IPv6

What is IPv6?

Internet Protocol Version 6 (IPv6) is the latest version of the Internet Protocol after IPv4. This communication protocol provides identification and local systems for computers on the network and routes communications on the Internet. Each device that uses the Internet is identified by its own IP address so that Internet communication can work properly.

Previous versions of IPv4 used a 32-bit addressing scheme to support 4.3 billion devices. With the rapid development of the Internet, personal computers, smartphones, and IoT devices, it is clear that connected devices require more addresses than the IPv4 address space.

IPv6 uses a 128-bit address, which allows approximately 3.4 × 10 ^ 38 addresses. IPv6 uses eight sets of four hexadecimal digits (separated by colons) instead of four sets of one to three digits IPv4 address methods.

IPv6 - Main Features

1. Larger Address Space

Compared with IPv4, IPv6 uses 4 times more bits to address devices on the Internet, which will provide an address space for approximately 3.4 × 10 ^ 38 devices. This address space can meet the aggressive requirements for allocating addresses for almost everything in the world.

2. Simplified Header

The IPv6 header was designed to be less complex and easier to process than the IPV4 header by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header.

3. End-to-End Connectivity

Now, each system has a unique IP address and can traverse the Internet without using NAT or other translating components. After IPv6 is fully implemented, each host can directly access other hosts on the Internet, but it will encounter some restrictions, such as firewalls and organizational policies.

4. Auto-configuration

IPv6 supports stateful and stateless auto-configuration modes of its host device. In this way, no DHCP server will not cause inter-segment communication to stop.

5. Faster Forwarding/Routing

The simplified header puts all unnecessary information at the end of the header. The first part of the header contains enough information to enable the router to make routing decisions, so it can make routing decisions as quickly as looking at the mandatory header.

6. IPSec

Initially, having IPSec security is mandatory for IPv6 protocol, making it more secure than IPv4. This feature is now optional.

7. Mobility

IPv6 aims to keep mobility in mind. This feature allows the host (such as a mobile phone) to roam in different geographic areas and keep connected using the same IP address. The mobility features of IPv6 take advantage of automatic IP configuration and extended headers.

8. Extensibility

One of the main advantages of the IPv6 header is that more information can be added in the options section. IPv4 only offers 40-byte options, while the options in IPv6 may be as large as the size of the IPv6 packet itself.

9. Smooth Transition

The large IP address scheme in IPv6 can allocate devices with globally unique IP addresses. This mechanism can save IP addresses and does not require NAT. Therefore, devices can send/receive data to each other, for example, VoIP and/or any streaming media can be used more efficiently. Another fact is that the header has less load, so the router can make forwarding decisions and forward them as soon as they arrive.

IPv6 - Addressing Modes

There are three addressing methods in IPv6 representation.

- Unicast

The unicast address identifies a single network interface. Packets sent to the unicast address will be delivered to the interface identified by the address.

- Multicast

Multicast addresses are used by multiple hosts called groups to obtain multicast destination addresses. These hosts do not have to be geographically together. If any packet is sent to the multicast address, it will be distributed to all interfaces corresponding to the multicast address.

- Anycast

Anycast addresses have been assigned to a group of interfaces. Any packets sent to anycast addresses will only be delivered to one member interface (probably the closest host).

IPv6 - Headers

The IPv6 header has a fixed header and zero or more optional (extended) headers. All necessary information necessary for the router is stored in a fixed header. The extended header contains optional information to help the router understand how to handle packets/flows.

Fixed Header

IPv6 fixed header is 40 bytes long and contains the following information.

1. Version (4-bits): It represents the version of Internet Protocol, i.e. 0110.

2. Traffic Class (8-bits): These 8 bits are divided into two parts. The first 6 bits are designed to notify the router what services should be provided to this packet. The least significant 2 bits are used for explicit congestion notification (ECN).

3. Flow Label (20-bits): This label is used to maintain the sequential flow of packets belonging to the communication. A source labels the sequence to help the router recognize that a specific data packet belongs to specific information flow. This field helps to avoid reordering of data packets. It is designed for streaming/real-time media.

4. Payload Length (16-bits): This field is used to tell the router how much information is contained in the payload of a particular data packet. The payload consists of an extension header and upper-layer data. 16 bits can indicate up to 65535 bytes; however, if the extension header includes a hop-by-hop extension header, the payload may exceed 65535 bytes, and this field is set to 0.

5. Next Header (8-bits): This field is used to indicate the type of extension header, or if there is no extension header, it indicates the upper layer PDU. The value of the upper layer PDU type is the same as IPv4.

6. Hop Limit (8-bits): This field is used to prevent data packets from looping into the network indefinitely. This is the same as TTL in IPv4. The value of the hop limit field is decremented by 1 when passing through the link (router/hop count). When this field reaches 0, the packet will be dropped.

7. Source Address (128-bits): This field indicates the address of the originator of the packet.

8. Destination Address (128-bits): This field provides the address of the intended recipient of the packet.

Extension Headers

In order to correct the limitation of the IPv4 option field, an extension header was introduced in IP version 6. The extension header mechanism is a very important part of the IPv6 architecture. The Next Header field of the IPv6 fixed header points to the first extended header, then the first extended header points to the second extended header, and so on.

The following Extension Headers must be supported as per RFC 2460:

1. Hop-by-Hop Options header: read all devices in transit network
2. Routing header: contains methods to support making routing decision
3. Fragment header: contains parameters of datagram fragmentation
4. Destination Options header: read by destination devices
5. Authentication header: Information regarding authenticity
6. Encapsulating Security Payload header: encryption information

Internet Protocol, Version 6 (IPv6) Specification

IPv6 specification is comprised of 8 parts in the table below.

Part	Title
1	Introduction
2	Terminology
3	IPv6 Header Format
4	IPv6 Extension Headers
5	Packet Size Issues
6	Flow Labels
7	Traffic Class
8	Upper-Layer Protocol Issues

Part 1: This part gives a overview about the IPv6 protocol and the changes from the previous version IPv4.

Part 2: This part explains the terminologies used in the IPv6 protocol.

Part 3: This part gives the header format of the IPv6 protocol and explains the structure of each section in IPv6 header.

Part 4: This part refers to the implementation of extension headers and gives the details about different extension headers.

Part 5: This part refers to the issue that MTU size may cause. It recommends the link in the Internet have an MTU of 1280 or greater. It also provides the solution if the MTU size is not enough.

Part 6: The part refers that flow labels may be required in the IPv6 header in order to handle special request such as non-default quality of service or 'real-time' service.

Part 7: This part refers that traffic classes field in the IPv6 header is available for use by originating nodes or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.

Part 8: This part refers to the four issues that may occur with the upper-layer protocol.

How the IPv6 protocol is used in the AXM-WEB2?

The AXM-WEB2 module also supports IPv6 which is the latest version of the internet protocol. The protocol uses 128-bit addressing in comparison to IPv4 which uses 32-bit addressing. The difference for addressing allows for more devices to be connected using IPv6 as opposed to the IPv4 protocol. The protocol is more efficient and provides more secure routing over the internet.

When the user wants to use IPv6 function on the AXM-WEB2, the user will need to enable the IPv6 function on the web interface of AXM-WEB2. Since AXM-WEB2 has two Ethernet ports available, both ports can be configured to use the IPv6 protocol. After the IPv6 is enabled, the user will need to determine if the DHCP is set as manual or auto. When set to manual, users must configure the IPv6 address, the Subnet Prefix Length, and the Gateway. When DHCP is set to Auto, the network will assign an IPv6 address automatically.

Reference: https://www.ietf.org/rfc/rfc2460.txt