

ECT-215 Homework #6 Solution Set

IP ADDRESSING (SYLLABUS)

Scoring: 27 points total.

1. Define the term “network.” (2 points)

A *network* is an organized interconnection of computers. Most IT professionals really mean “domain” when they use the word network, however.

A *network* (domain) is more precisely the set of computers sharing the same *network address*, which usually (but not always) means they are on the same physical (electrical) circuit, shared by a hub, switch, or router port.

2. What are the two parts of an IP address? (1 point)

An IP address consists of two parts, the network address and the host address.

3. In the notation “208.128.98.254 / 24”, what is the value of the subnet mask in:

- a) Binary: There are 24 logic 1s: 1111 1111 1111 1111 1111 1111 0000 0000 (1 pt)
b) Hex: 0xFFFFFFFF (or \$FFFFFFFF) (1pt)
c) Decimal: Each octet is written in decimal, giving: 255.255.255.0 (1pt)

4. Identify the network and host addresses in the following. Give your answers in decimal:

- a) 24.236.11.8 / 16 (2 points)

$N = IP \ \& \ M$ Where IP = IP address, M = Subnet mask, & = BITWISE AND

$N = (24.236.11.8 \ \& \ 255.255.0.0) = \underline{24.236.0.0}$

$H = IP \ \& \ \sim M$ Where $\sim M$ = 1's complement of subnet mask,

$H = (24.236.11.8 \ \& \ 0.0.255.255) = \underline{11.8}$

- b) 208.128.98.1 / 24 (2 points)

$N = (208.128.98.1 \ \& \ 255.255.255.0) = \underline{208.128.98.0}$

$H = (208.128.98.1 \ \& \ 0.0.0.255) = \underline{1}$

- c) 240.0.0.201 / 28 (2 points)

$N = (240.0.0.201 \ \& \ 255.255.255.240) = \underline{240.0.0.192}$

$H = (240.0.0.201 \ \& \ 0.0.0.15) = \underline{9}$

5. What are “unroutable” IP address blocks used for? (2 points)

Unroutable IP blocks are used within organizations. They allow devices inside the organization to have unique IP addresses without using up valuable public IP addresses. For example, IP addresses starting with 10, 168, and 172 are unroutable. It is entirely possible (and probable) that thousands of devices have the IP 10.0.0.1; however, no problem is caused by this, because these addresses are used only inside the organizations. No packets from these devices can travel through the Internet; routers automatically “drop” such IP packets.

6. What is the function of a gateway on a network? (2 points)

A gateway does exactly what its name says -- it acts as a portal or “gateway” to an internetwork. When a host needs to send a packet outside of its domain, it sends the packet to the default gateway, which then routes the packet onto the Internet, where routers determine the correct path for delivery.

7. Explain how a host determines whether it will send packets directly to another host on the network, or the gateway. (2 points)

A host determines whether it needs to use the gateway by examining the network address of the packet being sent. The steps are as follows:

- a) The network address (N) is extracted from the IP address by ANDing it with the subnet mask.
- b) If the network address is equal to the network address where the host is located, then the packet is emitted directly onto the local network.
- c) If the network address is *not* equal to that of the local domain, then the packet is sent to the gateway.

8. What is the function of a router? (1 point)

A router is a device that connects two or more networks (domains). It examines the IP addresses of packets (as well as other information in the packets) and calculates where to send the message packets.

9. What is the difference between UDP and TCP? (2 points)

UDP (User Datagram Protocol) is a connectionless, simplex protocol. Because it is connectionless, there’s no guarantee of delivery.

TCP (Transmission Control Protocol) is a connection-oriented protocol. It establishes a full-duplex virtual connection between two different machines. TCP includes mechanisms to ensure the delivery of messages (“lost” packets are retransmitted; the correct order of message packets is maintained; and so on.)

10. Issue the following command from a COMMAND window under either UNIX or WINDOWS: (2 points)

```
ping localhost
```

Copy the result (use the clipboard to paste it into your homework) and comment on what happened.

```
C:\>ping localhost

Pinging gw9100 [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms 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
```

Comment: “localhost” usually refers to the loopback address of the NIC card in a workstation. Pinging localhost (127.0.0.1) checks to see if the operating system can talk to the NIC card. It will work even if the NIC card is disconnected from the network. In this example, the computer is “talking to itself.” The NIC card is *probably* functional.

11. Issue the following command from a COMMAND window under either UNIX or WINDOWS: (2 points)

```
ping microsoft.com
```

Copy the result (use the clipboard to paste it into your homework) and comment on what happened.

```
C:\>ping microsoft.com

Pinging microsoft.com [207.46.197.102] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 207.46.197.102:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Comment: Oh no! Sound the alarm! Microsoft is down! The sky is falling! Actually, this is exactly what should happen. Microsoft blocks UDP traffic from outside of its organization. PING sends UDP packets to perform its task, therefore it fails. Moral: PING is not a fail-safe test of network connectivity!

12. Issue the following command from a COMMAND window under WINDOWS: (2 points)

```
tracert yahoo.com -d
```

The “-d” switch prevents *tracert* from performing a name lookup on each host, which speeds up the process. Copy the result (use the clipboard to paste it into your homework) and comment on what happened.

```
C:\>tracert yahoo.com -d

Tracing route to yahoo.com [66.218.71.113]
over a maximum of 30 hops:

  0  20 ms  10 ms  20 ms  64.218.107.254
  1  20 ms  20 ms  20 ms  151.164.8.2
  2  20 ms  20 ms  20 ms  151.164.8.246
  3  20 ms  10 ms  30 ms  151.164.242.49
  4  20 ms  20 ms  20 ms  151.164.242.158
  5  30 ms  30 ms  30 ms  151.164.242.153
  6  30 ms  30 ms  30 ms  151.164.242.134
  7  30 ms  30 ms  30 ms  151.164.89.102
  8  30 ms  40 ms  30 ms  63.250.222.42
  9  70 ms  71 ms  70 ms  216.115.101.85
 10  70 ms  80 ms  70 ms  66.218.64.138
 11  80 ms  70 ms  70 ms  66.218.71.113

Trace complete.
```

Comment: This trace was initiated from a network with a public IP address of 64.218.107.173. To get to “yahoo.com” required passage of the UDP packets through 11 intermediate routers on the network, starting with 64.218.107.254 (which is a gateway or “border” router on the Southwestern Bell network). Your results may vary.