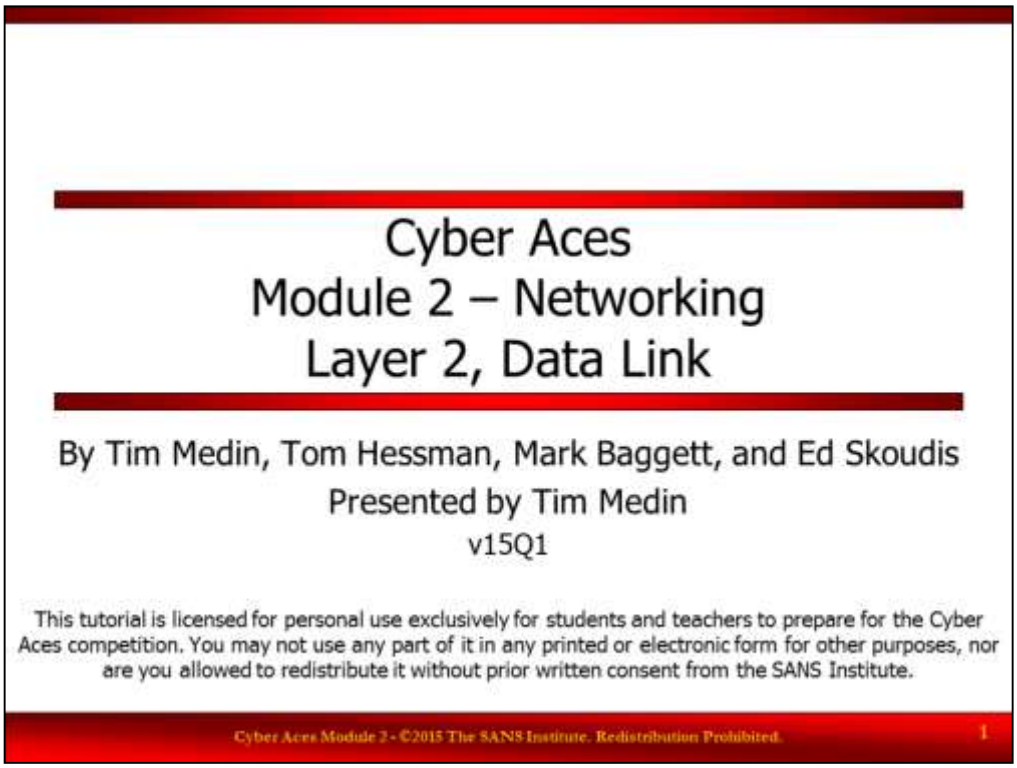
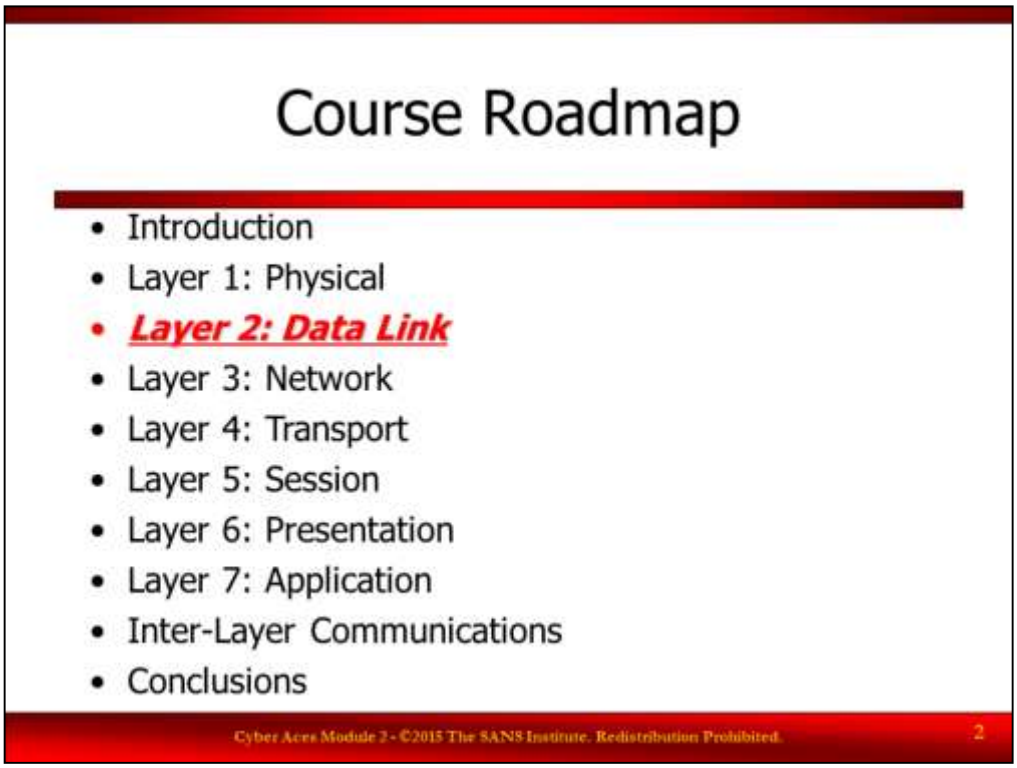
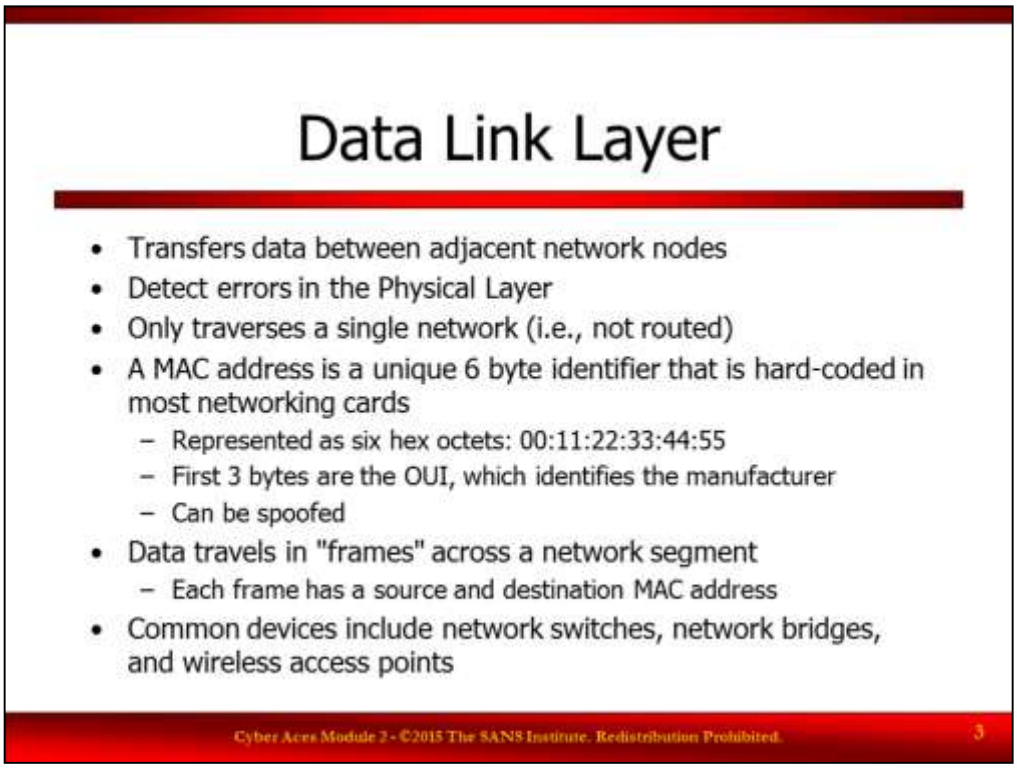


Welcome to Cyber Aces, Module 2! A firm understanding of network fundamentals is essential to being able to secure a network or attack one. This section provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective.



Course Roadmap

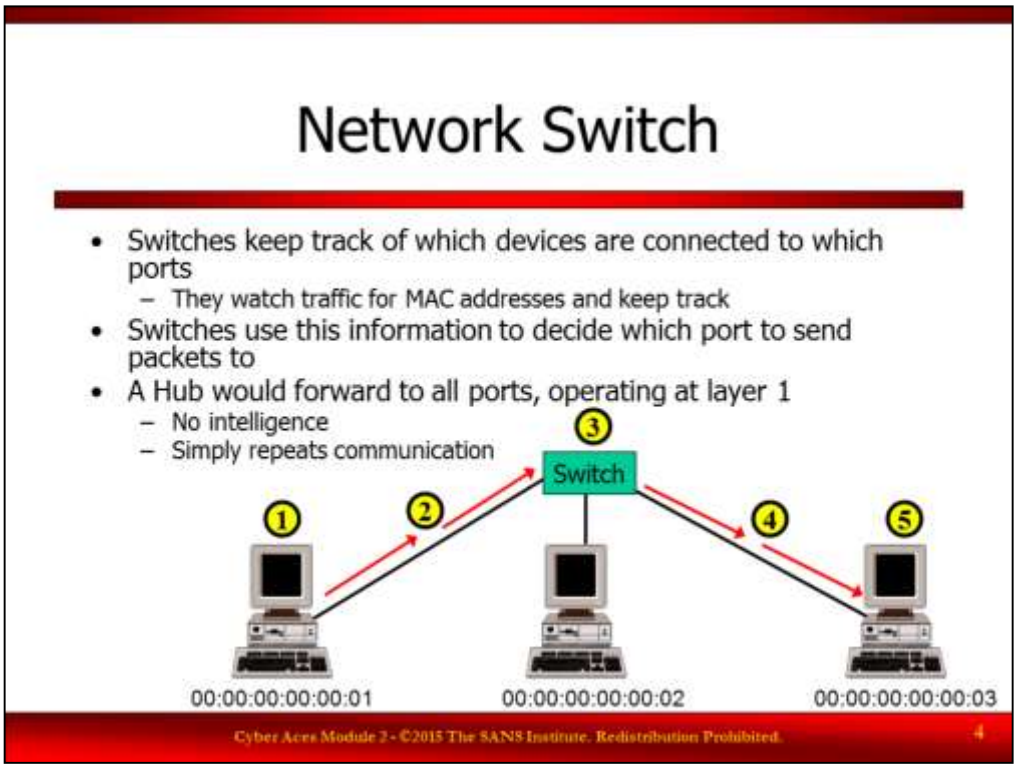
In this section, you'll learn about the Data Link Layer. We'll cover devices that operate at this layer, such as network switches, and ARP, an important networking protocol operating at this layer.



Data Link Layer

Now that we can physically connect our computers and transmit single bits of data, we need a way to organize those bits (1's and 0's) and identify the sender and receiver. That is where the data link layer comes in. The IEEE established the 802 standard, which gave us the MAC address. The MAC address is a 6 byte (each byte is 8 bits) address that is hard coded on most networking cards in computer systems and network devices. MAC addresses are generally represented as six hexadecimal (base 16) octets, such as "00:11:22:33:44:55". (Hexadecimal is a base 16 numbering system, where each digit represents a decimal number between 0 and 15 (A=10,B=11,C=12,D=13,E=14,F=15).) The first three octets are called the OUI (Organizationally Unique Identifier), and identify the company that manufactured the network device. Since the first 3 octets represent the manufacturer, you may sometimes see MAC addresses of the form "Dell_33:44:55", where "Dell" is the manufacturer associated with the first 3 octets. Although MAC addresses are hard-coded in network cards, it is possible for them to be spoofed in software. Therefore, it is not safe to rely exclusively on MAC addresses as a means of secure identification.

Leveraging the 802 standard, we have built standards such as Ethernet 802.3 and Wireless 802.11. A message, consisting of a collection of bits with a source MAC address and destination MAC address destined for a given system, is often referred to as a FRAME. Network switches and wireless access points operate at this layer, exchanging frames. Frames are only transmitted within a single network, and are not routed between different networks (routing occurs at Layer 3). Therefore, your MAC address is not sent across the Internet. Common Data Link Layer devices include network switches, network bridges, and wireless access points.

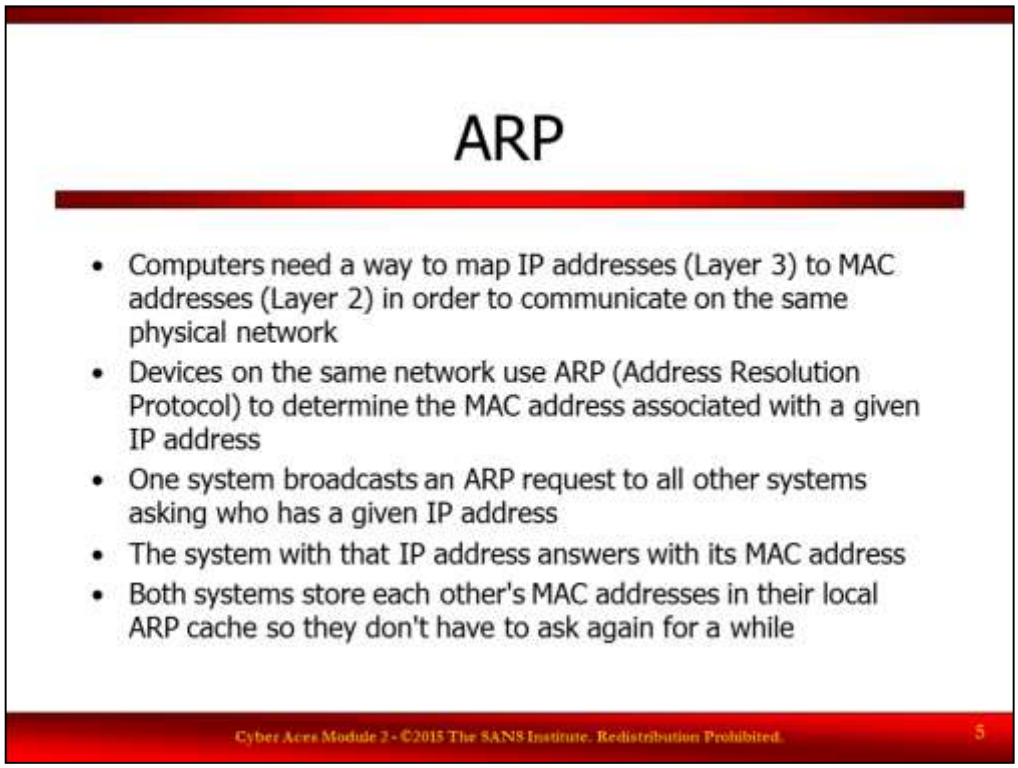


Network Switch

Switches track MAC addresses to make decisions about where to send Ethernet frames. They monitor traffic to determine which ports hosts are reachable through, and store a mapping of MAC addresses to switch port in the CAM (Content Addressable Memory) table. Using this information, switches only send packets to the necessary port, instead of to all ports (the way a hub would). This makes switches more efficient than hubs, since they reduce the amount of traffic each node must filter through. This efficiency helps with Carrier Sense Multiple Access/Collision Detection, as there will be less traffic on the local wires, and therefore less chance of a collision.

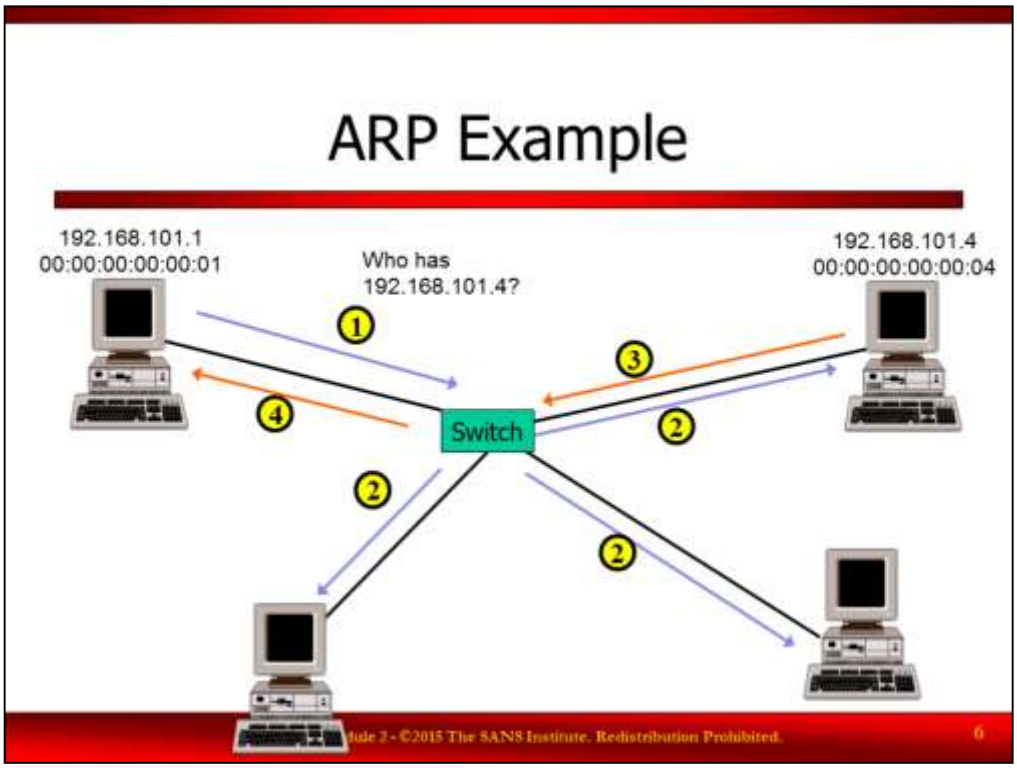
In the diagram above, imagine that a frame is being sent from 00:00:00:00:00:01 to 00:00:00:00:00:03. In Step 1, the frame is transmitted from the source computer through a network cable, and arrives at the switch. In Step 2, the switch consults its CAM table to determine which of its ports 00:00:00:00:00:03 is connected to, and then transmits the frame from the appropriate port, though the network cable to the destination (3). Other systems connected to the switch, such as 00:00:00:00:00:02, never see the frame.

Note that if a switch does not yet know which port a given host is attached to, or if the CAM table is full, it will send the frame to all ports.



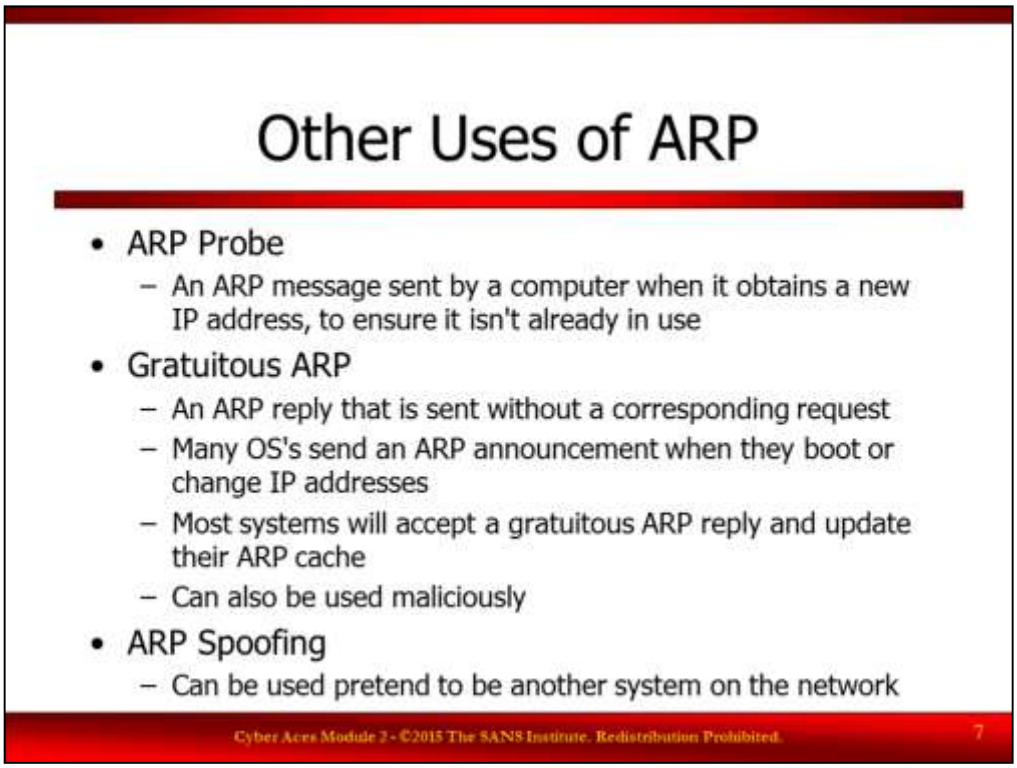
ARP

Address Resolution Protocol, or "ARP", is a Layer 2 protocol that enables the communications between Layer 2 and Layer 3 by maintaining a mapping of IP Addresses to MAC addresses and vice versa. When a system needs to know another system's MAC address, it sends a broadcast message to all systems on the network asking who has a given IP address (i.e., "Who has 192.168.23.42?"). The system with that IP address will then answer with its MAC address (i.e., "192.168.23.42 is at 00:01:02:03:04:05"). Both systems will then store the IP address to MAC address mapping in their local ARP cache.



ARP Example

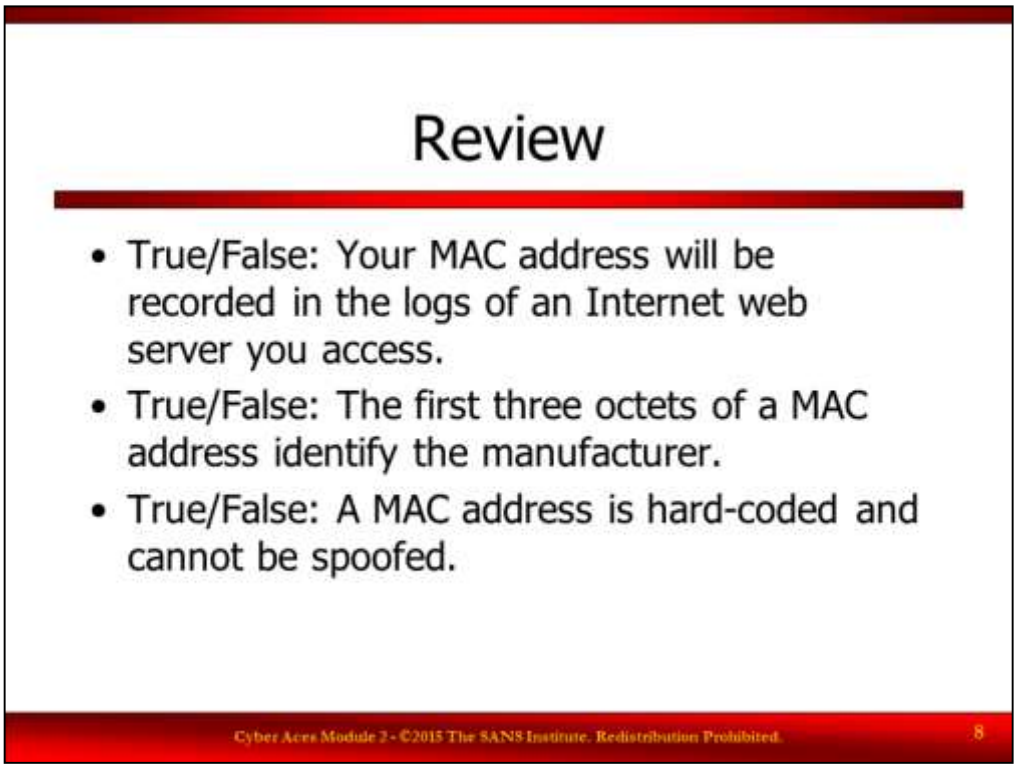
Let's say that the computer at 192.168.101.1 would like to communicate with 192.168.101.4. Since they are on the same local network, 192.168.101.1 will need 192.168.101.4's MAC address. In step 1, it sends an ARP request to the entire network asking who has the IP address 192.168.101.4. In step 2, the switch sends the request to every port, and every computer on the network receives it. In step 3, the computer with the IP address 192.168.101.4 answers with an ARP reply, which gets sent to the original computer (step 4). Note that all of the other computers on the network simply ignore the ARP request.



Other Uses of ARP

An ARP probe is a special ARP packet used to help prevent IP address conflicts. Before a system begins using a new IP address, it will send an ARP probe to the network asking if anyone is already using the IP address. If there is no response, then the IP address should be safe to use.

Gratuitous ARP messages are generally ARP replies that are sent without having received an ARP request. They are legitimately used by many operating systems to announce a system's new IP address after a reboot or IP address change, allowing other systems on the network to update their ARP caches right away. Otherwise, if a system had an outdated entry in its ARP cache, it may disrupt the ability to communicate with that host. Most systems will happily accept an unsolicited ARP reply and use it to update its ARP cache. Therefore, it can also be used maliciously, such as for ARP spoofing. ARP spoofing is used to pretend to be another system on the network by sending a gratuitous ARP reply with the desired IP address and the attacker's MAC address. This causes other systems on the network to believe the attacker's system has the desired IP address.

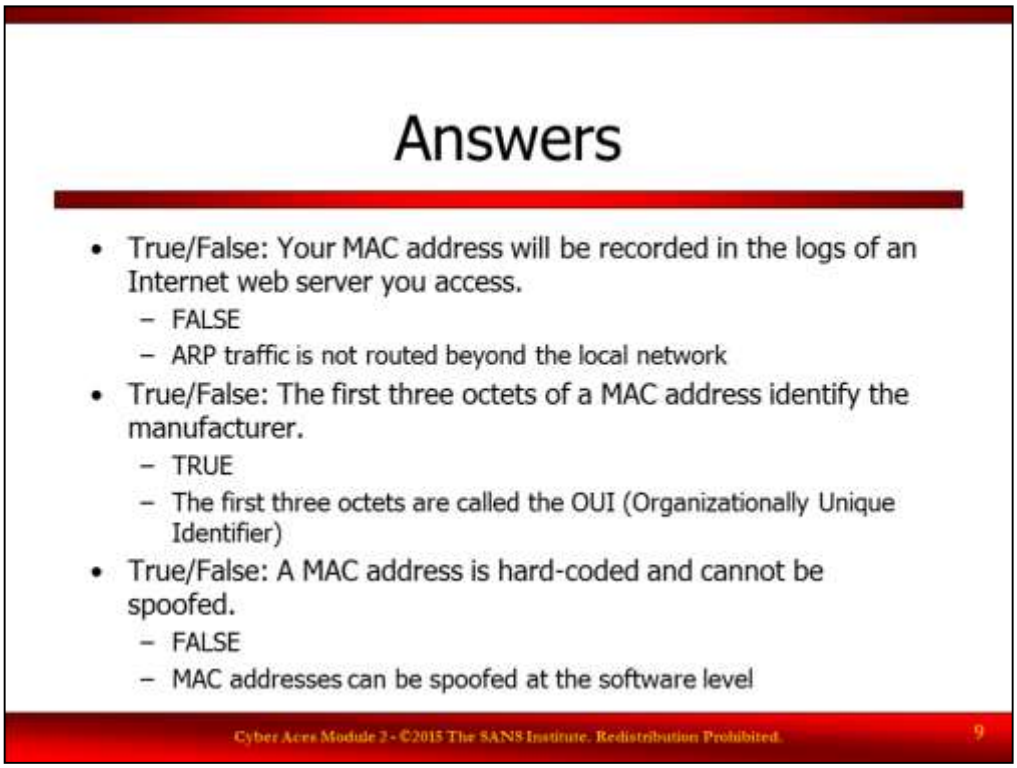


Review Questions

True/False: Your MAC address will be recorded in the logs of an Internet web server you access.

True/False: The first three octets of a MAC address identify the manufacturer

True/False: A MAC address is hard-coded and cannot be spoofed.



Answers

True/False: Your MAC address will be recorded in the logs of an Internet web server you access.

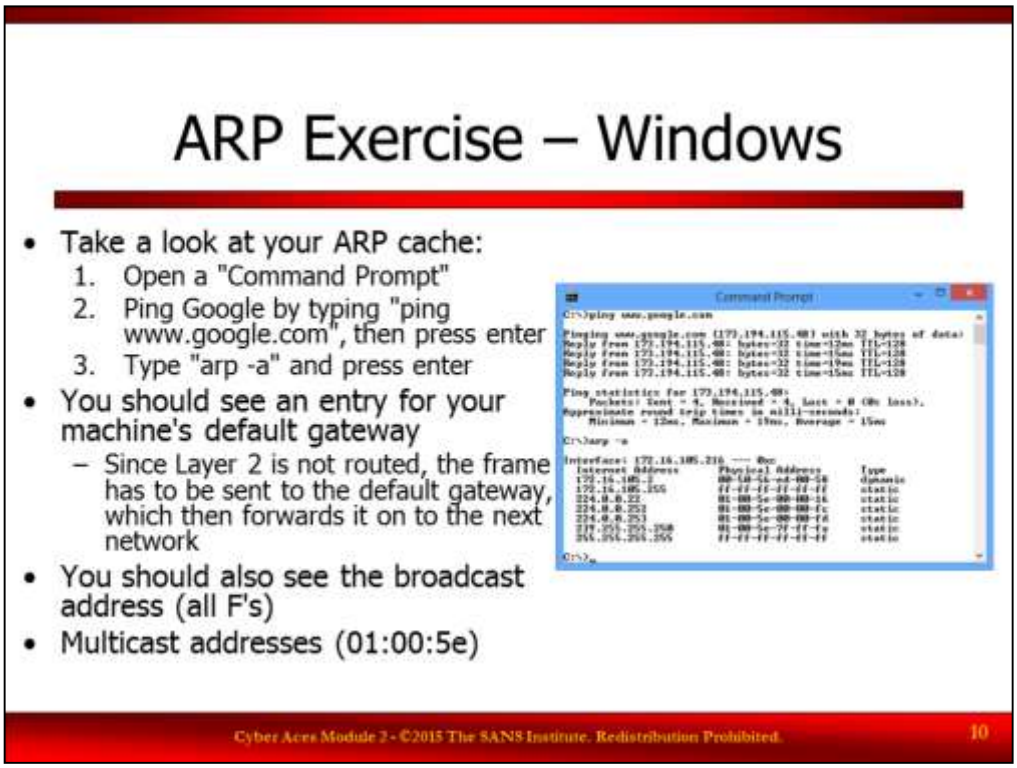
False, ARP traffic is not routed beyond the local network

True/False: The first three octets of a MAC address identify the manufacturer.

True, the first three octets are called the OUI (Organizationally Unique Identifier)

True/False: A MAC address is hard-coded and cannot be spoofed.

False, MAC addresses can be spoofed at the software level



ARP Exercise – Windows

As a quick exercise, try viewing your computer's ARP cache after pinging a server. First, open a "Command Prompt" or "Terminal" window, then ping Google by running the following command:

```
C:\> ping google.com
```

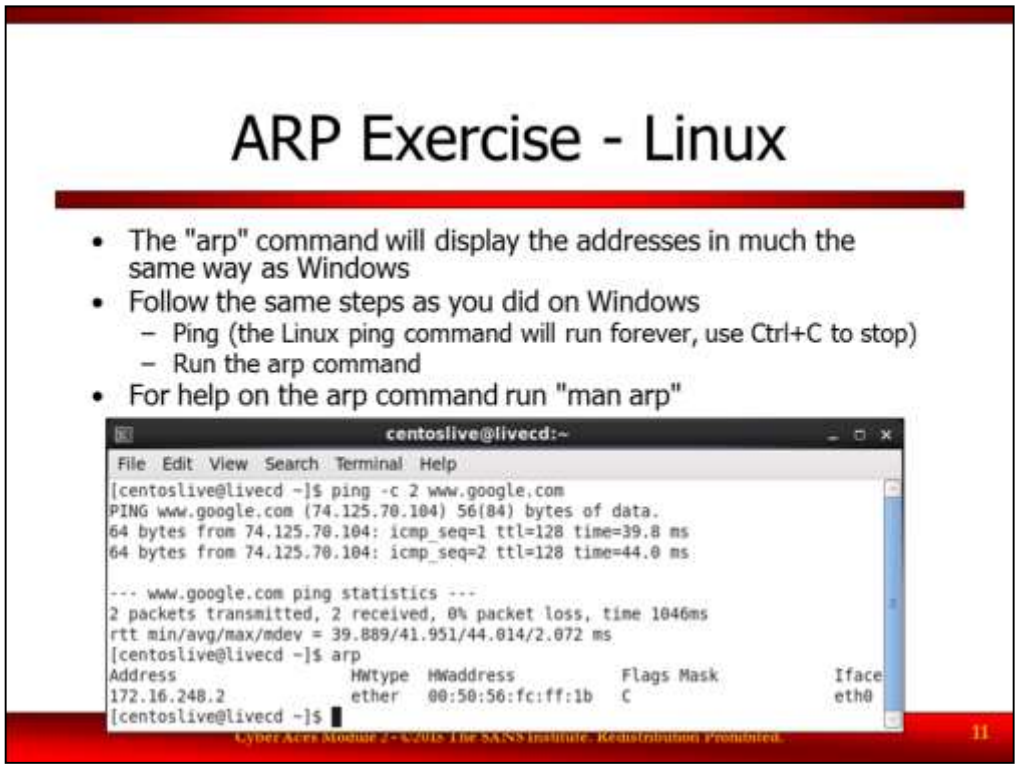
Then, to view your ARP cache, run:

```
C:\> arp -a
```

You should see an entry for your machine's default gateway (run **`ipconfig`** to confirm)! Note that since Layer 2 traffic is not routed between networks, you won't see an ARP entry for Google's IP address. Instead, you see your default gateway's IP and MAC addresses because your computer has to communicate through the default gateway to reach Google.

The "arp" command also has a "-d" option, which allows you to delete an entry from the ARP cache. For example, to remove the ARP entry for 192.168.198.2 above, you would run:

```
C:\> arp -d 192.168.198.2
```



ARP Exercise Linux

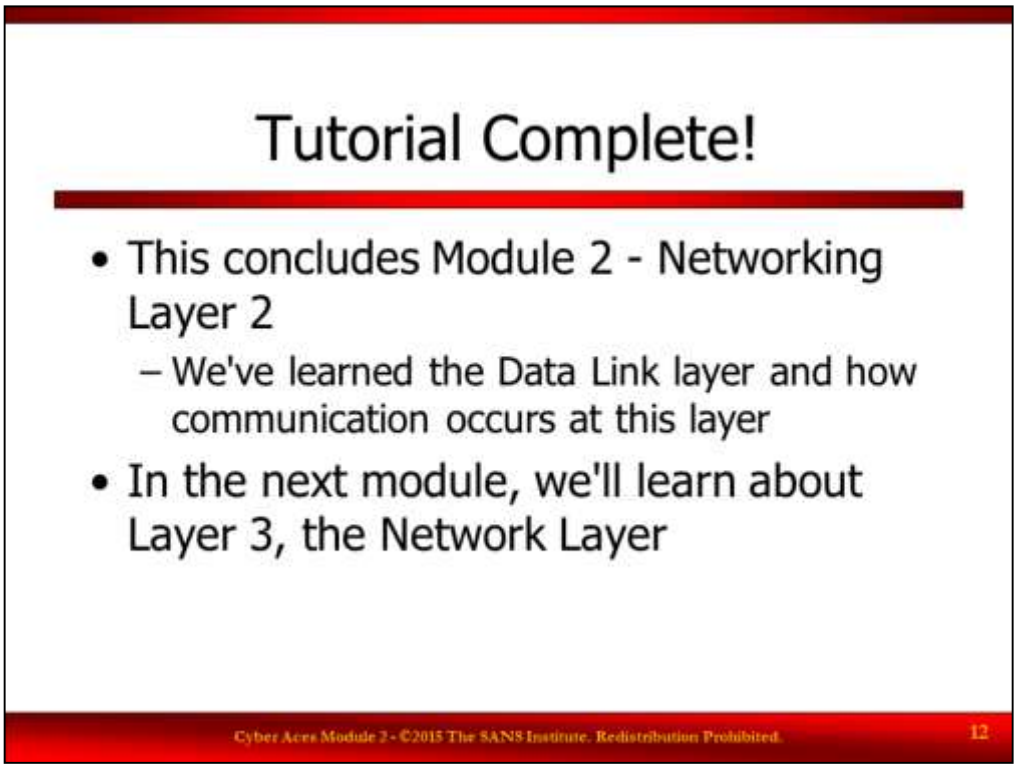
The "arp" command in Linux operates much in the same was as it does in Windows. First, ping www.google.com. The ping command in Linux will run forever, so press Ctrl+C or use the count option (-c) to specify the number if ICMP packets to send.

```
[centoslive@livecd ~]$ ping -c 2 www.google.com
PING www.google.com (74.125.70.104) 56(84) bytes of data.
64 bytes from 74.125.70.104: icmp_seq=1 ttl=128 time=39.8 ms
64 bytes from 74.125.70.104: icmp_seq=2 ttl=128 time=44.0 ms

--- www.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1046ms
rtt min/avg/max/mdev = 39.889/41.951/44.014/2.072 ms
```

Next, run the arp command to see the MAC address of your default gateway.

```
[centoslive@livecd ~]$ arp
Address                  HWtype  HWaddress           Flags Mask
Iface
172.16.248.2             ether   00:50:56:fc:ff:1b   C
eth0
[centoslive@livecd ~]$
```



Tutorial Complete

This concludes the discussion about Layer 2, the Data Link Layer.

In the next tutorial we'll discuss the next layer in the OSI model, the Network Layer.