HALMSTAD UNIVERSITY
CNAP HALMSTAD – SWEDEN

CISCO SYSTEMS
NETWORKING ACADEMY

Computer Networks I

Laboratory Exercise 2

The lab is divided into three parts where the first part is how to use Wireshark, a tool for packet analysis. The second and third part is IP addressing and subnetting. This is a very important part of the networking courses, and it is really important to understand and be able to use IP addresses, subnet masks and broadcast addresses for further laborations.

2.1 Using Wireshark to view Protocol Data Units

Objective

Wireshark is a software protocol analyzer, or “packet sniffer” application, used for network troubleshooting, analysis, software and protocol development, and education. A packet sniffer is computer software that can intercept and log data traffic passing over a data network. 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 programmed to recognize the structure of different network protocols. This enables it to display the encapsulation and individual fields of a PDU and interpret their meaning. It 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.

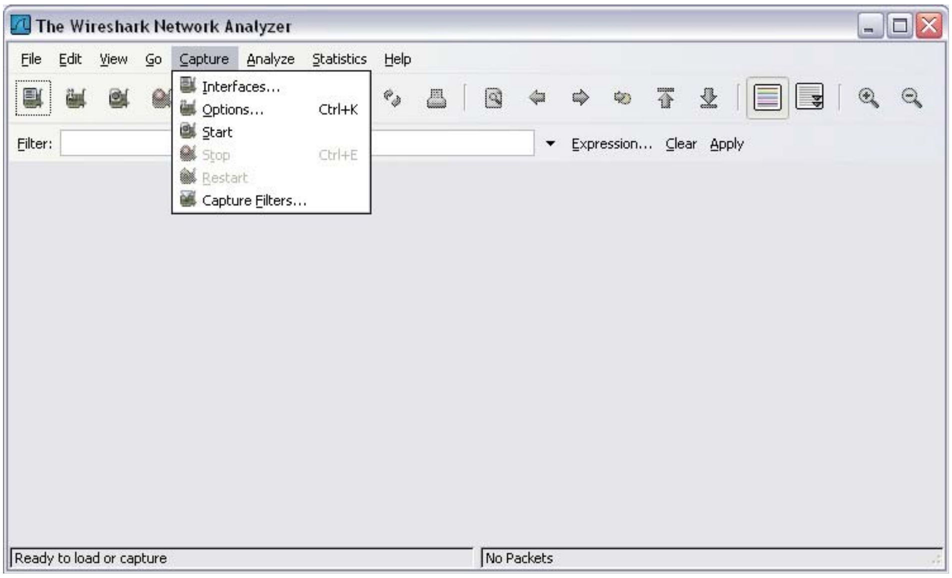
The following steps are included in this exercise:

- Be able to explain the purpose of a protocol analyzer (Wireshark)
- Be able to perform basic PDU capture using Wireshark
- Be able to perform basic PDU analysis on straight forwarded network data traffic
- Experiment with Wireshark features and options such as PDU capture and display filtering

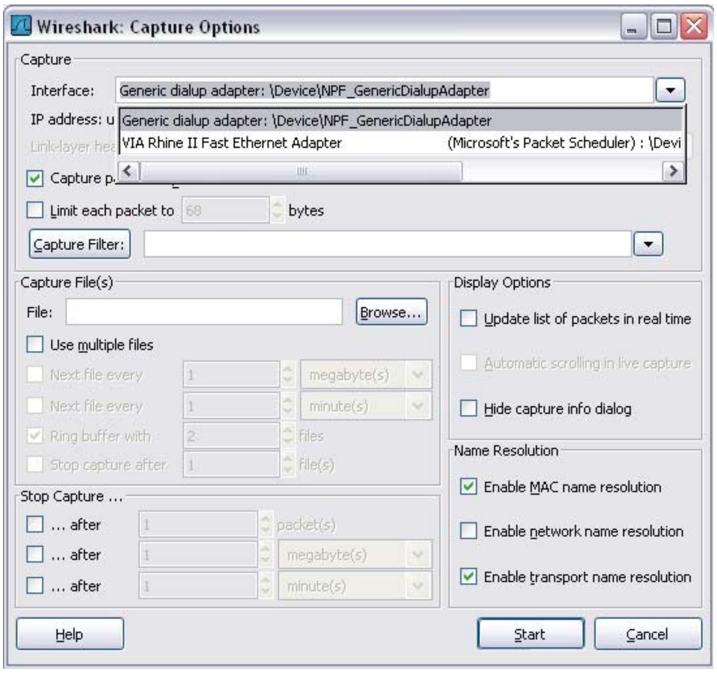
Step 1 Start Wireshark

To capture PDUs the computer on which Wireshark is installed must have a working connection to the network, and Wireshark must be running before any data can be captured. For information and to download the program, go to http://www.wireshark.com

Start Wireshark by clicking on the icon on the desktop. When Wireshark is launched, the screen below is displayed.

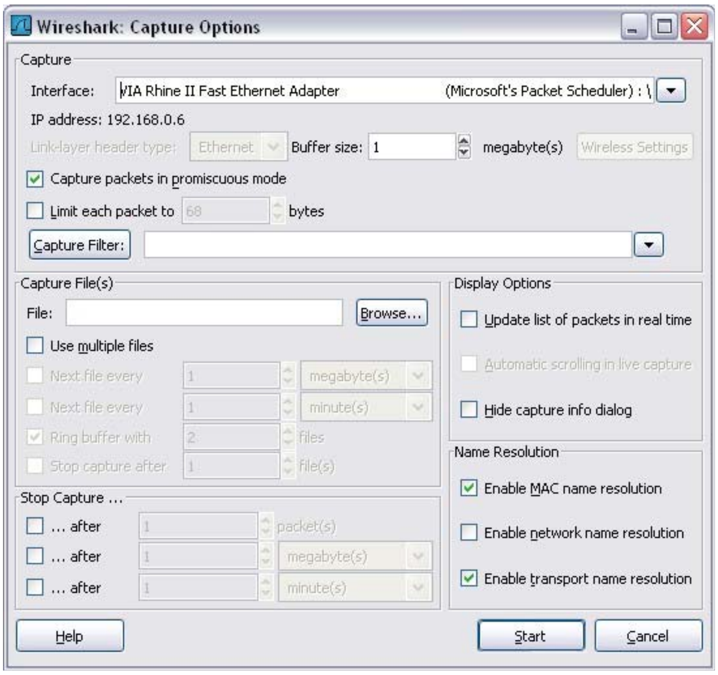


To start data capture it is first necessary to go to the **Capture** menu and select the **Options** choice. The **Options** dialog provides a range of setting and filters, which determines which and how much data traffic is captured.



First, it is necessary to ensure that Wireshark is set to monitor the correct interface. From the **Interface** drop down list, select the network adapter in use. Typically, for a computer this will be the connected Ethernet Adapter.

Then other Options can be set. Among those available in **Capture Options,** the two highlighted below are worth examination.

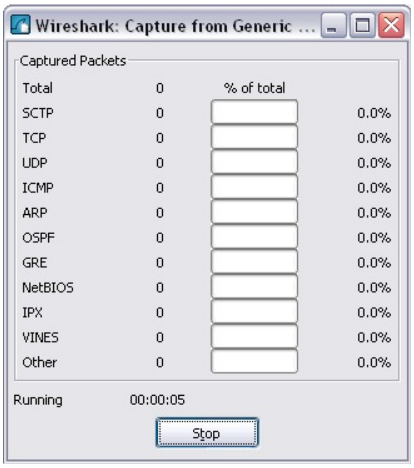


Setting Wireshark to capture packets in promiscuous mode
If this feature is NOT checked, only PDUs destined for this computer will be captured. If this feature is checked, all PDUs destined for this computer AND all those detected by the computer NIC on the same network segment (i.e., those that "pass by" the NIC but are not destined for the computer) are captured.

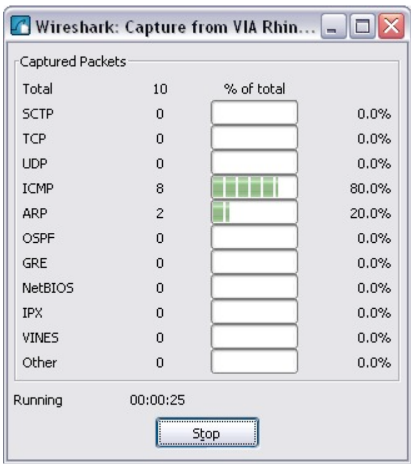
Note: The capturing of these other PDUs depends on the intermediary device connecting the end device computers on this network. As you use different intermediary devices (hubs, switches, routers) throughout these courses, you will experience the different Wireshark results.

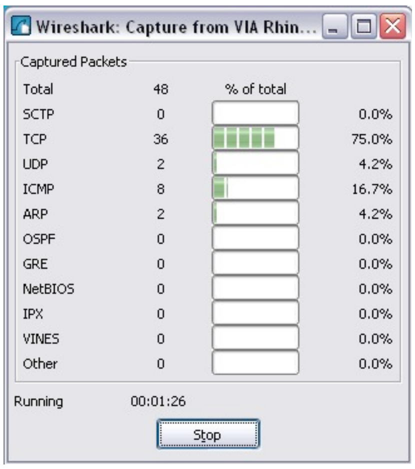
Setting Wireshark for network name resolution
This option allows you to control whether or not Wireshark translates network addresses found in PDUs into names. Although this is a useful feature, the name resolution process may add extra PDUs to your captured data perhaps distorting the analysis.

There are also a number of other capture filtering and process settings available. Clicking on the **Start** button starts the data capture process and a message box displays the progress of this process.



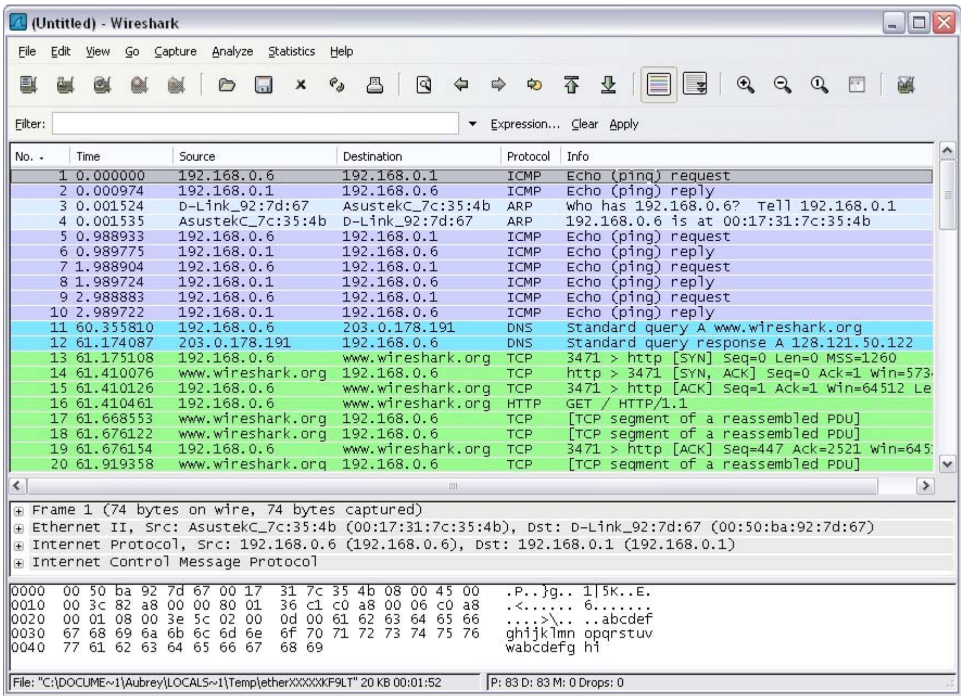
As data PDUs are captured, the types and numbers are indicated in the message box.





The examples above show the capture of a ping process, and then accessing a web page. When the **Stop** button is clicked, the capture process is terminated and the main screen is displayed.

This main display window of Wireshark has three panes.



The PDU (or Packet) List Pane at the top of the diagram displays a summary of each packet captured. By clicking on packets in this pane, you control what is displayed in the other two panes.

The PDU (or Packet) Details Pane in the middle of the diagram displays the packet selected in the Packet List Pane in more detail.

The PDU (or Packet) Bytes Pane at the bottom of the diagram displays the actual data (in hexadecimal form representing the actual binary) from the packet selected in the Packet List Pane, and highlights the field selected in the Packet Details Pane.

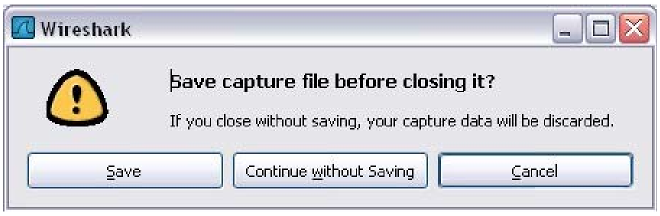
Each line in the Packet List corresponds to one PDU or packet of the captured data. If you select a line in this pane, more details will be displayed in the "Packet Details" and "Packet Bytes" panes. The example above shows the PDUs captured when the ping utility was used and http://www.Wireshark.org was accessed. Packet number 1 is selected in this pane.

The Packet Details pane shows the current packet (selected in the "Packet List" pane) in a more detailed form. This pane shows the protocols and protocol fields of the selected packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed.

The Packet Bytes pane shows the data of the current packet (selected in the "Packet List" pane) in what is known as "hexdump" style. In this lab, this pane will not be examined in detail. However, when a more in-depth analysis is required this displayed information is useful for examining the binary values and content of PDUs.

The information captured for the data PDUs can be saved in a file. This file can then be opened in Wireshark for analysis some time in the future, without the need to re-capture the same data traffic again. The information displayed when a capture file is opened is the same as the original capture.

When closing a data capture screen or exiting Wireshark you are prompted to save the captured PDUs.



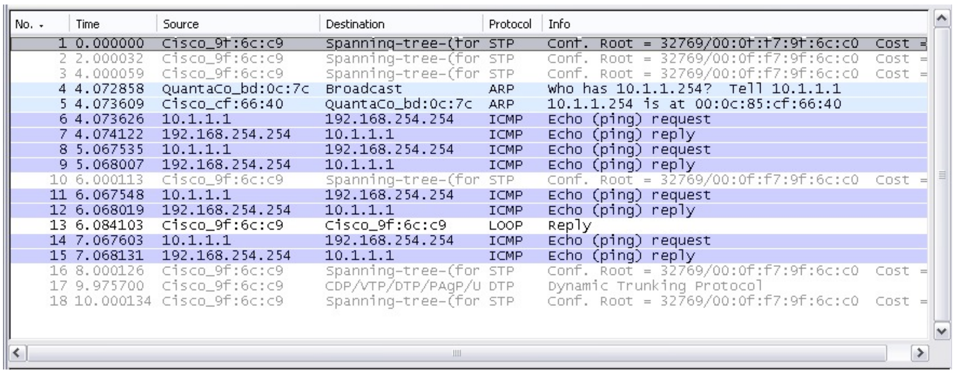
Clicking on **Continue without Saving** closes the file or exits Wireshark without saving the displayed captured data.

Step 2 Ping PDU Capture

Set the Capture Options as described above in the overview and start the capture process.

From the command line of the computer, ping the IP address of another network connected and powered on end device in the lab topology. You can, for example, ping the default gateway of your PC, or another PC connected to the network.

After receiving the successful replies to the ping in the command line window, stop the packet capture. The Packet List pane on Wireshark should now look something like this:



No.	Time	Source	Destination	Protocol	Info
1	0.000000	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
2	2.000032	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
3	4.000059	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
4	4.072858	QuantaCo_bd:0c:7c	Broadcast	ARP	Who has 10.1.1.254? Tell 10.1.1.1
5	4.073609	Cisco_cf:66:40	QuantaCo_bd:0c:7c	ARP	10.1.1.254 is at 00:0c:85:cf:66:40
6	4.073626	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
7	4.074122	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
8	5.067535	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
9	5.068007	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
10	6.000113	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
11	6.067548	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
12	6.068019	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
13	6.084103	Cisco_9f:6c:c9	Cisco_9f:6c:c9	LOOP	Reply
14	7.067603	10.1.1.1	192.168.254.254	ICMP	Echo (ping) request
15	7.068131	192.168.254.254	10.1.1.1	ICMP	Echo (ping) reply
16	8.000126	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =
17	9.975700	Cisco_9f:6c:c9	CDP/VTP/DTP/PAgP/U	DTP	Dynamic Trunking Protocol
18	10.000134	Cisco_9f:6c:c9	Spanning-tree-(for	STP	Conf. Root = 32769/00:0f:f7:9f:6c:c0 Cost =

Look at the packets listed above; we are interested in packet numbers 6, 7, 8, 9, 11, 12, 14 and 15. Locate the equivalent packets on the packet list on your computer.

Match the messages displayed in the command line window when the ping was issued with the six packets captured by Wireshark. From the Wireshark Packet List answer the following:

What protocol is used by ping? ____

What is the full protocol name? ____

What are the names of the two ping messages? ________________________________

____

Are the listed source and destination IP addresses what you expected? Yes / No

Why? ____

Step 3 Examine a packet in detail

Select (highlight) the first echo request packet on the list with the mouse. The Packet Detail pane will now display something similar to:

```
⊞ Frame 6 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
⊞ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
⊞ Internet Control Message Protocol
```

Click on each of the four "+" to expand the information. The Packet Detail pane will now be similar to:

```
⊟ Frame 6 (74 bytes on wire, 74 bytes captured)
    Arrival Time: Jan 10, 2007 01:54:07.860436000
    [Time delta from previous packet: 0.000017000 seconds]
    [Time since reference or first frame: 4.073626000 seconds]
    Frame Number: 6
    Packet Length: 74 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp]
⊟ Ethernet II, Src: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c), Dst: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  ⊞ Destination: Cisco_cf:66:40 (00:0c:85:cf:66:40)
  ⊞ Source: QuantaCo_bd:0c:7c (00:c0:9f:bd:0c:7c)
    Type: IP (0x0800)
⊟ Internet Protocol, Src: 10.1.1.1 (10.1.1.1), Dst: 192.168.254.254 (192.168.254.254)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
    Total Length: 60
    Identification: 0x0bf7 (3063)
  ⊞ Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (0x01)
  ⊞ Header checksum: 0x6421 [correct]
    Source: 10.1.1.1 (10.1.1.1)
    Destination: 192.168.254.254 (192.168.254.254)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2a5c [correct]
    Identifier: 0x0300
    Sequence number: 0x2000
```

As you can see, the details for each section and protocol can be expanded further. Spend some time scrolling through this information. At this stage of the course, you may not fully understand the information displayed but make a note of the information you do recognize.

Locate the two different types of 'Source" and "Destination". Why are there two types? ________

____

What protocols are in the Ethernet frame? ______________________________________

____

As you select a line in the Packets Detail pane all or part of the information in the Packet Bytes pane also becomes highlighted. For example, if the second line (+ Ethernet II) is highlighted in the Details pane the Bytes pane now highlights the corresponding values.

```
0000  00 0c 85 cf 66 40 00 c0  9f bd 0c 7c 08 00 45 00   ....f@.. ...|..E.
0010  00 3c 0b f7 00 00 80 01  64 21 0a 01 01 01 c0 a8   .<...... d!......
0020  fe fe 08 00 2a 5c 03 00  20 00 61 62 63 64 65 66   ....*\..  .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
```

This shows the particular binary values that represent that information in the PDU. At this stage of the course, it is not necessary to understand this information in detail

Go to the File menu and select **Close**. Click on the **Continue without Saving**.

Step 4 Reflection

Consider the encapsulation information pertaining to captured network data Wireshark can provide. Relate this to the OSI and TCP/IP layer models. It is important that you can recognize and link both the protocols represented and the protocol layer and encapsulation types of the models with the information provided by Wireshark.

Wireshark is a very useful tool for the course, and it is recommended to use it for troubleshooting, and for the understanding of further laborations. There are a lot of laborations in the curriculum on Cisco Academy Connection, which can be used to practice with Wireshark.

2.2 IPv4 Address Subnetting Part 1

Objective

Upon completion of this activity, you will be able to determine network information for a given IP address and network mask. This activity is designed to teach how to compute network IP address information from a given IP address.

When given an IP address and network mask, you will be able to determine other information about the IP address such as:

- Network address
- Network broadcast address
- Total number of host bits
- Number of hosts

Step 1 Determine network information

Given:

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**

Find:

Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Convert the host IP address and network mask to binary:

	172	**25**	**114**	**250**
IP Address	10101100	00011001	01110010	11111010
Network Mask	11111111	11111111	00000000	00000000
	255	**255**	**0**	**0**

To determine the network address, draw a line under the mask. Perform a bit-wise AND operation on the IP address and the subnet mask. **Note**: 1 AND 1 results in a 1; 0 AND anything results in a 0.

Express the results in dotted decimal notation. The result is the network address for this host IP address, which is **172.25.0.0**

	172	**25**	**114**	**250**
IP Address	10101100	00011001	01110010	11111010
Subnet Mask	11111111	11111111	00000000	00000000
Network Address	10101100	00011001	00000000	00000000
	172	**25**	**0**	**0**

Step 2 Determine the broadcast address

The network mask separates the network portion of the address from the host portion. The network address has all 0s in the host portion of the address and the broadcast address has all 1s in the host portion of the address.

	172	**25**	0	**0**
Network Add.	10101100	00011001	00000000	00000000
Mask	11111111	11111111	00000000	00000000
Broadcast.	10101100	00011001	11111111	11111111
	172	**25**	**255**	**255**

By counting the number of host bits, we can determine the total number of usable hosts for this network.

Host bits: 16

Total number of hosts:

2^{16} = 65,536

65,536 – 2 = 65,534 (addresses that cannot use the *all 0s* address, network address, or the *all 1s* address, broadcast address.)

Add this information to the table:

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**
Network Address	
Network Broadcast Address	
Total Number of Host Bits Number of Hosts	

Step 3 Challenge

For all problems:

Create a Subnetting Worksheet to show and record all work for each problem.

Problem 1

Host IP Address	**172.30.1.33**
Network Mask	**255.255.0.0**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Problem 2

Host IP Address	**172.30.1.33**
Network Mask	**255.255.255.0**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Problem 3

Host IP Address	**192.168.10.234**
Network Mask	**255.255.255.0**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Problem 4

Host IP Address	**172.17.99.71**
Network Mask	**255.255.0.0**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Problem 5

Host IP Address	**192.168.3.219**
Network Mask	**255.255.0.0**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

Problem 6

Host IP Address	**192.168.3.219**
Network Mask	**255.255.255.224**
Network Address	
Network Broadcast Address	
Total Number of Host Bits	
Number of Hosts	

2.3 IPv4 Address Subnetting Part 2

Objective

Upon completion of this activity, you will be able to determine subnet information for a given IP address and subnetwork mask.

When given an IP address, network mask and subnetwork mask, you will be able to determine other information about the IP address such as:

- The subnet address of the subnet
- The broadcast address of this subnet
- The range of host addresses for this subnet
- The maximum number of subnets for this subnet mask
- The number of hosts for each subnet
- The number of subnet bits
- The number of this subnet

Borrowing Bits

How many bits must be borrowed to create a certain number of subnets or a certain number of hosts per subnet? Using this chart, it is easy to determine the number of bits that must be borrowed.

Things to remember:

- Subtract 2 for the usable number of hosts per subnet, one for the subnet address and one for the broadcast address of the subnet.

2^{10}	2^{9}	2^{8}	2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}
1,024	**512**	**256**	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Number of bits borrowed:										
10	**9**	**8**	**7**	**6**	**5**	**4**	**3**	**2**	**1**	1
1,024	**512**	**256**	**128**	**64**	**32**	**16**	**8**	**4**	**2**	**1**
Hosts or Subnets										

Possible Subnet Mask Values

Because subnet masks must be contiguous 1's followed by contiguous 0's, the converted dotted decimal notation can contain one of a certain number of values:

Dec.	*Binary*
255	11111111
254	11111110
252	11111100
248	11111000
240	11110000
224	11100000
192	11000000
128	10000000
0	00000000

Step 1 Determine subnet information

Given:

Host IP Address	**172.25.114.250**
Network Mask	**255.255.0.0 (/16)**
Subnet Mask	**255.255.255.192 (/26)**

Find:

Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address for First Host on Subnet	
IP Address for Last Host on Subnet	
Broadcast Address for this Subnet	

Convert the host IP address and subnet mask to binary:

	172	25	114	250
IP Address	10101100	00011001	01110010	11111010
Subnet Mask	11111111	11111111	11111111	11000000
	255	**255**	**255**	**192**

To determine the network (or subnet) address, draw a line under the mask. Perform a bit-wise AND operation on the IP address and the subnet mask. **Note**: 1 AND 1 results in a 1; 0 AND anything results in a 0.

Express the results in dotted decimal notation. The result is the subnet address of this subnet, which is **172.25.114.192**

	172	**25**	**114**	**250**
IP Address	10101100	00011001	01110010	11111010
Subnet Mask	11111111	11111111	11111111	11000000
Subnet Address	10101100	00011001	01110010	11000000
	172	**25**	**114**	**192**

Add this information to the table:

Subnet Address for this IP Address	172.25.114.192

Step 2 Subnet and Host parts

To determine which bits in the address that contain network information and which contain host information:

1. Draw the Major Divide (M.D.) as a wavy line where the 1s in the major network mask end. In our example the major network mask is 255.255.0.0, or the first 16 left-most bits.
2. Draw the Subnet Divide (S.D.) as a straight line where the 1s in the given subnet mask end. The network information ends where the 1s in the mask end.
3. The result is the number of subnet bits, which can be determined by simply counting the number of bits between the M.D. and the S.D., which in this case is 10 bits. This is called the *Subnet Counting Range*.
4. The bits between the S.D. and the last bit at the end on right are called the *Host Counting Range*. This range contains the bits that are being incremented to create the host numbers or addresses.

		M.D.	S.D.		
IP Address	10101110	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10001010	11001000	01110010	11	000000
			← subnet → counting range		←host→ counting range

Step 3 Determine the range of host addresses and broadcast address

1. Copy down all of the network/subnet bits of the network address (all bits before the S.D.). In the host portion (to the right of the S.D.), make the host bits all 0s except for the right-most bit (or least significant bit), which you make a 1. This gives us the first host IP address on this subnet, which is the first part of the result for *Range of Host Addresses for This Subnet*. In this example it is **172.25.114.193**.
2. Next, in the host portion (to the right of the S.D.), make the host bits all 1s except for the right-most bit, which you make a 0. This gives us the last host IP address on this subnet, which is the last part of the result for *Range of Host Addresses for This Subnet*. In this example it is **172.25.114.254**.
3. In the host portion (to the right of the S.D.), make the host bits all 1s. This gives us the broadcast IP address on this subnet. This is the result for *Broadcast Address of This Subnet*, which in the example is **172.25.114.255**.

		M.D.	S.D.		
IP Address	10101100	11001000	01110010	11	111010
Subnet Mask	11111111	11111111	11111111	11	000000
Subnet Add.	10101100	11001000	01110010	11	000000
			← subnet → counting range		← host → counting range
First Host	10101100	11001000	01110010	11	000001
	172	25	114		193
Last Host	10101100	11001000	01110010	11	111110
	172	25	114		254
Broadcast	10101100	11001000	01110010	11	111111
	172	25	114		255

Now, this information can be added to our table:

Host IP Address	**172.25.114.250**
Major Network Mask	**255.255.0.0 (/16)**
Major (Base) Network Address	172.25.0.0
Major Network Broadcast Address	172.25.255.255
Total Number of Host Bits Number of Hosts	16 bits or 2^{16} or 65,536 total hosts 65,536 – 2 = 65,534 usable hosts
Subnet Mask	**255.255.255.192 (/26)**
Number of Subnet Bits Number of Subnets	
Number of Host Bits per Subnet Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Step 4 Determine the number of subnets

The number of subnets is determined by how many bits are in the *subnet counting range* (in this example, 10 bits).

Use the formula 2^n, where *n* is the number of bits in the *subnet counting range*.

1. $2^{10} = 1024$

Number of Subnet Bits Number of Subnets (all 0s used, all 1s not used)	10 bits 2^{10} = 1024 subnets

The number of hosts per subnet is determined by the number of host bits (in this example, 6 bits) minus 2 (1 for the subnet address and 1 for the broadcast address of the subnet).

$2^6 - 2 = 64 - 2 = 62$ hosts per subnet

Number of Host Bits per Subnet Number of Usable Hosts per Subnet	6 bits $2^6 - 2 = 64 - 2 = 62$ hosts per subnet

Final Answers

Host IP Address	**172.25.114.250**
Subnet Mask	**255.255.255.192 (/26)**
Number of Subnet Bits Number of Subnets	10 bits 2^{10} = 1024 subnets
Number of Host Bits per Subnet Number of Usable Hosts per Subnet	6 bits 2^{6} – 2 = 64 – 2 = 62 hosts per subnet
Subnet Address for this IP Address	172.25.114.192
IP Address of First Host on this Subnet	172.25.114.193
IP Address of Last Host on this Subnet	172.25.114.254
Broadcast Address for this Subnet	172.25.114.255

Step 5 Determine the number of subnets

For all problems:

Create a Subnetting Worksheet to show and record all work for each problem.

Problem 1

Host IP Address	**172.30.1.33**
Subnet Mask	**255.255.255.0**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Problem 2

Host IP Address	**172.30.1.33**
Subnet Mask	**255.255.255.252**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Problem 3

Host IP Address	**192.192.10.234**
Subnet Mask	**255.255.255.0**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Problem 4

Host IP Address	**172.17.99.71**
Subnet Mask	**255.255.0.0**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Problem 5

Host IP Address	**192.168.3.219**
Subnet Mask	**255.255.255.0**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	

Problem 6

Host IP Address	**192.168.3.219**
Subnet Mask	**255.255.255.252**
Number of Subnet Bits	
Number of Subnets	
Number of Host Bits per Subnet	
Number of Usable Hosts per Subnet	
Subnet Address for this IP Address	
IP Address of First Host on this Subnet	
IP Address of Last Host on this Subnet	
Broadcast Address for this Subnet	