Components of network layer communication

In the reading about the OSI model, you learned about the seven layers of the OSI model that are used to conceptualize the way data is transmitted across the internet. In this reading, you will learn more about operations that take place at layer 3 of the OSI model: the network layer.

Operations at the network layer

Functions at the network layer organize the addressing and delivery of data packets across the network from the host device to the destination device. This includes directing the packets from one router to another router across the internet, till it reaches the internet protocol (IP) address of the destination network. The destination IP address is contained within the header of each data packet. This address will be stored for future routing purposes in routing tables along the packet's path to its destination.

All data packets include an IP address. A data packet is also referred to as an IP packet for TCP connections or a datagram for UDP connections. A router uses the IP address to route packets from network to network based on information contained in the IP header of a data packet. Header information communicates more than just the address of the destination. It also includes information such as the source IP address, the size of the packet, and which protocol will be used for the data portion of the packet.

Format of an IPv4 packet

Next, you can review the format of an IP version 4 (IPv4) packet and review a detailed graphic of the packet header. An IPv4 packet is made up of two sections, the header and the data:

- An IPv4 header format is determined by the IPv4 protocol and includes the IP routing information that devices use to direct the packet. The size of the IPv4 header ranges from 20 to 60 bytes. The first 20 bytes are a fixed set of information containing data such as the source and destination IP address, header length, and total length of the packet. The last set of bytes can range from 0 to 40 and consists of the options field.
- The length of the data section of an IPv4 packet can vary greatly in size. However, the maximum possible size of an IPv4 packet is 65,535 bytes. It contains the message being transferred over the internet, like website information or email text.

There are 13 fields within the header of an IPv4 packet:

- **Version (VER):** This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.

- **IP Header Length (HLEN or IHL):** HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.
- **Type of Service (ToS):** Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.
- **Total Length:** This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.
- **Identification:** IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.
- **Flags:** This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.
- **Fragmentation Offset:** The fragment offset field tells routing devices where in the original packet the fragment belongs.
- **Time to Live (TTL):** TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.
- **Protocol:** The protocol field tells the receiving device which protocol will be used for the data portion of the packet.
- **Header Checksum:** The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.
- **Source IP Address:** The source IP address is the IPv4 address of the sending device.
- **Destination IP Address:** The destination IP address is the IPv4 address of the destination device.
- **Options:** The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

Difference between IPv4 and IPv6

In an earlier part of this course, you learned about the history of IP addressing. As the internet grew, it became clear that all of the IPv4 addresses would eventually be depleted; this is called IPv4 address exhaustion. At the time, no one had anticipated how many computing devices would need an IP address. IPv6 was developed to mitigate IPv4 address exhaustion and other related concerns.

Some of the key differences between IPv4 and IPv6 include the length and the format of the addresses. IPv4 addresses are made up of four decimal numbers separated by periods, each number ranging from 0 to 255. Together the numbers span 4 bytes, and allow for up to 4.3 billion possible addresses. An example of an IPv4 address would be: 198.51.100.0. IPv6 addresses are made of eight hexadecimal numbers separated by colons, each number consisting of up to four hexadecimal digits. Together, all numbers span 16 bytes, and allow for up to 340 undecillion addresses (340 followed by 36 zeros). An example of an IPv6 address would be: 2002:0db8:0000:0000:0000:ff21:0023:1234.

Note: *to represent one or more consecutive sets of all zeros, you can replace the zeros with a double colon "::", so the above IPv6 address would be "*2002:0db8::ff21:0023:1234."

There are also some differences in the layout of an IPv6 packet header. The IPv6 header format is much simpler than IPv4. For example, the IPv4 Header includes the IHL, Identification, and Flags fields, whereas the IPv6 does not. The IPv6 header only introduces the Flow Label field, where the Flow Label identifies a packet as requiring special handling by other IPv6 routers.

There are some important security differences between IPv4 and IPv6. IPv6 offers more efficient routing and eliminates private address collisions that can occur on IPv4 when two devices on the same network are attempting to use the same address.

Key takeaways

Analyzing the different fields in an IP data packet can be used to find out important security information about the packet. Some examples of security-related information found in IP address packets are: where the packet is coming from, where it's going, and which protocol it's using. Understanding the data in an IP data packet will allow you to make critical decisions about the security implications of packets that you inspect.