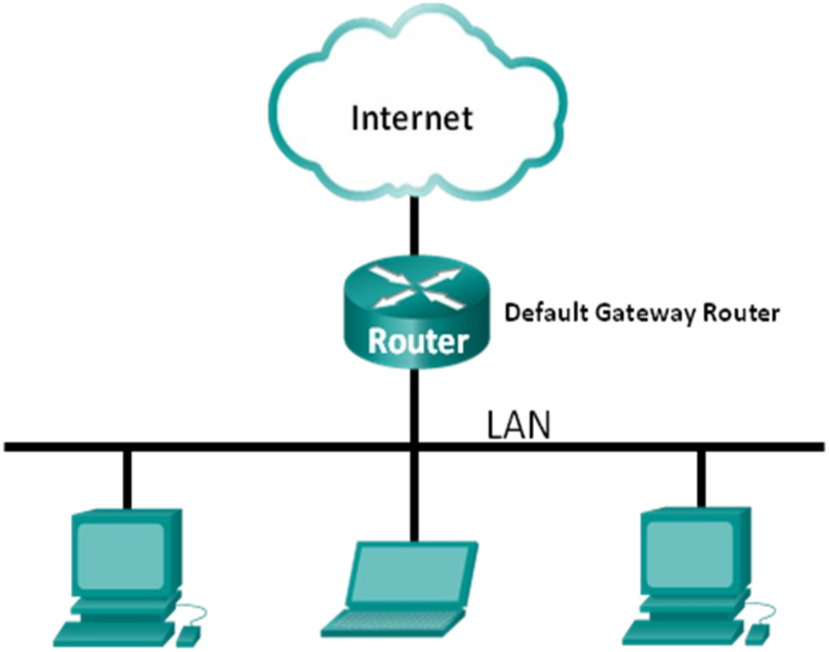
Week 3 Tutorial - Using Wireshark to View Network Traffic
(Instructor Version – Optional Lab)

Instructor Note: Red font color or gray highlights indicate text that appears in the instructor copy only. Optional activities are designed to enhance understanding and/or to provide additional practice.

Topology



Objectives

Part 1: Capture and Analyze Local ICMP Data in Wireshark

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

Background / Scenario

Wireshark is a software protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. As data streams travel back and forth over the network, the sniffer "captures" each protocol data unit (PDU) and can decode and analyze its content according to the appropriate RFC or other specifications.

Wireshark is a useful tool for anyone working with networks and can be used with most labs in the CCNA courses for data analysis and troubleshooting. In this lab, you will use Wireshark to capture ICMP data packet IP addresses and Ethernet frame MAC addresses.

Required Resources

- 1 PC (Windows 7 or 8 with Internet access)
- Additional PC(s) on a local-area network (LAN) will be used to reply to ping requests.

Instructor Note: This lab assumes that the student is using a PC with Internet access and can ping other PCs on the local area network.

Using a packet sniffer such as Wireshark may be considered a breach of the security policy of the school. It is recommended that permission is obtained before running Wireshark for this lab. If using a packet sniffer such as Wireshark is an issue, the instructor may wish to assign the lab as homework or perform a walk-through demonstration.

Part 1: Capture and Analyze Local ICMP Data in Wireshark

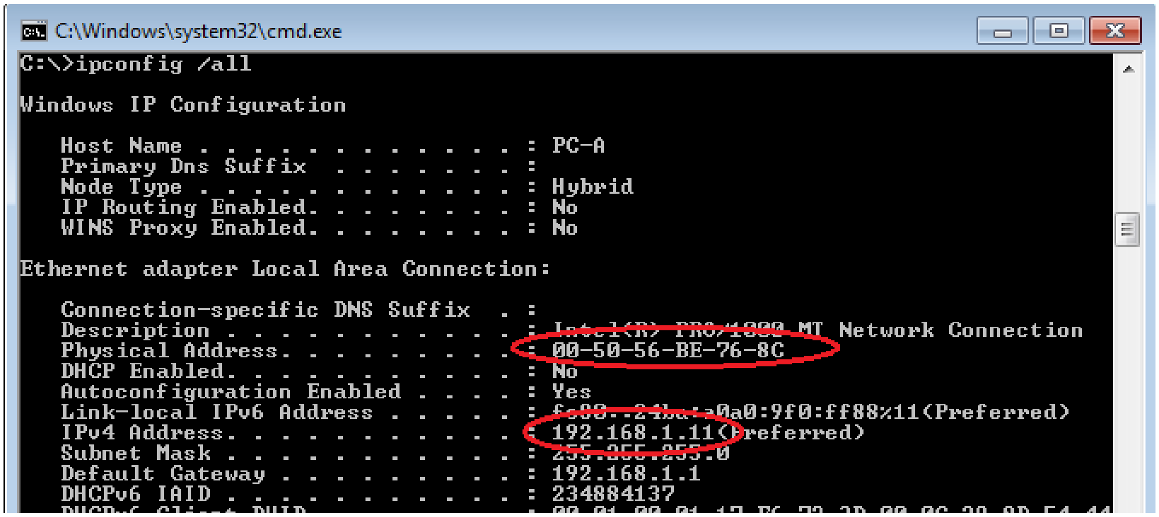
In Part 1 of this lab, you will ping another PC on the LAN and capture ICMP requests and replies in Wireshark. You will also look inside the frames captured for specific information. This analysis should help to clarify how packet headers are used to transport data to their destination.

Step 1: Retrieve your PC’s interface addresses.

For this lab, you will need to retrieve your PC’s IP address and its network interface card (NIC) physical address, also called the MAC address.

a. Open a command window, type **ipconfig /all**, and then press Enter.

b. Note your PC interface’s IP address and MAC (physical) address.



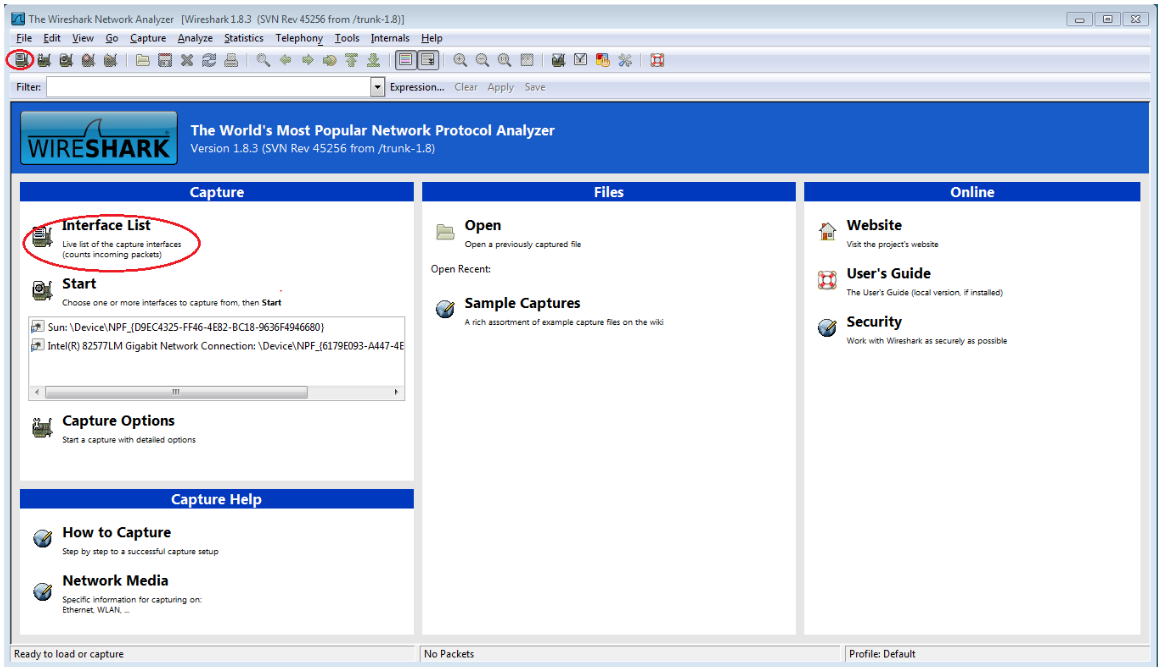
```
C:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : PC-A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-50-56-BE-76-8C
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::24ba:a0a0:9f0:ff88%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.11(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-17-F6-72-3D-00-0C-29-8D-E4-44
```

c. Ask a team member for their PC’s IP address and provide your PC’s IP address to them. Do not provide them with your MAC address at this time.

Step 2: Start Wireshark and begin capturing data.

a. On your PC, click the Windows **Start** button to see Wireshark listed as one of the programs on the pop-up menu. Double-click **Wireshark**.

b. After Wireshark starts, click **Interface List**.



The Wireshark Network Analyzer [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
Capture
Files
Online
Capture Help

The World's Most Popular Network Protocol Analyzer
Version 1.8.3 (SVN Rev 45256 from /trunk-1.8)

Interface List
Live list of the capture interfaces (counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

Sun: \Device\NPF_{D9EC4325-FF46-4E82-BC18-9636F4946680}
Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4E

Capture Options
Start a capture with detailed options

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

Website
Visit the project's website

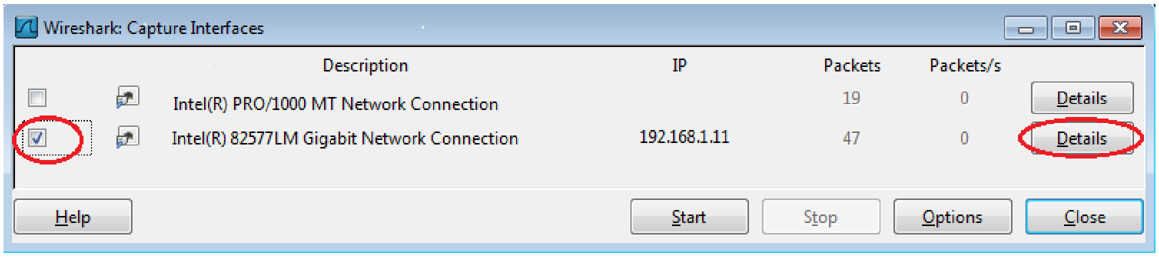
User's Guide
The User's Guide (local version, if installed)

Security
Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

Note: Clicking the first interface icon in the row of icons also opens the Interface List.

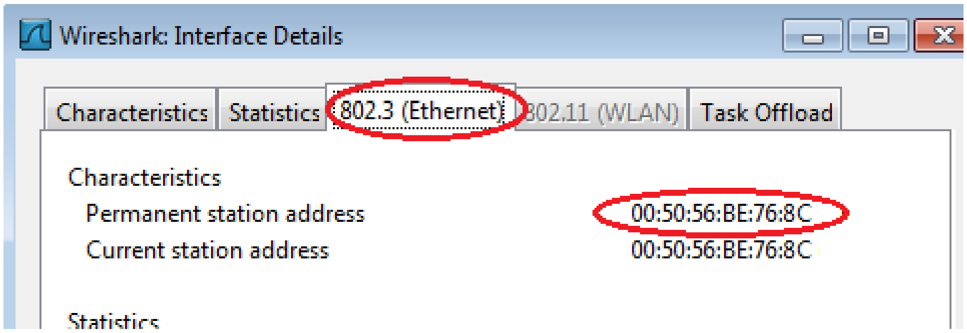
c. On the Wireshark: Capture Interfaces window, click the check box next to the interface connected to your LAN.



Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	
☐	Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details

Note: If multiple interfaces are listed and you are unsure which interface to check, click the **Details** button, and then click the **802.3 (Ethernet)** tab. Verify that the MAC address matches what you noted in Step 1b. Close the Interface Details window after verifying the correct interface.

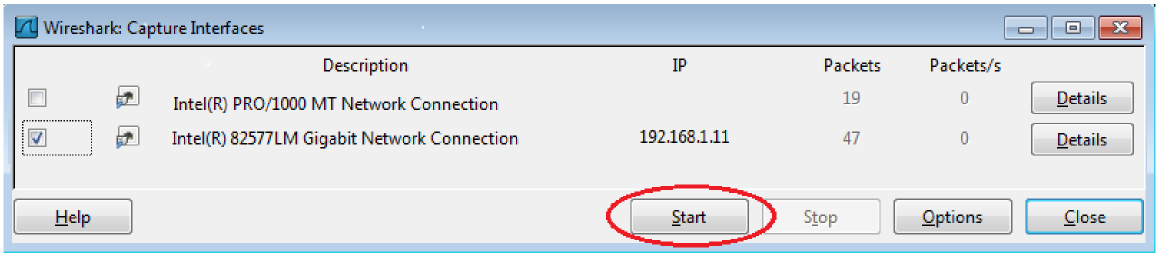


Wireshark: Interface Details

Characteristics
Permanent station address 00:50:56:BE:76:8C
Current station address 00:50:56:BE:76:8C

Statistics

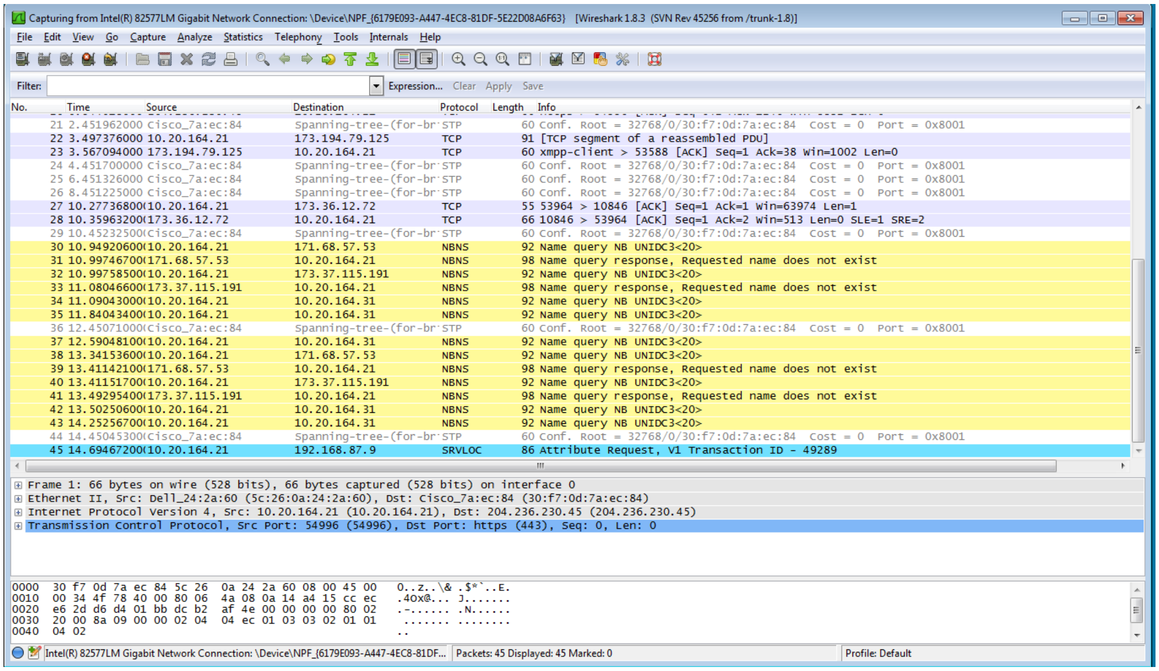
d. After you have checked the correct interface, click **Start** to start the data capture.



Wireshark: Capture Interfaces

		Description	IP	Packets	Packets/s	
□		Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑		Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details

Information will start scrolling down the top section in Wireshark. The data lines will appear in different colors based on protocol.



Capturing from Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63}   [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

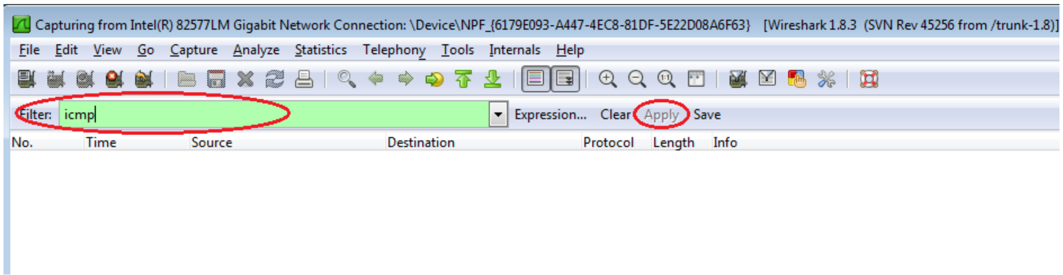
```
No.   Time         Source           Destination            Protocol Length Info
   21 2.451962000 Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   22 3.497376000 10.20.164.21     173.194.79.125        TCP     91 [TCP segment of a reassembled PDU]
   23 3.567094000 173.194.79.125   10.20.164.21          TCP     60 xmpp-client > 53588 [ACK] Seq=1 Ack=38 Win=1002 Len=0
   24 4.451700000 Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   25 6.451326000 Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   26 8.451225000 Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   27 10.27736800(10.20.164.21     173.36.12.72          TCP     55 53964 > 10846 [ACK] Seq=1 Ack=1 Win=63974 Len=1
   28 10.35963200(173.36.12.72     10.20.164.21          TCP     66 10846 > 53964 [ACK] Seq=1 Ack=2 Win=513 Len=0 SLE=1 SRE=2
   29 10.45232500(Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   30 10.94920600(10.20.164.21     171.68.57.53          NBNS    92 Name query NB UNIDC3<20>
   31 10.99746700(171.68.57.53     10.20.164.21          NBNS    98 Name query response, Requested name does not exist
   32 10.99758500(10.20.164.21     173.37.115.191        NBNS    92 Name query NB UNIDC3<20>
   33 11.08046600(173.37.115.191   10.20.164.21          NBNS    98 Name query response, Requested name does not exist
   34 11.09043000(10.20.164.21     10.20.164.31          NBNS    92 Name query NB UNIDC3<20>
   35 11.84043400(10.20.164.21     10.20.164.31          NBNS    92 Name query NB UNIDC3<20>
   36 12.45071000(Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   37 12.59048100(10.20.164.21     10.20.164.31          NBNS    92 Name query NB UNIDC3<20>
   38 13.34153600(10.20.164.21     171.68.57.53          NBNS    92 Name query NB UNIDC3<20>
   39 13.41142100(171.68.57.53     10.20.164.21          NBNS    98 Name query response, Requested name does not exist
   40 13.41151700(10.20.164.21     173.37.115.191        NBNS    92 Name query NB UNIDC3<20>
   41 13.49295400(173.37.115.191   10.20.164.21          NBNS    98 Name query response, Requested name does not exist
   42 13.50250600(10.20.164.21     10.20.164.31          NBNS    92 Name query NB UNIDC3<20>
   43 14.25256700(10.20.164.21     10.20.164.31          NBNS    92 Name query NB UNIDC3<20>
   44 14.45045300(Cisco_7a:ec:84   Spanning-tree-(for-br STP     60 Conf. Root = 32768/0/30:f7:0d:7a:ec:84  Cost = 0  Port = 0x8001
   45 14.69467200(10.20.164.21     192.168.87.9          SRVLOC  86 Attribute Request, V1 Transaction ID - 49289
```

```
⊞ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
⊞ Ethernet II, Src: Dell_24:2a:60 (5c:26:0a:24:2a:60), Dst: Cisco_7a:ec:84 (30:f7:0d:7a:ec:84)
⊞ Internet Protocol Version 4, Src: 10.20.164.21 (10.20.164.21), Dst: 204.236.230.45 (204.236.230.45)
⊞ Transmission Control Protocol, Src Port: 54996 (54996), Dst Port: https (443), Seq: 0, Len: 0
```

```
0000  30 f7 0d 7a ec 84 5c 26  0a 24 2a 60 08 00 45 00   0..z..\& .$*`..E.
0010  00 34 4f 78 40 00 80 06  4a 08 0a 14 a4 15 cc ec   .4Ox@... J.......
0020  e6 2d d6 d4 01 bb dc b2  af 4e 00 00 00 00 80 02   .-...... .N......
0030  20 00 8a 09 00 00 02 04  04 ec 01 03 03 02 01 01    ....... ........
0040  04 02                                              ..
```

Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF... | Packets: 45 Displayed: 45 Marked: 0 | Profile: Default

e. This information can scroll by very quickly depending on what communication is taking place between your PC and the LAN. We can apply a filter to make it easier to view and work with the data that is being captured by Wireshark. For this lab, we are only interested in displaying ICMP (ping) PDUs. Type **icmp** in the Filter box at the top of Wireshark and press Enter or click on the **Apply** button to view only ICMP (ping) PDUs.

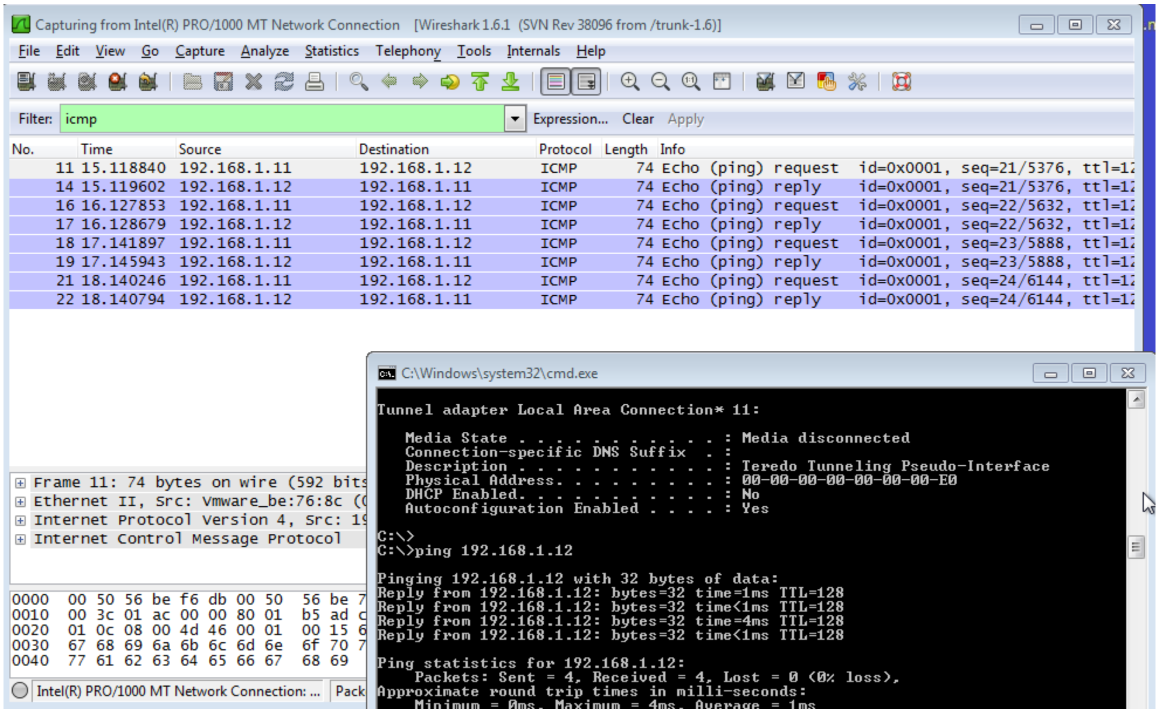


Capturing from Intel(R) 82577LM Gigabit Network Connection: \Device\NPF_{6179E093-A447-4EC8-81DF-5E22D08A6F63}   [Wireshark 1.8.3 (SVN Rev 45256 from /trunk-1.8)]

Filter: icmp

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info

f. This filter causes all data in the top window to disappear, but you are still capturing the traffic on the interface. Bring up the command prompt window that you opened earlier and ping the IP address that you received from your team member. Notice that you start seeing data appear in the top window of Wireshark again.


Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: icmp
Expression... Clear Apply
C:\Windows\system32\cmd.exe
Intel(R) PRO/1000 MT Network Connection: ...
Pack

```
No.   Time      Source         Destination    Protocol Length Info
   11 15.118840 192.168.1.11   192.168.1.12   ICMP         74 Echo (ping) request  id=0x0001, seq=21/5376, ttl=12
   14 15.119602 192.168.1.12   192.168.1.11   ICMP         74 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=12
   16 16.127853 192.168.1.11   192.168.1.12   ICMP         74 Echo (ping) request  id=0x0001, seq=22/5632, ttl=12
   17 16.128679 192.168.1.12   192.168.1.11   ICMP         74 Echo (ping) reply    id=0x0001, seq=22/5632, ttl=12
   18 17.141897 192.168.1.11   192.168.1.12   ICMP         74 Echo (ping) request  id=0x0001, seq=23/5888, ttl=12
   19 17.145943 192.168.1.12   192.168.1.11   ICMP         74 Echo (ping) reply    id=0x0001, seq=23/5888, ttl=12
   21 18.140246 192.168.1.11   192.168.1.12   ICMP         74 Echo (ping) request  id=0x0001, seq=24/6144, ttl=12
   22 18.140794 192.168.1.12   192.168.1.11   ICMP         74 Echo (ping) reply    id=0x0001, seq=24/6144, ttl=12
```

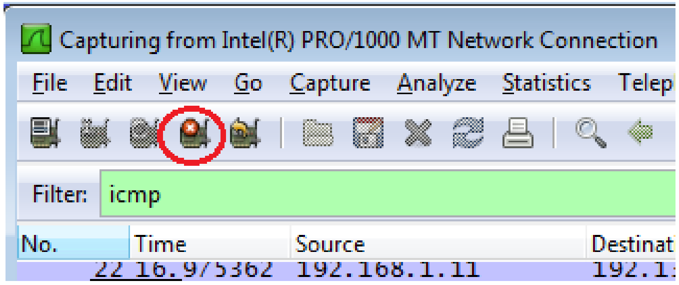
```
⊞ Frame 11: 74 bytes on wire (592 bits
⊞ Ethernet II, Src: Vmware_be:76:8c ((
⊞ Internet Protocol Version 4, Src: 19
⊞ Internet Control Message Protocol
```

```
0000  00 50 56 be f6 db 00 50  56 be 7
0010  00 3c 01 ac 00 00 80 01  b5 ad c
0020  01 0c 08 00 4d 46 00 01  00 15 6
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 7
0040  77 61 62 63 64 65 66 67  68 69
```

```
Tunnel adapter Local Area Connection* 11:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Teredo Tunneling Pseudo-Interface
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes

C:\>
C:\>ping 192.168.1.12

Pinging 192.168.1.12 with 32 bytes of data:
Reply from 192.168.1.12: bytes=32 time=1ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128
Reply from 192.168.1.12: bytes=32 time=4ms TTL=128
Reply from 192.168.1.12: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.12:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 4ms, Average = 1ms
```

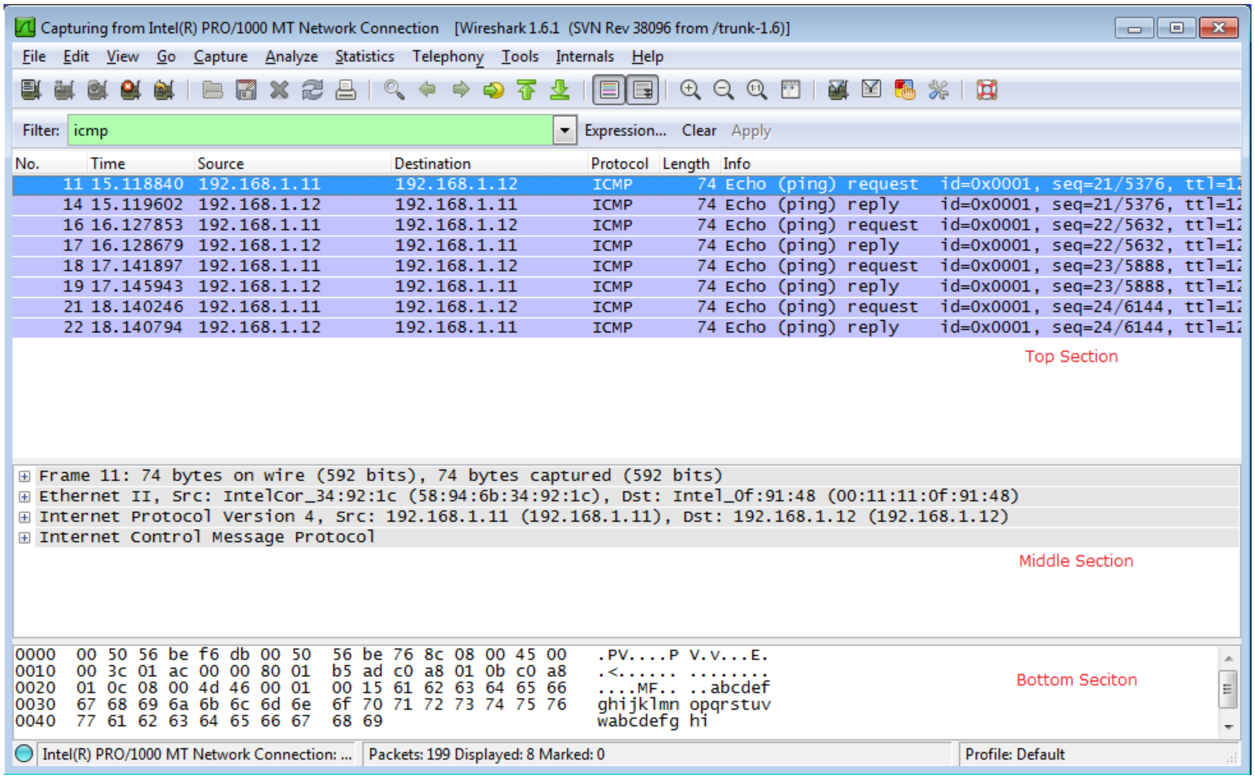
Note: If your team member’s PC does not reply to your pings, this may be because their PC firewall is blocking these requests. Please see **Appendix A: Allowing ICMP Traffic Through a Firewall** for information on how to allow ICMP traffic through the firewall using Windows 7.

g. Stop capturing data by clicking the **Stop Capture** icon.


Capturing from Intel(R) PRO/1000 MT Network Connection
File Edit View Go Capture Analyze Statistics Telep
Filter: icmp
No. Time Source Destinat
22 16.975362 192.168.1.11 192.1

Step 3: Examine the captured data.

In Step 3, examine the data that was generated by the ping requests of your team member’s PC. Wireshark data is displayed in three sections: 1) The top section displays the list of PDU frames captured with a summary of the IP packet information listed, 2) the middle section lists PDU information for the frame selected in the top part of the screen and separates a captured PDU frame by its protocol layers, and 3) the bottom section displays the raw data of each layer. The raw data is displayed in both hexadecimal and decimal form.


Capturing from Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply
Top Section
Middle Section
Bottom Seciton

Filter: icmp

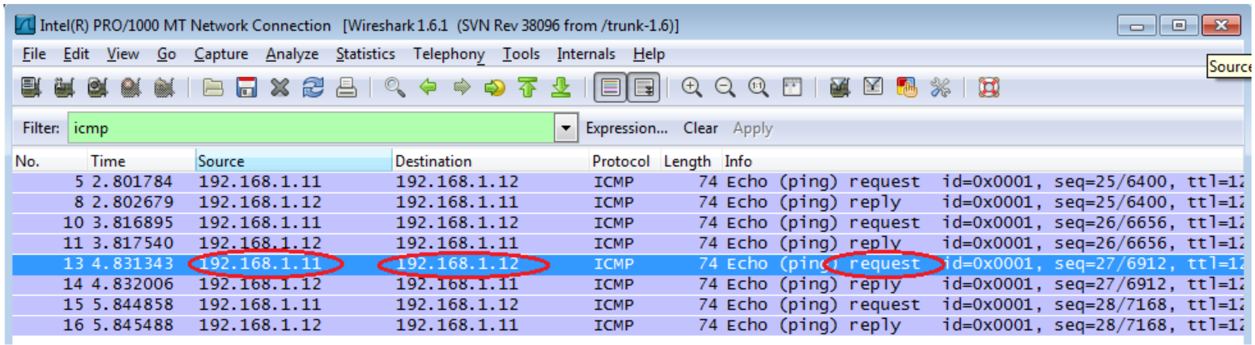
```
No.    Time        Source          Destination     Protocol Length Info
    11 15.118840  192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=21/5376, ttl=1
    14 15.119602  192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=21/5376, ttl=1
    16 16.127853  192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=22/5632, ttl=1
    17 16.128679  192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=22/5632, ttl=1
    18 17.141897  192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=23/5888, ttl=1
    19 17.145943  192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=23/5888, ttl=1
    21 18.140246  192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=24/6144, ttl=1
    22 18.140794  192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=24/6144, ttl=1
```

```
⊞ Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_0f:91:48 (00:11:11:0f:91:48)
⊞ Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)
⊞ Internet Control Message Protocol
```

```
0000  00 50 56 be f6 db 00 50  56 be 76 8c 08 00 45 00   .PV....P V.v...E.
0010  00 3c 01 ac 00 00 80 01  b5 ad c0 a8 01 0b c0 a8   .<...... ........
0020  01 0c 08 00 4d 46 00 01  00 15 61 62 63 64 65 66   ....MF.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Intel(R) PRO/1000 MT Network Connection: ... | Packets: 199 Displayed: 8 Marked: 0 | Profile: Default

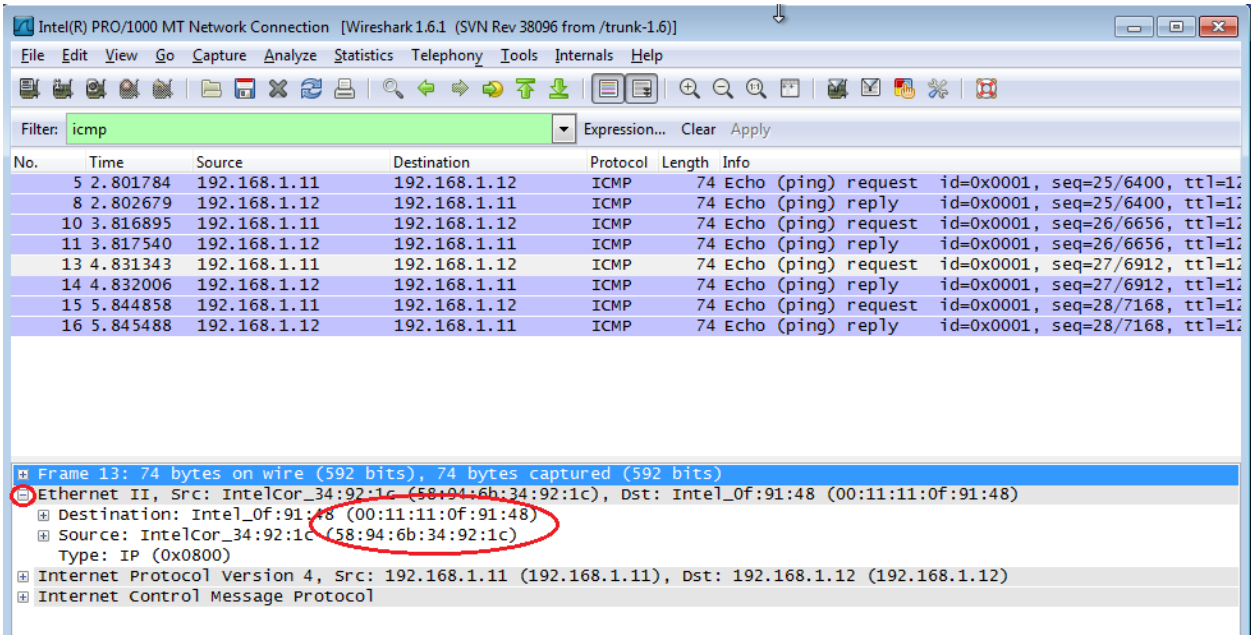
a. Click the first ICMP request PDU frames in the top section of Wireshark. Notice that the Source column has your PC’s IP address, and the Destination contains the IP address of the teammate’s PC you pinged.


Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Source
Expression... Clear Apply

Filter: icmp

```
No.    Time        Source          Destination     Protocol Length Info
     5 2.801784   192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=25/6400, ttl=1
     8 2.802679   192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=1
    10 3.816895   192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=26/6656, ttl=1
    11 3.817540   192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=1
    13 4.831343   192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=27/6912, ttl=1
    14 4.832006   192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=1
    15 5.844858   192.168.1.11    192.168.1.12    ICMP       74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=1
    16 5.845488   192.168.1.12    192.168.1.11    ICMP       74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=1
```

b. With this PDU frame still selected in the top section, navigate to the middle section. Click the plus sign to the left of the Ethernet II row to view the Destination and Source MAC addresses.


Intel(R) PRO/1000 MT Network Connection [Wireshark 1.6.1 (SVN Rev 38096 from /trunk-1.6)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: icmp

```
No.   Time      Source        Destination   Protocol Length Info
    5 2.801784  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=25/6400, ttl=1
    8 2.802679  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=25/6400, ttl=1
   10 3.816895  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=26/6656, ttl=1
   11 3.817540  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=26/6656, ttl=1
   13 4.831343  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=27/6912, ttl=1
   14 4.832006  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=27/6912, ttl=1
   15 5.844858  192.168.1.11  192.168.1.12  ICMP     74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=1
   16 5.845488  192.168.1.12  192.168.1.11  ICMP     74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=1

⊞ Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊟ Ethernet II, Src: IntelCor_34:92:1c (58:94:6b:34:92:1c), Dst: Intel_0f:91:48 (00:11:11:0f:91:48)
  ⊞ Destination: Intel_0f:91:48 (00:11:11:0f:91:48)
  ⊞ Source: IntelCor_34:92:1c (58:94:6b:34:92:1c)
    Type: IP (0x0800)
⊞ Internet Protocol Version 4, Src: 192.168.1.11 (192.168.1.11), Dst: 192.168.1.12 (192.168.1.12)
⊞ Internet Control Message Protocol
```

Does the Source MAC address match your PC's interface? ______ Yes

Does the Destination MAC address in Wireshark match your team member's MAC address?

_____ Yes

How is the MAC address of the pinged PC obtained by your PC?

____

The MAC address is obtained through an ARP request.

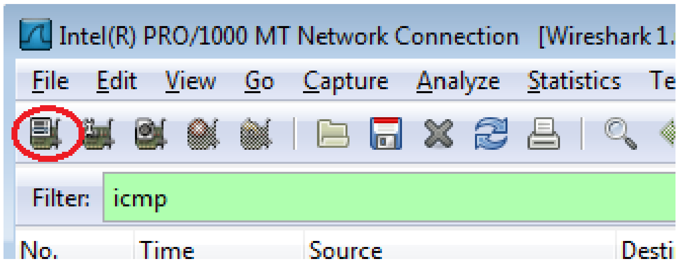
Note: In the preceding example of a captured ICMP request, ICMP data is encapsulated inside an IPv4 packet PDU (IPv4 header) which is then encapsulated in an Ethernet II frame PDU (Ethernet II header) for transmission on the LAN.

Part 2: Capture and Analyze Remote ICMP Data in Wireshark

In Part 2, you will ping remote hosts (hosts not on the LAN) and examine the generated data from those pings. You will then determine what is different about this data from the data examined in Part 1.

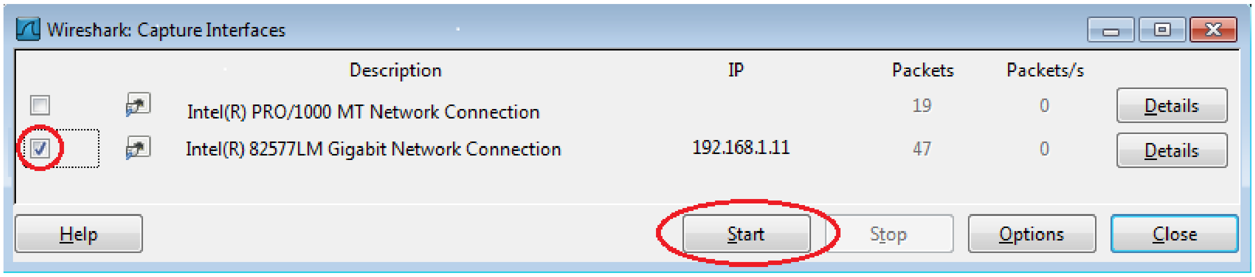
Step 1: Start capturing data on the interface.

a. Click the **Interface List** icon to bring up the list PC interfaces again.


Intel(R) PRO/1000 MT Network Connection [Wireshark 1.
File Edit View Go Capture Analyze Statistics Te
No. Time Source Desti

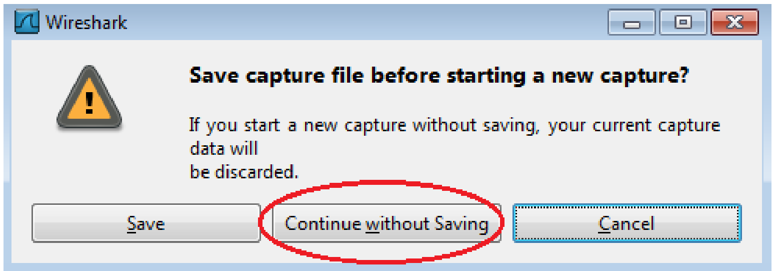
Filter: icmp

b. Make sure the check box next to the LAN interface is checked, and click **Start**.



	Description	IP	Packets	Packets/s	
□	Intel(R) PRO/1000 MT Network Connection		19	0	Details
☑	Intel(R) 82577LM Gigabit Network Connection	192.168.1.11	47	0	Details

c. A window prompts to save the previously captured data before starting another capture. It is not necessary to save this data. Click **Continue without Saving**.



Save capture file before starting a new capture?

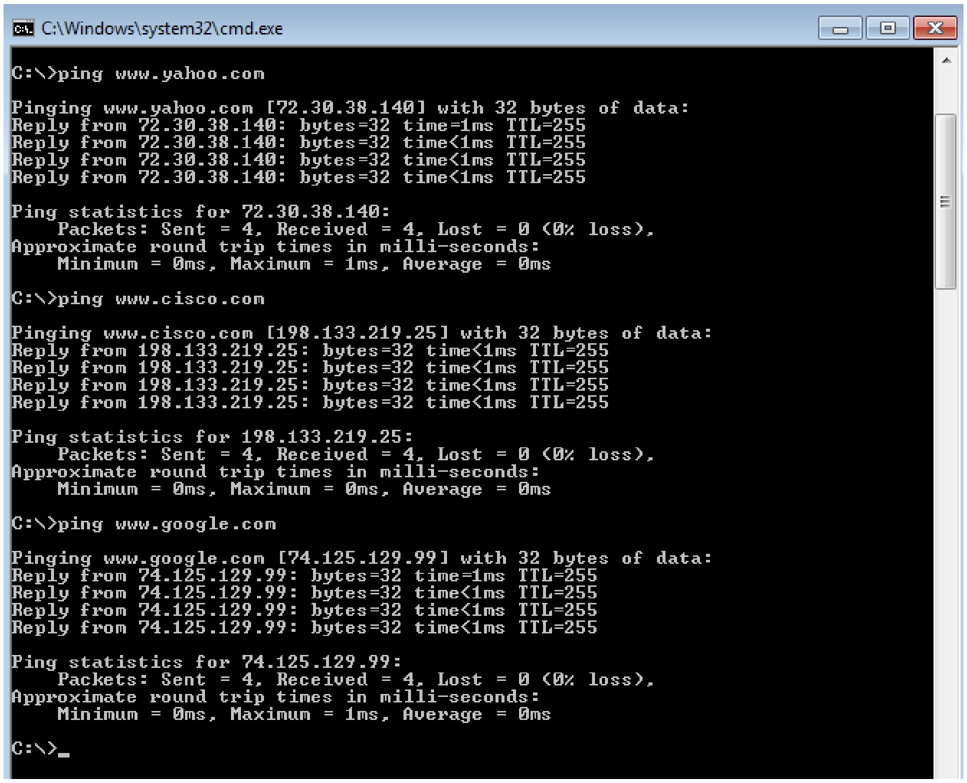
If you start a new capture without saving, your current capture data will
be discarded.

d. With the capture active, ping the following three website URLs:

1) www.yahoo.com

2) www.cisco.com

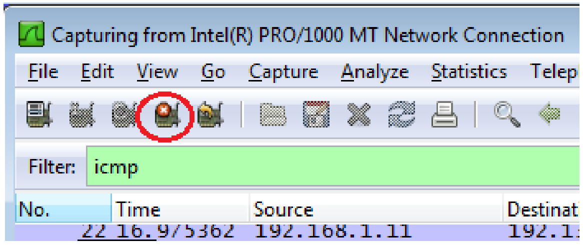
3) www.google.com



```
C:\>ping www.yahoo.com

Pinging www.yahoo.com [72.30.38.140] with 32 bytes of data:
Reply from 72.30.38.140: bytes=32 time=1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255
Reply from 72.30.38.140: bytes=32 time<1ms TTL=255

Ping statistics for 72.30.38.140:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping www.cisco.com

Pinging www.cisco.com [198.133.219.25] with 32 bytes of data:
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255
Reply from 198.133.219.25: bytes=32 time<1ms TTL=255

Ping statistics for 198.133.219.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping www.google.com

Pinging www.google.com [74.125.129.99] with 32 bytes of data:
Reply from 74.125.129.99: bytes=32 time=1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255
Reply from 74.125.129.99: bytes=32 time<1ms TTL=255

Ping statistics for 74.125.129.99:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>_
```

Note: When you ping the URLs listed, notice that the Domain Name Server (DNS) translates the URL to an IP address. Note the IP address received for each URL.

e. You can stop capturing data by clicking the **Stop Capture** icon.


Capturing from Intel(R) PRO/1000 MT Network Connection
File Edit View Go Capture Analyze Statistics Telep

Filter: icmp

No.	Time	Source	Destinat
22	16.975362	192.168.1.11	192.1

Step 2: Examining and analyzing the data from the remote hosts.

a. Review the captured data in Wireshark, examine the IP and MAC addresses of the three locations that you pinged. List the destination IP and MAC addresses for all three locations in the space provided.

1st Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

2nd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

3rd Location: IP: _____._____._____._____ MAC: ____:____:____:____:____:____

IP addresses: 72.30.38.140, 192.133.219.25, 74.125.129.99 (these IP addresses may vary)

MAC address: This will be the same for all three locations. It is the physical address of the router's default-gateway LAN interface.

b. What is significant about this information?

The MAC addresses for all three locations are the same.

c. How does this information differ from the local ping information you received in Part 1?

A ping to a local host returns the MAC address of the PC's NIC. A ping to a remote host returns the MAC address of the default gateway's LAN interface.

Reflection

Why does Wireshark show the actual MAC address of the local hosts, but not the actual MAC address for the remote hosts?

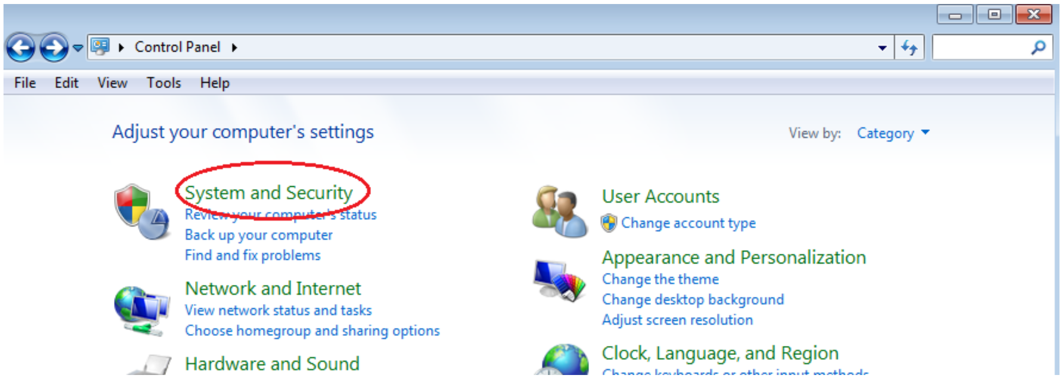
MAC addresses for remote hosts are not known on the local network, so the MAC address of the default-gateway is used. After the packet reaches the default-gateway router, the layer 2 information is stripped from the packet and a new Layer 2 header is attached with the destination MAC address of the next hop router.

Appendix A: Allowing ICMP Traffic Through a Firewall

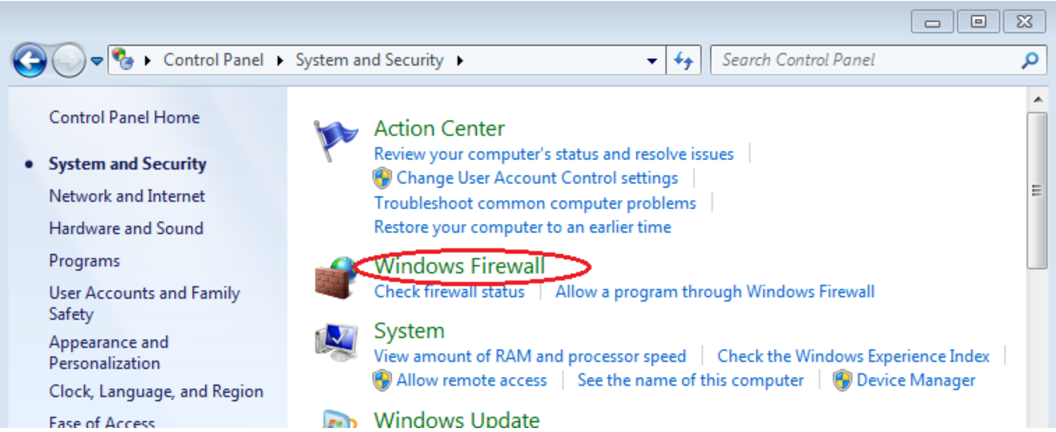
If the members of your team are unable to ping your PC, the firewall may be blocking those requests. This appendix describes how to create a rule in the firewall to allow ping requests. It also describes how to disable the new ICMP rule after you have completed the lab.

Step 1: Create a new inbound rule allowing ICMP traffic through the firewall.

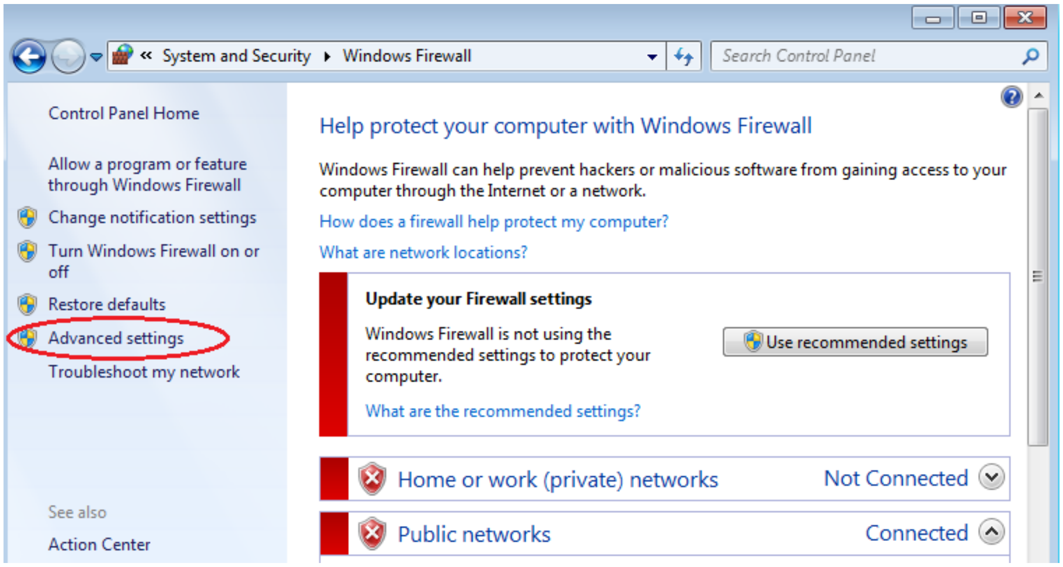
a. From the Control Panel, click the **System and Security** option.


Control Panel
File Edit View Tools Help
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
User Accounts
Change account type
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods

b. From the System and Security window, click **Windows Firewall**.


Control Panel ▸ System and Security ▸
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts and Family Safety
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Action Center
Review your computer's status and resolve issues
Change User Account Control settings
Troubleshoot common computer problems
Restore your computer to an earlier time
Windows Firewall
Check firewall status
Allow a program through Windows Firewall
System
View amount of RAM and processor speed
Check the Windows Experience Index
Allow remote access
See the name of this computer
Device Manager
Windows Update

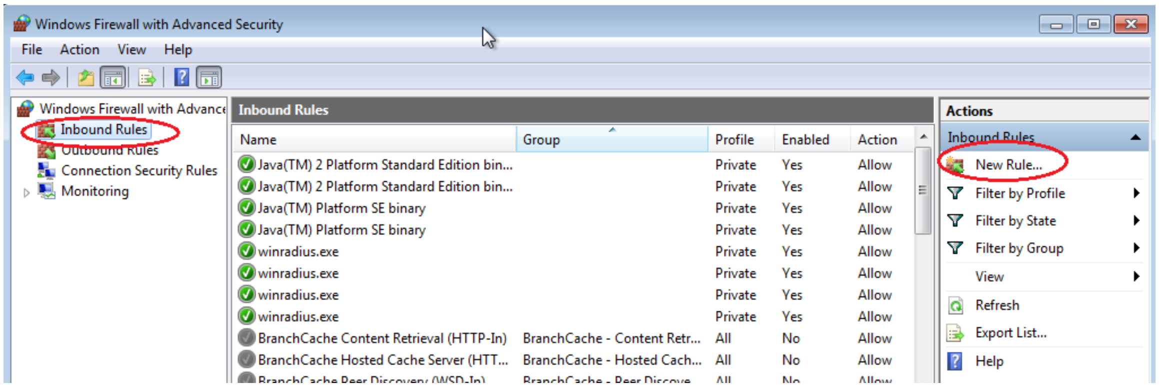
c. In the left pane of the Windows Firewall window, click **Advanced settings**.


« System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Action Center
Help protect your computer with Windows Firewall
How does a firewall help protect my computer?
What are network locations?
Update your Firewall settings
Use recommended settings
What are the recommended settings?
Home or work (private) networks
Not Connected
Public networks
Connected

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

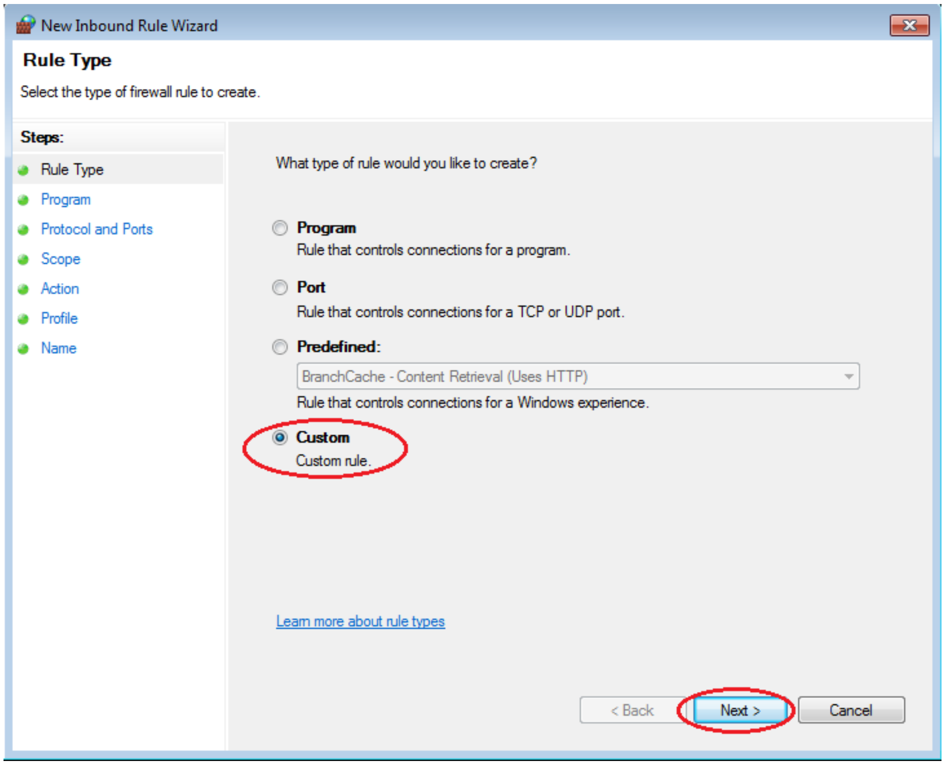
Windows Firewall is not using the recommended settings to protect your computer.

d. On the Advanced Security window, choose the **Inbound Rules** option on the left sidebar and then click **New Rule…** on the right sidebar.



Name	Group	Profile	Enabled	Action
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow

e. This launches the New Inbound Rule wizard. On the Rule Type screen, click the **Custom** radio button and click **Next**



Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

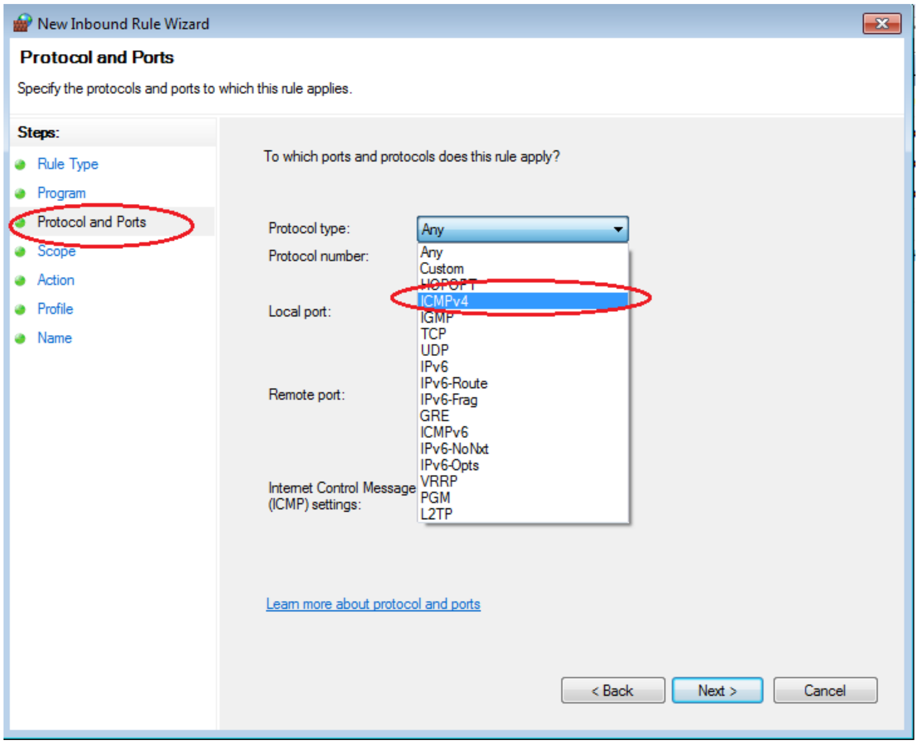
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
BranchCache - Content Retrieval (Uses HTTP)
Rule that controls connections for a Windows experience.

● **Custom**
Custom rule.

f. In the left pane, click the **Protocol and Ports** option and using the Protocol type drop-down menu, select **ICMPv4**, and then click **Next**.


New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: Any

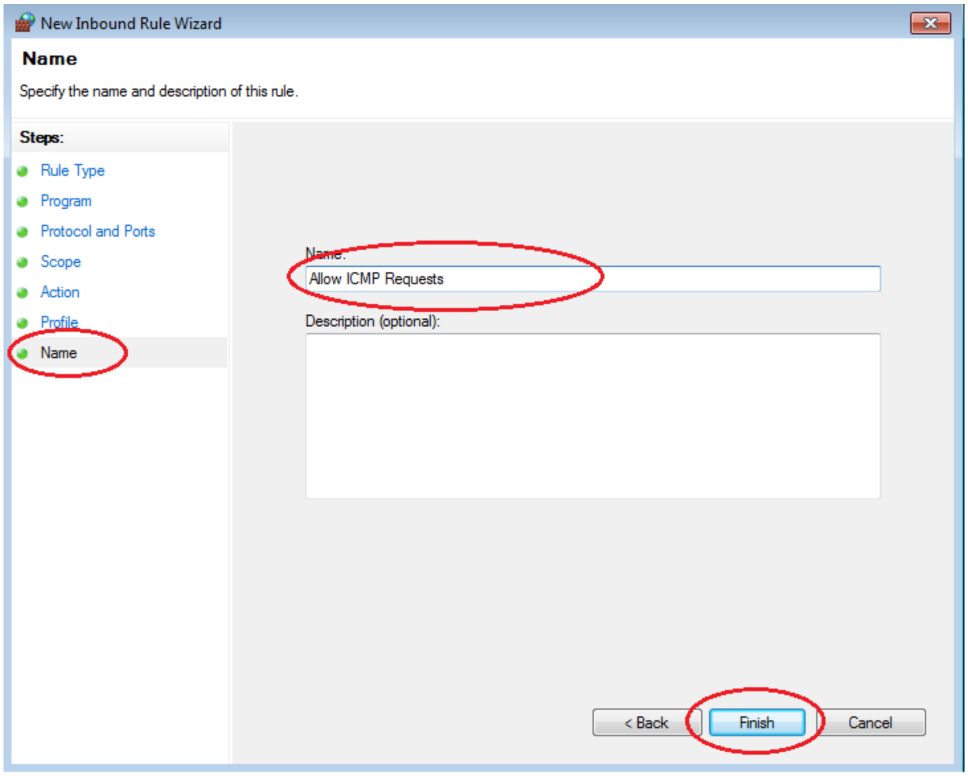
Protocol number:

Local port:

Remote port:

Internet Control Message (ICMP) settings:

g. In the left pane, click the **Name** option and in the Name field, type **Allow ICMP Requests**. Click **Finish**.


New Inbound Rule Wizard

Name

Specify the name and description of this rule.

Steps:
- Rule Type
- Program
- Protocol and Ports
- Scope
- Action
- Profile
- Name

Name: Allow ICMP Requests

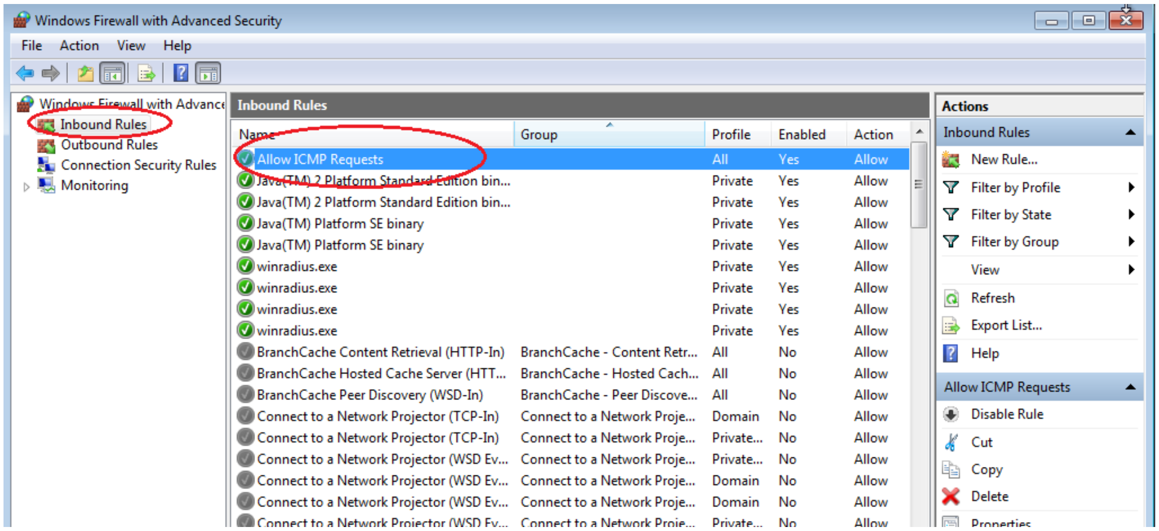
Description (optional):

This new rule should allow your team members to receive ping replies from your PC.

Step 2: Disabling or deleting the new ICMP rule.

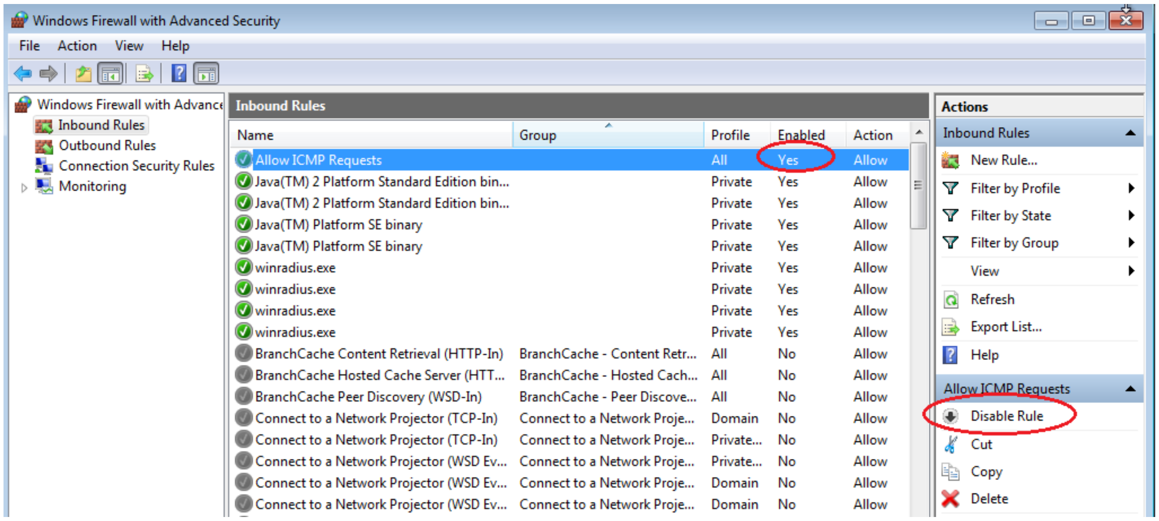
After the lab is complete, you may want to disable or even delete the new rule you created in Step 1. Using the **Disable Rule** option allows you to enable the rule again at a later date. Deleting the rule permanently deletes it from the list of Inbound Rules.

a. On the Advanced Security window, click **Inbound Rules** in the left pane and then locate the rule you created in Step 1.



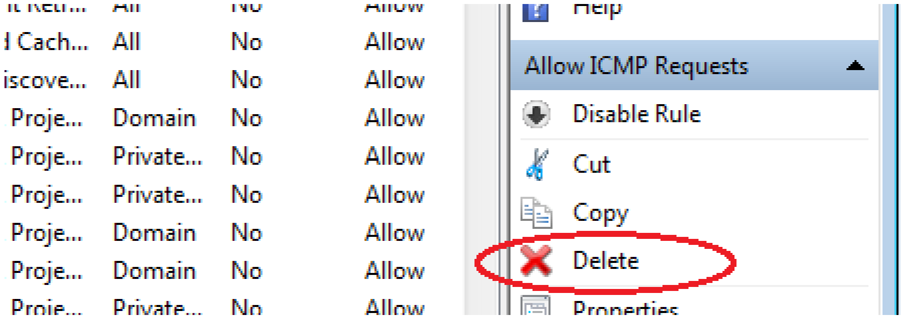
Name	Group	Profile	Enabled	Action
Allow ICMP Requests		All	Yes	Allow
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow

b. To disable the rule, click the **Disable Rule** option. When you choose this option, you will see this option change to **Enable Rule**. You can toggle back and forth between Disable Rule and Enable Rule; the status of the rule also shows in the Enabled column of the Inbound Rules list.



Name	Group	Profile	Enabled	Action
Allow ICMP Requests		All	Yes	Allow
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) 2 Platform Standard Edition bin...		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
Java(TM) Platform SE binary		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
winradius.exe		Private	Yes	Allow
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No	Allow
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No	Allow
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (TCP-In)	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Private...	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow
Connect to a Network Projector (WSD Ev...	Connect to a Network Proje...	Domain	No	Allow

c. To permanently delete the ICMP rule, click **Delete**. If you choose this option, you must re-create the rule again to allow ICMP replies.



t Retr...	All	No	Allow
d Cach...	All	No	Allow
iscove...	All	No	Allow
Proje...	Domain	No	Allow
Proje...	Private...	No	Allow
Proje...	Private...	No	Allow
Proje...	Domain	No	Allow
Proje...	Domain	No	Allow
Proje...	Private...	No	Allow