SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

19ITT302 INTERNET OF THINGS

III YEAR – V SEM

UNIT 04

IPv6 TECHNOLOGIES FOR THE IOT

Syllabus

UNIT I **IoT INTRODUCTION AND APPLICATIONS** **8**

Overview and Motivations - IPv6 Role - IoT Definitions - Observations - ITU-T Views – Working Definition - IoT Frameworks - Basic Nodal Capabilities – Physical Design of IoT - Logical Design of IoT – Applications:- City Automation Automotive Applications - Home Automation - IoT Levels & Deployment Templates - IoT and M2M

UNIT II **FUNDAMENTAL MECHANISMS & KEY TECHNOLOGIES** **8**

Identification of IoT Objects and Services- Structural aspects of IoT-Environment Characteristics Traffic Characteristics-Scalability-Interoperability-Security and privacy -Key IoT Technologies :Device Intelligence - Communication Capabilities - Mobility Support - Device Power –Sensor Technology -RFID Technology - Satellite Technology - IoT Enabling Technologies- WSN, Cloud computing, Big data Analytics, communication protocols, embedded systems

UNIT III **EVOLVING IoT STANDARDS & PROTOCOLS** **11**

IETF IPv6 Routing Protocol for RPL Roll – Constrained Application Protocol (CoAP) – Representational State Transfer (REST) – Third Generation Partnership Project Service Requirements for Machine Type Communications- Over Low Power WPAN (6LoWPAN)- IP in Small Objects (IPSO) - WPAN Technologies for IoT/M2M – ZigBee/IEEE 802.15.4, RF4CE,Bluetooth and its Low Energy Profile.

Syllabus

UNIT IV **IPv6 TECHNOLOGIES FOR THE IOT** **9**

Motivations - Address Capabilities - IPv6 Protocol Overview - IPv6 Tunneling - IPsec in IPv6 - Header Compression Schemes - Quality of Service in IPv6 - MOBILE IPv6 -Protocol Details - Generic Mechanisms - New IPv6 Protocol - Message Types - Destination Option - Modifications to IPv6 Neighbor Discovery - Requirements for Various IPv6 Nodes - Correspondent Node Operation - HA Node Operation-Mobile Node Operation Relationship to IPV4 Mobile IPV4(MIP)-IPV6 Over Low-Power WPAN-Goals-Transmission of IPV6 Packets Over IEEE 802.15.4.

UNIT V **DESIGN METHODOLOGY & FUTURE TRENDS** **9**

IoT System Management with NETCONF-YANG: Need for IoT Systems Management – Simple Network Management Protocol (SNMP) –Limitations of SNMP, Network Operator Requirements NETCONF-YANG-IoT Systems Management with NETCONF-YANG -IoT Platforms Design Methodology – IoT Physical Devices & Endpoints - Raspberry Pi- Linux on Raspberry Pi –Raspberry Pi Interfaces - Programming Raspberry Pi with Python - Designing a RESTful WebAPI – Amazon Web Services for IoT

TEXT BOOKS

1 Daniel Minoli, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, Wiley Publications, First Edition, 2013.

2 Arsheep Bahga, Vijay Madisetti, Internet of Things: A Hands-On Approach, Universities Press, First Edition, 2014.

REFERENCES

1 Jean-Philippe Vasseur, Adam Dunkels, Interconnecting Smart Objects with IP: The Next Internet, Elsevier Publications, 2010

2 Adrian McEwen, Hakim Cassimally, Designing the Internet of Things, Wiley Publications, First Edition, 2013.

3 N. Ida, Sensors, Actuators and Their Interfaces, SciTech Publishers, 2014.

IPv6 TECHNOLOGIES FOR THE IOT

Motivations - Address Capabilities - IPv6 Protocol Overview - IPv6 Tunneling - IPsec in IPv6 - Header Compression Schemes - Quality of Service in IPv6 - MOBILE IPv6 -Protocol Details - Generic Mechanisms - New IPv6 Protocol - Message Types - Destination Option - Modifications to IPv6 Neighbor Discovery - Requirements for Various IPv6 Nodes - Correspondent Node Operation - HA Node Operation-Mobile Node Operation Relationship to IPV4 Mobile IPV4(MIP)-IPV6 Over Low-Power WPAN-Goals-Transmission of IPV6 Packets Over IEEE 802.15.4.

Internet Protocol version 6 (IPv6)

- The Internet Protocol version 6, or IPv6, is the latest version of the Internet Protocol (IP), which is the system used for identifying and locating computers on the Internet.
- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the problem of IPv4 exhaustion.
- IPv6 is a 128-bit address having an address space of 2128, which is way bigger than IPv4.
- IPv6 uses a Hexa-Decimal format separated by a colon (:).

Internet Protocol version 6 (IPv6) - What is IP Address?

- An IP address, which stands for Internet Protocol address, is like a home address for your computer or any device connected to the internet.
- Just as your home address lets mail find its way to your house, an IP address helps information find its way to your device.

- **<u>Components in IPv6 Address Format</u>**
- There are 8 groups and each group represents 2 Bytes (16-bits).
- Each Hex-Digit is of 4 bits (1 nibble)
- Delimiter used – colon (:)

Need For IPv6

- The Main reason of IPv6 was the address depletion as the need for electronic devices rose quickly when Internet Of Things (IOT) came into picture after the 1980s & other reasons are related to the slowness of the process due to some unnecessary processing, the need for new options, support for multimedia, and the desperate need for security.
- IPv6 protocol responds to the above issues using the following main changes in the protocol:

- **Large Address Space**:
- An IPv6 address is 128 bits long, compared with the 32 bit address of IPv4, this is a huge(2 raised 96 times) increases in the address space.
- **Better Header Format**:
- IPv6 uses a new header format in which options are separated from the base header and inserted, when needed, between the base header and the upper layer data .
- This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

Need For IPv6

- **New Options**:
- IPv6 has new options to allow for additional functionalities.

- **Allowance for extension**:
- IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

- **Support For Resource Allocation**:
- In IPv6,the type of service field has been removed, but two new fields , traffic class and flow label have been added to enables the source to request special handling of the packet . this mechanism can be used to support traffic such as real-time audio and video.

- **Support For More Security**:
- The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet. In IPv6 representation, we have three addressing methods :
- Unicast., Multicast., Anycast

Addressing Methods

- **Unicast Address :**
  - Unicast Address identifies a single network interface.
  - A packet sent to a unicast address is delivered to the interface identified by that address.

- **Multicast Address** :
  - Multicast Address is used by multiple hosts, called as groups, acquires a multicast destination address.
  - These hosts need not be geographically together.
  - If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.
  - And every node is configured in the same way.
  - In simple words, one data packet is sent to multiple destinations simultaneously.

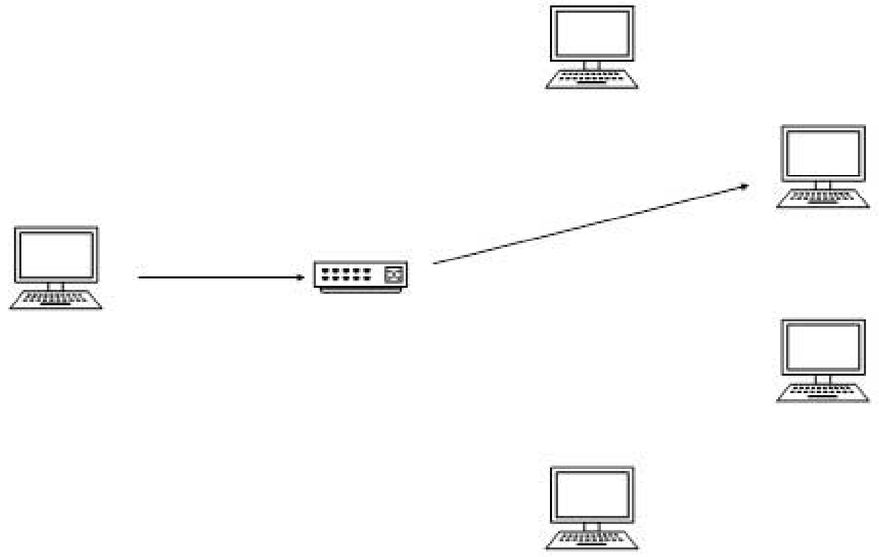
- **Anycast Address**:
  - Anycast Address is assigned to a group of interfaces.
  - Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

Addressing Methods

- In computer networking, addressing mode refers to the mechanism of hosting an address on the network.
- IPv6 offers several types of modes by which a single host can be addressed.
- More than one host can be addressed at once or the host at the closest distance can be addressed.

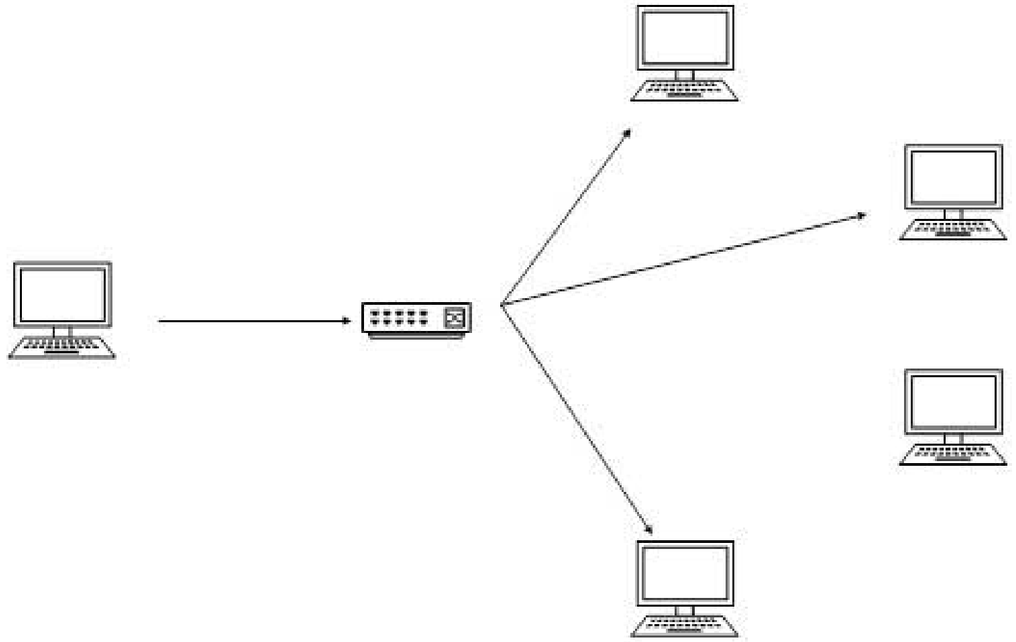
Addressing Methods - Unicast

- In unicast mode of addressing, an IPv6 interface (host) is uniquely identified in a network segment.
- The IPv6 packet contains both source and destination IP addresses.
- A host interface is equipped with an IP address which is unique in that network segment.
- When a network switch or a router receives a unicast IP packet, destined to a single host, it sends out one of its outgoing interface which connects to that particular host.



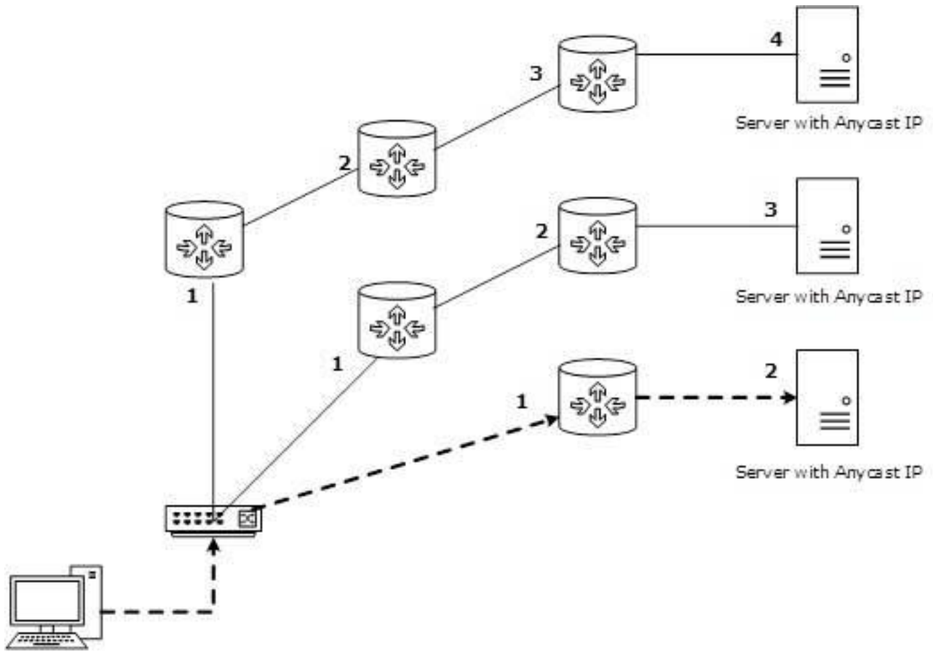
Addressing Methods - Multicast

- The IPv6 multicast mode is same as that of IPv4.
- The packet destined to multiple hosts is sent on a special multicast address.
- All the hosts interested in that multicast information, need to join that multicast group first.
- All the interfaces that joined the group receive the multicast packet and process it, while other hosts not interested in multicast packets ignore the multicast information.



Addressing Methods - Anycast

- IPv6 has introduced a new type of addressing, which is called Anycast addressing.
- In this addressing mode, multiple interfaces (hosts) are assigned same Anycast IP address.
- When a host wishes to communicate with a host equipped with an Anycast IP address, it sends a Unicast message.
- With the help of complex routing mechanism, that Unicast message is delivered to the host closest to the Sender in terms of Routing cost.



Types of IPv6 Address

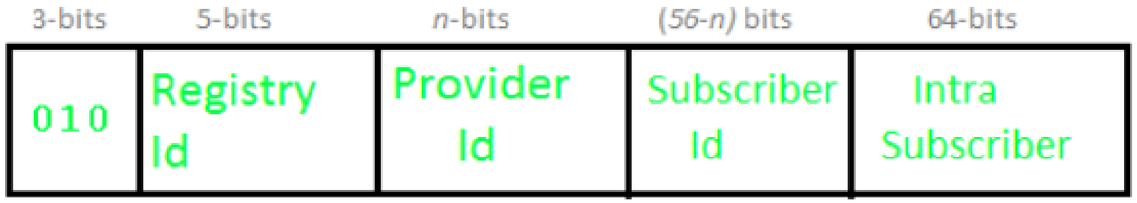
We have 128 bits in IPv6 address but by looking at the first few bits we can identify what type of address it is.

Prefix	Allocation	Fraction of Address Space
0000 0000	Reserved	1/256
0000 0001	Unassigned (UA)	1/256
0000 001	Reserved for NSAP	1/128
0000 01	UA	1/64
0000 1	UA	1/32
0001	UA	1/16
001	Global Unicast	1/8

Types of IPv6 Address

Provider-Based Unicast Address

These are used for global communication.



The First 3 bits identify it as of this type.

Registry Id (5-bits): Registry Id identifies the region to which it belongs. Out of 32 (i.e. 2^5), only 4 registry IDs are being used.

Registry Id	Registry
10000	Multi regional (IANA)
01000	RIPE NCC
11000	INTER NIC
00100	APNIC

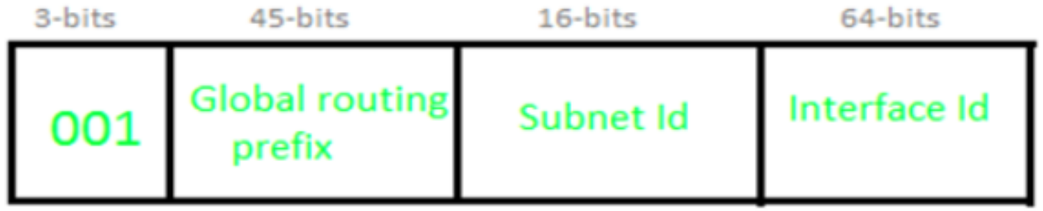
Types of IPv6 Address

Provider Id: Depending on the number of service providers that operate under a region, certain bits will be allocated to the Provider Id field. This field need not be fixed. Let's say if Provider Id = 10 bits then Subscriber Id will be 56 – 10 = 46 bits.

Subscriber Id: After Provider Id is fixed, the remaining part can be used by ISP as a normal IP address.

Intra Subscriber: This part can be modified as per the need of the organization that is using the service

Geography Based Unicast Address



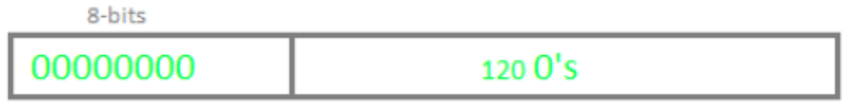
Global Routing Prefix: Global routing prefix contains all the details of Latitude and Longitude. As of now, it is not being used. In Geography-based Unicast address routing will be based on location.

Interface Id: In IPv6, instead of using Host Id, we use the term Interface Id.

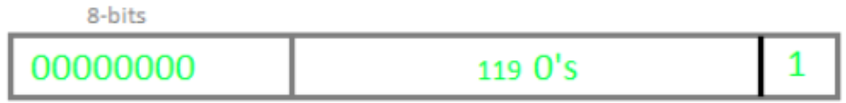
Types of IPv6 Address

Some Special Addresses

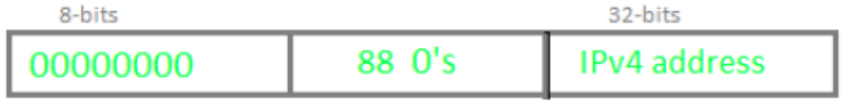
Unspecified



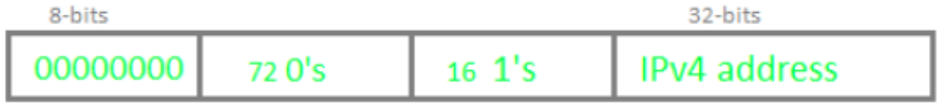
Loopback



IPv4 Compatible



IPv4 mapped

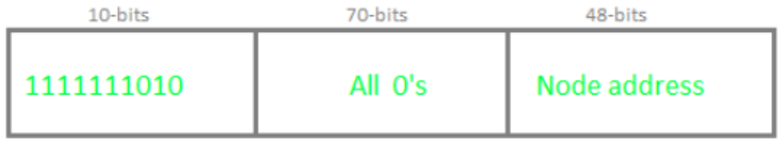


Types of IPv6 Address

Local Unicast Addresses

These are of two types: ***Link-local*** and ***Site-Local***

1. Link-Local Address



A link-local address is used for addressing a single link. It can also be used to communicate with nodes on the same link. The link-local address always begins with 1111111010 (i.e. FE80). The router will not forward any packet with Link-local address.

2. Site Local Address

Site local addresses are equivalent to a private IP address in IPv4. Likely, some address space is reserved, which can only be routed within an organization. The first 10-bits are set to 1111111011, which is why Site local addresses always begin with FEC0. The following 32 bits are Subnet IDs, which can be used to create a subnet within the organization. The node address is used to uniquely identify the link; therefore, we use a 48-bits MAC address here.

Advantages of IPv6

- 1. **Realtime Data Transmission** :
  - Realtime data transmission refers to the process of transmitting data in a very fast manner or immediately.
  - Example : Live streaming services such as cricket matches, or other tournament that are streamed on web exactly as soon as it happens with a maximum delay of 5-6 seconds.

- 2. **IPv6 supports authentication**:
  - Verifying that the data received by the receiver from the sender is exactly what the sender sent and came through the sender only not from any third party.
  - Example : Matching the hash value of both the messages for verification is also done by IPv6.

Advantages of IPv6

- 3. **IPv6 performs Encryption**:
- Ipv6 can encrypt the message at network layer even if the protocols of application layer at user level didn’t encrypt the message which is a major advantage as it takes care of encryption.

- **4. Faster processing at Router**:
- Routers are able to process data packets of Ipv6 much faster due to smaller Base header of fixed size – 40 bytes which helps in decreasing processing time resulting in more efficient packet transmission.
- Whereas in Ipv4, we have to calculate the length of header which lies between 20-60 bytes.

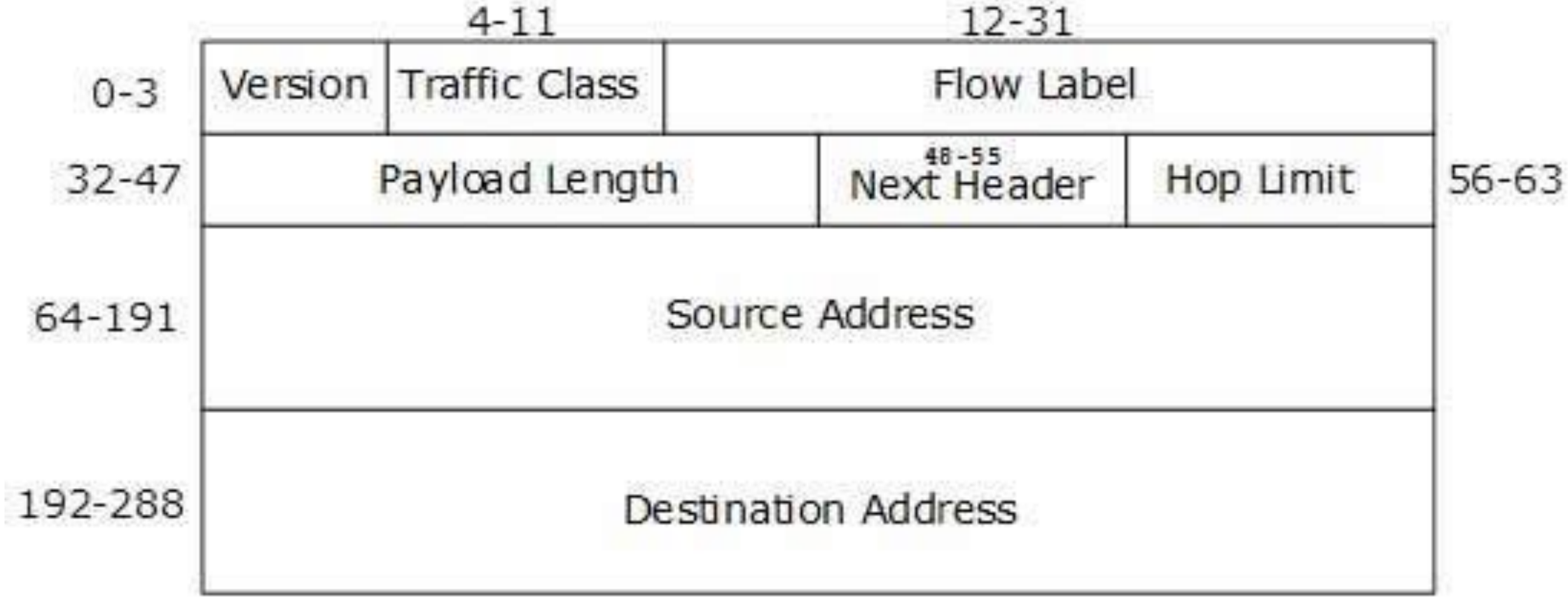
Disadvantages of IPV6

- **Transition Period**:
  - Due to widespread use of IPv4, shifting completely to IPv6 will take a long time.
  - **Communication Barrier**:
  - IPv4 and IPv6 machines cannot communicate directly with each other.
  - **No Backward Compatibility**:
  - IPv6 cannot run on IPv4-capable computers because it’s not supported by IPv4 systems.
  - **Conversion Challenges**:
  - IPv6’s inability to uniquely identify each device on the network makes the transition from IPv4 time-consuming.
  - **Protocol Isolation**:
  - IPv4 and IPv6 cannot communicate with each other directly, preventing cross-protocol communication.

IPv6 - Headers

- The wonder of IPv6 lies in its header.
- An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4.
- IPv6 headers have one Fixed Header and zero or more Optional (Extension) Headers.
- All the necessary information that is essential for a router is kept in the Fixed Header.
- The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

IPv6 – Headers - Fixed Header



IPv6 – Headers - Fixed Header

S.N.	Field & Description
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 most significant 6 bits are used for Type of Service to let the Router Known 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 the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.
4	**Payload Length** (16-bits): This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

IPv6 – Headers - Fixed Header

5	**Next Header** (8-bits): This field is used to indicate either the type of Extension Header, or if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.
6	**Hop Limit** (8-bits): This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.
7	**Source Address** (128-bits): This field indicates the address of originator of the packet.
8	**Destination Address** (128-bits): This field provides the address of intended recipient of the packet.

IPv6 – Headers - Extension Headers

- In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required or is rarely used.
- All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers.
- Each Extension Header is identified by a distinct value.

- When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header.
- If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on.
- The last Extension Header's 'Next-Header' field points to the Upper Layer Header.
- Thus, all the headers points to the next one in a linked list manner.

- If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header. The following Extension Headers must be supported as per RFC 2460:

IPv6 – Headers - Extension Headers

Extension Header	Next Header Value	Description
Hop-by-Hop Options header	0	read by all devices in transit network
Routing header	43	contains methods to support making routing decision
Fragment header	44	contains parameters of datagram fragmentation
Destination Options header	60	read by destination devices
Authentication header	51	information regarding authenticity
Encapsulating Security Payload header	50	encryption information

IPv6 – Headers - Extension Headers

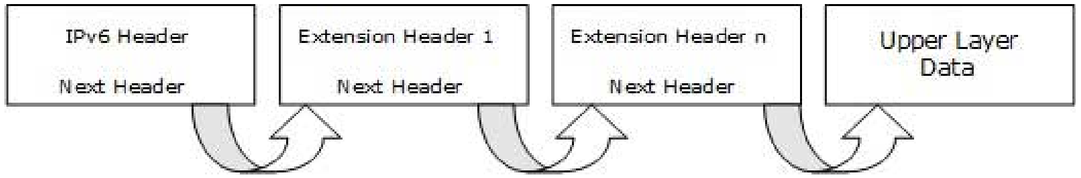
The sequence of Extension Headers should be:

IPv6 header
Hop-by-Hop Options header
Destination Options header[1]
Routing header
Fragment header
Authentication header
Encapsulating Security Payload header
Destination Options header[2]
Upper-layer header

These headers:

- 1. should be processed by First and subsequent destinations.
- 2. should be processed by Final Destination.

Extension Headers are arranged one after another in a linked list manner, as depicted in the following diagram:



[Image: Extension Headers Connected Format]

IPv6 Tunneling

What is IPv6 Tunneling?

IPv6 Tunneling is a mechanism for encapsulating IPv4 and IPv6 packets inside IPv6 packets. It is used to form a virtual point-to-point link between two IPv6 nodes.

IPv6 Tunnels are stateless and have no knowledge of the configuration or even existence of the remote tunnel endpoint. Once an IPv6 Tunnel is configured, packets are encapsulated and forwarded regardless of whether the decapsulating device is present or not.

IPv6 Tunneling allows hosts in one private IP network to communicate with hosts in another private IP network by providing a tunnel between two routers across the Internet.

The IPv6 tunnel connection endpoints are terminated via a Virtual Tunnel Interface (VTI) configured in each device.

Figure 1: An IPv6 tunnel encapsulated packet form

IPv6 Tunneling

Virtual Tunnel Interface (VTI)

A Virtual Tunnel Interface has similar characteristics to any other interface on the device. It is virtual because it does not directly map to any of the physical interfaces on the device, but instead is actually the endpoint of a tunnel from another device. VTIs are commonly layer 3 interfaces, can have IP configuration applied directly to them and are compatible with layer 3 routing protocols. The actual tunneling mechanism depends on the protocol used (GRE, RFC2473, L2TP and so on), but commonly uses IP as its transport.

Tunnel header

This is the outer or encapsulating IPv6 header. IPv6 Tunneling uses a standard IPv6 outer header and can be followed by extension headers as specified in IPv6 standards.

Payload header

This is the inner or encapsulated header. IPv6 Tunnels can be used to transport IPv4 and IPv6 packets.

IP packets from the private IP network destined for a host in the private IP network are encapsulated by Router A and forwarded to Router B. Intermediate routers route the packets using addresses in the delivery protocol header. Router B extracts the original payload packet and routes it to the appropriate destination within network.

IPv6 Tunneling

- The device supports the following features:
- IPv6 Tunneling as specified in RFC2473
- Virtual Tunnel Interfaces for terminating IPv6 encapsulated traffic
- IPv6 as the delivery protocol, used to transport the private data across the public network
- IPv4 as the payload, including DHCP, DNS
- IPv6 as the payload, including PIM6
- Configurable tunnel source using IPv6 address
- Configurable tunnel source using interface
- Configurable tunnel destination IPv6 address
- Configurable tunnel destination using hostname
- Configurable hop limit TTL value for insertion into the outer header
- Configurable DSCP value for insertion into the outer header
- Display of tunnel parameters in show interface output
- Tunnels are compatible with dynamic routing protocols
- Inherit the Flow Label from the inner header
- Insert Encapsulation Limit Extension Header if inner packet contains that header
- Path-MTU-discovery in the underlying tunnel interface
- TCP MSS Clamping

IPv6 Tunneling

- The device does not support the following features:
-
- Non-IPv4/IPv6 protocol as the payload
- Configurable Flow Label insertion
- IP Security tunnel protection

IPv6 Tunneling

Configuration Example

This example shows how to configure a IPv6 tunnel between Device A and Device B. It assumes that IP has been configured correctly and is operational on both devices.

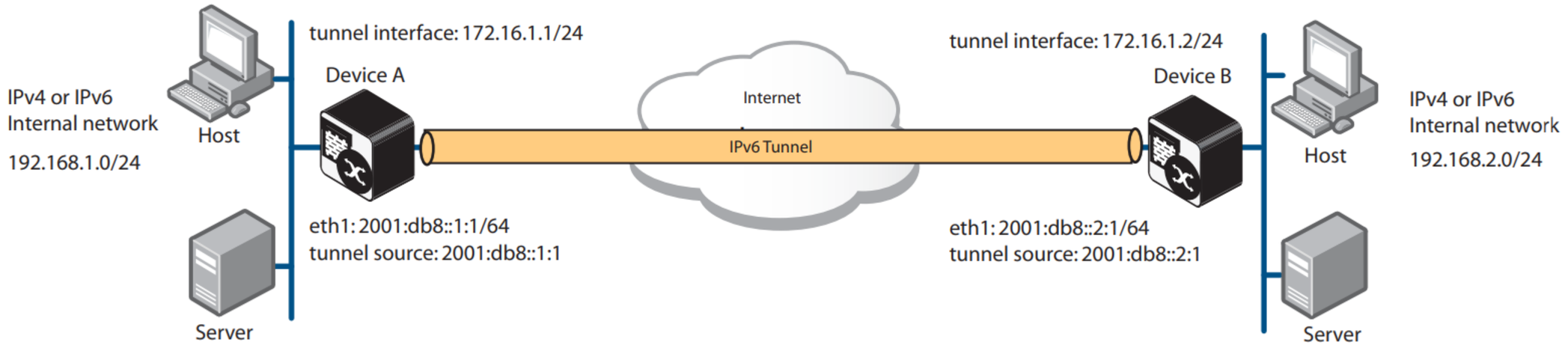
The following table lists the parameter values in the example. Note public IP addresses are used in this example.

Table 1: Parameters in IPv6 Tunnel Configuration Example

PARAMETER	DEVICE A	DEVICE B
IP address of Ethernet interface eth1	2001:db8::1:1/64	2001:db8::2:1/64
Tunnel source IP address	2001:db8:1::1	2001:db8::2:1
Tunnel destination IP address	2001:db8::2:1	2001:db8::1:1
IP address of tunnel interface	172.16.1.1/24	172.16.1.2/24
Subnet of connected internal network	192.168.1.0/24	192.168.2.0/24

IPv6 Tunneling

Figure 2: IPv6 Tunnel



IPv6 Tunneling

Configuring device A

Step 1: **Assign an IP address for interface eth1.**

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:db8::1:1/64
```

Step 2: **Create tunnel interface tunnel1.**

```
awplus(config-if)# interface tunnel1
```

Step 3: **Assign an IP address to the tunnel interface.**

```
awplus(config-if)# ip address 172.16.1.1/24
```

Step 4: **Set the encapsulation tunneling mode to IPv6 Tunneling.**

```
awplus(config-if)# tunnel mode ipv6
```

Step 5: **Assign an IP address to the tunnel source for the tunnel.**

```
awplus(config-if)# tunnel source 2001:db8::1:1
```

Step 6: **Designate the tunnel destination address.**

```
awplus(config-if)# tunnel destination 2001:db8::2:1
```

Step 7: **Configure a static route.**

```
awplus(config-if)# exit
awplus(config)# ip route 192.168.2.0 255.255.255.0 172.16.1.2
```

IPv6 Tunneling

Configuring device B

Step 1: **Assign an IP address for interface eth1.**

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 address 2001:db8::2:1/64
```

Step 2: **Create tunnel interface tunnel1.**

```
awplus(config-if)# interface tunnel1
```

Step 3: **Assign an IP address to the tunnel interface.**

```
awplus(config-if)# ip address 172.16.1.2/24
```

Step 4: **Set the encapsulation tunneling mode to IPv6 Tunneling.**

```
awplus(config-if)# tunnel mode ipv6
```

Step 5: **Assign an IP address to the tunnel source for the tunnel.**

```
awplus(config-if)# tunnel source 2001:db8::2:1
```

Step 6: **Designate the tunnel destination address.**

```
awplus(config-if)# tunnel destination 2001:db8::1:1
```

Step 7: **Configure a static route.**

```
awplus(config-if)# exit
awplus(config)# ip route 192.168.1.0 255.255.255.0 172.16.1.1
```

IPv6 Tunneling

Verifying connectivity

You can use the **ping** command to verify that the tunnel is established:

```
awplus# ping 192.168.2.1
```

You should receive ICMP Echo reply message.

Verifying the tunnel settings

You can use the **show interface tunnel** command to check that all settings are correctly configured:

```
awplus# show interface tunnel1
```

The output will show the settings for the tunnel.

IPv6 Tunneling

- IPv6 tunneling is a powerful technique that enables the transmission of IPv6 packets over an IPv4 network, even in cases where IPv6 connectivity is not natively available.
- This technology is essential for establishing connections between endpoints that support IPv6, allowing for seamless communication across different networks.

- There are various types of IPv6 tunneling mechanisms, each with its own benefits and drawbacks.
- For example, 6to4 tunneling is a popular method that automatically configures tunnels between IPv6 networks over IPv4 networks.
- Another method, called Teredo tunneling, is specifically designed for use in situations where the IPv6 network is located behind a NAT device.
- Other types of tunneling mechanisms include ISATAP, GRE, and so on.
- Overall, IPv6 tunneling is an important technology that helps to facilitate the transition from IPv4 to IPv6, and enables seamless communication between networks that your network is able to communicate effectively and securely, even in situations where native IPv6 connectivity is not available.

IPv6 Tunneling - 1. IPv6 over IPv4 tunneling (6in4)

1. IPv6 over IPv4 tunneling (6in4)

- This is the most commonly used technique for IPv6 tunneling, which involves encapsulating IPv6 packets within IPv4 packets.
- This method requires two endpoints, the source and the destination, which establish a connection over an IPv4 network.
- In this process, the source endpoint encapsulates the IPv6 packets within IPv4 packets, which are then transmitted through the IPv4 network.
- When the destination endpoint is reached, the IPv6 packets are extracted from the IPv4 packets and delivered to their destination.
- This technique is commonly used to connect IPv6 networks over an IPv4 infrastructure.

IPv6 Tunneling - 2. 6to4 tunneling

2. 6to4 tunneling

- 6to4 tunneling is a fascinating mechanism that allows IPv6 connectivity over an IPv4 network without the need for explicit tunnel setup.
- This is particularly useful for organizations that want to transition from IPv4 to IPv6, as it enables them to seamlessly connect both networks.

- The 6to4 tunneling mechanism relies on a 6to4 relay router to encapsulate IPv6 packets in IPv4 packets and vice versa.
- This means that the encapsulation process is performed automatically and does not require any additional configuration.
- This is a significant advantage over other tunneling mechanisms By the way, 6to4 tunneling uses a public IPv4 address because it relies on the IPv4 network to transport IPv6 packets.
- To ensure each packet is correctly routed to its destination, a unique IPv6 prefix is also required..

- 6to4 tunneling uses an IPv4-compatible IPv6 address as the destination address for the encapsulated packets.
- This address format is usually represented as “2002:IPv4 address::/48.

IPv6 Tunneling - 3. Teredo tunneling

3. Teredo tunneling

- Teredo tunneling is a mechanism that allows hosts behind a NAT device, which can only understand IPv4, to communicate with other hosts that use IPv6.
- This is important because the world is transitioning from IPv4 to IPv6, and without Teredo tunneling, it will cause the interoperability issues.
- For example, the devices that are behind a NAT device would not be able to communicate with devices that use IPv6.

- Teredo tunneling encapsulates IPv6 packets in UDP packets and sends them through the NAT device.
- When the UDP packets reach the Teredo server, they are decapsulated and sent to their destination.
- The Teredo server is responsible for managing the encapsulation and decapsulation of packets, as well as providing information about the IPv6 network to the Teredo client so that the connection can be established between them.

- Teredo address format includes a Teredo prefix, the server IPv4 address, and a client port number.
- The format is usually represented as “Teredo prefix:Server IPv4 address:Client port number”.
- The Teredo prefix is “2001::/32”.

IPv6 Tunneling - 4. ISATAP tunneling

4. ISATAP tunneling

- ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) tunneling is a mechanism that enables IPv6 connectivity within a site that uses IPv4.
- This is particularly useful in scenarios where a site has a mix of IPv4 and IPv6 devices, and the network infrastructure is unable to support native IPv6.
- It works by encapsulating IPv6 packets in IPv4 packets and sending them through an IPv4 network.
- The communication between the ISATAP routers allows for the dynamic assignment of IPv6 addresses to devices within the site, eliminating the need for manual configuration.
- The use of a unique ISATAP address ensures that the IPv6 packets are routed correctly within the site.
- Despite its advantages, ISATAP tunneling has some limitations, including potential security issues and the need for a reliable and robust network infrastructure to support the encapsulation and decapsulation of packets.

IPv6 Tunneling - 5. GRE tunneling

5. GRE tunneling

- Generic Routing Encapsulation (GRE) tunneling is a widely-used mechanism in computer networking that allows the encapsulation of any protocol over another network protocol.
- It is a useful tool in situations where one network protocol may not be directly supported by another.
- The process of GRE tunneling involves the use of a GRE tunnel endpoint and a GRE tunnel interface.
- The GRE endpoint is responsible for initiating the tunnel, while the interface is responsible for defining the parameters.
- These parameters include the network information, such as the source and destination IP addresses, the protocols and so on.
- However, there are some drawbacks to using GRE tunneling.
- One of the most significant concerns is the possibility of increased network latency due to the overhead to encapsulate and decapsulate the packets.

IPv6 Tunneling - 6. IP over DNS tunneling (DNS64)

6. IP over DNS tunneling (DNS64)

- IP over DNS (Domain Name System) tunneling is a mechanism that allows the transmission of IP packets over a DNS resolver.
- In this method, the IP packets are encapsulated inside DNS queries or responses.
- This is useful in situations where the network only supports IPv4 or when transitioning from IPv4 to IPv6, as it enables the transmission of IPv6 packets over an IPv4 network without the need for additional infrastructure.

- To use this mechanism, a DNS64 server and a DNS64 client are required.
- The DNS64 server is responsible for translating IPv6 addresses to IPv4 addresses, while the DNS64 client is responsible for encapsulating IPv6 packets inside DNS queries or responses before sending them to the DNS64 server.
- Once the packets have been translated with the IP obtained, they are sent to their intended destination.