

Chapter 2

IP Addressing and Related Topics

At a Glance

Instructor's Manual Table of Contents

- Overview
- Objectives
- Teaching Tips
- Quick Quizzes
- Class Discussion Topics
- Additional Projects
- Additional Resources
- Key Terms
- Technical Notes for Hands-On Projects

Lecture Notes

Overview

This chapter covers the structure and function of IPv4 (Internet Protocol version 4) addresses - those arcane four-number sequences, such as 24.29.72.3, which uniquely identify all public network interfaces that use TCP/IP on the entire Internet. IPv6 (Internet Protocol version 6) and its addressing scheme are also discussed in this chapter, as are the differences between IPv4 and IPv6 and the latest updates of and features included with version 6. As you come to understand and appreciate IP addresses, you will learn how they are constructed, the classes into which they may (or may not) be relegated, and what roles these addresses play as traffic finds its way around a network.

Chapter Objectives

- Describe IP addressing, anatomy and structures, and addresses from a computer's point of view
- Recognize and describe IPv4 addressing and address classes, describe the nature of IPv4 address limitations, and define the terms *subnet*, *supernet*, *subnetting*, and *supernetting*
- Describe how to obtain public and private Internet addresses
- Explore IPv4 addressing schemes
- Describe the nature of IPv4 address limitations and why IPv6 is needed
- Discuss new and enhanced IPv6 features
- Recognize and describe IPv6 addressing schemes, features, and capacities
- Describe the impediments involved in transitioning from IPv4 to IPv6

Teaching Tips

IP Addressing Basics

1. Often we think of the “language” of computers as binary. While this is true, the computer does not “see” binary numbers. Instead, it responds to the presence or absence of electrical current. Binary ones and zeros are actually the presence and absence of that current.
2. Referring back to Chapter 1, students can think of domain names in the same way they think of a model. Network communication does not require domain names in order to work. That is why they are *symbolic*. The naming system is there to make it easier for people to use and understand networks, just like modeling systems.

3. The method of expressing IP addresses as octets is for human convenience. It is easier for a person to remember a group of numbers that are “broken up” in some manner, like a social security number or phone number, than to remember a long string of digits. The octet system represents a long string of binary numbers.
4. IP or OSI model Layer 3 addresses are routable and changeable, unlike the MAC or Layer 2 addresses. It is important for students that how a computer communicates on a network differs greatly depending on which addressing system is being used. In addition, both addressing systems work together to allow network communication.
5. On an individual computer, the network interface card (NIC) has the MAC address permanently “burned in” or assigned to the NIC. As long as that particular NIC is part of the computer, the computer’s MAC address never changes.
6. When a computer sends a datagram out onto the wire, the Layer 2 MAC address field contains the MAC address of the sending computer. The layer address field permanently contains the sending computer’s address. In order for the datagram to be forwarded throughout the network, whenever the datagram is received by a router or switch and is forwarded, the Layer 2 address encapsulation is stripped off and replaced with the Layer 2 MAC address of the router or switch’s sending interface. When the datagram is finally received by the destination computer, it reads the source MAC address of the datagram as the interface of the switch that most recently forwarded the datagram to the receiver, not the MAC address of the source computer.
7. Remind the class that, in a sense, a computer’s MAC address is part of the NIC installed on the computer, the MAC address is considered permanent and unchanging. In the sense that a datagram traveling across a network must change the source MAC address field every time it passes through a router or switch, the MAC address as a field in a datagram is considered changed.

IPv4 Addressing

1. Point out that if an IP address is manually assigned to a computer and another computer is already using that address, a message will be generated stating this and requesting that the user sets a different IP address.
2. Most networks of any size at all use DHCP (Dynamic Host Configuration Protocol) services to automatically assign IP addresses to all the hosts on a network. If the DHCP server is configured correctly, there should not be an issue with IP address conflict.

IP Address Classes

1. The idea of a network versus a host address is perhaps like the difference between a person’s city address and street address. Someone may live in a “network” like Chicago, New York, or Denver, but the “host” address within that network is 321 Bannock Street or 5678 Glenwood Avenue. The first address gets the “mail” to the general area and the second address delivers it to the specific location.

Quick Quiz 1

1. The physical numeric address functions at a sub-layer of the Data Link layer in the OSI network reference model, called the _____ layer.
Answer: Media Access Control (MAC)
2. True or False: Multicast addresses come in handy when a class of devices, such as routers, must be updated with the same information on a regular basis.
Answer: True
3. A(n) _____ is the router or other device that will forward traffic to the host's physical network.
Answer: IP gateway
4. True or False: Duplication of numeric IP addresses is not allowed because that would lead to confusion.
Answer: True

Network, Broadcast, Multicast, and Other Special IPv4 Addresses

1. As mentioned before, your students can think of addresses as being broken down from larger areas (like cities) to smaller areas (like street addresses). This is how IP addresses work. They are hierarchical and each portion describes a different aspect of the address. This is also how a zip code works on a letter a person mails.
2. Part of the hierarchy of addresses includes the host address and the broadcast address. These two addresses are held out or deducted from the total pool of addresses in any class.
3. The network portion is the address for the overall network. If you mail a letter to a friend in Austin, it first has to make it to Austin before finding the particular house. "Austin" is the network address.
4. A broadcast address is a bit more difficult to explain in the above analogy. If someone wants to send a message to all the devices on a single network, it would be like sending copies of the same letter to everyone in Austin. Perhaps this is akin to a mass mailing of some advertisement. Everybody gets the same information at pretty much the same time. Other than a broadcast, a network device will ignore any traffic on the network that is not addressed specifically to them.

<i>Teaching Tip</i>	For more information on broadcast, see: http://tools.ietf.org/html/rfc919
--------------------------------	--

Broadcast Packet Structures

1. The text mentions that IPv4 packets have two address fields: one at the Network Layer and one at the Data Link Layer. Broadcasts use the Data Link Layer (Layer 2 on the OSI Model) and these addresses are not forwarded by routers. The relationship between Network and Data Link Layer addresses and how computers communicate using them will be developed as class progresses.
2. Generally, network devices will ignore any traffic on the wire except for broadcasts and messages specifically addressed to them. This includes multicast (Class D) transmissions. Routers using multicast transmissions must be configured to “listen” for them or they will be ignored. This will result in a router that is “out of touch” with changes to the routing tables, such as if a driver on the modern U.S. freeway system was using a map from 1964.

Quick Quiz 2

1. A(n) _____ is a network address that all hosts on a network must read.
Answer: broadcast address
2. Formerly, addresses were under the auspices of _____.
Answer: Internet Assigned Numbers Authority (IANA)
3. True or False: If two network interfaces are on the same physical network, they can communicate directly with one another at the MAC layer.
Answer: True
4. True or False: Originally, when IP addresses were assigned for public use, they were assigned on a per-network basis.
Answer: True

IPv4 Networks and Subnets Masks

1. Introduce the concept of a subnet mask. Note that this topic can be particularly challenging for students.

IPv4 Subnets and Supernets

1. The key to supernetting is to use subnets that are contiguous, that is, their ranges are numerically (in binary) “next to” each other. This allows two or more subnets to be combined. Typically, you will see Class C addresses most often supernetted.
2. Constant-length subnet masks (CLSM) are what most people think of when they think of subnet masks. In a production environment, you are more likely to hear the word “subnet” thrown around than “CLSM”.

3. A variable-length subnet mask (VLSM) is subnetting across a class boundary. Basically, it is subnetting a subnet. The protocol used by routers in these network environments must support extended network prefix information.
4. Generally when you create a particular subnet, you are trying to satisfy a set of requirements for a number of networks in your environment and a number of valid host addresses within each network. Do not forget to figure in potential growth. If a network designer calculates subnets to only satisfy the current requirements of the organization, these networks will not have the ability to expand when more users are added.
5. Supernetting is actually a form of Classless Inter-Domain Routing (CIDR), as will be seen in the next major section.
6. The one restriction in supernetting is one of boundaries. The value of the 3rd octet of the lower address must be divisible by 2 in order to combine two subnets, divisible by 4 to combine four subnets, and so on.

Classless Inter-Domain Routing (CIDR) in IPv4

1. As mentioned earlier, all addresses in a CIDR address must be contiguous.
2. To clarify this point, address aggregation is where a single address will represent multiple networks in a routing table. These “multiple addresses” are combined by CIDR to appear as a single network.
3. Unlike CLSM, where you lose a significant number of host addresses by subdividing a network, in CIDR you can use the entire range of addresses available. For example, with the network address of 224.127.97.8/20, the “/20” (called the “CIDR notation”) is interpreted to mean that the network portion of the address is the first 20 bits leaving the remaining 12 bits for host addresses. This results in 4094 host addresses available in this network.
4. In terms of “classful” networks, a standard Class A network uses 8 bits for the network portion of its address so it is a /8 address. A Class B network uses 16 bits for the network address so it is a /16 and a Class C network uses 24 bits for the network address so it is a /24. In CIDR, you can use any number of bits for the network address ignoring class limitations (leaving two bits available to support hosts).

Public versus Private IPv4 Addresses

1. Most private networks including home labs and small office/home office (SOHO) networks use private IP addresses. It is very typical to have one computer act as the interface between the internal network and the Internet, even on home networks. This computer will have a NIC configured to a private IP address on the same subnet as the other internal computers and a dial-up, xDSL (Digital Subscriber Service), or cable modem creating the link to the Internet. The modem interface will be assigned a public IP address from the ISP and this computer must be configured to share its Internet connection with the other computers on the private network.

2. The text mentions that IP Security (IPSec), a form of secure, encrypted information transfer, cannot be used in conjunction with NAT since the private address cannot be translated and thus routed to the Internet. There is a way around this. Instead of establishing an IPSec tunnel directly from computer to computer, establish it from perimeter device that does the NAT translation to the other computer outside the network. This is typically done firewall to firewall and would only apply to this particular link. All other standard traffic to and from the Internet would go through NAT translation.
3. The text mentions the issue of lag time in changing name to address resolution in this section. A practical example would be eBay or Amazon. Imagine how much revenue each one of them would lose if they had to re-establish name to address resolution, waiting up to 72 hours to be able to send and receive traffic on the Internet.
4. This would be a good time to review RFCs 2709 and 3104 with your students.

Quick Quiz 3

1. A(n) _____ is a special bit pattern that “blocks off” the network portion of an IP address with an all-ones pattern.
Answer: subnet mask
2. The simplest form of subnet masking uses a technique called _____, in which each subnet includes the same number of stations and represents a simple division of the address space made available by subnetting into multiple equal segments.
Answer: constant-length subnet masking (CLSM)
3. True or False: CIDR addresses are commonly applied to Class A addresses.
Answer: False
4. A(n) _____ is a device that interconnects multiple IP networks or subnets.
Answer: IP gateway

Managing Access to IPv4 Address Information

1. Although it is valid to use NAT as part of your network security strategy, it is generally recommended that multiple methods of security be employed. Reverse proxying would be part of a layered security approach.

Obtaining Public IP Addresses

1. To emphasize what the text already mentions, it is extremely common for organizations and individuals alike to lease their public addresses from an ISP rather than purchase them.

IPv4 Addressing Schemes

1. In this section, you will discuss the need for IP addressing schemes, and how to create and document one.

The Network Space

1. There are a number of critical factors that typically constrain IP addressing schemes, and we look at these in two groups. The first group of constraints determines the number and size of networks. These are:
 - Number of physical locations
 - Number of network devices at each location
 - Amount of broadcast traffic at each location
 - Availability of IP addresses
 - Delay caused by routing from one network to another
2. The second group that helps us determine how to choose which IP addresses go where are these design objectives:
 - Minimize the size of the routing tables.
 - Minimize the time required for the network to “converge.”
 - Maximize flexibility and facilitate management and troubleshooting.

The Host Space

1. The point of planning growth for networks was previously mentioned. You can re-emphasize it here. One of the important things that go along with an organized host space and network addressing scheme is accurate documentation of the network. While this is not a requirement of the class, it would be helpful for the students to see the relationship between having a logical and organized network and being able to document it.

**Teaching
Tip**

For more information on documentation tools, see:
<http://www.more.net/technical/netserv/diagrams/index.html>

The End of the IPv4 Address Space

1. As corporate network use and the Internet grew in popularity, vast numbers of IP address were purchased including large sections of Class A addresses. A single Class A network address includes a huge number of hosts per network. Owners of these Class A networks, even now, possess a large storehouse of unused host addresses.
2. In addition to the program, the text mentions about a “brisk trade” in IP addresses, there is a voluntary “buy back” program run by ICANN to reclaim portions of the above-mentioned addresses that have never been used.
3. The text mentions how many companies rent rather than buy their addresses from ISPs. You might mention to your class that they are also part of the group that rents IP addresses. Every time we go on the Internet, our ISP temporarily assigns us an IP address from a pool they own, allowing us to have an address that is routable on the Internet and saving us the expense of buying one of our own.
4. Point out that if your private network will never go on the Internet, you can use any address. However, if you try to use those addresses to surf the Web, you will find they are already owned. Encourage your students to use a private IP addressing scheme, even for their home or lab networks.

Quick Quiz 4

1. _____ permits the proxy server to front for servers inside the boundary by advertising only the proxy server’s address to the outside world, and then forwarding only legitimate requests for service to internal servers for further processing.
Answer: Reverse proxying
2. Because all devices accessible to the Internet must have public IP addresses, changing providers often means going through a tedious exercise called _____.
Answer: IP renumbering
3. Switches make their decisions with specialized hardware known as _____.
Answer: Application Specific Integrated Circuits (ASICs)
4. True or False: The time it takes to route from one network to another is affected by the size of the routing table.
Answer: True

Introducing IPv6

1. As described before, IPv6 solves many of the problems in IPv4, including the size of the address space and the lack of security by using encryption and authentication. In this section, you will discuss IPv6 in greater detail.

Request for Comments Pages and Depreciation

1. We already discussed RFCs in Chapter 1. Nonetheless, take this opportunity to reinforce this concept and point your students to RFCs specific to IPv6 such as the RFC 5156.

Teaching Tip	RFC 5156 could be found at: http://tools.ietf.org/html/rfc5156 .
-------------------------	---

IPv6 Addressing

1. Although IPv6 addresses are very different from their IPv4 counterparts, there are some similarities. For example, the notion of host and network portions is present on both schemes.

Address Format and Notation

1. At first, IPv6 addresses might look strange, especially if you compare them with IPv4 addresses. Take this opportunity to explain the basic format and notation of IPv6 addresses. In the next section, you will talk about the network and host portion of the address.

Network and Host Address Portions

1. Explain how to represent the network and host portion of an IPv6 address, which is similar to the CIDR notation studied before.

Scope Identifier

1. Later in this chapter, you will review multicast addresses in IPv6 but for now, explain to your students that multicast addresses in IPv6 use a scope identifier, a 4-bit field that limits the valid range for a multicast address to define the portion of the Internet to which the multicast group pertains.

Interface Identifiers

1. Like IPv4, IPv6 also requires that every network interface have its own unique identifier. But although IPv6 specified that interface identifiers follow the modified EUI-64 format, many software makers, including Microsoft, use the privacy format defined in RFC 4941.

2. This is a good opportunity to ask your students to think about the problems of following different standards, something that is somewhat common in the networking industry.

**Teaching
Tip**

RFC 4941 could be found at: <http://tools.ietf.org/html/rfc4941>.

Native IPv6 Addresses in URLs

1. A typical URL contains the colon character (:) and can be confusing when studying IPv6 addresses. RFC 2732 describes a method to express IPv6 addresses in a form compatible with HTTP URLs.

Address Types

1. While the old IPv4 classful address structure was designed as much for ease of human understanding as it was for machine usability, the new IPv6 address types take advantage of years of experience with routing across large hierarchical domains to streamline the whole operation.
2. Describe the following address types, emphasizing how each type relates to an specific IPv4 addressing need:
 - a. Unspecified
 - b. Loopback
 - c. Multicast
 - d. Anycast
 - e. Unicast
 - f. Aggregatable global unicast
 - g. Link-local
 - h. Site-local
3. Mention that IPv4 broadcast addresses have been replaced by multicast addresses in IPv6.

Address Allocations

1. Mention that IPv6 pre-allocates only about 15 percent of its available addresses. Using Table 2-7, describe address allocations in IPv6.

IPv6 Addressing and Subnetting Considerations

1. Remind your students about the purposes of subnetting. Explain that “subnetting” an IPv6 address space isn’t technically necessary, but totally possible.
2. Use the example provided in the text to explain how to subnet an IPv6 address.

The IPv4 to IPv6 Transition

1. As you can imagine, moving from IPv4 to its newer version is not an easy matter. In this section, describe the following techniques that will allow IPv4 and IPv6 hosts and networks to exist together until a full transition is reached:
 - a. Teredo tunneling
 - b. ISATAP or Intra-Site Automatic Tunnel Addressing Protocol
 - c. 6to4 tunneling
 - d. NAT-PT (Network Address Translation-Protocol Translation)

Class Discussion Topics

1. Have the class discuss why a large corporation that bought a Class A network 20 years ago would be reluctant to sell back even a portion of their unused host addresses to help conserve overall resources.
2. Have the class discuss the pros and cons of using a subnet mask calculator versus manually calculating subnet masks.
3. Have the class discuss the benefits of using reverse proxying from a security standpoint. Are additional methods required to protect the network from external attack? Why or why not? If more security methods are required, which ones would they choose?
4. Have the class discuss the pros and cons of start using IPv6 immediately.

Additional Projects

1. Assign the class the task of briefly documenting the classroom LAN including PCs, switches, routers, and printers, making sure they assign an IP addressing scheme. The class can break up into small groups for this project.
2. Have the class open a command prompt on their computers and type in: “ipconfig/all”. Have them identify the class of address used, the subnet mask, the default gateway address and the DNS server address(es). If your class LAN uses a customized subnet mask, how many bits were borrowed? Have them calculate the number of networks and hosts supported by this network address configuration.

Additional Resources

1. For a good essay on IP multicast as well as the OSI model in general, go to <http://ntrg.cs.tcd.ie/undergrad/4ba2/multicast/>.

2. The article: “What is an IP Address?” is basic, but helpful, and can be found at <http://www.howstuffworks.com>. Search for the title of the article once on the site.
3. A very good article on NAT can be found at: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml
4. A review of the relevant Request for Comment documents will be helpful. The students should be able to look up this information with a search engine or by entering the RFC numbers in the browser address window:

NAT and IPsec	RFC 2709 and 3104
Subnets	RFC 950
Private Addresses	RFC 1918
VLSN	RFC 1878
CIDR	RFC 1517, 1518, and 1519
Multicast extensions to OSPF (open shortest path first)	RFC 1584

Key Terms

- **::**—In IPv6 addresses, a pair of colon characters stands for several contiguous 16-bit groups, each of which is all zeroes. This notation can be used only once in any address.
- **address masquerading** — A method of mapping many internal (i.e., private), nonroutable addresses to a single external (i.e., public) IP address for the purpose of sharing a single Internet connection (also referred to as “address hiding”).
- **aggregatable global unicast address** — The layout of these IPv6 addresses breaks the leftmost 64 bits of the address into explicit fields to allow for easier routing. Specifically, it allows routes to these addresses to be “aggregated”—that is, combined into a single entry in the router table.
- **anycast address** —A type of address in IPv6, an anycast address is an ordinary address that can be assigned to more than one host or interface. Packets pointed to an anycast address are delivered to the holder of that address nearest to the sender in terms of routing distance. An anycast address does not apply to IPv4.
- **Application Specific Integrated Circuit (ASIC)** — A special-purpose form of integrated circuit. An ASIC provides a way to implement specific programming logic directly into chip form, thereby also providing the fastest possible execution of such programming logic when processing data. ASICs are what make it possible for high-speed, high-volume routers to perform complex address recognition and management functions that can keep up with data volumes and time-sensitive processing needs.
- **Bitcricket IP Calculator** — A downloadable subnet mask calculator produced by WildPackets that provides both IPv4 and IPv6 support.
- **broadcast address** —The all-ones address for a network or subnet, this address provides a way to send the same information to all interfaces on a network.

- **Classless Inter-Domain Routing (CIDR)** —A form of subnet masking that does away with placing network and host address portions precisely on octet boundaries, but instead uses the */n* prefix notation, in which *n* indicates the number of bits in the network portion of whatever address is presented.
- **constant-length subnet masking (CLSM)** — An IP subnetting scheme in which all subnets use the same size subnet mask, which therefore divides the subnetted address space into a fixed number of equal-size subnets.
- **domain name** —A symbolic name for a TCP/IP network resource; the Domain Name System (DNS) translates such names into numeric IP addresses so outbound traffic may be addressed properly.
- **Domain Name System (DNS)** —The TCP/IP Application layer protocol and service that manages an Internet-wide distributed database of symbolic domain names and numeric IP addresses so users can ask for resources by name, and get those names translated into the correct numeric IP addresses.
- **dot quad** — *See* dotted decimal notation.
- **dotted decimal notation** — The name for the format used to denote numeric IP addresses, such as 172.16.1.7, wherein four numbers are separated by periods (dots).
- **end-to-end connection** — A network connection in which the original sending and receiving IP addresses may not be altered, and where a communications connection extends all the way from sender to receiver while that connection remains active.
- **EUI-64 format** — An IEEE transformation permitting the burned-in MAC addresses of NICs to be padded in particular ways to create globally unique 64-bit interface identifiers for each interface.
- **extended network prefix** —The portion of an IP address that represents the sum of the network portion of the address, plus the number of bits used for subnetting that network address. A Class B address with a three-bit subnetting scheme would have an extended network prefix of /19, 16 bits for the default network portion, plus three bits for the subnetting portion of that address, with a corresponding subnet mask of 255.255.224.0.
- **firewall** —A network boundary device that sits between the public and private sides of a network, and provides a variety of screening and inspection services to ensure that only safe, authorized traffic flows from outside to inside (used in the sense of a barrier designed specifically to block the spread of fire in houses or cars).
- **hop** — A single transfer of data from one network to another, through some kind of networking device. Router-to-router transfers are often called hops. The number of hops often provides a rough metric of the distance between a sender's network and a receiver's network. The number of routers that a packet must cross, or the number of routers that a packet crosses, represents the hop count from the source network to the target network.
- **host portion** — The rightmost bits in an IP address, allocated to identify hosts on a supernetwork, network, or subnetwork.
- **Internet Assigned Numbers Authority (IANA)** — The arm of the ISOC originally responsible for registering domain names and allocating public IP addresses. This job is now the responsibility of ICANN.
- **Internet Service Provider (ISP)** — An organization that provides Internet access to individuals or organizations as a primary line of business. Currently, ISPs are the source for public IP addresses for most organizations seeking Internet access.

- **IP gateway** —TCP/IP terminology for a router that provides access to resources outside the local subnet network address. (A default gateway is the name given to the TCP/IP configuration entry for clients that identifies the router they must use to send data outside their local subnet areas.)
- **IP renumbering**—The process of replacing one set of numeric IP addresses with another set of numeric IP addresses because of a change in ISPs, or an address reassignment.
- **Layer 3 switch** — A type of networking device that combines hub, router, and network management functions within a single box. Layer-3 switches make it possible to create and manage multiple virtual subnets in a single device, while offering extremely high bandwidth to individual connections between pairs of devices attached to that device.
- **link layer** — This is the lowest level of the Internet Protocol suite and represents the elements and protocols found in the OSI layer's Data Link and Physical layers.
- **link-local address** — An addressing scheme that is designed to be used only on a single segment of a local network.
- **Loopback address**—An address that points directly back to the sender. In IPv4, the ClassA domain 127.0.0.0 (or 127.0.0.1 for a specific machine address) is reserved for loopback. In IPv6, there is a single loopback address, written “::1” (all 0s, except for that last bit, which is 1). By passing traffic down through the TCP/IP stack, then back up again, the loopback address can be used to test a computer's TCP/IP software.
- **Media Access Control (MAC) layer** —A sub-layer of the Data Link layer. This layer is part of the Media Access Control definition, in which network access methods, such as Ethernet and token ring, apply.
- **Media Access Control (MAC) layer address** — A special type of network address, handled by a sublayer of the Data Link layer, normally pre-assigned on a per-interface basis to uniquely identify each such interface on any network cable segment (or virtual facsimile).
- **multicast address** — One of a block of addresses reserved for use in sending the same message to multiple interfaces or nodes. Members of a community of interest subscribe to a multicast address in order to receive router updates, streaming data (video, audio, teleconferencing), and so on. In IPv4, the Class D block of addresses is reserved for multicast. In IPv6, all multicast addresses begin with 0xFF. ICANN, with the help of IANA, manages all such address adjustments.
- **network address** —That portion of an IP address that consists of the network prefix for that address; an extended network prefix also includes any subnetting bits. All bits that belong to the extended network prefix show up as 1s in the corresponding subnet mask for that network.
- **Network Address Translation (NAT)** — A special type of networking software that manages network connections on behalf of multiple clients on an internal network and translates the source address for all outbound traffic from the original source to the address of the outbound network interface. NAT software also manages forwarding replies to all outgoing traffic back to its original sender. NAT software is often used to allow clients using private IP addresses to access the Internet.
- **network portion** — The leftmost octets or bits in a numeric IP address, the network portion of an IP address identifies the network and subnet portions of that address. The value assigned to the prefix number identifies the number of bits in the network portion of any IP address. (For example, 10.0.0.0/8 indicates that the first eight bits of the address are the network portion for the public Class A IP address.)

- **network prefix** —That portion of an IP address that corresponds to the network portion of the address; for example, the network prefix for a Class B address is /16 (meaning that the first 16 bits represent the network portion of the address, and 255.255.0.0 is the corresponding default subnet mask).
- **Network Service Access Point (NSAP)** — A type of hierarchical address scheme used to implement Open System Interconnection (OSI) network layer addressing and a logical point between the network and transport layers in the OSI model.
- **numeric address** — *See* numeric IP address.
- **numeric IP address** —An IP address expressed in dotted decimal or binary notation.
- **octet** —TCP/IP terminology for an eight-bit number; numeric IPv4 addresses consist of four octets.
- **organizationally unique identifier (OUI)** —A unique identifier assigned by IANA or ICANN that's used as the first three bytes of a NIC's MAC layer address to identify its maker or manufacturer.
- **physical numeric address** —Another term for MAC layer address (or MAC address).
- **private IP address** —Any of a series of Class A, B, and C IP addresses reserved by IANA for private use, documented in RFC 1918, and intended for uncontrolled private use in organizations. Private IP addresses may not be routed across the Internet because there is no guarantee that any such address is unique.
- **proxy server** —A special type of network boundary service that interposes itself between internal network addresses and external network addresses. For internal clients, a proxy server makes a connection to external resources on the client's behalf and provides address masquerading. For external clients, a proxy server presents internal resources to the public Internet as if they are present on the proxy server itself.
- **public IP address**—Any TCP/IP address allocated for the exclusive use of some particular organization, either by IANA or ICANN, or by an ISP to one of its clients.
- **Quality of Service (QoS)** — A specific level of service guarantee associated with Application layer protocols in which time-sensitivity requirements for data (such as voice or video) require that delays be controlled within definite guidelines to deliver viewable or audible data streams.
- **reverse proxying** —The technique whereby a proxy server presents an internal network resource (for example, a Web, e-mail, or FTP server) as if it were present on the proxy server itself so external clients can access internal network resources without seeing internal network IP address structures.
- **route aggregation**—A form of IP address analysis that permits routers to indicate general interest in a particular network prefix that represents the “common portion” of a series of IP network addresses, as a way of reducing the number of individual routing table entries that routers must manage.
- **scope identifier** — In IPv6, a 4-bit field limiting the valid range for a multicast address. In IPv6 multicast addresses, not all values are defined, but among those defined are the site-local and the link-local scope. Multicast addresses are not valid outside their configured scope and will not be forwarded beyond it.
- **site-local address** — An addressing scheme limited to use in private networks within a specific site.
- **subnet mask** —A special bit pattern that masks off the network portion of an IP address with all 1s.
- **subnetting**—The operation of using bits borrowed from the host portion of an IP address to extend and subdivide the address space that falls beneath the network portion of a range of IP addresses.

- **summary address** — A form of specialized IP network address that identifies the “common portion” of a series of IP network addresses used when route aggregation is in effect. This approach speeds routing behavior and decreases the number of entries necessary for routing tables.
- **supernetting** — The technique of borrowing bits from the network portion of an IP address and lending those bits to the host part, creating a larger address space for host addresses.
- **symbolic name**—A human-readable name for an Internet resource, such as *www.course.com* or *www.microsoft.com*. Also, a name used to represent a device instead of an address. For example, the name *serv1* could be a symbolic name for a device that uses the IP address 10.2.10.2.
- **unspecified address** — In IPv6, the unspecified address is all zeroes and can be represented as “::” in normal notation. This is essentially the address that is no address. It cannot be used as a destination address.
- **variable-length subnet masking (VLSM)** —A subnetting scheme for IP addresses that permits containers of various sizes to be defined for a network prefix. The largest subnet defines the maximum container size, and any individual container in that address space may be further subdivided into multiple, smaller sub-containers (sometimes called sub-subnets).
- **words** — Blocks of four, 16-bit values in an IPv6 address; each word is separated by a colon, and there are eight words in every IPv6 address. If a word is made up of contiguous zeros, it can be compressed so that the zeros do not appear in the address but the colon separators remain.

Technical Notes for Hands-On Projects

The lab setup for Chapter 2 includes the following elements:

HANDS-ON PROJECT	NETWORK DEVICES REQUIRED	WORKSTATION OPERATING SYSTEM REQUIRED	OTHER RESOURCES REQUIRED
2 – 1	Internet Connection	Windows XP/Vista/7	Download and install Bitcricket IP Calculator
2 – 2		Windows XP/Vista/7	Bitcricket IP Calculator
2 – 3		Windows XP/Vista/7	Bitcricket IP Calculator
2 – 4	Internet Connection	Windows XP/Vista/7	Web browser
2 – 5	Internet Connection	Windows XP/Vista/7	Web browser
2 – 6	Network interface card	Windows XP/Vista/7	
2 – 7	Network interface card	Windows XP/Vista/7	