IP Addressing

An IP address has 32 bits divided into four octets (four sets of eight binary digits). To make the address easier to read, people use decimal numbers to represent the binary digits. For example, the IP address 192.168.1.1 is 11000000.10101000.00000001.00000001 when written in binary. Notice that 32 binary digits create the address. The lowest number of any octet is 00000000, or zero, and the highest number of any octet is 11111111, or 255. When binary IP addresses are written in decimal format, it is often called dotted decimal notation. To understand how eight binary ones are equal to the decimal 255, you must look at the places for each of the binary values. Table 4-1 illustrates the places of the binary digits 128, 64, 32, 16, 8,4, 2, and 1. Notice that the decimal number 192 is created when the first two binary digits are ones and the following six digits are zeros. To determine the decimal equivalent, you add the binary places that are identified by ones. In the first row of Table 4-1, the 128 and 64 places have ones, which creates the decimal number:

192 (i.e., 128 + 64 = 192).

	128	**64**	**32**	**16**	**8**	**4**	**2**	**1**
192	1	1	0	0	0	0	0	0
168	1	0	1	0	1	0	0	0
1	0	0	0	0	0	0	0	1
255	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0

Table 4-1 Binary to decimal conversion

MAC to IP Address Comparison

The MAC address identifies a specific NIC in a computer on a network, so each MAC address is unique. TCP/IP networks can use MAC addresses in communication. However, network devices could not efficiently route traffic on a large internetwork or on the Internet using MAC addresses; MAC addresses are not grouped logically, they cannot be modified, and they do not give information about physical or logical network configuration. Therefore, another addressing scheme called IP addressing was devised for use on large networks. Unlike MAC addresses, IP addresses have a hierarchical structure and do provide logical groupings. The structure of the IP address makes packet routing possible on large internetworks. You can compare driver's license numbers to MAC addresses. The license allows you to drive a car, and it uniquely identifies you as a vehicle operator. However, when people want to talk with you, they do not call your driver's license number. Instead, they call your phone number, which identifies your location with an area code and other digits specific to you. Similarly, IP addresses identify your computer and the specific network on which it resides. For example, if your IP address is 192.168.1.3, your computer is host 3 on network 192.168.1.0. Because the IP address identifies both a network and a host, you can route communications through large networks, including the Internet. Routers can send communications in a more efficient manner by using the hierarchical IP address. If the Internet used MAC addresses, huge tables would have to be maintained containing not only the MAC addresses of each and every computer, but also each device along the path to that computer. Clearly, that would be unmanageable, especially given that network cards can malfunction. Every time someone replaced a network card, the giant MAC table would have to be updated!

IP Classes

The **Internet Assigned Numbers Authority** (IANA) devised the hierarchical IP addressing structure, and the **American Registry of Internet Numbers** (ARIN) manages IP addresses in the United States. These organisations work in conjunction with the **Internet Corporation for Assigned Names and Numbers** (ICANN), which is a global, government-independent entity with overall responsibility for the Internet. ICANN has effectively replaced IANA. Five different groups of IP addresses (labelled Class A through E) exist on the Internet. Classes A, B, and C are assigned to governments, companies, schools, and public entities for use on the Internet. Classes D and E are reserved for multicasting and experimentation. Therefore, you will mainly be concerned with managing Class A, B, and C addresses.

Class A ARIN reserves Class A IP addresses for governments and large corporations throughout the world. Class A addresses, when written in binary format, will always begin with a zero. You can tell what class an Internet address belongs to by looking at its first octet. For example, Class A addresses in decimal notation will have 1 to 126 as their first octet. Figure 4-1 displays the binary digits associated with these decimal numbers.

Binary Place Values									Decimal Equivalent	Description
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**			
0	0	0	0	0	0	0	0	=	0	Subnet
0	0	0	0	0	0	0	1	=	1	Bottom of Class A Range
0	1	1	1	1	1	1	0	=	126	Top of Class A range
0	1	1	1	1	1	1	1	=	127	Loopback address

Figure 4-1 Class A address begins with a number 1 and 126

Notice that all zeros identify the subnet, which is not a usable IP address. The first Class A address that can be assigned is 1.0.0.0 (decimal) or 00000001.00000000.00000000.00000000 (binary). The last Class A address that can be assigned is 126.0.0.0 in decimal notation, which is 01111110.00000000.00000000.00000000 in binary format.

It seems that 127.0.0.1 (decimal) is the highest assignable Class A address, but that particular address range is reserved as the loopback address. The loopback address is widely known as 127.0.0.1, but all addresses with 127 as their first octet are part of the loopback range. You can use the loop back address range for diagnostics, such as ping. If you ping 127.0.0.1 or any other IP address on the 127.0.0.0 network, your internal IP configuration should respond. This response verifies a properly installed TCPIIP protocol suite. Because the entire 127 Class A address is reserved for diagnostics, the highest Class A address that can be assigned is 126. (It is important to note that a successful loop back test does not mean the device can communicate with other devices. You can get a successful loopback response from a computer with no network cable attached to the NIC card.)

Notice that you cannot create a decimal number higher than 127 with eight binary digits if the first digit must be zero. The IANA specified that the first binary digit in a class A address would be zero to separate it from the other four categories (B, C, D, and E).

For Class A addresses, the ARIN only assigns the first octet. However, the same is not true for Class B and Class C addresses. Class B addresses are assigned with the first two octets set. Class C addresses are assigned with the first three octets set. This means that there is a difference between the number of hosts that you can assign based on the type of address you are assigned:

- **Class A:** Each Class A address supports 16,777,214 hosts.
- **Class B:** Each Class B address supports 65,534 hosts.
- **Class C:** Each Class C address supports 254 hosts.

Why is there a significant difference in the number of hosts supported? When you are assigned a Class A network, you can use the last three octets for your network hosts. When you use a Class B network, only the last two octets can be used. A Class C address only has a single octet for you to modify.

Class B Class B IP addresses are assigned to large- and medium-sized companies. The IANA specifies that Class B addresses will lead with 10 when written in binary format. This means that the range in decimal notation for the first octet of Class B addresses is 128 through 19l.

Figure 4-2 illustrates the binary to decimal calculations that specify this range.

Binary Place Values									Decimal Equivalent	Description
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**			
1	0	0	0	0	0	0	0	=	128	First Class B address
1	0	1	1	1	1	1	1	=	191	Last Class B address

Figure 4-2 Class B addresses begin with a number between 128 and 191

With the first two binary digits of the first octet in the Class B category defined, the address range is limited. When the last six configurable bits of the first octet are set to zero, the lowest configurable number is obtained (128). When those same six digits are set to one, the highest configurable number is set (191).

Class C Class C IP addresses are assigned to groups that do not meet the qualifications to obtain Class A or B addresses. The IANA specified that the first three binary digits of a Class C address must be 110, which means that Class C addresses can range from 192 through 223 in decimal notation. Figure 4-3 illustrates the binary to decimal equivalents for the Class C addresses.

Binary Place Values									Decimal Equivalent	Description
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**			
1	1	0	0	0	0	0	0	=	192	First Class C address
1	1	0	1	1	1	1	1	=	223	Last Class C address

Figure 4-3 Class C addresses begin with numbers between 192 and 223

In Class C addresses, the last five digits are configurable. The graphic shows that when the last five digits are set to all zeros, the decimal equivalent is 192. When those same five digits are set to binary ones, the decimal equivalent is 223.

Class D Class D addresses (also known as multicast addresses) are reserved for multicasting. Multicasting is the sending of a stream of data (usually audio and video) to multiple computers simultaneously. Compared to broadcasting, this saves bandwidth. Many routers forward multicasts, and computers configured to receive the multicast information accept the packets and can receive the data stream. Because Class D addresses must have 1110 as their first four I binary digits, the range for Class D starts with decimal 224 and ends at 239 in the first octet.

Figure 4-4 illustrates the binary and decimal range for Class D addresses.

Binary Place Values									Decimal Equivalent	Description
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**			
1	1	1	0	0	0	0	0	=	224	First Class D address
1	1	1	0	1	1	1	1	=	239	Last Class D address

Figure 4-4 Class 0 addresses begin with a number between 224 and 239

Class E The IANA reserved Class E addresses for research, testing, and experimentation. The Class E range starts where Class D leaves off. Figure 4-5 illustrates the first address in the "experimental" range as 240. The top of the range is 255, which is the highest possible 8-bit number. Therefore, Class E defines 240 to 255 (decimal) as the first octet.

Binary Place Values									Decimal Equivalent	Description
128	**64**	**32**	**16**	**8**	**4**	**2**	**1**			
1	1	1	1	0	0	0	0	=	240	First Class E address
1	1	1	1	1	1	1	1	=	255	Last Class E address

Figure 4-5 Class E addresses begin with a number between 240 and 255

Private IP Ranges Many companies today use private IP addresses for their internal networks. This prevents the organisations from having to obtain official IP addresses from their ISP every time they add a host to the network. Class A, B, and C private address ranges have been defined by RFC1918 (www.faqs.org/rfcs/rfc1918.html). Table 4-2 illustrates the private IP address ranges that network administrators can use. If these private ranges are used for an internal network, they will not be routable on the Internet. This is fine for most organisations because they have one or more gateway devices (such as routers, firewalls, or proxy servers) that provide connectivity to the Internet. These gateway devices have network interface connections to both the internal network and the Internet and route packets between them (thereby providing Internet connectivity to internal clients). The company will simply have to obtain one or more official IP addresses if it chooses to provide services (like an organisational Web site) to people using the Internet.

Class	Private Address Range
A	10.x.x.x
B	172.16.x.x - 172.31.x.x
C	192.168.x.x

Table 4-2 The private IP ranges

Network Addressing

As previously mentioned, IP addresses identify both the network and the host. However, the division between the two is not specific to a certain number of octets. In an earlier example, the IP address 192.168.1.3 was used to illustrate that 192.168.1.0 was the network and 3 was the host identifier on that network. This suggests that the first three octets comprise the network identifier and the last octet is the host identifier, but that is not always true. In fact, the network portion can be as small as the first octet or as large as 30 of the 32 binary digits of the IP address.

How do you determine how many digits are used for the network identifier? You must look at the sub net mask, which is a required component for all IP hosts. On every TCP/IP network, hosts must have both an IP address and a subnet mask. The subnet mask indicates how much of the IP address represents the network or subnet (short for sub-network).

Standard (default) subnet masks are as follows:

- **Class A** subnet mask is 255.0.0.0 or 11111111. 00000000.00000000.00000000
- **Class B** subnet mask is 255.255.0.0 or 11111111.11111111.00000000.00000000
- **Class C** subnet mask is 255.255.255.0 or 11111111.11111111.11111111.00000000

Notice that Class A addresses come with the first octet masked, Class B addresses have the first two octets masked, and Class C addresses have the first three octets masked.

The mask is essentially a continuous string of binary one digits. TCP/IP hosts use the combination of the IP address and the subnet mask to determine if other addresses are local or remote. The binary AND operation is used to perform the calculation. The binary AND operation is simple-each of the 32 binary digits in the IP address is compared with the corresponding digit on the subnet mask to arrive at the ANDing result. One and one results in one, and all other combinations result in zero. When devices AND the IP address with the corresponding subnet mask, the network (or subnetwork) number is the result. Computers and routers use the AND computation to determine the subnet identifier for each IP address.

If the subnet identifier for the local IP address is the same as that of the IP address to which it wants to communicate, then the packet is sent on the local subnet (ARP is used, as necessary, to locate the destination MAC address on the local subnet). However, if the subnet identifiers are different, then the packet is sent to the default gateway (usually the local router) to be routed to the remote subnet. Figure 4-6 illustrates ANDing.

In the figure, the first comparison uses the subnet mask 255.255.255.0, which defines the first three octets as the network identifier. A quick look will tell you that these hosts are on two different subnets. Notice that the first three octets from the ANDing result of the source host are 64.168.1, while those of the destination host are 64.168.5. This means that the source is on subnetwork 64.168.1.0 and the destination is on subnet 64.168.5.0. The source host will have to send communications for 64.168.5.7 through its default gateway.

Now consider the calculations shown on the bottom half of Figure 4-6. The subnet mask has been changed to 255.255.0.0. Given this configuration, the two hosts are on the same subnet because the network identifier in this case is 64.168.0.0 for both. This means that the source host would use ARP, if necessary, to determine the MAC address of host 64.168.5.7 and then transmit its data to that MAC address. Notice that in both of these examples, the default mask is not used. The 64 in the first octet identifies this as a Class A address, which would have a default subnet mask of 255.0.0.0. This means the network administrator has manipulated the mask to get more network numbers.

IP:	64.168.1.1	01000000.10101000.00000001.00000001
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
ANDing result:	64.168.1.0	01000000.10101000.00000001.00000000
Destination IP:	64.168.5.7	01000000.10101000.00000101.00000111
Sub net mask:	255.255.255.0	11111111.11111111.11111111.00000000
ANDing result:	64.168.5.0	01000000.10101000.00000101.00000000

When the mask 255.255.255.0 is used the hosts are remote.

Source IP:	64.168.1.1	01000000.10101000.00000001.00000001
Subnet mask:	255.255.0.0	11111111.11111111.00000000.00000000
ANDing result:	64.168.1.0	01000000.10101000.00000000.00000000
Destination IP:	64.168.5.7	01000000.10101000.00000101.00000111
Sub net mask:	255.255.0.0	11111111.11111111.00000000.00000000
ANDing result:	64.168.5.0	01000000.10101000.00000000.00000000

When the mask 255.255.0.0 is used the hosts are local.

Figure 4-6 ANDing operations

Subnet Address If you look at the preceding network and host number divisions, you will notice that the network is identified by the first, or first few, octets. Notice that after the masked portion of the subnet mask, the network identifier changes to zero(s). For example, the network identifier of a host that has IP address 192.168.23.45 with subnet mask 255.255.255.0 is 192.168.23.0.

One of the IP networking rules stipulates that a TCP/IP host must have a nonzero host identifier. From this information, you can determine that on a subnet using mask 255.255.255.0, the IP address 222.12.150.4 is a valid host IP address. However, the address 222.12.150.0 is not a host address, but a network identifier. In other words, you could not assign 222.12.150.0 to a computer.

Broadcast Address IP addressing has another rule that you must commit to memory. On any subnet, when the entire host portion of an IP address is all binary ones, it is a broadcast to all of the computers on that segment. For example, on subnet 192.168.1.0, the IP address 192.168.1.255 is a broadcast. This also can apply to larger subnetworks such as 190.55.0.0; the IP address 190.55.255.255 is a broadcast on that network.

Converting these addresses into binary digits can quickly show if an IP address is a broadcast. If all the binary digits in the host identifier are ones, the address is a broadcast. Figure 4-7 illustrates a broadcast address for a subnet.

Subnet ID:	199.192.65.0	11000111.11000000.01000001.00000000
Subnet mask:	255.255.255.0	11111111.11111111.11111111.00000000
Broadcast Address:	199.192.65.255	11000111.11000000.01000001.11111111

Figure 4-7 Broadcast addresses

By looking at Figure 4-7, you can quickly determine the broadcast address (199.192.65.255) because the decimal 255 represents eight binary ones. The binary calculation is not necessary if you know that all bits in the octet that represents the host portion are ones. However, the determination is not so easy when an octet is partially masked, as shown in Figure 4-8.

Subnet ID:	199.192.65.32	11000111.11000000.01000001.00100000
Subnet mask:	255.255.255.224	11111111.11111111.11111111.11100000
Broadcast Address:	199.192.65.63	11000111.11000000.01000001.00111111

Figure 4-8 Broadcasts on partially masked octets

In Figure 4-8, you can see that subnetwork identifiers do not always end in a zero-decimal value. In this case, the last octet has been partially masked (three binary places), leaving the last five binary digits of the last octet to represent the host identifier. In decimal format, it may be difficult to determine that 199.192.65.63 is a broadcast address for the subnet 199.192.65.32, but in binary format, it is much easier. You can see that the last five binary digits are all ones, which indicates a broadcast on the local subnet.

Notice how important the subnet mask is in determining the logical subdivision of the network. For example, if the subnet mask in Figure 4-8 were 255.255.255.0 instead of 255.255.255.224, the broadcast address would not be 199.192.65.63. Instead, 199.192.65.255 would be the correct broadcast address.

Broadcast Types

The two different types of broadcasts are flooded and directed. Flooded broadcasts are broadcasts for any subnet and use the IP address 255.255.255.255. A router does not propagate flooded broadcasts because they are considered local. When a host sends a packet to the IP address 255.255.255.255, the packet remains on the local subnet.

On the other hand, directed broadcasts are for a specific subnet. Routers can forward directed broadcasts. For example, a packet sent to the Class B address 129.30.255.255 would be a broadcast for network 129.30.0.0. The router would forward that packet to the identified I network. For security purposes, directed broadcasting is often disabled on a router.

Key Terms

American Registry of Internet Numbers (ARIN) An organisation that manages IP address allocation in the United States.

classful A routing process that involves using subnet masks with traditional octet boundaries.

classless A routing process that allows subnet masks to partition the network and the node portions on any bit boundary.

Classless Inter-Domain Routing (CIDR) A system of allocating IP network numbers based on arbitrary subnet mask boundaries. CIDR notation uses a prefix to designate the network portion of the subnet mask.

directed broadcasts Broadcasts sent to specific segments. For example, a broadcast on segment 192.168.1.0 would be 192.168.1.255.

flooded broadcasts A broadcast for any subnet that uses the IP address 255.255.255.255. Routers do not pass flooded broadcasts.

Internet Assigned Numbers Authority (IANA) The regulatory agency originally responsible for subdividing and administering the address hierarchy used on the Internet. IANA has been replaced by ICANN.

Internet Corporation for Assigned Names and Numbers (ICANN) The global, government independent entity responsible for the Internet.

IP addressing The act of assigning (unique) IP addresses to devices on the network.

loopback The TCP/IP Class A address 127.x.x.x that is reserved for diagnostic purposes.

Any address on this network allows you to check if TCP/IP has been properly installed on the system. (Specifically, the IP address 127.0.0.1 is the address usually given as the loopback.)

multicast address A special subdivision of IP categories reserved for data streaming.

Multicast addresses are used to send information to groups of computers. The range for multicasting addresses is 224.0.0.0 to 239.255.255.255.

multicasting The sending of a stream of data to multiple computers simultaneously.

Network Address Translation (NAT) A standard that allows inside IP addresses to be translated to different outside IP address(es). NAT maps inside IP addresses to different outside IP addresses or just one outside address. NAT is used to slow the exhaustion of IPv4 addresses as well as to hide a company's internal IP scheme.