soundtraining.net
training for information technology
and business professionals

Technical Brief

Designing and Configuring the TCP/IP Protocol

By Don R. Crawley, MCSE, MCT, CCNA-certified
President/Trainer, soundtraining.net

Contents

A Brief History of TCP/IP and the Internet

A discussion of the background of TCP/IP should also include a discussion of the background of the Internet as TCP/IP is the protocol of the Internet. TCP/IP is, in fact, often referred to as "The Internet Protocol".

The Internet was conceived in the early 1960s as a fault-tolerant network for the United States Department of Defense. The idea was to create a network that could withstand a Soviet nuclear attack and continue to function (remember, this was during the Cold War). The concept was one of a packet-switching network over public lines connected by switching nodes called IMPs (Internet Message Processors). The original network was built under the auspices of DARPA (Defense Advanced Research Projects Agency) and consisted of four IMPs (one at the University of Utah and three in California) and was first activated in the late 1960's. The network was called ARPAnet. The original protocols were fairly limited, so in 1974 Vinton Cerf and Robert Kahn began work on a set of protocols that eventually led to today's TCP/IP.

Vinton Cerf and Robert Kahn are generally considered to be the "Fathers of the Internet". They conceived and, with many other people, developed what has become Internet Protocol version 4, which was standardized in 1981.

NSFNet (National Science Foundation Network) is created in 1986, linking five supercomputers with 56Kbps lines. As bandwidth demands increase, it was upgraded to T1 lines (1.544Mbps) in 1988 and upgraded again in 1991 to T3 service (44.736Mbps).

ARPANet was decommissioned in 1990.

As other networks were connected to the NSFNet, it became known as "The Internet". The name "Internet" comes from the concept of interconnected networks. For example, the University of Washington's network, Microsoft's network, the University of Missouri's network, the Department of Energy's network, and the General Electric network might all be connected via the same backbone. Each network is discreet, yet each network is interconnected with other networks on this public backbone.

In much the same way that Vinton Cerf and Robert Kahn are considered the Fathers of the Internet, Tim Berners-Lee is considered to be the founder of the World Wide Web. (The Internet is the physical network of routers, cables, servers, etc. while the "Web" is the content: The web sites, web pages, links, etc.) Berners-Lee invented HTML and HTTP while working at CERN, the European Organization for Particle Research, in Switzerland to facilitate global collaboration. The development and growth of the Internet and the World Wide Web was further facilitated by the development of Mosaic, the first graphical point-and-click hypertext browser. Mosaic was created in 1992 by Marc Andreesen, an undergraduate computer science major and Eric Bina at the National Center for Supercomputing Applications at the University of Illinois at Urbana-Champaign.

Mosaic technology is at the heart of both Internet Explorer and Netscape Navigator. It is possible to download a copy of Mosaic from http://archive.ncsa.uiuc.edu/

In 1995, NSFNet was returned to its original purpose as a research backbone. Responsibility for the Internet backbone was turned over to commercial providers such as AT&T, UUNet, and others. For more information about Internet technologies and procedures, visit the Internet Engineering Task Force web site at www.ietf.org.

Much of the above information came from the PBS series "Nerds 2.0.1". Visit www.pbs.org/opb/nerds2.0.1 Another excellent source of information about the history of the Internet is Hobbes' Internet Timeline at www.zakon.org/robert/internet/timeline

The TCP/IP Protocol Suite

TCP/IP is a layered suite of many protocols. The name itself includes two protocols: Transmission Control Protocol and Internet Protocol. There are many other protocols that make up the TCP/IP suite. TCP/IP is sometimes called the DoD protocol because of its development by the Department of Defense.

The Layers of TCP/IP

Similar to the OSI model, TCP/IP is a layered suite of protocols.

Process/Application Layer (FTP, Telnet, SMTP)
Host-to-Host Layer (Error-free connections (TCP))
Internetwork Layer (Provides logical address (IP))
Network Access Layer (The physical connection components)

The Network Access Layer

This layer describes the physical connection components such as cabling and connectors. It describes the physical layout of the network such as the star, bus, or ring topologies. It also deals with the network access methods such as Ethernet or Token Ring.

The Internetwork Layer

This layer deals with the hierarchical IP address space. Addresses are divided into the categories of class, network, subnet, and host at this layer.

The Host-to-Host Layer

Error-free connections take place here through TCP. TCP and UDP both deal with sequencing at this layer.

The Process/Application Layer

Network applications such as Telnet and FTP operate at this layer. This layer maps to the top three layers of the OSI model.

OSI Model	DoD Model
Layer Seven—Application Layer	Process/Application Layer
Layer Six—Presentation Layer	
Layer Five—Session Layer	
Layer Four—Transport Layer	Host-to-Host
Layer Three—Network Layer	Internetwork
Layer Two—Data Link Layer	Network Interface
Layer One—Physical Layer	

Protocol Data Units (PDUs)

OSI Layers	What the data is called (PDU)
Layer Seven—Application Layer	Upper-Layer Data
Layer Six—Presentation Layer	
Layer Five—Session Layer	
Layer Four—Transport Layer	Segment
Layer Three—Network Layer	Packet
Layer Two—Data Link Layer	Frame
Layer One—Physical Layer	Bits

Protocols in the TCP/IP Suite

Some of the protocols in the TCP/IP suite include:

IP (Internet protocol): Provides connectionless, best-effort delivery of packets. It is not concerned with content of packets. See RFC 791.

TCP (Transmission Control Protocol): A connection-oriented protocol that provides error checking, acknowledgement, and flow control. See RFC 793.

UDP (User Datagram Protocol): A connection-less protocol that is very fast, but unreliable. See RFC 768.

FTP (File Transfer Protocol): One of the original IPv4 protocols, used for file transfer. See RFC 959.

TFTP (Trivial File Transfer Protocol): Similar to FTP, but only allows “put” and “get”. See RFC 1350.

ICMP (Internet Control Message Protocol): Provides control and messaging capabilities. See RFC 792.

ARP (Address Resolution Protocol): Resolves IP address to 48 bit MAC (Ethernet) address. See RFC 826.

RARP (Reverse Address Resolution Protocol): Resolves MAC address to IP address. See RFC 903.

HTTP (HyperText Transfer Protocol): Used for WWW services. See RFC 1945.

HTTPS (Secure HyperText Transfer Protocol): Used for secure WWW services incorporating Secure Sockets Layer. See experimental RFC 2660.

IMAP (Internet Message Access Protocol): Used for receiving and reading email messages which are stored on a server. See RFC 2060.

DHCP (Dynamic Host Configuration Protocol): Dynamically assigns IP addresses and other options to hosts on an IP network. See RFC 2131.

Telnet: Used for remote login (can also be used for testing). See RFC 854.

SNMP (Simple Network Management Protocol): Used for monitoring and managing network devices. See RFC 1157.

SMTP (Simple Mail Transfer Protocol): Used for sending email in conjunction with POP3 and/or IMAP. Usually operates over port 25. See RFC 821.

POP3 (Post Office Protocol): Used for receiving email which is ultimately stored on the client’s computer. Usually operates over port 110. See RFC 1939.

NTP (Network Time Protocol). Used for synchronizing time in a large, diverse internet. See RFC 1305.

SNTP (Simple Network Time Protocol): An adaptation of NTF, used for synchronizing time with Internet time servers when the full NTP implementation is not necessary. See RFC 2030.

There are, of course, hundreds of other protocols that together make up the TCP/IP suite used on the Internet and in LANs and other WANs.

The RFCs (Requests for Comments) are the technical papers that describe the various technologies used LANs and WANs. An excellent source of information about the RFCs is the Internet Engineering Task Force website at www.ietf.org.

There are also many tools included in the TCP/IP suite such as PING, TraceRoute, DNS, and Telnet.

Socket and Ports

Sockets connect an application to a network protocol. Sockets are a software object, not a physical object.
Ports are points of entrance to the TCP/IP stack.
TCP and UDP ports are similar to extensions on a telephone switchboard. Some common ports include:

- 80—WWW
- 25—SMTP
- 69—TFTP
- 21—FTP
- 443—HTTPS

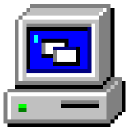
There are three broad ranges of port numbers:

- Well-Known Ports (0-1023) are assigned by IANA (Internet Assigned Numbers Authority). They can usually be used only by system (or root) processes or programs when executed by privileged users.
- Registered Ports (1024-49151) are listed by IANA and can typically be used by ordinary user processes and programs when executed by ordinary users. These ports are registered by IANA as a convenience to the community.
- Dynamic and/or Private Ports (49152-65535) available for private use
- There are 65,535 TCP port numbers and 65,535 UDP port numbers. For the most part, the TCP and UDP port numbers match. The complete listing of all TCP and UPD port numbers is available at www.iana.org/assignments/port-numbers.

Two Types of Nodes

A node is anything in an IP network that has an IP address.

- Host Nodes
  - The source or destination of IP traffic.
- Router Nodes
  - Directs the packets from one network or subnet to another. Think of a router as a traffic cop or a dispatcher.


Host

Router

IP Addresses

IP addresses are 32 bits long and made up of four eight-bit octets (also called fields or bytes). The decimal numbers within each octet can range from zero to 255.

Bits are ones and zeros. A bit that's turned on is represented by a "1" and a bit that's turned off is represented by a "0". There are eight bits in a byte. Each bit has a decimal value that increases from right to left:

Decimal Value	128	64	32	16	8	4	2	1

Here's an example of the binary number 11010000:

Decimal Value	128	64	32	16	8	4	2	1
Bits	1	1	0	1	0	0	0	0

The decimal value of the above byte is 208.

Here's an example of the IP address 208.79.115.3:

IP Address in Decimal	208	79	115	3
IP Address in Binary	11001000	01001111	01110011	00000011

To determine the decimal value of a byte, add the decimal values of each bit that's turned on. The following byte (11010000) converts to decimal by adding 128, 64, and 16 (the bits that are 1s). The resulting byte value is 208.

Here's an example of the IP address 208.115.79.3:

Decimal Number	208	115	79	3
Binary Conversion	11001000	01110011	01001111	00000011

Classful IP Addresses

IP addresses contain three distinct parts:

- The class (A, B, C, D, or E): The class is determined by the value of the first octet. If the first octet falls within the range of 1-126, the address is part of a Class A network. If the first octet falls within the range of 128-191, the address is part of a Class B network. If the first octet falls within the range of 192-223, the address is part of a Class C network.
- The network address: The network ID is similar to an area code within the telephone system. Unlike the telephone numbering system, however, the network ID's length changes based on the class of address. In a Class A network, the network ID is eight bits long (or one octet), in a Class B network, the network ID is 16 bits long (or two octets), and in a Class C network, the network ID is 24 bits long (or three octets).
- Host ID. The host ID is similar to a local phone number within the telephone system. As with network IDs, the length of the host ID will change based on the class of address. In a Class A network, the host ID is 24 bits long (or three octets), in a Class B network, the host ID is 16 bits long (or two octets), and in a Class C network, the host ID is eight bits long (or one octet).

Of the five classes of IP addresses, three are commonly used in LANs (Class A, B, and C). Class D is used for IP multicasting and Class E is reserved for experimental purposes. Often, IP addresses are compared to telephone numbers in that a network address must be unique to the Internet in much the same way an area code must be unique to the Public Switched Telephone Network, and the host address must be unique to the individual network or subnet in much the same way that a local telephone number must be unique within an area code.

When the Internet was originally designed, Class A addresses were reserved for very large networks, Class B was used for medium sized networks, and Class C was used for smaller networks. Classful IP addresses are still used in LAN environments, so it's important to understand the proper configuration of Classful IP addressing. There is a technology called CIDR (Classless Internet Domain Routing) that is replacing Classful IP Addressing on the Internet. Ultimately, however, IPv6 will replace all IPv4 addressing schemes.

Class	First Part of Address	Maximum # of hosts
A	1-126 (1-126).h.h.h	16,777,214
B	128-191 (128-191).n.h.h	65,534
C	192-223 (192-223).n.n.h	254

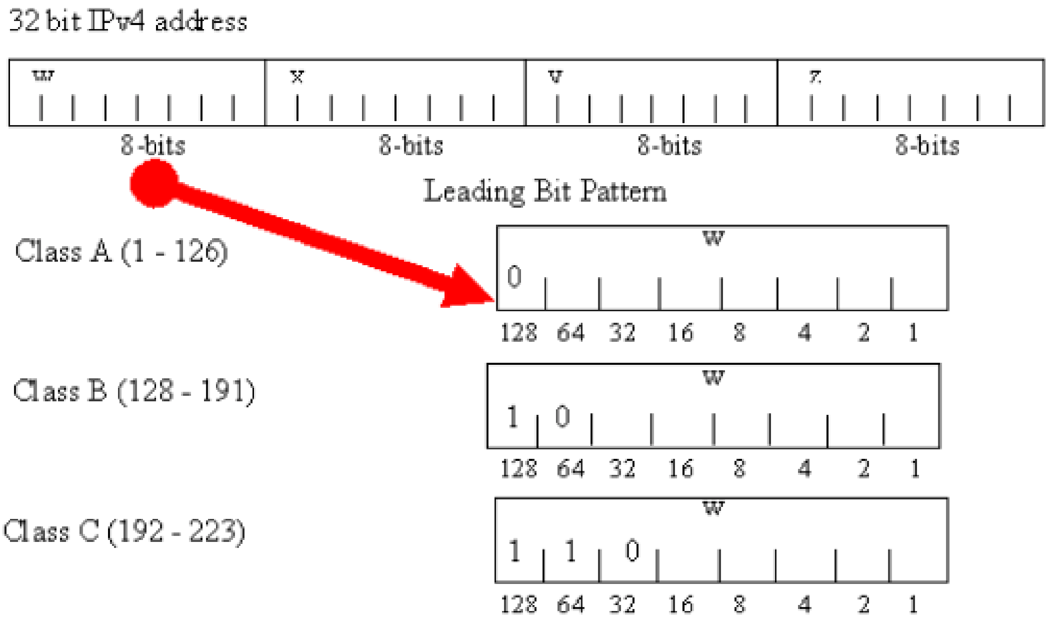
IP Addresses

In discussions of IP addresses, they are often identified as follows: w.x.y.z

- A class A network is represented by the "w" octet
- A class B network is represented by the "w" and "x" octets
- A class C network is represented by the "w", "x", and "y" octets

The Leading Bit Pattern

When an IP address is converted from dotted decimal to binary (base 2) notation, the leading bit patterns identify the class of address.



A router examines each packet, looking at the first bit of its address. If it sees a zero in the first bit position, it knows the address of the packet is a class A address. If it sees a one in the first bit position and a zero in the second bit position, it knows the address is a class B address. If it sees a one in the first two bit positions and a zero in the third bit position, it knows that the address is a class C address.

If you do the math, you'll see that when the leading bit of a byte is a 0, the only possible decimal values for the byte are 0 through 127. Internet rules further restrict the range of first octet values for a Class A address to the 1 through 126 range. Similarly, when the leading bits of a byte are 10, the only possible decimal values for the byte are 128-191 and when the leading bits are 110, the only possible decimal values for the byte are 192-223.

In much the same way that the PSTN assigns unique numbers to each telephone, TCP/IP assigns unique numbers to each node in an IP network. Although IP addresses are obtained from ISPs, an organization called ICANN is the governing body.

ICANN stands for "Internet Corporation for Assigned Names and Numbers". ICANN is the body that, in concert with IANA (Internet Assigned Numbers Authority) and InterNIC (Internet Network Information Center), controls the IP address space.

IP Addressing—Basic Rules

- Each network must have a unique network ID
- Each workstation on a network must have a unique host ID
- Your IP address must be globally unique in all the world if you are on the public Internet
- Network addresses cannot use the number 127
- The class A network 127 is reserved for loopback testing on hosts
  - You can PING 127.0.0.1 on a host to test your IP stack (this does not work on routers)

PING is a very common tool for testing connectivity at layer three and below.
The proper procedure for using PING from an IP host follows several logical steps:

- PING 127.0.0.1 to test your IP stack
- PING “localhost” to test for a properly configured HOSTS file
- Run the IPCONFIG utility (or WINIPCFG on Windows 9x hosts) to determine your host’s IP configuration
- From the results of IPCONFIG (or WINIPCFG), PING your default gateway
- PING a remote host on the next subnet

The IP Address Rule:

IP addresses, whether network, subnet, or host ID, can never consist of all *binary* ones nor all *binary* zeros.

There are, of course, exceptions to this rule (including the CIOS’ support for IP subnet zero). It is, however, an excellent starting point for understanding basics of IP addressing.

A thinking point:

Is 111.111.111.111 a valid IP address? Why or why not? It is valid, because it’s a decimal number, not binary. If it were binary, there would have to be eight 1s in each octet.

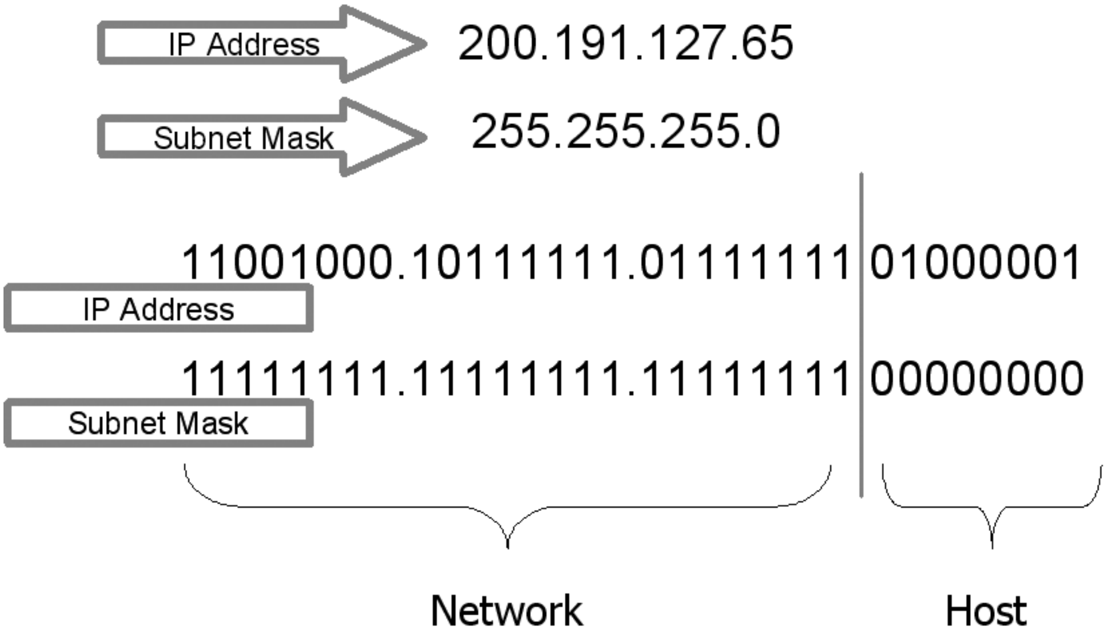
Binary Conversion

The easiest way to convert between decimal and binary numbers is, of course, with a calculator. You can use Windows’ built-in calculator in scientific mode or download various IP subnet calculators from the Internet. In order to understand the fundamental concepts of IP, however, it’s helpful to understand the theory of binary conversion. A table can be used for this purpose in which the columns represent the decimal values of each bit in an eight-bit binary number and the rows represent each of the octets of an IP address to be converted.

Begin by attempting to the subtract the decimal value of the leading bit (128) from the value of the first octet (200). Since 128 can be subtracted from 200 (leaving a remainder of 72), put a “1” in the 128s column. Continue by attempting to subtract the decimal value of the next bit (64) from the remainder (72). Since 64 can be subtracted from 72 (leaving a remainder of 8), place a “1” in the 64s column. Next, attempt to subtract the decimal value of the next bit (32) from the remainder (8). Since 32 cannot be subtracted from 8, put a “0” in the 32s column. Continue in this manner until 1s or 0s have been placed in each column.

	128	64	32	16	8	4	2	1
200								
191								
127								
65								

What good does this do? For the answer, study the graphic.

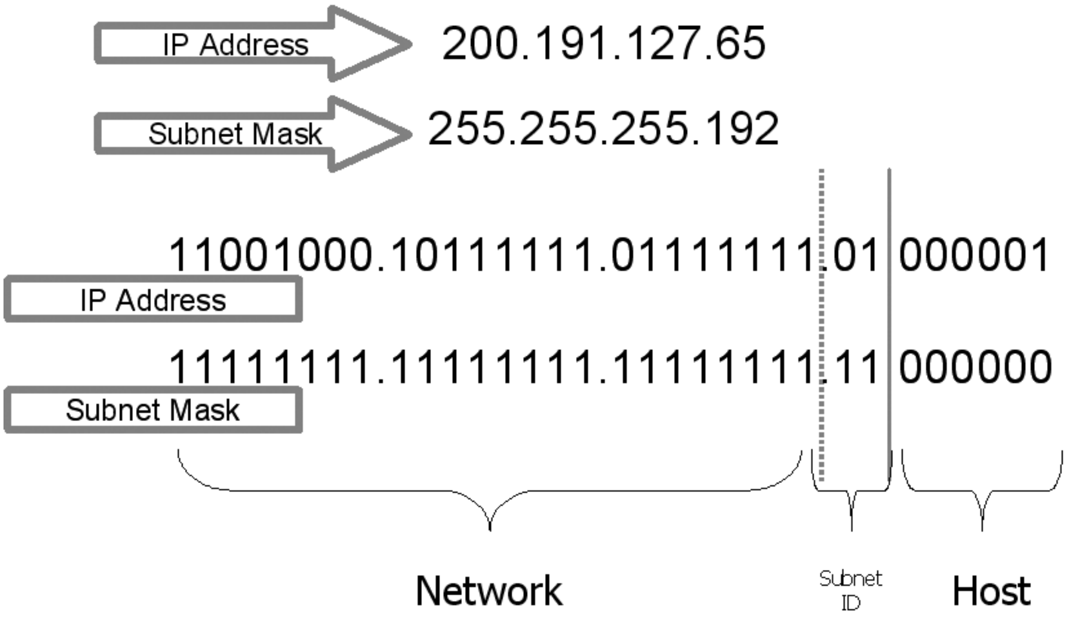


With every IP address, there is always an associated subnet mask. Notice that the address is a Class C address (its first octet falls within the range of 192-223). How many bits are used for the network portion of any given Class C address? It’s the same number as the number of bits that are turned on (represented by 1s) in the subnet mask. If the bits are turned on in the subnet mask, the corresponding bits in the IP address are network (and/or subnet) bits. In the example, bits 1-24 are turned on in the subnet mask, therefore bits 1-24 of the associated IP address are network bits (and bits 25-32 are host bits).

Soundthinking point

In order for two hosts to communicate on a network, the network bits of their IP address must match or a router must be placed between them.

Suppose, however, that the subnet mask is 255.255.255.192. What happens now?



The dividing line between network and host has moved over two bits, creating a 26 bit network address and a six bit host address. The “major network” address is still actually 24 bits (that’s the default for a Class C), but the network designer has taken two bits from the host portion of the address. This creates a subnet of two bits and a subnet mask of 26 bits.

As in the previous example, in order for two hosts to communicate on a network, their network bits in their IP addresses must match, but now there are 26 bits that have to match instead of 24.

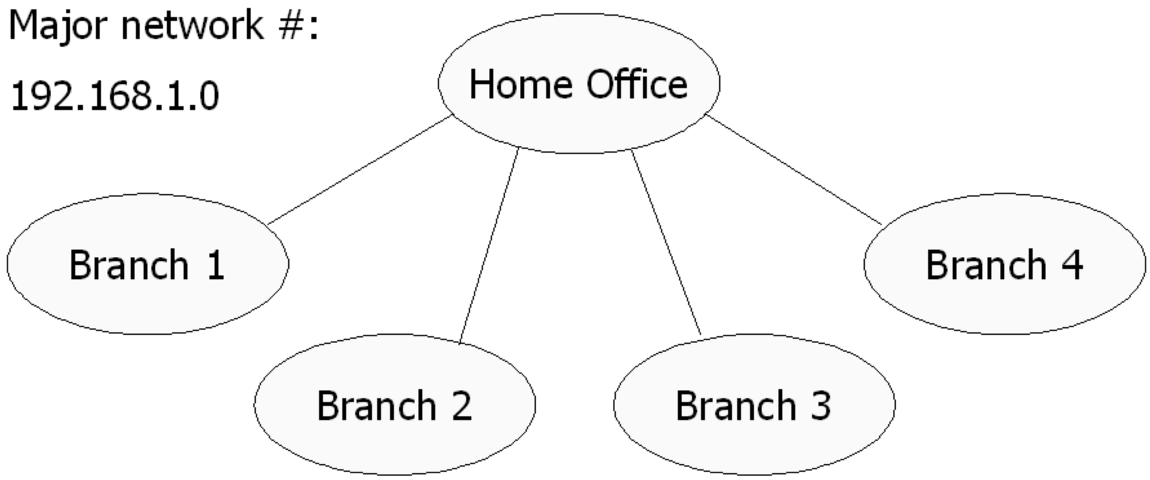
Network architects and designers use the practice of subnetting to isolate heavy traffic networks, to minimize broadcasts, and to control excessive WAN traffic.

The purpose of the subnet mask is to identify which bits of the associated IP address are network bits, subnet bits, and host bits.

IP Addressing Design: How Do You Determine the Addresses to Use in Your Network?

The following exercise will help you learn how to design an IP addressing scheme.

Student Exercise 4.1: Home Office and Branches



For the purpose of this exercise, assume that each location has no more than 20 hosts at this time and will grow by no more than 50% in the foreseeable future.

Step One: How many subnets are needed? What number of bits borrowed from the host will provide that number?

Step Two: Use the formula of 2^n-2 to determine the number of bits needed to get the necessary number of subnets.

Think of it this way: We use “2” because it’s the binary number system. “N” is the number of bits upon which we’re acting. We subtract two from the result because we can’t use all binary 1’s nor or all binary 0’s in any Internet address.

2^2-2=2, 2^3-2=6, 2^4-2=14, 2^5-2=30, 2^6-2=62, etc. Based on these formulas, we can see that three bits must be borrowed in order to get the needed number of subnets.

Step Three: Create the appropriate subnet mask by turning on three more bits. The default mask is 11111111.11111111.11111111.00000000 or 255.255.255.0. By turning on three more bits we create a mask of 11111111.11111111.11111111.11100000 or 255.255.255.224.

Step Four: Identify the Subnet IDs

Subnet IDs	128	64	32	16	8	4	2	1
32	0	0	1	Will be used later for host IDs				
64	0	1	0					
96	0	1	1					
128	1	0	0					
160	1	0	1					
192	1	1	0					

Step Five: Add the Subnet IDs to the Major Network Numbers

Major Network: 192.168.1.0/24

Network Numbers with Subnet IDs:

- 192.168.1.32
- 192.168.1.64
- 192.168.1.96
- 192.168.1.128
- 192.168.1.160
- 192.168.1.192

Step Six: Identify the host IDs

Subnet IDs			Host IDs					
128	64	32	16	8	4	2	1	
Identified in previous step			0	0	0	0	1	1
			0	0	0	1	0	2
			0	0	0	1	1	3
			0	0	1	0	0	4
			0	0	1	0	1	5
			0	0	1	1	0	6
			0	0	1	1	1	7
			0	1	0	0	0	8

Step Seven: Combine the subnet ID and the host ID to get the fourth octet value:

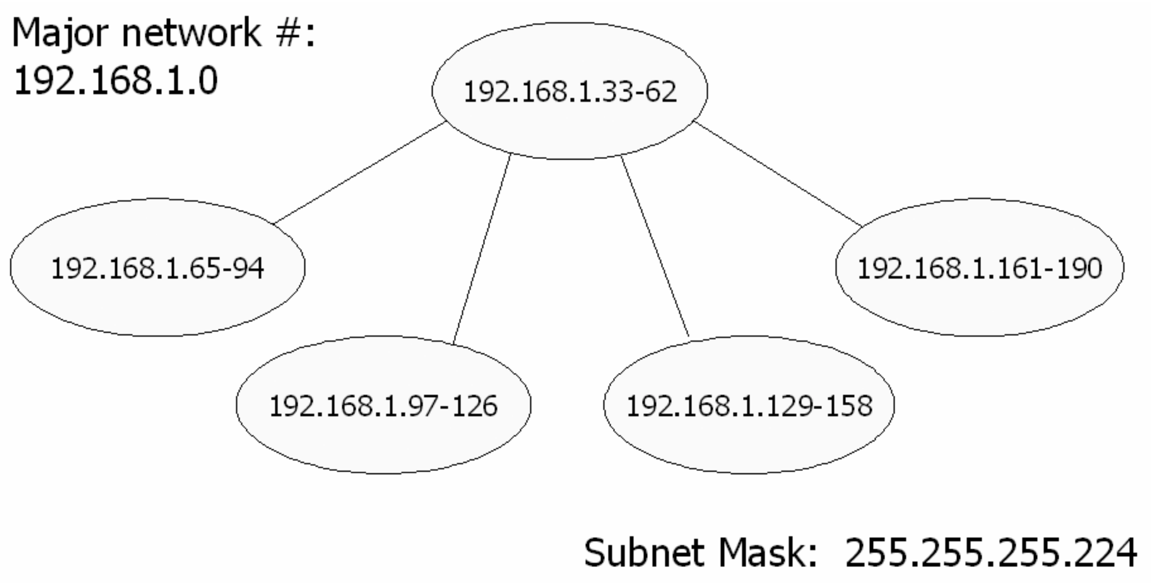
Subnet ID			Host ID					4th Octet Value
128	64	32	16	8	4	2	1	
0	0	1	0	0	0	0	1	

Combine the subnet and the host:

Subnet IDs	*1st Host ID*	*Last Host ID*	*Range*
192.168.1.32	32+1=33	32+30=62	192.168.1.33-62
192.168.1.64	64+1=65	64+30=94	192.168.1.65-94
192.168.1.96	96+1=97	96+30=126	192.168.1.97-126
192.168.1.128	128+1=129	128+30=158	192.168.1.128-158
192.168.1.160	160+1=161	160+30=190	192.168.1.161-190
192.168.1.192	192+1+193	192+30=222	192.168.1.193-222

In a class C network environment, the total number of hosts per subnet will always be two less than the smallest subnet ID number. Note in the example that the lowest subnet ID is 32 (207.201.142.32) and there are 30 hosts per subnet.

Assign to Locations



The Broadcast Address

Broadcasts are used when the unicast address is not known. The broadcast address is determined by turning on all host bits.

Host ID								4th Octet Value
128	64	32	16	8	4	2	1	
1	1	1	1	1	1	1	1	
255								255

A more challenging problem arises when the network is subnetted. It's still the same concept: Turn on all the host bits. The difference is in where the subnet (network) bits end and the host bits begin.

Subnet ID			Host ID					4th Octet Value
128	64	32	16	8	4	2	1	
1	0	1	1	1	1	1	1	

Private Range Addresses and Default Subnet Masks

Private Range IP Addresses

- Class A (10.h.h.h)
- Class B (172.16.h.h-172.31.h.h)
- Class C (192.168.0.h-192.168.255.h)
- These addresses are specified in RFC 1597

Default subnet masks

- Class A is 255.0.0.0 (/8)
- Class B is 255.255.0.0 (/16)
- Class C is 255.255.255.0 (/24)

You must specify at least the default subnet mask
Notice the use of the "slash" following the above addresses (255.0.0.0 (/8)

Obtaining an IP Address

IP Addresses are generally obtained through an ISP. For computers that will not be directly connected to the Internet, use private range IP addresses. Do not use any address not assigned to you except for private range addresses.
For more information about IP addresses, visit ICANN.org or InterNIC.net.

Student Exercise 4.2: TCP/IP Configuration

This exercise teaches you how to design a complex subnet addressing scheme.

Objectives:

Gain a solid understanding of the binary number system and how to convert binary numbers into decimal format and vice versa

Learn fundamentals of subnetting in IP network design

Part I:

Identifying the dotted-decimal representation of the subnet mask

Determining the total number of subnets

Determining the total number of available hosts per subnet

From the information on the following two tables, fill in the empty cells.

NIC Number	Subnet Bits	Subnet Mask in Dotted Decimal	Total # of Subnets	Total Hosts per Subnet
200.56.200.0	/28	255.255.255.240	14	14
192.100.15.0	/26			
193.101.16.0	/29			
194.58.24.0	/30			
157.201.0.0	/23	255.255.254.0	126	510
191.254.0.0	/24			
128.10.0.0	/19			
174.200.0.0	/21			
185.14.0.0	/18			

Registered users may email for the solution. Send your request to solutions@soundtraining.net Be sure to specify which exercise solution you want.

Part II:

Identify the first available subnet

Identify the first range of IP addresses

NIC Number	Subnet Bits	1st Available Subnet	1st Range of IP Addresses
200.56.200.0	/28	200.56.200.16	200.56.200.17-30
192.100.15.0	/26		
193.101.16.0	/29		
194.58.24.0	/30		
157.201.0.0	/23	157.201.2.0	157.201.2.1-157.201.3.254
191.254.0.0	/24		
128.10.0.0	/19		
174.200.0.0	/21		
185.14.0.0	/18		

Registered users may email for the solution. Send your request to solutions@soundtraining.net Be sure to specify which exercise solution you want.

Student Exercise 4.3: IP Subnetting and Broadcasts

Calculate the following for your router (based on the lab map):
What is the class of address?
Calculate the subnet mask (in dotted decimal).
What is the subnet ID number? (Remember that the subnet ID and the subnet mask are two totally separate components.)
What is the broadcast address?
What is the total number of subnet bits? Host bits?
How many hosts per subnet?

Example: IP address 207.201.142.65/27
Remember to take it to binary.

Address:	11001111.11001001.10001110.01000001
Mask:	11111111.11111111.11111111.11100000

Subnet mask:	255.255.255.224
Subnet ID #:	64 (You could say “207.201.142.**64**”.)
Broadcast address:	207.201.142.95
Total # of subnet bits:	3
Total # of host bits:	5
Hosts per subnet:	30 (Remember 2^n-2?)

Internet Protocol Version 6

IPv6 is an evolutionary step from IPv4. The IPv4 protocol has many limitations including its 32 bit address space which supports only about 4,000,000,000 hosts. In addition, IPv4 is complicated to configure and has no built-in security.
IPv6 is designed to overcome those limitations. Its 128 bit address space supports 2^{128} addresses. That equates to 340 undecillion addresses! IPv6 includes built-in security technologies and supports auto-configuration.
IPv6 is installable as a software upgrade on Internet devices. It is designed for backwards compatibility and interoperability with IPv4 devices.
IPv6 is supported in CIOS 12.2(1)T.
For more information about IPv6, visit www.ipv6.org and www.6bone.net

Verifying Address Configuration

Traceroute

Supported by IP, VINES, and AppleTalk, Traceroute uses TTL values to generate messages from each router used along the path. TRACE shows each router between the source and destination. It probes each router three times and shows the duration of each probe.

PING

PING was created by Mike Muuss of the Army Research Laboratory in December of 1983 in about a day. It was developed in response to network difficulties he encountered.

PING is a very basic testing mechanism that is supported in IP, IPX, AppleTalk, and DECNet. It uses ICMP to verify hardware connection and logical address of the network layer. Simple ping works with defaults; extended ping allows custom configuration of the ping.

Many people believe that PING is an acronym for “Packet Internet Groper”, but Mike Muuss said that wasn’t his intent. He said that it was named after Navy SONAR, but suggested that the definition came later at the hands of Dr. Dave Mills, who had also done some work on a system to measure path latency using timed ICMP Echo packets.

Mike Muuss was killed in a car accident on November 20, 2000.

Telnet

Telnet is used to login to a remote site. The successful use of Telnet generally results in the login prompt of the destination host. A successful Telnet attempt verifies application layer software between source and destination stations. Telnet is the most complete test mechanism available, because it uses all seven layers of the OSI model.

Telnet is not only a remote login tool; it's also a comprehensive testing mechanism. Even if you can't authenticate on a remote machine, you can still use Telnet for testing. If you can get to an authentication prompt, you know that your IP configuration is working properly. Telnet requires all seven layers of the OSI model to function properly. If Telnet works, IP is correctly configured.

About this guide…

This guide is taken from soundtraining.net's workbook for ***Unlocking the Secrets of Cisco Router Configuration and Operation 2-Day Hands-On Workshop***. You can request information concerning onsite scheduling of this fast-paced, information-packed workshop by call 206.988.5858 or emailing cisco@soundtraining.net. Onsite training can be affordable for as few as two people! Also, be sure to check online at www.soundtraining.net for information concerning our public seminars and workshops schedules.

soundtraining.net is a Seattle, Washington based training firm, specializing in training for information technology professionals and business professionals. Training programs include Microsoft and Cisco networking and desktop workshops and seminars, project management and business process analysis seminars and workshops, and our one-day ***Trends in Technology*** briefing.

Contact soundtraining.net via email at trainers@soundtraining.net, by telephone at 206.988.5858, or via postal mail at:

soundtraining.net
Box 1321
Seahurst, WA 98062-1321

soundtraining.net
training for information technology
and business professionals