to have lower reliability than Tier 1 ISPs.

Tier 3

Tier 3 ISPs purchase their Internet service from Tier 2 ISPs. The focus of these ISPs is the retail and home markets in a specific locale. Tier 3 customers typically do not need many of the services required by Tier 2 customers. Their primary need is connectivity and support.

These customers often have little or no computer or network expertise. Tier 3 ISPs often bundle Internet connectivity as a part of network and computer service contracts for their customers. While they might have reduced bandwidth and less reliability than Tier 1 and Tier 2 providers, they are often good choices for small- to medium-size companies.

Interactive Graphic **Activity 8.1.4.7: Public or Private IPv4 Addresses**

Go to the course online to perform this practice activity.

Lab 8.1.4.8: Identifying IPv4 Addresses

In this lab, you will complete the following objectives:

- Part 1: Identify IPv4 Addresses
- Part 2: Classify IPv4 Addresses

IPv6 Network Addresses (8.2)

This section will introduce IPv6.

IPv4 Issues (8.2.1)

The useful life of IPv4 has almost been reached. This section will examine the reasons for the migration to IPv6.

The Need for IPv6 (8.2.1.1)

IPv6 is designed to be the successor to IPv4. IPv6 has a larger 128-bit address space, providing for 340 undecillion addresses (that is the number 340, followed by 36 zeroes). However, IPv6 is much more than just larger addresses. When the IETF began its development of a successor to IPv4, it used this opportunity to fix the limitations of IPv4 and include additional enhancements. One example is Internet Control Message Protocol version 6 (ICMPv6), which includes address resolution and address autoconfiguration not found in ICMP for IPv4 (ICMPv4). ICMPv4 and ICMPv6 will be discussed later in this chapter.

Need for IPv6

The depletion of IPv4 address space has been the motivating factor for moving to IPv6. As Africa, Asia, and other areas of the world become more connected to the Internet, there are not enough IPv4 addresses to accommodate this growth. On Monday, January 31, 2011, the IANA allocated the last two /8 IPv4 address blocks to the Regional Internet Registries (RIR). Various projections show that all five RIRs will have run out of IPv4 addresses between 2013 and 2020. At that point, the remaining IPv4 addresses will have been allocated to ISPs.

IPv4 has a theoretical maximum of 4.3 billion addresses. RFC 1918 private addresses in combination with Network Address Translation (NAT) have been instrumental in slowing the depletion of IPv4 address space. NAT has limitations that severely impede peer-to-peer communications.

Internet of Things

The Internet of today is significantly different than the Internet of past decades. The Internet of today is more than email, web pages, and file transfer between computers. The evolving Internet is becoming an Internet of things. No longer will the only devices accessing the Internet be computers, tablets and smartphones. The sensor-equipped, Internet-ready devices of tomorrow will include everything from automobiles and biomedical devices to household appliances and natural ecosystems. Imagine a meeting at a customer site that is automatically scheduled on your calendar application to begin an hour before you normally start work. This could be a significant problem, especially if you forget to check the calendar or adjust the alarm clock accordingly. Now imagine that the calendar application communicates this information directly to your alarm clock for you and to your automobile. Your car automatically warms up to melt the ice on the windshield before you enter the car and reroutes you to your meeting.

With an increasing Internet population, a limited IPv4 address space, issues with NAT and an Internet of things, the time has come to begin the transition to IPv6.

IPv4 and IPv6 Coexistence (8.2.1.2)

There is not a single date to move to IPv6. For the foreseeable future, both IPv4 and IPv6 will coexist. The transition is expected to take years. The IETF has created various protocols and tools to help network administrators migrate their networks to IPv6. The migration techniques can be divided into three categories:

- **Dual-stack:** As shown in Figure 8-9a, dual-stack allows IPv4 and IPv6 to coexist on the same network. Dual-stack devices run both IPv4 and IPv6 protocol stacks simultaneously.

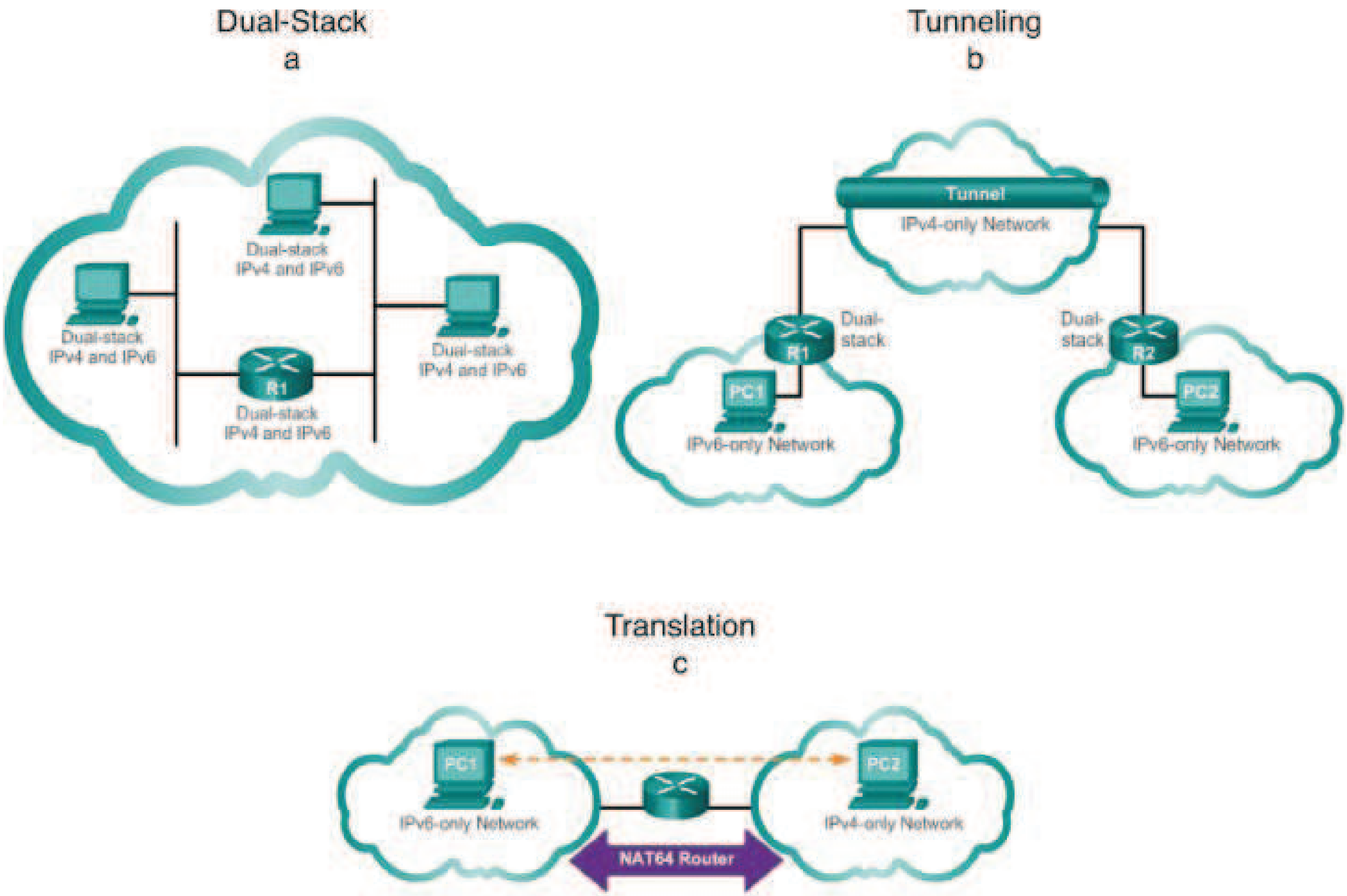

Figure 8-9 IPv4 and IPv6 Coexistence Methods

- **Tunneling:** As shown in Figure 8-9b, tunneling is a method of transporting an IPv6 packet over an IPv4 network. The IPv6 packet is encapsulated inside an IPv4 packet, similar to other types of data.
- **Translation:** As shown in Figure 8-9c, Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. An IPv6 packet is translated to an IPv4 packet and vice versa.

Interactive Graphic **Activity 8.2.1.3: IPv4 Issues and Solutions**

Go to the course online to perform this practice activity.

IPv6 Addressing (8.2.2)

At their core, both IPv4 and IPv6 are binary. However, to make it easier to work with the expanded address range of IPv6, these addresses are represented differently. This section will present the representation of IPv6 addresses.

Hexadecimal Number System (8.2.2.1)

Unlike IPv4 addresses that are expressed in dotted-decimal notation, IPv6 addresses are represented using hexadecimal values. You have seen hexadecimal used in the Packets Byte pane of Wireshark. In Wireshark, hexadecimal is used to represent the binary values within frames and packets. Hexadecimal is also used to represent Ethernet Media Access Control (MAC) addresses.

Hexadecimal Numbering

Hexadecimal ("hex") is a convenient way to represent binary values. Just as decimal is a base 10 numbering system and binary is base 2, hexadecimal is a base 16 system.

The base 16 numbering system uses the numbers 0 to 9 and the letters A to F. Table 8-10 shows the equivalent decimal, binary, and hexadecimal values. There are 16 unique combinations of 4 bits, from 0000 to 1111. The 16-digit hexadecimal is the perfect number system to use, because any 4 bits can be represented with a single hexadecimal value.

Hexadecimal	Decimal	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
A	10	1010
B	11	1011
C	12	1100
D	13	1101
E	14	1110
F	15	1111

Table 8-10 Hexadecimal Numbers

Understanding Bytes

Given that 8 bits (a byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range from 00 to FF. Leading 0s can be displayed to complete the 8-bit representation. For example, the binary value 0000 1010 is shown in hexadecimal as 0A.

Representing Hexadecimal Values

Note

It is important to distinguish hexadecimal values from decimal values regarding the characters 0 to 9.

Hexadecimal is usually represented in text by the value preceded by 0x (for example 0x73) or a subscript 16. Less commonly, it can be followed by an H, for example 73H. However, because subscript text is not recognized in command-line or programming environments, the technical representation of hexadecimal is preceded with “0x” (zero X). Therefore, the previous examples would be shown as 0x0A and 0x73, respectively.

Hexadecimal Conversions

Number conversions between decimal and hexadecimal values are straightforward, but quickly dividing or multiplying by 16 is not always convenient. With practice, it is possible to recognize the binary bit patterns that match the decimal and hexadecimal values.

IPv6 Address Representation (8.2.2.2)

IPv6 addresses are 128 bits in length and written as a string of hexadecimal values. Every 4 bits is represented by a single hexadecimal digit, for a total of 32 hexadecimal values. IPv6 addresses are not case sensitive and can be written in either lowercase or uppercase.

Preferred Format

As shown in Figure 8-10, the preferred format for writing an IPv6 address is x:x:x:x:x:x:x:x, with each “x” consisting of four hexadecimal values. When referring to 8 bits of an IPv4 address, we use the term *octet*. In IPv6, a ***hextet*** is the unofficial term used to refer to a segment of 16 bits or four hexadecimal values. Each “x” is a single hextet, 16 bits, or four hexadecimal digits.

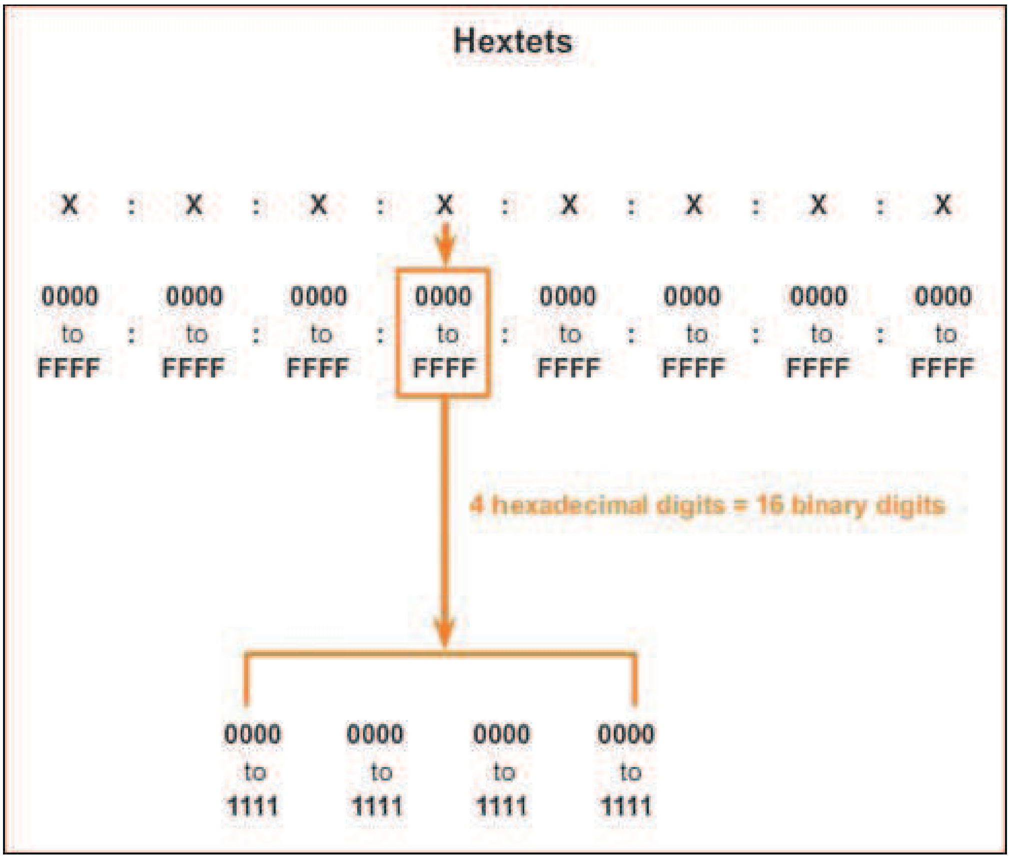

Figure 8-10 IPv6 Preferred Format

Preferred format means that the IPv6 address is written using all 32 hexadecimal digits. It does not necessarily mean that it is the ideal method for representing the IPv6 address. In the following pages, we will see two rules to help reduce the number of digits needed to represent an IPv6 address.

Some examples of IPv6 addresses in the preferred format are

Click here to view code image

```
2001:0DB8:0000:1111:0000:0000:0000:0200
FE80:0000:0000:0000:0123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200
0000:0000:0000:0000:0000:0000:0000:0001
```

Rule 1: Omit Leading 0s (8.2.2.3)

The first rule to help reduce the notation of IPv6 addresses is that any leading 0s in any 16-bit section or hextet can be omitted. For example:

- 01AB can be represented as 1AB.
- 09F0 can be represented as 9F0.
- 0A00 can be represented as A00.
- 00AB can be represented as AB.

This rule only applies to leading 0s, *not* to trailing 0s; otherwise, the address would be ambiguous. For example, the hextet "ABC" could be either "0ABC" or "ABC0."

Table 8-11 shows several examples of how omitting leading 0s can be used to reduce the size of an IPv6 address. For each example, the preferred format is shown. Notice how omitting the leading 0s in most examples results in a smaller address representation.

Preferred	No Leading 0s
2001:0DB8:0000:1111:0000:0000:0000:0200	2001: DB8: 0:1111: 0: 0: 0:200
FE80:0000:0000:0000:0123:4567:89AB:CDEF	FE80: 0: 0: 0: 123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200	FF02: 0: 0: 0: 0: 1:FF00: 200
0000:0000:0000:0000:0000:0000:0000:0001	0: 0: 0: 0: 0: 0: 0: 1

Table 8-11 IPv6 Addresses Omitting Leading 0s

Rule 2: Omit All 0 Segments (8.2.2.4)

The second rule to help reduce the notation of IPv6 addresses is that a double colon (::) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0s.

The double colon (::) can only be used once within an address; otherwise, there would be more than one possible resulting address. When used with the omitting leading 0s technique, the notation of IPv6 address can often be greatly reduced. This is commonly known as the compressed format.

Here is an incorrect address:

- 2001:0DB8::ABCD::1234

Possible expansions of the ambiguous compressed address are

- 2001:0DB8::ABCD:0000:0000:1234
- 2001:0DB8::ABCD:0000:0000:0000:1234
- 2001:0DB8:0000:ABCD::1234
- 2001:0DB8:0000:0000:ABCD::1234

Table 8-12 shows several examples of how using the double colon (::) and omitting leading 0s can reduce the size of an IPv6 address.

Preferred	No Leading 0s
2001:0DB8:0000:1111:0000:0000:0000:0200	2001:DB8:0:1111::200
FE80:0000:0000:0000:0123:4567:89AB:CDEF	FE80::123:4567:89AB:CDEF
FF02:0000:0000:0000:0000:0001:FF00:0200	FF02::1:FF00:200
0000:0000:0000:0000:0000:0000:0000:0001	::1

Table 8-12 IPv6 Addresses Using Double Colons

Interactive Graphic

Activity 8.2.2.5: Practicing IPv6 Address Representations

Go to the course online to perform this practice activity.

Types of IPv6 Addresses (8.2.3)

This section will introduce the different types and uses of IPv6 addresses.

IPv6 Address Types (8.2.3.1)

There are three types of IPv6 addresses:

- **Unicast:** An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A source IPv6 address must be a unicast address.
- **Multicast:** An IPv6 multicast address is used to send a single IPv6 packet to multiple destinations.
- **Anycast:** An IPv6 anycast address is any IPv6 unicast address that can be assigned to multiple devices. A packet sent to an anycast address is routed to the nearest device having that address. Anycast addresses are beyond the scope of this course.

Unlike IPv4, IPv6 does not have a broadcast address. However, there is an IPv6 all-nodes multicast address that essentially gives the same result.

IPv6 Prefix Length (8.2.3.2)

Recall that the prefix, or network, portion of an IPv4 address can be identified by a dotted-decimal subnet mask or prefix length (slash notation). For example, an IP address of 192.168.1.10 with dotted-decimal subnet mask 255.255.255.0 is equivalent to 192.168.1.10/24.

IPv6 uses the prefix length to represent the prefix portion of the address. IPv6 does not use the dotted-decimal subnet mask notation. The prefix length is used to indicate the network portion of an IPv6 address using the IPv6 address/prefix length.

The prefix length can range from 0 to 128. A typical IPv6 prefix length for LANs and most other types of networks is /64. This means that the prefix or network portion of the address is 64 bits in length, leaving another 64 bits for the interface ID (host portion) of the address.

IPv6 Unicast Addresses (8.2.3.3)

An IPv6 unicast address uniquely identifies an interface on an IPv6-enabled device. A packet sent to a unicast address is received by the interface that is assigned that address. Similar to IPv4, a source IPv6 address must be a unicast address. The destination IPv6 address can be either a unicast or a multicast address.

There are six types of IPv6 unicast addresses, described in the following sections.

Global Unicast

A global unicast address is similar to a public IPv4 address. These are globally unique, Internet routable addresses. Global unicast addresses can be configured statically or assigned dynamically. There are some important differences in how a device receives its IPv6 address dynamically compared to DHCP for IPv4.

Link-Local

Link-local addresses are used to communicate with other devices on the same local link. With IPv6, the term *link* refers to a subnet. Link-local addresses are confined to a single link. Their uniqueness must only be confirmed on that link because they are not routable beyond the link. In other words, routers will not forward packets with a link-local source or destination address.

Loopback

The loopback address is used by a host to send a packet to itself and cannot be assigned to a physical interface. Similar to an IPv4 loopback address, you can ping an IPv6 loopback address to test the configuration of TCP/IP on the local host. The IPv6 loopback address is all-0s except for the last bit, represented as ::1/128, or just ::1 in the compressed format.

Unspecified Address

An ***unspecified address*** is an all-0s address represented in the compressed format as ::/128, or just :: in the compressed format. It cannot be assigned to an interface and is only to be used as a source address in an IPv6 packet. An unspecified address is used as a source address when the device does not yet have a permanent IPv6 address or when the source of the packet is irrelevant to the destination.

Unique Local

IPv6 unique local addresses have some similarity to RFC 1918 private addresses for IPv4, but there are significant differences as well. ***Unique local addresses*** are used for local addressing within a site or between a limited number of sites. These addresses should not be routable in the global IPv6. Unique local addresses are in the range of FC00::/7 to FDFF::/7.

With IPv4, private addresses are combined with NAT/PAT to provide a many-toone translation of private to public addresses. This is done because of the limited availability of IPv4 address space. Many sites also use the private nature of RFC 1918 addresses to help secure or hide their network from potential security risks. However, this was never the intended use of these technologies, and the IETF has always recommended that sites take the proper security precautions on their Internet-facing router. Although IPv6 does provide site-specific addressing, it is not intended to be used to help hide internal IPv6-enabled devices from the IPv6 Internet. IETF recommends that limiting access to devices should be accomplished using proper, best-practice security measures.

Note

The original IPv6 specification defined site-local addresses for a similar purpose, using the prefix range FEC0::/10. There were several ambiguities in the specification, and site-local addresses were deprecated by the IETF in favor of unique local addresses.

IPv4 embedded

The last type of unicast address type is the IPv4 embedded address. These addresses are used to help transition from IPv4 to IPv6. IPv4 embedded addresses are beyond the scope of this course.

IPv6 Link-Local Unicast Addresses (8.2.3.4)

An IPv6 link-local address enables a device to communicate with other IPv6-enabled devices on the same link and only on that link (subnet). Packets with a source or destination link-local address cannot be routed beyond the link from where the packet originated.

Unlike IPv4 link-local addresses, IPv6 link-local addresses have a significant role in various aspects of the network. The global unicast address is not a requirement; however, every IPv6-enabled network interface is required to have a link-local address.

If a link-local address is not configured manually on an interface, the device will automatically create its own without communicating with a DHCP server. IPv6-enabled hosts create an IPv6 link-local address even if the device has not been assigned a global unicast IPv6 address. This allows IPv6-enabled devices to communicate with other IPv6-enabled devices on the same subnet. This includes communication with the default gateway (router).

IPv6 link-local addresses are in the FE80::/10 range. The /10 indicates that the first 10 bits are 1111 1110 10xx xxxx. The first hextet has a range of 1111 1110 10**00 0000** (FE80) to 1111 1110 10**11 1111** (FEBF).

Figure 8-11 shows the format of an IPv6 link-local address.

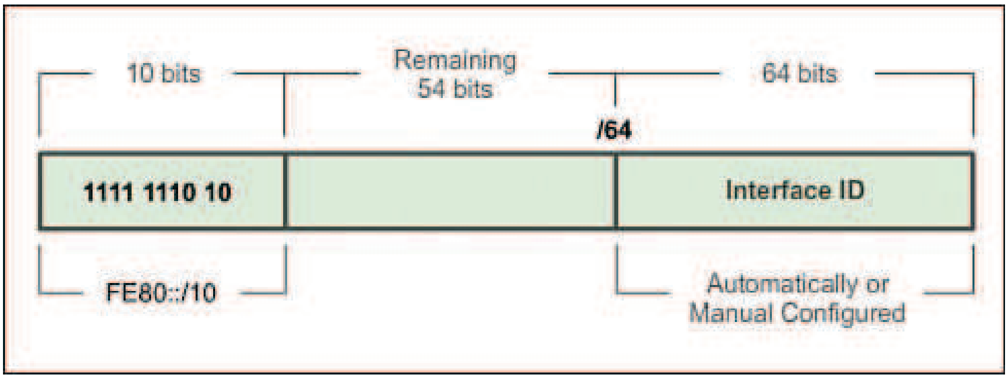

Figure 8-11 IPv6 Link-Local Address

IPv6 link-local addresses are also used by IPv6 routing protocols to exchange messages and as the next-hop address in the IPv6 routing table. Link-local addresses are discussed in more detail in a later course.

Note

Typically, it is the link-local address of the router and not the global unicast address that is used as the default gateway for other devices on the link.

Activity 8.2.3.5: Identify Types of IPv6 Addresses

Go to the course online to perform this practice activity.

IPv6 Unicast Addresses (8.2.4)

This section will introduce IPv6 unicast addressing.

Structure of an IPv6 Global Unicast Address (8.2.4.1)

IPv6 global unicast addresses are globally unique and routable on the IPv6 Internet. These addresses are equivalent to public IPv4 addresses. The Internet Committee for Assigned Names and Numbers (ICANN), the operator for the Internet Assigned Numbers Authority (IANA), allocates IPv6 address blocks to the five RIRs. Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned. This is only 1/8th of the total available IPv6 address space, excluding only a very small portion for other types of unicast and multicast addresses.

Note

The 2001:0DB8::/32 address has been reserved for documentation purposes, including use in examples.

Figure 8-12 shows the structure and range of a global unicast address.

A global unicast address has three parts:

- Global routing prefix
- Subnet ID
- Interface ID

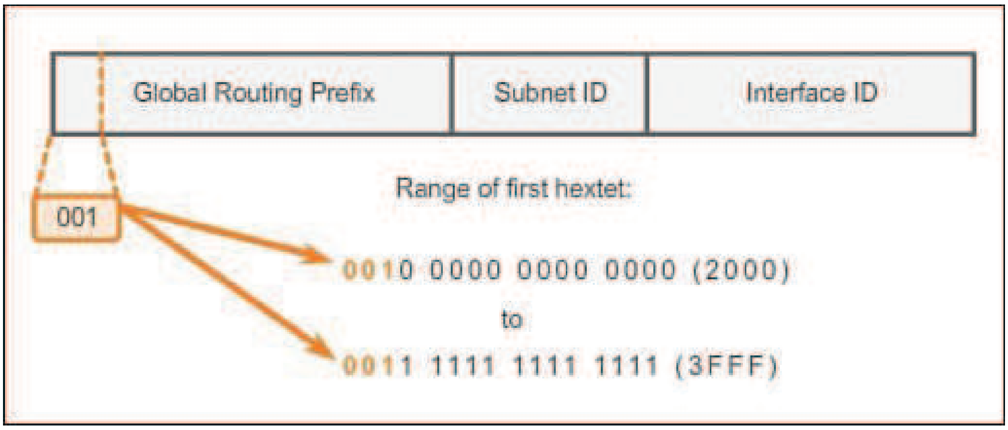

Figure 8-12 Parts of a IPv6 Global Unicast Address

Global Routing Prefix

The global routing prefix is the prefix, or network, portion of the address that is assigned by the provider, such as an ISP, to a customer or site. Currently, RIRs assign a /48 global routing prefix to customers. This includes everyone from enterprise business networks to individual households. This is more than enough address space for most customers.

Figure 8-13 shows the structure of a global unicast address using a /48 global routing prefix. /48 prefixes are the most common global routing prefixes assigned and will be used in most of the examples throughout this course.

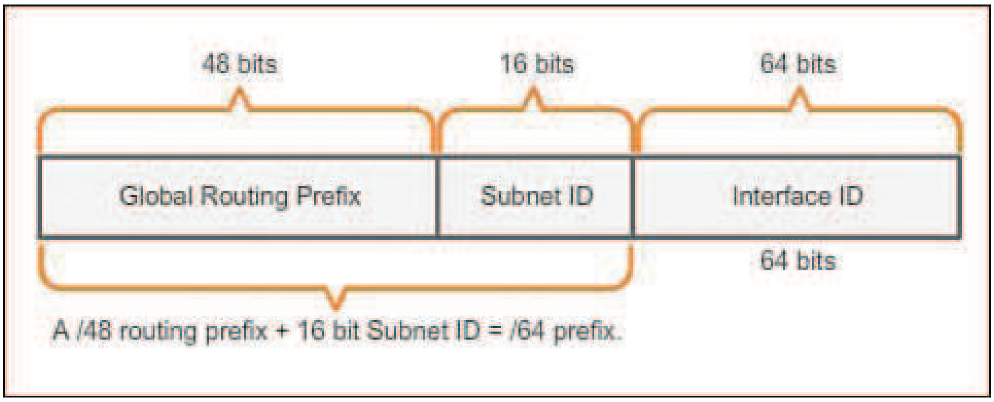

Figure 8-13 Division of an IPv6 Global Unicast Address

For example, the IPv6 address 2001:0DB8:ACAD::/48 has a prefix that indicates that the first 48 bits (3 hextets) (2001:0DB8:ACAD) is the prefix or network portion of the address. The double colon (::) prior to the /48 prefix length means that the rest of the address contains all 0s.