Physical, Logical, and Virtual Addressing

Physical, logical, and virtual addressing in computer networks requires a basic understanding of decimal (base10), binary (base2), and hexadecimal (base16) numbering (see Table 2-1).

The decimal (base10) numbering system is, of course, what we all are taught in school. It comprises the numerals 0 through 9. After the number 9, we add a digit ("1") in the "tens" position and begin again at zero in the "ones" position, thereby creating the number 10. Humans use the decimal numbering system because we have ten fingers, so a base10 numbering system is easiest for humans to understand.

Table 2-1 Decimal, Hexadecimal, and Binary Notation

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

A binary (base2) numbering system comprises only two digits: 1 (“on”) and 0 (“off”). Binary numbering is used in computers and networking because they use electrical transistors (rather than fingers) to count. The basic function of a transistor is a gate: When electrical current is present, the gate is closed (“1” or “on”). When no electrical current is present, the gate is open (“0” or “off”). With only two digits, a binary numbering system increments to the next position more frequently than a decimal numbering system. For example, the decimal number one is represented in binary as “1,” number two is represented as “10,” number three is represented as “11,” and number four is represented as “100.”

A hexadecimal (base16) numbering system comprises 16 digits (0 through 9, and A through F). Hexadecimal numbering is used because it is more convenient to represent a byte (which consists of 8 bits) of data as two digits in hexadecimal, rather than eight digits in binary. The decimal numbers 0 through 9 are represented as in hexadecimal “0” through “9,” respectively. However, the decimal number 10 is represented in hexadecimal as “A,” the number 11 is represented as “B,” the number 12 is represented as “C,” the number 13 is represented as “D,” the number 14 is represented as “E,” and the number 15 is represented as “F.” The number 16 then increments to the next numeric position, represented as “10.”

The physical address of a network device, known as a *media access control* (MAC) address (also referred to as a burned-in address [BIA] or hardware address), is used to forward traffic on a local network segment. The MAC address is a unique 48-bit identifier assigned to the network adapter of a device. If a device has multiple NICs, each NIC must have a unique MAC address. The MAC address is usually assigned by the device manufacturer and is stored in the device read-only memory (ROM) or firmware. MAC addresses are typically expressed in hexadecimal format with a colon or hyphen separating each 8-bit section. An example of a 48-bit MAC address is:

00:40:96:9d:68:16

The logical address of a network device, such as an IP address, is used to route traffic from one network to another. An IP address is a unique 32-bit or 128-bit (IPv4 and IPv6, respectively) address assigned to the NIC of a device. If a device has multiple NICs, each NIC may be assigned a unique IP address, or multiple NICs may be assigned a virtual IP address to enable bandwidth aggregation or failover capabilities. IP addresses are statically or dynamically (most commonly using *Dynamic Host Configuration Protocol*, or DHCP) assigned, typically by a network administrator or network service provider (NSP). IPv4 addresses are usually expressed in dotted decimal notation with a dot separating each decimal section (known as an *octet*). An example of an IPv4 address is:

192.168.0.1

IPv6 addresses are typically expressed in hexadecimal format (32 hexadecimal numbers grouped into eight blocks) with a colon separating each block of four hexadecimal digits (known as a *hextet*). An example of an IPv6 address is:

2001:0db8:0000:0000:0008:0800:200c:417a

IPv4 and IPv6 addressing is explained later in this document.

Key Terms

A *media access control* (MAC) address is a unique 48-bit or 64-bit identifier assigned to a network interface card (NIC) for communications at the Data Link layer of the OSI model (discussed in Section 2.2.1).

Dynamic Host Configuration Protocol (DHCP) is a network management protocol that dynamically assigns (leases) IP addresses and other network configuration parameters (such as *default gateway* and DNS information) to devices on a network.

A *default gateway* is a network device, such as a router or switch, to which an endpoint sends network traffic when a specific destination IP address is not specified by an application or service, or when the endpoint does not know how to reach a specified destination.

An *octet* is a group of 8 bits in a 32-bit IPv4 address.

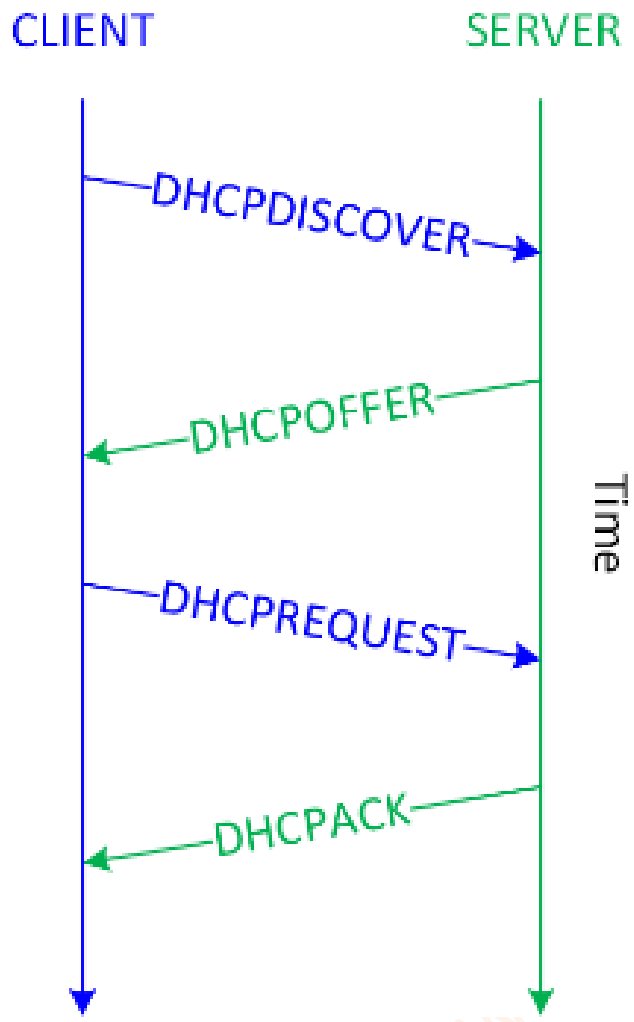
A *hextet* is a group of four 4-bit hexadecimal digits in a 128-bit IPv6 address.

Address Resolution Protocol (ARP) translates a logical address, such as an IP address, to a physical MAC address. *Reverse Address Resolution Protocol* (RARP) translates a physical MAC address to a logical address.

DHCP is a network management protocol used to dynamically assign IP addresses to devices that do not have a statically assigned (manually configured) IP address on a TCP/IP network. Bootstrap Protocol (BOOTP) is a similar network management protocol that is commonly used on Unix and Linux TCP/IP networks. When a network-connected device that does not have a statically assigned IP address is powered on, the DHCP client software on the device broadcasts a DHCPDISCOVER message on UDP port 67. When a DHCP server on the same subnet (or a different subnet if a DHCP Helper or DHCP Relay Agent is configured) as the client receives the DHCPDISCOVER message, it reserves an IP address for the client and sends a DHCPOFFER message to the client on UDP port 68. The DHCPOFFER message contains the MAC address of the client, the IP address that is being offered, the subnet mask, the lease duration, and the IP address of the DHCP server that made the offer. When the client receives the DHCPOFFER, it broadcasts a DHCPREQUEST message on UDP port 67, requesting the IP address that was offered. A client may receive DHCPOFFER messages from multiple DHCP servers on a subnet but can accept only one offer. When the DHCPREQUEST message is broadcast, the other DHCP servers that sent an offer that was not requested (in effect, accepted) in the DHCPREQUEST message will withdraw their offers. Finally, when the correct DHCP server receives the DHCPREQUEST message, it sends a DHCPACK (acknowledgment) message on UDP port 68, and the IP configuration process is completed (see Figure 2-1).

Figure 2-1

DHCP operation



Network address translation (NAT) virtualizes IP addresses by mapping private, non-routable IP addresses that are assigned to internal network devices to public IP addresses when communication across the internet is required. NAT is commonly implemented on firewalls and routers to conserve public IP addresses.

Key Terms

Network address translation (NAT) virtualizes IP addresses by mapping private, non-routable IP addresses assigned to internal network devices to public IP addresses.

IP addressing basics

Data packets are routed over a Transmission Control Protocol/Internet Protocol (TCP/IP) network using IP addressing information. IPv4, which is the most widely deployed version of IP, consists of a 32-bit logical IP address. The first four bits in an octet are known as the *high-order* bits; the first bit in the octet is referred to as the *most significant* bit. The last four bits in an octet are known as the *low-order* bits; the last bit in the octet is referred to as the *least significant* bit.

As shown in Table 2-2, each bit position represents its value if the bit is "on" (1); otherwise, the bit's value is zero ("off" or 0).

Key Terms

The first four bits in a 32-bit IPv4 address octet are referred to as the *high-order* bits.

The last four bits in a 32-bit IPv4 address octet are referred to as the *low-order* bits.

The first bit in a 32-bit IPv4 address octet is referred to as the *most significant* bit.

The last bit in a 32-bit IPv4 address octet is referred to as the *least significant* bit.

Table 2-2

Bit Position Values in an IPv4 Address

High-order bits				Low-order bits			
128	64	32	16	8	4	2	1

Each octet contains an 8-bit number with a value of 0 to 255. Table 2-3 shows a partial list of octet values in binary notation.

Table 2-3

Binary Notation of Octet Values

Decimal	Binary	Decimal	Binary	Decimal	Binary
255	1111 1111	172	1010 1100	64	0100 0000
254	1111 1110	170	1010 1010	32	0010 0000
253	1111 1101	160	1010 0000	16	0001 0000
252	1111 1100	150	1001 0110	8	0000 1000
251	1111 1011	140	1000 1100	7	0000 0111
250	1111 1010	130	1000 0010	6	0000 0110
249	1111 1001	128	1000 0000	5	0000 0101
248	1111 1000	120	0111 1000	4	0000 0100
224	1110 0000	110	0110 1110	3	0000 0011
200	1100 1000	100	0110 0100	2	0000 0010
192	1100 0000	96	0110 0000	1	0000 0001
180	1011 0100	90	0101 1010	0	0000 0000

The five IPv4 address classes (indicated by the high-order bits) are shown in Table 2-4.

Table 2-4

IP Address Classes

Class	Purpose	High-Order Bits	Address Range	Max. # of Hosts
A	Large networks	0	1 to 126	16,777,214
B	Medium-size networks	10	128 to 191	65,534
C	Small networks	110	192 to 223	254
D	Multicast	1110	224 to 239	–
E	Experimental	1111	240 to 254	–

The address range 127.0.0.1 to 127.255.255.255 is a loopback network used for testing and troubleshooting. Packets sent to a loopback (or localhost) address – such as 127.0.0.1 – are immediately routed back to the source device.

A *subnet mask* is a number that hides the network portion of an IPv4 address, leaving only the host portion of the IP address. The network portion of a subnet mask is represented by contiguous "on" (1) bits beginning with the most significant bit. For example, in the subnet mask 255.255.255.0, the first three octets represent the network portion and the last octet represents the host portion of an IP address. Recall that the decimal number 255 is represented in binary notation as 1111 1111 (refer to Table 2-2).

Key Terms

A *subnet mask* is a number that hides the network portion of an IPv4 address, leaving only the host portion of the IP address.

The default (or standard) subnet masks for Class A, B, and C networks are:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0

Several IPv4 address ranges are reserved for use in private networks and are not routable on the internet, including:

10.0.0.0–10.255.255.255 (Class A)

172.16.0.0–172.31.255.255 (Class B)

192.168.0.0–192.168.255.255 (Class C)

The 32-bit address space of an IPv4 address limits the total number of unique public IP addresses to about 4.3 billion. The widespread use of NAT (discussed in Section 2.1) delayed the inevitable depletion of IPv4 addresses, but, as of 2018, the pool of available IPv4 addresses that can be assigned to organizations has officially been depleted. (A small pool of IPv4 addresses has been reserved by each regional internet registry to facilitate the transition to IPv6.) IPv6 addresses, which use a 128-bit hexadecimal address space providing about 3.4×10^{38} (340 hundred undecillion) unique IP addresses, was created to replace IPv4 when the IPv4 address space was exhausted.

IPv6 addresses consist of 32 hexadecimal numbers grouped into eight hextets of four hexadecimal digits, separated by a colon. A hexadecimal digit is represented by 4 bits (refer to Table 2-1), so each hextet is 16 bits (four 4-bit hexadecimal digits), and eight 16-bit hextets equals 128 bits.

An IPv6 address is further divided into two 64-bit segments: The first (also referred to as the "top" or "upper") 64 bits represent the network part of the address, and the last (also referred to as the "bottom" or "lower") 64 bits represent the node or interface part of the address. The network part is further subdivided into a 48-bit global network address and a 16-bit subnet. The node or interface part of the address is based on the MAC address (discussed in Section 2.1) of the node or interface.

The basic format for an IPv6 address is:

xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx

where x represents a hexadecimal digit (0–f).

This is an example of an IPv6 address:

2001:0db8:0000:0000:0008:0800:200c:417a

The Internet Engineering Task Force (IETF) has defined several rules to simplify an IPv6 address:

- Leading zeros in an individual hextet can be omitted, but each hextet must have at least one hexadecimal digit, except as noted in the next rule. Applying this rule to the previous example yields this result: 2001:db8:0:0:8:800:200c:417a.
- Two colons (::) can be used to represent one or more groups of 16 bits of zeros, and leading or trailing zeroes in an address; the two colons (::) can appear only once in an IPv6 address. Applying this rule to the previous example yields this result: 2001:db8::8:800:200c:417a.
- In mixed IPv4 and IPv6 environments, the form x:x:x:x:x;x:d.d.d.d can be used, in which x represents the six high-order 16-bit hextets of the address and d represents the four low-order 8-bit octets (in standard IPv4 notation) of the address. For example, 0db8:0:0:0:0:FFFF:129.144.52.38 is a valid IPv6 address. Application of the previous two rules to this example yields this result: db8::ffff:129.144.52.38.

IPv6 security features are specified in Request for Comments (RFC) 7112 and include techniques to prevent fragmentation exploits in IPv6 headers and implementation of Internet Protocol Security (IPsec, discussed in Section 2.3.4.6) at the Network layer of the OSI model (discussed in Section 2.2.1).

2.1.2 Introduction to subnetting

Subnetting is a technique used to divide a large network into smaller, multiple subnetworks by segmenting an IP address into two parts: the network and the host. Subnetting can be used to limit network traffic or limit the number of devices that are visible to, or can connect to, each other. Routers examine IP addresses and subnet values (called masks) and determine whether to forward packets between networks. With IP addressing, the subnet mask is a required element.

Key Terms

Subnetting is a technique used to divide a large network into smaller subnetworks.

For a Class C IPv4 address, there are 254 possible node (or host) addresses (2^8 or 256 potential addresses, but you lose two addresses for each network: one for the base network address and the other for the broadcast address). A typical Class C network uses a default 24-bit subnet mask (255.255.255.0). This subnet mask value identifies the network portion of an IPv4 address, with the first three octets being all ones (11111111 in binary notation, 255 in decimal notation). The mask displays the last octet as zero (00000000 in binary notation). For a Class C IPv4 address with the default subnet mask, the last octet is where the node-specific values of the IPv4 address are assigned.

For example, in a network with an IPv4 address of 192.168.1.0 and a mask value of 255.255.255.0, the network portion of the address is 192.168.1, and there are 254 node addresses (192.168.1.1 through 192.168.1.254) available. Remember, the first address (192.168.1.0) is the base network, and the last address (192.168.1.255) is the broadcast address.

Class A and Class B IPv4 addresses use smaller mask values and support larger numbers of nodes than Class C IPv4 addresses for their default address assignments. Class A networks use a default 8-bit (255.0.0.0) subnet mask, which provides a total of more than 16 million (256 x 256 x 256) available IPv4 node addresses. Class B networks use a default 16-bit (255.255.0.0) subnet mask, which provides a total of 65,534 (256 x 256, minus the network address and the broadcast address) available IPv4 node addresses.

Unlike subnetting, which divides an IPv4 address along an arbitrary (default) classful 8-bit boundary (8 bits for a Class A network, 16 bits for a Class B network, 24 bits for a Class C network), *classless inter-domain routing* (CIDR) allocates address space on any address bit boundary (known as *variable-length subnet masking*, or VLSM). For example, using CIDR, a Class A network could be assigned a 24-bit mask (255.255.255.0, instead of the default 8-bit 255.0.0.0 mask) to limit the subnet to only 254 addresses, or a 23-bit mask (255.255.254.0) to limit the subnet to 512 addresses.

CIDR is used to reduce the size of routing tables on internet routers by aggregating multiple contiguous network prefixes (known as *supernetting*), and it also helps slow the depletion of public IPv4 addresses (discussed in Section 2.1.1).

Key Terms

Classless inter-domain routing (CIDR) is a method for allocating IP addresses and IP routing that replaces classful IP addressing (for example, Class A, B, and C networks) with classless IP addressing.

Variable-length subnet masking (VLSM) is a technique that enables IP address spaces to be divided into different sizes.

Supernetting aggregates multiple contiguous smaller networks into a larger network to enable more efficient internet routing.

An IP address can be represented with its subnet mask value, using “netbit” or CIDR notation. A netbit value represents the number of ones in the subnet mask and is displayed after an IP address, separated by a forward slash. For example, 192.168.1.0/24 represents a subnet mask consisting of 24 ones:

11111111.11111111.11111111.00000000 (in binary notation)

or

255.255.255.0 (in decimal notation)

2.1 Knowledge Check

Test your understanding of the fundamentals in the preceding section. Review the correct answers in Appendix A.

1. **Multiple Choice.** Which option is an example of a logical address? (Choose one.)
    a) IP address
    b) hardware address
    c) MAC address
    d) burned-in address
2. **Fill in the Blank.** An IPv4 address consists of four __-bit octets.
3. **Fill in the Blank.** _____ is a technique used to divide a large network into smaller subnetworks by segmenting an IPv4 address into network and host portions.