



CompTIA Network+® Lab Series Network Concepts

Lab 12: TCP/IP Protocols - The Core Protocols

Objective 1.1: TCP/IP Model

Objective 1.6: Explain the function of common networking protocols

Document Version: 2015-09-18



This work by the National Information Security and Geospatial Technologies Consortium (NISGTC), and except where otherwise noted, is licensed under the [Creative Commons Attribution 3.0 Unported License](https://creativecommons.org/licenses/by/3.0/).

Development was funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48; The National Information Security, Geospatial Technologies Consortium (NISGTC) is an entity of Collin College of Texas, Bellevue College of Washington, Bunker Hill Community College of Massachusetts, Del Mar College of Texas, Moraine Valley Community College of Illinois, Rio Salado College of Arizona, and Salt Lake Community College of Utah.

This workforce solution was funded by a grant awarded by the U.S. Department of Labor's Employment and Training Administration. The solution was created by the grantee and does not necessarily reflect the official position of the U.S. Department of Labor. The Department of Labor makes no guarantees, warranties or assurances of any kind, express or implied, with respect to such information, including any information on linked sites, and including, but not limited to accuracy of the information or its completeness, timeliness, usefulness, adequacy, continued availability or ownership.



Contents

1	Use Network Utilities and Protocols from the TCP/IP suite	7
1.1	Using ipconfig to Locate and Document your TCP/IP Settings	7
1.2	Using ping to Verify Network Layer Connectivity	8
2	Using the arp Command to Inspect and Clear the Cache Created by the ARP Protocol.....	10
2.1	Use the arp Command to View and Clear the arp Cache	10
3	Use a Network Packet Analyzer: Wireshark to Examine the ARP Protocol.....	11
3.1	Launching and Configuring Wireshark	11
3.2	Examining the ARP Protocol Using Wireshark	12
3.3	Review Questions.....	15
4	Capture and Analyze Transport Layer Protocol Packets.....	16
4.1	Capture and Analyze TCP Session Establishment and Data Segment Exchange	16
4.2	Capture and Analyze a UDP Datagram.....	18
4.3	Review Questions.....	19



Introduction

This lab is part of a series of lab exercises designed to supplement coursework and provide students with a hands-on training experience based on real world applications. This series of lab exercises is intended to support courseware for CompTIA Network+® certification.

This lab will review protocols that operate at the internetwork and transport layers of TCP/IP. These protocols are internetwork layer protocols such as ARP, ICMP, and IP and at the transport layer, UDP and TCP. Students will review IP address configuration, discover facts about network communication using ICMP and the ping utility and will examine the TCP/IP layers and become familiar with their status and function on a network.

This lab includes the following tasks:

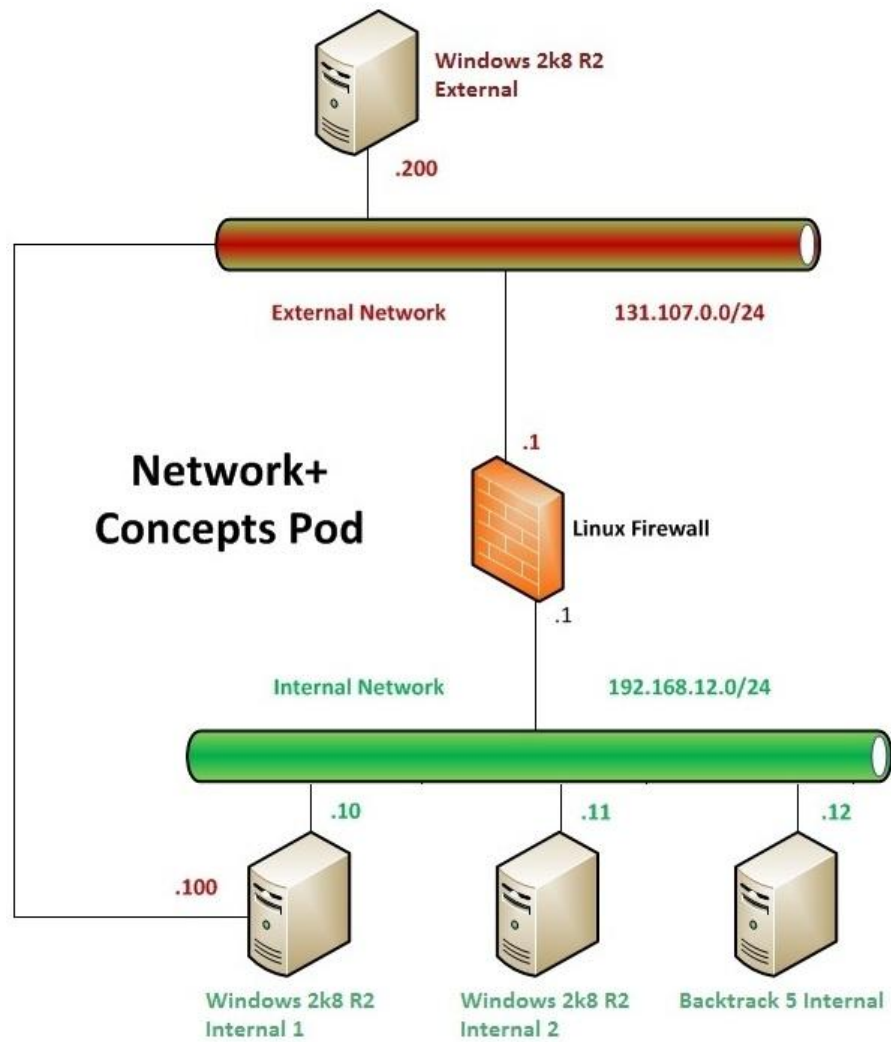
1. Use Network Utilities and Protocols from the TCP/IP suite
2. Use a network packet analyzer: Wireshark® to examine the ARP protocol
3. Capture and Analyze Transport Layer Packets

Objective: Reviewing TCP/IP Protocols

The objectives of this lab are:

- Reinforce understanding of certain protocols in the TCP/IP protocol suite such as ARP and ICMP.
- Demonstrate the usage of a packet sniffer tool, Wireshark, to capture and examine a packet trace.
- Gain insight into the operations TCP and UDP.

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

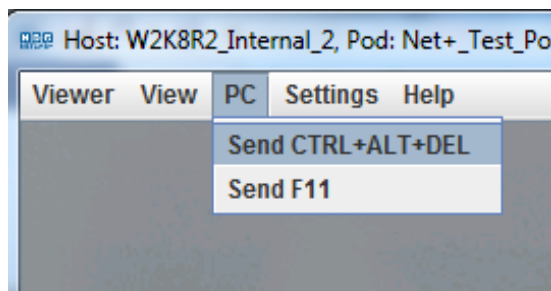
Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

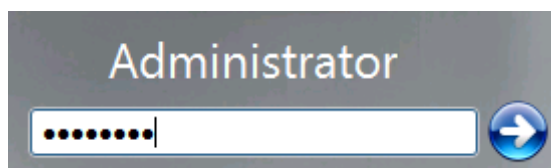
Windows 2k8 R2 Internal 1	192.168.12.10
Windows 2k8 R2 Internal 1 password	P@ssw0rd
Windows 2k8 R2 Internal 2	192.168.12.11
Windows 2k8 R2 Internal 2 password	P@ssw0rd

Windows 2k8 R2 Login (applies to all Windows machines)

1. Click on the Windows 2k8 R2 icon on the topology that corresponds to the machine you wish to log in to.
2. Use the PC menu in the NETLAB+ Remote PC Viewer to send a **Ctrl-Alt-Del** (version 2 viewer), or click the **Send Ctrl-Alt-Del** link in the bottom right corner of the viewer window (version 1 viewer).



3. In the password text box, type P@ssw0rd and press enter to log in.



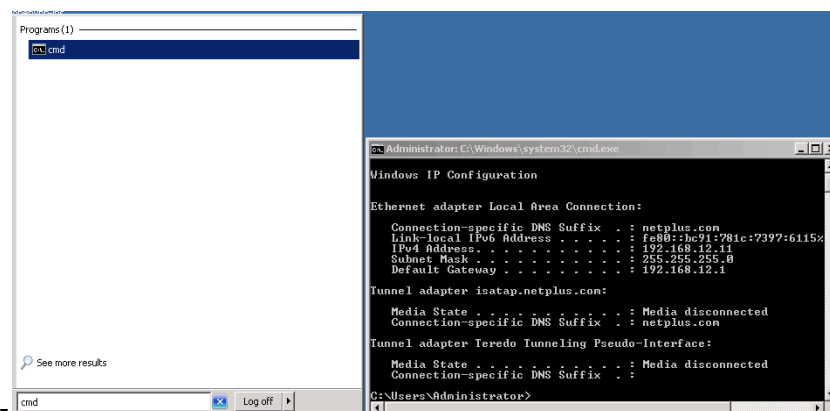
4. If the **Initial Configuration Tasks** and/or **Server Manager** windows appear, close them by clicking on the "X" in the top-right corner of the window.

1 Use Network Utilities and Protocols from the TCP/IP suite

The `ipconfig` command allows you to view your network configurations and to test communication with other computers. Used on its own, the `ipconfig` command shows basic information such as the name of the network interface, the IP address, the subnet mask, and the default gateway. Combined with the `/all` switch, it shows a detailed set of information about the TCP/IP settings. The `ipconfig` command lists the IP address configuration for your computer's network interfaces along with other network settings.

1.1 Using ipconfig to Locate and Document your TCP/IP Settings

1. Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 Internal 2 machine, if you are not logged in already.
2. Click on **Start**. In the **Search** dialog box, type **cmd** and press Enter to open the command prompt.
3. Type **ipconfig** at the prompt and press Enter. This will display a list of IP address configurations for your network adapter(s).



4. Type **ipconfig /all**, which will display more details about the IP address configuration. Under the heading "Ethernet adapter Local Area Connection" find the Physical Address, this is the MAC address of your NIC. Next, find the IPv4 Address and the Default Gateway. Record all three addresses in the table below for later use.

Windows 2k8 R2 Internal 2	
Physical Address (MAC address)	
IPv4 Address	
Default Gateway	

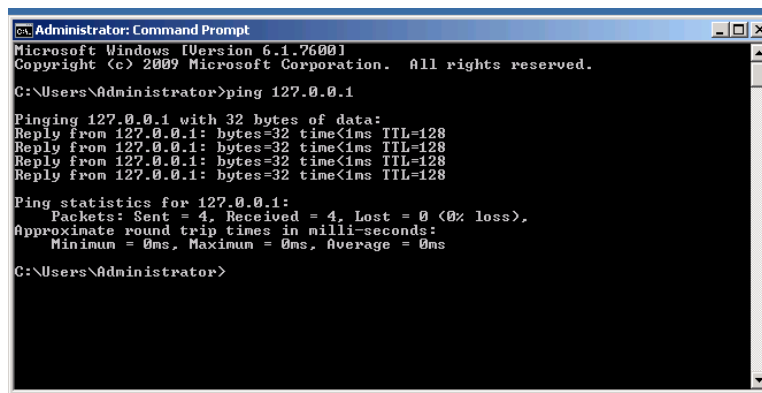
- Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 External machine, if you are not logged in already.
- Repeat Steps 2-4 and record the information for the Windows 2k8 R2 External machine in the table below.

Windows 2k8 R2 External	
Physical Address (MAC address)	
IPv4 Address	
Default Gateway	

1.2 Using ping to Verify Network Layer Connectivity

You will use the **ping** command to verify network layer connectivity and that the host computer can connect to the network resources. When using **ping**, the system sends an ICMP echo request to the target; this can be done using a host name or IP address. Ping can also be used to troubleshoot network problems and incompatible configurations. It is usually best to verify that a connection exists between the local computer and a network host by first using the **ping** command and the IP address of the network host to which you want to connect. In this task, you use ping to verify local host settings, network connectivity to the default gateway, and a remote host to see if it responds.

- On the Windows 2k8 R2 Internal 2 machine, click on **Start**. In the **Search** dialog box, type **cmd** and then press Enter to open the command prompt.
- At the prompt, type **ping 127.0.0.1** and press Enter. Pinging the loopback address will verify the TCP/IP socket on the local computer.



```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>

```

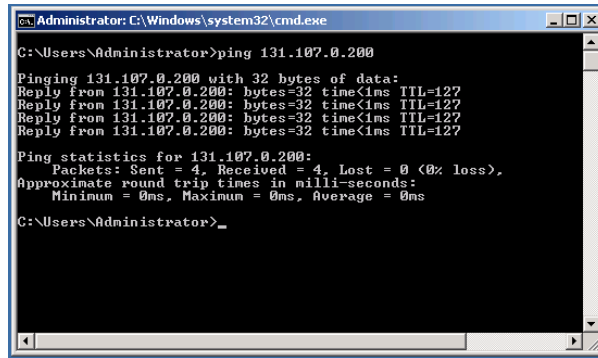
- Next, you will ping the IP address of the local host.

- What is the local host IP address?
- What is the reason for pinging this address?

4. Next, you will ping the IP address of the default gateway. This is one of the IP addresses recorded in the earlier exercise.

3. *What does pinging this IP address verify?*

5. Next, from the command prompt in the Windows 2k8 R2 Internal 2 machine, you will ping the ipv4 address of the Windows 2k8 R2 External machine recorded in 1.1 , Step 6, which is a remote host. Pinging this host will verify that you can communicate outside of your local network.



```

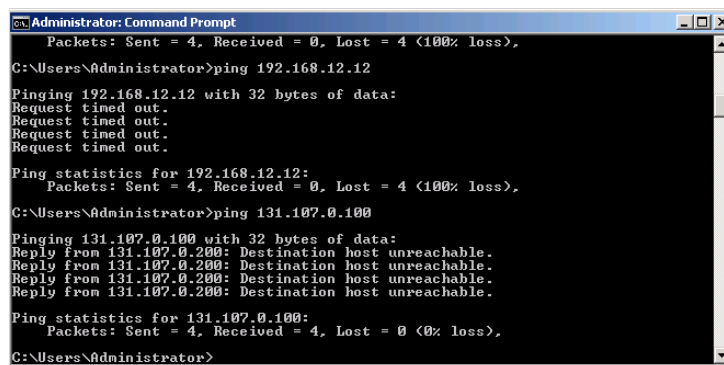
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 131.107.0.200

Pinging 131.107.0.200 with 32 bytes of data:
Reply from 131.107.0.200: bytes=32 time<1ms TTL=127
Reply from 131.107.0.200: bytes=32 time<1ms TTL=127
Reply from 131.107.0.200: bytes=32 time<1ms TTL=127
Reply from 131.107.0.200: bytes=32 time<1ms TTL=127

Ping statistics for 131.107.0.200:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
  
```

6. Log on to the Windows 2k8 R2 External machine and click on **Start**. In the **Search dialog box**, type **cmd** and press Enter to open the command prompt.
7. Ping the IP address of Windows 2k8 R2 Internal 2. Due to firewall settings and security reasons for not allowing external hosts to be able to access an internal network, the ping return will not be successful.



```

Administrator: Command Prompt
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>ping 192.168.12.12

Pinging 192.168.12.12 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.12.12:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>ping 131.107.0.100

Pinging 131.107.0.100 with 32 bytes of data:
Reply from 131.107.0.200: Destination host unreachable.
Reply from 131.107.0.200: Destination host unreachable.
Reply from 131.107.0.200: Destination host unreachable.
Reply from 131.107.0.200: Destination host unreachable.

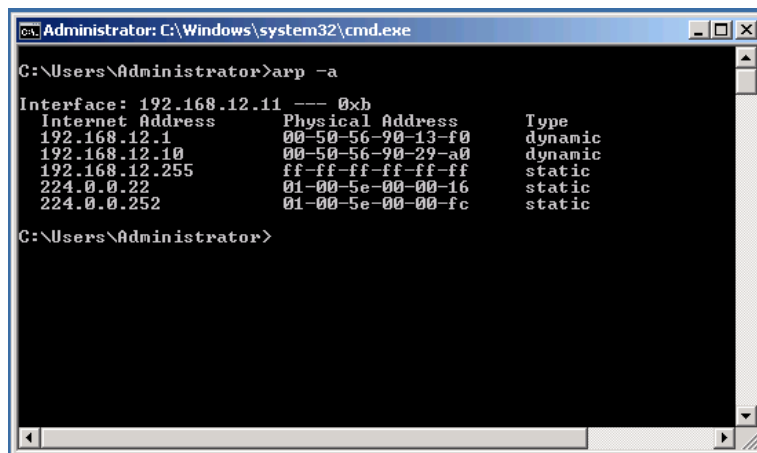
Ping statistics for 131.107.0.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\Administrator>
  
```

2 Using the arp Command to Inspect and Clear the Cache Created by the ARP Protocol.

In a previous lab exercise, you found the hardware address for your network adapter, the hardware address is also known as a MAC address. The ARP protocol typically maintains a cache of IP to MAC address mappings on the local computer. Remember all hosts must have both a MAC address and an IP address to communicate with other hosts. Given the IP address of a host, the ARP protocol can discover the MAC address of another host on the same physical network. ARP tables and caches are built by the protocol on each computer to maintain the mappings of IP to MAC address so repetitive ARP broadcast requests can be diminished. The **arp** command is used to view and manipulate the contents of the arp cache. The ARP protocol defines the message format and its meaning.

2.1 Use the arp Command to View and Clear the arp Cache

1. On the Windows 2k8 R2 Internal 2 machine, click on **Start**. in the **Search** dialog box, type **cmd** press Enter to open the command prompt.
2. At the prompt type **arp -a** (note there is a space between the p and the dash) and press Enter. The **arp -a** command displays the current contents of the ARP cache on your computer.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>arp -a
Interface: 192.168.12.11 --- 0xb
Internet Address      Physical Address      Type
192.168.12.1          00-50-56-90-13-f0     dynamic
192.168.12.10         00-50-56-90-29-a0     dynamic
192.168.12.255        ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
C:\Users\Administrator>
```

1. What is the meaning of each column of the ARP Cache?

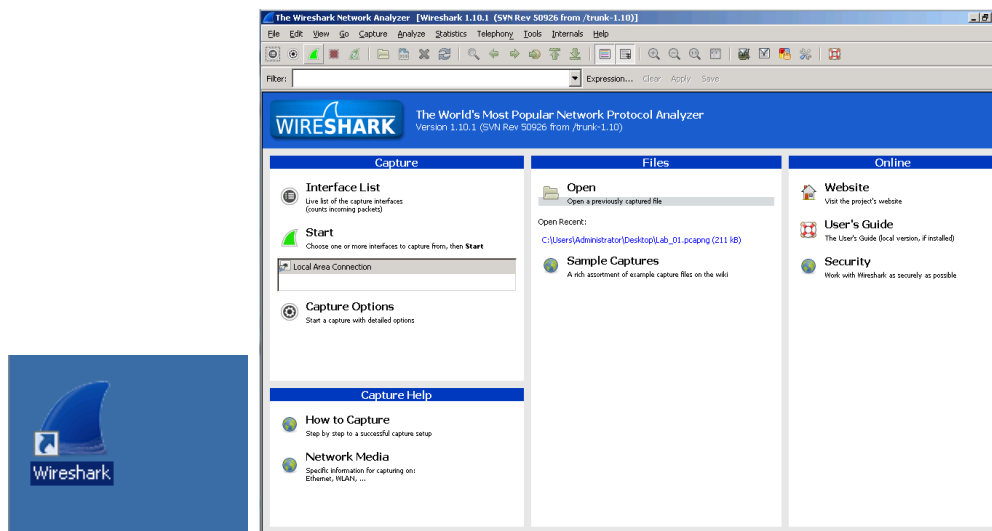
In order to observe your computer sending and receiving ARP messages, you will need to clear the ARP cache, otherwise your computer is likely to find a needed IP-Ethernet address translation pair in its cache and consequently not need to send out an ARP message. You will be using a network packet analyzer, Wireshark, to observe ARP.

3 Use a Network Packet Analyzer: Wireshark to Examine the ARP Protocol

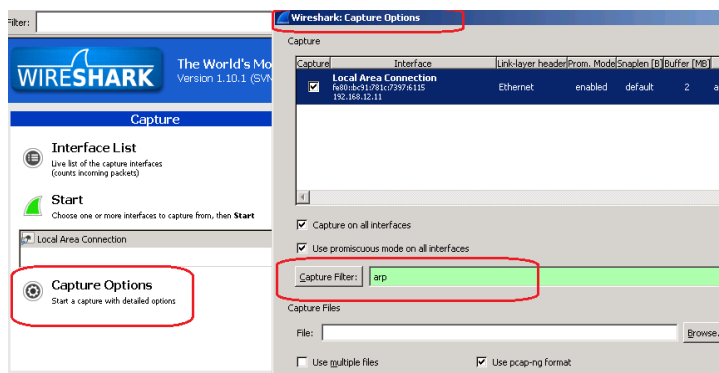
Wireshark is a network packet analyzer that captures packets and allows you to examine their contents. A network packet analyzer will capture network packets and display that packet data as detailed as possible. In this task, you will use Wireshark to capture ARP packets and examine operation of the protocol.

3.1 Launching and Configuring Wireshark

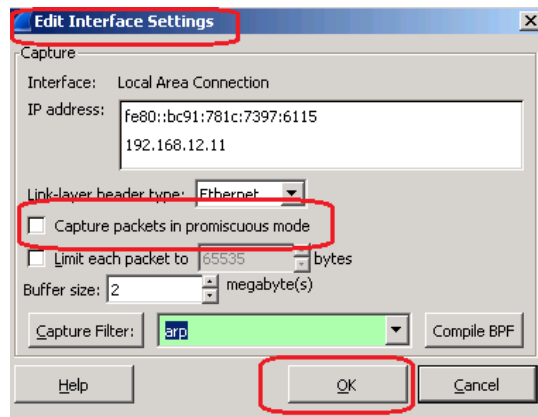
1. Use the instructions provided in the Lab Settings section to log into the Windows 2k8 R2 Internal 2 machine, if you are not logged in already.
2. On the desktop, double-click the Wireshark icon to launch the program.



3. Click on Capture Options on the main page of Wireshark and in the Capture Filter dialog box, type **arp**. (must be lower case) The capture filter is set to **arp** to prevent the capture of other traffic your computer may send or receive for easier tracking of ARP packets.
4. Next, double-click on the Local Area Connection.



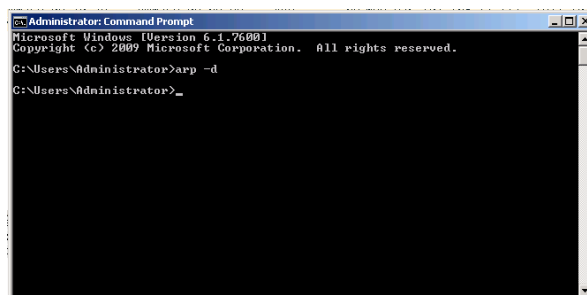
- On the **Edit Interface Settings** page, uncheck **Capture Packets** in promiscuous mode. This mode is useful to allow your system to listen to packets sent to/from other computers on broadcast networks, but in this case, you only want to record packets sent to/from your computer. Leave other options at their default values. Click OK.



- Next, click the **Start** button at the bottom-right corner of the **Capture Options** page to start the capture. From the Windows 2K8R2 Internal 2 machine ping Windows 2K8R2 Internal 1 machine.

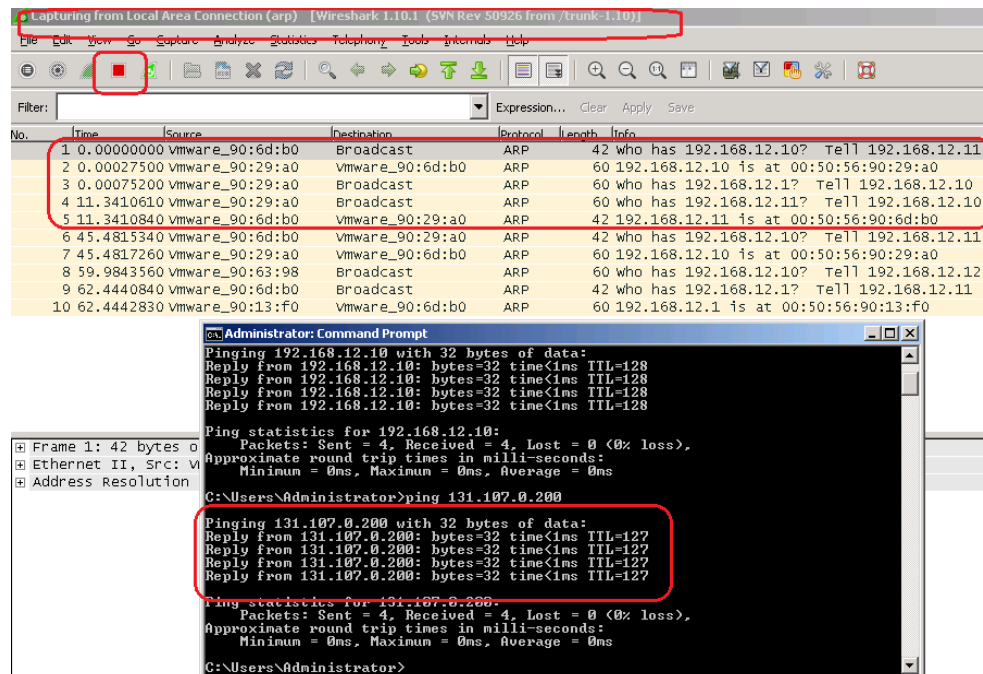
3.2 Examining the ARP Protocol Using Wireshark

- On the W2K8R2 Internal 2 machine, click on **Start** and in the **Search** dialog box, type **cmd** press Enter to open the command prompt.
- Type the command, **arp -a** to view the current entries in the ARP cache.
- Type the command, **arp -d** to clear the arp cache. If you do not clear the cache, the stored ARP records will prevent the system from needing to send ARP request to map the IP address to MAC addresses on local machines because they will already exist.

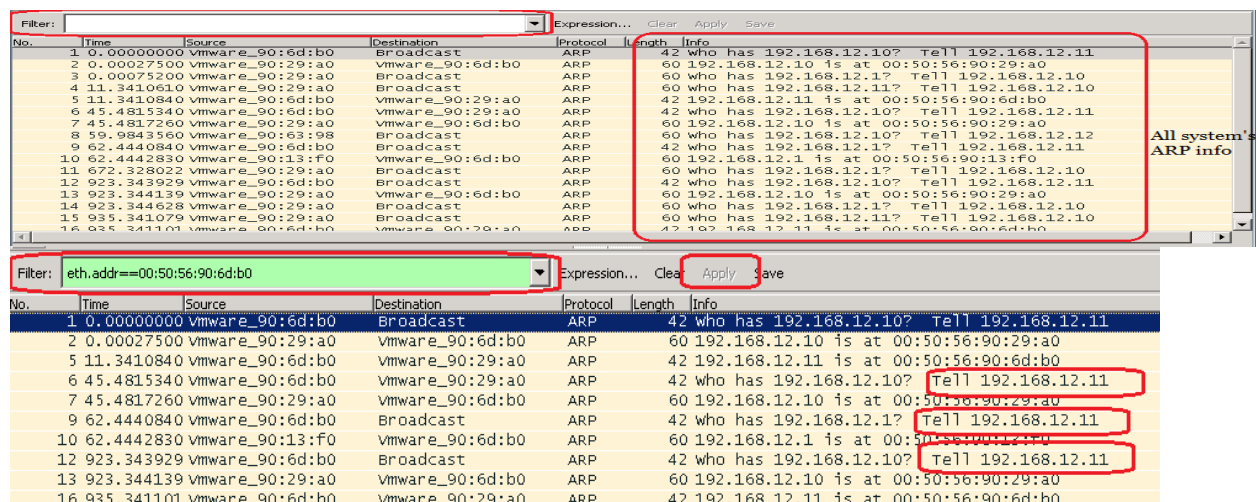


- Ping the Windows 2k8 R2 Internal 1 machine and the Windows 2k8 R2 External machine. This will force the system to send ARP messages other systems on your local network and you will be able to capture the packets to examine the ARP traffic. Watch the Wireshark program as it captures packets

- Click the red square to stop the capture when you see the ARP traffic showing up in Wireshark.



- Back on the Windows 2k8 R2 Internal 2 machine, in the open command prompt window, type **ipconfig /all** to view the MAC address of the system and IP address of the default gateway.
- To make it easier to view ARP requests that originate from your computer or are destined to your computer, create another filter. To do this, near the top of the main page, click in the Filter text input area and add a filter that will show only captures for your system. An example of the filter syntax is: **eth.addr==01:02:03:04:05:06**. Then click Apply.



Now you will examine the ARP packets for the default gateway. ARP uses two types of packets, the request packet and the reply packet. You will examine both types. Refer to step 6, where you recorded the default gateway IP address information. Review the filtered captures in Wireshark, to find one that is an **ARP request** for the default gateway. ARP requests will start with 'Who has xxx.xxx.xxx.xxx so you will look for the one that has the IP address of the default gateway.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
2	0.00027500	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
5	11.3410840	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0
6	45.4815340	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
7	45.4817260	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
9	62.4440840	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.1? Tell 192.168.12.11
10	62.4442830	Vmware_90:13:f0	Vmware_90:6d:b0	ARP	60	192.168.12.1 is at 00:50:56:90:13:f0
12	923.343929	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
13	923.344139	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
16	935.341101	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0

On the Wireshark capture window, there are three panes. The top pane is the summary information for each capture; the middle pane is detailed information about the highlighted captured packet. The lower pane is the packets byte pane and shows the packet information in hexadecimal.

8. In the top pane, look for an ARP request for the default gateway and select it. Then, click on the + sign next to Address Resolution Protocol (request) in the middle pane to expand it and examine the field details of the ARP request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
2	0.00027500	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
5	11.3410840	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0
6	45.4815340	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
7	45.4817260	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
9	62.4440840	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.1? Tell 192.168.12.11
10	62.4442830	Vmware_90:13:f0	Vmware_90:6d:b0	ARP	60	192.168.12.1 is at 00:50:56:90:13:f0
12	923.343929	Vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
13	923.344139	Vmware_90:29:a0	Vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
16	935.341101	Vmware_90:6d:b0	Vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0

Frame 9: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0						
Ethernet II, Src: Vmware_90:6d:b0 (00:50:56:90:6d:b0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
Address Resolution Protocol (request)						
Hardware type: Ethernet (1)						
Protocol type: IP (0x0800)						
Hardware size: 6						
Protocol size: 4						
Opcode: request (1)						
Sender MAC address: Vmware_90:6d:b0 (00:50:56:90:6d:b0)						
Sender IP address: 192.168.12.11 (192.168.12.11)						
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)						
Target IP address: 192.168.12.1 (192.168.12.1)						

Now you will examine an ARP reply packet. The ARP reply will be a response to the request and will have the sender and target information reversed. The reply will be answering the question, Who has xxx.xxx.xxx.xxx with the original target's IP address 'at' the physical address (MAC) location?

In the top pane, look for an **ARP reply** from the default gateway and select it. Click on the + sign next to Address Resolution Protocol (reply) in the middle pane to expand it and examine the field details of the ARP reply.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
2	0.00027500	vmware_90:29:a0	vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
5	11.3410840	vmware_90:6d:b0	vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0
6	45.4815340	vmware_90:6d:b0	vmware_90:29:a0	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
7	45.4817260	vmware_90:29:a0	vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
9	62.4440840	vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.1? Tell 192.168.12.11
10	62.4442830	vmware_90:13:f0	vmware_90:6d:b0	ARP	60	192.168.12.1 is at 00:50:56:90:13:f0
12	923.343929	vmware_90:6d:b0	Broadcast	ARP	42	who has 192.168.12.10? Tell 192.168.12.11
13	923.344139	vmware_90:29:a0	vmware_90:6d:b0	ARP	60	192.168.12.10 is at 00:50:56:90:29:a0
16	935.341101	vmware_90:6d:b0	vmware_90:29:a0	ARP	42	192.168.12.11 is at 00:50:56:90:6d:b0

Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 Ethernet II, Src: vmware_90:13:f0 (00:50:56:90:13:f0), Dst: vmware_90:6d:b0 (00:50:56:90:6d:b0)
 Address Resolution Protocol (reply)
 Hardware type: Ethernet (1)
 Protocol type: IP (0x0800)
 Hardware size: 6
 Protocol size: 4
 opcode: reply (2)
 Sender MAC address: vmware_90:13:f0 (00:50:56:90:13:f0)
 Sender IP address: 192.168.12.1 (192.168.12.1)
 Target MAC address: vmware_90:6d:b0 (00:50:56:90:6d:b0)
 Target IP address: 192.168.12.11 (192.168.12.11)

9. Close Wireshark.

3.3 Review Questions

1. What is the opcode for an ARP request?
2. What is the opcode for an ARP reply?
3. What type of packet is an ARP request?
4. Why would an ARP frame have a destination MAC address of 00:00:00:00:00:00?
5. What type of packet is an ARP reply?

4 Capture and Analyze Transport Layer Protocol Packets

In this task, you examine both TCP and UDP packets. These are *transport layer protocols*. TCP provides guarantees in its delivery and it creates a point-to-point connection between two hosts. Using a three-way handshake, TCP establishes a session between two hosts. Once the session is established, the hosts can exchange data, then when the session is finished, TCP closes the session. TCP takes the messages being exchanged between the hosts, disassembles and reassembles them using sequential numbering and acknowledgement of receipt of the data segment. TCP segments are encapsulated into an IP datagram.

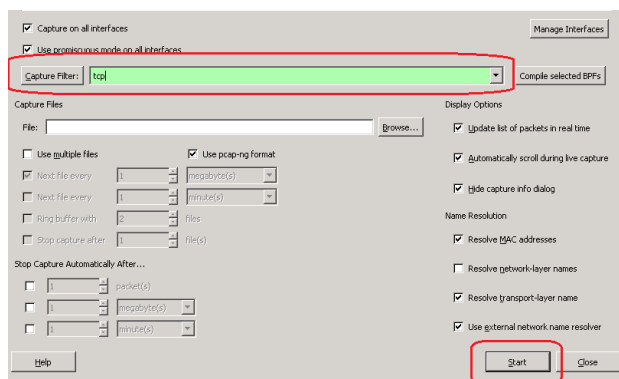
4.1 Capture and Analyze TCP Session Establishment and Data Segment Exchange

TCP uses specific program ports for data delivery and the pairing of IP address and TCP ports allows TCP to manage multiple connections. TCP ports include FTP (20,21), Telnet (23), and Web Services- http (80). In this task, you will use Wireshark to capture a series of TCP segments and examine the three-way handshake, acknowledgements, and the termination of the session.

1. Log on to the Windows 2k8 R2 Internal 2 and Windows 2k8 R2 External machines, using the instructions provided in the Lab Settings section, if you are not logged in already to these machines.
2. On the desktop of the Windows 2k8 R2 Internal 2 machine, double-click the **Wireshark** icon to launch the program.



3. Click on Capture Options on the main page of Wireshark and in the Capture Filter dialog box, type **tcp**. (must be lower case). Click the **Start** button.



- Click on the icon for Windows Internet Explorer and open your Browser. Wait a minute or so to allow Wireshark time to capture packets, and then press Stop.

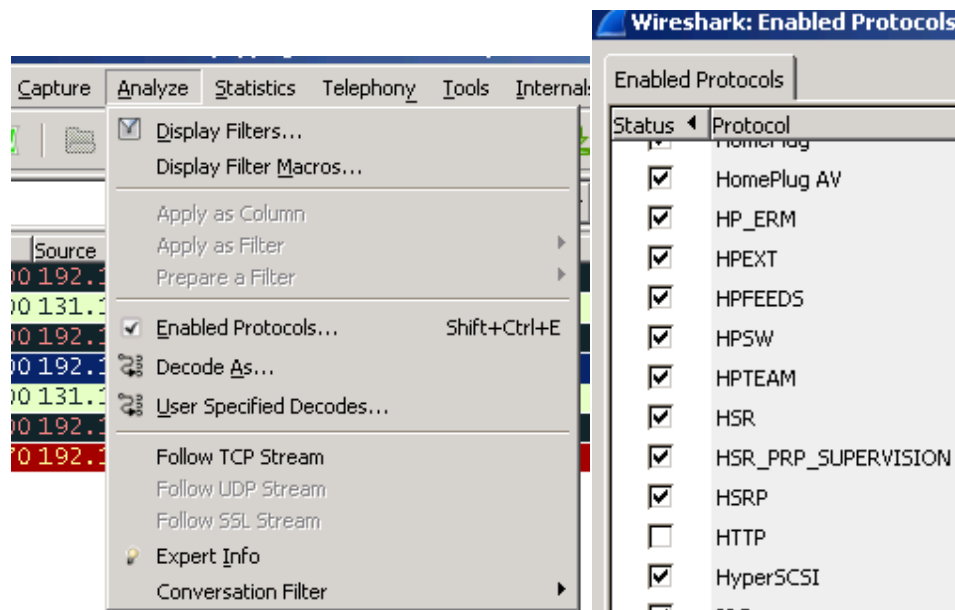
No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.12.11	131.107.0.200	TCP	66	mtqp > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_
2	0.00025900	131.107.0.200	192.168.12.11	TCP	66	http > mtqp [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
3	0.00028000	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [ACK] Seq=1 Ack=1 win=65700 Len=0
4	0.00087300	192.168.12.11	131.107.0.200	HTTP	529	GET / HTTP/1.1
5	0.00167200	131.107.0.200	192.168.12.11	HTTP	242	HTTP/1.1 304 Not Modified
6	0.23650600	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [ACK] Seq=476 Ack=189 win=65512 Len=0
7	65.0024370	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [RST, ACK] Seq=476 Ack=189 win=0 Len=0

Frame 4: 529 bytes on wire (4232 bits), 529 bytes captured (4232 bits) on interface 0					
Ethernet II, Src: Vmware_90:6d:b0 (00:50:56:90:6d:b0), Dst: Vmware_90:13:f0 (00:50:56:90:13:f0)					
Internet Protocol Version 4, Src: 192.168.12.11 (192.168.12.11), Dst: 131.107.0.200 (131.107.0.200)					
Transmission Control Protocol, Src Port: mtqp (1038), Dst Port: http (80), Seq: 1, Ack: 1, Len: 475					
Hypertext Transfer Protocol					

You will use the captured packets to examine the TCP protocol operation. You can see the initial three-way handshake containing a TCP SYN message and a returning TCP SYN/ACK from the web server and the final ACK from the client.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.12.11	131.107.0.200	TCP	66	mtqp > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_
2	0.00025900	131.107.0.200	192.168.12.11	TCP	66	http > mtqp [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
3	0.00028000	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [ACK] Seq=1 Ack=1 win=65700 Len=0

- Select **Analyze -> Enabled Protocols** and scroll down to HTTP and uncheck the box then click OK. That will remove all the HTTP packet captures from the top pane so you can focus on the just the TCP segments.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.12.11	131.107.0.200	TCP	66	mtqp > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_
2	0.00025900	131.107.0.200	192.168.12.11	TCP	66	http > mtqp [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460
3	0.00028000	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [ACK] Seq=1 Ack=1 win=65700 Len=0
4	0.00087300	192.168.12.11	131.107.0.200	TCP	529	mtqp > http [PSH, ACK] Seq=1 Ack=1 win=65700 Len=475
5	0.00167200	131.107.0.200	192.168.12.11	TCP	242	http > mtqp [PSH, ACK] Seq=1 Ack=476 win=65536 Len=188
6	0.23650600	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [ACK] Seq=476 Ack=189 win=65512 Len=0
7	65.0024370	192.168.12.11	131.107.0.200	TCP	54	mtqp > http [RST, ACK] Seq=476 Ack=189 win=0 Len=0

6. In the top pane, highlight the first **TCP SYN**. Then **Click** on the **+ sign** next to Transmission Control Protocol in the middle pane to expand it and examine the field details of the TCP segment.
 1. *What is the IP address of the computer that initiated the HTTP session?*
 2. *What control bit must be on to initiate the three-way handshake?*
 3. *What is the destination port in the first TCP SYN?*
 4. *What identifies a segment as a FIN segment?*
7. Close Wireshark.

4.2 Capture and Analyze a UDP Datagram

Another transport layer protocol is UDP. UDP is used by some programs instead of TCP for fast, lightweight, unreliable transportation of data between hosts.

UDP provides connectionless datagrams that offer best-effort delivery, which means that UDP does not guarantee delivery or verify sequencing for any datagrams.

There are no SYNs or ACKs used by the UDP protocol so it does not know how to sequentially organize the reassembly of the data. The UDP protocol data unit is a datagram - not a segment.

1. Log on to the Windows 2k8 R2 Internal 2 and Windows 2k8 R2 External machines, using the instructions provided in the Lab Settings section, if you are not logged into the machines already. On the Windows 2k8 R2 Internal 2 machine desktop, double-click the **Wireshark** icon to launch the program.



2. Click on Capture Options on the main page of Wireshark and in the Capture Filter dialog box, type **udp** (must be lower case). Click the Start button.
3. Select **Analyze -> Enabled Protocols** and scroll down to DNS and uncheck the box then click OK. That will remove all the DNS packet captures from the top pane so you can focus on the just the UDP datagrams.
4. Select a datagram and view the UDP header. In the top pane, highlight any UDP datagram.
5. **Click** on the **+ sign** next to User Datagram Protocol in the middle pane to expand it and examine the field details.

4.3 Review Questions

1. *List the fields in a UDP header.*
2. *Describe the use of the source and destination ports in both UDP or TCP packets in a request for a service*
3. *Describe the use of the source and destination ports in both UDP or TCP packets in a response back to the client.*

