Understanding TCP/IP addressing and subnetting basics

This article was previously published under Q164015

INTRODUCTION

When you configure the TCP/IP protocol on a Microsoft Windows computer, an IP address, subnet mask, and usually a default gateway are required in the TCP/IP configuration settings.

To configure TCP/IP correctly, it is necessary to understand how TCP/IP networks are addressed and divided into networks and subnetworks. This article is intended as a general introduction to the concepts of IP networks and subnetting. A glossary is included at the end of article.

MORE INFORMATION

The success of TCP/IP as the network protocol of the Internet is largely because of its ability to connect together networks of different sizes and systems of different types. These networks are arbitrarily defined into three main classes (along with a few others) that have predefined sizes, each of which can be divided into smaller subnetworks by system administrators. A subnet mask is used to divide an IP address into two parts. One part identifies the host (computer), the other part identifies the network to which it belongs. To better understand how IP addresses and subnet masks work, look at an IP (Internet Protocol) address and see how it is organized.

IP addresses: Networks and hosts

An IP address is a 32-bit number that uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

IP addresses are normally expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. To understand how subnet masks are used to distinguish between hosts, networks, and subnetworks, examine an IP address in binary notation.

For example, the dotted-decimal IP address 192.168.123.132 is (in binary notation) the 32 bit number 11000000010100001111011100000100. This number may be hard to make sense of, so divide it into four parts of eight binary digits.

These eight bit sections are known as octets. The example IP address, then, becomes 11000000.10101000.01111011.10000100. This number only makes a little more sense, so for most uses, convert the binary address into dotted-decimal format (192.168.123.132). The decimal numbers separated by periods are the octets converted from binary to decimal notation.

For a TCP/IP wide area network (WAN) to work efficiently as a collection of networks, the routers that pass packets of data between networks do not know the exact location of a host for which a packet of information is destined. Routers only know what network the host is a member of and use information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

For this process to work, an IP address has two parts. The first part of an IP address is used as a network address, the last part as a host address. If you take the example 192.168.123.132 and divide it into these two parts you get the following:

```
192.168.123.    Network
          .132 Host
```

-or-

```
192.168.123.0 - network address.
0.0.0.132     - host address.
```

Subnet mask

The second item, which is required for TCP/IP to work, is the subnet mask. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network.

In TCP/IP, the parts of the IP address that are used as the network and host addresses are not fixed, so the network and host addresses above cannot be determined unless you have more information. This information is supplied in another 32-bit number called a subnet mask. In this example, the subnet mask is 255.255.255.0. It is not obvious what this number means unless you know that 255 in binary notation equals 11111111; so, the subnet mask is:

```
11111111.11111111.11111111.0000000
```

Lining up the IP address and the subnet mask together, the network and host portions of the address can be separated:

```
11000000.10101000.01111011.10000100 -- IP address (192.168.123.132)
11111111.11111111.11111111.00000000 -- Subnet mask (255.255.255.0)
```

The first 24 bits (the number of ones in the subnet mask) are identified as the network address, with the last 8 bits (the number of remaining zeros in the subnet mask) identified as the host address. This gives you the following:

```
11000000.10101000.01111011.00000000 -- Network address (192.168.123.0)
00000000.00000000.00000000.10000100 -- Host address (000.000.000.132)
```

So now you know, for this example using a 255.255.255.0 subnet mask, that the network ID is 192.168.123.0, and the host address is 0.0.0.132. When a packet arrives on the 192.168.123.0 subnet (from the local subnet or a remote network), and it has a destination address of 192.168.123.132, your computer will receive it from the network and process it.

Almost all decimal subnet masks convert to binary numbers that are all ones on the left and all zeros on the right. Some other common subnet masks are:

```
Decimal                 Binary
255.255.255.192         1111111.11111111.1111111.11000000
255.255.255.224         1111111.11111111.1111111.11100000
```

Internet RFC 1878 (available from http://www.internic.net) describes the valid subnets and subnet masks that can be used on TCP/IP networks.

Network classes

Internet addresses are allocated by the InterNIC (http://www.internic.net), the organization that administers the Internet. These IP addresses are divided into classes. The most common of these are classes A, B, and C. Classes D and E exist, but are not generally used by end users. Each of the address classes has a different default subnet mask. You can identify the class of an IP address by looking at its first octet. Following are the ranges of Class A, B, and C Internet addresses, each with an example address:

- Class A networks use a default subnet mask of 255.0.0.0 and have 0-127 as their first octet. The address 10.52.36.11 is a class A address. Its first octet is 10, which is between 1 and 126, inclusive.

- Class B networks use a default subnet mask of 255.255.0.0 and have 128-191 as their first octet. The address 172.16.52.63 is a class B address. Its first octet is 172, which is between 128 and 191, inclusive.

- Class C networks use a default subnet mask of 255.255.255.0 and have 192-223 as their first octet. The address 192.168.123.132 is a class C address. Its first octet is 192, which is between 192 and 223, inclusive.

In some scenarios, the default subnet mask values do not fit the needs of the organization, because of the physical topology of the network, or because the numbers of networks (or hosts) do not fit within the default subnet mask restrictions. The next section explains how networks can be divided using subnet masks.

Subnetting

A Class A, B, or C TCP/IP network can be further divided, or subnetted, by a system administrator. This becomes necessary as you reconcile the logical address scheme of the Internet (the abstract world of IP addresses and subnets) with the physical networks in use by the real world.

A system administrator who is allocated a block of IP addresses may be administering networks that are not organized in a way that easily fits these addresses. For example, you have a wide area network with 150 hosts on three networks (in different cities) that are connected by a TCP/IP router. Each of these three networks has 50 hosts. You are allocated the class C network 192.168.123.0. (For illustration, this address is actually from a range that is not allocated on the Internet.) This means that you can use the addresses 192.168.123.1 to 192.168.123.254 for your 150 hosts.

Two addresses that cannot be used in your example are 192.168.123.0 and 192.168.123.255 because binary addresses with a host portion of all ones and all zeros are invalid. The zero

address is invalid because it is used to specify a network without specifying a host. The 255 address (in binary notation, a host address of all ones) is used to broadcast a message to every host on a network. Just remember that the first and last address in any network or subnet cannot be assigned to any individual host.

You should now be able to give IP addresses to 254 hosts. This works fine if all 150 computers are on a single network. However, your 150 computers are on three separate physical networks. Instead of requesting more address blocks for each network, you divide your network into subnets that enable you to use one block of addresses on multiple physical networks.

In this case, you divide your network into four subnets by using a subnet mask that makes the network address larger and the possible range of host addresses smaller. In other words, you are 'borrowing' some of the bits usually used for the host address, and using them for the network portion of the address. The subnet mask 255.255.255.192 gives you four networks of 62 hosts each. This works because in binary notation, 255.255.255.192 is the same as 1111111.11111111.1111111.11000000. The first two digits of the last octet become network addresses, so you get the additional networks 00000000 (0), 01000000 (64), 10000000 (128) and 11000000 (192). (Some administrators will only use two of the subnetworks using 255.255.255.192 as a subnet mask. For more information on this topic, see RFC 1878.) In these four networks, the last 6 binary digits can be used for host addresses.

Using a subnet mask of 255.255.255.192, your 192.168.123.0 network then becomes the four networks 192.168.123.0, 192.168.123.64, 192.168.123.128 and 192.168.123.192. These four networks would have as valid host addresses:

```
192.168.123.1-62
192.168.123.65-126
192.168.123.129-190
192.168.123.193-254
```

Remember, again, that binary host addresses with all ones or all zeros are invalid, so you cannot use addresses with the last octet of 0, 63, 64, 127, 128, 191, 192, or 255.

You can see how this works by looking at two host addresses, 192.168.123.71 and 192.168.123.133. If you used the default Class C subnet mask of 255.255.255.0, both addresses are on the 192.168.123.0 network. However, if you use the subnet mask of 255.255.255.192, they are on different networks; 192.168.123.71 is on the 192.168.123.64 network, 192.168.123.133 is on the 192.168.123.128 network.

Default gateways

If a TCP/IP computer needs to communicate with a host on another network, it will usually communicate through a device called a router. In TCP/IP terms, a router that is specified on a

host, which links the host's subnet to other networks, is called a default gateway. This section explains how TCP/IP determines whether or not to send packets to its default gateway to reach another computer or device on the network.

When a host attempts to communicate with another device using TCP/IP, it performs a comparison process using the defined subnet mask and the destination IP address versus the subnet mask and its own IP address. The result of this comparison tells the computer whether the destination is a local host or a remote host.

If the result of this process determines the destination to be a local host, then the computer will simply send the packet on the local subnet. If the result of the comparison determines the destination to be a remote host, then the computer will forward the packet to the default gateway defined in its TCP/IP properties. It is then the responsibility of the router to forward the packet to the correct subnet.

Troubleshooting

TCP/IP network problems are often caused by incorrect configuration of the three main entries in a computer's TCP/IP properties. By understanding how errors in TCP/IP configuration affect network operations, you can solve many common TCP/IP problems.

Incorrect Subnet Mask: If a network uses a subnet mask other than the default mask for its address class, and a client is still configured with the default subnet mask for the address class, communication will fail to some nearby networks but not to distant ones. As an example, if you create four subnets (such as in the subnetting example) but use the incorrect subnet mask of 255.255.255.0 in your TCP/IP configuration, hosts will not be able to determine that some computers are on different subnets than their own. When this happens, packets destined for hosts on different physical networks that are part of the same Class C address will not be sent to a default gateway for delivery. A common symptom of this is when a computer can communicate with hosts that are on its local network and can talk to all remote networks except those that are nearby and have the same class A, B, or C address. To fix this problem, just enter the correct subnet mask in the TCP/IP configuration for that host.

Incorrect IP Address: If you put computers with IP addresses that should be on separate subnets on a local network with each other, they will not be able to communicate. They will try to send packets to each other through a router that will not be able to forward them correctly. A symptom of this problem is a computer that can talk to hosts on remote networks, but cannot communicate with some or all computers on their local network. To correct this problem, make sure all computers on the same physical network have IP addresses on the same IP subnet. If you run out of IP addresses on a single network segment, there are solutions that go beyond the scope of this article.

Incorrect Default Gateway: A computer configured with an incorrect default gateway will be able to communicate with hosts on its own network segment, but will fail to communicate with hosts on some or all remote networks. If a single physical network has more than one router, and the wrong router is configured as a default gateway, a host will be able to communicate with some remote networks, but not others. This problem is common if an organization has a router to an

internal TCP/IP network and another router connected to the Internet.

REFERENCES

Two popular references on TCP/IP are:

"TCP/IP Illustrated, Volume 1: The Protocols," Richard Stevens, Addison Wesley, 1994

"Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture," Douglas E. Comer, Prentice Hall, 1995

It is strongly recommended that a system administrator responsible for TCP/IP networks have at least one of these references available.

Glossary

Broadcast address -- An IP address with a host portion that is all ones.

Host -- A computer or other device on a TCP/IP network.

Internet -- The global collection of networks that are connected together and share a common range of IP addresses.

InterNIC -- The organization responsible for administration of IP addresses on the Internet.

IP -- The network protocol used for sending network packets over a TCP/IP network or the Internet.

IP Address -- A unique 32-bit address for a host on a TCP/IP network or internetwork.

Network -- There are two uses of the term network in this article. One is a group of computers on a single physical network segment; the other is an IP network address range that is allocated by a system administrator.

Network address -- An IP address with a host portion that is all zeros.

Octet -- An 8-bit number, 4 of which comprise a 32-bit IP address. They have a range of 00000000-11111111 that correspond to the decimal values 0- 255.

Packet -- A unit of data passed over a TCP/IP network or wide area network.

RFC (Request for Comment) -- A document used to define standards on the Internet.

Router -- A device that passes network traffic between different IP networks.

Subnet Mask -- A 32-bit number used to distinguish the network and host portions of an IP address.

Subnet or Subnetwork -- A smaller network created by dividing a larger network into equal parts.

TCP/IP -- Used broadly, the set of protocols, standards and utilities commonly used on the Internet and large networks.

Wide area network (WAN) -- A large network that is a collection of smaller networks separated by routers. The Internet is an example of a very large WAN.

Properties

Article ID: 164015 - Last Review: 09/23/2011 22:03:00 - Revision: 6.0

Applies to
Microsoft Windows 2000 Server

Microsoft Windows 2000 Advanced Server

Microsoft Windows 2000 Professional Edition

Microsoft Windows NT Server 3.51

Microsoft Windows NT Server 4.0 Standard Edition

Microsoft Windows NT Workstation 3.1

Microsoft Windows NT Workstation 3.5

Microsoft Windows NT Workstation 3.51

Microsoft Windows NT Workstation 4.0 Developer Edition

Microsoft Windows NT Advanced Server 3.1

Microsoft Windows 95

Keywords:

kbnetwork kbusage KB164015

Support

Account support

Supported products list

Product support lifecycle

Security

Safety & Security Center

Download Security Essentials

Malicious Software Removal Tool

Contact Us

Report a support scam

Disability Answer Desk

Locate Microsoft addresses worldwide

English (United States)