Networking

Networking Fundamentals

1.4.2 - IPv4 and IPv6

What are the differences between IPv4 and IPv6?

Overview
Given a scenario, the student will configure a subnet and use appropriate IP addressing schemes

Grade Level(s)
10, 11, 12

Cyber Connections

- Threats & Vulnerabilities
- Networks & Internet
- Hardware & Software

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Teacher Notes:

CompTIA N10-008 Network+ Objectives

Objective 1.4

- Given a scenario, configure a subnet and use appropriate IP addressing schemes
  - IPv4 vs. IPv6
    - Automatic Private IP Addressing (APIPA)
    - Extended unique identifier (EUI-64)
    - Multicast
    - Unicast
    - Anycast
    - Broadcast
    - Link local
    - Loopback
    - Default gateway
  - IPv4 subnetting
    - Classless (variable-length subnet mask)
    - Classful
      - A
      - B
      - C
      - D
      - E
    - Classless Inter-Domain Routing (CIDR) notation
  - IPv6 concepts
    - Tunneling
    - Dual Stack
    - Shorthand notation
    - Router advertisement
    - Stateless address autoconfiguration (SLAAC)

IPv4 and IPv6

Although IPv4 has been around since the early 1980's, it is still the one of the most used protocols to route traffic across the internet. IPv4 uses 32-bit addresses that contain 4 octets separated by three periods. For example, in binary form, the IPv4 addresses range from 00000000.00000000.00000000.00000000 – 11111111.11111111.11111111.11111111. Since each octet contains 8 binary digits, there are 28 numbers, or 256 numbers that range from 0 – 255 in each octet.

Teacher Notes:

Combining the 4 octets, there are 2564 (or 4,294,967,296) possible IPv4 addresses. Also, in the more common decimal form, IP addresses range from 0.0.0.0 – 255.255.255.255. An example of an IP Address is one of CYBER.ORG's IP Addresses which is 67.207.83.25.

With so many devices that were connected to the internet, like computers, tablets, phones, cameras, refrigerators, etc…, people quickly realized that 4.2 billion IP addresses were not enough, thus, IPv6 protocol started to be created in 1998 and officially ratified in 2017. IPv6 has over 340 trillion trillion (or 340,282,366,920,938,463,463,374,607,431,768,211,456) IP addresses, now that's a lot of addresses. IPv6 addresses have 8 groups separated by colons, that contain 4 hexadecimal numbers each. An example of an IPv6 address is d778:e150:0000:81d6:37a4:0000:8eee:d64d, and this can be shortened to d778:e150::81d6:37a4::8eee:d64d.

There are a lot of similarities and differences between IPv4 and IPv6 protocol, below are some properties of each of the two protocols.

Automatic Private IP Addressing (APIPA) – This is for IPv4 protocol and not IPv6. When a device is connected to a private network, the DHCP assigns that device an IP address for that network. However, if the DHCP server is not working, APIPA can auto-assign an IP address for that device on the network. The IP address range for APIPA is 169.254.0.1 – 169.254.255.254 and cannot assign addresses outside of these.

Extended unique identifier (EUI-64) – This is IPv6's way to uniquely assign a system their own unique 64-bit IPv6 interface identifier. Like the APIPA, this does not involve a DHCP or some other system on the network manually configuring this. It works by using two things, the MAC address of the machine and the 16-bit hex value 0xFFFE. The MAC address is 48-bits long, and is split exactly in half, so 24 on each side and the 16-bit hex value is inserted in between them. Since the MAC address is unique to the device, this keeps the address unique and can be designated to that specific machine.

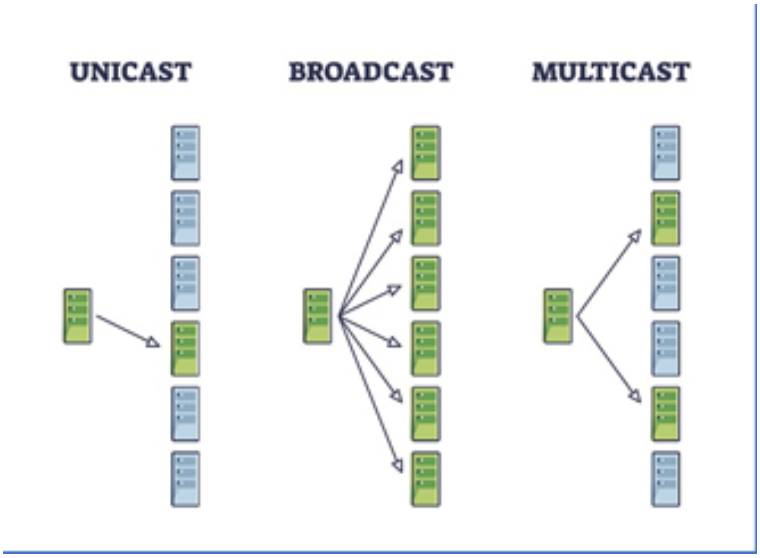
Multicast – This is a routing scheme that works on both IPv4 and IPv6 protocols. This allows for packets to be delivered to multiple addresses set by the sender. Thus, if there are 10 devices on the network, the sender can multicast and send the packets to three receivers who will get them.

Teacher Notes:

Unicast – While multicast sends the packets to a group of specific devices, unicast only sends the packets to 1 specific device. This is also works on both IPv6 and IPv4 devices.

Anycast – This only works on IPv6 and is a mix of Unicast and Multicast. A group of addresses can be assigned to receive the packets like in multicast, however, in the end only 1 of those devices on the group end up receiving the packets.

Broadcast – This is when all the packets go to every other device on the network. Thus, when a sender sends out the packets, every other device on the network acts as a receiver and gets them. This was inefficient, thus IPv6 does not use this feature, it can only be used with IPv4 protocol.



Visual of unicast, broadcast, and multicast

Link-local – A link-local address is very similar to how a APIPA works, when a device connects to a network and is not automatically assigned an IP, the link-local can find a free address and assign their own. It will ask the network, does anyone have 169.254.1.1, and then use it if no one has it. If someone did, it would go to 169.254.1.2, and so on. The range of link-local for IPv4 is 169.254.0.0/16 (169.254.0.0 – 169.254.255.255) and IPv6 is in the block FE80::/10.

Teacher Notes:

Loopback – The loopback address allows a machine to send packets to itself. This might sound like it's unnecessary, but it can be very useful for debugging and testing purposes. It's very simple, the data packets will be sent to the network and sent back to where they came from

The loopback address on IPv4 is 127.0.0.1 and the loopback for IPv6 is 0:0:0:0:0:0:0:1, which can be shortened to ::1.

Default gateway – This is a critical network component that allows devices on different networks to communicate. These devices find the easiest route to another machine, they can even connect machines using different protocols.

IPv4 Subnetting Classful

The oldest form of allocating IP addresses in IPv4 protocol is with ***classful*** subnetting. This is when IP addresses are divided into 5 different categories, A through E. Here are the A through E classes:

Class A – This is a public addressing system that sends one-to-one communication between the destination and the source. This has a subnet mask of 255.0.0.0 and has a range from 0.0.0.0 – 127.255.255.255. However, 0.x.x.x is reserved for the default network and 127.x.x.x is reserved for the loopback, so the range is actually 1.0.0.0 – 126.255.255.255. An example of a class A IP address is 17.1.1.1.

Class B - This public addressing system is like class A, but the first two numbers signify the network, while the last two numbers signify the host. Thus, having the subnet address of 255.255.0.0. The range of class B addresses is 128.0.0.0 to 191.255.255.255. An example of a class B IP address is 172.17.13.15, here the 172.17 signifies the network the device is located on, while the 13.15 is the device on the network.

Class C – This is like classes A and B, but now the subnet mask is 255.255.255.0 where the first three numbers signify the network and only the last number signifies the host/device. The range is from 192.0.0.0 to 223.255.255.255. An example is 192.168.17.145. Here, 192.168.17 is the network while 145 signifies the device.

Teacher Notes:

Class D – The range of these IP addresses is 224.0.0.0 – 239.255.255.255 and is used for multicast addresses.

Class E – This has the range of 240.0.0.0 – 255.255.255.255 and is saved for scientific research and future use.

IPv4 Classless

Using the classful addresses, people quickly realized that the number of IP Addresses quickly run out. For example, look at the following chart below:

Class	Networks Supported	Devices per Network	Total Addresses
A	128	16,777,216	2,147,483,648
B	16,384	65,536	1,073,741,824
C	2,097,152	256	536,870,912

If a company requires 3,000 IP addresses for the devices on their network, the best class for them would be Class B. However, this means that 62,536 IP Addresses are left unused, taking from the total number of IP addresses. To counter this, they could be given multiple Class C networks, but then it takes from the total number of networks that Class C is able to support. This leading to the Classless subnetting, which is sometimes referred to as CIDR notation (Classless Inter-Domain Routing).

CIDR notation is known as a variable length subnet mask. Here, subnets are given in blocks, with the most common being /0, /8, /16, /24, and /32. Look at the chart below to see how these CIDR blocks work.

CIDR Block	CIDR Range	Total Number of IP Addresses
0.0.0.0/0	0.0.0.0 – 255.255.255.255	4,294,967,296
0.0.0.0/8	0.0.0.0 – 0.255.255.255	16,777,216
0.0.0.0/16	0.0.0.0 – 0.0.255.255	65,536
0.0.0.0/24	0.0.0.0 – 0.0.0.255	256
0.0.0.0/32	0.0.0.0 – 0.0.0.0	1

Teacher Notes:

The /0 to /32, actually refers back to the 32-bits that make up an entire IP address. For example, if using the /0, this signifies that none of the entire 32-bits will change, while /16 means that half, or 16, of the 32-bits are able to change. Below is the IP address 124.55.7.240 in binary form:

01111100.00110111.00000111.11110000

The CIDR notation 124.55.7.240/16 means that the first 16 binary digits remain the same. Thus, 01111100.00110111 will not change while the second half of 00000111.11110000 can all be changed, giving this IP the range of 124.55.0.0 – 124.55.255.255. Using this same idea, what is the range of the CIDR block 124.55.7.240/17. Here, the first 17 digits remain the same, those are 01111100.00110111.0, meaning the last 15 binary digits can go from 0000000.00000000 – 1111111.1111111. This giving the total range of:

01111100.00110111.00000000.00000000 - 01111100.00110111.01111111.11111111

This in decimal, is the range of 124.55.0.0 – 124.55.127.255.

IPv6 Concepts

Here are some concepts for IPv6 protocol.

Tunneling – This allows for two networks/devices that use IPv6 to communicate over a network using IPv4. Not all networks use IPv6 yet, thus trying to only use IPv6 protocol over the WAN can get messy, so creating a tunnel/VPN will help two devices using IPv6 to communicate over a network not controlled by them.

Dual stack – This is when a device uses both IPv4 and IPv6 protocol. This allows for a network to start upgrading to IPv6 without having to do all the devices at once.

Shorthand notation – This allows an IPv6 address to be shortened since they can be very long to write out. For example, the IPv6 address 2004:0fb8:3c4d:0015:0000:0000:1b2f:1a2b can be shortened/collapsed to 2004:fb8:3c4d:15::1b2f:1a2b

Teacher Notes:

Router advertisement – This is the router sending messages to an IPv6 network to all the nodes on the network, typically around every 200 seconds. It's providing updates to the network in which the hosts can learn the prefixes and parameters of that network.

Stateless address autoconfiguration (SLAAC) - This is an automatic IPv6 address allocation like APIPA. However, the stateless signifies that there is not a server holding/keeping track of what device has what IP address. Just like EUI-64, SLAAC uses the MAC address to help create unique IP addresses that should not be used by other devices.