**PRACTICAL – 1**

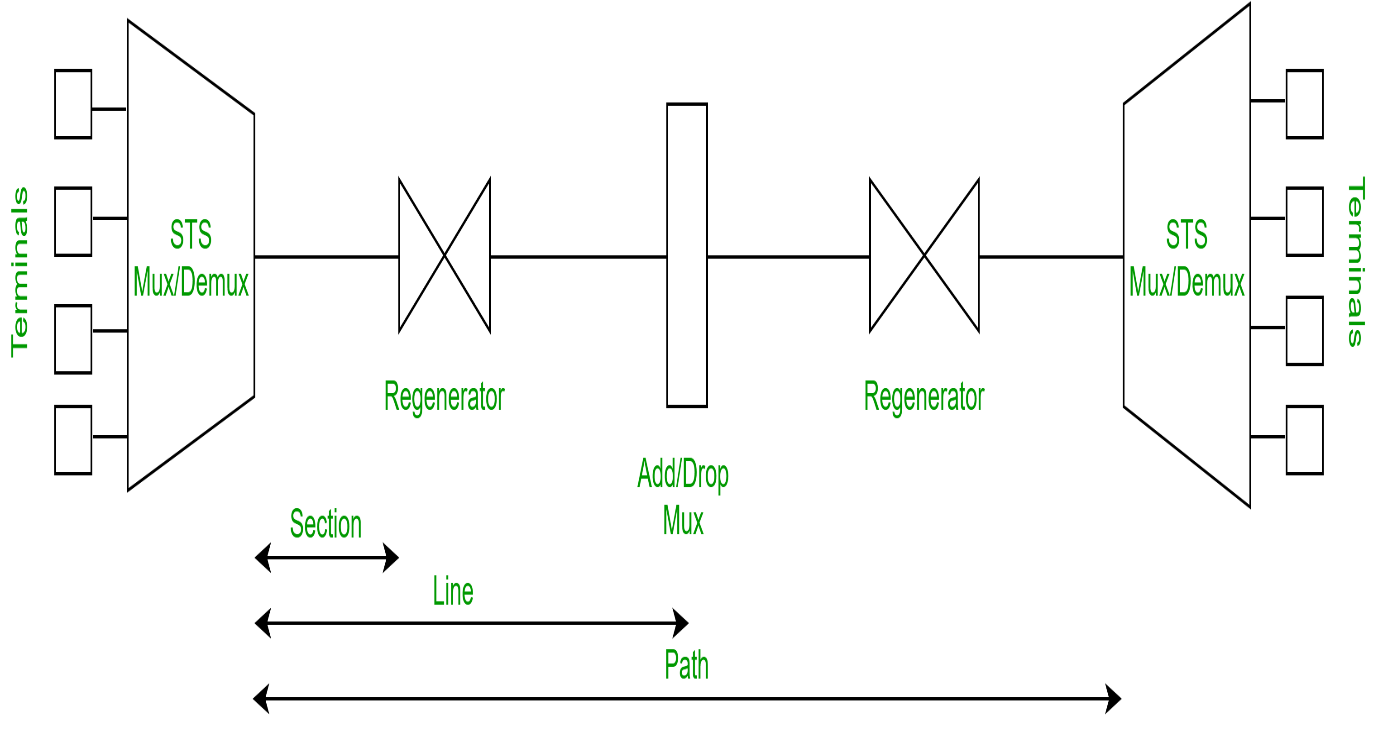
**Aim : Introduction to SONET / SDH networks**

**Synchronous Optical Network(SONET)**

SONET stands for Synchronous Optical Network. SONET is a communication protocol, developed by Bellcore – that is used to transmit a large amount of data over relatively large distances using optical fibre. With SONET, multiple digital data streams are transferred at the same time over the optical fibre.

**Why SONET is called a Synchronous Network?**

A single clock (Primary Reference Clock, PRC) handles the timing of transmission of signals & equipments across the entire network.  
  
**SONET Network Elements:**



1. **STS Multiplexer:**
   * Performs multiplexing of signals
   * Converts electrical signal to optical signal
2. **STS Demultiplexer:**
   * Performs demultiplexing of signals
   * Converts optical signal to electrical signal
3. **Regenerator:**

It is a repeater, that takes an optical signal and regenerates (increases the strength) it.

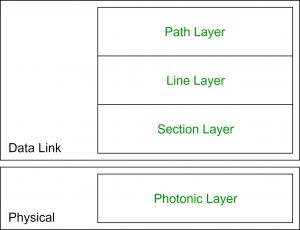
1. **Add/Drop Multiplexer:**

It allows to add signals coming from different sources into a given path or remove a signal.

**Why SONET is used?**

SONET is used to convert an electrical signal into an optical signal so that it can travel longer distances.  
  
**SONET Connections:**

* **Section:** Portion of network connecting two neighbouring devices.
* **Line:** Portion of network connecting two neighbouring multiplexers.
* **Path:** End-to-end portion of the network.



**SONET Layers:**

SONET includes four functional layers:

1. **Path Layer:**
   * It is responsible for the movement of signals from its optical source to its optical destination.
   * STS Mux/Demux provides path layer functions.
2. **Line Layer:**
   * It is responsible for the movement of signal across a physical line.
   * STS Mux/Demux and Add/Drop Mux provides Line layer functions.
3. **Section Layer:**
   * It is responsible for the movement of signal across a physical section.
   * Each device of network provides section layer functions.
4. **Photonic Layer:**
   * It corresponds to the physical layer of the OSI model.
   * It includes physical specifications for the optical fibre channel (presence of light = 1 and absence of light = 0).

**Advantages of SONET:**

* Transmits data to large distances
* Low electromagnetic interference
* High data rates
* Large Bandwidth

**Synchronous Digital Hierarchy (SDH)**

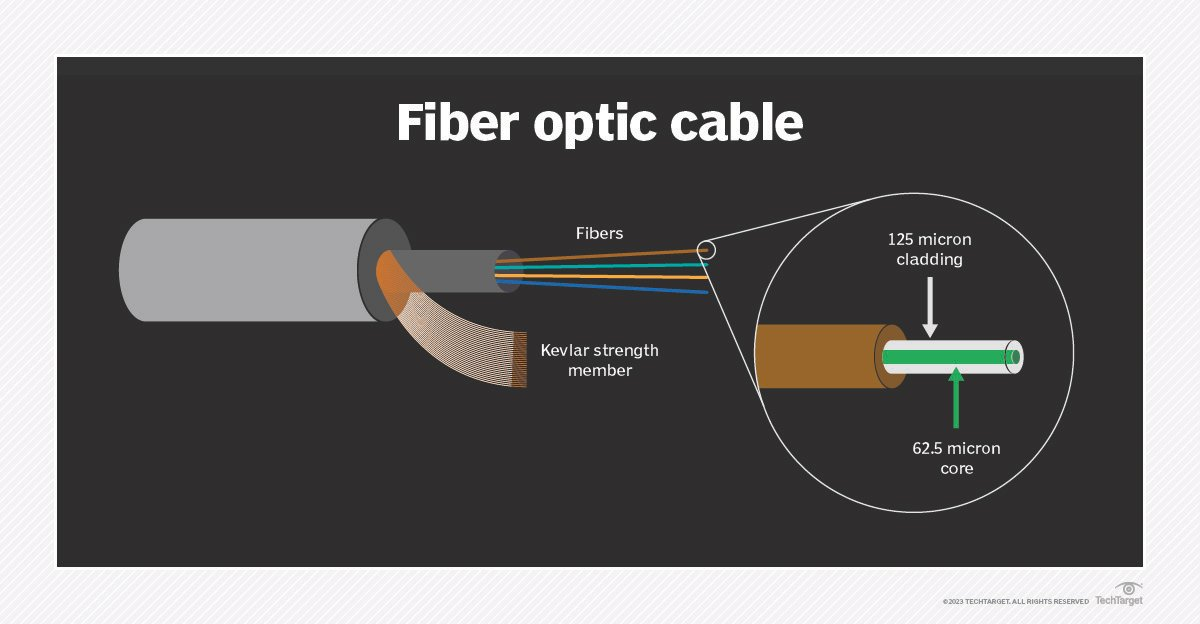
SDH stands for **Synchronous Digital Hierarchy** and it refers to a multiplex technology used in the telecommunication. Synchronous Optical Network is internationally used and is taken equal to SDH. Both technologies provide quite fast and low-priced network interconnection than PDH which stands for Plesiochronous Digital Hierarchy.

SDH allows the data stream to pass having low bit rates to be combined into high rate data streams. As the entire network is synchronous, individual bitstreams can be embedded into and are extracted from high rate data streams quiet easily. Initially, it was developed back in 1985 in the USA under the name of SONET.

**How does Synchronous Digital Hierarchy work?**

On a synchronously clocked network, SDH combines a bit rate of *b* with *n* signals to create data streams with bit rates of *n x b*. This differs significantly from PDH, as PDH comes with individual transmission paths that have minimal clock discrepancies.

The synchronous mode in SDH enables low-order multiplex systems to be added and dropped from higher hierarchy levels. For example, this is how communication links in telephone systems operate. It achieves all this in accordance with the standard that recognizes different hierarchies, such as STM-1, STM-4, STM-16 or STM-64.

The data is transparently transported over the SDH network in containers. In this scenario, users can reserve approximately 5% of the gross data rate for operations, administration and maintenance purposes.SDH basically works with the software running on the network. It often uses [Transaction Language 1](https://www.dpstele.com/network-monitoring/alarm/tl1/faq.php)/[Q3](http://www.cellsoft.de/telecom/dcn.htm) protocols to transport network management data between the system terminal and SDH equipment. Finally, it transports network management data between SDH systems using dedicated embedded data communications channels. So, users can achieve SDH within the section and line [overhead](https://www.techtarget.com/whatis/definition/overhead).

SDH also uses connections based on fiber optic cables, copper lines, and satellite and directional radio links on the physical layer. Regenerators refresh muted or distorted signals, and the multiplexers combine the signals into high-bit rate data streams on the superior layer. However, users can also use virtual containers to transport individual containers of data.

It enables the control mapping of the various signals of different bit rates as well.

**What are key advantages of using SDH technology?** SDH is more extensive and less expensive than traditional PDH technologies. Other benefits of using SDH systems include the following:

* It consistently uses more simplified multiplexing and demultiplexing techniques.
* The optical fiber bandwidth can increase without limit.
* It has improved maintenance protocols with easy growth to higher bit rates.
* Rings provide switching protection to data traffic.
* It quickly interconnects with various networks.
* It has a comprehensive [network management system](https://www.techtarget.com/searchnetworking/definition/network-management-system).
* It has a flexible self-healing network.
* It can transport existing PDH, broadband and broadcast signals.
* It continues to remain popular within telecommunications networks and operators.
* It enables rapid recovery from failure.
* It offers network transmission services on [local area networks](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN) for interactive multimedia, like video conferencing.
* It supports multiple operators or vendors.
* It supports multipoint networking.

**What are key disadvantages of using SDH technology?**

SDH also has a few drawbacks, and while pros far outweigh the cons, these include the following:

* Complexity is increased by directly adding and dropping lower-rate signals that were archived using pointers.
* It demands complicated SDH equipment to manage different traffic types and options.
* It provides a lower bandwidth utilization ratio.
* It is largely software-based and is vulnerable to [cyber attacks](https://www.techtarget.com/searchsecurity/definition/cyber-attack).

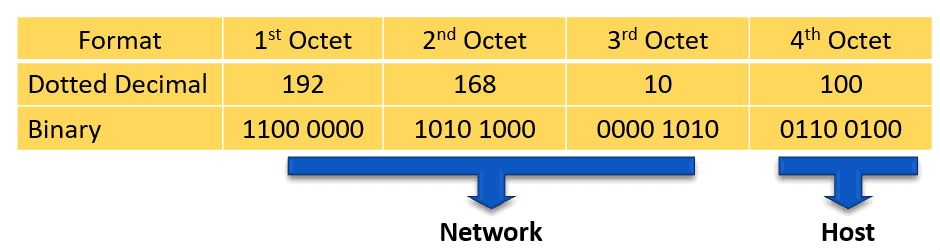
**PRACTICAL – 2**

**Aim : To study about IPV4 addresses.**

**IP** stands for **Internet Protocol** and **v4** stands for **Version Four** (IPv4). IPv4 was the primary version brought into action for production within the ARPANET in 1983.   
IP version four addresses are 32-bit integers which will be expressed in decimal notation.   
Example- 192.0.2.126 could be an IPv4 address.

#### Parts of IPv4

* **Network part:**   
  The network part indicates the distinctive variety that’s appointed to the network. The network part conjointly identifies the category of the network that’s assigned.

[](https://study-ccna.com/wp-content/uploads/ipv4-address-2.png)For example, we have the IPv4 address 192.168.10.100 and a /24 subnet mask. /24 simply means that the first 24 bits, starting from the left side, is the network portion of the IPv4 address. The 8 remaining bits of the 32 bits will be the host portion.

* **Host Part:**   
  The host part uniquely identifies the machine on your network. This part of the IPv4 address is assigned to every host.   
  For each host on the network, the network part is the same, however, the host half must vary.
* **Subnet number:**   
  This is the nonobligatory part of IPv4. Local networks that have massive numbers of hosts are divided into subnets and subnet numbers are appointed to that.

## **IPv4 Address Allocation**

The Internet Protocol address can be allocated to hosts or interfaces either manually or dynamically.

* **Static** – static IP address is set manually on the device. It is best practice to set static IP addresses on network devices, such as routers and switches, and on servers as well.
* **Dynamic** – dynamic IP address can be automatically allocated to a device via Dynamic Host Configuration Protocol (DHCP). Dynamic IP addresses are best to be used on end devices, such as PCs.

#### **Characteristics of IPv4**

* IPv4 could be a 32-Bit IP Address.
* IPv4 could be a numeric address, and its bits are separated by a dot.
* The number of header fields is twelve and the length of the header field is twenty.
* It has Unicast, broadcast, and multicast style of addresses.
* IPv4 supports VLSM (Virtual Length Subnet Mask).
* IPv4 uses the Post Address Resolution Protocol to map to the MAC address.
* RIP may be a routing protocol supported by the routed daemon.
* Networks ought to be designed either manually or with DHCP.
* Packet fragmentation permits from routers and causing host.

#### **Advantages of IPv4**

* IPv4 security permits encryption to keep up privacy and security.
* IPV4 network allocation is significant and presently has quite 85000 practical routers.
* It becomes easy to attach multiple devices across an outsized network while not NAT.
* This is a model of communication so provides quality service also as economical knowledge transfer.
* IPV4 addresses are redefined and permit flawless encoding.
* Routing is a lot of scalable and economical as a result of addressing is collective more effectively.
* Data communication across the network becomes a lot of specific in multicast organizations.
  + Limits net growth for existing users and hinders the use of the net for brand new users.
  + Internet Routing is inefficient in IPv4.
  + IPv4 has high System Management prices and it’s labor-intensive, complex, slow & frequent to errors.
  + Security features are nonobligatory.
  + Difficult to feature support for future desires as a result of adding it on is extremely high overhead since it hinders the flexibility to attach everything over IP.

#### **Limitations of IPv4**

* IP relies on network layer addresses to identify end-points on network, and each network has a unique IP address.
* The world’s supply of unique IP addresses is dwindling, and they might eventually run out theoretically.
* If there are multiple host, we need IP addresses of next class.
* Complex host and routing configuration, non-hierarchical addressing, difficult to re-numbering addresses, large routing tables, non-trivial implementations in providing security, QoS (Quality of Service), mobility and multi-homing, multicasting etc. are the big limitation of IPv4 so that’s why IPv6 came into the picture.

**PRACTICAL - 3**

**Aim : Introduction and installation of Network Simulator (NS-2.30).**

* Network Simulator (NS-2.30) is a widely used open-source software tool for simulating and analyzing computer networks. It allows researchers, network engineers, and students to model and simulate various network protocols, applications, and scenarios in a controlled environment. NS-2.30 provides a platform to study the behavior and performance of network technologies, evaluate new protocols, and analyze network designs without the need for expensive hardware setups.
* The simulator is primarily used for academic and research purposes, enabling users to design, implement, and evaluate network algorithms and protocols. NS-2.30 supports both wired and wireless networks, allowing for the simulation of different types of communication technologies and topologies.
* Key features of NS-2.30 include the ability to define network topologies, traffic patterns, mobility models, and routing algorithms. Users can customize and configure various parameters to recreate real-world network scenarios. NS-2.30 provides detailed trace files and visualization tools to analyze simulation results, aiding in the understanding of network behavior and performance.
* It's important to note that my knowledge is based on information available up until September 2021, and there may have been updates or newer versions of NS-2 beyond 2.30 since then.
* To install Network Simulator (NS-2.30), you can follow these general steps:

1. Download NS-2.30: Obtain the NS-2.30 source code from a reliable source. You might find it on the official NS-2 website or other trusted repositories.
2. Prerequisites: Make sure your system has the necessary dependencies like C++ compiler, Tcl/Tk libraries, and other required packages. You might need to install additional libraries based on your operating system.
3. Extract the Source Code: Unzip or extract the downloaded NS-2.30 source code to a directory of your choice.
4. Configuration and Compilation: Navigate to the extracted directory in the terminal and follow the instructions in the README or INSTALL files. Typically, you'll need to configure the build using commands like ./configure and then compile using make.
5. Testing: After successful compilation, you can run some test scripts to ensure NS-2.30 is working correctly.
6. Environment Variables: Set any necessary environment variables, paths, or aliases that are required for running NS-2.30.
7. Usage: Now you should be able to use NS-2.30 by running various simulation scripts and scenarios.
8. Remember, these are general steps, and the actual process might vary depending on your operating system and any specific requirements of NS-2.30. Always refer to the documentation or guides provided with the source code for accurate and detailed installation instructions.

**PRACTICAL – 4**

**Aim: To study about simple TCL example in NS2.**

##### **What is TCL :**

* TCL[Tool command language] is also an scripting programming language
* NS2 also uses OTCL[Object oriented extension of TCL]
* OTCL is also written in C++ [OTCL=OOPS concepts+ TCL]
* OTCL-configures the system while C++ is also used to implement the code that is frequently executed

##### **Define a Simulator :**

* Create a simulator also using the following TCL code,

               Set nssim [new simulator]

##### **Define the topology :**

* Define the size of the area in which simulation should take place
* Next, we need to define the position of nodes in the network based on the size.

settopo       [new Topography]

$topoload\_flatgrid $val(x) $val(y)

##### **Defining the Output trace files :**

* Used to record the events also which occurs during the simulation
* Here events are also used to signify the node creation, data transfer etc.
* Several trace files are available; we can also choose the trace file as per the result we are also looking for.
* TCL Script for defining the output trace files as follows:

      Set tracef [open results.tr w]

      $ nssimtrace-all $tracef

##### **Defining a General Operations Director[GOD] :**

* GOD is used to store the global information about the network, nodes and state of environment.
* Used to manage detailed operations like Movement patterns of mobile nodes. To create a god object, use the following command,

Create-god (1)

##### **To Define AP/BS and Configure AP/BS :**

* In Ns2, formation of complete network also includes the presence of Access points/Base stations.
* It is necessary to initialize and also configure AP/BS in most of the network
* Commands to create and also configure AP/BS using TCL

To create AP/BS:

               Set ap\_name [$nssimap]

To configure AP/BS:

$nssimap-config –optn\_1 val\_1\

…………………………………

–optn\_nval\_n

    All the above mention TCL scripts are also used to design a network with all the required parameters and also characteristics of the network in NS2.  Next, we have provide a simple TCL script, which also explains you completely about how to program using TCL.

##### [**Simple TCL Program in NS2**](http://networksimulator2.com/ns2-projects-for-cse/)**:**

set ns [new Simulator]**\”Defining Simulator”\**

settracefd       [open Smart\_Grid\_Network\_Topology.tr w]**\”Intializing trace file”\**

settopo       [new Topography]**\”Defining Topography”\**

$topoload\_flatgrid $val(x) $val(y)

set windowVsTime2 [open win.tr w]

setnamtrace      [open Smart\_Grid\_Network\_Topology.nam w]

$ns trace-all $tracefd

$ ns namtrace-all-wireless $namtrace $val(x) $val(y)

###### create-god (1)**\”Creating GOD”\**

set god\_ [God instance]

$ns at 0.5000 “$node\_(0) setdest 100 400 0.15667896543”

$node\_(0) set Z\_ 0.0

$ node\_(0) set Y\_ 128

$node\_(0) set X\_ 142

$ns at 0.5000 “$node\_(1) setdest 150 450 0.15667896543”

$node\_(1) set Z\_ 0.0

$ node\_(1) set Y\_ 128

$node\_(1) set X\_ 44

$ns at 0.5000 “$node\_(2) setdest 140 400 0.15667896543”

$node\_(2) set Z\_ 0.0

$ node\_(2) set Y\_ 193

$node\_(2) set X\_ 144

$ns at 0.5000 “$node\_(3) setdest 160 350 0.15667896543”

$node\_(3) set Z\_ 0.0

$ node\_(3) set Y\_ 199

$node\_(3) set X\_ 55

$ns at 0.5000 “$node\_(4) setdest 120 270 0.15667896543”

$ node\_(4) set Z\_ 0.0

$node\_(4) set Y\_ 243

$ node\_(4) set X\_ 107

if { “$val(traffic)” == “tcp” } {

setpktTypetcp

} else {

setpktTypeexp

}

###### $ns duplex-link $node\_(0) $node\_(2) 2Mb 40ms RED

$ ns duplex-link $node\_(2) $node\_(4) 2Mb 40ms RED

$ns duplex-link $node\_(4) $node\_(3) 2Mb 40ms RED

$ ns duplex-link $node\_(3) $node\_(1) 2Mb 40ms RED

$ns duplex-link-op $node\_(0) $node\_(2) color “lavender”

$ ns duplex-link-op $node\_(2) $node\_(4) color “lavender”

$ns duplex-link-op $node\_(4) $node\_(3) color “lavender”

$ ns duplex-link-op $node\_(3) $node\_(1) color “lavender”

settcp [new Agent/TCP]

$tcp set class\_ 2

$ns attach-agent $n0 $tcp

set sink [new Agent/TCPSink]

$ ns attach-agent $n3 $sink

$ns connect $tcp $sink

$tcp set fid\_ 1

$ ns at 0.1 “$cbr start”

$ns at 1.0 “$ftp start”

$ ns at 4.0 “$ftp stop”

$ns at 4.5 “$cbr stop”

$ ns at 4.5 “$ns detach-agent $n0 $tcp ; $ns detach-agent $n3 $sink”

$ns at 5.0 “finish”

puts “CBR packet size = [$cbr set packet\_size\_]”

puts”CBR interval = [$cbr set interval\_]”

$ns run

     Hope you also would have learnt some basics about TCL. If you wish to have more information about TCL or feel to work on NS-2 also using TCL, approach our online tutoring service. Our experts will teach you completely about TCL in such a way that you will also able to code your own project in the future. We have focused mainly on TCL in this article, if you need any other information regarding NS2 programming, refer also our other articles. Once you are also done with NS2 programming basics, you can approach us for further project guidance and code support. We are also always ready to support you with all your needs and also requirements

**PRACTICAL – 5**

**Aim :- To study about Bluetooth.**

### What is Bluetooth?

Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

**Points to remember for Bluetooth:**

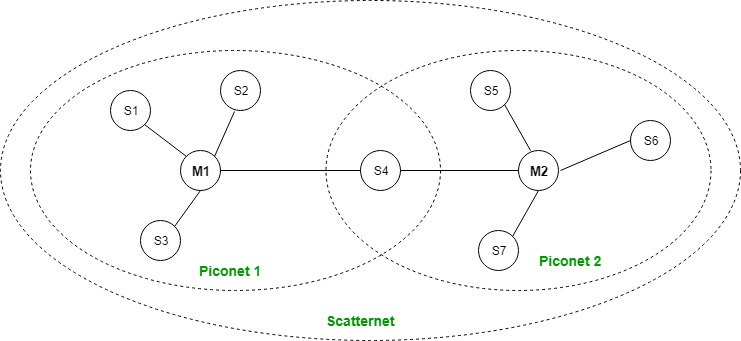
* Bluetooth Transmission capacity 720 kbps.
* Bluetooth is Wireless.
* Bluetooth is a Low-cost short-distance radio communications standard.
* Bluetooth is robust and flexible.
* Bluetooth is cable replacement technology that can be used to connect almost any device to any other device.
* The basic architecture unit of Bluetooth is a piconet.

### Bluetooth Architecture:

The architecture of Bluetooth defines two types of networks:

1. Piconet

2. Scatternet



### Piconet:

Piconet is a type of Bluetooth network that contains**one primary node** called the master node and **seven active secondary nodes** called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has **255 parked nodes**, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

### Scatternet :

It is formed by using **various piconets**. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.

**Types of Bluetooth :**

Various types of Bluetooth are available in the market nowadays. Let us look at them.

* In-Car Headset: One can make calls from the car speaker system without the use of mobile phones.
* Stereo Headset: To listen to music in car or in music players at home.
* Webcam: One can link the camera with the help of Bluetooth with their laptop or phone.
* Bluetooth-equipped Printer: The printer can be used when connected via Bluetooth with mobile phone or laptop.
* Bluetooth Global Positioning System (GPS): To use GPS in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

**Advantage:**

* It is a low-cost and easy-to-use device.
* It can also penetrate through walls.
* It creates an Ad-hoc connection immediately without any wires.
* It is used for voice and data transfer.

**Disadvantages:**

* It can be hacked and hence, less secure.
* It has a slow data transfer rate: of 3 Mbps.
* It has a small range: 10 meters.
* Bluetooth communication does not support routing.
* The issues of handoffs have not been addressed.

**Applications:**

* It can be used in laptops, and in wireless PCs, printers.
* It can be used in wireless headsets, wireless PANs, and LANs.
* It can connect a digital camera wirelessly to a mobile phone.
* It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
* It is used in the sectors of Medical health care, sports and fitness, Military.

**PRACTICAL – 6**

**Aim : To study on Delay Tolerant Networks.**

What is DTN?

Delay/Disruption Tolerant Networking (DTN) is a suite of standard protocols that use information within the data stream (headers attached to data units) to accomplish end-to-end data delivery through network nodes. DTN enables data delivery in situations that involve

• Disconnections (e.g., end-to-end link unavailability)

• Delays (e.g., Deep Space missions)

• Data rate mismatches (e.g., high data rate Science downlinks but lower rate terrestrial connections)

A DTN architecture is a store-and-forward communications architecture in which source nodes send DTN bundles through a network to destination nodes.

Delay-tolerant network architecture

The TCP/IP protocol provides a general-purpose network- and transport-layer service for the terrestrial internet. A DTN does the same in a space environment.

The DTN architecture consists of an end-to-end message-oriented overlay known as the bundle layer. Devices implementing the bundle layer are known as DTN nodes. This layer exists above the transport (or other) layers of the network and below applications.

It provides functionality similar to the layer of gateways described in the original internet and ARPANET designs. But unlike ARPANET, the DTN bundle layer is layer-agnostic and focuses on virtual message forwarding rather than on packet switching.

The bundle layer employs persistent storage for store-and-forward. This allows it to combat network interruptions and delays. The DTN architecture uses variable-length or arbitrary-length messages instead of streams or limited-sized packets. These application data units are transformed by the bundle layer into protocol data units called bundles, which are forwarded by DTN nodes.

This communication abstraction enhances the DTN's ability to make good scheduling and path selection decisions.

In the DTN, bundle sources and destinations are identified by endpoint identifiers (EIDs), which may refer to one or more DTN nodes or endpoints. Security mechanisms are also provided in the DTN to protect the infrastructure from unauthorized use.

Traffic in delay-tolerant networks

In a DTN, traffic can be classified in three ways: expedited, normal and bulk. These traffic types move across the DTN in order of decreasing priority:

• Expedited packets. These are always transmitted, reassembled and verified before data of any other class from a given source to a given destination.

• Normal traffic. This traffic is sent after all expedited packets have been successfully assembled at their intended destination.

• Bulk traffic. This is not dealt with until all packets of other classes from the same source and bound for the same destination have been successfully transmitted and reassembled. In this sense, bulk bundles are sent on a "least effort" basis.

How Does DTN Work?

The DTN protocol suite can operate in tandem with the terrestrial IP suite or it can operate independently. DTN provides assured delivery of data using automatic store-and-forward mechanisms. Each data packet that is received is forwarded immediately if possible, but stored for future transmission if forwarding is not currently possible but is expected to be possible in the future. As a result, only the next hop needs to be available when using DTN.

The DTN suite also contains network management, security, routing and quality-of-service capabilities, which are similar to the capabilities provided by the terrestrial Internet suite.

• Improved Operations and Situational Awareness: The DTN store-and-forward mechanism along with automatic retransmission provides more insight into events during communication outages that occur as result of relay or ground station handovers and poor atmospheric conditions, and significantly reduces the need to schedule ground stations to send or receive data, which can sometimes require up to five days of planning before a transmission takes place.

• Interoperability and Reuse: A standardized DTN protocol suite enables interoperability of ground stations and spacecraft operated by any space agency or private entity with space assets. It also allows NASA to use the same communication protocols for future missions (low-Earth orbit, near-Earth orbit or deep space).

• Space Link Efficiency, Utilization and Robustness: DTN enables more reliable and efficient data transmissions resulting in more usable bandwidth. DTN also improves link reliability by having multiple network paths and assets for potential communication hops.

• Security: The DTN Bundle Protocol Security allows for integrity checks, authentication and encryption, even on links where not previously used.

• Quality-of-Service: The DTN protocol suite allows for many priority levels to be set for different data types, ensuring that the most important data is received ahead of less important data.

Need for delay-tolerant networks

Introduced in 2003, delay-tolerant networks have proved most useful in deep space communications. In space, communications between Earth and spacecrafts involve long distances of thousands and even millions of miles, consequently making delays, disruptions, errors and data losses inevitable. Existing terrestrial networking technologies proved unable to handle such issues, which must be addressed at the application level. That's where DTNs come in.

The Consultative Committee for Space Data Systems (CCSDS) has developed other protocols that incorporate some aspects of delay-tolerant networking. However, they cannot provide the same level of flexibility or automated data transfer as DTNs.

Two such protocols are Space Packet Protocol and CCSDS File Delivery Protocol:

• Space Packet Protocol: This protocol can forward packets across a managed data path through the network. However, it cannot address the scheduled nature of connectivity, which may be why it has not been implemented in a space system.

• CCSDS File Delivery Protocol (CFDP): CFDP provides reliable delivery of files, but it is limited to file transfers only. It does not support messaging, streaming or other applications.

Advantages of delay-tolerant networks

DTN is a suite of protocols developed by the Delay & Disruption Tolerant Networking Research Group administered by the Internet Engineering Task Force (IETF). These protocols are versatile enough to operate either with terrestrial IP protocols or independently.

Terrestrial IP networks are based on store-and-forward operation. However, they assume that the storing will persist for only a modest amount of time, depending on the queuing and transmission delay.

DTN architecture expects nodes to store bundles for an extended period. Whenever possible, each received data packet is forwarded immediately. If forwarding is not currently possible but is expected to be possible in the future, the packet is stored for future transmission. Thus, when using a DTN, only the next hop is required to be available. Delay-tolerant networking uses this automatic store-and-forward mechanism to assure data delivery, which conventional terrestrial networks cannot do.

Other important benefits of DTNs include the following:

• enabled interoperability of ground stations and spacecraft;

• more efficient data transmissions and more usable bandwidth;

• improved link reliability;

• support for integrity checks, authentication and encryption for more secure communications; and

• ability for many priority levels to be set for different data types for improved quality of service (QoS).

Applications of delay-tolerant networks

In addition to space communications and interplanetary networking, DTNs are also useful over terrestrial applications and more modest distances when interference is extreme, high error rates are common or network resources are severely overburdened.

Other key applications of DTNs include the following:

• military and tactical systems;

• disaster recovery networks;

• vehicular communications;

• wildlife tracking/monitoring networks;

• communication in remote or rural areas;

• underwater acoustic networks; and

• other sensor-based networks.

**PRACTICAL – 7**

**Aim : To study about different routing protocols.**

* Routing Information Protocol (RIP)
* Interior Gateway Protocol (IGRP)
* Open Shortest Path First (OSPF)
* Exterior Gateway Protocol (EGP)
* Enhanced Interior Gateway Routing Protocol (EIGRP)
* Border Gateway Protocol (BGP)
* Intermediate System-to-Intermediate System (IS-IS)

Before we get to looking at the routing protocols themselves, it is important to focus on the categories of protocols.

#### **All routing protocols can be classified into the following:**

* Distance Vector or Link State Protocols

| **Distance Vector** | **Link State** |
| --- | --- |
| Sends entire routing table during updates | Only provides link state information |
| Sends periodic updates every 30-90 seconds | Uses triggered updates |
| Broadcasts updates | Multi casts updates |
| Vulnerable to routing loops | No risk of routing loops |
| RIP, IGRP | OSPF, IS-IS |

* Interior Gateway Protocols (IGP) or Exterior Gateway Protocols (EGP)
* Classful or Classless Protocols

## Distance Vector and Link State Protocols

Distance vector routing protocols are protocols that **use distance to work out the best routing path for packets**within a network.

These protocols measure the distance based on how many hops data has to pass to get to its destination. The number of hops is essentially the number of routers it takes to reach the destination.

Generally, distance vector protocols send a routing table full of information to neighboring devices. This approach makes them low investment for administrators as they can be deployed without much need to be managed. The only issue is that they require more bandwidth to send on the routing tables and can run into routing loops as well.

## Link State Routing Protocols

Link state protocols take a different approach to finding the best routing path in that they share information with other routers in proximity. The **route is calculated based on the speed of the path to the destination** and the cost of resources.

Link state routing protocols use an algorithm to work this out. One of the key differences to a distance vector protocol is that link state protocols don’t send out routing tables; instead, routers notify each other when route changes are detected.

Routers using the link state protocol creates three types of tables; **neighbor table**, **topology table**, and **routing table**. The neighbor table stores details of neighboring routers using the link state routing protocol, the topology table stores the whole network topology, and the routing table stores the most efficient routes.

## IGP and EGPs

Routing protocols can also be categorized as **Interior Gateway Protocols** (**IGPs**) or **Exterior Gateway Protocols** (**EGPs**).

### ****IPGs****

**IGPs** are routing protocols that exchange routing information with other routers within a single autonomous system (AS). An AS is defined as one network or a collection of networks under the control of one enterprise. The company AS is thus separate from the ISP AS.

#### **Each of the following is classified as an IGP:**

* Open Shortest Path First (OSPF)
* Routing Information Protocol (RIP)
* Intermediate System to Intermediate System (IS-IS)
* Enhanced Interior Gateway Routing Protocol (EIGRP)

### EGPs

On the other hand, **EGPs** are routing protocols that are used to transfer routing information between routers in different autonomous systems. These protocols are more complex and BGP is the only EGP protocol that you’re likely to encounter. However, it is important to note that there is an EGP protocol named EGP.

#### **Examples of EGPs include:**

* Border Gateway Protocol (BGP)
* Exterior Gateway Protocol (EGP)
* The ISO’s InterDomain Routing Protocol (IDRP)

## Types of Routing Protocol

### Routing Protocols Timeline

* 1982 – EGP
* 1985 – IGRP
* 1988 – RIPv1
* 1990 – IS-IS
* 1991 – OSPFv2
* 1992 – EIGRP
* 1994 – RIPv2
* 1995 – BGP
* 1997 – RIPng
* 1999 – BGPv6 and OSPFv3
* 2000 – IS-ISv6

### Routing Information Protocol (RIP)

Routing Information Protocol or RIP is one of the first routing protocols to be created. RIP is used in both **Local Area Networks** (LANs) and **Wide Area Networks**(WANs), and also runs on the Application layer of the [**OSI model**](https://www.comparitech.com/net-admin/osi-model-explained/). There are multiple versions of RIP including **RIPv1** and **RIPv2**. The original version or RIPv1 determines network paths based on the IP destination and the hop count of the journey.

RIPv1 interacts with the network by broadcasting its IP table to all routers connected to the network. RIPv2 is a little more sophisticated than this and sends its routing table on to a multicast address. RIPv2 also uses authentication to keep data more secure and chooses a subnet mask and gateway for future traffic. The main limitation of RIP is that it has a maximum hop count of 15 which makes it unsuitable for larger networks.

### Pros:

* **Historical Significance**: RIP is one of the oldest and widely recognized routing protocols.
* **Operational Simplicity**: It’s relatively straightforward to understand and implement.
* **Application Layer Operation**: Operates on the application layer, making it easy to manage and configure.
* **Multicast Capability (RIPv2)**: RIPv2 can multicast its routing table, providing a more efficient way to communicate with other routers than broadcasting.
* **Enhanced Security (RIPv2)**: RIPv2 offers authentication measures to enhance data security.

### Cons:

* **Maximum Hop Count**: RIP’s maximum hop count of 15 restricts its use in larger networks.
* **Lack of Scalability**: Due to its hop count limitation, it is not suited for modern expansive networks.
* **Broadcaster (RIPv1)**: RIPv1’s method of broadcasting its entire table can lead to increased traffic and potential inefficiencies.
* **Limited Route Metric**: RIP uses hop count as its sole metric, which may not always represent the best path in complex networks.
* **Slower Convergence**: RIP can be slower to adapt to network changes, leading to potential temporary routing loops.

**Interior Gateway Protocol (IGRP)**

Interior Gateway Protocol or IGRP is a distance vector routing protocol produced by Cisco. IGRP was designed to build on the foundations laid down on RIP to function more effectively within larger connected networks and **removed the 15 hop cap**that was placed on RIP. IGRP uses metrics such as bandwidth, delay, reliability, and load to compare the viability of routes within the network. However, only bandwidth and delay are used under IGRP’s default settings.

IGRP is ideal for larger networks because it **broadcasts updates every 90 seconds and has a maximum hop count of 255**. This allows it to sustain larger networks than a protocol like RIP. IGRP is also widely used because it is resistant to routing loops because it updates itself automatically when route changes occur within the network.

**Pros:**

* **Enhanced Scalability**: IGRP addresses the shortcomings of RIP by allowing a maximum hop count of 255, making it suitable for larger networks.
* **Multiple Metrics**: Uses a combination of metrics (bandwidth, delay, reliability, and load) for improved routing decisions.
* **Frequent Updates**: Broadcasts updates every 90 seconds, ensuring the network is well-informed and up-to-date.
* **Loop Resistance**: Built-in features that automatically update routes, making IGRP resistant to routing loops.
* **Cisco Legacy**: Developed by Cisco, it benefits from being backed by one of the industry leaders in networking.

**Cons:**

* **Proprietary Protocol**: Being a Cisco product, IGRP isn’t universally adaptable across all devices from different manufacturers.
* **Limited Default Metrics**: Even though it has multiple metrics, only bandwidth and delay are considered under default settings, potentially overlooking other valuable information.
* **Superseded by EIGRP**: IGRP has been replaced by Enhanced IGRP (EIGRP), which offers more advantages, leading to its diminished use in modern networks.
* **Larger Overhead**: Given its broader capabilities, IGRP can generate more network overhead compared to simpler protocols like RIP.
* **Potential Complexity**: The multiple metrics and larger hop count can make configuration and troubleshooting more complex than simpler protocols.

**Open Shortest Path First (OSPF)**

Open Shortest Path First or OSPF protocol is a link-state IGP that was tailor-made for IP networks using the **Shortest Path First** (**SPF**) **algorithm**. The SPF routing algorithm is used to calculate the shortest path spanning-tree to ensure efficient data transmission of packets. OSPF routers maintain databases detailing information about the surrounding topology of the network. This database is filled with data taken from **Link State Advertisements (LSAs)** sent by other routers. LSAs are packets that detail information about how many resources a given path would take.

OSPF also uses the **Dijkstra algorithm** to recalculate network paths when the topology changes. This protocol is also relatively secure as it can authenticate protocol changes to keep data secure. It is used by many organizations because it’s scalable to large environments. Topology changes are tracked and OSPF can recalculate compromised packet routes if a previously-used route has been blocked.

**Pros:**

* **Efficient Routing**: Utilizes the Shortest Path First (SPF) algorithm to ensure optimal data packet transmission.
* **Detailed Network Insight**: OSPF routers maintain a database on the network’s topology, offering a detailed perspective on its structure.
* **Dynamic Adaptability**: Employs the Dijkstra algorithm to dynamically adjust to network topology changes, ensuring continuity in data transmission.
* **Security Features**: Offers protocol change authentication to maintain data security, ensuring that only authorized updates are made.
* **Highly Scalable**: Suitable for both small and large-scale network environments, making it versatile for various organizational sizes.

**Cons:**

* **Complex Configuration**: Given its many features, OSPF can be complex to set up and maintain.
* **Higher Overhead**: Maintaining detailed databases and frequently recalculating routes can generate more network overhead.
* **Sensitive to Topology Changes**: While OSPF can adapt to changes, frequent topology alterations can cause performance dips as it recalculates routes.
* **Resource Intensive**: OSPF routers require more memory and CPU resources due to their database maintenance and route recalculations.
* **Potential for Large LSDB**: In very large networks, the Link State Database (LSDB) can grow significantly, necessitating careful design and segmenting.

**Exterior Gateway Protocol (EGP)**

Exterior Gateway Protocol or EGP is a protocol that is used to exchange data between gateway hosts that neighbor each other within autonomous systems. In other words, EGP provides a forum for routers to share information across different domains. The most high profile example of an EGP is the internet itself. The routing table of the EGP protocol includes known routers, route costs, and network addresses of neighboring devices. EGP was widely-used by larger organizations but has since been replaced by BGP.

The reason why this protocol has fallen out of favor is that it doesn’t support multipath networking environments. The EGP protocol works by keeping a database of nearby networks and the routing paths it could take to reach them. This route information is sent on to connected routers. Once it arrives, the devices can update their routing tables and undertake more informed path selection throughout the network.

**Pros:**

* **Data Exchange Between Autonomous Systems**: Allows gateway hosts to share information across distinct network domains, effectively acting as a bridge.
* **Foundation of Early Internet**: Served as a precursor and essential component to the modern internet’s formation.
* **Routing Database**: Contains comprehensive information, including known routers, route costs, and the addresses of neighboring devices.
* **Path Information Sharing**: Sends route data to neighboring routers, helping them update their tables and make better routing decisions.

**Cons:**

* **Lack of Multipath Support**: EGP isn’t suitable for modern multipath networking environments, limiting its adaptability.
* **Obsolete**: Has been largely phased out in favor of more advanced protocols, notably BGP.
* **Limited Scalability**: As networks grew, EGP struggled with handling larger and more intricate systems.
* **Static Path Determination**: While EGP keeps a database of nearby networks, its path determinations are more static, making it less flexible than newer protocols.
* **Potential for Redundancy**: EGP’s method of sharing all route data with neighboring routers can lead to redundant data transmission and larger routing tables.

**Enhanced Interior Gateway Routing Protocol (EIGRP)**

Enhanced Interior Gateway Routing Protocol or EIGRP is a distance vector routing protocol that is used for **IP**, **AppleTalk**, and **NetWare** networks. EIGRP is a Cisco proprietary protocol that was designed to follow on from the original IGRP protocol. When using EIGRP, a router takes information from its neighbors’ routing tables and records them. Neighbors are queried for a route and when a change occurs the router notifies its neighbors about the change. This has the end result of making neighboring routers aware of what is going on in nearby devices.

EIGRP is equipped with a number of features to maximize efficiency, including **Reliable Transport Protocol** (**RTP**) and a **Diffusing Update Algorithm** (**DUAL**). Packet transmissions are made more effective because routes are recalculated to speed up the convergence process.

**Pros:**

* **Versatility**: Supports multiple network protocols, including IP, AppleTalk, and NetWare.
* **Advanced Design**: A successor to the original IGRP, EIGRP incorporates more modern features for routing.
* **Neighbor Information Exchange**: By collecting data from neighbors’ routing tables, EIGRP maintains a real-time understanding of the network environment.
* **Efficient Notification System**: Routers promptly inform neighboring routers of any route changes, fostering a responsive network environment.
* **Reliable Transport Protocol (RTP)**: Ensures the reliability of packet transmissions and acknowledges receipt of routing updates.
* **Diffusing Update Algorithm (DUAL)**: Enhances route calculations and accelerates network convergence, reducing the time the network takes to stabilize after a change.

**Cons:**

* **Proprietary Protocol**: EIGRP is Cisco-specific, which can limit interoperability with equipment from other manufacturers.
* **Overhead**: The frequent exchange of routing updates and queries, especially in larger networks, can consume bandwidth and processing resources.
* **Complex Configuration**: While powerful, EIGRP’s array of features might pose a steeper learning curve for those unfamiliar with its intricacies.
* **Potential for Routing Loops**: As with many distance-vector protocols, there’s a risk of routing loops, although measures like split horizon and route poisoning help mitigate this.
* **Lack of Wide Adoption**: Being proprietary means EIGRP isn’t as universally adopted as open standard protocols.

**Border Gateway Protocol (BGP)**

**Border Gateway Protocol or BGP** is the routing protocol of the internet that is classified as a distance path vector protocol. BGP was **designed to replace EGP** with a decentralized approach to routing. The BGP Best Path Selection Algorithm is used to select the best routes for data packet transfers. If you don’t have any custom settings then BGP will select routes with the shortest path to the destination.

However many administrators choose to change routing decisions to criteria in line with their needs. **The best routing path selection algorithm can be customized by changing the BGP cost community attribute**. BGP can make routing decisions based Factors such as weight, local preference, locally generated, AS\_Path length, origin type, multi-exit discriminator, eBGP over iBGP, IGP metric, router ID, cluster list and neighbor IP address.

BGP only sends updated router table data when something changes. As a result, there is no auto-discovery of topology changes which means that the user has to configure BGP manually. In terms of security, BGP protocol can be authenticated so that only approved routers can exchange data with each other.

**Pros:**

* **Internet Backbone**: As the primary routing protocol of the internet, BGP plays a pivotal role in global data exchanges.
* **Decentralized Design**: Unlike its predecessor EGP, BGP’s decentralized nature ensures more robust and adaptable network operations.
* **Customizable Path Selection**: BGP’s Best Path Selection Algorithm can be tailored to meet unique network demands by adjusting attributes.
* **Efficient Updates**: Only transmitting updates when there’s a change, BGP reduces unnecessary network traffic.
* **Granular Routing Decisions**: Administrators have a plethora of factors like weight, AS\_Path length, and IGP metric to inform routing decisions, allowing for a high degree of routing precision.
* **Authentication**: BGP provides security measures allowing only authorized routers to participate in data exchanges, enhancing the security of routing updates.

**Cons:**

* **Complex Configuration**: BGP requires meticulous manual configuration since it doesn’t auto-discover topology changes.
* **Potential Instability**: Mistakes or malicious actions in BGP configurations can inadvertently or intentionally divert internet traffic, potentially leading to large-scale outages.
* **Scalability Concerns**: As the internet grows, BGP’s scalability, in its current form, might pose challenges.
* **Vulnerabilities**: Despite authentication measures, BGP is historically susceptible to certain security issues, like prefix hijacking.
* **Learning Curve**: Given its complexity and significance, mastering BGP can be challenging for many network administrators.
* **Convergence Time**: BGP can sometimes take longer to converge after a network change compared to some other protocols.

**Intermediate System-to-Intermediate System (IS-IS)**

Intermediate System-to-Intermediate System (IS-IS) is a link-state, IP routing protocol and IGPP protocol used on the internet to send IP routing information. **IS-IS uses a modified version of the Dijkstra algorithm**. An IS-IS network consists of a range of components including end systems, (user devices), intermediate systems (routers), areas, and domains.

Under IS-IS routers are organized into groups called areas and multiple areas are grouped together to make up a domain. Routers within the area are placed with Layer 1 and routers that connect segments together are classified as Layer 2. There are two types of network addresses used by IS-IS; **Network Service Access Point** (**NSAP**) and **Network Entity Title** (**NET**).

**Pros:**

* **Hierarchical Design**: Organizing routers into areas and domains simplifies management and optimizes routing within large networks.
* **Scalability**: The division into areas and domains allows for efficient operation in large-scale networks, avoiding unnecessary routing overhead.
* **Flexibility**: The protocol is not tied exclusively to IP, making it adaptable to various network architectures.
* **Efficient Path Selection**: Utilizes a modified version of the Dijkstra algorithm for optimal path determination.
* **Distinct Addressing Mechanism**: With unique addresses like NSAP and NET, IS-IS provides granularity in addressing which can assist in network troubleshooting and management.
* **Dual-Level Operation**: Layer 1 and Layer 2 classification enables segregation of intra-area routing from inter-area routing, ensuring efficiency and simplifying router roles.

**Cons:**

* **Learning Curve**: Given its unique terminology and addressing mechanism, mastering IS-IS might pose a challenge for network engineers unfamiliar with it.
* **Address Length**: NSAP addresses can be lengthy, which may complicate manual configuration and troubleshooting.
* **Lesser Adoption**: IS-IS is less commonly used in certain segments of the internet when compared to OSPF, potentially leading to compatibility considerations.
* **Complex Configuration**: Its hierarchical structure, while providing scalability benefits, might complicate the initial configuration.
* **Interoperability**: As a protocol with roots in the ISO OSI model, there may be issues when trying to interoperate with purely IP-based protocols.
* **Protocol Evolution**: While IS-IS has been adapted for IP, its origins in the OSI model mean it might not be as naturally suited to some IP-centric tasks as newer protocols.

**PRACTICAL – 9**

**Aim : To study about Cisco IOS**

Cisco IOS (Internetwork Operating System) is a proprietary operating system that runs on Cisco Systems [routers](https://www.techtarget.com/searchnetworking/definition/router) and [switches](https://www.techtarget.com/searchnetworking/definition/switch). The core function of Cisco IOS is to enable data communications between network [nodes](https://www.techtarget.com/searchnetworking/definition/node).

In addition to routing and switching, Cisco IOS offers dozens of additional services that an administrator can use to improve the performance and security of network traffic. Such services include encryption, authentication, firewall capabilities, policy enforcement, [deep packet inspection](https://www.techtarget.com/searchnetworking/definition/deep-packet-inspection-DPI), Quality of Service ([QoS](https://www.techtarget.com/searchunifiedcommunications/definition/QoS-Quality-of-Service)), intelligent routing and [proxy](https://www.techtarget.com/whatis/definition/proxy-server) capability. In Cisco's Integrated Services Routers (ISRs), IOS can also support call processing and [unified communications](https://www.techtarget.com/searchunifiedcommunications/definition/unified-communications) services.

Cisco IOS software releases are organized into what Cisco calls "families" and "trains." Each family shares the same code base and trains are how new IOS releases are delivered.

There are two types of IOS operating systems:

IOS XE -  runs on top of a Linux kernel. IOS XE  and IOS share a lot of the same code, but IOS XR is considered to be a completely different code base.

IOS XR -  based on QNX a commercial Unix-like real-time operating system. IOS XR supports software-defined networking (SDN) and the embedded systems market.

**PRACTICAL – 10**

**Aim : Configure a mail server for IMAP/POP protocols and write a simple SMTP client in C/C++/Java client to send and receive mails.**