

Module 8 Recap

Network Layer Characteristics

The network layer (OSI Layer 3) provides services to allow end devices to exchange data across networks. IPv4 and IPv6 are the principle network layer communication protocols. The network layer also includes the routing protocol OSPF and messaging protocols such as ICMP. Network layer protocols perform four basic operations: addressing end devices, encapsulation, routing, and de-encapsulation. IPv4 and IPv6 specify the packet structure and processing used to carry the data from one host to another host. IP encapsulates the transport layer segment by adding an IP header, which is used to deliver the packet to the destination host. The IP header is examined by Layer 3 devices (i.e., routers) as it travels across a network to its destination. The characteristics of IP are that it is connectionless, best effort, and media independent. IP is connectionless, meaning that no dedicated end-to-end connection is created by IP before data is sent. The IP protocol does not guarantee that all packets that are delivered are, in fact, received. This is the definition of the unreliable, or best effort characteristic. IP operates independently of the media that carry the data at lower layers of the protocol stack.

IPv4 Packet

An IPv4 packet header consists of fields containing information about the packet. These fields contain binary numbers which are examined by the Layer 3 process. The binary values of each field identify various settings of the IP packet. Significant fields in the IPv4 packet header include: version, DS, header checksum, TTL, protocol, and the source and destination IPv4 addresses.

IPv6 Packet

IPv6 is designed to overcome the limitations of IPv4 including: IPv4 address depletion, lack of end-to-end connectivity, and increased network complexity. IPv6 increases the available address space, improves packet handling, and eliminates the need for NAT. The fields in the IPv6 packet header include: version, traffic class, flow label, payload length, next header, hop limit, and the source and destination IPv6 addresses.

How a Host Routes

A host can send a packet to itself, another local host, and a remote host. In IPv4, the source device uses its own subnet mask along with its own IPv4 address and the destination IPv4 address to determine whether the destination host is on the same network. In IPv6, the local router advertises the local network address (prefix) to all devices on the network, to make this determination. The default gateway is the network device (i.e., router) that can route traffic to other networks. On a network, a default gateway is usually a router that has a local IP address in the same address range as other hosts on the local network, can accept data into the local network and forward data out of the local network, and route traffic to other networks. A host routing table will typically include a default gateway. In IPv4, the host receives the IPv4 address of the default gateway either dynamically via DHCP or it is configured manually. In IPv6, the router advertises the default gateway address, or the host can be configured manually. On a Windows host, the **route print** or **netstat -r** command can be used to display the host routing table.

Introduction to Routing

When a host sends a packet to another host, it consults its routing table to determine where to send the packet. If the destination host is on a remote network, the packet is forwarded to the default gateway which is usually the local router. What happens when a packet arrives on a router interface? The router examines the packet's destination IP address and searches its routing table to determine where to forward the packet. The routing table contains a list of all known network addresses (prefixes) and where to forward the packet. These entries are known as route entries or routes. The router will forward the packet using the best (longest) matching route entry. The routing table of a router stores three types of route entries: directly connected networks, remote networks, and a default route. Routers learn about remote networks manually, or dynamically using a dynamic routing protocol. Static routes are route entries that are manually configured. Static routes include the remote network address and the IP address of the next hop router. OSPF and EIGRP are two dynamic routing protocols. The **show ip route** privileged EXEC mode command is used to view the IPv4 routing table on a Cisco IOS router. At the beginning of an IPv4 routing table is a code that is used to identify the type of route or how the route was learned. Common route sources (codes) include:

- L** - Directly connected local interface IP address
- C** - Directly connected network
- S** - Static route was manually configured by an administrator
- O** - Open Shortest Path First (OSPF)
- D** - Enhanced Interior Gateway Routing Protocol (EIGRP)