons of using the MAN network:

- You need more cable to establish MAN connection from one place to another.
- In MAN network it is tough to make the system secure from hackers

## WAN

WAN (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN's using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.

Characteristics of WAN:

- The software files will be shared among all the users; therefore, all can access to the latest files.
- Any organization can form its global integrated network using WAN.

Advantages of WAN

Here are the benefits/ pros of using WAN:

- WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
- Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
- WLAN connections work using radio transmitters and receivers built into client devices.

Disadvantage of WAN

Here are drawbacks/cons of using WAN:

- The initial setup cost of investment is very high.
- It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
- There are more errors and issues because of the wide coverage and the use of different technologies.
- It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
- Offers lower security compared to other types of networks.

## Transmission medium

We are generally going to focus on LAN cables in the upcoming section.

### Wired Medium

This type of networking is more reliable as it uses cables(wires). Mainly there are:

- UTP (Unshielded Twisted Pair) cables:

  *Works on electrical pulses with 2 wires completing the circuit to transfer data*

  UTP cable is up to four twisted pairs of copper wires, enclosed in a protective plastic cover, with the greater number of pairs corresponding to more bandwidth

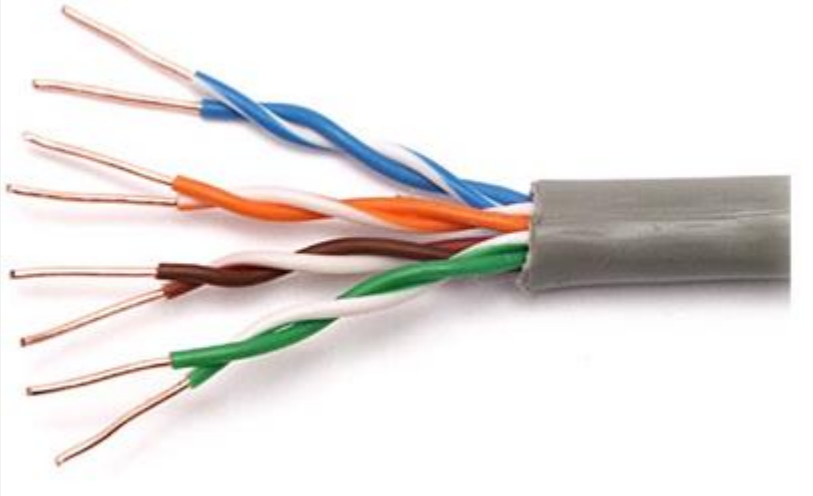


*Figure 1 Unshielded Twisted Pair cable*

There are different types of UTP listed below

| Category | Standard | Data rate | Frequency | # of cores |
|---|---|---|---|---|
| Cat 5 | 100BASE-TX | 100 Mbit | 100 MHz | 4 or 8 |
| Cat 5e | 1000BASE-TX | 1 Gbit | 100 MHz duplex | 8 |
| Cat 6 | EIA/TIA 568B2.1 | 1-10 G bit* | 250 MHz | 8 |
| Cat6A | 10GBASE-T | 10 Gbit | 500 MHz | 8 |
| Cat 7 | 10GBASE-T | 10 Gbit | 600 MHz | 8 |
| Cat 7A | 10GBASE-T | 10 Gbit | 1000 MHz | 8 |
| Cat 8 | 40GBASE-T | 40 Gbit | 1600-2000 MHz | 8 |
| *Depends on length and cable type | | | | |

*Table 1 UTP/STP Categories*

- STP (Shielded Twisted Pair) cable

  *Works on electrical pulses with 2 wires completing the circuit to transfer data.*

  STP Cabling is twisted-pair cabling with additional shielding to reduce crosstalk and other forms of electromagnetic interference (EMI).

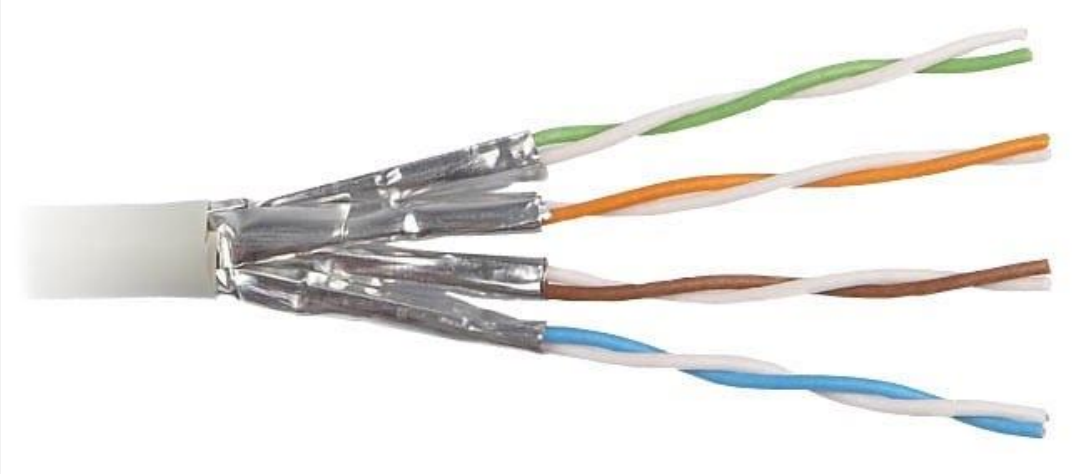


*Figure 2 Shielded Twisted Pair*

- Fiber optic

A fiber-optic cable, also known as an optical-fiber cable, is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. The optical fiber elements are typically individually coated with plastic layers and contained in a protective tube suitable for the environment where the cable will be deployed

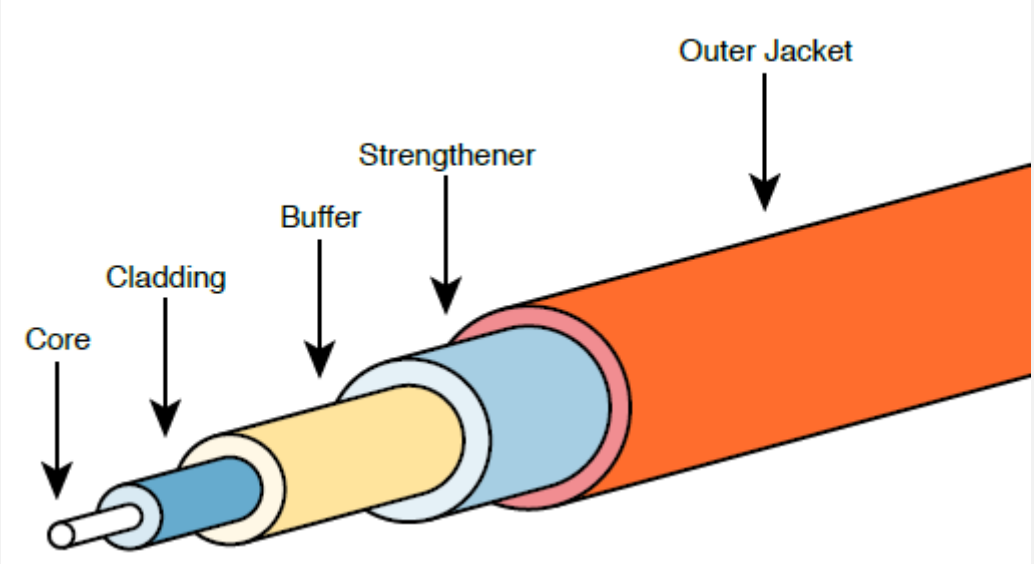



*Figure 3 Fiber cables*

A light source, called the optical transmitter, shines a light into the core. Light can pass through the core; however, light reflects off the cladding back into the core. Figure 4 shows an example with a light emitting diode (LED) transmitter. You can see how the cladding reflects the light back into the core as it travels through the core.

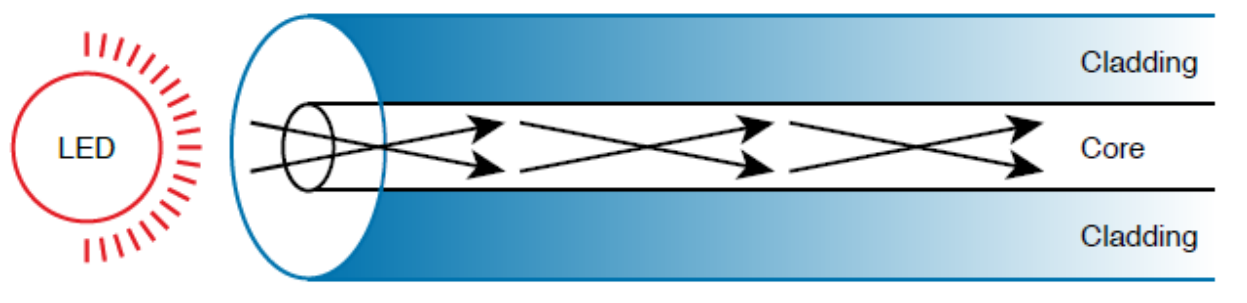



*Figure 4 Single Mode Fiber*

The figure shows the normal operation of a multimode fiber, characterized by the fact that the cable allows for multiple angles (modes) of light waves entering the core.

In contrast, single-mode fiber uses a smaller-diameter core, around one-fifth the diameter of common multimode cables (see Figure 5). To transmit light into a much smaller core, a laser-based transmitter sends light at a single angle (hence the name single-mode).


*Figure 5 Single Mode Fiber*

The standards for fiber optic cables are defined in IEEE 802.3

| Standard | Cable Type | Max Distance |
|---|---|---|
| **10GBASE-S** | Multi-Mode | 400 m |
| **10GBASE-LX4** | Multi-Mode | 300 m |
| **10GBASE-LR** | Single-Mode | 10 km |
| **10GBASE-E** | Single-Mode | 30 km |

*Table 2 Sample fiber standards*

## Wireless Medium

Wireless communication takes place over free space through the use of radio frequency (RF) signals.

See wireless folder for more in AnandMys github repository

## Topology

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

## BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.

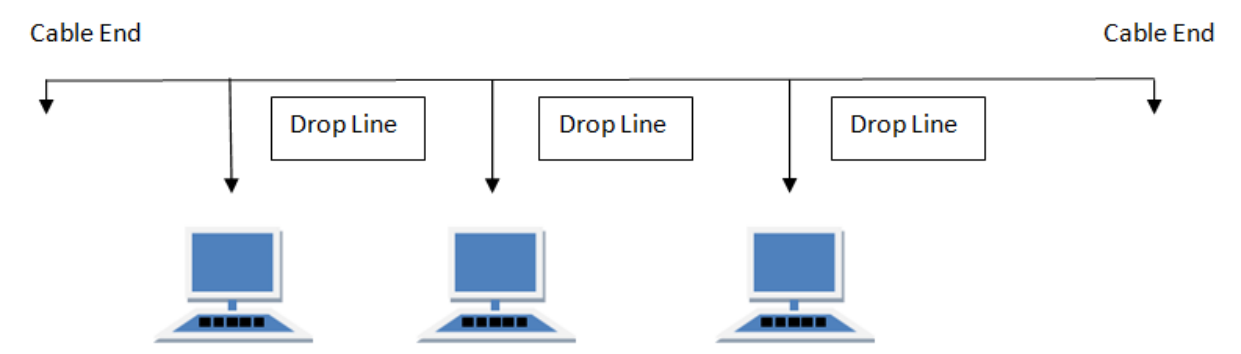



*Figure 6 Bus Topology*



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

## RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

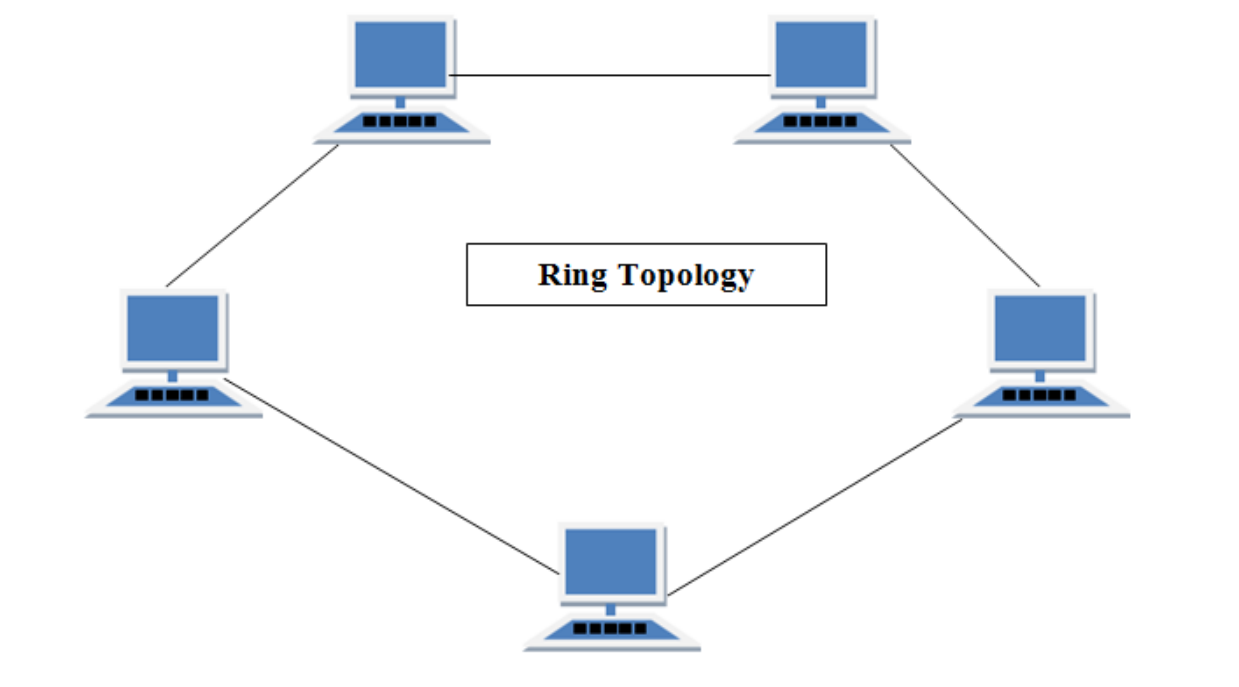



*Figure 7 Ring Topology*

Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

## STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

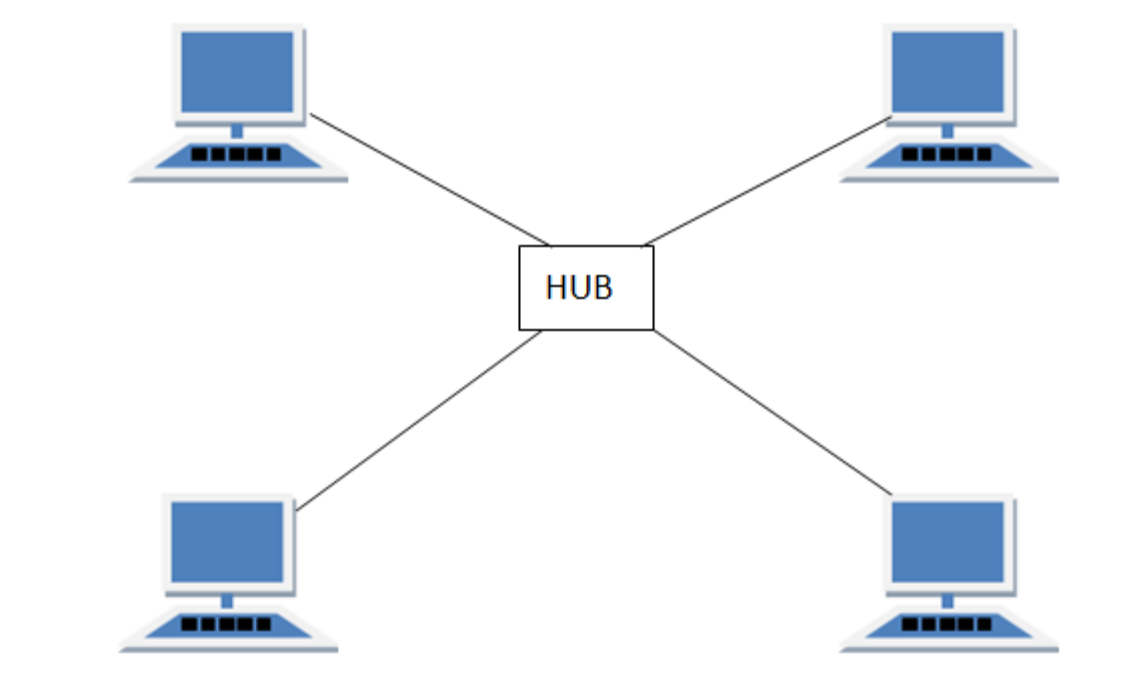



*Figure 8 Star Topology*

Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.

3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity



## MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

1. Routing
2. Flooding

MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

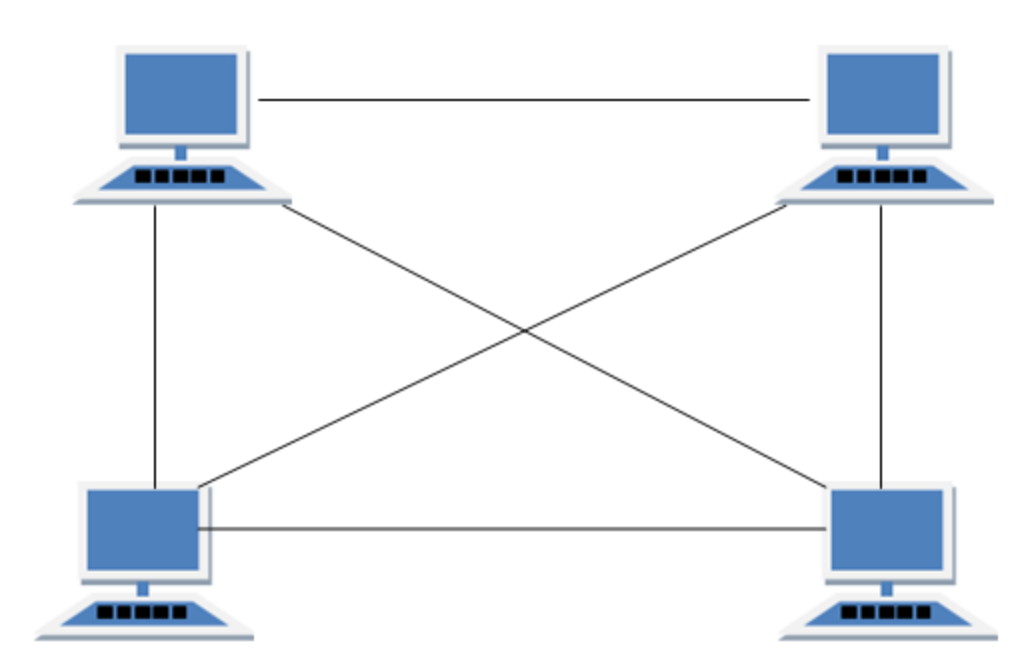


*Figure 9 Mesh Topology*

Types of Mesh Topology

1. **Partial Mesh Topology:** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology:** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

## TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.

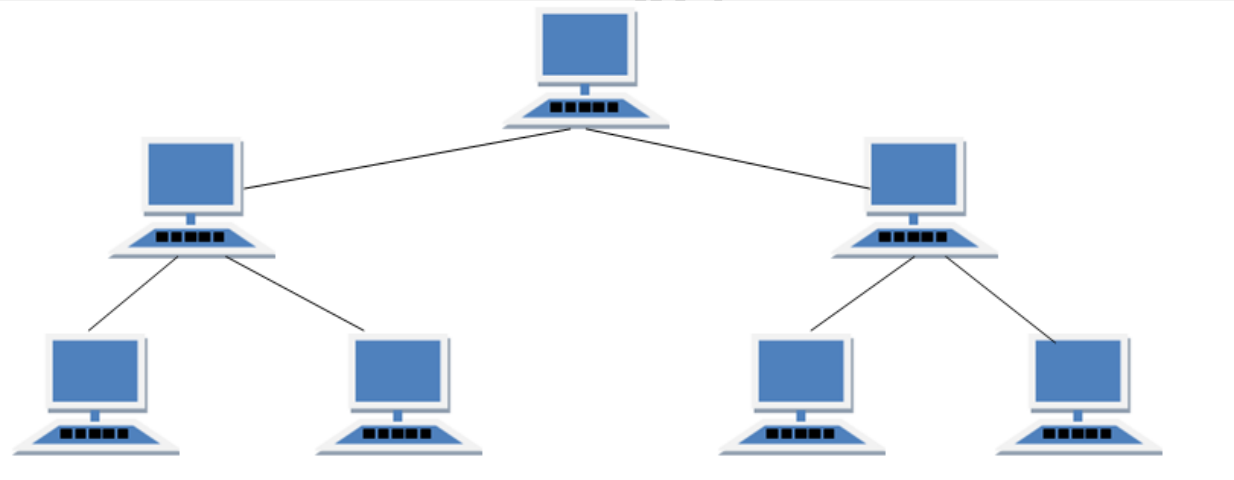


*Figure 10 Tree Topology*

Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.

3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

## HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example, if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

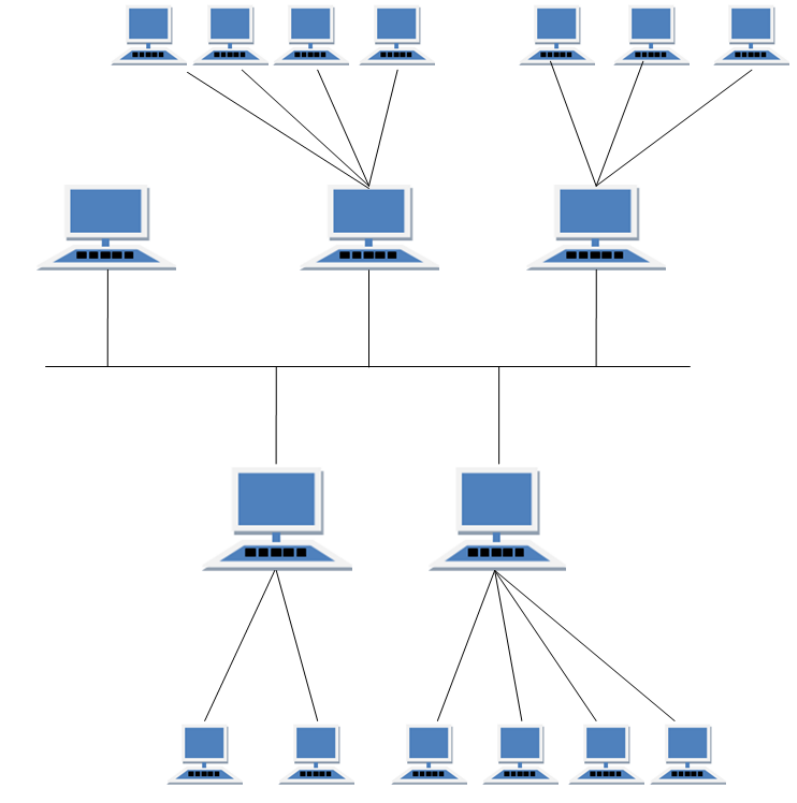


*Figure 11 Hybrid Topology*

Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and troubleshooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

# The TCP/IP model

A *networking model*, sometimes also called either a networking architecture or networking blueprint, refers to a comprehensive set of documents. Individually, each document describes one small function required for a network; collectively, these documents define everything that should happen for a computer network to work. Some documents define a *protocol, which is a set of logical rules that devices must follow to communicate*. Other documents define some physical requirements for networking. For example, a document could define the voltage and current levels used on a particular cable when transmitting data.

## Overview

The TCP/IP model both defines and references a large collection of protocols that allow computers to communicate. To define a protocol, TCP/IP uses documents called Requests For Comments (RFC). (You can find these RFCs using any online search engine.) The TCP/IP model also avoids repeating work already done by some other standards body or vendor consortium by simply referring to standards or protocols created by those groups. For example, the Institute of Electrical and Electronic Engineers (IEEE) defines Ethernet LANs; the TCP/IP model does not define Ethernet in RFCs, but refers to IEEE Ethernet as an option.



The TCP/IP model creates a set of rules that allows us all to take a computer (or mobile device) out of the box, plug in all the right cables, turn it on, and connect to and use the network. You can use a web browser to connect to your favorite website, use most any app, and it all works.

How? Well, the OS on the computer implements parts of the TCP/IP model. The Ethernet card, or wireless LAN card, built in to the computer implements some LAN standards referenced by the TCP/IP model. In short, the vendors that created the hardware and software implemented TCP/IP.

To help people understand a networking model, each model breaks the functions into a small number of categories called layers. Each layer includes protocols and standards that relate to that category of functions, as shown in Figure 12.

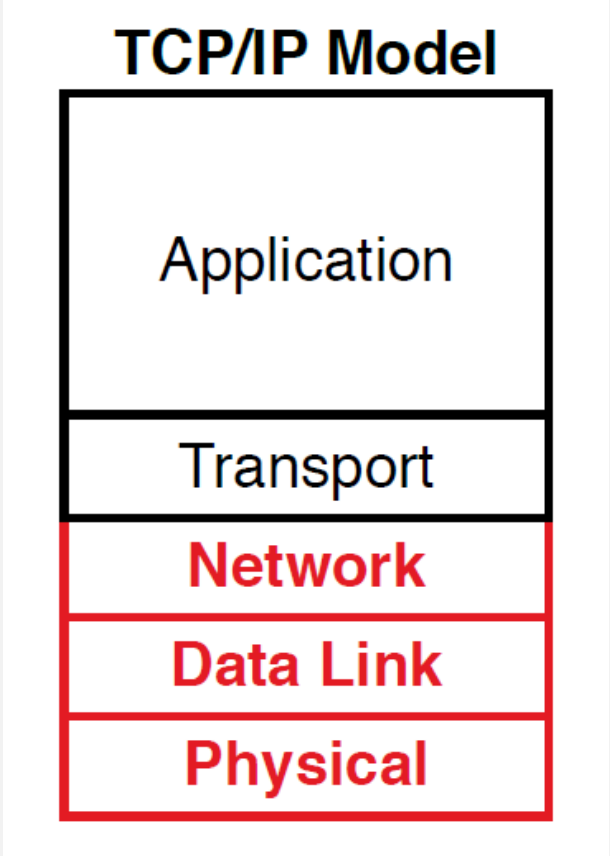



*Figure 12 TCP/IP Stack*

*A slightly different four-layer original version of the TCP/IP model exists in RFC 1122, but for the purposes of both real networking and for CCNA, use the five-layer model shown here*

The TCP/IP model shows the more common terms and layers used when people talk about TCP/IP today.

**Physical layer**: The physical layer focuses on how to transmit bits over each individual link.

**Data Link layer**: The data-link layer focuses on sending data over one type of physical link: for instance, networks use different data-link protocols for Ethernet LANs versus wireless LANs.

**Network Layer**: The network layer focuses on delivering data over the entire path from the original sending computer to the final destination computer.

**Transport Layer**: The transport layer focuses more on the applications that need to send and receive data.

**Application layer**: User interacts with this layer. Ex. A browser, WhatsApp etc

Virtually everything you study for CCNA comes under the networking models. Also it should be noted that **OSI (Open System Interconnect)** model is a reference model which has 7 layers and encompasses everything in CCNA

*We will delve into detailed topics later*

## Protocols

| TCP/IP Layers | TCP/IP Prototocols | | | | |
|---|---|---|---|---|---|
| Application Layer | HTTP | FTP | Telnet | SMTP | DNS |
| Transport Layer | TCP | | | UDP | |
| Network Layer | IP | | ARP | ICMP | IGMP |
| Network Interface Layer | Ethernet | | Token Ring | Other Link-Layer Protocols | |

*Table 3 Prtocol Stack of TCP/IP*

# Help!

An operating system which helps the user's effort in typing the commands. Here are just a few ways in which it does.

- *help* (does not work in packet tracer)

  Provides a brief description of the Help feature in any command mode.

- *?*

  Lists all commands available for a particular command mode.

- *partial command?*

  Provides a list of commands that begin with the character string (no space between the command and the question mark). partial command Completes a partial command name (no space between the command and the ?).

- *command ?*

  Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).

- *command keyword ?*

  Lists the arguments that are associated with the keyword (space between the keyword and the question mark).



## Help examples

*Router> help* (not in packet tracer)

Help may be requested at any point in a command by entering a question mark '?'. If nothing matches, the help list will be empty and you must backup until entering a '?' shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?') and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input (e.g. 'show pr?'.)

*?*

*Router>?*

*Exec commands:*

*<1-99> Session number to resume*

*connect Open a terminal connection*

*disable Turn off privileged commands*

*disconnect Disconnect an existing network connection*

*enable Turn on privileged commands*

*exit Exit from the EXEC*

*logout Exit from the EXEC*

*ping Send echo messages*

*resume Resume an active network connection*

*show Show running system information*

*ssh Open a secure shell client connection*

*telnet Open a telnet connection*

*terminal Set terminal line parameters*

*traceroute Trace route to destination*

*partial command?*

*Router(config)# host?*

*hostname*

*partial command<Tab>*

*Router> en<Tab> enable*

*command ?*

*Router(config-if)#ip ?*

*access-group Specify access control for packets*

*address Set the IP address of an interface*

*authentication authentication subcommands*

*flow NetFlow Related commands*

*hello-interval Configures IP-EIGRP hello interval*

*helper-address Specify a destination address for UDP broadcasts*

*mtu Set IP Maximum Transmission Unit*

*nat NAT interface commands*

*ospf OSPF interface commands*

*proxy-arp Enable proxy ARP*

*split-horizon Perform split horizon*

*summary-address Perform address summarization*

# Cisco iOS modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. Given below are the modes in which Cisco IOS operating system functions:

| Command mode | Access Method | Prompt | Exit Method | Usage |
|---|---|---|---|---|
| **User EXEC** | ***login*** | *R1>* | Issue ***logout*** or ***exit*** command | • Change terminal settings.<br>• Perform basic tests.<br>• Display device status |
| **Privileged EXEC** | From user EXEC mode, issue the ***enable*** command. | *R1#* | Issue the ***disable*** command or the ***exit*** command to return to user EXEC mode. | • Issue show and debug commands.<br>• Copy images to the device.<br>• Reload the device.<br>• Manage device configuration files.<br>• Manage device file systems |
| **Global configuration** | From privileged EXEC mode, issue the ***configure terminal*** command. | R1(config)# | Issue the ***exit*** command or the ***end*** command to return to privileged EXEC mode | Configure the device. |

| Command mode | Access Method | Prompt | Exit Method | Usage |
|---|---|---|---|---|
| **Interface configuration** | From global configuration mode, issue the ***interface*** command. | R1(config-if)# | Issue the ***exit*** command to return to global configuration mode or the ***end*** command to return to privileged EXEC mode | Configure individual interfaces |
| **Line Configuration** | From global configuration mode, issue the ***line vty*** or ***line console*** command | R1(config-line)# | Issue the ***exit*** command to return to global configuration mode or the ***end*** command to return to privileged EXEC mode. | Configure individual terminal lines. |
| **ROMMON mode*** | ROM monitor From privileged EXEC mode, issue the ***reload*** command. Press the Break key during the first 60 seconds | rommon # > | Issue the ***continue*** Command | • Used when iOS image is not available/corrupted<br>• Recovering passwords for the devices |

*Table 4 Cisco iOS modes*

* Does not work under packet tracer

# Overview of Interface Configuration

By default, all interfaces are enabled. The 10/100-Mbps Ethernet interfaces autonegotiate connection speed and duplex. The 10/100/1000-Mbps Ethernet interfaces negotiate speed, duplex, and flow control. The 1000-Mbps Ethernet interfaces negotiate flow control only. Autonegotiation automatically selects the fastest speed possible on that port for the given pair. If a speed is explicitly stated for an interface, that interface will default to half duplex unless it is explicitly set for full duplex.

Many features are enabled on a per-interface basis. When you enter the interface command, you must specify the following:

- Interface type:
  - Fast Ethernet (use the fastethernet keyword)
  - Gigabit Ethernet (use the gigabitethernet keyword)
  - 10-Gigabit Ethernet (use the tengigabitethernet keyword)
- Slot number—The slot in which the interface module is installed. Slots are numbered starting with 1, from top to bottom.
- Interface number—The interface number on the module. The interface numbers always begin with 1. When you are facing the front of the switch, the interfaces are numbered from left to right.

You can identify interfaces by physically checking the slot/interface location on the switch. You can also use the Cisco IOS show commands to display information about a specific interface or all the interfaces.

## Using the interface Command

These general instructions apply to all interface configuration processes:

**Step 1** At the privileged EXEC prompt, enter the **configure terminal** command to enter global configuration mode:

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

**Step 2** In global configuration mode, enter the **interface** command. Identify the interface type and the number of the connector on the interface card. The following example shows how to select Fast Ethernet, slot 5, interface 1:

```
Switch(config)# interface fastethernet 5/1
Switch(config-if)#
```

**Step 3** Interface numbers are assigned at the factory at the time of installation or when modules are added to a system. Enter the **show interfaces** EXEC command to see a list of all interfaces installed on your switch. A report is provided for each interface that your switch supports, as shown in this display:

```
Switch(config-if)#Ctrl-Z

Switch#show interfaces

Vlan1 is up, line protocol is down
  Hardware is Ethernet SVI, address is 0004.dd46.7aff (bia 0004.dd46.7aff)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 interface resets
```

```
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/1 is up, line protocol is down
  Hardware is Gigabit Ethernet Port, address is 0004.dd46.7700 (bia
0004.dd46.7700)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet1/2 is up, line protocol is down
  Hardware is Gigabit Ethernet Port, address is 0004.dd46.7701 (bia
0004.dd46.7701)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
```

```
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
--More--
<...output truncated...>
```

**Step 4** To begin configuring Fast Ethernet interface 5/5, as shown in the following example, enter the **interface** keyword, interface type, slot number, and interface number in global configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet 5/5
Switch(config-if)#
```

## Configuring a Range of Interfaces

The interface-range configuration mode allows you to configure multiple interfaces with the same configuration parameters. When you enter the interface-range configuration mode, all command parameters you enter are attributed to all interfaces within that range until you exit interface-range configuration mode.

To configure a range of interfaces with the same configuration, perform this task:

| Command | Purpose |
|---|---|
| Switch(config)# **interface range** {**vlan** vlan_ID – vlan_ID} \| {{**fastethernet** \| **gigabitethernet** \| **tengigabitethernet** \| **macro** macro_name} slot/interface - interface} [, {**vlan** vlan_ID – vlan_ID} {{**fastethernet** \| **gigabitethernet** \| **tengigabitethernet** \| **macro** macro_name} slot/interface - interface}] | Selects the range of interfaces to be configured. Note the following:<br>You are required to enter a space before the dash.<br>You can enter up to five comma-separated ranges.<br>You are not required to enter spaces before or after the comma. |

**Note** When you use the interface range command, you must add a space between the vlan, fastethernet, gigabitethernet, tengigabitethernet, or macro keyword and the dash. For example, the command interface range fastethernet 5/1 - 5 specifies a valid range; the command interface range fastethernet 1-5 does not contain a valid range command.

**Note** The **interface range** command works only with VLAN interfaces that have been configured with the **interface vlan** command (the **show running-configuration** command displays the configured VLAN interfaces). VLAN interfaces that are not displayed by the **show running-configuration** command cannot be used with the **interface range** command.

This example shows how to reenable all Fast Ethernet interfaces 5/1 to 5/5:

```
Switch(config)# interface range fastethernet 5/1 - 5
Switch(config-if-range)# no shutdown
Switch(config-if-range)#
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to
up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to
up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to
up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to
up
*Oct  6 08:24:35: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to
up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
5, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
3, changed state to up
*Oct  6 08:24:36: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
4, changed state to up
Switch(config-if)#
```



This example shows how to use a comma to add different interface type strings to the range to reenable all Fast Ethernet interfaces in the range 5/1 to 5/5 and both Gigabit Ethernet interfaces 1/1 and 1/2:

```
Switch(config-if)# interface range fastethernet 5/1 - 5, gigabitethernet 1/1 - 2
Switch(config-if)# no shutdown
Switch(config-if)#
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/1, changed state to
up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/2, changed state to
up
```

```
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/3, changed state to
up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/4, changed state to
up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface FastEthernet5/5, changed state to
up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/1, changed state
to
 up
*Oct  6 08:29:28: %LINK-3-UPDOWN: Interface GigabitEthernet1/2, changed state
to
 up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
5, changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
3, changed state to up
*Oct  6 08:29:29: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet5/
4, changed state to up
Switch(config-if)#
```

If you enter multiple configuration commands while you are in interface-range configuration mode, each command is run as it is entered (they are not batched together and run after you exit interface-range configuration mode). If you exit interface-range configuration mode while the commands are being run, some commands might not be run on all interfaces in the range. Wait until the command prompt is displayed before exiting interface-range configuration mode.