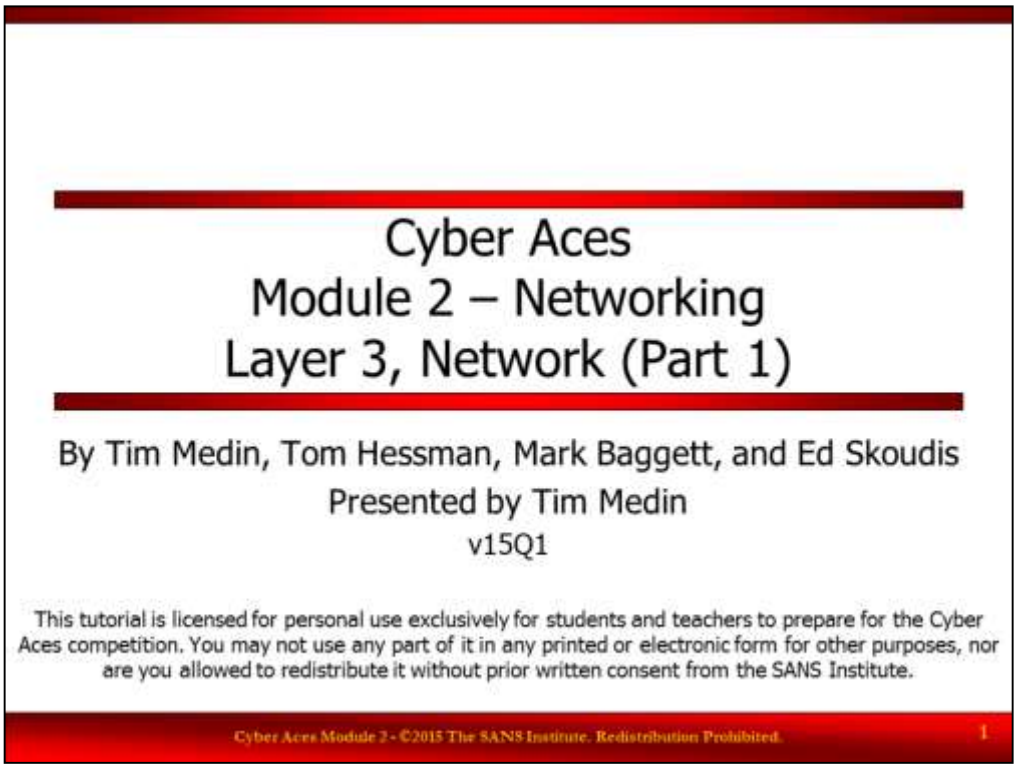
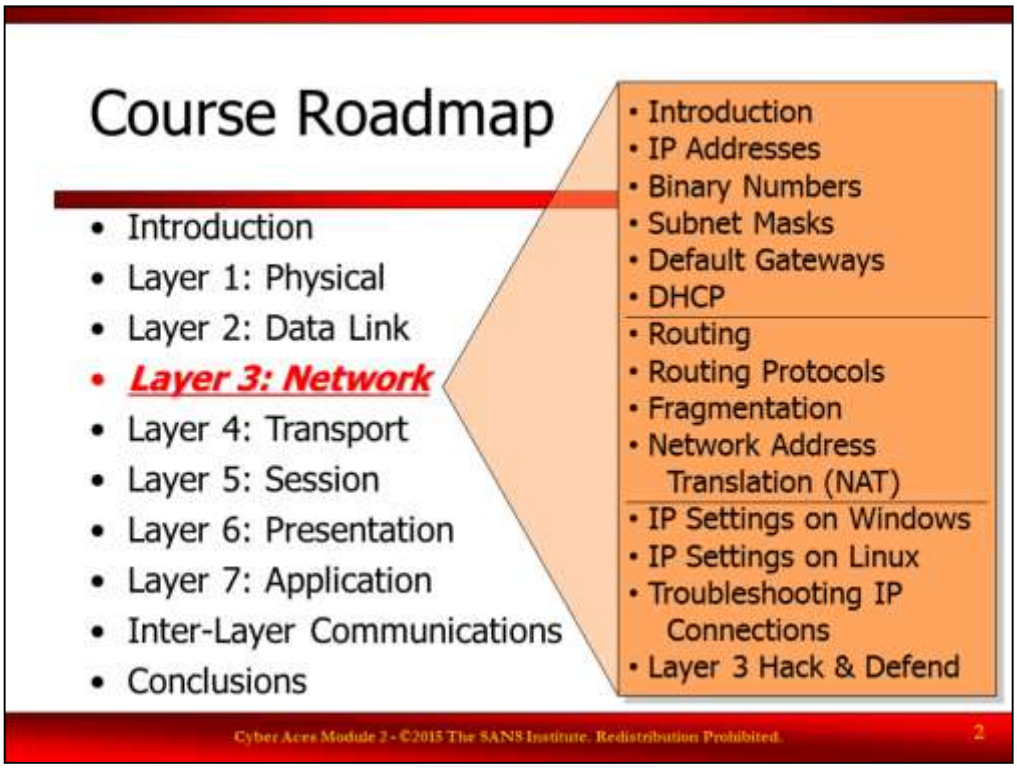
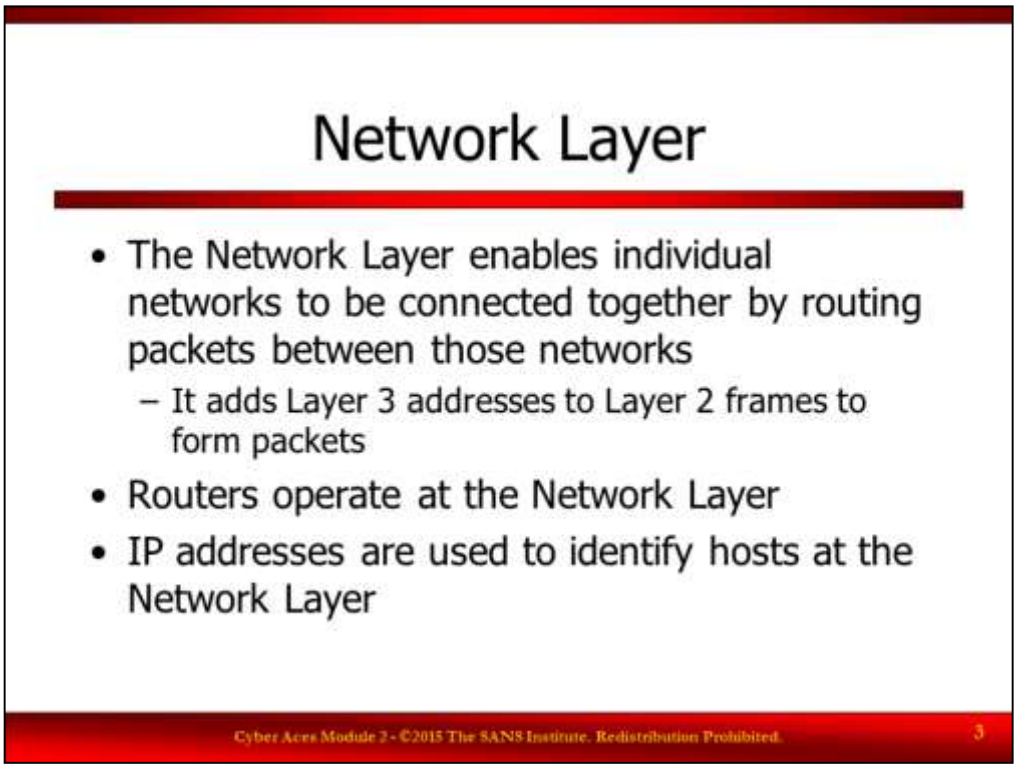


Welcome to Cyber Aces, Module 2! A firm understanding of network fundamentals is essential to being able to secure a network or attack one. This section provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective. Specifically, in this section we will be discussing layer 3 of the OSI model, the Network Layer.



Course Roadmap

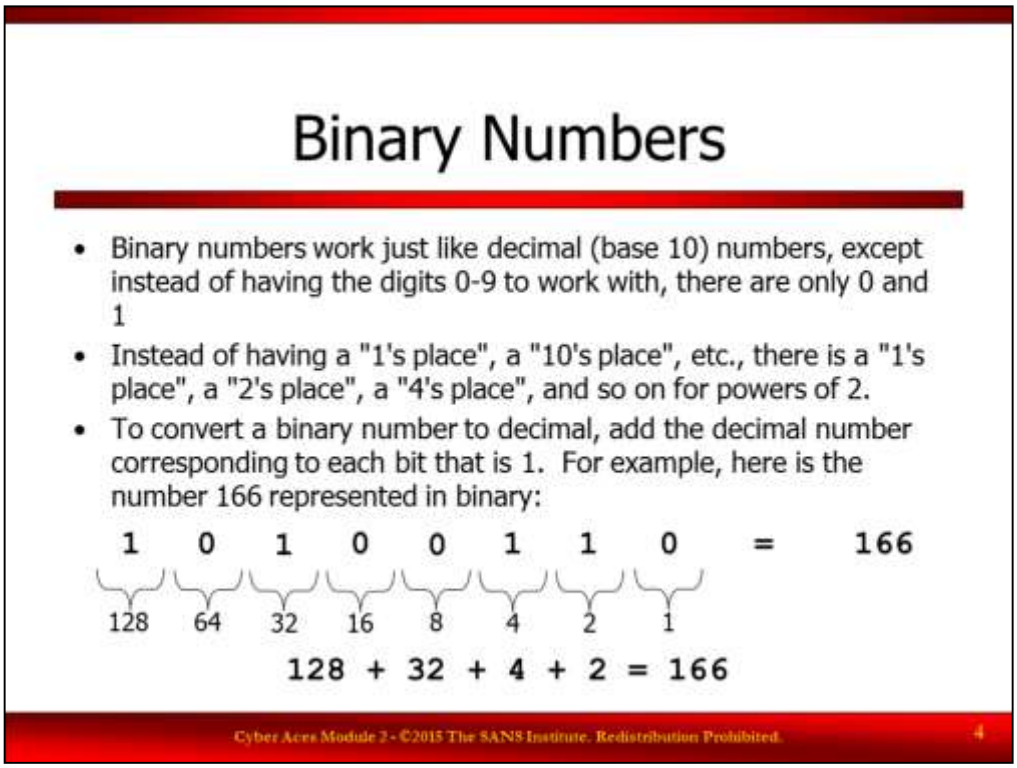
In this section, you'll learn about the Network Layer. You'll learn about IP addressing, subnet masks, default gateways, routing, NAT, and more!



Network Layer

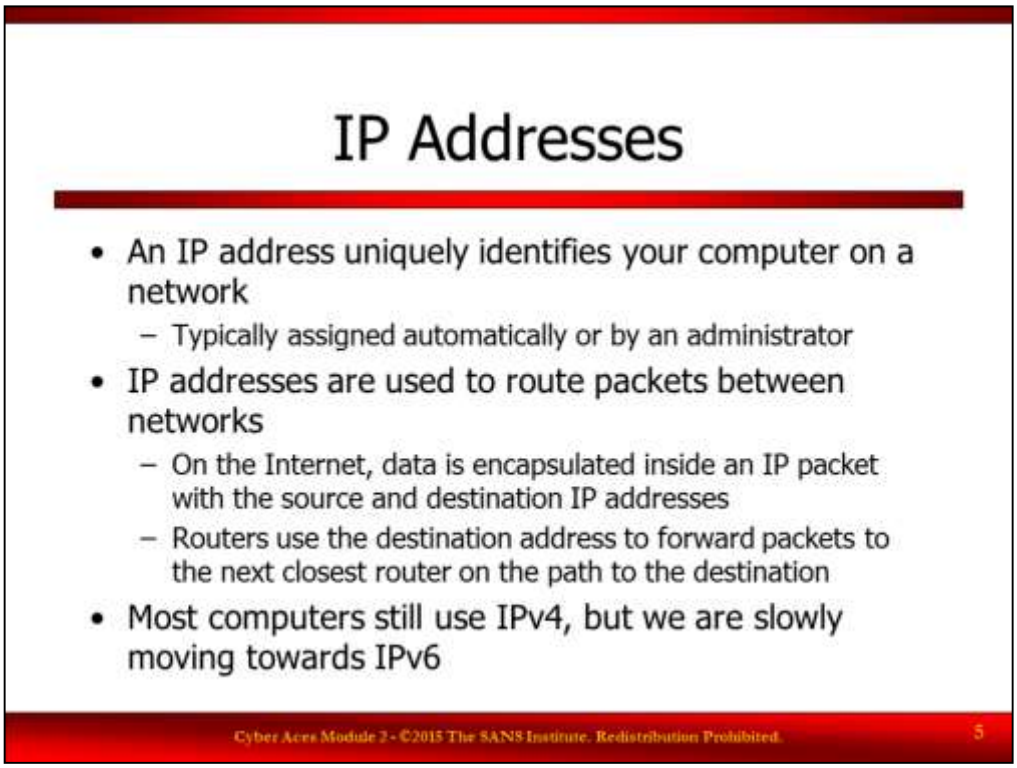
The Network Layer sits on top of the Data Link Layer. Using the Data Link Layer we can communicate with other devices over a Local Area Network. The Network Layer enables the interconnection of many Local Area Networks by routing packets between those networks. It enables communications across networks by taking our Layer 2 FRAMES and adding Layer 3 addresses to it. A frame with a Layer 3 address on it is often referred to as a PACKET. Routers operate at this layer of the OSI model. On the Internet, IP addresses are used to identify hosts at the Network layer.

Before we dive into IP addresses, let's take a quick look at understanding binary numbers.



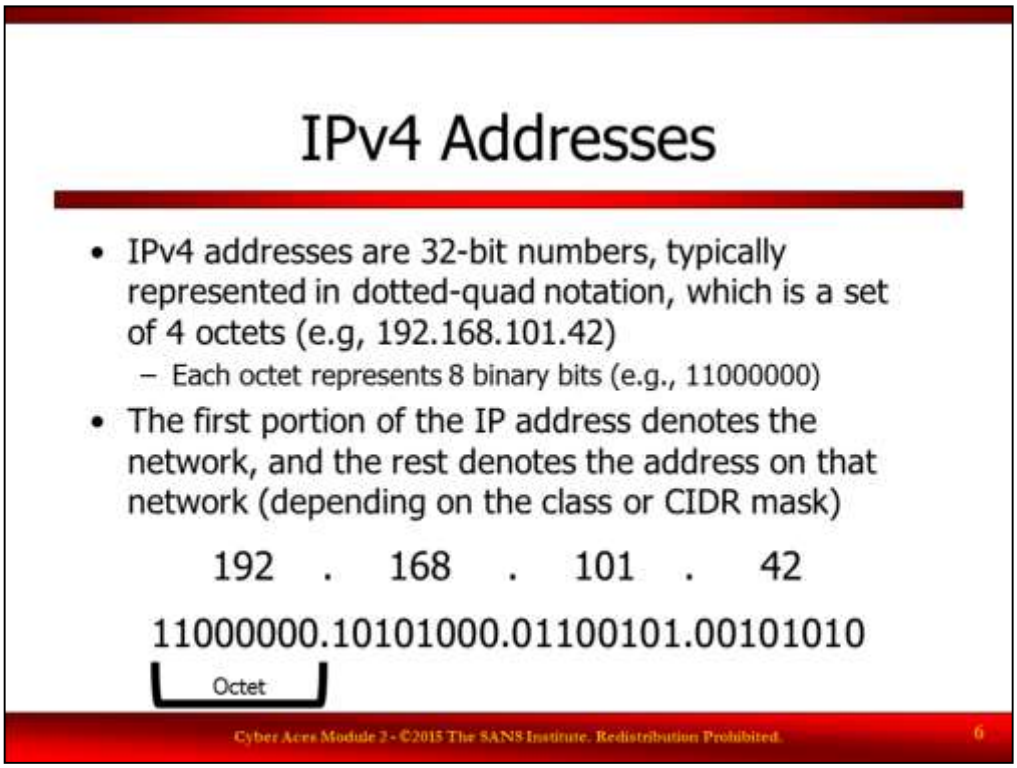
Binary Numbers

While many people think that binary (base 2) numbers are confusing on first glance, they work very much like decimal (base 10) numbers. With decimal numbers, the position of each digit (from right to left) represents increasing powers of ten, and there are ten digits to work with (0-9). So, for example, the number 166 is one 100, six 10's, and six 1's. In binary, the only digits are 0 and 1, and each position represents increasing powers of two. The binary number 101, for example, is one 4, zero 2's, and one 1. In the example above, 10100110 is 1x128, 0x64, 1x32, 0x16, 0x8, 1x4, 1x2, and 0x1. If you add up the bits that are 1, you can easily convert this to the decimal number 166.



IP Addresses

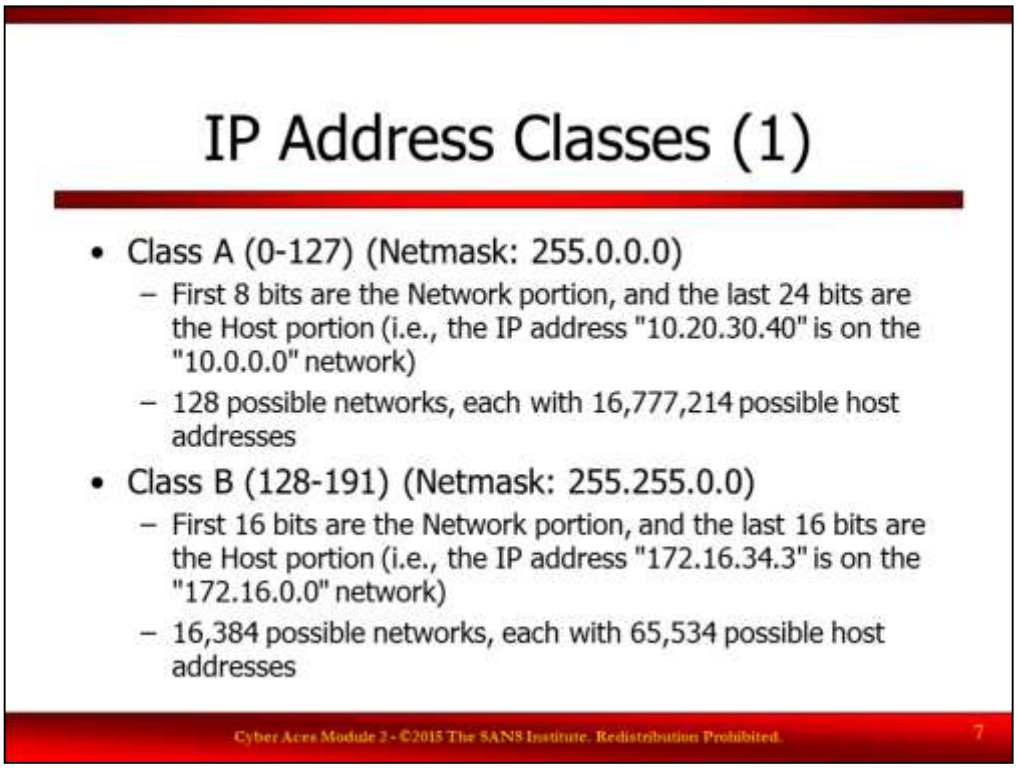
An IP Address is a unique set of numbers that identifies your computer on a network. Unlike a MAC address, IP addresses are mutable (i.e., they may be changed during normal operation), and are typically assigned either automatically (using a protocol such as DHCP) or manually by an administrator. Internet routers use IP addresses similar to the way the postal service uses your street address. Messages that travel across the Internet are placed in an envelope (an IP packet) with the sender's address and the destination address. By looking at the destination address, routers continuously forward packets to the next closest router along a path until the packets eventually reach the destination. Although today most of our computers are using IP Version 4 (IPv4) to access resources, we are slowly moving towards IP Version 6 (IPv6).



IPv4 Addresses

IPv4 addresses are 32-bit numbers, meaning they are made up of 32 binary digits. The 32 bits are split into 4 groups called "octets", which are each composed of 8 bits. 8 bits are equal to 1 byte, so an IP address is a 4 byte number. They are generally displayed in a more human-readable form called "dotted-quad notation", which consists of 4 decimal (base 10) numbers, 0-255, separated by dots. For example, the IP address "11000000.10101000.01100101.00101010" would normally be displayed as "192.168.101.42".

The first portion of the IP address is the Network portion, which denotes what network the address is a part of. The rest of the IP address denotes a specific host on that network. How much of the IP address is the Network portion depends on the class or CIDR mask in use.

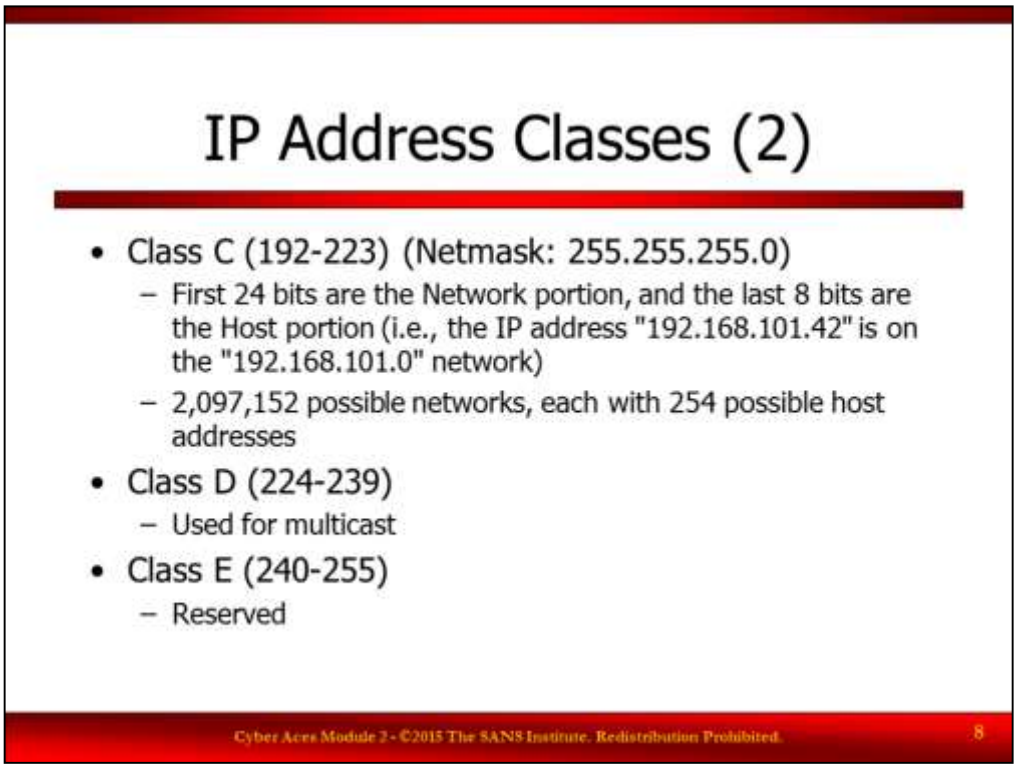


IP Address Classes (1)

Originally, blocks of IP addresses on the Internet were assigned based on just the first octet. However, as Local Area Networks became popular, it soon became clear that more than 254 networks would be necessary (and that most individual organizations would probably need less than 16,777,214 IP addresses). The concept of IP address classes was introduced to be able to assign smaller blocks of addresses.

In a Class A network, the first binary bit of the first octet is a 0 (zero), corresponding to the addresses 0.0.0.0-127.255.255.255. The first octet identifies the network, and the last three octets identify the specific host on the network. So, for example, the IP address "10.20.30.40" would be on the network "10.0.0.0". Class A allows for 128 possible networks within a given block, and each network can have 16,777,214 hosts on it.

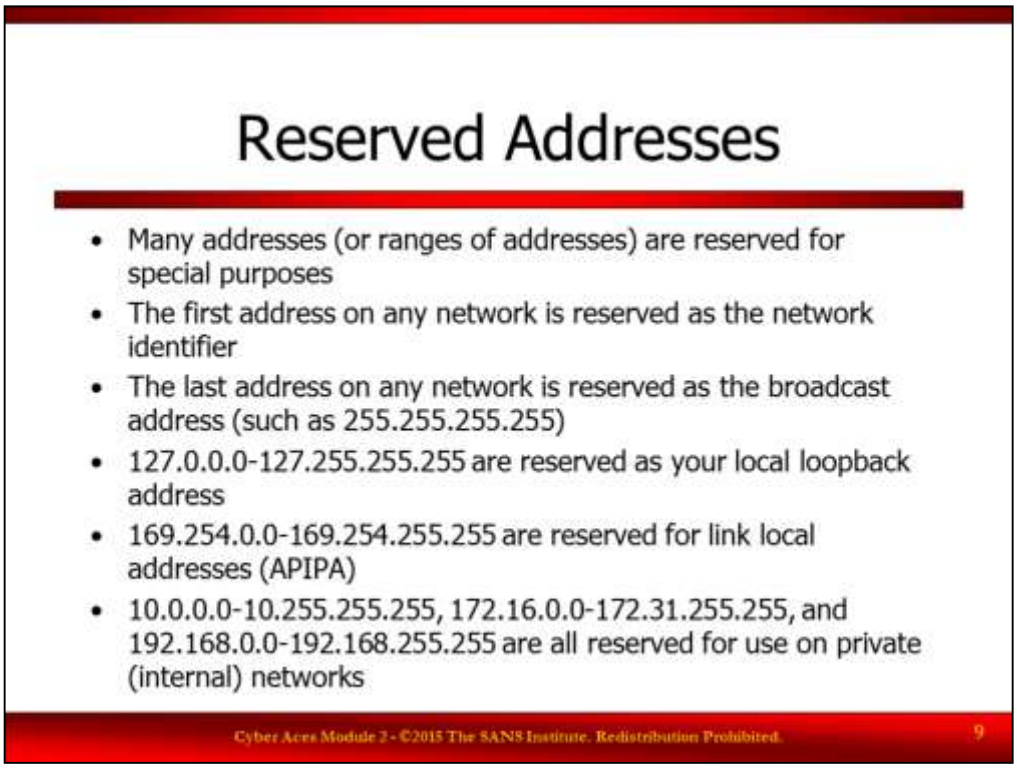
In a Class B network, the first two binary bits of the first octet are 10 (one-zero), corresponding to the addresses 128.0.0.0-191.255.255.255. The first two octets identify the network, and the last two octets identify the specific host on the network. So, for example, the IP address "172.16.34.3" would be on the network "172.16.0.0". Class B allows for 16,384 possible networks within a given block, and each network can have 65,534 hosts on it.



IP Address Classes (2)

In a Class C network, the first three binary bits of the first octet are 110 (one-one-zero), corresponding to the addresses 192.0.0.0-223.255.255.255. The first three octets identify the network, and the last octet identifies the specific host on the network. So, for example, the IP address "192.168.101.42" would be on the network "192.168.101.0". Class C allows for 2,097,152 possible networks within a given block, and each network can have 254 hosts on it.

Class D network addresses are reserved for use with multicast, a protocol for broadcasting data to multiple hosts simultaneously. The multicast address ranges are from 224.0.0.0-239.255.255.255. Class E network addresses (240.0.0.0-255.255.255.254) are reserved for future use.



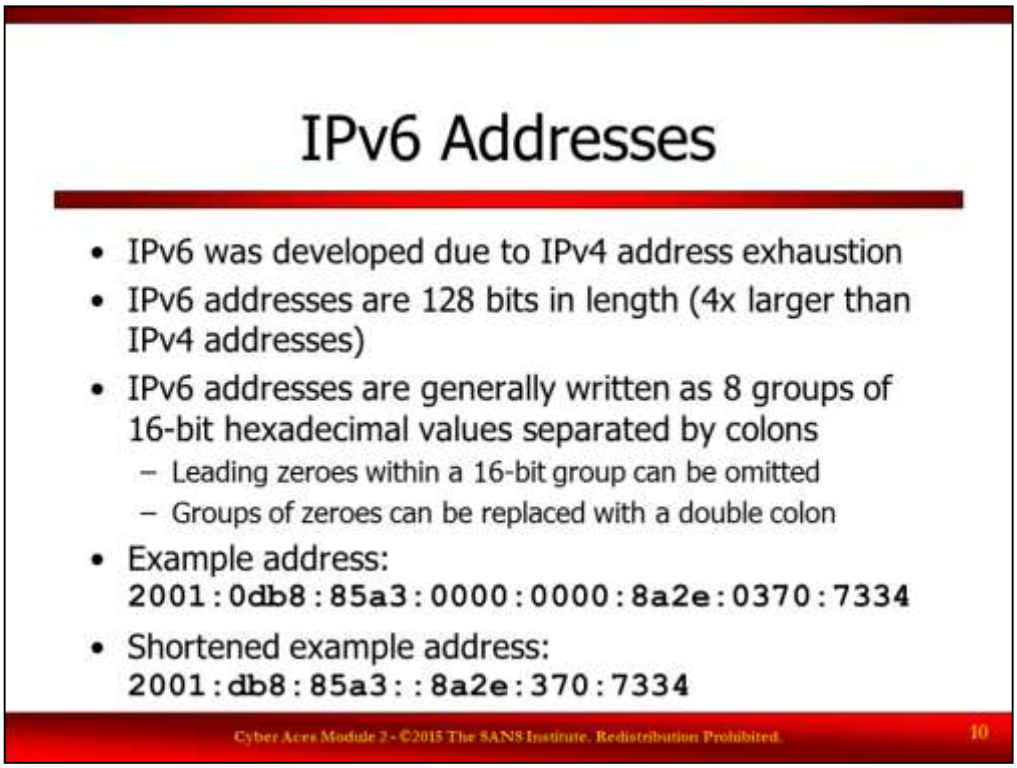
Reserved Addresses

Many potential IPv4 addresses are reserved for special purposes, making them unavailable for general use. For example, the first and last addresses on any given network are reserved. The first address on any network (such as 192.168.0.0) is reserved as the network identifier. The last address on any network (such as 192.168.255.255) is reserved as that network's broadcast address. Any traffic sent to that address is broadcasted to all addresses on the network. 255.255.255.255 is a special broadcast address for all potential networks.

The IP range 127.0.0.0-127.255.255.255 is reserved for local loopback addresses, which are special addresses that point to your own machine (i.e., any traffic sent to it loops straight back to where it came from). The most commonly used loopback address is 127.0.0.1, though any address in that range will work.

The IP range 169.254.0.0-169.254.255.255 is reserved for link local addresses (also known as APIPA, or Automatic Private IP Addressing). When a computer is connected to a network and is not configured with a manual IP address, it tries to obtain one automatically. If it is unable to, then it assigns itself a link local address in this range, allowing it to communicate with other nearby computers with link local addresses. This is particularly important for IPv6.

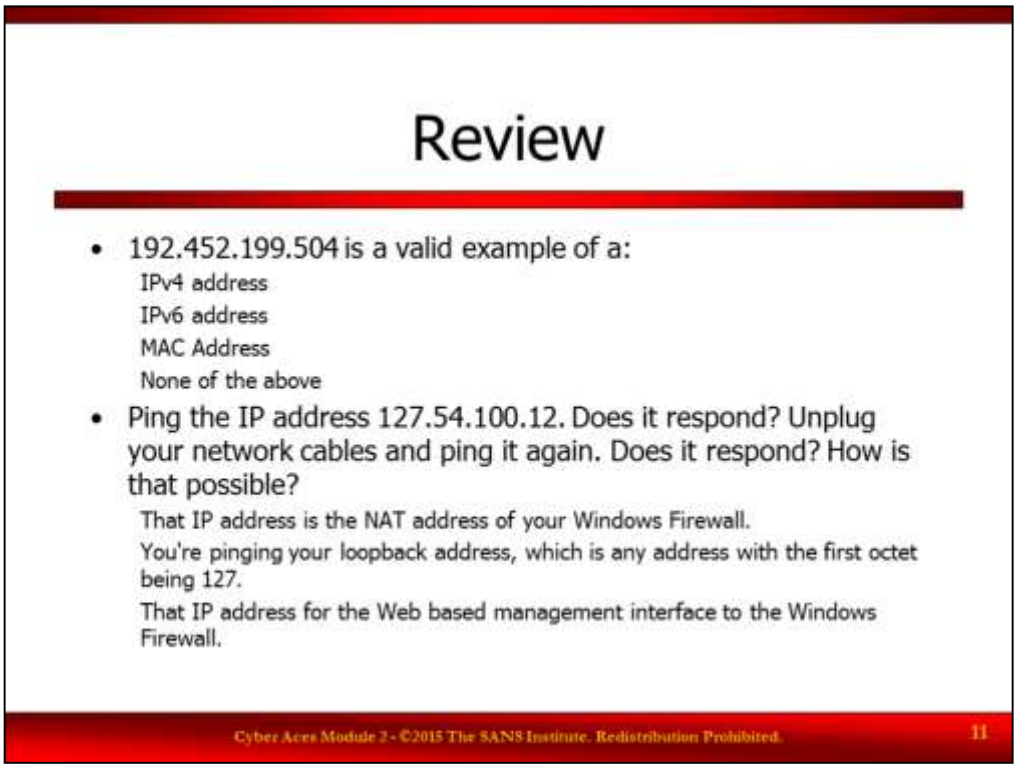
Finally, there are 3 IP ranges set aside for private use (10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255). These addresses are intended to be used on internal networks, for machines that don't require direct Internet access. In fact, these addresses are non-routable, meaning that their traffic cannot be directly routed on the Internet. Private IP addresses are commonly used everywhere from large enterprise networks to small home networks. They are not assigned to any specific organization, allowing anyone to use them (similar to unlicensed spectrum). By using private IP addresses, organizations don't have to waste precious public IP addresses, since a single Internet connection can be shared by means of a proxy server or NAT (more on that later).



IPv6 Addresses

When the Internet was first developed, 4,294,967,296 (2^{32}) possible IPv4 addresses seemed like more than enough. However, as the Internet grew, it became apparent that the address space would run out, particularly since many addresses have reserved purposes, and many address blocks are not efficiently allocated. While many short term solutions have been enacted (such as NAT), the long term solution was to create a new address scheme, IPv6, that supports more addresses (2^{128}).

IPv6 addresses are 128 bits in length (four times larger than IPv4 addresses), and are generally written as 8 groups of 16-bit hexadecimal values separated by colons. An example IPv6 address is: **`2001:0db8:85a3:0000:0000:8a2e:0370:7334`**. Within a 16-bit group, leading zeroes can be omitted, and entire groups of zeroes can be replaced with a double colon. So, the example address above could also be written as: **`2001:db8:85a3::8a2e:370:7334`**.



Review Questions

192.452.199.504 is an example of a:

IPv4 address

IPv6 address

MAC Address

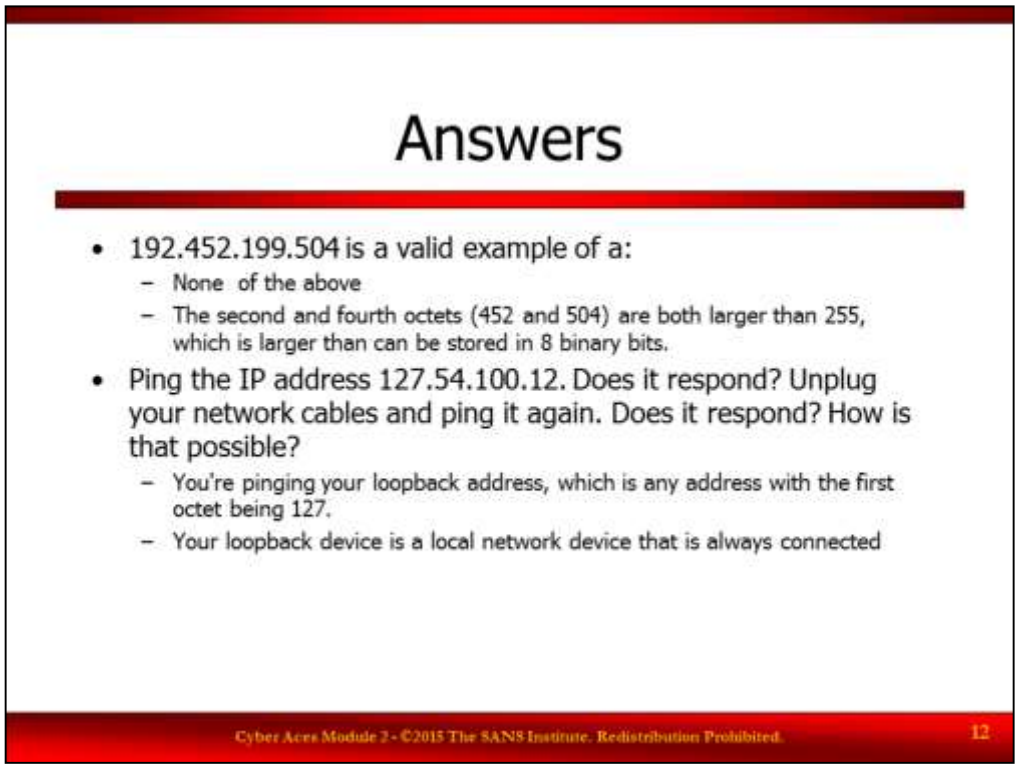
None it is not valid

Ping the IP address 127.54.100.12. Does it respond? Unplug your network cables and ping it again. Does it respond? How is that possible?

That IP address is the NAT address of your Windows Firewall.

You're pinging your loopback address, which is any address with the first octet being 127.

That IP address for the Web based management interface to the Windows Firewall.



Answers

192.452.199.504 is an example of a:

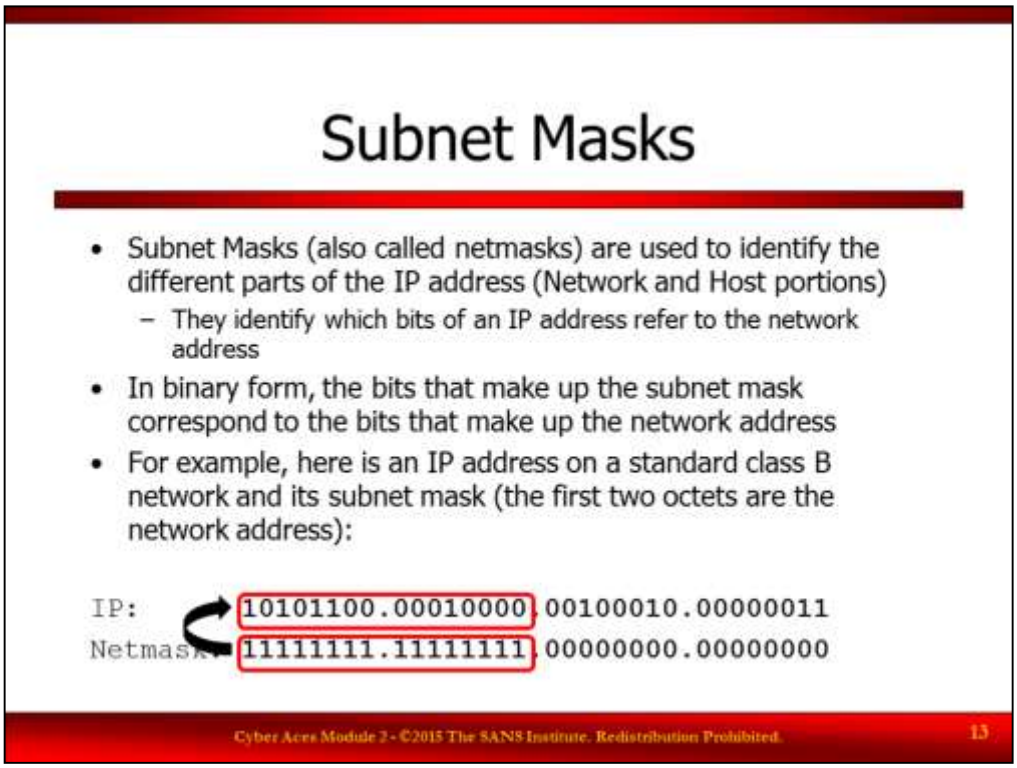
None it is not valid

The second and fourth octets (452 and 504) are both larger than 255, which is larger than can be stored in 8 binary bits.

Ping the IP address 127.54.100.12. Does it respond? Unplug your network cables and ping it again. Does it respond? How is that possible?

You're pinging your loopback address, which is any address with the first octet being 127.

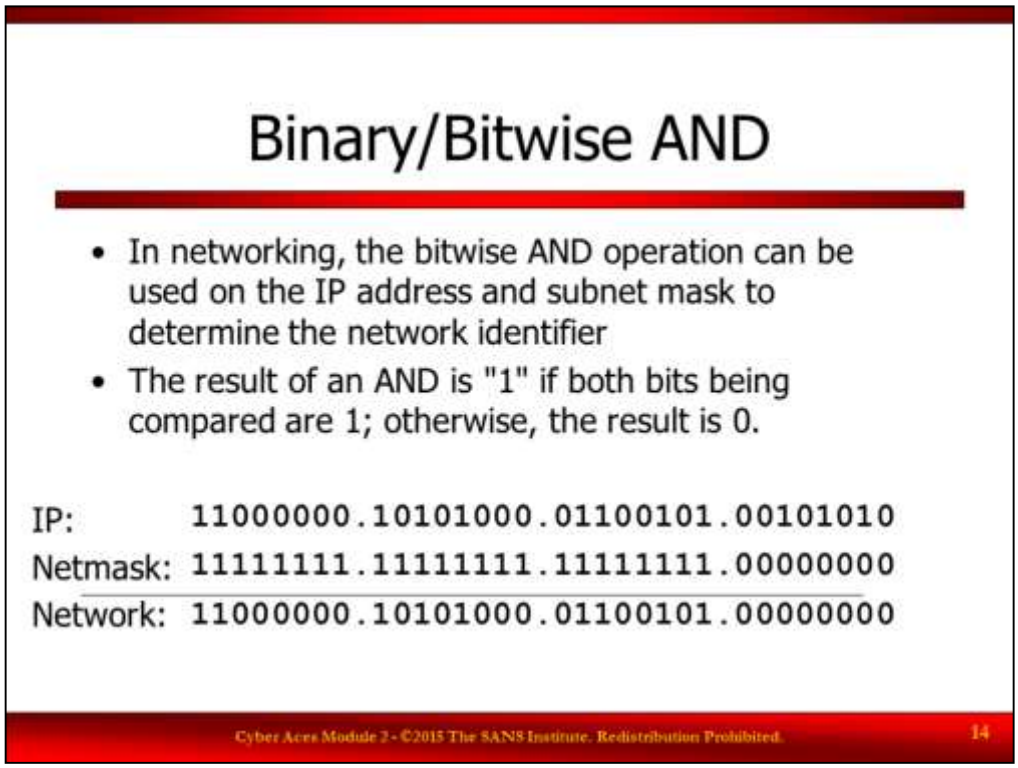
Your loopback device is a local network device that is always connected



Subnet Maskes

The Subnet mask is used identify different parts of your IP address. We said that the IP address is similar to your street address. Your street address usually has more than one part. There is a Street Name and a house number. There are also multiple parts to an IP addresses. There is a HOST portion and a NETWORK portion. We use the subnet masks to identify which part of the address is the host and which part is the network. The bits in the subnet mask correspond to the bits that make up the network address. In other words, all of the bit positions in the subnet mask that are set to 1 are part of the network address in the actual IP address.

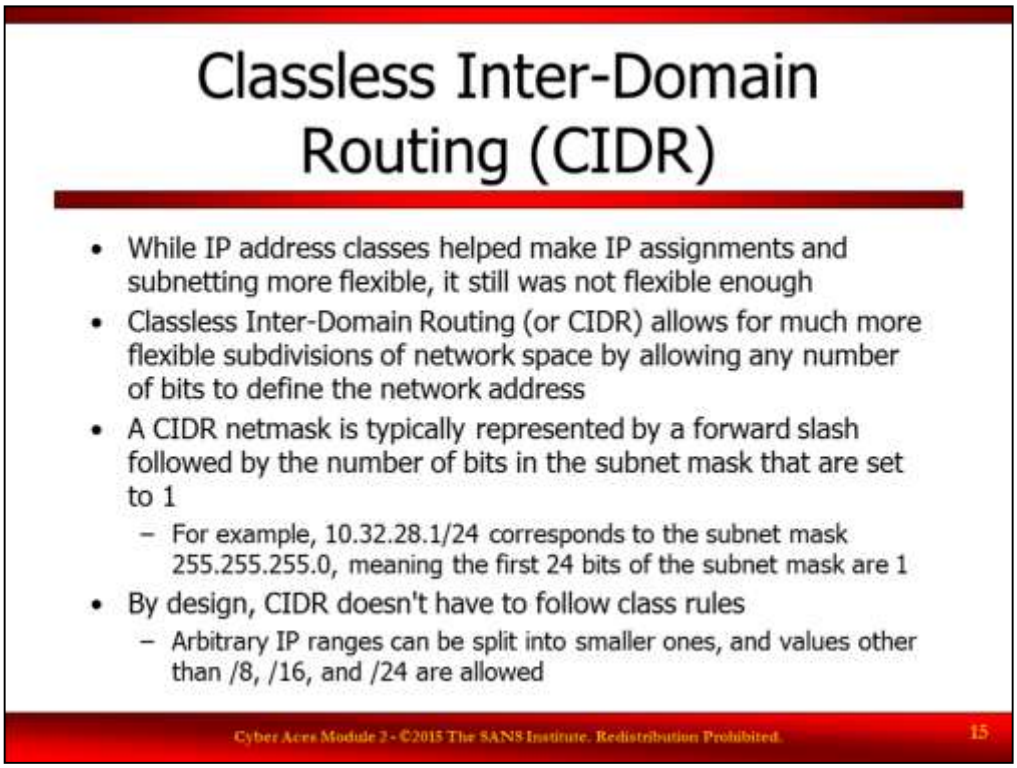
In the example above, the first 16 bits of the subnet mask are set to 1, and the last 16 bits are 0. Therefore, the first 16 bits of the IP address are the network address, and the other 16 are the node address.



Binary/Bitwise AND

In networking, the bitwise "AND" operation can be used to determine the network identifier from the IP address and subnet mask, which can subsequently be used to determine if two hosts are on the same network (which is particularly important for routing). When performing an AND, the result for any two bits is "1" if both bits are 1, and are 0 in all other cases.

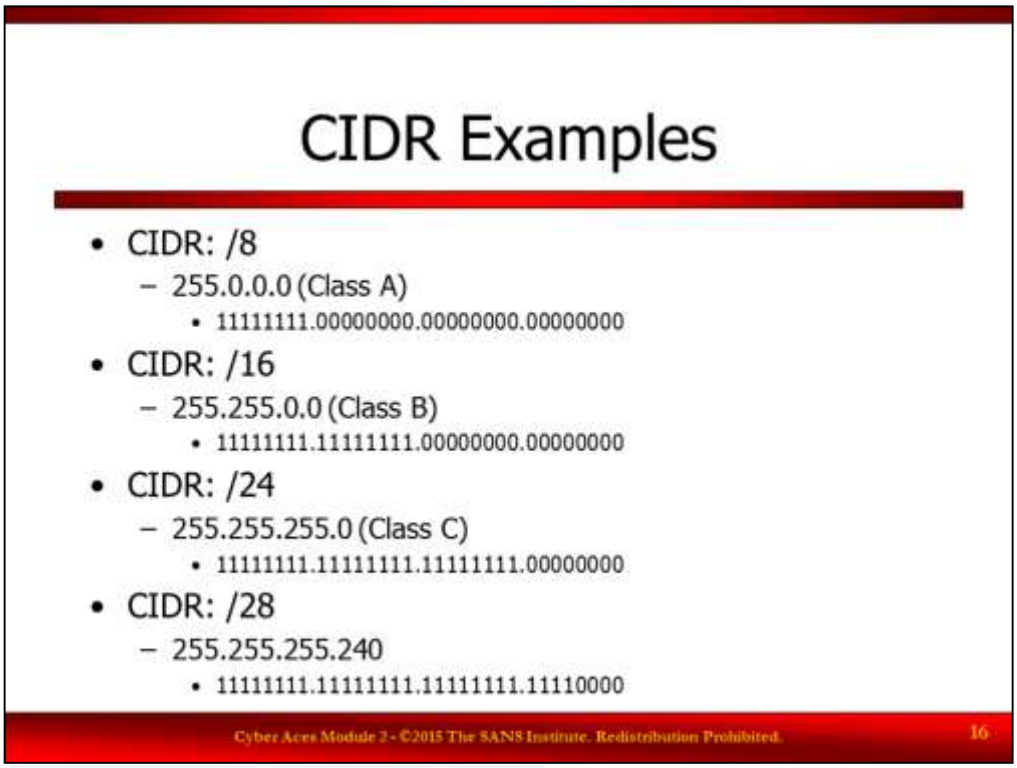
In the example above, the first line is the IP address (192.168.101.42), and the second line is the subnet mask (255.255.255.0). By performing the bitwise AND operation, the network ID is determined to be 192.168.101.0.



Classless Inter-Domain Routing (CIDR)

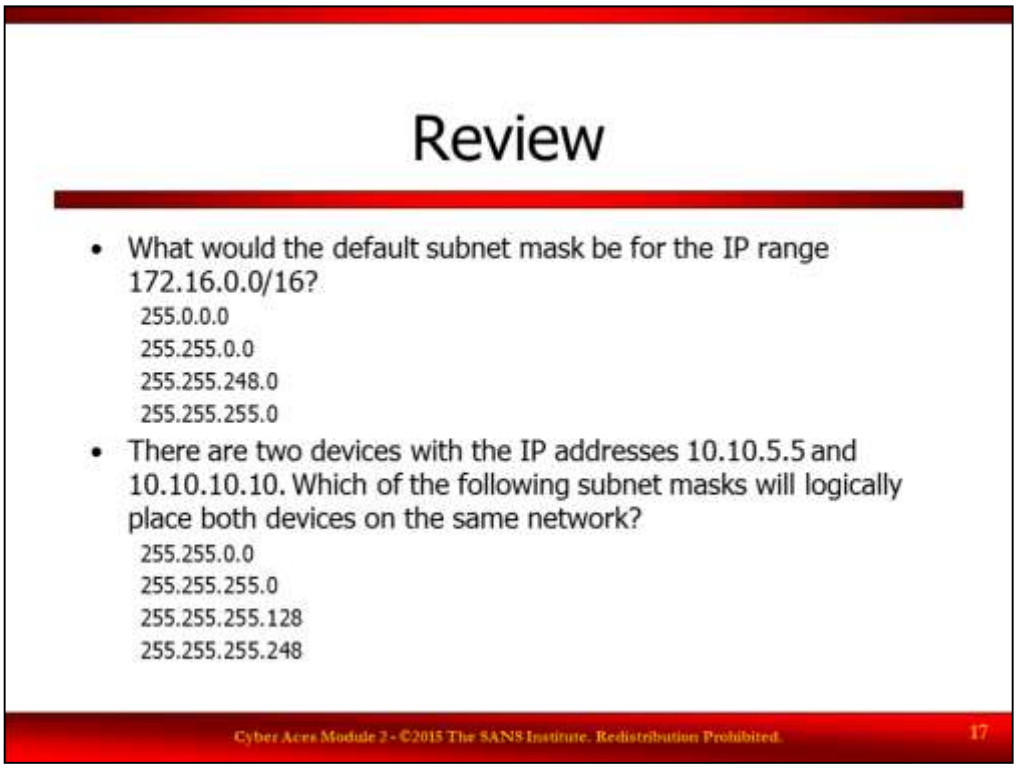
Classful addressing was originally designed to make IP address assignments and subnetting more flexible. However, eventually it was proven that classful addressing still was not flexible enough, as people sought to sub-divide networks more and more. The size of IP routing tables was also growing rapidly. So, a new standard called Classless Inter-Domain Routing (or CIDR) was introduced, which breaks away from the rigid rules of traditional classful addressing. Rather than being limited to 8, 16, or 24 bits, CIDR allows for any number of leading bits in an IP address to define the network address. This allows for many more individual networks, of increasingly small size.

A CIDR netmask is typically represented by a forward slash (/) followed by the number of bits in the subnet mask that are set to 1. For example, 10.32.28.1/24 represents a machine on the network 10.32.28.0 with a subnet mask of 255.255.255.0 (so, the first 24 bits are 1). Note that the IP address is part of the 10.0.0.0 range...with CIDR, it's okay to split that into less than a /8! CIDR also makes it more organized and hierarchical when splitting larger IP blocks into smaller ones, since the CIDR masks will always be subsets of the larger one.



CIDR Examples

Above are some examples of CIDR netmasks and their corresponding subnet masks. Note that with CIDR, you are not limited to having an entire octet be either 0 or 255. We refer to the CIDR mask by the number of bits in the mask. I.E, A mask of 255.255.255.0 is referred to as a "slash 24".



Review Questions

What would the default subnet mask be for the IP range 172.16.0.0/16?

255.0.0.0

255.255.0.0

255.255.248.0

255.255.255.0

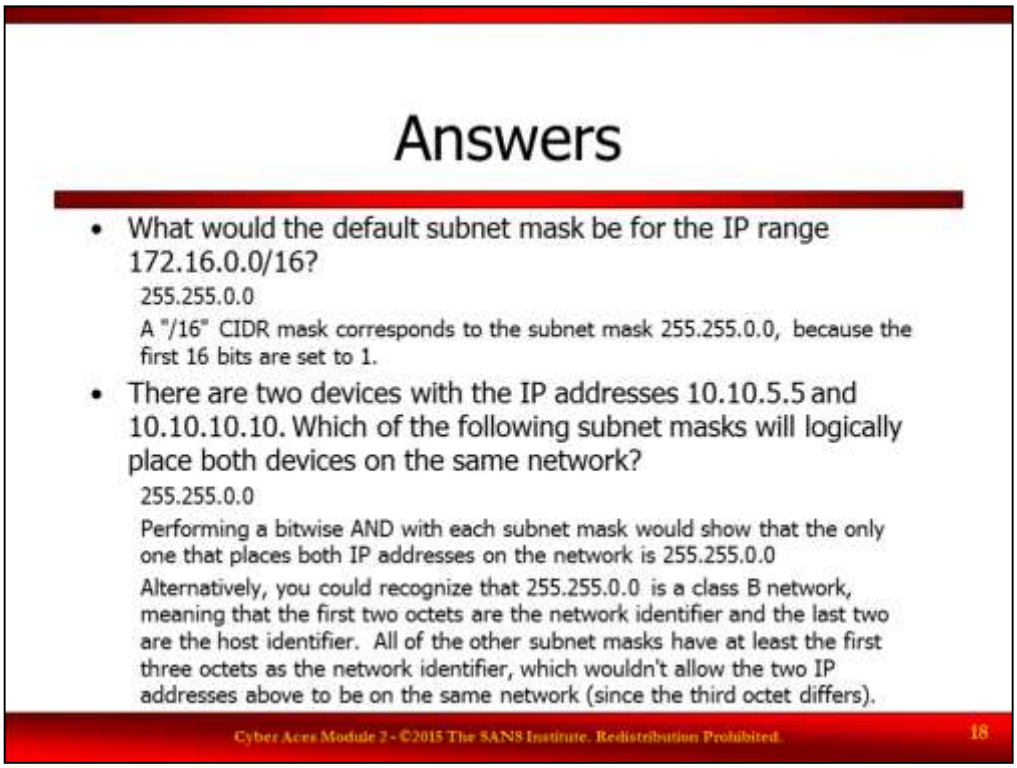
There are two devices with the IP addresses 10.10.5.5 and 10.10.10.10. Which of the following subnet masks will logically place both devices on the same network?

255.255.0.0

255.255.255.0

255.255.255.128

255.255.255.248



Answers

What would the default subnet mask be for the IP range 172.16.0.0/16?

255.255.0.0

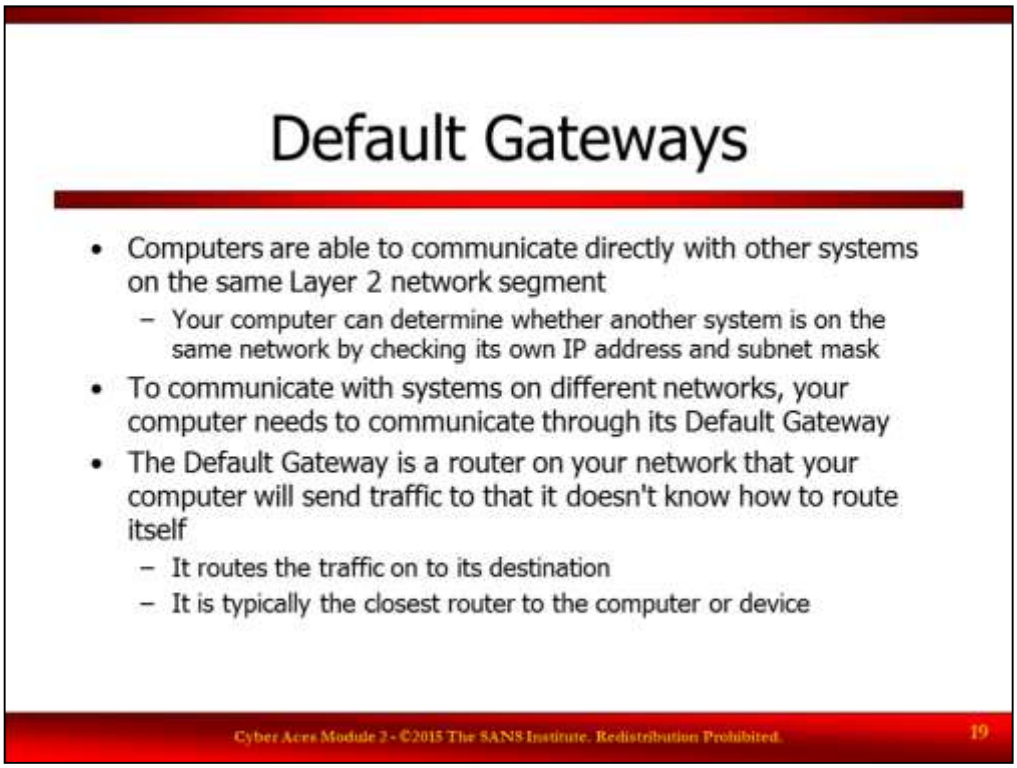
A "/16" CIDR mask corresponds to the subnet mask 255.255.0.0, because the first 16 bits are set to 1.

There are two devices with the IP addresses 10.10.5.5 and 10.10.10.10. Which of the following subnet masks will logically place both devices on the same network?

255.255.0.0

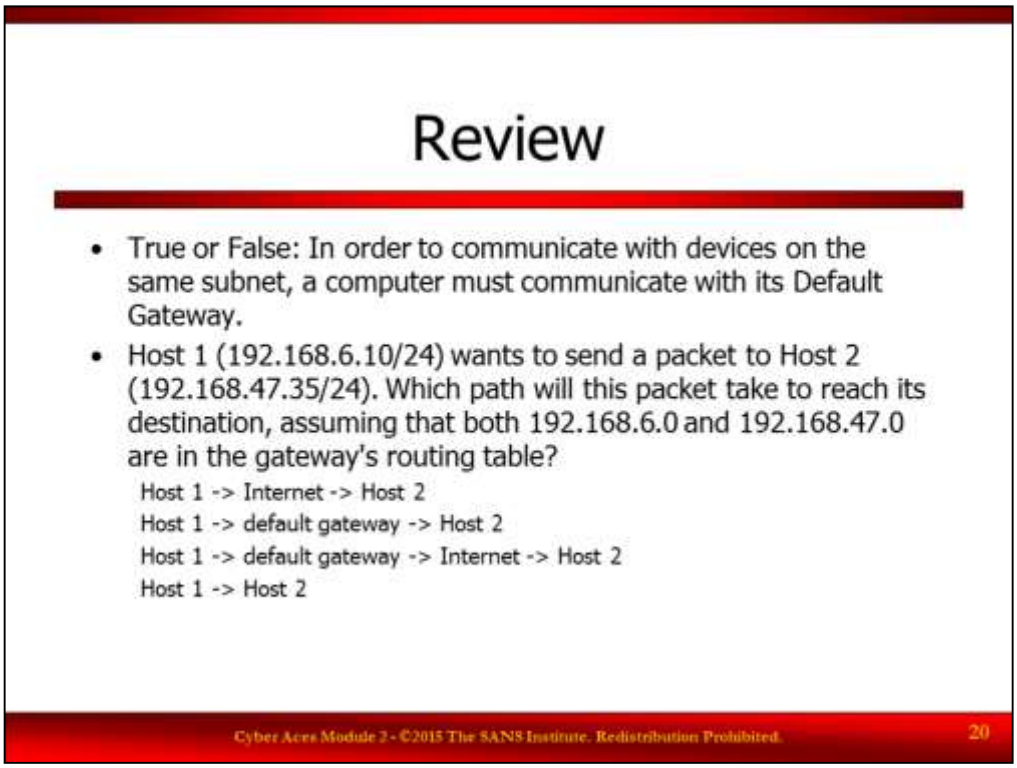
Performing a bitwise AND with each subnet mask would show that the only one that places both IP addresses on the network is 255.255.0.0

Alternatively, you could recognize that 255.255.0.0 is a class B network, meaning that the first two octets are the network identifier and the last two are the host identifier. All of the other subnet masks have at least the first three octets as the network identifier, which wouldn't allow the two IP addresses above to be on the same network (since the third octet differs).



Default Gateways

Computers are able to communicate directly with other systems on the same Layer 2 network segment. By looking at its own IP address and subnet mask, your computer knows whether or not a computer it wants to communicate with is on the same network. If it is not, the computer will send the packets to a router for delivery. The default gateway is the IP address of the router that a computer sends its network packets to if it doesn't know where else to send them. The default gateway will then route the traffic on to its destination, which will likely involve a series of other routers. The default gateway is typically the closest router to a computer or device.



Review Questions

True or False: In order to communicate with devices on the same subnet, a computer must communicate with its Default Gateway.

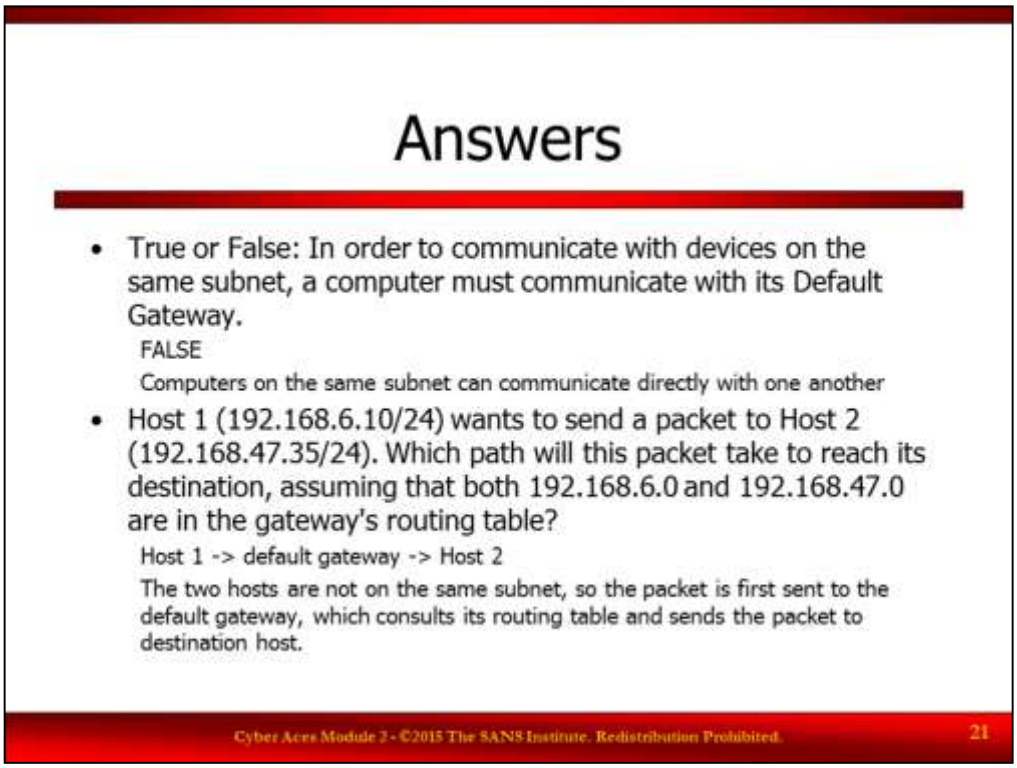
Host 1 (192.168.6.10/24) wants to send a packet to Host 2 (192.168.47.35/24). Which path will this packet take to reach its destination, assuming that both 192.168.6.0 and 192.168.47.0 are in the gateway's routing table?

Host 1 -> Internet -> Host 2

Host 1 -> default gateway -> Host 2

Host 1 -> default gateway -> Internet -> Host 2

Host 1 -> Host 2



Answers

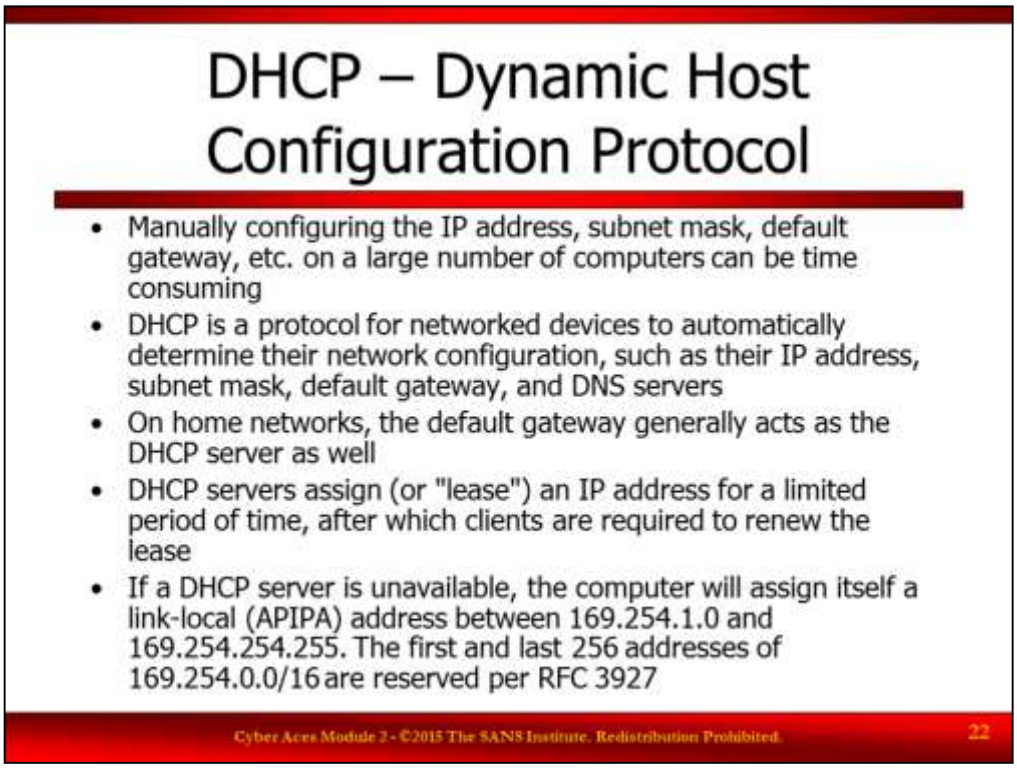
True or False: In order to communicate with devices on the same subnet, a computer must communicate with its Default Gateway.

False, computers on the same subnet can communicate directly with one another

Host 1 (192.168.6.10/24) wants to send a packet to Host 2 (192.168.47.35/24). Which path will this packet take to reach its destination, assuming that both 192.168.6.0 and 192.168.47.0 are in the gateway's routing table?

Host 1 -> default gateway -> Host 2

The two hosts are not on the same subnet, so the packet is first sent to the default gateway, which consults its routing table and sends the packet to destination host.

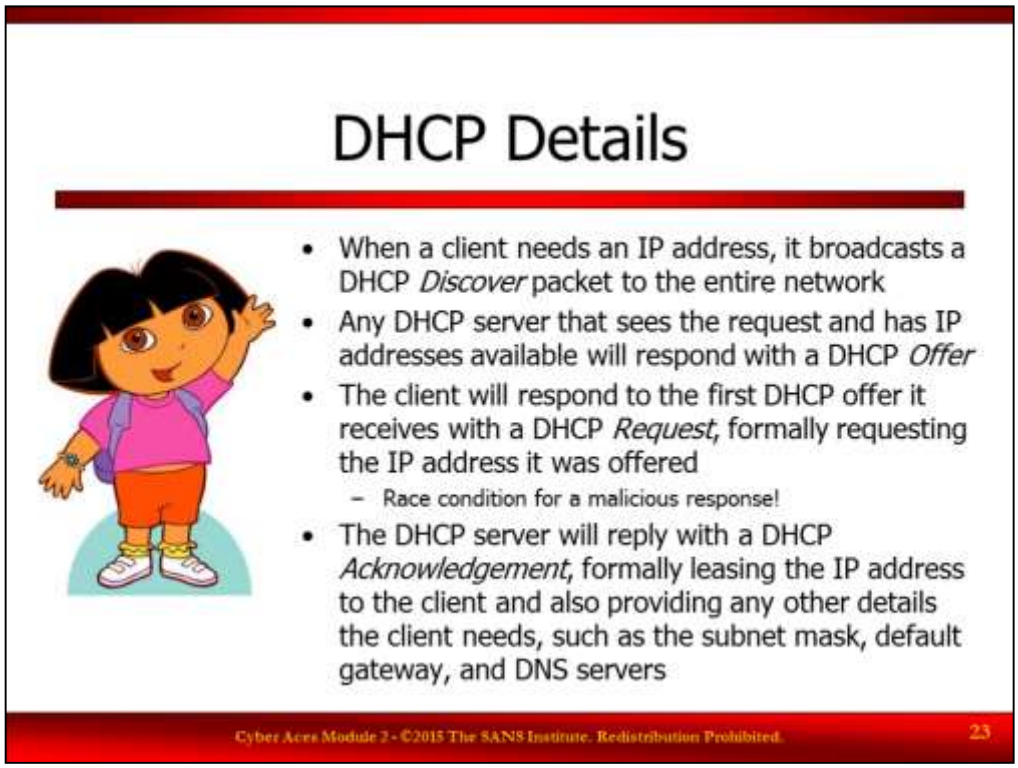


DHCP – Dynamic Host Configuration Protocol

Configuring the IP Address, Subnet Mask, Default Gateway and other networking options on more than just a few computers can be time consuming. To automate the assignment of networking information, we can use DHCP. In most home networks, DHCP services are provided by the default gateway. The DHCP server assigns an address to a device for a limited period of time called a "lease". Hosts periodically renew their IP addresses with the DHCP server, extending their lease time.

If a computer tries to obtain a DHCP address and no server responds, the computer will assign itself a link-local (APIPA) address, in the range 169.254.0.0/16. RFC 3927 defines the available addresses and it reserves the first and last 256 addresses, so a computer would randomly select an address in the range 169.254.1.0-169.254.254.255.

Note that static or pre-configured IP addresses are necessary or desirable in many situations where a consistent connection is necessary, such as network printers, DNS servers, etc. DHCP is generally only used for client computers, not for servers.

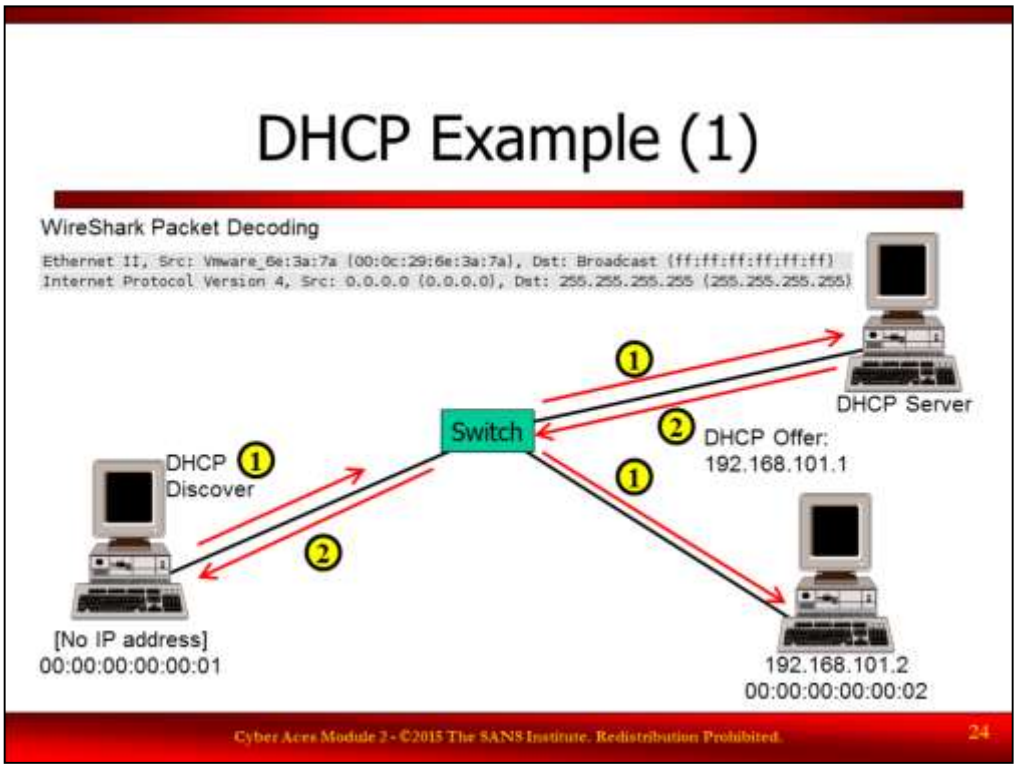


DHCP Details

When a client needs an IP address, it first broadcasts a "DHCP discover" packet to the entire network. All DHCP servers that see the request will check to see if they have any IP addresses available to lease to the client. They may also check to see if the client is allowed to request from them, or if there is a pre-configured IP address that they should assign to that client. Any servers that do have an IP available for that client will respond with a DHCP offer, which tentatively assigns that IP address to that client. The client will then accept the first DHCP offer that it receives, and reply to that particular DHCP server with a DHCP request. That DHCP server will then reply with a DHCP acknowledgement, which officially leases that IP address to that client, and also provides the client with any other network details needed (such as the subnet mask, default gateway, DNS servers, NTP servers, WINS servers, etc.).

Note that a race condition exists with the DHCP offer, as the client accepts the first one it receives. If an attacker sets up a malicious DHCP server that is able to respond faster than the legitimate DHCP server, than the attacker will be able to control the victim's network configuration. For example, the attacker could configure the client to use a malicious DNS server, or even a malicious default gateway that would allow the attacker to monitor (or even manipulate) all of the victim's traffic! Being able to respond faster than the legitimate server is fairly easy, as chances are the attacker's malicious server will be located less network hops away than the legitimate one.

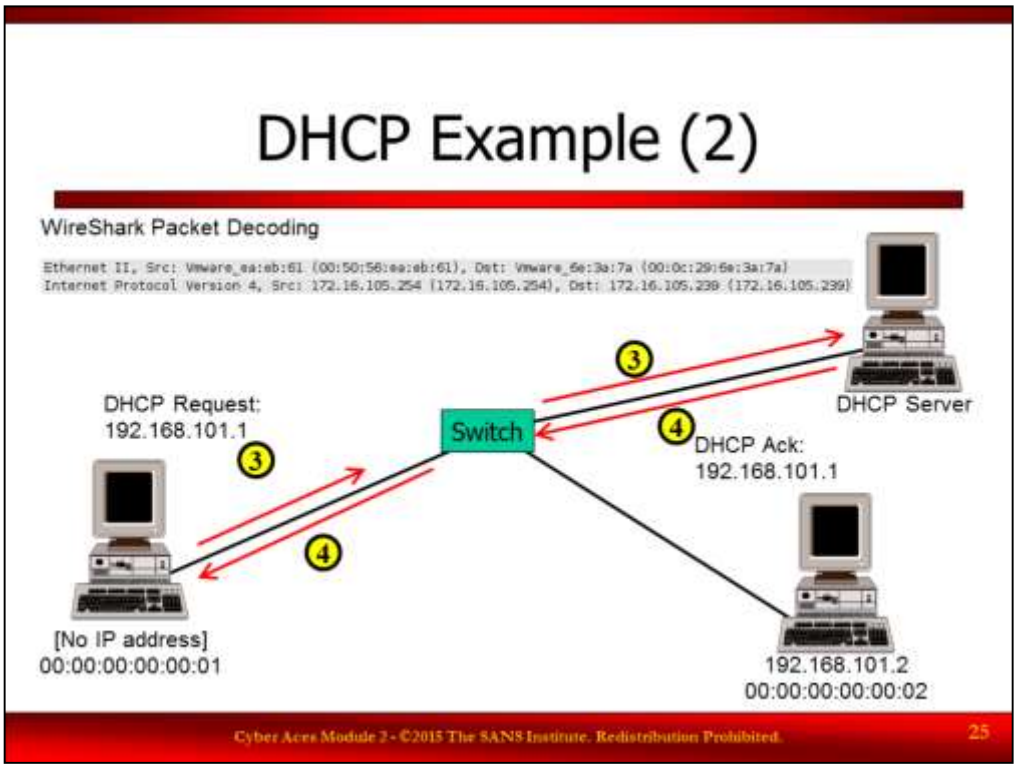
Dora the Explorer serves as a useful pneumonic device for remembering the DHCP process: **D**iscover, **O**ffer, **R**equest**, A**cknowledgment. Unfortunately, saying "Swiper, no swiping!" does not protect against rogue DHCP servers.



DHCP Example (1)

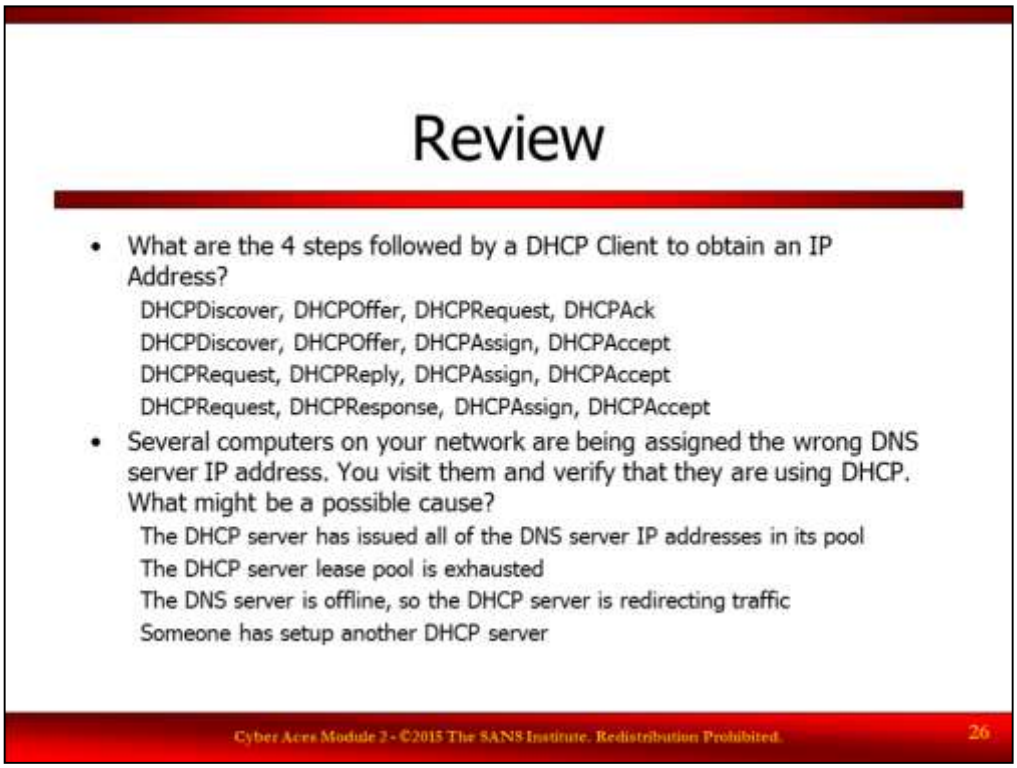
In Step 1, the machine with no IP address (00:00:00:00:00:01) sends a DHCP discover packet, which gets sent out to the entire network. In step 2, the DHCP server responds with a DHCP offer of 192.168.101.1.

Note that since the initial DHCP discover packet is sent everywhere, any other machine on the network could have responded with a DHCP offer and likely have reached the client machine first. If an attacker controlled the machine at 192.168.101.2, for example, his malicious DHCP offer likely would reach the client first, allowing him to control the client's network configuration.



DHCP Example (2)

In step 3, the client answers the DHCP offer with a DHCP request, and then the DHCP server responds with a DHCP acknowledgement, assigning the client the IP address 192.168.101.1.



Review Questions

What are the 4 steps followed by a DHCP Client to obtain an IP Address?

DHCPDiscover, DHCPOffer, DHCPRequest, DHCPAck

DHCPDiscover, DHCPOffer, DHCPAssign, DHCPAccept

DHCPRequest, DHCPReply, DHCPAssign, DHCPAccept

DHCPRequest, DHCPResponse, DHCPAssign, DHCPAccept

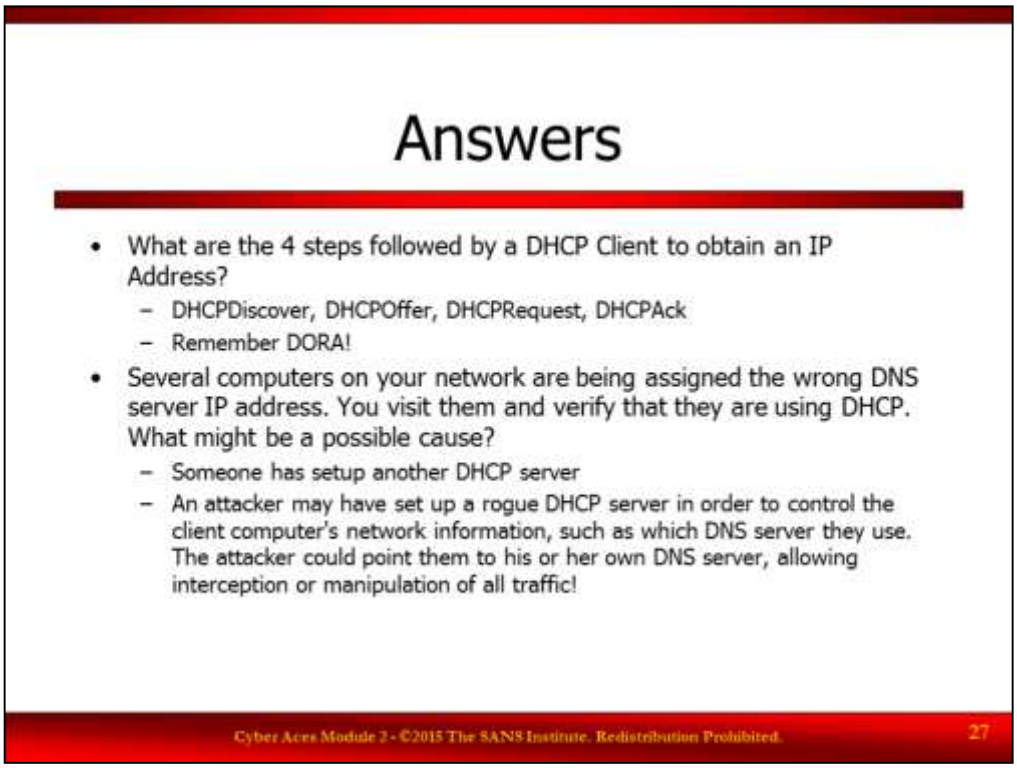
Several computers on your network are being assigned the wrong DNS server IP address. You visit them and verify that they are using DHCP. What might be a possible cause?

The DHCP server has issued all of the DNS server IP addresses in its pool

The DHCP server lease pool is exhausted

The DNS server is offline, so the DHCP server is redirecting traffic

Someone has setup another DHCP server



Answers

What are the 4 steps followed by a DHCP Client to obtain an IP Address?

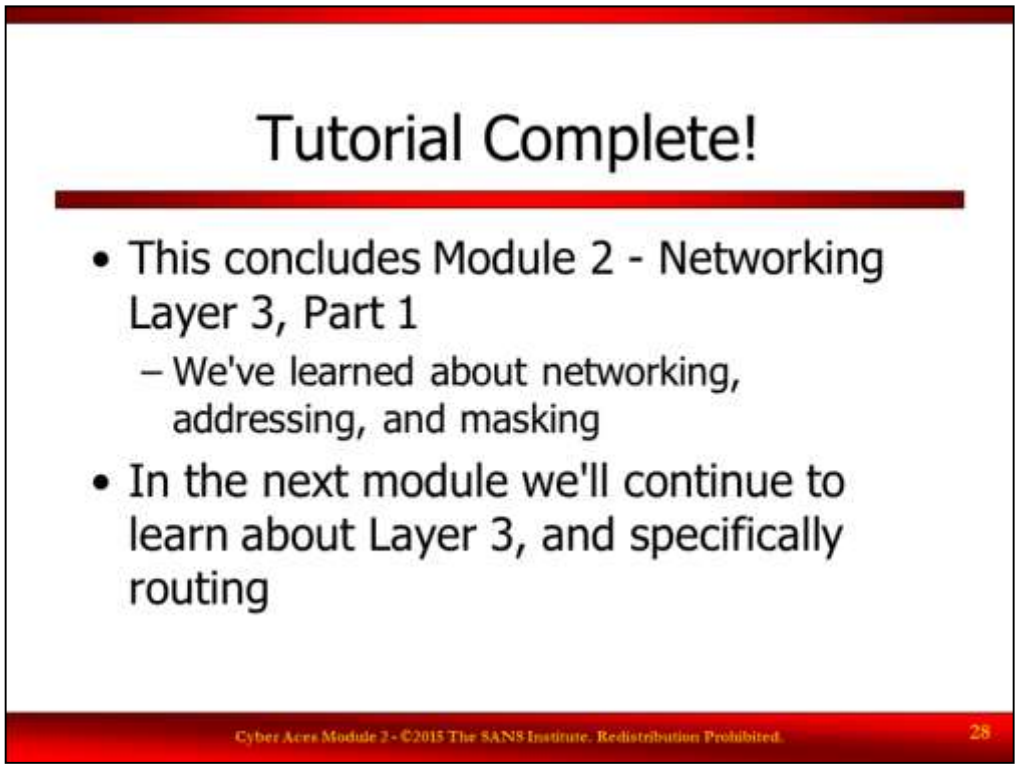
DHCPDiscover, DHCPOffer, DHCPRequest, DHCPAck

Remember DORA!

Several computers on your network are being assigned the wrong DNS server IP address. You visit them and verify that they are using DHCP. What might be a possible cause?

Someone has setup another DHCP server

An attacker may have set up a rogue DHCP server in order to control the client computer's network information, such as which DNS server they use. The attacker could point them to his or her own DNS server, allowing interception or manipulation of all traffic!



Tutorial Complete!

This concludes the discussion about Layer 3 and addressing. In the next tutorial we'll discuss the continue the discussion of Layer 3 and cover routing.