About IPv6 address

IPv6 (Internet Protocol version 6) is the latest version of Internet Protocol (IP), a communication protocol that provides a positioning system for computers on the network and routes traffic on the Internet. IPv6 has been developed by IETF to address IPv4 address exhaustion. IPv6 is intended to replace IPv4.

What is IPv6?

IPv6(Internet Protocol version 6) is the latest version of Internet Protocol (IP), a communication protocol that provides a positioning system for computers on the network and routes traffic on the Internet.IPv6 has been developed by IETF to address IPv4 address exhaustion.IPv6 was created to replace IPv4.

As such, the IPv6 protocol is gradually gaining popularity and we have written this series to introduce you to the IPv6 protocol.

The birth history of IPv6

The Internet Engineering Task Force (IETF) is the organization responsible for defining Internet Protocol (IP) standards. When developing IPv4, IETF did not anticipate the rapid development of global Internet as well as other important Internet security issues. In the original design of IPv4, network security was not taken seriously. In the 1980s, when IPv4 was being developed, the new Internet was being built under the cooperation of several organizations. By the time IPv4 was complete, it was also when the Internet began to explode, threats on the Internet became popular. If the current environment of online threats is predicted right from the development of IPv4, we have more security measures combined with its design. But that did not happen.

In the early 1990s, the IETF admitted that a new version of IP was needed and that they started by drafting the requirements that this IP needed. IP Next Generation (IPng) was created, then became IPv6 (RFC 1883) as it is today. IPv6 is the second standard network layer protocol after IPv4, used for computer communication via the Internet and other computer networks. IPv6 provides some interesting functions and is really the next step in the IP development process. These improvements include increasing address space, streamlined header formats, scalable headers, and the ability to maintain the privacy and integrity of information transmitted within the network. IPv6 was then fully standardized by the end of 1998 in RFC 2460. IPv6 has perfected the shortcomings left by IPv4 and created new ways to communicate that IPv4 cannot support.

IPv6 provides some improvements over IPv4. Advantages of IPv6 are presented in detail in the relevant documents. Below are the summary features of IPv6 and the improvements it can provide:

1. **Larger address space:** Increase from 32bit to 128bit.
2. **Improved protocol header:** Improved packet forwarding performance.
3. **Automatic stateless configuration:** Let the buttons determine their own addresses.

4. **Multicast:** Enhance the use of effective one-way communication.
5. **Jumbograms:** Support for large payload packets for greater efficiency.
6. **Network layer security:** Communication encryption and authentication.
7. **QoS (Quality of service) capability:** Mark QoS for packets and labeling to help determine which traffic should be prioritized.
8. **Anycast:** Backup service uses non-special addresses.
9. **Mobility:** Easier when handling mobile or roaming devices.

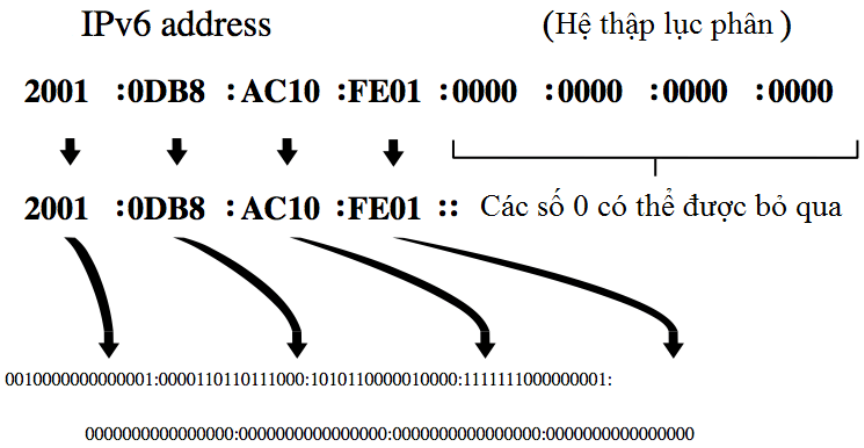

Photo source: Wikipedia

IPv6 address space

The most significant difference between these two protocols is the length of the source address and their address. Switching to IPv6 is due to the lack of IP addresses. This IPv6 protocol has a larger address space than the IPv4 protocol.

The IPv4 protocol uses a source address and a destination address of 32bit. These addresses are represented in four parts. A typical IPv4 address looks like 192.168.0.1 .
In contrast to IPv4, IPv6 addresses are 128 bits long. That allows to be able to perform to 3.4x1038 (340,000,000,000,000,000,000,000,000,000,000 VND) address. There are a few differences in IPv6 address representation. An IPv6 address is usually written in 8 groups, each consisting of 4 hex numbers and each group is separated by a ' **:** ' sign. The following example shows this 2001: 0f68: 0000: 0000: 0000: 0000: 1986: 69af .

You are considering the sample address above and thinking that typing an IPv6 address takes a lot of time and effort? But not so, IPv6 addresses can only be written briefly by minimizing zeros. There are two rules to follow here when representing an IP address. First, a sequence of four consecutive 0s can be replaced by two ' **::** ' signs. In that way the above IPv6 address can be abbreviated as follows: 2001: 0f68 :: 0000: 0000: 0000: 1986: 69af .

In the example above, we can only estimate a block of 0s because this rule states that there is only one pair of ' **::** ' in an address. Obviously, the address that is example above still has a lot of digits that need to be typed. However, the second rule will allow you to make this address shorter. The second principle says that *zeroes in a group can be ignored. If a 4-digit block starts with a zero, this zero can be omitted to leave 3 zeros in the block. If the three-digit block also starts with a leading zero, we can continue to eliminate it* . And so on until you meet another number 0 in the group, stop. In case if the 4 numbers in the group are 0, the last retained number is a zero. If you keep talking and do not perform in a specific example for you to follow easily, it is an omission. Here's what we can apply both to the example address:

2001: 0f68: 0000: 0000: 0000: 1986: 69af
2001: f68: 000: 000: 000: 000: 1986: 69af
2001: f68: 00: 00: 00: 00: 1986: 69af
2001: f68: 0: 0: 0: 0: 1986: 69af
2001: f68 :: 1986: 69af

Note that in each line, we omitted one zero from each group. When the rest of the numbers are zeros, we can apply 4 consecutive zeroes with two ' **::** ' signs. This can only be done if four zeroes go together. If that condition is not satisfied, we must leave the numbers 0.

Use the IPv6 addresses in the URL

Although DNS servers can access a website using a domain name instead of using an IP address, you can still enter an IP address instead of a part of a URL. For example, a personal website uses the URL www.quantrimang.com , which corresponds to the IP address 24.235.10.4. With such an IP address, I can access the website completely by entering the URL: http://24.235.10.4

Most web surfers often do not use the habit of entering IP addresses. However, this type of access still exists. This is especially true for individual web applications. When not related to a domain name, an application has the ability to avoid unauthorized users fumbling and jumping into your application by accident.

When an IP address is used instead of a domain name, the port number is sometimes specified as part of the address. If you simply enter after **HTTP: //** then an address then the browser will assume that you want to use port 80. However, you can specify any port to access the website. For example, if you want to access the website www.quantrimang.com using an IP address and specifically port 80 is used, the command should be used http://24.235.10.4:80

The IPv6 protocol, too, is used as part of a URL. But if you are interested in IPv6 format, you should note that an IPv6 address consists of many ' **:** ' signs. This raises a problem when your browser treats anything behind the ' **:** ' sign as a port number. In that case, IPv6 addresses are distinguished within parentheses when they are used as part of the URL. For example, if you used the sample IPv6 address in a URL, it would look like this:

HTTP: // [2001: 0f68: 0000: 0000: 0000: 0000: 1986: 69af] /

Just as you can specify the port number with an IPv4 address, you can also specify the port number when using an IPv6 address. The port number must follow the same mandatory format as when using IPv4. And outside the brackets. For example, if you want to access the website at the above sample IPv6 address on port 80, the input URL will be as follows:

HTTP: // [2001: 0f68: 0000: 0000: 0000: 0000: 1986: 69af]: 80 /

Note that the port number in this case is 80, between the parentheses and the slash. A ' **:** ' is also used to specify the port number as in the IPv4 protocol.

Components of IPv6

If you are familiar with IPv4 then you must know that an IPv4 address consists of four sections, each of which is distinguished by a dot. Part of this address denotes the network number and the remaining bits are used to distinguish a specific host on the network. The number of real bits is designed for different network numbers and hosts depending on the subnet mask.

An IPv4 address is divided into different sections, as does the IPv6 address. In the previous article, you learned about IPv6 addresses with 128 bits in length. When an IPv6 address is written in full form, it is expressed in 8 different sections, each with 4 numbers and separated by a ' **:** '. Each of these 4-digit sections represents 16 data bits, each of which is used for specific purposes.

Specifically, each IPv6 address is divided into three different parts: ***site prefix*** , ***subnet ID*** , ***interface ID*** . These three components are identified by the location of the bits inside an address. The first three fields in IPv6 are denoted site prefix, the next field represents the subnet ID and the last 4 fields represent the interface ID.

Site prefix is the same as IPv4 network number. It is the number assigned to your site by an ISP. Typically, all computers in the same location will share the same site prefix. Site prefix is ??intended to be shared when it recognizes your network and allows the network to be accessible from the Internet.

Unlike the site prefix, the **subnet ID** is unique because it is inside your network, the subnet ID describes the network structure of the network. Subnet ID works very similar to how the subnet works in the IPv4 protocol. The biggest difference here is that networks that can be 16 bytes long are represented in hex format rather than decimal point symbols. A typical IPv6 subnet is equivalent to a single network branch (page) as an IPv4 subnet.

The Interface ID works like an IPv4 configuration ID. This number uniquely identifies a private host in the network. Interface ID (which is sometimes referred to as a tag) is typically configured automatically based on the MAC address of the network interface. Interface IDs can be configured in EUI-64 format.

To see how an IPv6 address is divided into its various sub-sections, look at the address below:

2001: 0f68: 0000: 0000: 0000: 1986: 69af

The site prefix section of this address is: **2001: 0f68: 0000** . The next field is **0000** indicating the subnet ID. The

remaining bytes (**0000: 0000: 1986: 69af**) denote the interface ID.

Typically when a prefix is ??represented, it is written in a special format. The zeros are explained in the previous article and the prefixes are followed by a slash and number. The number after the slash indicates the number of bits in the prefix. In the previous example I mentioned site prefix for address 2001: 0f68: 0000: 0000: 0000: 1986: 69af was **2001: 0f68: 0000** . When this prefix is ??48 bits in length, we should add **a / 48** to end it properly. With omitted numbers 0, the prefix will write as follows: **2001: f68 :: / 48**

Types of IPv6 addresses

IPv6 has three different types of addresses: Unicast, Multicast and Anycast. Unicast addresses are used to distinguish individual hosts on a network. Multicast addresses are used to distinguish a group of network interfaces that typically reside in complex computers. When a packet is sent to a multicast address, the packet is sent to all network interfaces in the Multicast group.

Like multicast addresses, Anycast addresses also distinguish a specific group of network interfaces that often reside in complex computers. So what makes an Anycast route different from a multicast group? When packets are sent to a Multicast address they are sent to all network interfaces in the group. Contrary to that, when packets are sent to an Anycast address, these packets are not sent to the entire group but instead they are only sent to members physically closest to the sender.

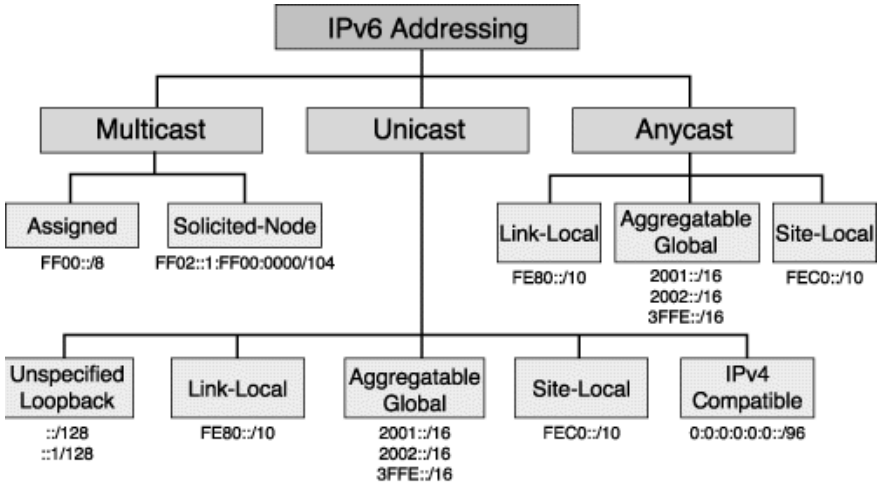

Photo source: Cisco

Unicast addresses:

We have shown you the format of an IPv6 address and the different bit locations used. There are indeed two different types of Unicast addresses: global and local. A global Unicast address is widely accessible, while the locally linked Unicast address is only accessible to other computers that share the link. The IP address format I showed you earlier is a global unicast address. We talked about this type of address because it is the most common type of address.

Local linked Unicast addresses used a different address format than global Unicast addresses. Like global Unicast addresses, locally linked Unicast addresses also contain 128 bytes of length. The differences in these two

types are different distributed bytes and the address uses a special site prefix.

In an internal link Unicast address, a site prefix occupies the first 10 bits of the address instead of the first 48 bits as in the case of a global Unicast address. Site prefix is ??used with a locally linked Unicast address: **fe80** .

When the site prefix is ??shortened (compared to a global Unicast address), you might not be surprised to see that the number of specified spaces in the subnet ID has been extended from 16 bits to 64 bits. What is here is that 64 bits is not really used. Remember that a locally linked IP address is only valid for computers that share a common link. As such, there is no reason to need a subnet ID. 64 bits of address space that is reserved for subnet IDs are represented as zeroes.

The interface ID for a local link unicast address is 54 bits long. Interface ID is almost always derived from 48 bits of MAC address assigned to the network interface card so that the protocol is gender-delimited. Below is an example of a local link unicast address.

Fe80: 0000: 0000: 0000: 0000: 0000: 23a1: b152

Of course, when the IPv6 addresses are written, they are often expressed with a zero number that has been annihilated. Therefore, a proper abbreviation formula for this address technology is:

Fe80 :: 23a1: b152

When the addresses described with zeros have been suppressed, the first address looks like any IPv6 address. Remember that you can tell the difference between a local Unicast address and other addresses because a local Unicast address will always start with fe80.

Multicast address:

As we explained in the previous section, multicast addresses are used to identify a group of network interfaces, known as a multicast group. Typical network interfaces are located on complex computers but this is not a pure device. Multicast addresses are used to send information to any network interface defined by the Multicast

group.
One of the most interesting things about multicast addresses is that they are completely separate, a network interface that has a Multicast address does not mean that the machine cannot have a Unicast address or is in other Multicast groups. In fact, some operating systems have added a computer network adapter to different Multicast groups at the time the adapter's unicast address is defined. For example, the Solaris operating system automatically adds network adapters to the Solicited node and all node multicast groups (or all routers). In case you are unfamiliar with Solaris, the Solicited button group is used for discovering other IPv6 enabled devices on the network. Windows Vista also has a similar function.

We have explained to you how multicast addresses are used for Multicast addresses. Although an IPv6 address is 128 bits long, the first 8 bits of the address re-define the Multicast address. Each Multicast address uses a prefix format of 11111111. When represented in hex notation and ':', a multicast address always starts with FF.

The next four bits of the Multicast address are flag bits. At the present time, the first three bits in the four-bit group are unused (so they are set to 0). The fourth flag bit is known as a padlock bit. Its mission is to indicate whether the address is a temporary or permanent address. If the address is a regular address, this bit will be assigned to 0, otherwise it will be assigned to 1.

The next four bits in the Multicast address are known as Scope ID bits. The amount of reserved space for Scope ID bits is 4 bits, which means that there are 16 different values ??expressed. Although not all 16 values ??are used at the present time, 7 of those values ??are used to determine the scope of the address. For example, if an address has a global scope, the address is valid across the entire Internet. Currently, Scope ID bits are used as follows:

Decimal value Binary value Address range 0 0000 Reserve 1 0001 Internal node range 2 0010 Internal link range 5 0101 Internal page range 8 1000 Internal organization scope 14 1110 Scope Global 15 1111 Reserve

The remaining 112 bits are used for group IDs. The size of the ID group allows Multicast addresses to use up 1/256 of the IPv6 address space.

To set this addressing scheme in the upcoming section, we show you some of the most frequently used Multicast addresses:

FF0x0: 0: 0: 0: 0: 1

This is a Multicast for all nodes. You may have to pay attention to the 'x' in the address, it is not a hex coefficient character. It is a placeholder for scope. This specific address can use the internal node range (FF01: 0: 0: 0: 0: 0: 1) or the internal link range (FF02: 0: 0: 0: 0: 0: 1).

FF0x: 0: 0: 0: 0: 0: 2

This Multicast address is assigned to all routers within the defined range. There is also an 'x' here, it also has the same function. Valid ranges are internal nodes (FF01: 0: 0: 0: 0: 0: 2), internal links (FF02: 0: 0: 0: 0: 0: 2) and internal pages (FF05 : 0: 0: 0: 0: 0: 2).

Anycast address:

If you have studied the IPv4 protocol, you may know that Unicast and Multicast concepts also exist in IPv4, although in IPv6 they are added with many other issues. Anycast is unique to IPv6. Anycast works like a

combination of Unicast and Multicast addresses. An unicast address is used to send data to a specific recipient, a Multicast address is used to send data to a group of recipients and an anycast address is used to send data to a specific recipient is outside the recipient group.

In case you are wondering, anycast is created as a way to make load balancing easier. Imagine a situation where you need to provide a large number of users so they can access services or go to their router. In such a situation, it often makes you have to use multiple servers to configure the service that is being provided or use complex routers or whatever is possible. The reason for this is because it can allow distribution of workflows between complex devices.

This type of load balancing is very difficult if using IPv4 (although it has been done). Using anycast addresses with IPv6 will be absolutely effective with load balancing. You need to send a user request to one of the devices, while not being able to care for the designated device that manages the request, but only a requirement to be concerned. By using Anycast addresses, each request is automatically sent to the device that is nearest geographically to the requested computer. In some situations, anycast can even be used to provide tolerance errors for a faulty router. Errors can be detected and requests can be resubmitted via another nearby router.

The strangest problem with anycast addresses is that there is no special addressing scheme. With this article, you have seen many types of rules covering use and the structure of unicast addresses and Multicast addresses to assign the same Unicast address to complex hosts. By doing so, Unicast addresses become an Anycast address.

In this series of articles, we have tried to skim fundamentally about the IPv6 protocol. Most administrators may not need to become experts right away but IPv6 is an essential component in Windows Vista and Longhorn Server. Therefore, it is necessary to learn a little about it.