Asan, Breech Kirby
CC10 – 1C

IPV6 is what ?

IPv6 (Internet Protocol Version 6) is the latest iteration of the Internet Protocol, designed by the Internet Engineering Task Force (IETF). Its primary purpose is to address the limitations of its predecessor, IPv4, which was running out of available addresses due to the explosive growth of internet-connected devices.

Here are some advantages of IPV6:

1. Larger Address Space: IPv6 uses 128-bit addresses, allowing for an enormous number of unique addresses—approximately 3.4×10^38. This abundance ensures that we won't run out of addresses anytime soon.
2. Hierarchical Addressing: IPv6's addressing structure allows for efficient route aggregation. This means that routing tables can be more concise, improving overall network performance.
3. Simplified Header Format: The IPv6 header is streamlined compared to IPv4, reducing processing overhead for routers and devices.
4. Stateless Address Autoconfiguration: IPv6 devices can automatically configure their own addresses without relying on external services (like DHCP in IPv4). This simplifies network setup.
5. Built-in Security: IPv6 includes features like IPsec (Internet Protocol Security) by default, enhancing communication security.
6. Multicast Enhancements: IPv6 improves multicast support, making it more efficient for distributing data to multiple recipients.
7. Jumbograms: IPv6 supports larger packet sizes (jumbograms), which can enhance performance over high-MTU (Maximum Transmission Unit) links.
8. Transition Mechanisms: While IPv4 and IPv6 are not directly interoperable, transition mechanisms (such as dual-stack, tunneling, and translation) allow coexistence during the migration.

IPV6 also have some disadvantages which are :

1. Compatibility with Existing IPv4 Infrastructure: While IPv6 was designed to coexist with IPv4 during the transition, it doesn't directly interoperate with it. This means that organizations need to maintain both protocols during the transition period, which can be complex and resource intensive.
2. Learning Curve: IPv6 introduces new concepts and features, which require network administrators and engineers to learn and adapt. This learning curve can slow down adoption.
3. Address Configuration Complexity: Unlike IPv4, which often relies on DHCP for address assignment, IPv6 uses stateless autoconfiguration. While this simplifies setup in some cases, it can be challenging to manage and troubleshoot.
4. Address Scanning and Privacy Concerns: IPv6 addresses are globally routable and more predictable due to their structure. This makes it easier for attackers to scan for devices and potentially compromise security. Privacy extensions exist, but they're not always widely implemented.
5. Transition Challenges: Migrating from IPv4 to IPv6 involves planning, testing, and potential disruptions. Organizations must carefully manage the transition to avoid service interruptions.

how IPv6 is implemented in a network scenario?

Dual Stack Configuration: In a dual-stack configuration, both IPv4 and IPv6 are enabled on network devices (such as routers, switches, and servers). Devices have both IPv4 and IPv6 addresses assigned to their interfaces. This allows seamless communication between devices using either protocol.

For instance, a router might have both an IPv4 address (e.g., 192.168.1.1) and an IPv6 address (e.g., 2001:db8::1).

Tunnelling: Tunnelling is used when native IPv6 connectivity is not available. One common method is 6 in 4 tunnelling, where IPv6 packets are encapsulated within IPv4 packets.

An example is the IPv6-to-IPv4 (6-to-4) tunnelling technique. In this approach, an IPv6 packet is encapsulated in an IPv4 packet and sent over an IPv4 network. The receiving end decapsulates the IPv6 packet and processes it which allows communication between IPv6 islands across an IPv4 network.

Mobile IPv6: IPv6 includes built-in support for mobility that means mobile IPv6 enables devices to move seamlessly between different networks without losing connectivity. When a mobile device changes its point of attachment (e.g., switches from Wi-Fi to cellular), it maintains its IPv6 address thus the routing headers in IPv6 make mobile IPv6 more efficient than mobile IPv4.

Security with IPsec: IPsec (IP security) is mandatory in IPv6. Every IPv6 node supports IPsec, enhancing network security because IPsec provides encryption, authentication, and integrity checks for data packets making it require keys for each device, ensuring secure communication.

Native IPv6 Network: The ultimate goal is to have a native IPv6 network. In such a network, all devices communicate directly using IPv6 addresses without tunnelling or dual-stack configurations.

TABLE :

Aspect	**IPv4**	**IPv4**
Number System	32-bit addresses (approximately 4.3 billion unique addresses)	128-bit addresses (approximately 3.4×10^38 unique addresses)
Unicast Addresses	IPv4 uses unicast addresses for one-to-one communication.	IPv6 also uses unicast addresses for one-to-one communication
Address Representation	192.168.1.1	2001:0db8:85a3:0000:0000:8a2e:0370:7334

What is GUA?

A global unicast address (GUA) is a type of IPv6 address that is globally routable and reachable on the Internet. It is equivalent to a public IPv4 address. GUAs play a significant role in the IPv6 addressing architecture, serving as unique identifiers for interfaces on IPv6 devices

Structure of GUA:

Global Routing Prefix (GRP):

The Global Routing Prefix is the most significant part of a GUA. It is assigned by the Internet service provider (ISP) to the customer site. The GRP identifies the network segment within the global IPv6 address space. Think of it as the “network portion” of the address, similar to the network ID in IPv4.

For example, 2001:0db8:1234::/48 has a GRP of 2001:0db8:1234.

Subnet ID:

The Subnet ID is used for subnetting within the customer site. It allows further division of the address space into smaller subnets.

In the example 2001:0db8:1234:5678::/64, the Subnet ID is 5678.

Interface ID:

The Interface ID uniquely identifies a specific interface (device) within the subnet. It is typically derived from the device’s MAC address or generated using other methods (such as EUI-64). The Interface ID completes the 128-bit address. For instance, in 2001:0db8:1234:5678::1, the Interface ID is 1