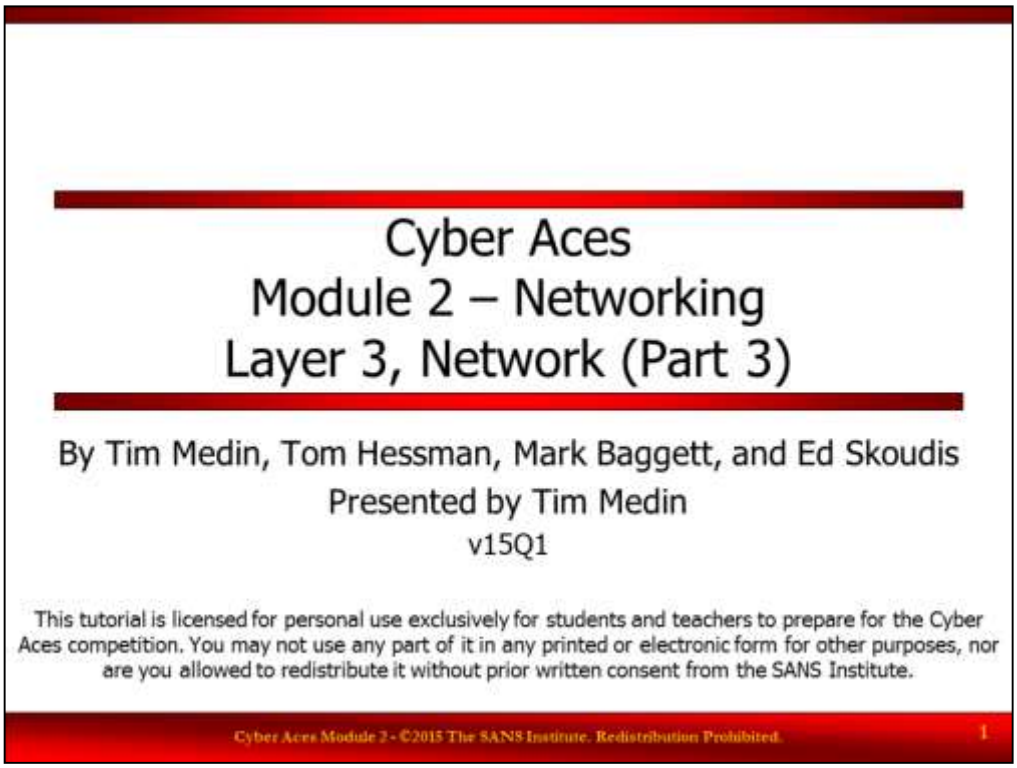
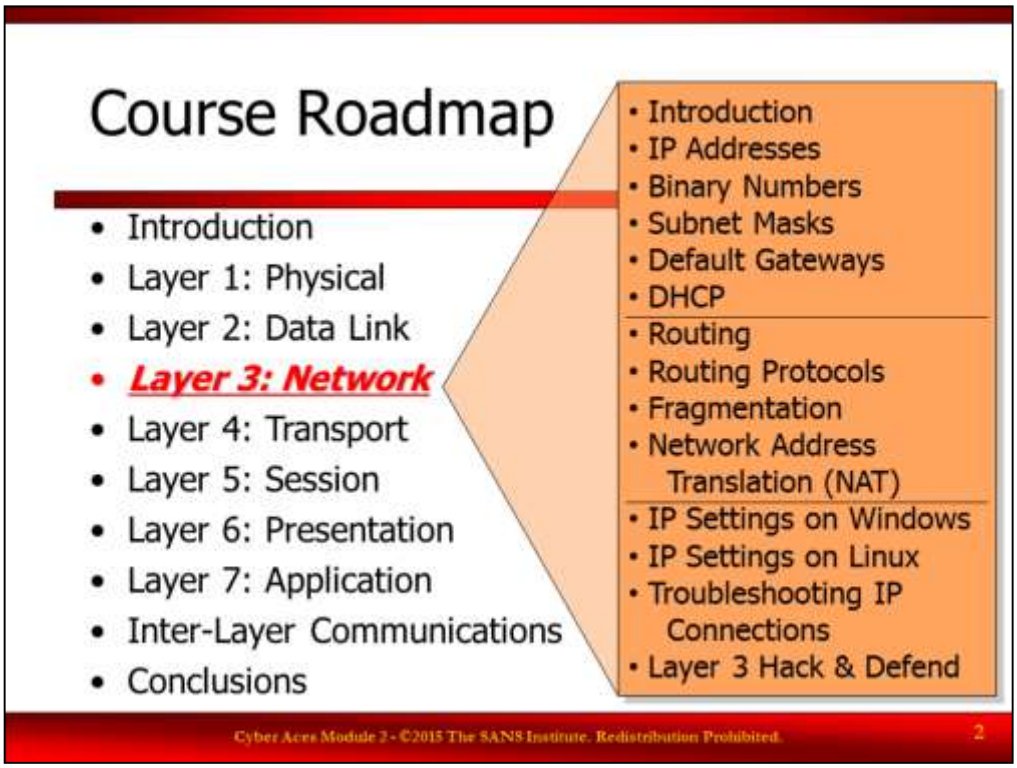
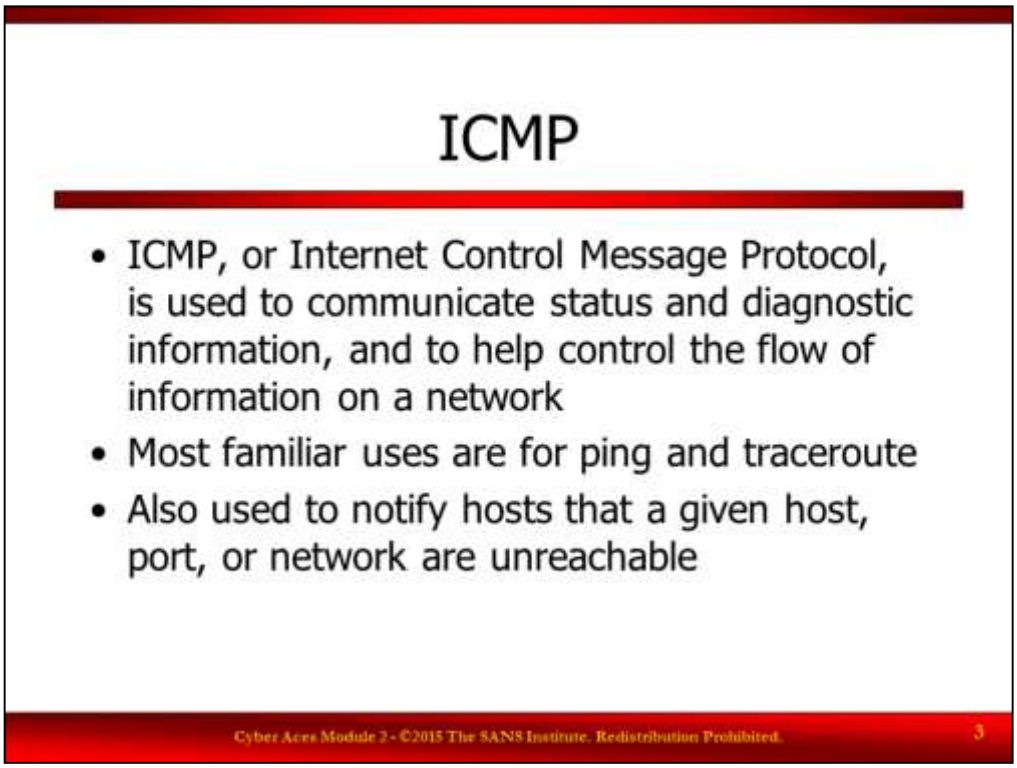


Welcome to Cyber Aces, Module 2! A firm understanding of network fundamentals is essential to being able to secure a network or attack one. This section provides a broad overview of networking, covering the fundamental concepts needed to understand computer attacks and defenses from a network perspective.

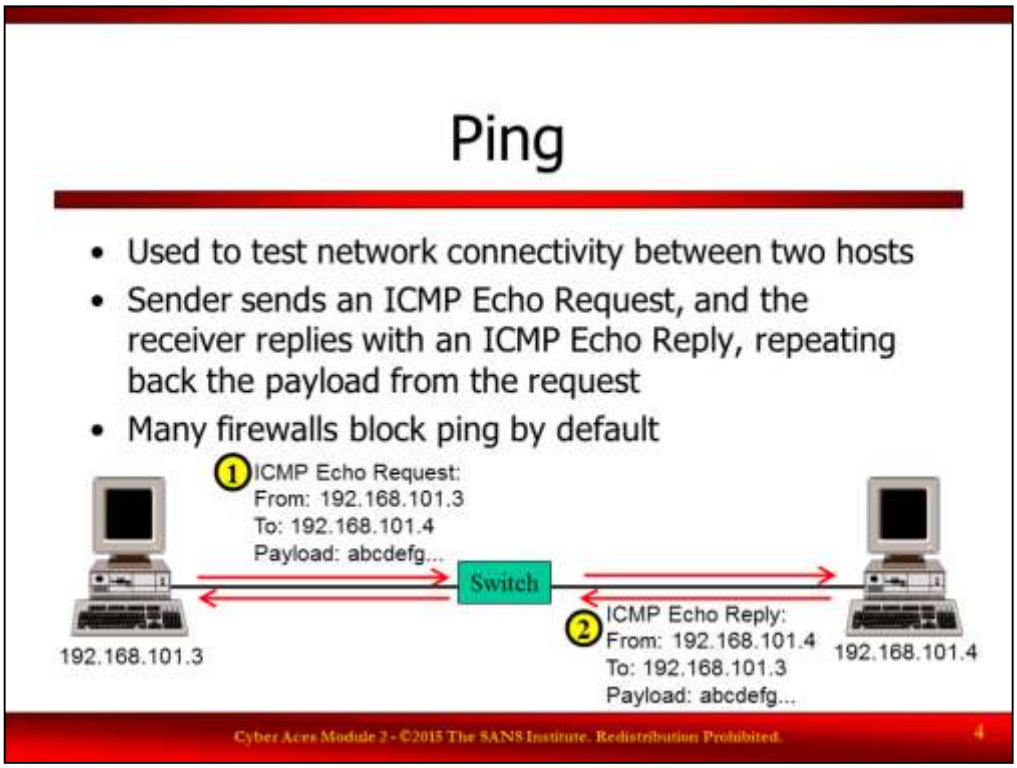


In this section, you'll learn about the Network Layer. You'll learn about IP addressing, subnet masks, default gateways, routing, NAT, and more!



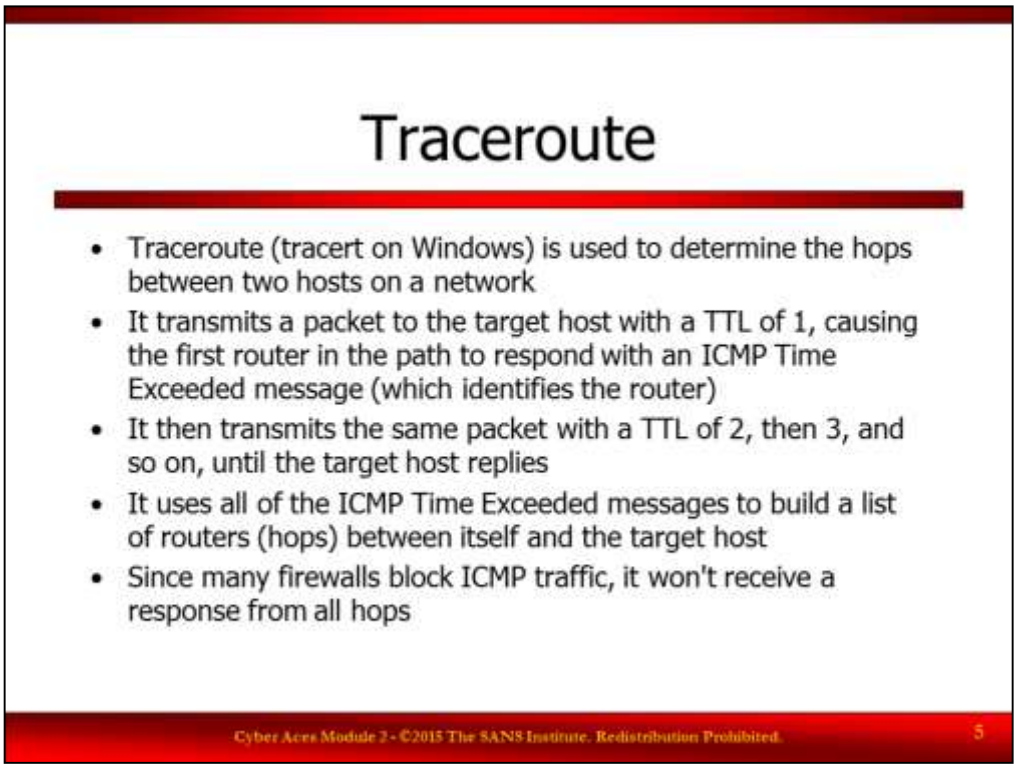
ICMP

ICMP can be a little confusing because it is a Layer 3 protocol that depends upon another Layer 3 protocol (IP). ICMP is used by devices on the Internet to communicate their status and control the flow of information. For example, routers might use ICMP to communicate with a host on their network and notify them of another router that is better for them to use to reach a specific network. The most familiar use of ICMP for most people is the ICMP Echo Request. The program PING uses ICMP Echo Request's to determine if another host on the network is up. PING sends ICMP Echo Requests to a remote host, which in turn will ECHO the information they receive back to the sender in an ICMP Echo Response. Many of the tools we use to troubleshoot connectivity issues use ICMP. ICMP is also used to notify hosts of network errors, such as a given host, port, or network being unreachable.



Ping

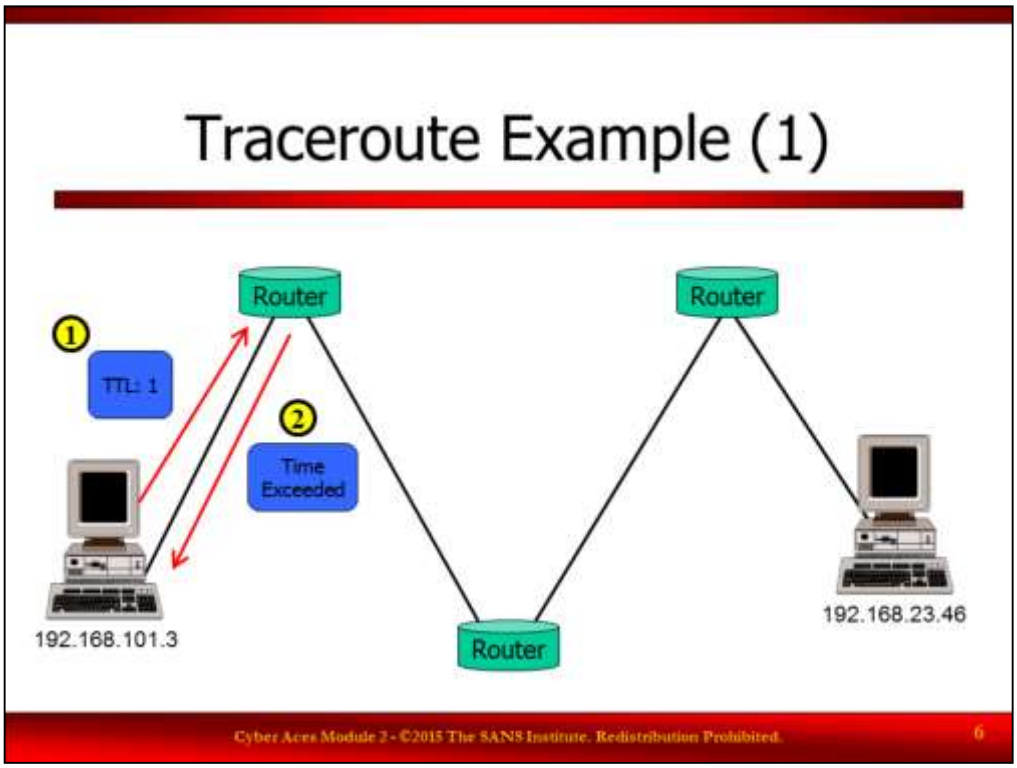
Ping is a network utility found on all major operating systems that tests the network connectivity between two hosts on a network. Ping works by sending an ICMP Echo Request to a target system that contains a known payload (usually something sequential like "abcdefg[...]"). When the target receives the request, it responds with an ICMP Echo Reply, containing the same payload mirrored back. If the original system receives the response, and it contains the same payload, then it knows that the target host is reachable. It can also determine the time it took (typically in milliseconds) for the packet to travel back and forth, and can recognize if the payload has been altered in transit. Many firewalls block ICMP traffic by default, since it can reveal potentially sensitive details about the inside of a network. Therefore, the mere fact that a host doesn't respond to an ICMP Echo Request doesn't necessarily mean that it is not reachable.



Traceroute

Traceroute (called "tracert" on Windows) is a network utility found on all major operating systems that can be used to determine all of the routers (or hops) between two hosts on a network. It works by transmitting a packet to the target host with a TTL of 1, which will cause the first router in the path to respond with an "ICMP Time Exceeded: TTL Expired in Transit" message. That error serves to identify that router as the first hop. Traceroute then transmits the same packet again with a TTL of 2, then 3, and so on, gathering information on every router in the path, until the target host itself replies. As it's running, it uses the information gleaned from the ICMP Time Exceeded messages to display a list of routers between the two hosts. However, since many firewalls block ICMP traffic, it won't receive a response from all hops. Routers that don't respond are indicated with a set of asterisks (*).

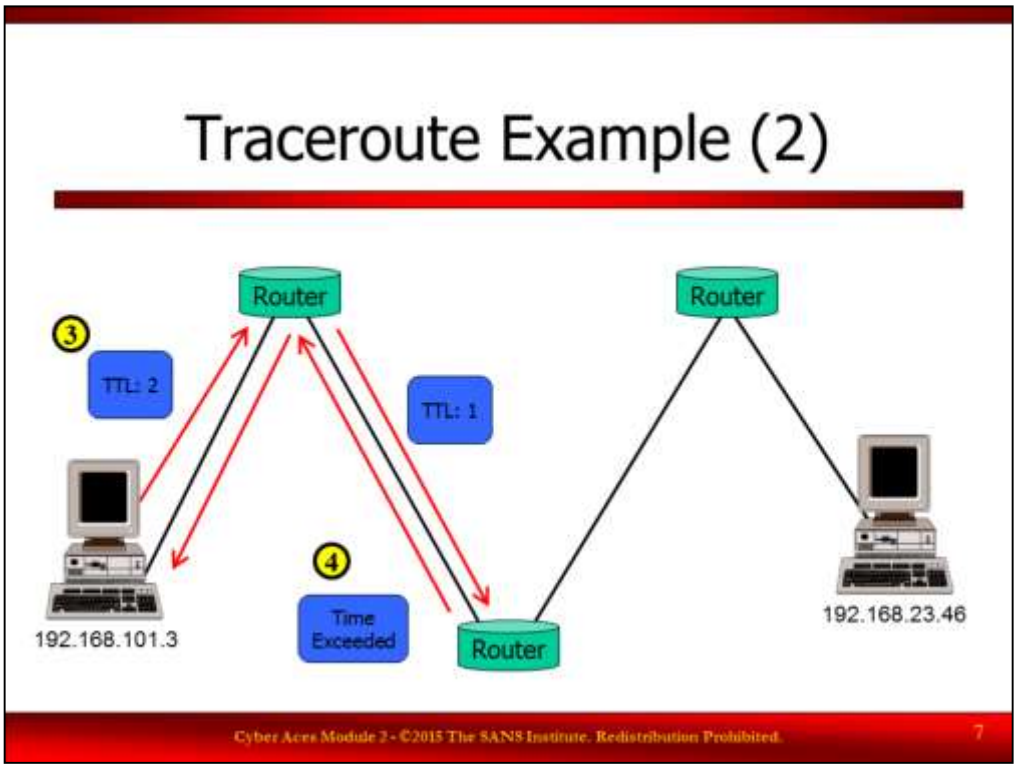
By default, the Linux version of traceroute sends UDP packets to high numbered ports (33434 to 33534), and the Windows version sends ICMP Echo Request packets. Both, of course, would trigger the ICMP Time Exceeded messages on the routers, and the Linux version has an option to use ICMP Echo Request's instead (`-I`).



Traceroute Example (1)

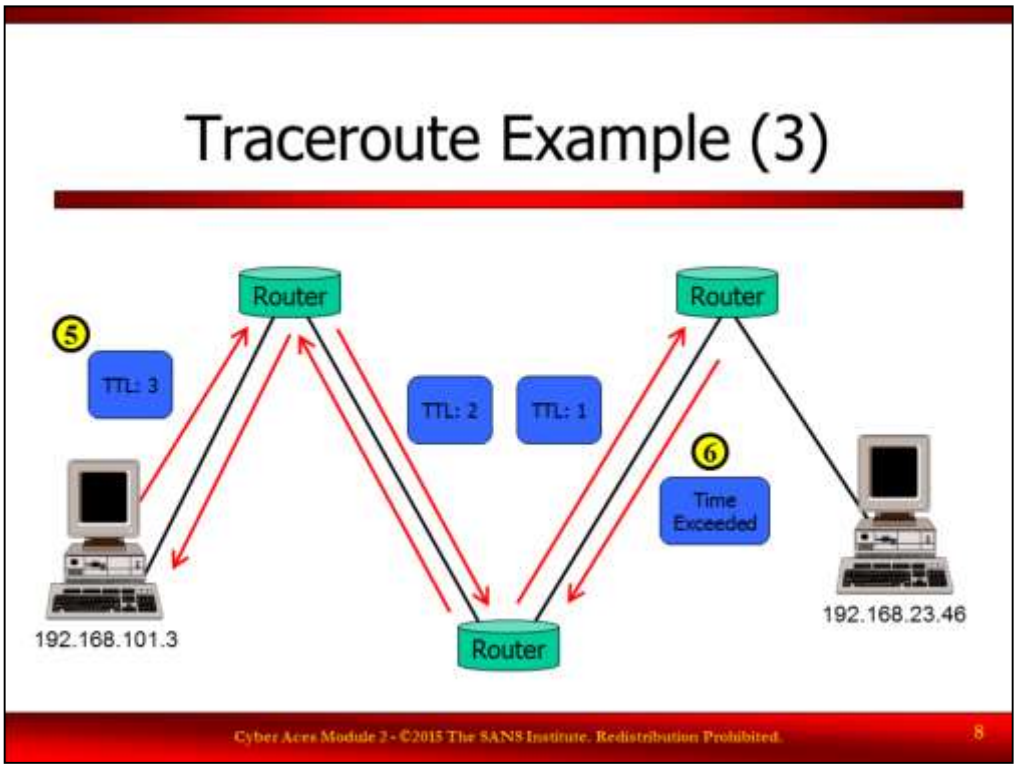
Here is an example network, which has three routers between 192.168.101.3 and 192.168.23.46. The user at 192.168.101.3 decides to use Traceroute to determine the path to 192.168.23.46.

In Step 1, 192.168.101.3 sends an ICMP Echo Request to 192.168.23.46, with a TTL of 1. In Step 2, the first router in the path responds with an ICMP Time Exceeded message. 192.168.101.3 now knows the address of the first hop.



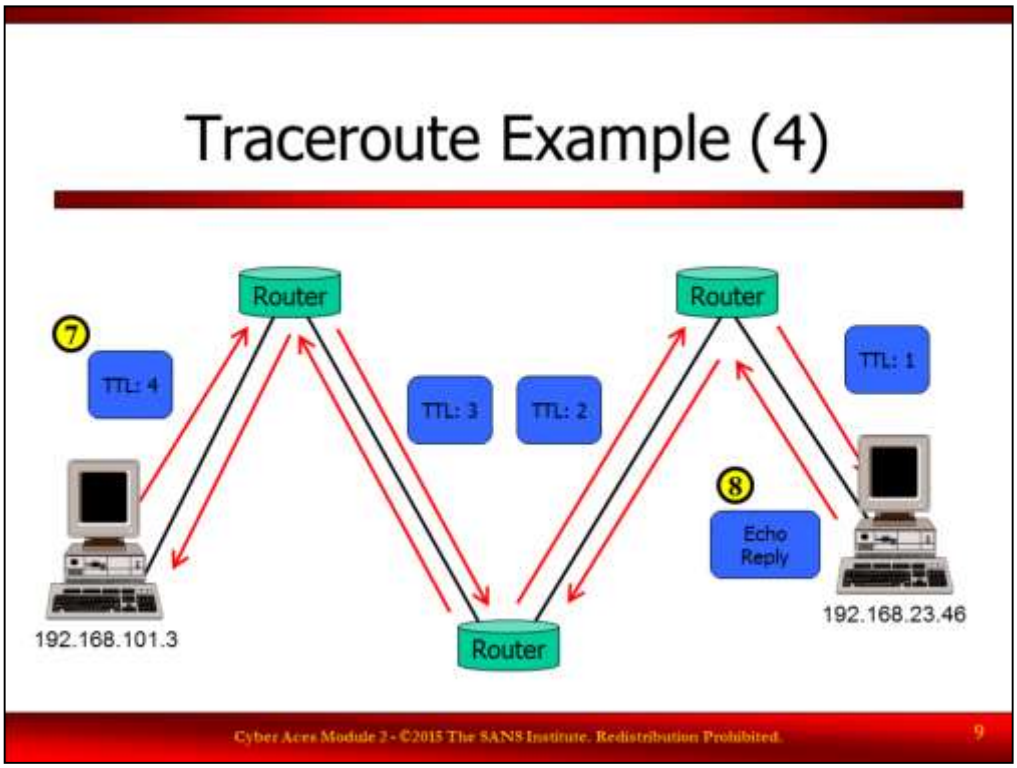
Traceroute Example (2)

In Step 3, 192.168.101.3 sends another ICMP Echo Request to 192.168.23.46, this time with a TTL of 2. When the first router receives it, it decrements the TTL to 1 and sends it to the next router. In Step 4, that router receives it and responds to 192.168.101.3 with an ICMP Time Exceeded message, which passes through the first router and reaches 192.168.101.3, revealing the address of the second hop.



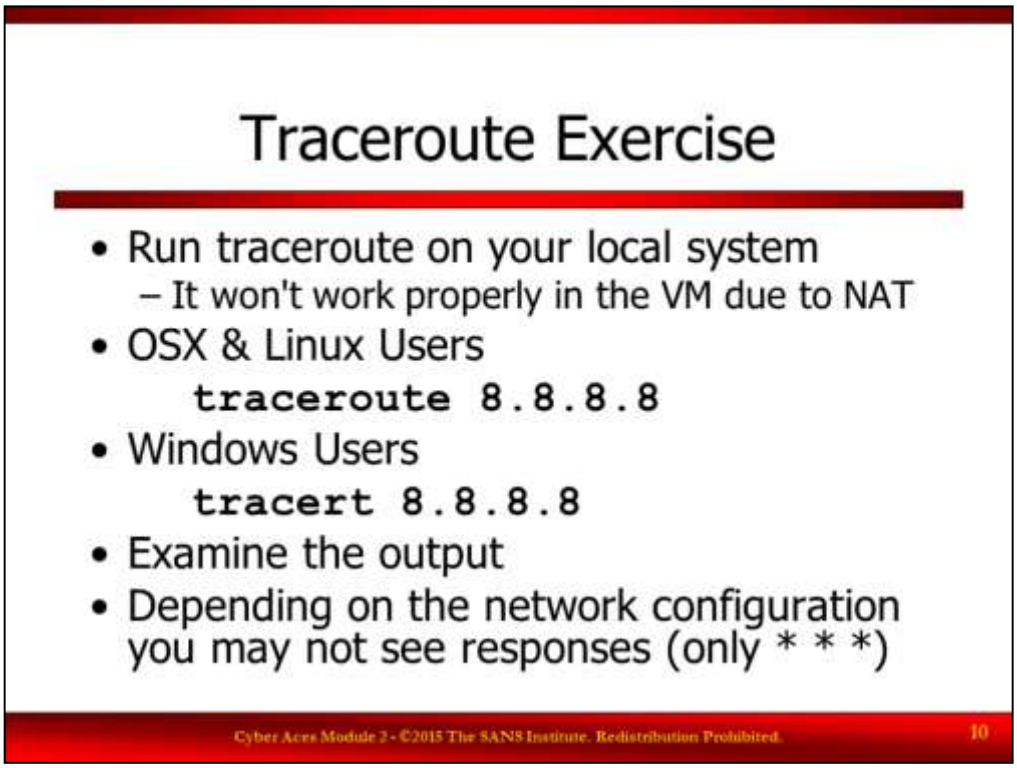
Traceroute Example (3)

In Step 5, 192.168.101.3 sends another ICMP Echo Request to 192.168.23.46, this time with a TTL of 3. When the first router receives it, it decrements the TTL to 2 and sends it to the next router. When the second router receives it, it decrements the TTL to 1 and sends it to the next one. In Step 6, that router receives it and responds to 192.168.101.3 with an ICMP Time Exceeded message, which passes through the first two routers and reaches 192.168.101.3, revealing the address of the third hop.



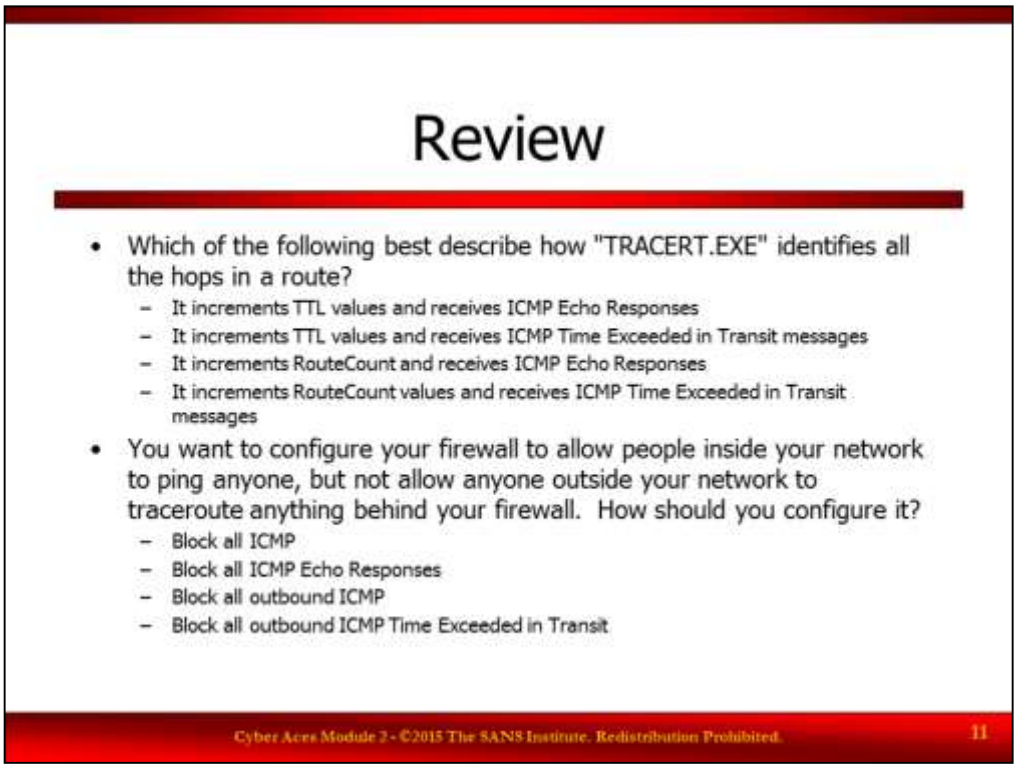
Traceroute Example (4)

In Step 7, 192.168.101.3 sends another ICMP Echo Request to 192.168.23.46, this time with a TTL of 4. When the first router receives it, it decrements the TTL to 3 and sends it to the next router. When the second router receives it, it decrements the TTL to 2 and sends it to the next one. When the third router receives it, it decrements the TTL to 1 and sends it to 192.168.23.46. In Step 8, the host at 192.168.23.46 receives it and responds to 192.168.101.3 with an ICMP Echo Reply message, which passes through the first three routers and reaches 192.168.101.3. This indicates to 192.168.101.3 that it has determined the full route, and that it takes 3 hops.



Traceroute Exercise

Run the traceroute command on your system towards the 8.8.8.8 system. Take a look at the responses. You should see responses, but you may not if your ISP blocks the response traffic. If you do see valid responses you will see the various hops between you and Google including your default gateway and your ISPs routers.



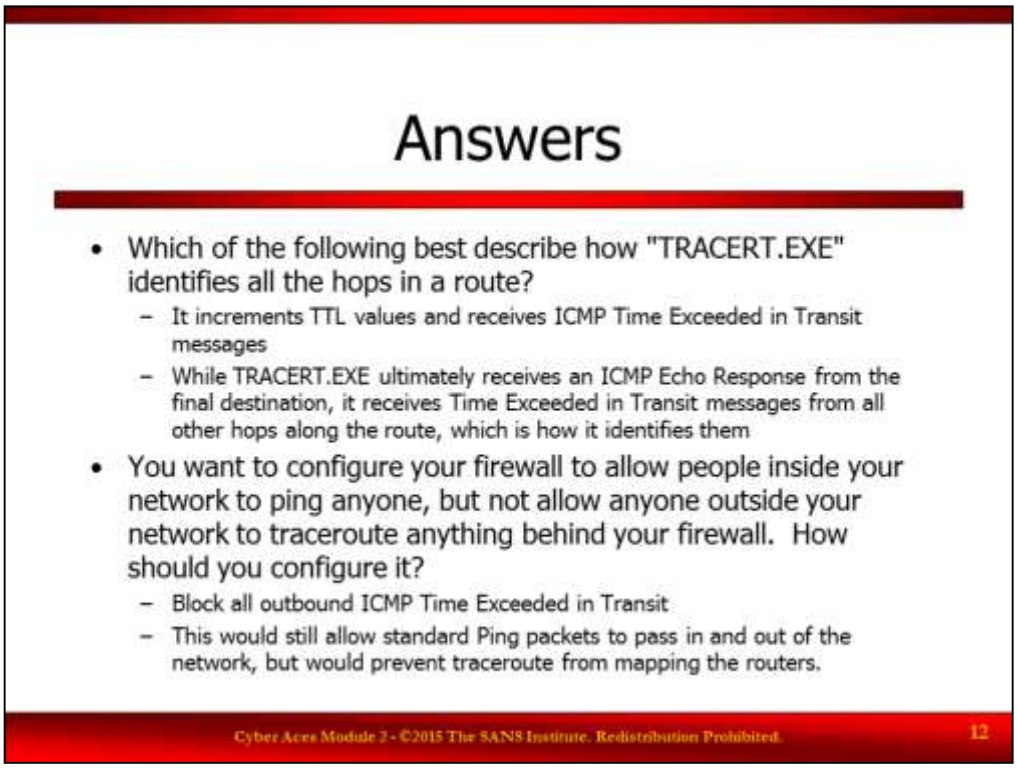
Review Questions

Which of the following best describe how "TRACERT.EXE" identifies all the hops in a route?

- It increments TTL values and receives ICMP Echo Responses
- It increments TTL values and receives ICMP Time Exceeded in Transit messages
- It increments RouteCount and receives ICMP Echo Responses
- It increments RouteCount values and receives ICMP Time Exceeded in Transit messages

You want to configure your firewall to allow people inside your network to ping anyone, but not allow anyone outside your network to traceroute anything behind your firewall. How should you configure it?

- Block all ICMP
- Block all ICMP Echo Responses
- Block all outbound ICMP
- Block all outbound ICMP Time Exceeded in Transit



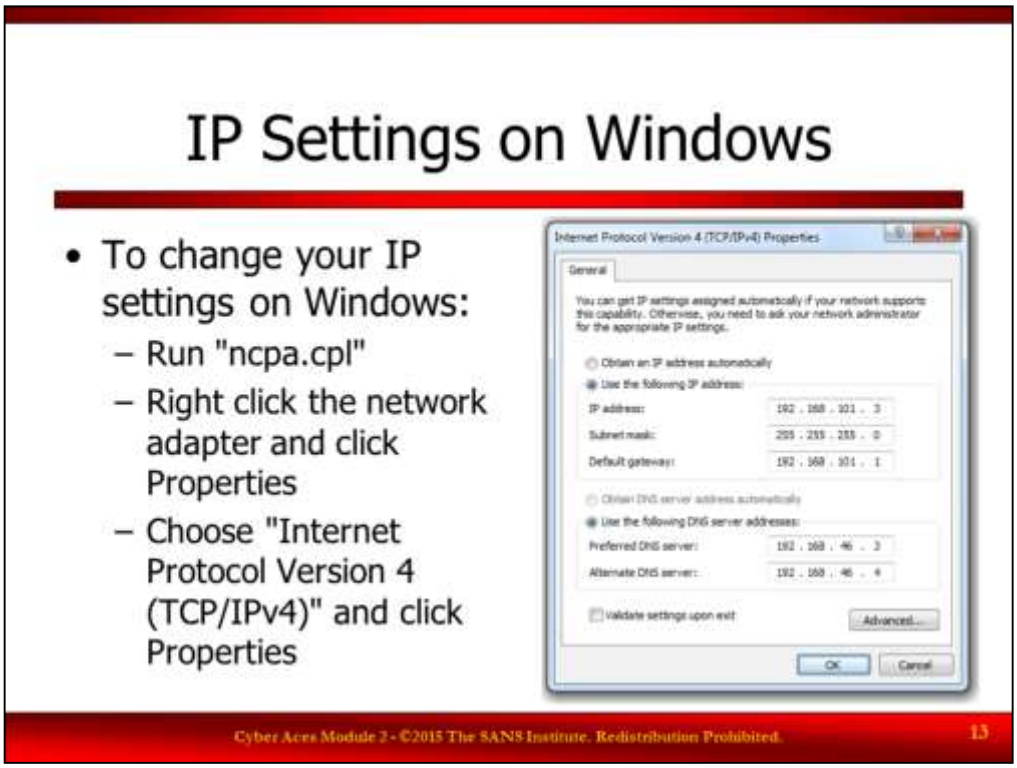
Answers

Which of the following best describe how "TRACERT.EXE" identifies all the hops in a route?

- It increments TTL values and receives ICMP Time Exceeded in Transit messages
- While TRACERT.EXE ultimately receives an ICMP Echo Response from the final destination, it receives Time Exceeded in Transit messages from all other hops along the route, which is how it identifies them

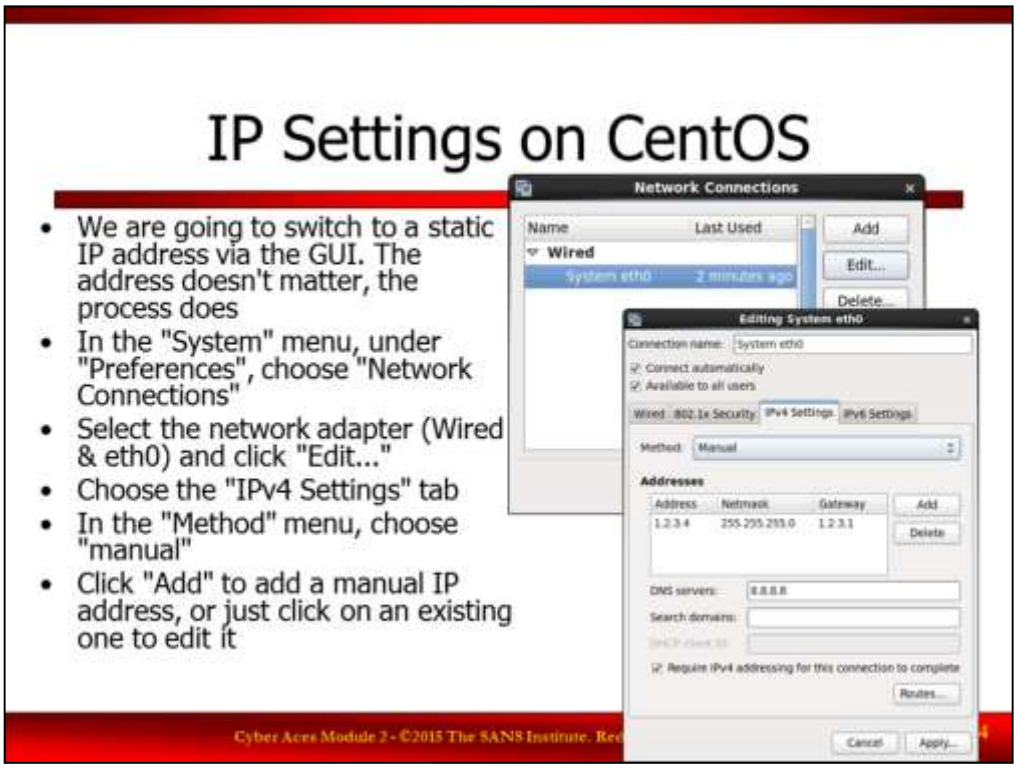
You want to configure your firewall to allow people inside your network to ping anyone, but not allow anyone outside your network to traceroute anything behind your firewall. How should you configure it?

- Block all outbound ICMP Time Exceeded in Transit
- This would still allow standard Ping packets to pass in and out of the network, but would prevent traceroute from mapping the routers.



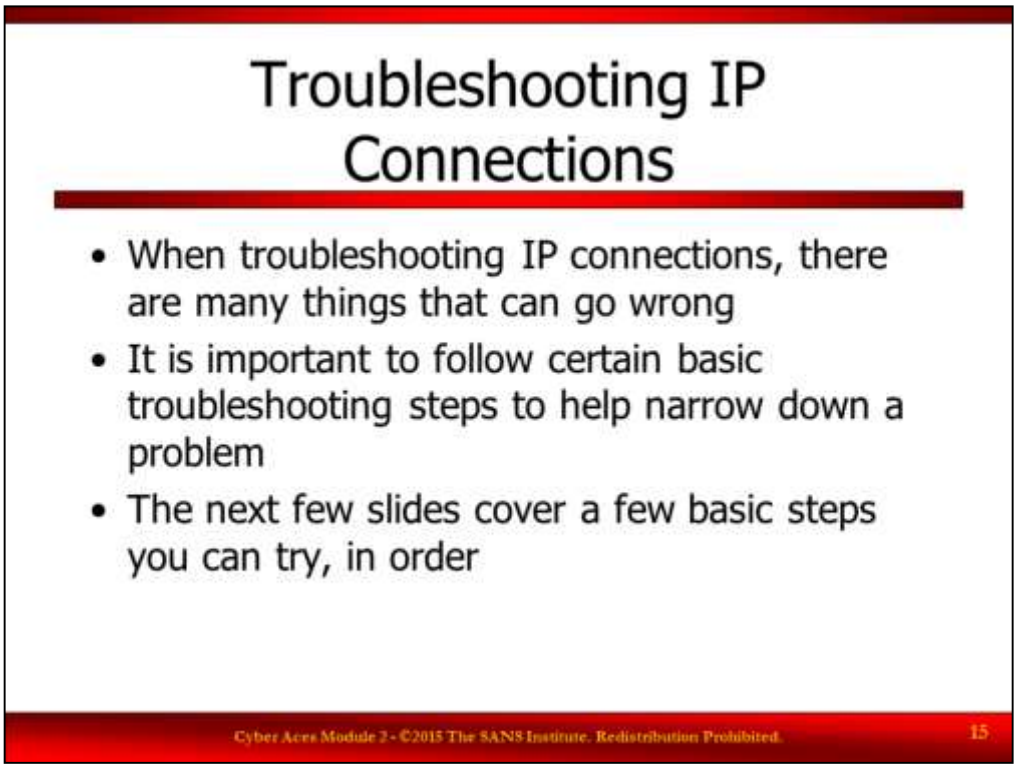
IP Settings on Windows

To change your IP settings on Windows, first open the Network Control Panel. The easiest way to do this is to run "ncpa.cpl" from either the Run dialog or the search box on the Start menu. Then, right click the appropriate network adapter and click Properties. Then, choose "Internet Protocol Version 4 (TCP/IPv4)" and click Properties, which will display the screen above. To use DHCP to automatically configure your network settings, choose "Obtain an IP address automatically". To manually set your IP settings, choose "Use the following IP address", and specify the IP address, subnet mask, default gateway, and at least one DNS server.



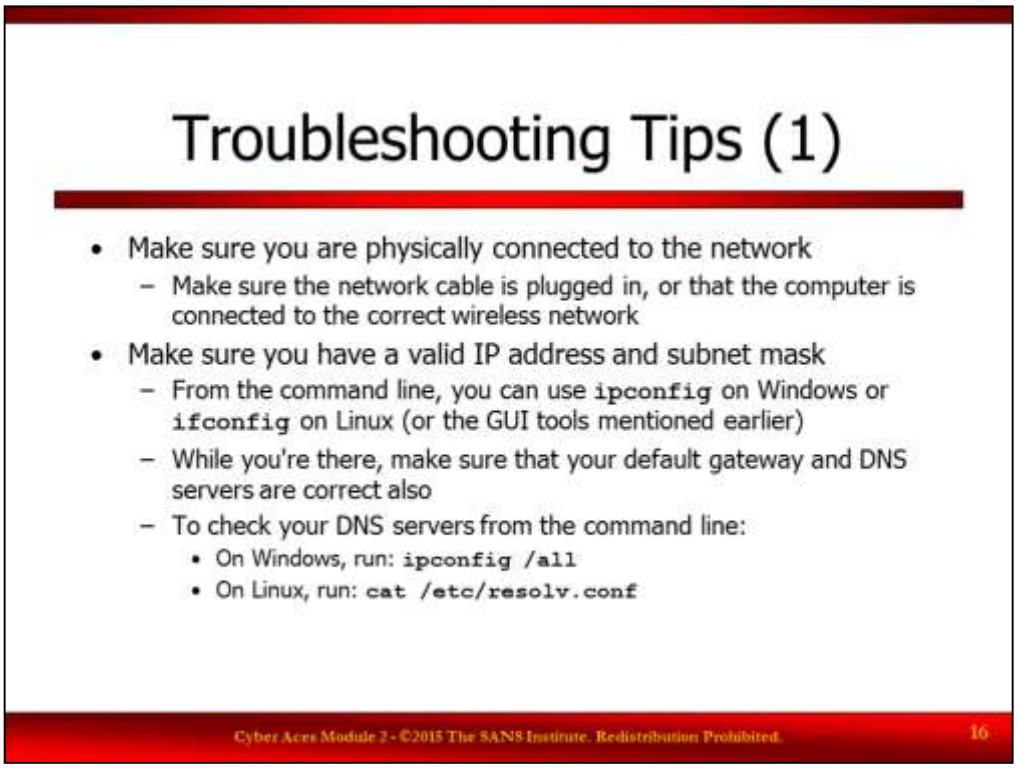
IP Settings on Centos

The procedure for changing your IP settings on Linux varies depending on the distribution. Here, we will focus on CentOS, which uses the cross-distro "NetworkManager" package (so, the steps will be similar for other Linux distributions as well). In the System menu, under Preferences, choose "Network Connections". Select the network adapter (such as "Auto eth0") and click "Edit...". Then, choose the "IPv4 Settings" tab, and you'll see the screen above. To manually set an IP address, choose "Manual" from the "Method" menu, and then click "Add" and enter the IP address, netmask, and default gateway. DNS servers can be specified in a comma-separated list.



Troubleshooting IP Connections

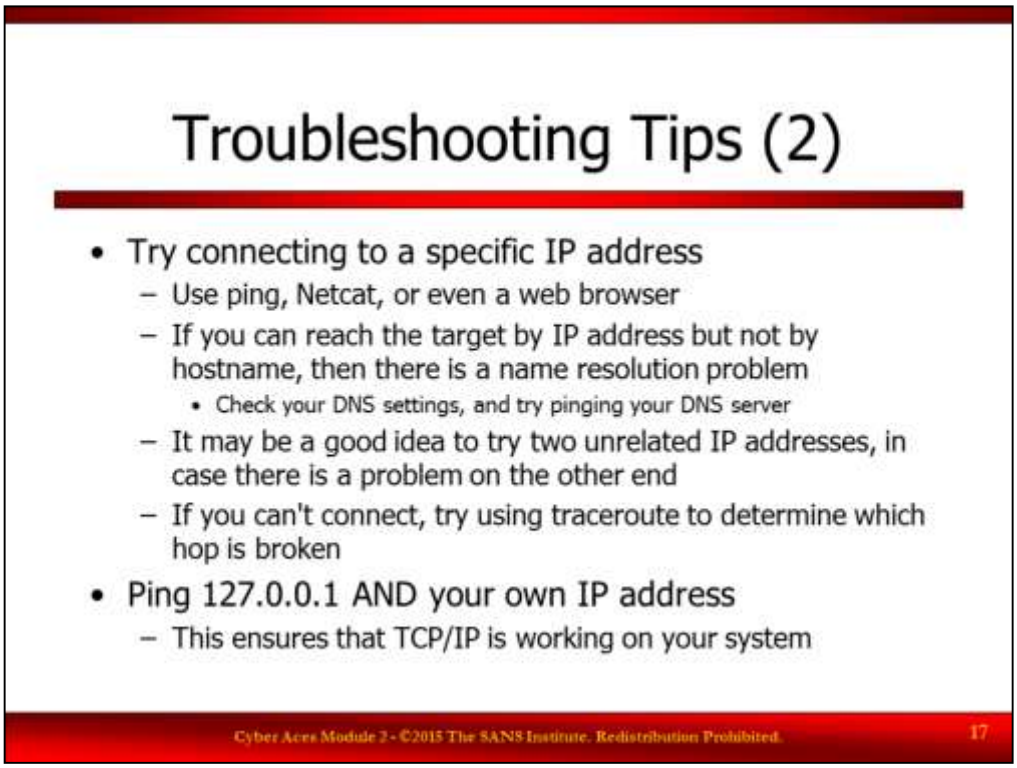
Several issues can arise in complex systems such as our modern day networks. Determining the specific cause preventing two computers from communicating can be a frustrating exercise if you don't follow some basic network troubleshooting steps. It is important to follow certain basic troubleshooting steps to help narrow down a problem. The next few slides cover a few basic steps you can try, in order, to determine where the problem is.



Troubleshooting Tips (1)

A good first step is to make sure that your computer is, in fact, connected to the network. For a wired network, make sure that the network cable is plugged in. For a wireless network, make sure that the computer's wireless adapter is turned on, and that it is connected to the correct wireless network.

Next, make sure that you have a valid IP address and subnet mask. From the command line, you can use the "**`ipconfig`**" command on Windows or the "**`ifconfig`**" command on Linux, or you can use the GUI tools that were mentioned earlier. You should also verify that your default gateway and DNS server are set correctly. To check your DNS servers from the command line on Windows, run "**`ipconfig /all`**". On Linux, run "**`cat /etc/resolv.conf`**".

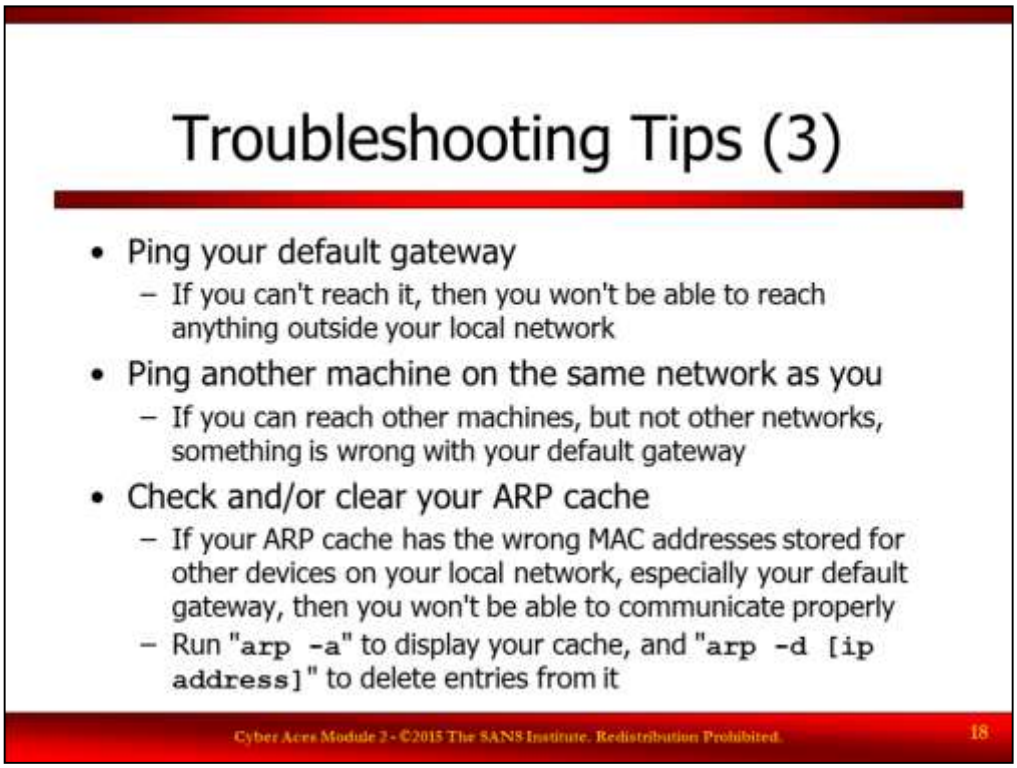


Troubleshooting Tips (2)

One of the best ways to test your network connectivity is to try connecting to something that you know should work. You should try connecting to a remote host directly by IP address, in case there are problems with name resolution. Try pinging a specific IP address on the Internet, such as 8.8.8.8 (Google's public DNS service). You could also try connecting to something with Netcat, or opening a web page in your browser.

If you are able to reach the remote host by IP address but not by hostname, then there is something wrong with name resolution. You should check your DNS settings, and try pinging your DNS server to make sure that it is reachable. You should try connecting to at least two unrelated IP addresses, in case there is some sort of problem on the other end with one of them. If you can't connect, you may want to try running traceroute on the IP you can't reach to see if you can determine which hop along the path is broken.

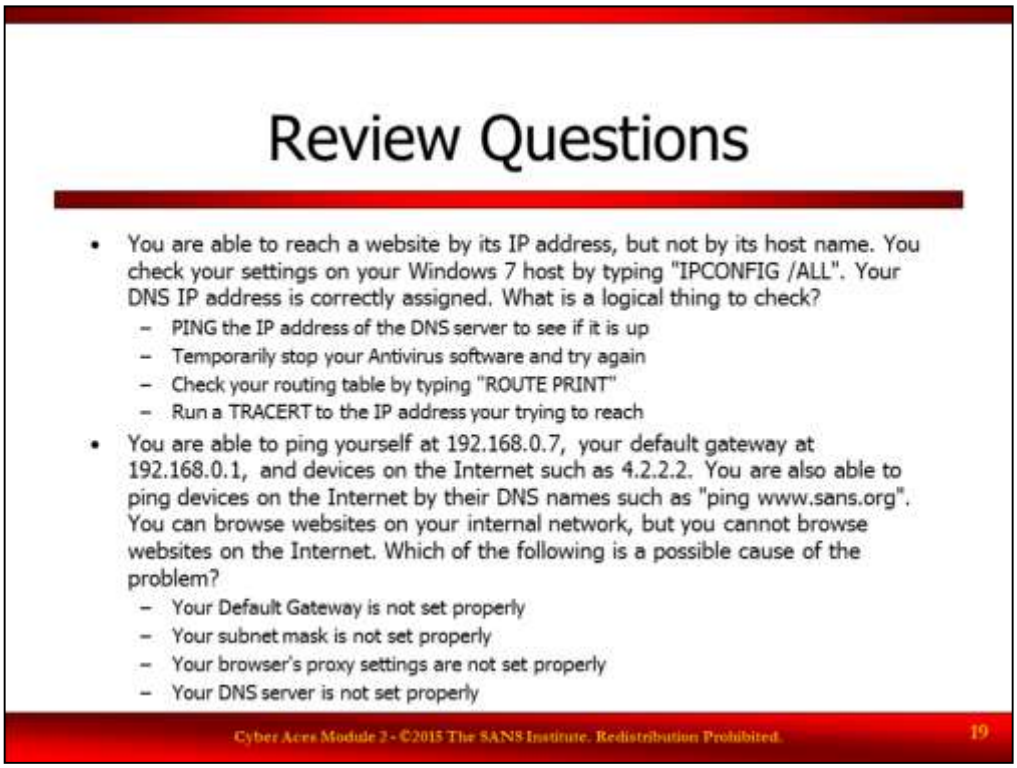
You should also try pinging your local loopback address (127.0.0.1), as well as your machine's own IP address. This will ensure that TCP/IP is working properly on your system, and that the problem is not entirely internal.



Troubleshooting Tips (3)

Try pinging your default gateway. If you can't reach it, then you won't be able to reach anything outside your local network. If you can reach it, but you still can't reach anything beyond it, then either something is wrong with the gateway, or something is wrong between the gateway and the system you're trying to reach. Again, traceroute should be able to help determine this. If the gateway is connected to something like a cable modem, you may want to check that.

Try pinging another machine on the same network as you. If you can reach other machines on the same subnet, this is further evidence that something is wrong with your default gateway. However, if you can't reach other machines on the same subnet, then something is likely wrong on your computer. You should check your ARP cache for invalid entries. If your ARP cache has the wrong MAC addresses stored for other devices on your local network, especially your default gateway, then you won't be able to communicate properly. Try clearing your ARP cache (run "**`arp -d [ip address]`**" on each entry).



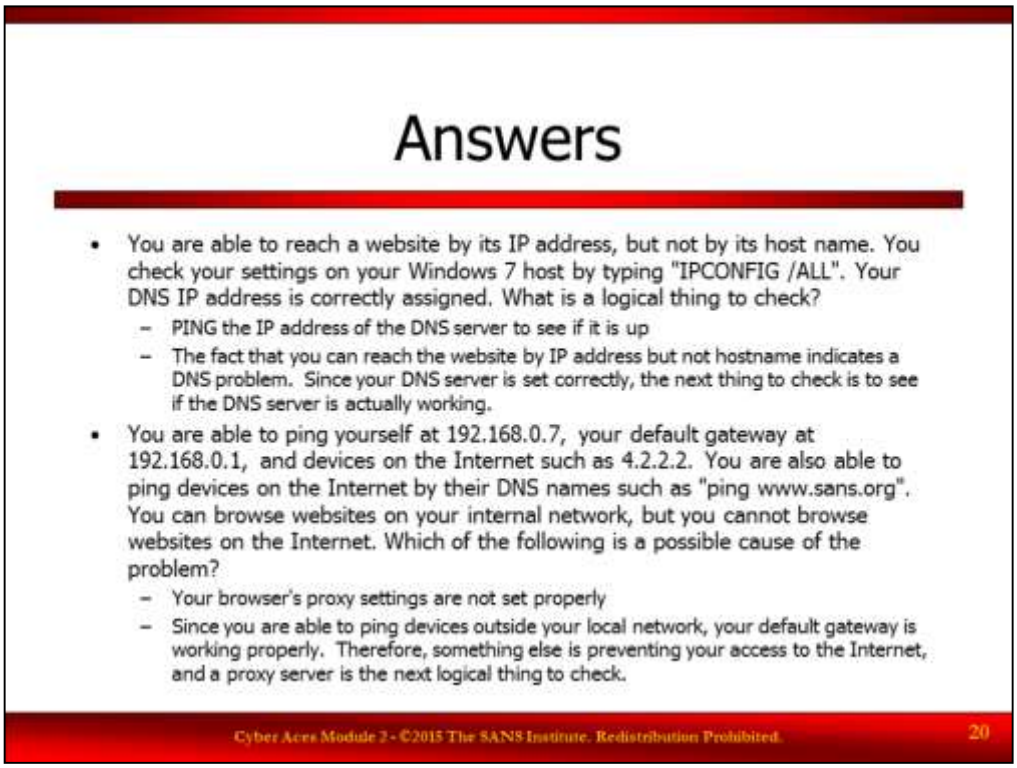
Review Questions

You are able to reach a website by its IP address, but not by its host name. You check your settings on your Windows 7 host by typing "IPCONFIG /ALL". Your DNS IP address is correctly assigned. What is a logical thing to check?

- PING the IP address of the DNS server to see if it is up
- Temporarily stop your Antivirus software and try again
- Check your routing table by typing "ROUTE PRINT"
- Run a TRACERT to the IP address your trying to reach

You are able to ping yourself at 192.168.0.7, your default gateway at 192.168.0.1, and devices on the Internet such as 4.2.2.2. You are also able to ping devices on the Internet by their DNS names such as "ping www.sans.org". You can browse websites on your internal network, but you cannot browse websites on the Internet. Which of the following is a possible cause of the problem?

- Your Default Gateway is not set properly
- Your subnet mask is not set properly
- Your browser's proxy settings are not set properly
- Your DNS server is not set properly



Answers

You are able to reach a website by its IP address, but not by its host name. You check your settings on your Windows 7 host by typing "IPCONFIG /ALL". Your DNS IP address is correctly assigned. What is a logical thing to check?

- PING the IP address of the DNS server to see if it is up
- The fact that you can reach the website by IP address but not hostname indicates a DNS problem. Since your DNS server is set correctly, the next thing to check is to see if the DNS server is actually working.

You are able to ping yourself at 192.168.0.7, your default gateway at 192.168.0.1, and devices on the Internet such as 4.2.2.2. You are also able to ping devices on the Internet by their DNS names such as "ping www.sans.org". You can browse websites on your internal network, but you cannot browse websites on the Internet. Which of the following is a possible cause of the problem?

- Your browser's proxy settings are not set properly
- Since you are able to ping devices outside your local network, your default gateway is working properly. Therefore, something else is preventing your access to the Internet, and a proxy server is the next logical thing to check.

Layer 3 Hack & Defend

Read more about these topics online:

IP spoofing:

http://www.sans.org/security-resources/idfaq/spoofed_ip.php

ARP Spoofing Attacks:

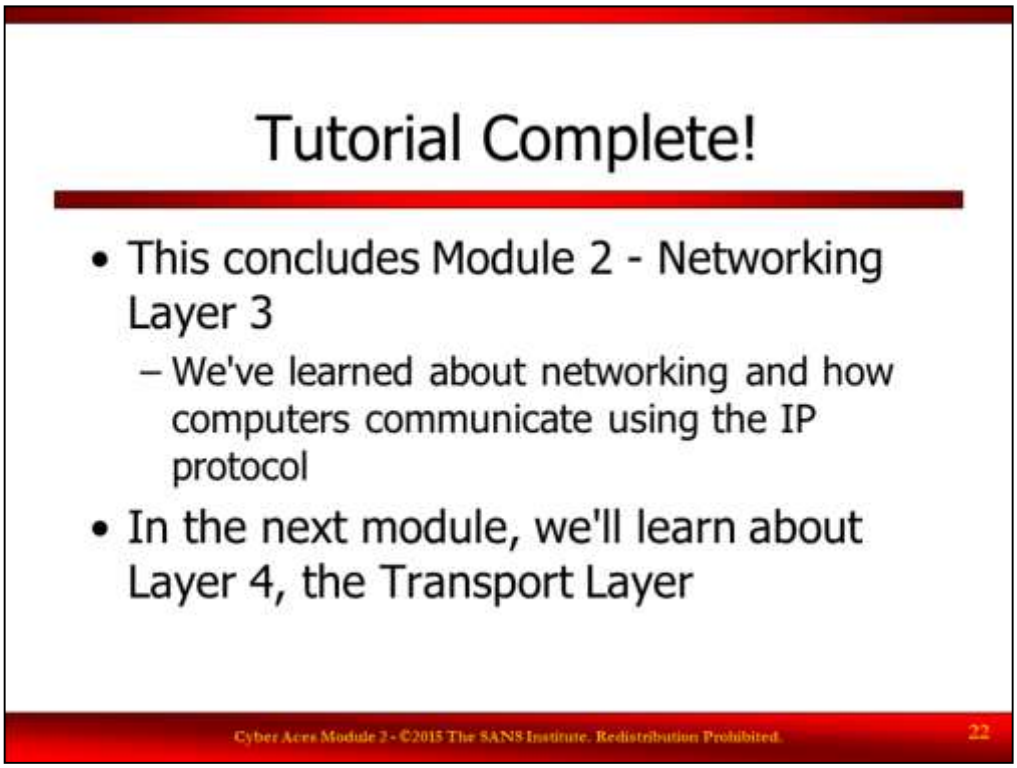
http://www.youtube.com/watch?v=7cK2bj1FpIs

Defending IP Spoofing Attacks:

https://www.youtube.com/watch?v=Mg5TLN1ELFk

Using ICMP to intercept communications:

http://packetheader.blogspot.com/2010/06/better-spoofing-of-icmp-host-redirect.html



Tutorial Complete

This concludes the discussion about Layer 3, the Network Layer. In the next tutorial we'll discuss the next layer in the OSI model, the Transport Layer.