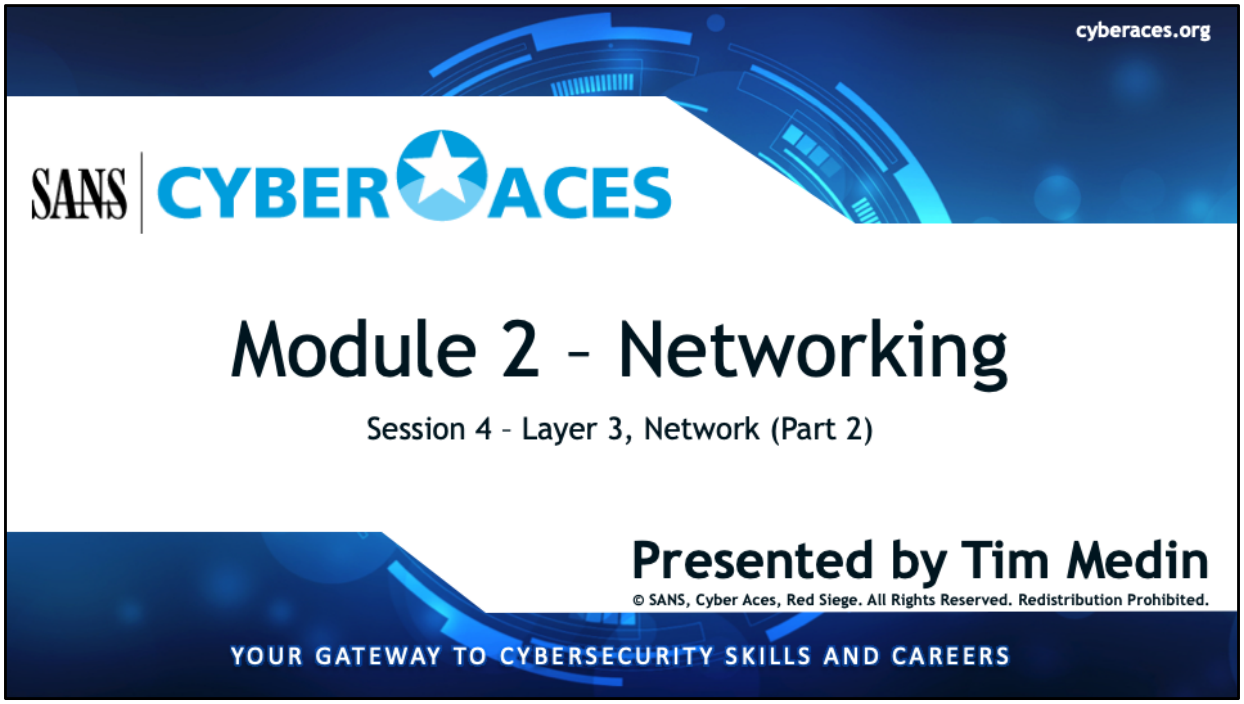
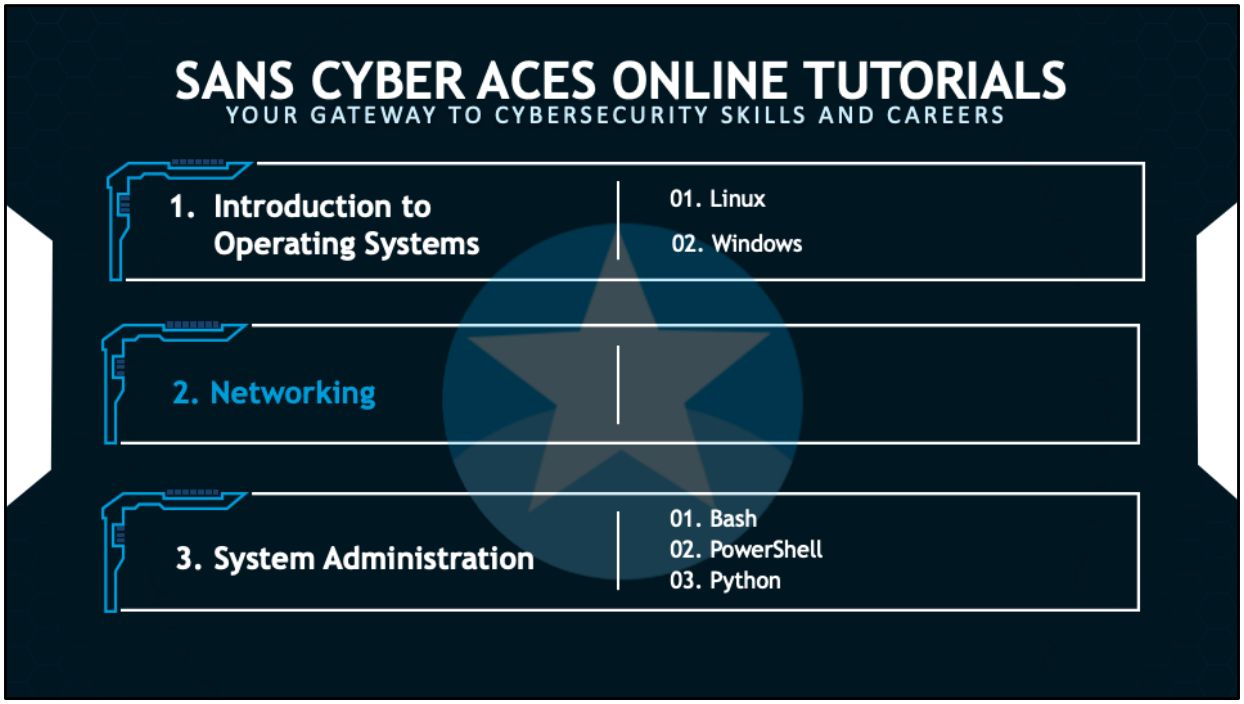


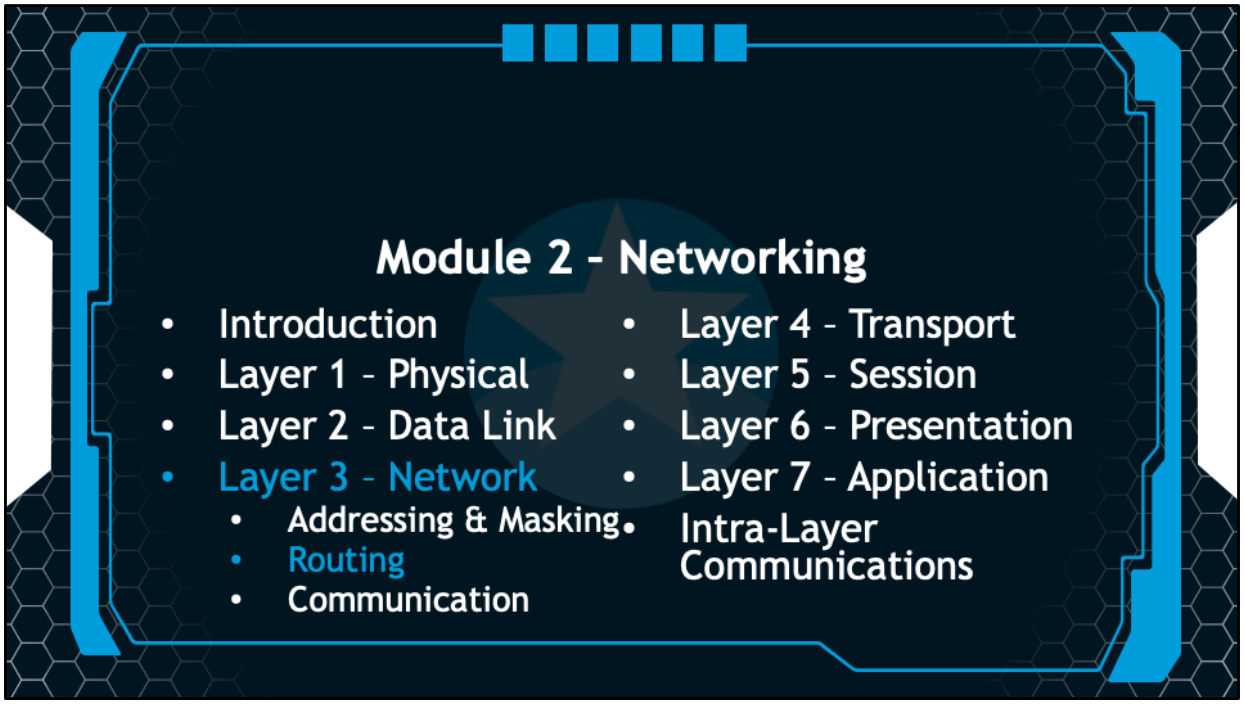
Welcome to Cyber Aces, Module 2! A firm understanding of network fundamentals is essential to being able to secure a network or attack one. This section provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective. In this session we'll continue discussion the third layer of the OSI model, the Network Layer.



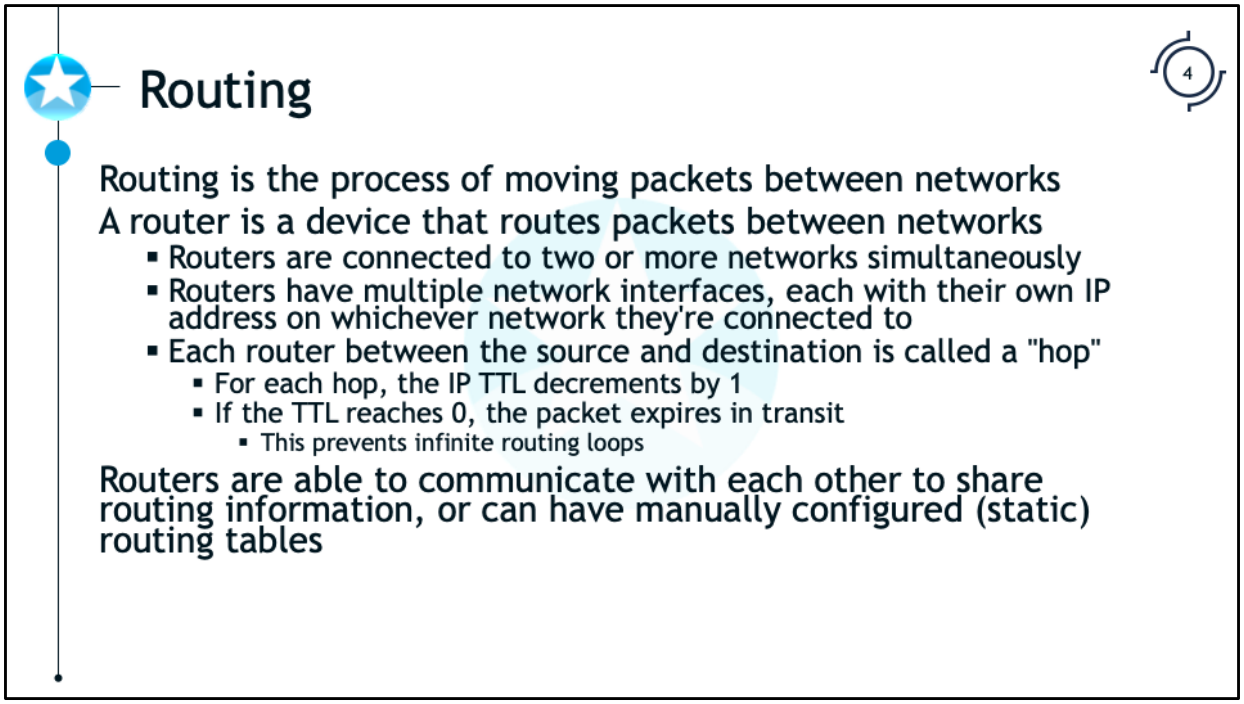
This training material was originally developed to help students, teachers, and mentors prepare for the Cyber Aces Online Competition. This module focuses on the basics of networking. This session is part of Module 2, Networking.

The three modules of Cyber Aces Online are Operating Systems, Networking, and System Administration.

For more information about the Cyber Aces program, please visit the Cyber Aces website at https://CyberAces.org/.



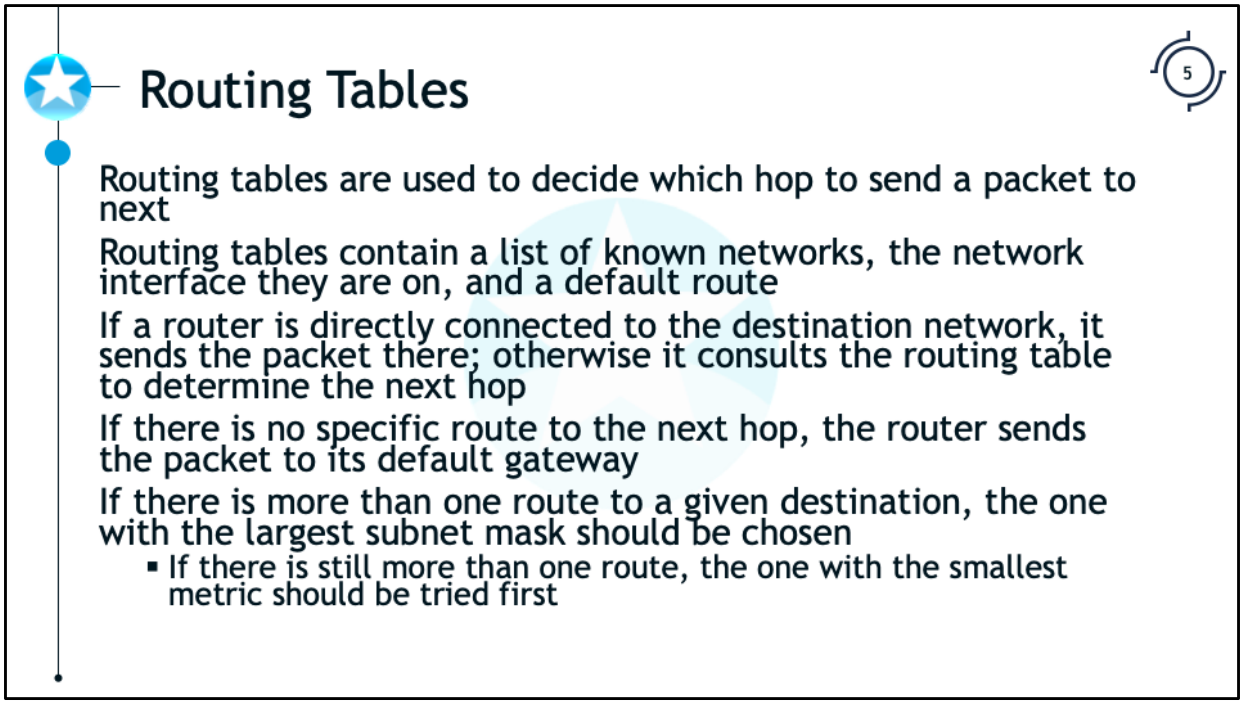
In this section, you'll learn about the Network Layer. You'll learn about IP addressing, subnet masks, default gateways, routing, NAT, and more!



In order to travel from one network to another, packets need to be routed. Routers are devices that move packets from one network to another, one hop at a time, until they reach their destination. Each router is connected to at least two networks simultaneously, and has its own IP address (and network interface) on each network that it's connected to. When discussing routing, each router on the path between the source and destination is referred to as a "hop". For example, if a packet has to travel through three routers to reach its destination, the destination could be described as being three hops away. IP packets have a TTL (Time to Live) field that specifies the maximum number of hops a packet is allowed to travel through in order to reach its destination. Every time a packet passes through a router, the TTL is reduced by one. If the TTL reaches zero, the packet expires, and the router sends an ICMP "Time Exceeded" message. This is how traceroute works; it repeatedly sends a packet to the destination, starting with a TTL of one and increasing it by one each time to discover each router on the path.

There are TTL limits on packets to ensure that traffic is not constantly sent in the unfortunate case of things such as a routing loop. If the TTL did not deprecate, the packets would still be forwarded to this day for every mistake made in the routing tables.

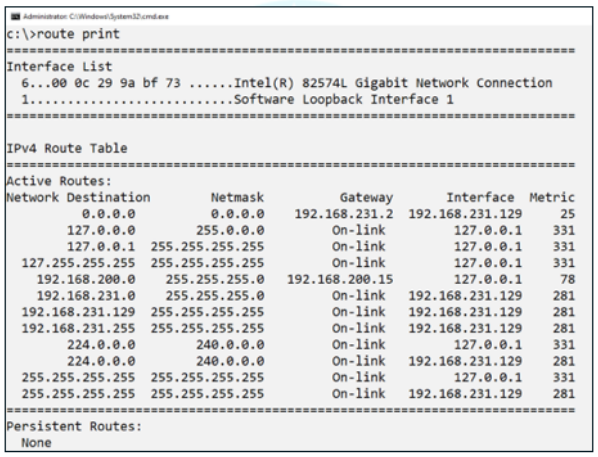
Routers are able to communicate with each other to share routing information using various protocols, or can have manually configured (static) routing tables. The source machine is also able to specify the path a packet should take, which is called source routing.



Your computer and routers decide where to transmit packets by looking at their Routing Table. A Routing table consists of a list of known networks, the network interface they are on and a default route. By consulting this table, computers and routers send the packets to the "next hop," bringing them one step closer to their destination. The "next hop" consults its routing table and passes the packets to its next hop. If a router is directly connected to the destination network, it sends the packet to that network. This continues until the packets reach their destination.

If there is no specific route to the next hop, the router sends the packet to its default gateway (which has the smallest subnet mask, since it's all zeroes). If there is more than one route to a given destination, the route with the largest subnet mask should be chosen, as that is the route that most specifically targets that destination network. If there is still more than one choice, then the route with the smallest metric should be tried first. The metric is the number of hops between the two routers.

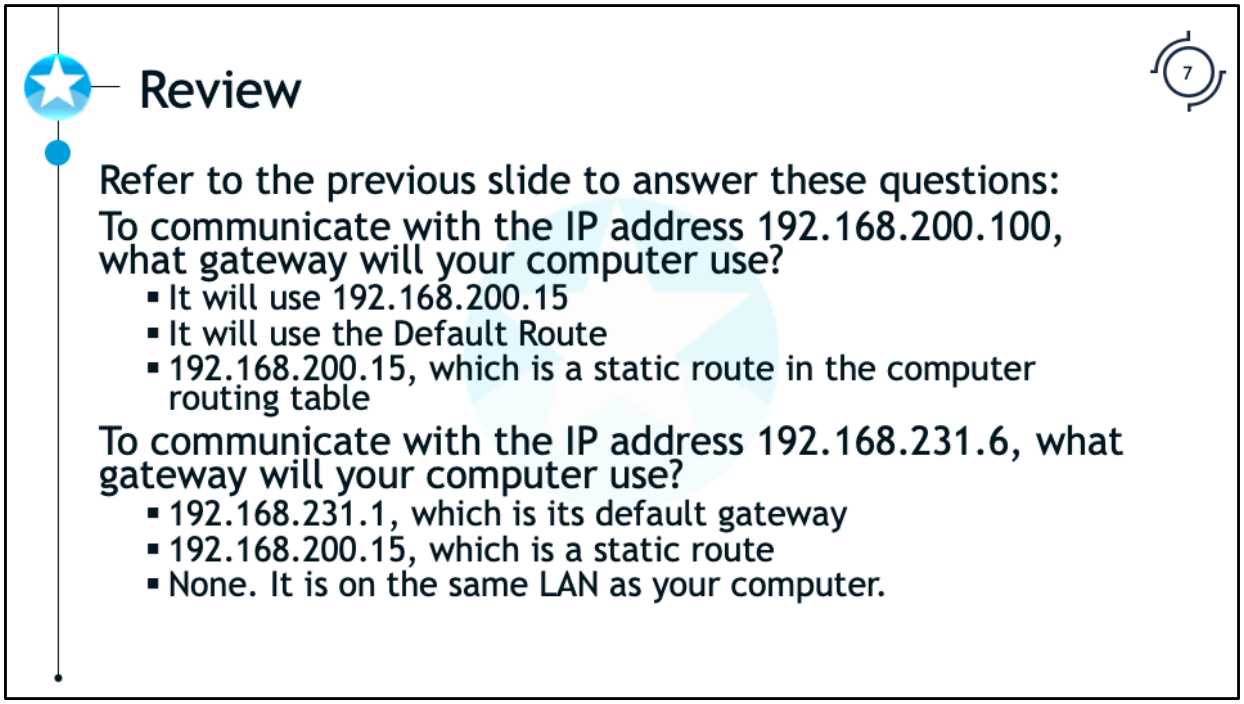
Routing Table Example



```
Administrator: C:\Windows\System32\cmd.exe
c:\>route print
===========================================================================
Interface List
  6...00 0c 29 9a bf 73 ......Intel(R) 82574L Gigabit Network Connection
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.231.2  192.168.231.129     25
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    331
    192.168.200.0    255.255.255.0   192.168.200.15         127.0.0.1     78
    192.168.231.0    255.255.255.0         On-link   192.168.231.129    281
  192.168.231.129  255.255.255.255         On-link   192.168.231.129    281
  192.168.231.255  255.255.255.255         On-link   192.168.231.129    281
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link   192.168.231.129    281
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    331
  255.255.255.255  255.255.255.255         On-link   192.168.231.129    281
===========================================================================
Persistent Routes:
  None
```

Here is an example of a routing table on a Windows machine, which can be obtained by running either "**route print**" or "**netstat -r**". The machine's current IP address is 192.168.231.129, as indicated by the fact that it is listed as the Interface address, and the route to it is for subnet mask 255.255.255.255. There are two routers listed in this routing table: the first is the default gateway, which is 192.168.231.2. The second is at 192.168.200.15, which is configured to be the destination for packets heading to the network 192.168.200.0/24.



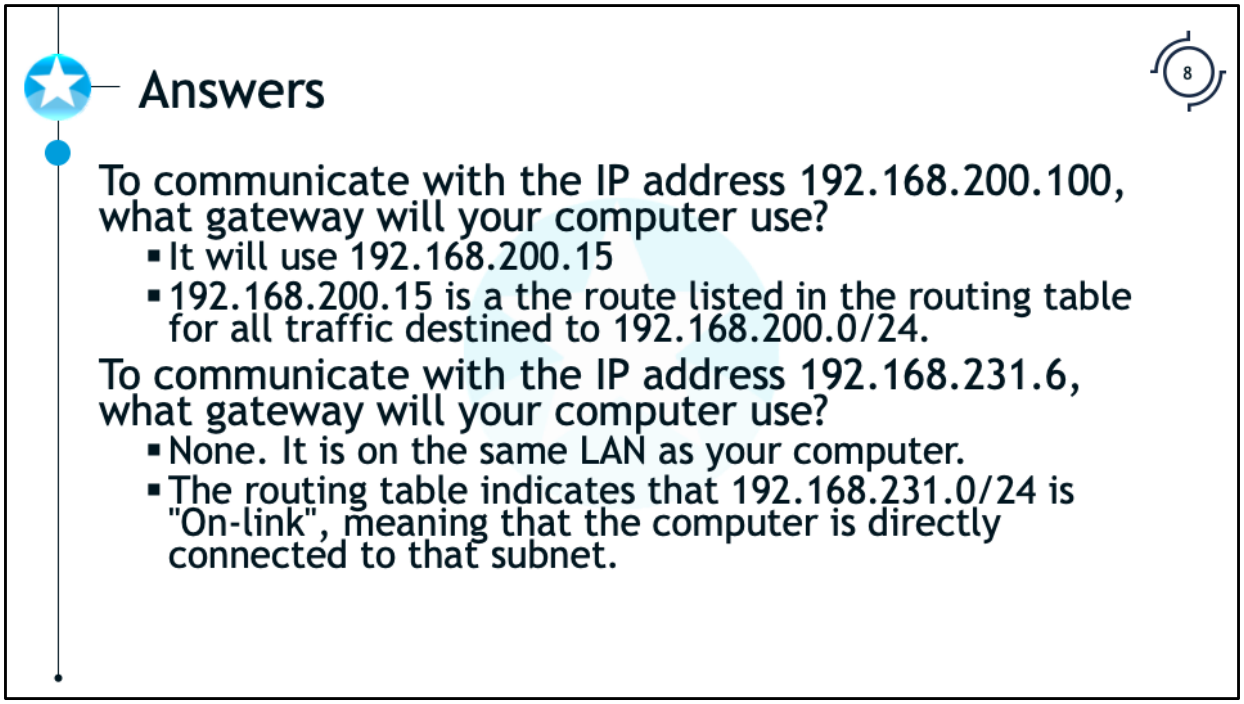
Refer to the previous slide to answer these questions:

To communicate with the IP address 192.168.200.100, what gateway will your computer use?

- It will use 192.168.200.15
- It will use the Default Route
- 192.168.200.25, which is a static route in the computer routing table

To communicate with the IP address 192.168.100.6, what gateway will your computer use?

- 192.168.100.1, which is its default gateway
- 192.168.100.5, which is a static route
- None. It is on the same LAN as your computer.



To communicate with the IP address 192.168.200.100, what gateway will your computer use?

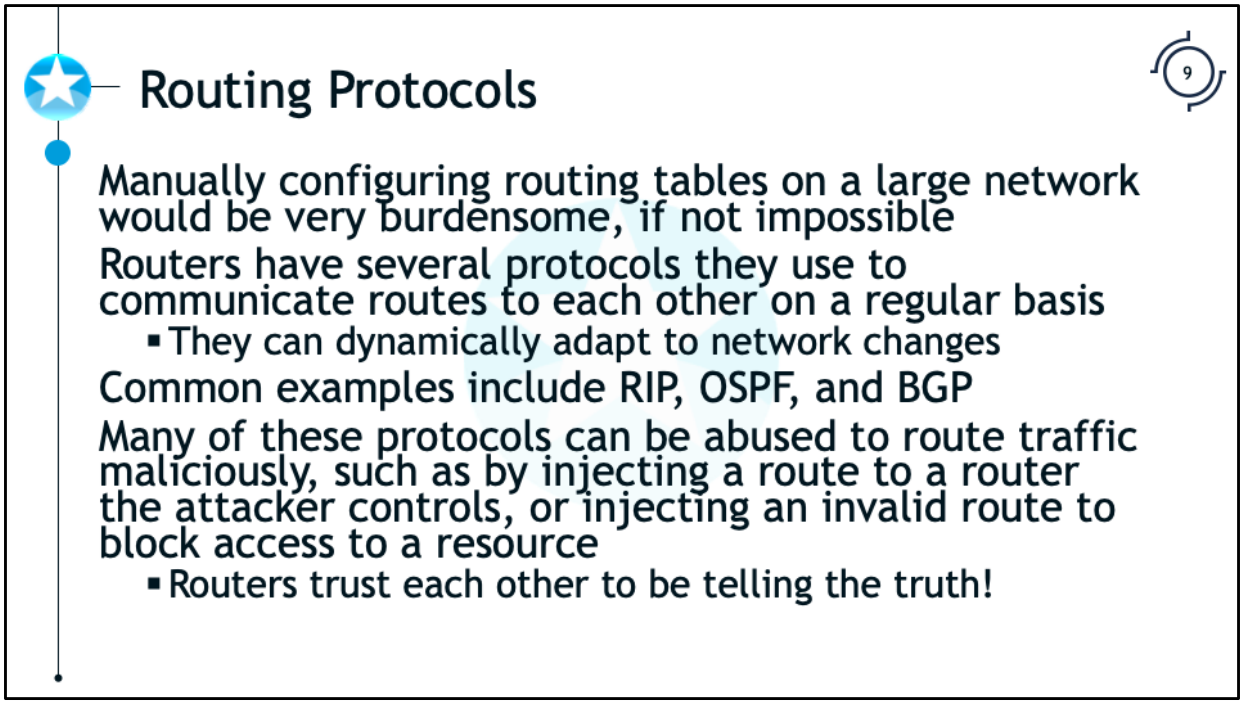
It will use 192.168.200.15

192.168.200.15 is the route listed in the routing table for all traffic destined to 192.168.200.0/24.

To communicate with the IP address 192.168.100.6, what gateway will your computer use?

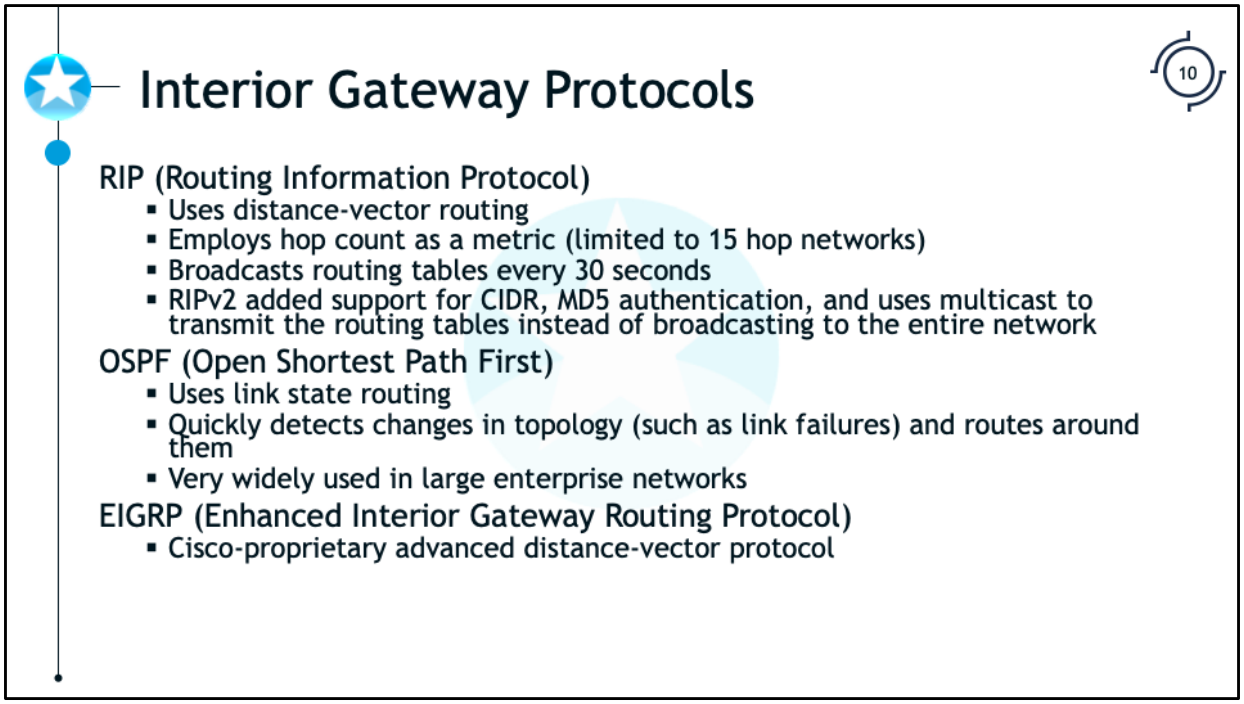
None. It is on the same LAN as your computer.

The routing table indicates that 192.168.100.0/24 is "On-link", meaning that the computer is directly connected to that subnet.



An Internet router has tables defining which interface it should use to communicate with various networks. The networks in these tables are constantly changing, and manually populating these tables would be very slow. To solve this problem, routers on the Internet have several protocols they use to exchange lists of networks and how to reach them, as well as which paths are the most efficient. These protocols are referred to as Routing Protocols. There are many different routing protocols such as RIP, OSPF, EIGRP, BGP, and others. This is the world in which most networking professionals live, but a security professional should have at least a basic understanding of the terms and techniques used by these protocols, if not the specifics of the protocols.

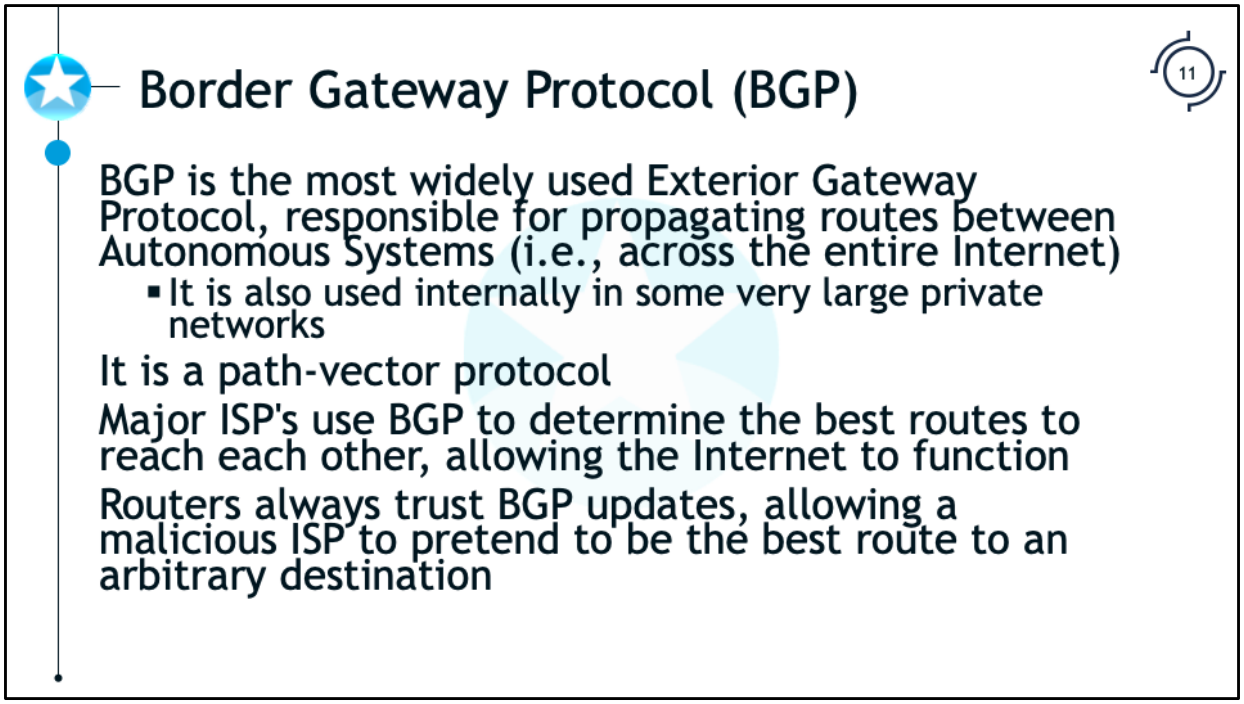
Many of these protocols can be abused to route traffic maliciously, such as by injecting a route to a router the attacker controls, or injecting an invalid route to block access to a resource. In fact, this has happened even on the Internet itself, such as in 2008 when Pakistan accidentally propagated a routing rule worldwide that effectively blocked access to YouTube. Researchers also demonstrated this technique at DefCon in 2008 by routing all traffic to the conference network in Las Vegas through their own routers in New York.



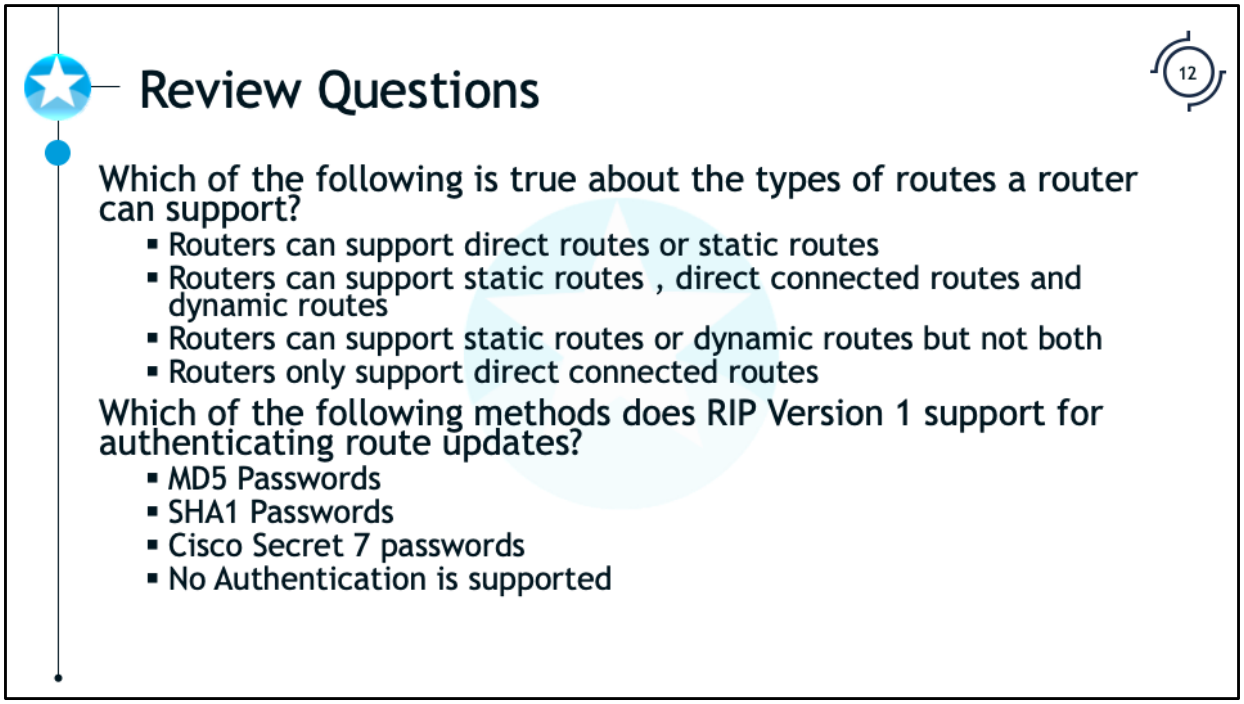
Interior Gateway Protocols are routing protocols used to route traffic within a single autonomous system (routing domain). Two common interior gateway protocols are RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). RIP uses distance-vector routing, employing the hop count as a metric. However, it is limited to networks with no more than 15 hops between any two points, as it considers anything higher than that to be a routing loop. RIP broadcasts the routing tables every 30 seconds, which can cause a large amount of traffic to be generated. However, RIP requires a minimum amount of configuration, making it easy to deploy. RIPv2 added support for CIDR, and also uses multicast to transmit the routing table updates instead of simply broadcasting them.

OSPF uses link state routing. It is able to quickly detect changes to the network topology, such as link failures, and route around them accordingly. OSPF is very widely used in large enterprise networks.

EIGRP (Enhanced Interior Gateway Routing Protocol) is a Cisco-proprietary routing protocol. While it is commonly described as being a hybrid protocol, it is technically a very advanced distance-vector protocol.



Border Gateway Protocol, or BGP, is the most widely used Exterior Gateway Protocol, which is responsible for propagating routes between all of the Autonomous Systems (individual routing domains) on the Internet. It is also used internally in some very large private networks. BGP is classified as a path-vector protocol. All major ISP's on the Internet use BGP to determine the best routes to each other, which is what allows the Internet to function in a decentralized manner. Routers always trust BGP updates to be the truth, which allows a malicious ISP to send BGP updates announcing that it is the best route to an arbitrary destination, even if it isn't. This is how Pakistan accidentally blocked access to YouTube worldwide in 2008 (while trying to block it just for its own citizens), and how the researchers at DefCon were able to route all traffic heading to the conference network (in Las Vegas) through their own routers in New York.

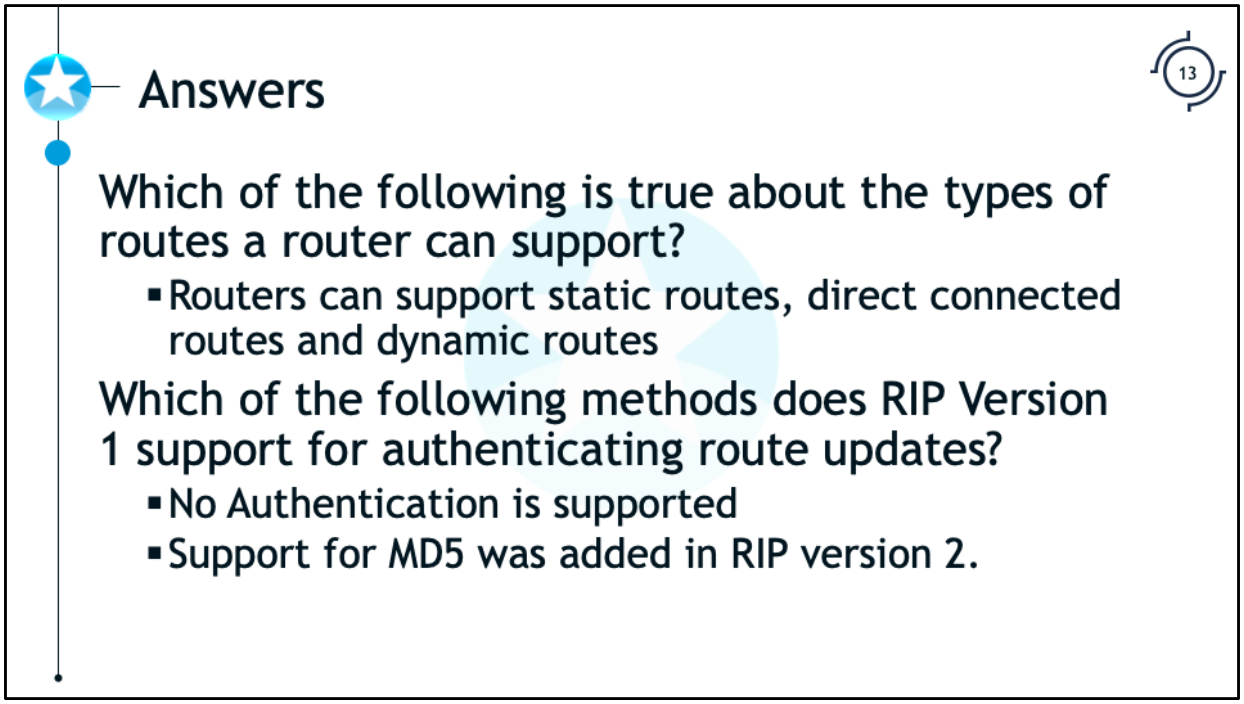


Which of the following is true about the types of routes a router can support?

- Routers can support direct routes or static routes
- Routers can support static routes , direct connected routes and dynamic routes
- Routers can support static routes or dynamic routes but not both
- Routers only support direct connected routes

Which of the following methods does RIP Version 1 support for authenticating route updates?

- MD5 Passwords
- SHA1 Passwords
- Cisco Secret 7 passwords
- No Authentication is supported



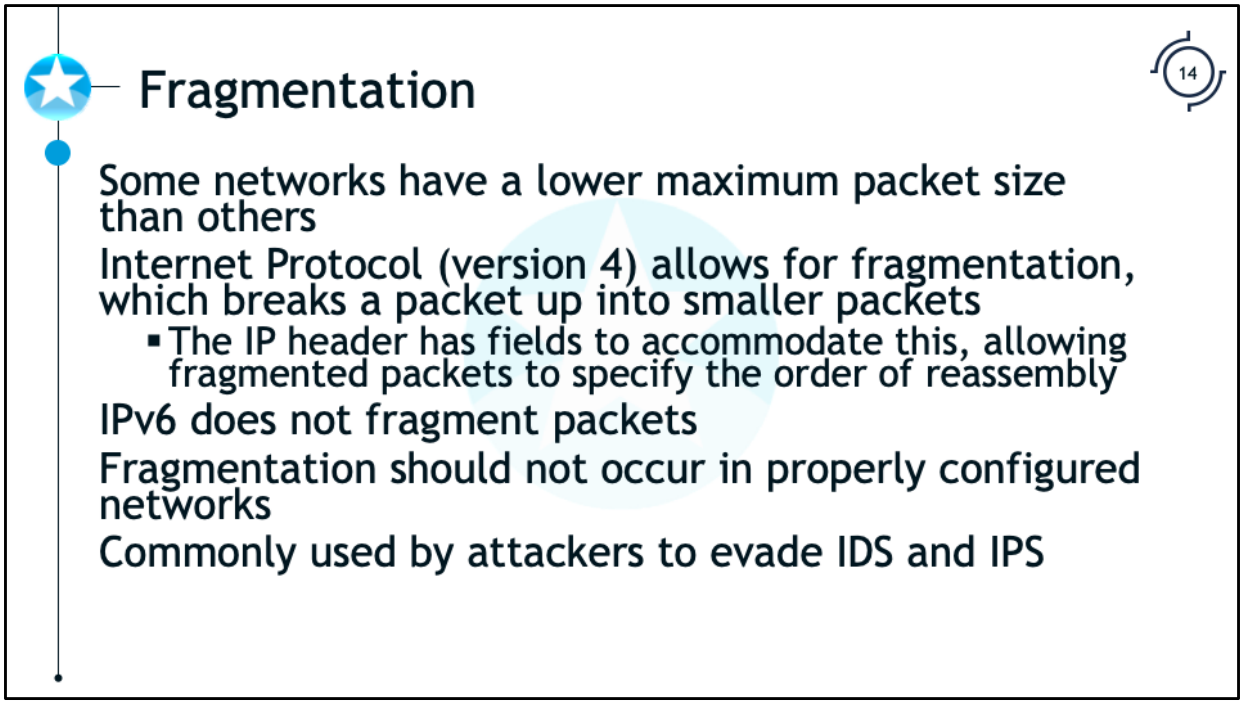
Which of the following is true about the types of routes a router can support?

Routers can support static routes, direct connected routes and dynamic routes

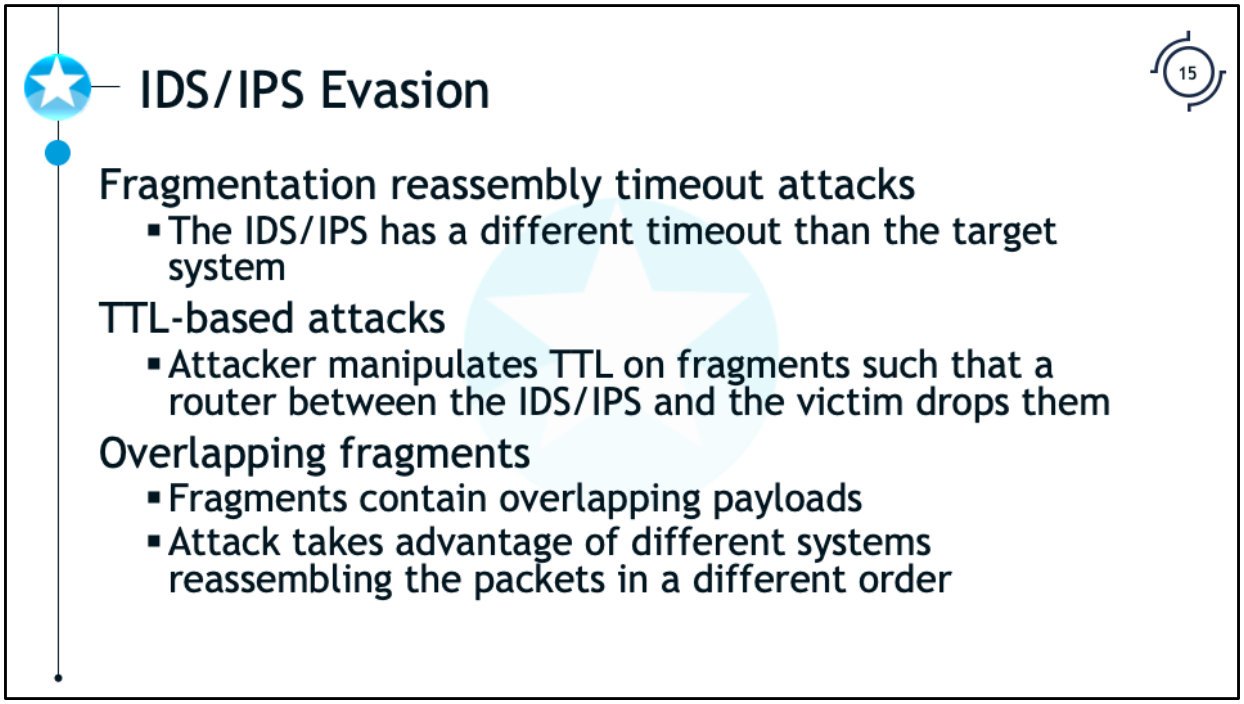
Which of the following methods does RIP Version 1 support for authenticating route updates?

No Authentication is supported

Support for MD5 was added in RIP version 2.



As a packet travels from a source to destination, it may travel across networks that support different maximum packet sizes. If a network router has a packet that is 1500 bytes long and the destination interface for that packet can only accept packet that is 1400 bytes, fragmentation will occur. Fragmentation is when an IP packet is broken up into two or more smaller packets. When fragmentation occurs, special fields in the IP header are set so the packets can be reassembled at the destination. Normally, hosts will determine the "MTU" or Maximum Transmission Unit when they establish the connection to the remote destination. As a result, fragmentation shouldn't occur in a properly configured network. However, attackers use packet fragmentation to avoid Intrusion Detection and Intrusion Prevention Systems.

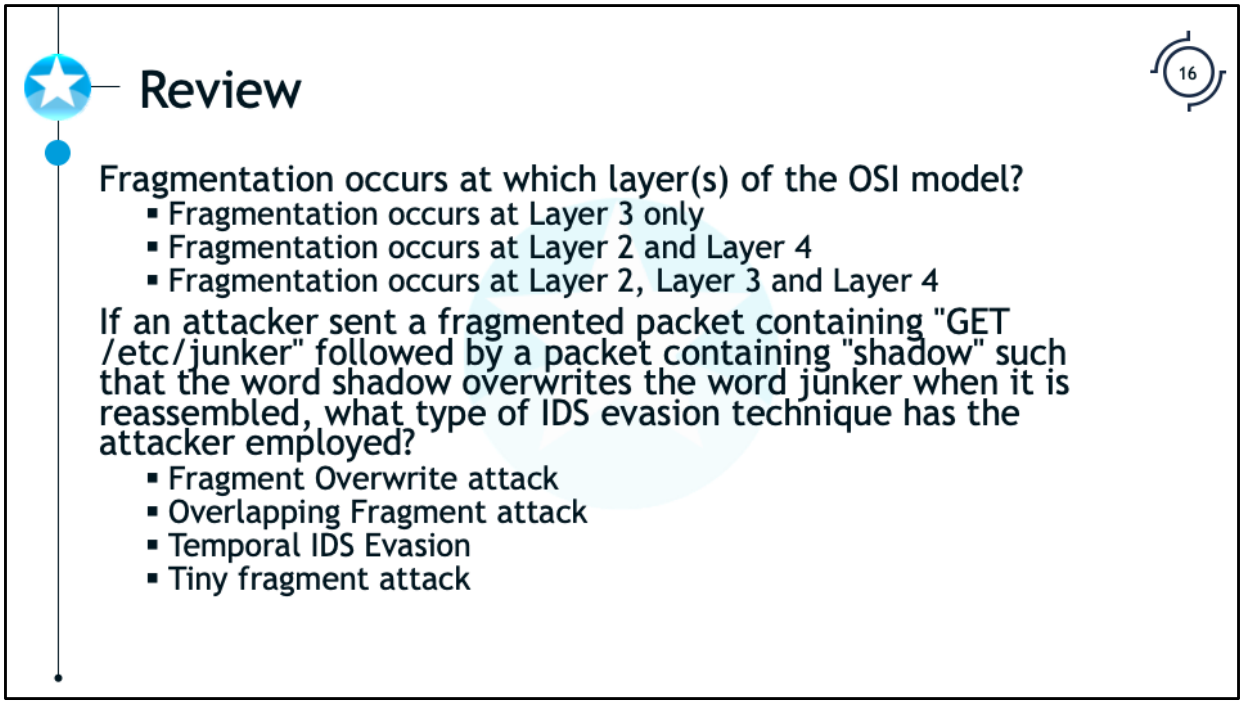


Here are some examples of common IDS/IPS evasion techniques:

Fragmentation reassembly timeout attacks take advantage of the IDS/IPS having a different reassembly timeout than the target system. If the IDS/IPS has a lesser timeout than the target system, the attacker can send the packets far enough apart for the IDS/IPS to timeout on the earlier ones, but still within the window for the target system to receive and successfully reassemble them. Conversely, if the IDS/IPS has a longer timeout than the target system, the attacker can send later fragments first with a false payload, wait for them to timeout on the victim, and then send the earlier fragments followed by the later fragments with the correct payload.

TTL-based attacks take advantage of a router existing between the IDS/IPS and the target system. The attacker manipulates the TTL on selected fragments such that the IDS/IPS will process them but the router will drop them before they reach the victim. Then, the attacker sends further fragments that the IDS/IPS won't process because it thinks it already has, but that will get through to the victim.

Overlapping fragment attacks take advantage of the fact that IP fragment payloads are able to overlap with one another, and different systems reassemble the overlapping payloads differently. If the IDS/IPS and the target system reassemble the packets differently, it is possible to bypass the IDS/IPS rules.

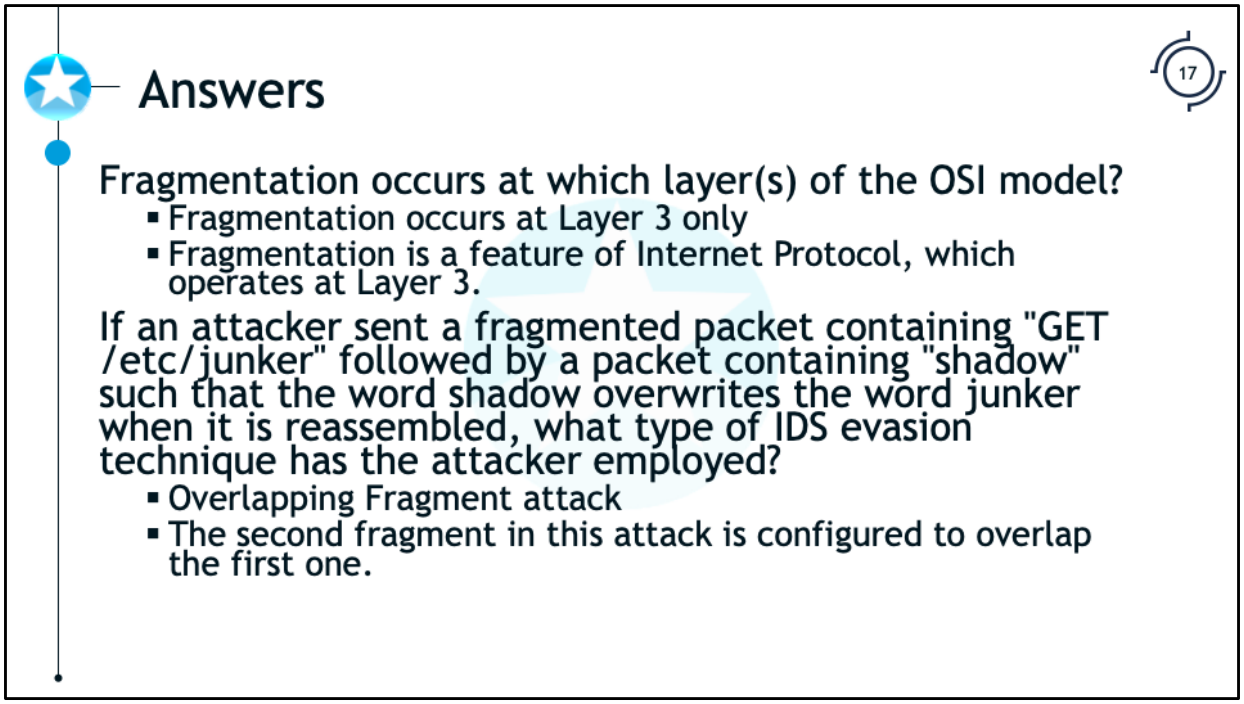


Fragmentation occurs at which layer(s) of the OSI model?

- Fragmentation occurs at Layer 3 only
- Fragmentation occurs at Layer 2 and Layer 4
- Fragmentation occurs at Layer 2, Layer 3 and Layer 4

If an attacker sent a fragmented packet containing "GET /etc/junker" followed by a packet containing "shadow" such that the word shadow overwrites the word junker when it is reassembled, what type of IDS evasion technique has the attacker employed?

- Fragment Overwrite attack
- Overlapping Fragment attack
- Temporal IDS Evasion
- Tiny fragment attack



Fragmentation occurs at which layer(s) of the OSI model?

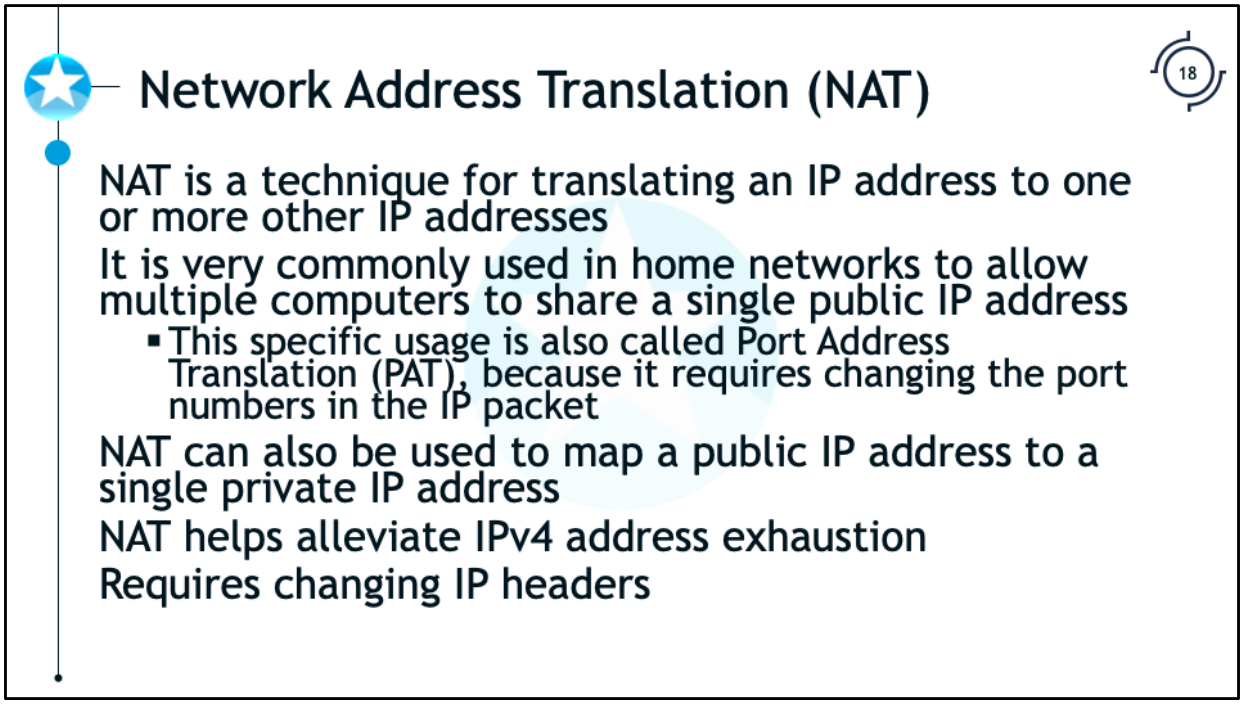
Fragmentation occurs at Layer 3 only

Fragmentation is a feature of Internet Protocol, which operates at Layer 3.

If an attacker sent a fragmented packet containing "GET /etc/junker" followed by a packet containing "shadow" such that the word shadow overwrites the word junker when it is reassembled, what type of IDS evasion technique has the attacker employed?

Overlapping Fragment attack

The second fragment in this attack is configured to overlap the first one.

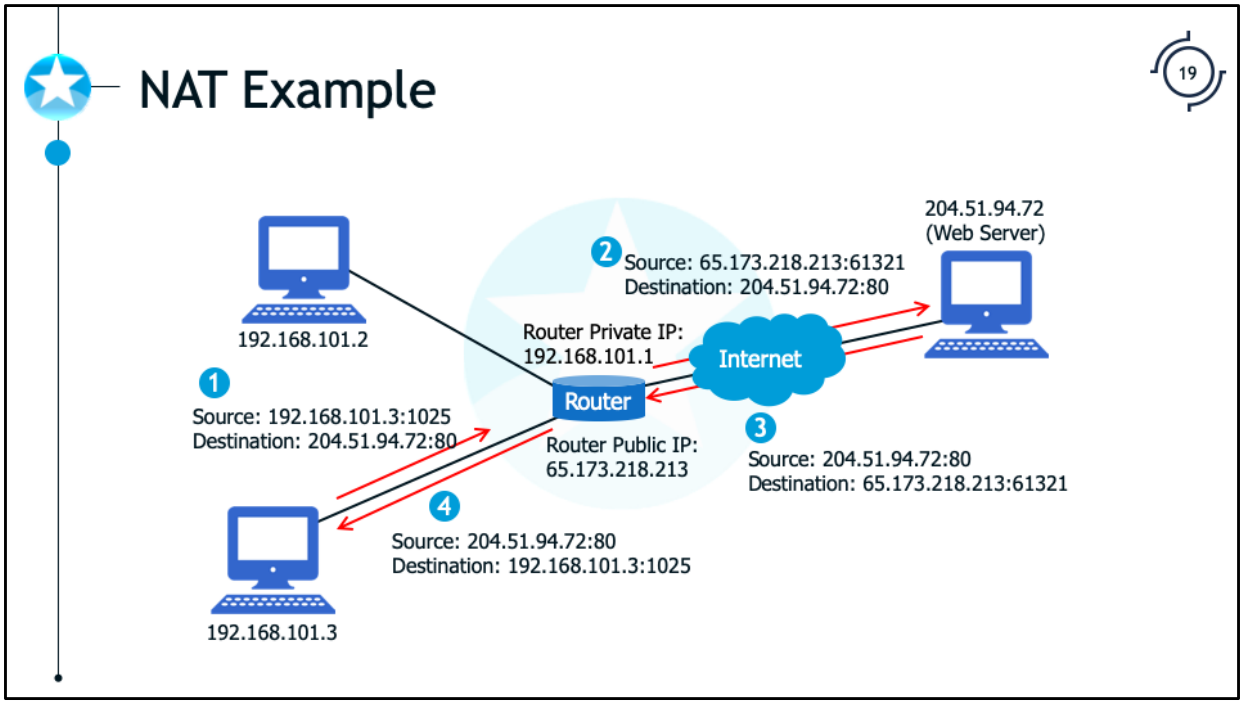


Typically, on your Local Area Network you are assigned a Private IP address. When your traffic leaves your LAN, your router will translate it to a Public Internet Address. This is known as Network Address Translation or NAT. Internet routers can map several thousand computers behind a single public IP address using NAT. This form of NAT, also known as Port Address Translation (PAT) or IP masquerading, is very commonly used on home networks.

NAT can also be used to map a single private IP address to a single public IP address, or to map a private IP address to one of a set of public IP addresses (allowing multiple hosts to share a limited set of public IP addresses). NAT is also used to merge two private IP networks with conflicting IP addresses, allowing them to share resources without needing to renumber the entire network. Note that when a computer with a private IP address connects through NAT to a resource on the public Internet, the Internet server only sees the public IP address, not the client's private IP address.

One of NAT's main purposes is to alleviate IPv4 address exhaustion. By allowing an entire network to share a single Internet-accessible IP address, not nearly as many IP addresses need to be allocated.

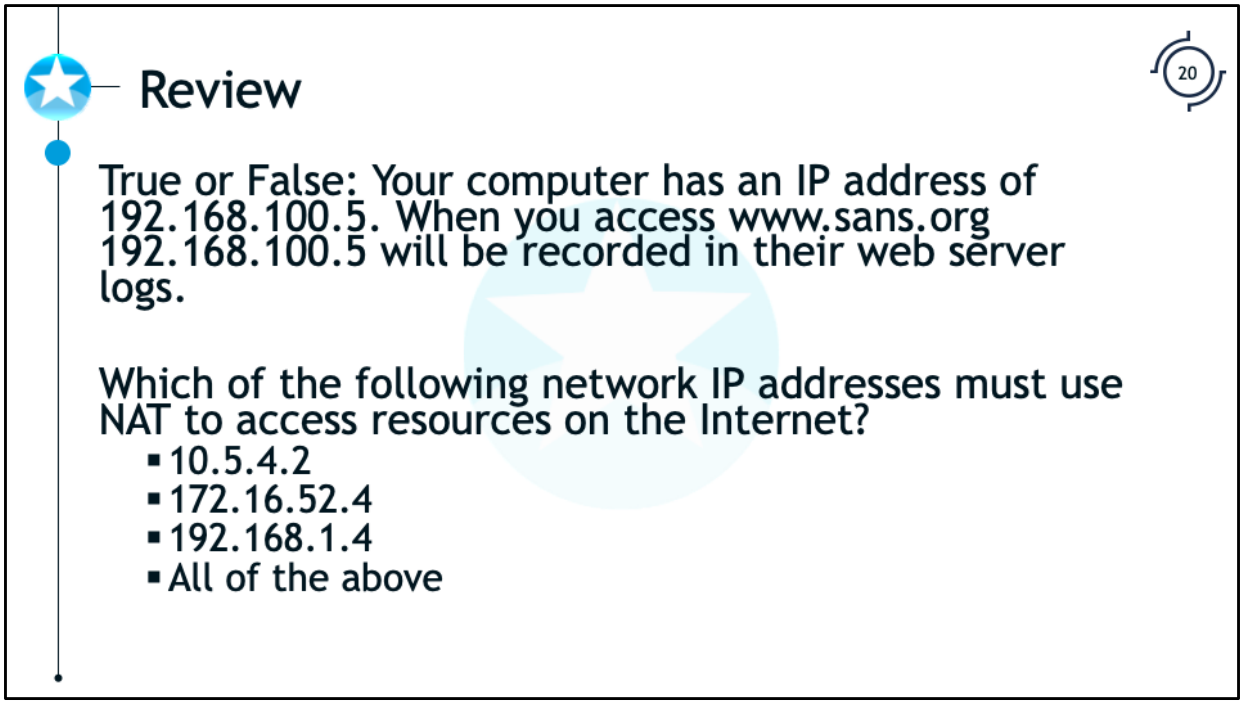
The major disadvantage of NAT is that it breaks end-to-end connectivity of devices on a network. A client on a public network cannot connect directly to a client on a private NAT'ed network; it has to connect to the NAT router, which then forwards packets to the appropriate client. In order to use NAT, the router needs to alter various fields of the IP header to accommodate the forwarding that is taking place. The router has to maintain a table mapping which private IP address to route a packet to and change the address fields in the packet accordingly. This is particularly true for PAT, which also has to change the source and destination ports of packets when forwarding.



The above diagram represents a typical home network using NAT (specifically, PAT/IP masquerading). The computers on the home network (left) are on the private IP range 192.168.101.0/24, and are connected to the Internet through a NAT-enabled router. The router's private (internal) IP address is 192.168.101.1, and the router's public (external) IP address is 65.173.218.213. Let's say that the computer at 192.168.101.3 would like to fetch a web page from the web server at 204.51.94.72.

In Step 1, the client at 192.168.101.3 sends a packet to 204.51.94.72, port 80 (the TCP port for HTTP). In Step 2, the client's NAT-enabled router changes the source address to its public IP address (65.173.218.213), and changes the port number to one that is available on its public interface. The router keeps a connection table that keeps track of which port numbers are associated with each host on the internal network, so that it knows where to route responses. The router also has to re-compute the packet's checksums, since it changed various header fields in the packet. The router then passes the packet on to the Internet, where it gets routed to the destination web server.

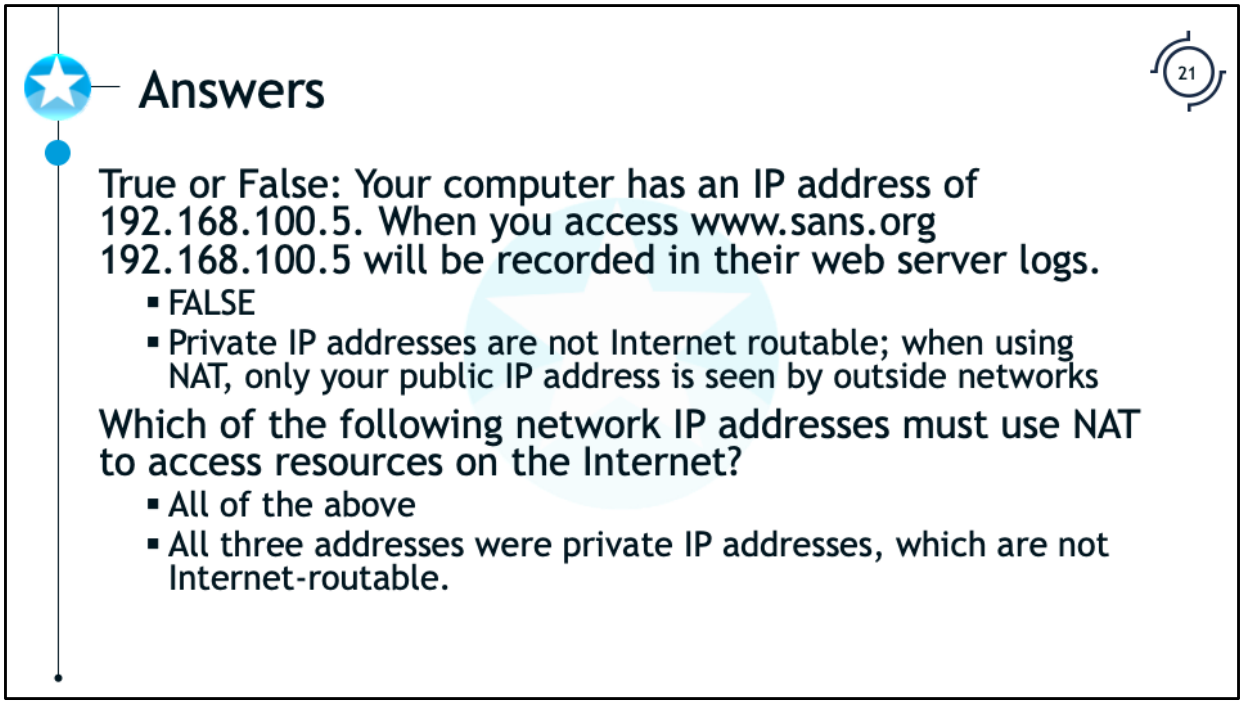
In Step 3, the web server responds to the request with the web page, sending it to the public IP address of the router (65.173.218.213) at the same port number the request originated from (61321). The packet gets routed across the Internet and ultimately arrives at the client's router. In Step 4, the router checks its connection table to determine which host and port to send the packet to based on the port number it received the packet on, and then rewrites the packet headers and sends it to the final destination, 192.168.101.3, at the same port the request originated from (port 1025). The client machine is none the wiser!



True or False: Your computer has an IP address of 192.168.100.5. When you access www.sans.org 192.168.100.5 will be recorded in their web server logs.

Which of the following network IP addresses must use NAT to access resources on the Internet?

10.5.4.2
172.16.52.4
192.168.1.4
All of the above



True or False: Your computer has an IP address of 192.168.100.5. When you access www.sans.org 192.168.100.5 will be recorded in their web server logs.

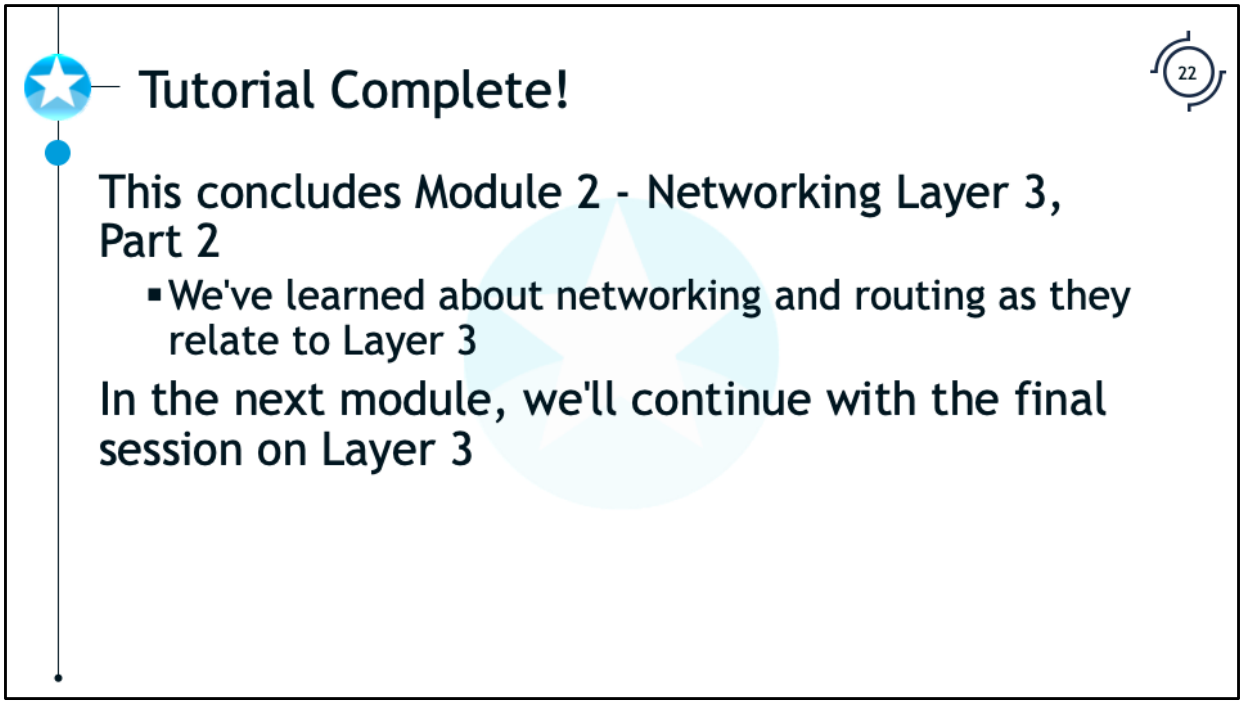
FALSE

Private IP addresses are not Internet routable; when using NAT, only your public IP address is seen by outside networks

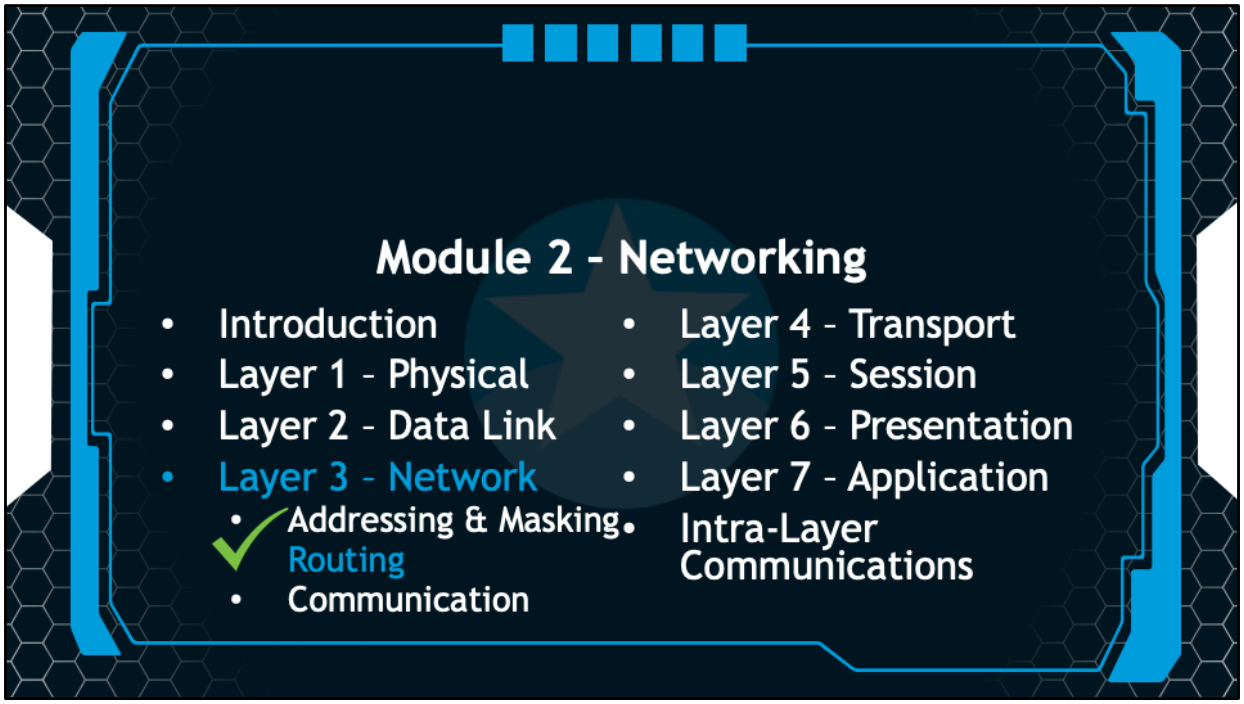
Which of the following network IP addresses must use NAT to access resources on the Internet?

All of the above

All three addresses were private IP addresses, which are not Internet-routable.



This concludes the discussion about Layer 3 and routing. In the next tutorial we'll finish the discussion of Layer 3.



In the next session we will concluded our discussion of Layer 3, the Network Layer.