./



Learning Report -Networking

**Document History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver. Rel. No.** | **Release Date** | **Prepared. By** | **Reviewed By** | **To be approved By** | **Remarks/Revision Details** |
| 1 |  | Name/PS No | Name/PS No | Module Owner Name | Comments |
| 2 | 23/03/21 | Rohan Roy/99003755 |  |  |  |
| 3 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Contents

[1. NETWORK 4](#_Toc67501538)

[1.1 NETWORK COMPONENTS 4](#_Toc67501539)

[1.HUB 5](#_Toc67501540)

[2.SWITCH 5](#_Toc67501541)

[3.ROUTER 5](#_Toc67501542)

[4.GATEWAY 5](#_Toc67501543)

[4.BRIDGE 6](#_Toc67501544)

[4.ACCESS POINTS 6](#_Toc67501545)

[2. WIRED & WIRELESS NETWORKS 6](#_Toc67501546)

[2.1 WIRED NETWORKS 6](#_Toc67501547)

[2.2 WIRELESS NETWORKS 6](#_Toc67501548)

[2.3 PAN 7](#_Toc67501549)

[2.4 LAN 7](#_Toc67501550)

[2.5 WAN 7](#_Toc67501551)

[2.6 WLAN 7](#_Toc67501552)

[2.7 MAN 7](#_Toc67501553)

[2.8 Wi-Fi 8](#_Toc67501554)

[2.9 WiMAX 8](#_Toc67501555)

[3. OSI MODEL 8](#_Toc67501556)

[3.1 Physical Layer (Layer 1) 9](#_Toc67501557)

[3.2 Data Link Layer (Layer 2) 9](#_Toc67501558)

[3.3 Network Layer (Layer 3) 9](#_Toc67501559)

[3.4 Transport Layer (Layer 4) 9](#_Toc67501560)

[3.5 Session Layer (Layer 5) 10](#_Toc67501561)

[3.6 Presentation Layer (Layer 6) 10](#_Toc67501562)

[3.7 Application layer (Layer 7) 10](#_Toc67501563)

[4. TCP Protocol 11](#_Toc67501564)

[5. UDP PROTOCOL 12](#_Toc67501565)

[6. IP Protocol 13](#_Toc67501566)

[7. L2 PROTOCOLS 13](#_Toc67501567)

[7.1 ARP 13](#_Toc67501568)

[7.2 RARP 14](#_Toc67501569)

[7.3 DHCP 14](#_Toc67501570)

[7.4 ICMP 14](#_Toc67501571)

[8. L3 PROTOCOLS 15](#_Toc67501572)

[8.1 BGP 15](#_Toc67501573)

[8.2 EIGRP 15](#_Toc67501574)

[8.3 RIP PROTOCOL 16](#_Toc67501575)

[8.4 OSPF 16](#_Toc67501576)

[9. IPv4 16](#_Toc67501577)

# 1. NETWORK

A network is a collection of computers, servers, mainframes, network devices, peripherals, or other devices connected to one another to allow the sharing of data.

## 1.1 NETWORK COMPONENTS

A Computer Network is built up by use of many devices/components. These devices are called Network Components. They are responsible for data transfer and smooth communication between 2 devices.

The network components are Hub, Switch, Router, Gateway, Bridge, Access points.

### 1.HUB

Hub is a multiple Port device which is present in the Physical Layer of the OSI Model.

It is used to connect the segments of a LAN.

It acts as a common point for the Devices in a network.

When packet enters one port, it is copied to other ports and made visible for all segments of the LAN.

2.SWITCH

It operates at Data Link Layer on OSI Model.

Switch filters and forwards the packet between LAN segments.

3.ROUTER

Router operates in Network Layer.

It is usually located between 2 or 3 networks.

It has a routing/forwarding table which helps determine the best path to forward the packets between 2 hosts or networks.

It uses ICMP to communicate with each other and configures the best route.

4.GATEWAY

A gateway, as the name suggests, is a passage to connect two networks together that may work upon different networking models.

They basically work as the messenger agents that take data from one system, interpret it, and transfer it to another system.

Gateways are also called protocol converters and can operate at any network layer.

Gateways are generally more complex than switch or router.

4.BRIDGE

A bridge is a network device that connects multiple LANs (Local Area Networks) together to form a larger LAN. The process of aggregating networks is called network bridging.

A bridge connects the different components so that they appear as parts of a single network. Bridges operate at the data link layer of the OSI model and hence also referred as Layer 2 switches.

Since they operate at data link layer, they transmit data as data frames. On receiving a data frame, the bridge consults a database to decide whether to pass, transmit or discard the frame.

If the frame has a destination MAC (media access control) address in the same network, the bridge passes the frame to that node and then discards it.

If the frame has a destination MAC address in a connected network, it will forward the frame toward it.

4.ACCESS POINTS

An access point is a device that creates a wireless local area network, or WLAN, usually in an office or large building.

An access point connects to a wired router, switch, or hub via an Ethernet cable, and projects a Wi-Fi signal to a designated area.

# 2. TOPOLOGY

Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Physical topology is the geometric representation of all the nodes in a network.

## 2.1Bus topology

* The bus topology is designed in such a way that all the stations are connected through a single cable known as a backbone cable.
* Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
* When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not.
* The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The backbone cable is considered as a "single lane" through which the message is broadcast to all the stations.
* The most common access method of the bus topologies is CSMA (Carrier Sense Multiple Access).

## 2.2 CSMA

* It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.
  + CSMA CD: CSMA CD (Collision detection) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "recovery after the collision".
  + CSMA CA: CSMA CA (Collision Avoidance) is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until
* the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

## 2.3 Ring Topology

* Ring topology is like a bus topology, but with connected ends.
* The node that receives the message from the previous computer will retransmit to the next node.
* The data flows in one direction, i.e., it is unidirectional.
* The data flows in a single loop continuously known as an endless loop.
* It has no terminated ends, i.e., each node is connected to other node and having no termination point.
* The data in a ring topology flow in a clockwise direction.

## 2.4 Star Topology

* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a server, and the peripheral devices attached to the server are known as clients.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a physical star topology.
* Star topology is the most popular topology in network implementation.

## 2.5 Tree Topology

* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

## 2.6 Mesh Topology

* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point of communication.
* The Internet is an example of the mesh topology.

# 3. WIRED & WIRELESS NETWORKS

## 3.1 WIRED NETWORKS

Wired Network refers to the transmission and reception of data through a wired based communication Technology. It is also referred as Wireline Communication. It uses cables or data line for Communication.

## 3.2 WIRELESS NETWORKS

It is a network in which data is transferred without use of physical entities like cables or wires. It keeps the devices connected in a network. It is usually done using radio waves.

## 3.3 PAN

* A personal area network (PAN) is a computer network organized around an individual for personal use only. They typically involve a computer, phone, printer, tablet, or some other device like a PDA.
* It typically ranges within 10m and WLAN ranges from10m to 100m.
* PAN supports 250 kbps in ZigBee, from kbps to 24 Mbps in Bluetooth case.

## 3.4 LAN

* A local area network (LAN) is a collection of devices connected in one physical location, such as a building, office, or home.
* A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
* It ranges from 10 to 100m and more in case of wireless LAN.
* LAN supports 10, 100 and 1000 Mbps.
* Wired LAN devices are connected using Ethernet cables.

## 3.5 WAN

* A local area network (LAN) is a collection of devices connected together in one physical location, such as a building, office, or home.
* A LAN can be small or large, ranging from a home network with one user to an enterprise network with thousands of users and devices in an office or school.
* It ranges from 10 to 100m and more in case of wireless LAN.
* LAN supports 10, 100 and 1000 Mbps.
* Wired LAN devices are connected using Ethernet cables.

## 3.6 WLAN

* WLAN is a local area network (LAN) that doesn’t rely on wired ethernet connections.
* A wireless local area network (WLAN) is a wireless distribution method for two or more devices.
* WLAN supports 54 Mbps or above.
* WLANs use high-frequency radio waves and often include an access point to the Internet.
* A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

## 3.7 MAN

* A metropolitan area network (MAN) is like a local area network (LAN) but spans an entire city or campus, or some other municipal or organizational territory.
* MANs are formed by connecting multiple LANs.
* It serves geographical area of 5-50kms in range.
* Thus, MANs are larger than LANs, but smaller than wide area networks (WAN) that cover dispersed geographical areas, sometimes directly connecting users around the world.
* It supports a speed of 5-10 Mbps.

## 3.8 Wi-Fi

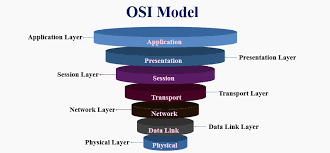
* Wi-Fi is a wireless networking protocol that devices use to communicate without direct cable connections. It is an industry term that represents a type of wireless local area network (LAN) protocol based on the 802.11 IEEE network standard.
* The 802.11a will transmit data at a frequency level of 5GHz – transmits a maximum of 54Mbps.
* The 802.11b will transmit data at a frequency level of 2.4GHz – transmits a maximum of 11 Mbps.
* The 802.11g will transmit data at 2.4GHz – transmits a maximum of 54 Mbps.
* The main requirement for Wi-Fi is a device that receives and transmits a wireless signal, usually a router, but sometimes a phone or computer.

## 3.9 WiMAX

* Worldwide Interoperability for Microwave Access is a technology standard for long-range wireless networking for both mobile and fixed connections.
* A single WiMAX tower can provide coverage to a very large area big as 3,000 square miles i.e., 8,000 square km.
* WiMAX should be able to handle up to 70 megabits per second.

# 4. OSI MODEL

OSI stands for Open System Interconnection. It describes the Standard Architecture of a network. It is a 7 Layer Architecture, in which each layer is having its specific functionality. The data is sent/received from one person to another across the globe.



## 4.1 Physical Layer (Layer 1)

* This is the first and lowest layer of the OSI model.
* It is responsible for the actual physical connection between the Devices.
* The data is in term of bits.
* The data is transferred from one node to another.
* It receives the data in term of 0’s and 1’s and send it to DLL, which will put frame back together.

## 4.2 Data Link Layer (Layer 2)

* This layer sits above Physical Layer and is the 2nd Layer of OSI.
* Data is transferred between two nodes a Physical layer.
* It helps to detect and correct the error which occurs on the physical layer.

## 4.3 Network Layer (Layer 3)

* Here the data is transmitted between hosts which are located in different network.
* Router is present in Network Layer.
* With the use of packet routing, it helps find the shortest path the transmit the data.
* The sender and receiver IP address are placed in the header.

## 4.4 Transport Layer (Layer 4)

* It takes services from Network layer and provides service to Application layer.
* Here it checks for End-to-End delivery of complete message.
* It also provides acknowledgement upon successful reception of message.
* It re-transmits the message if there is any error.

## 4.5 Session Layer (Layer 5)

* This layer is responsible for establishment of connection, maintenance of sessions.
* It also ensures Security and Authentication.

## 4.6 Presentation Layer (Layer 6)

* The data from application layer is extracted and manipulated as per required format.

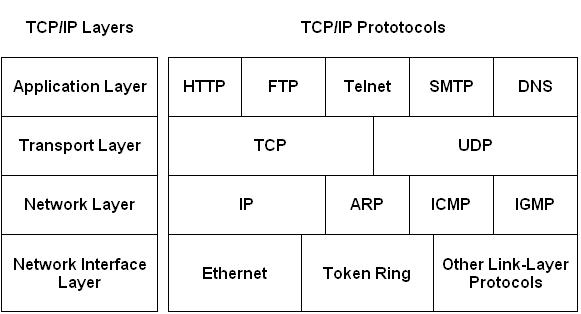
## 4.7 Application layer (Layer 7)

* This is the uppermost layer of OSI Model.
* Here the end user and application layer interact directly with the software application.
* The application layer identifies communication partners, resource availability, and synchronizes communication.

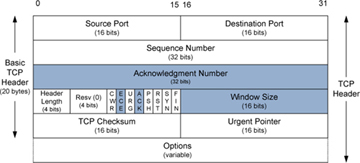
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| OSI Layer | Purpose | TCP/IP Layer | Protocol | Packet Data Unit | Address | Device |
| Application | Interface (API) |  | HTTP, SMTP | Message | - | - |
| Presentation | Encryption, Formatting |  | HTTP, SMTP | Message | - | - |
| Session | Authentication,  Authorization |  | HTTP, SMTP | Message | - | Gateway |
| Transport | Reliability |  | TCP, UDP | Segment, Datagram | Port | Firewall |
| Network | Addressing,  Routing |  | IP, ICMP | Packet | IP Address | Router |
| Data Link | Logical Link Control,  Media Access Control |  | Ethernet,  Wi-Fi | Frame | MAC Address | Switch,  Bridge,  Access Point |
| Physical | Transmission |  | CAT 5,  RJ-45 | Bit | - | Hub, NIC, Cable |

# 5. TCP Protocol

* TCP is a transport layer protocol which that helps in the transmission of data from source to destination.
* It is a connection oriented protocol i.e. It establishes connection between the devices before they start communicating.
* It is used with IP protocol.
* TCP is a reliable protocol as it follows the flow and error control mechanism.
* It ensures that the data reaches the intended receiver in the same order in which it is sent. It orders and numbers each segment so that the TCP layer on the destination side can reassemble them based on their ordering.
* It is a full-duplex i.e. the data can transfer in both directions at the same time.



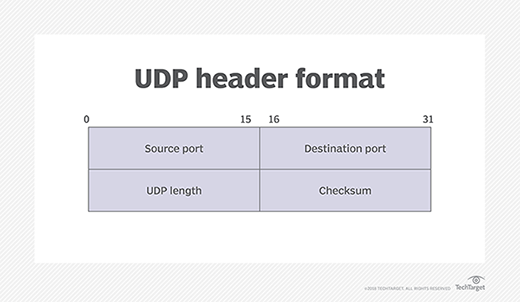
TCP Protocol Framework



TCP Header

# 6. UDP PROTOCOL

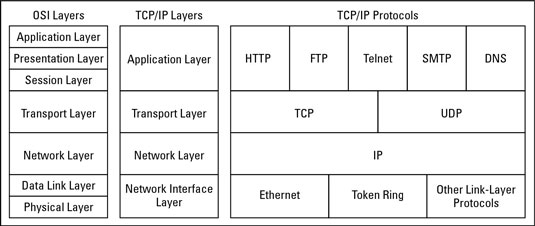
* UDP stands for User Datagram Protocol, it is used to send the messages in the form of datagrams from one device to another.
* It works on IP protocol.
* The UDP works by encapsulating the data into the packet and providing its own header information to the packet.
* It is a connectionless protocol.



UDP Header

# 7. IP Protocol

* The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
* Data traversing the Internet is divided into smaller pieces, called packets.
* IP information is attached to each packet, and this information helps routers to send packets to the right place.
* Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

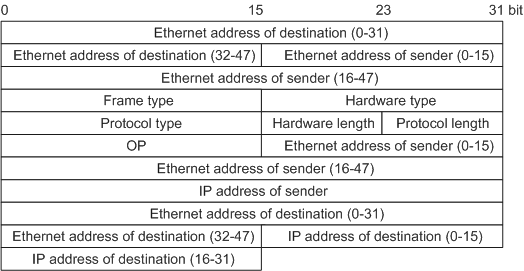


IP Protocol

# 8. L2 PROTOCOLS

## 8.1 ARP

* ARP stands for Address Resolution Protocol.
* It determines the MAC address of a device if the IP address is known.
* The MAC address is required because the device cannot communicate with another device in Local Network if the MAC address is not known.
* ARP converts 32-bit logical address (IPv4 address) to the 48-bit physical address (MAC address).



## 8.2 RARP

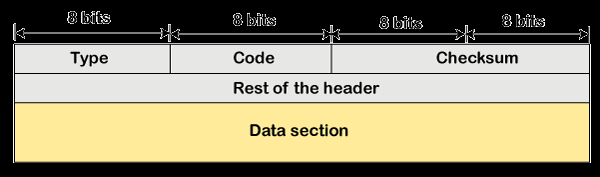
* It stands for Reverse Address Resolution Protocol.
* If the Host wants to know the IP address then it broadcasts the RARP query packet which contains the physical address to entire network. The RARP server identifies the packet and sends back the IP address.
* The message format is similar ARP protocol.
* A RARP request is created and broadcast on the local network.
* Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

## 8.3 DHCP

* Dynamic Host Configuration Protocol allocates IP address to a any device or node so that it can communicate in the Network.
* DHCP provides static and dynamic address allocation that can be manual or automatic.
* A DHCP server has a database that statically binds physical addresses to IP addresses known as static allocation.
* DHCP has a second database with a pool of available IP addresses known as dynamic allocation.
* When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period.

## 8.4 ICMP

* The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues.
* ICMP is mainly used to determine whether data is reaching its intended destination in a timely manner.
* ICMP messages are divided into two broad categories: error-reporting messages and query messages.
* The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
* The query messages help a host or a network manager get specific information from a router or another host.



# 9. L3 PROTOCOLS

## 9.1 BGP

* It is an interdomain routing protocol, and it uses the path-vector routing.
* Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISPs.
* The main role of BGP is to provide communication between two autonomous systems. ▪ BGP supports Next-Hop Paradigm.
* BGP conserve network Bandwidth.
* BGP supports CIDR.
* In BGP protocol, the path between source and destination (list of autonomous systems) is represented as a list of attributes. Each attribute gives some information about the path.
* To create a reliable environment, BGP uses the services of TCP.

## 9.2 EIGRP

* Enhanced Interior Gateway Routing Protocol (EIGRP) is a dynamic routing Protocol which is used to find the best path between any two layer-3 devices to deliver the packet.
* EIGRP works on network layer protocol of OSI model and uses the protocol number 88.
* It uses some messages to communicate with the neighbor devices that operates EIGRP.

These are:

• Hello message

• NULL update

• Full Update

• Partial update

• Query message

• Reply message

• Acknowledgement message

## 9.3 RIP PROTOCOL

* Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network.
* The metric used by RIP is defined as the number of links (networks) to reach the destination. For this reason, the metric in RIP is called a hop count. GENESIS - NETWORKING L&T Technology Services CONFIDENTIAL Page 20 of 29.
* Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
* In RIP, the route is chosen based on the hop count metric. If another route of better bandwidth is available, then that route would not be chosen.
* It broadcasts the routing updates to the entire network that creates a lot of traffic.

## 9.4 OSPF

* Open shortest path first (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own shortest path first (SPF) algorithm.
* OSPF divides an autonomous system into areas which is a collection of networks, hosts, and routers all contained within an autonomous system.
* The OSPF protocol assign a cost, called the metric, to each route. The metric can be based on a type of service like minimum delay, maximum throughput, and so on.
* In OSPF terminology, a connection is called a link.
* OSPF is the first widely deployed routing protocol. It can converge with a network in a few seconds and it is one of the protocols that can provide loop-free paths.

# 10. IPv4

* IPv4 stands for Internet Protocol version 4.
* It defines and enables internetworking at the internet layer of the Internet Protocol Suite.
* It has 32-bit long address which is represented in Hexadecimal format.
* All hosts within a single network share the same network address. Each host also has an address that uniquely identifies it. Depending on the scope of the network and the type of device, the address is either globally or locally unique.
* Devices that are visible to users outside the network (webservers, for example) must have a globally unique IP address. Devices that are visible only within the network must have locally unique IP addresses.

## 10.1 IPv4 Classful Addressing

* To provide flexibility in the number of addresses distributed to networks of different sizes, 4-octet (32-bit) IP addresses were originally divided into three different categories or classes: class A, class B, and class C. Each address class specifies a different number of bits for its network prefix and host number:
* Class A addresses use only the first byte (octet) to specify the network prefix, leaving 3 bytes to define individual host numbers.
* Class B addresses use the first 2 bytes to specify the network prefix, leaving 2 bytes to define host addresses.
* Class C addresses use the first 3 bytes to specify the network prefix, leaving only the last byte to identify hosts.

## 10.2 IPv4 Dotted Decimal Notation

The 32-bit IPv4 addresses are most often expressed in dotted decimal notation, in which each octet (or byte) is treated as a separate number. Within an octet, the rightmost bit represents 20 (or 1), increasing to the left until the first bit in the octet is 27 (or 128). Following are IP addresses in binary format and their dotted decimal equivalents.

## 10.3 IPv4 Subnetting

Because of the physical and architectural limitations on the size of networks, you often must break large networks into smaller subnetworks. Within a network, each wire or ring requires its own network number and identifying subnet address.

## 10.4 IPv4 Variable-Length Subnet Masks

Traditionally, subnets were divided by address class. Subnets had either 8, 16, or 24 significant bits, corresponding to 224, 216, or 28 possible hosts. As a result, an entire /16 subnet had to be allocated for a network that required only 400 addresses, wasting 65,136 (216 – 400 = 65,136) addresses.

To help allocate address spaces more efficiently, variable-length subnet masks (VLSMs) were introduced. Using VLSM, network architects can allocate more precisely the number of addresses required for a subnet.

# 11. IPv6

* IPv4 stands for Internet Protocol version 6.
* IPv6 addresses consist of 128 bits, instead of 32 bits, and include a scope field that identifies the type of application suitable for the address.
* IPv6 does not support broadcast addresses, but instead uses multicast addresses for broadcast.
* In addition, IPv6 defines a new type of address called anycast.
* The IPv6 architecture allows 3 types of transmission: unicast, anycast & multicast.

## 11.1 IPv6 Address Scope

* Unicast and multicast IPv6 addresses support address scoping, which identifies the application suitable for the address.
* Unicast addresses support global address scope and two types of local address scope:
  + Link-local unicast addresses- Used only on a single network link. The first 10 bits of the prefix identify the address as a link-local address. Link-local addresses cannot be used outside the link.
  + Site-local unicast addresses- Used only within a site or intranet. A site consists of multiple network links. Site-local addresses identify nodes inside the intranet and cannot be used outside the site.
* Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

## 11.2 IPv6 Address Structure

Unicast addresses identify a single interface. Each unicast address consists of n bits for the prefix, and 128 – n bits for the interface ID.

## 11.3 Understanding IPv6 Address Format

All IPv6 addresses are 128 bits long, written as 8 sections of 16 bits each. They are expressed in hexadecimal representation, so the sections range from 0 to FFFF. Sections are delimited by colons, and leading zeroes in each section may be omitted. If two or more consecutive sections have all zeroes, they can be collapsed to a double colon.

# 12. NETWORK TOOLS

## 12.1 Packet Tracer

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit. The software is mainly focused towards Certified Cisco Network Associate Academy students as an educational tool for helping them learn fundamental CCNA concepts. Previously students enrolled in a CCNA Academy program could freely download and use the tool free of charge for educational use.

## 12.2 Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark.