IPv6

Internet Protocol Version 6

https://t.me/learningnets

IPv6 Course Outline

- Business Drivers – Why IPv6

- IPv6 Addressing
- IPv6 Address Plan

- IPv4 and IPv6 Transition Mechanisms
  1. Dual Stack
  2. Tunneling Mechanisms
  3. Translation

https://t.me/learningnets

IPv6 Course Outline

- IPv6 Tunneling
- Manuel Tunnels/Configured Tunnels
    - IP in IP and GRE Tunnels
- Semi Automatic Tunnels
    - Tunnel Brokers
    - Elements of a Tunnel Brokers – TB/TS
    - Hurricane Electric Tunnel Broker Service
- Automatic Tunnels
    1. 6 to 4
    2. 6rd – IPv6 Rapid Deployment

https://t.me/learningnets

IPv6 Course Outline

- IPv6 Routing Protocols
  1. OSPFv3 and comparison with OSPFv2
  2. IS-IS and comparison with OSPF
  3. EIGRP

- IPv6 in BGP

- IPv6 in MPLS
  - LDPv6 – RFC 7552
  - 6PE and 6VPE in MPLS

https://t.me/learningnets

IPv6 Course Outline

- Segment Routing (SRv6) – SR IPv6 Dataplane
- IPv6 Discussions:
  - Will IPv6 replace IPv4?
  - Does IPv6 have Better Security?
  - Will IPv6 reduce NAT Deployment?
  - Does IPv4 Really Running Out?
- Key Points in IPv6/Summary
- IPv6 Quiz Questions and the Answers

https://t.me/learningnets

IPv6 Business Drivers

- **IPv4 address exhaustion**
- **Business Continuity (E-Commerce, Content Providers, Content Delivery Networks)**
- **Easier Network Mergers and Acquisitions (No overlap, NAT etc.)**
- **Government IT Strategy , National IPv6 Strategy and Regulations (Government mandates, if Private companies want to work with them)**
- **Infrastructure Evolution**
- **Some Developers may want to use IPv6 in the company**

https://t.me/learningnets

IPv6 Addressing

- 24 September 2015 ARIN said “There is no more IPv4!” As of 2019, none of the five RIRs has IPv4

- IPv7 , IPv8 and IPv9 are already been deprecated. IPv10 is known as NDN – Named Data Networking – Van Jacobsen

- In IPv6, number of hosts is not important as there is 64 bits for the host portion, number of network which needs to be aggregated is an important consideration

https://t.me/learningnets

IPv6 Addressing

- IPv6 addresses are 128 bits long - 32 hexadecimal characters

- Hexadecimal is widely used in computing
- Hex is a base 16 numerical system
- Every Hex character is knows as **Nibble**
- Total 8 groups , groups are known as words or quads
- Each group is 16 bits and separated by ":"

Binary	Hex	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

https://t.me/learningnets

IPv6 Addressing

- 128 bit address has two portion ?: Network and Host
- Network (Sometimes called as Topology portion) is 64 bits
- Host Portion is 64 bits as well

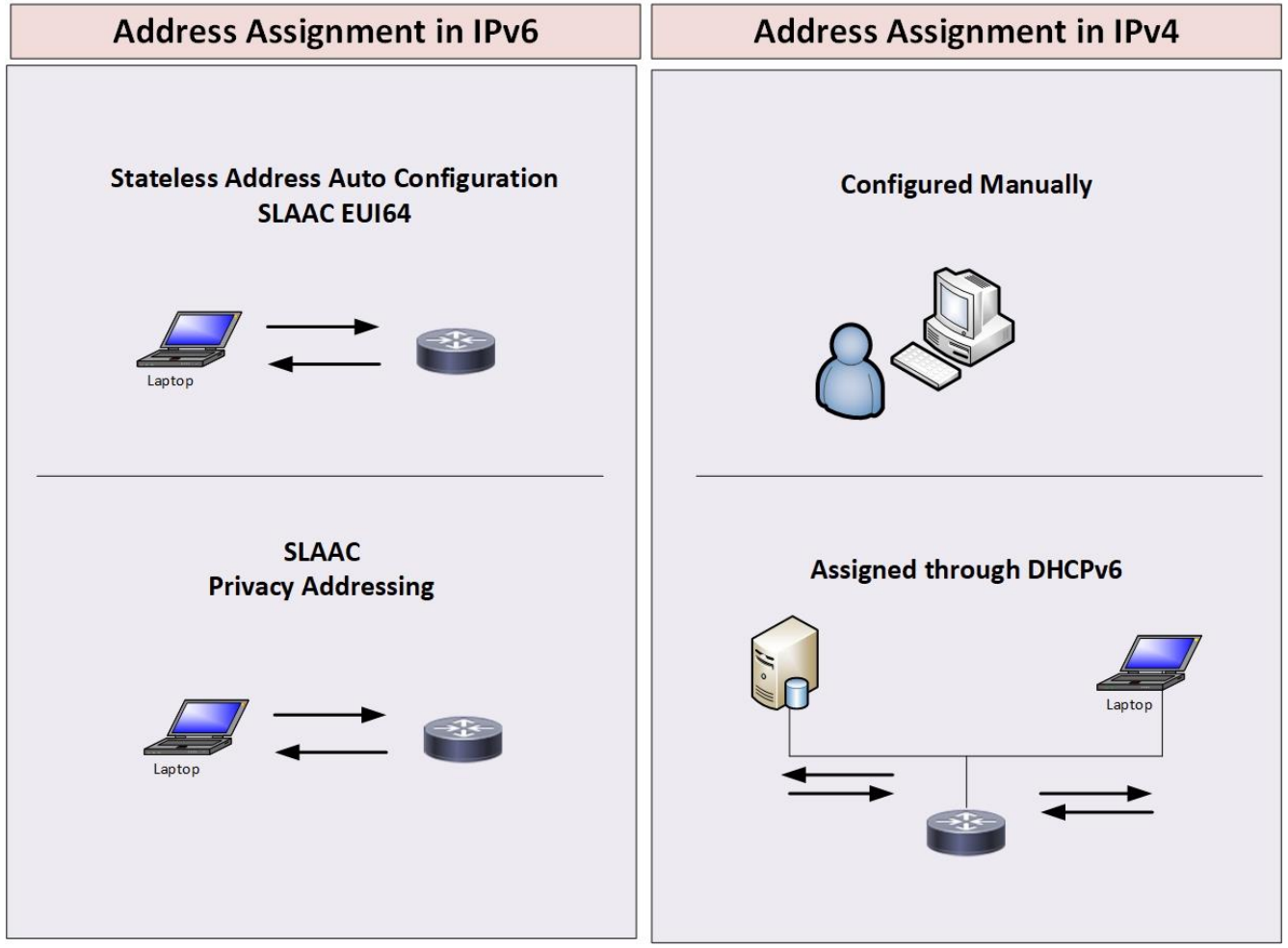
2001:0db8:1010:aaaa:0000:0000:0000:0001

Network Portion Host Portion

https://t.me/learningnets

IPv6 Address Assignment

- IPv6 Hosts can have an address manually or automatically similar to IPv4, there are some differences though



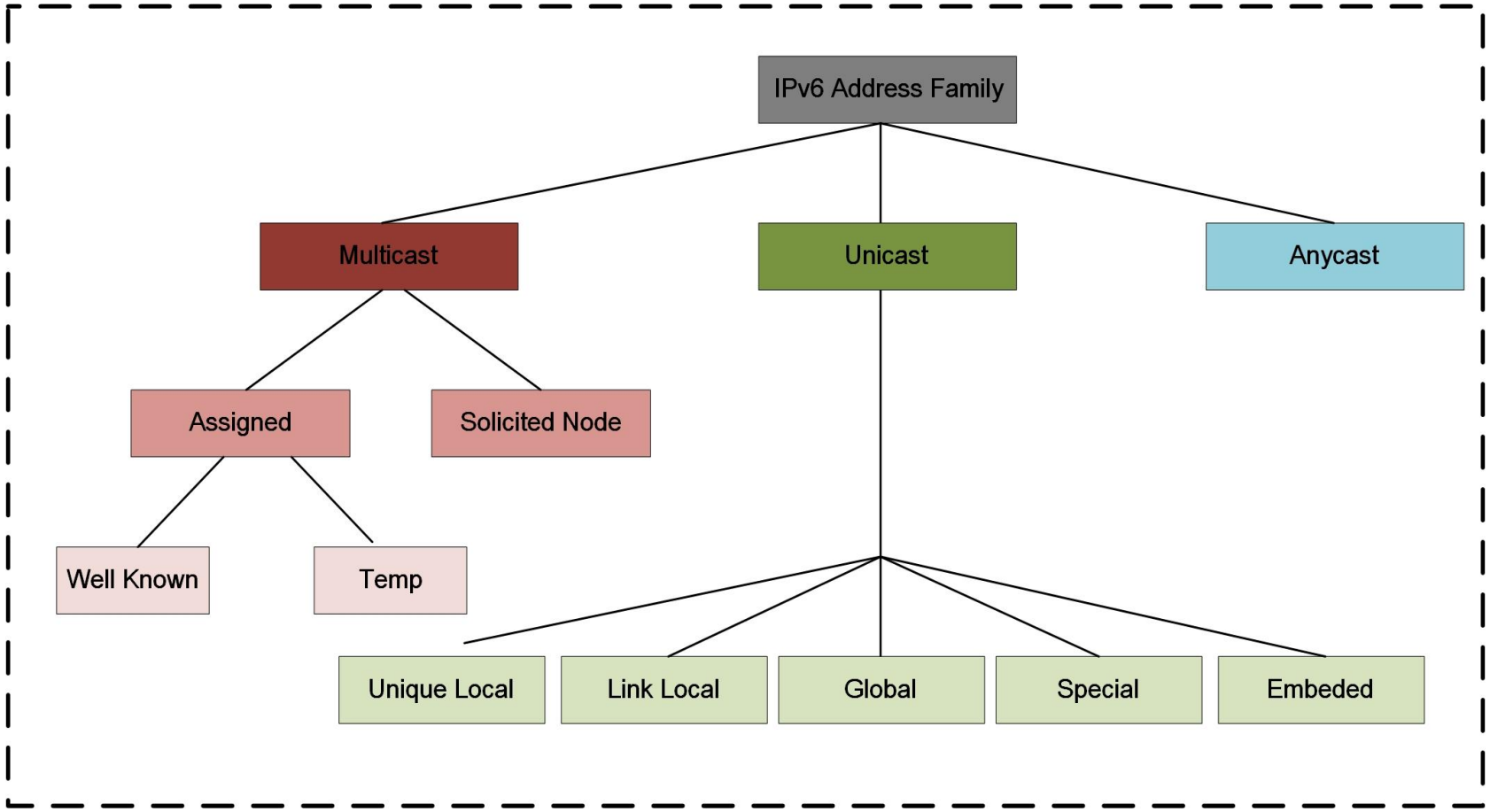
https://t.me/learningnets

IPv6 Address Assignment – Comparison

	Address	Default Gateway	DNS server	Delegated Prefix
SLAAC	✔	✔	✖	
Stateful DHCPv6	✔	✖	✔	✔
Stateless DHCPv6	✖	✖	✔	✖
RDNSS	✖	✖	✔	✖

https://t.me/learningnets

IPv6 Addressing



There is no Broadcast Addressing in IPv6

https://t.me/learningnets

IPv6 Addressing

- With IPv4, host portion of the IP address is used to create subnet, this is not the case with IPv6
- Every IPv6 interface has Link Local IPv6 address (fe80::/10). All interfaces on specific router can have identical LLA (Link Local Address) Ex : FE80::10.10.10.10
- If router will talk to outside world, then interface should have at least two addresses, link local and GUA (Global Unicast Address)

https://t.me/learningnets

Unicast IPv6 Address Types

- Three types of Unicast IPv6 Address Types:

1. Link-Local – Non-routable , exists on single layer 2 domain
fe80::/10

2. Unique-Local : Routable within AS
fc00::/7

3. Global Unicast Address – Routable across Inter domain
2000::/3
(Range is between 2000 – 3fff – First 2 byte)

https://t.me/learningnets

Unicast IPv6 Address Types

- ULA – Unique Local Addressing is not routable in DFZ but inside the AS, similar to RFC 1918 address space. General recommendation is to not use ULA. If it is used, for the IPv6 Internet destinations, local network needs an NPT (Network Prefix Translation – from ULA to Global Unicast Address)

- In IPv6, every bit position (called as Nibble), can have 16 different option, 0 to F.

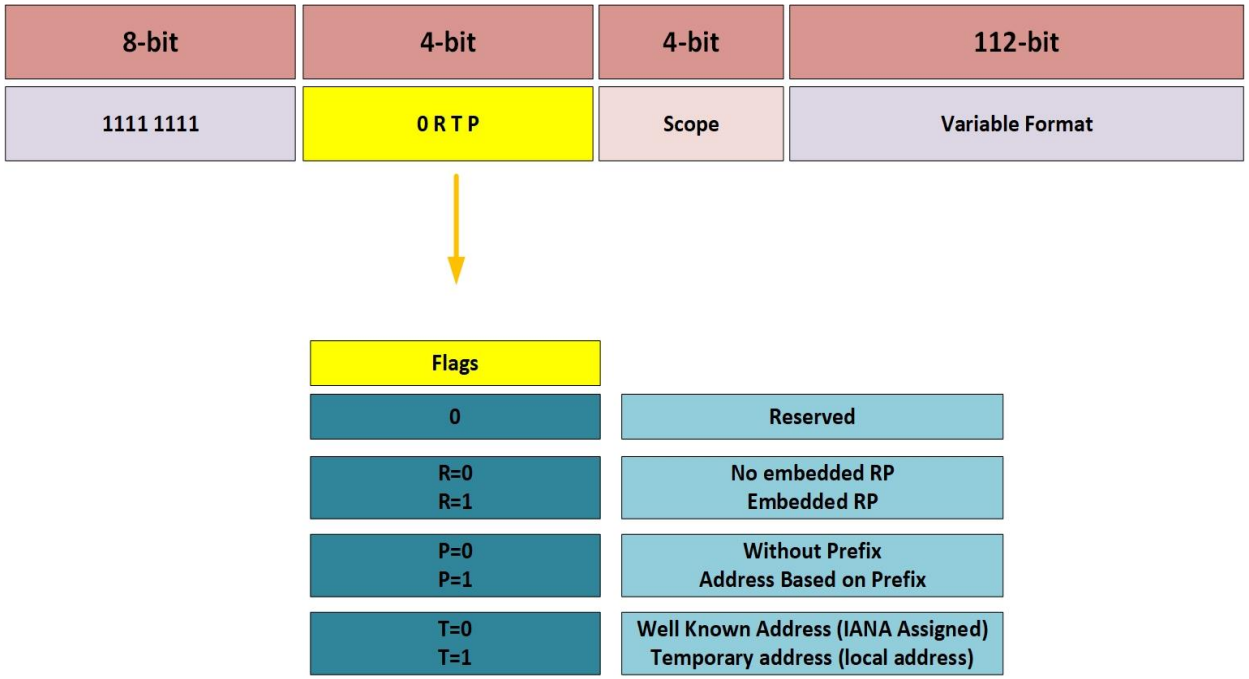
- Global unicast address for example is assigned as 2000::/3 mean, 2000 – 3fff for the first 16 bits, which mean only 2 bits are used of the first nibble. Thus, only 1/8 of the entire IPv6 address space is currently allocated by IANA

https://t.me/learningnets

Multicast IPv6 Address

- IPv6 Multicast Address was defined in the RFC 4291 (It specifies Solicited-Node Multicast Address as well, you will see next)

- IPv6 Multicast uses ff00::/8 range



https://t.me/learningnets

Solicited-Node Multicast Address

- Every Unicast address must build corresponding Solicited-Node Multicast Address
- Solicited-Node Multicast provides the functionality for Neighbor Discovery in IPv6
- So, it serves the purpose of IPv4 ARP and also used for Duplicate Address Detection

https://t.me/learningnets

Solicited-Node Multicast Address

- There is no broadcast in IPv6, instead IPv6 uses Multicast

- A device comes up and sends an ICMPv6 neighbor solicitation message to check if anyone else is already using the address it wants to use. The source for this messages is an unspecified address (::) and the destination address is the solicited node address of the unicast address being checked for duplicates

https://t.me/learningnets

Solicited-Node Multicast Address

- Second use case of Solicited-Node Multicast Address is to learn Layer 2 address of IPv6 Unicast address

- When a Router attempts to learn a layer 2 address of the remote Router, it sends NS (Neighbor Solicitation) message to the remote router's solicited node address which is generated from the remote router's unicast address

https://t.me/learningnets

Well Known IPv6 Multicast Addresses

Ff02 is Well Known Multicast Address , and the operation with it Is limited to single link. Routing protocols and link operations use it

Address	Scope	Meaning
ff02::1	Link Local	All Nodes
ff02::2	Link Local	All Routers
ff02::5	Link Local	OSPF v3 Routers
ff02::6	Link Local	OSPF v3 DR Routers
ff02::9	Link Local	RIPng
ff02::A	Link Local	EIGRP

https://t.me/learningnets

Special Use IPv6 Addresses

- RFC 5156 defines Special Use IPv6 Addresses :

- Default Route ::/0
- Loopback ::1
- 6to4 Auto Tunnel 2002::/16
- Documentation Prefix 2001:0db8::/32 (I used in many examples in this document as well)
- ::/128 Unspecified address (Similar to APIPA address in IPv4) used in Duplicated Address Detection

https://t.me/learningnets

IPv6 Header – Some fields

- IPv4 Protocol field is replaced with IPv6 Next Header Field
- IPv4 Header is 20 byte, IPv6 Header is 40 byte
- IPv4 TTL is IPv6 Hop Limit
- IPv6 Minimum MTU and Maximum MTU

https://t.me/learningnets

IPv6 Fragmentation

- In IPv6 Routers don’t perform fragmentation, Routers participate (help) for fragmentation
- Path MTU Discovery is done by the Hosts, not the Routers in IPv6.
- For PMTUD to work, ICMPv6 Type 2 Packet Too Big (PTB) shouldn’t be prevented on the path from receiver to sender
- Otherwise MTU should be set to Minimum IPv6 MTU which is 1280 bytes

https://t.me/learningnets

IPv6 Fragmentation

- Minimum MTU 1280 means, when IPv6 packet with this size is sent from sender to receiver, none of the device on the path should never fragment the packet

- If ICMP Type 2 PTB reaches from Receiver to Sender, it tells sender what value it should set the packet so packet can be send between source and the destination

https://t.me/learningnets

IPv6 Address Plan

https://t.me/learningnets

IPv6 QoS

- IPv4 TOS byte is renamed with IPV6 Traffic Class , it is same as IPv4 8 bits TOS byte

https://t.me/learningnets

IPv6 Transition Mechanisms

- Vast majority of the content is working on IPv4 as of 2019. How IPv6 users can connect to the IPv4 world and How IPv4 users can reach to the IPv6 content

- This is accomplished with the IPv6 transition technologies

https://t.me/learningnets

IPv6 Transition Mechanisms

- Probably the IPv6 transition technologies is a misleading term. Because; IPv4 infrastructure is not removed with these technologies. Thus probably the IPv6 integration or co-existence mechanisms are the better terms

- But still throughout this course I will be using IPv6 transition technologies

https://t.me/learningnets

IPv6 Transition Mechanisms

- If the underlay transport is MPLS; best methods are 6PE and 6VPE
- If the underlay transport is IP; dual stack, tunneling and translation are the options
- Depends on the company, their customer requirements and many other factors, one method might be better than other

https://t.me/learningnets

IPv6 Transition Mechanisms

There are three types of IPv6 Transition Mthods:

1. Dual Stack
- IPv6 + IPv4

The entire infrastructure is running both IPv4 and IPv6

2. Tunnels
- IPV6 - IPv4 – IPv6
- IPv4 – IPv6 – IPv4

Two IPv6 islands communicate over IPv4 part of the network or two IPv4 islands communicate over IPv6 part of the network

3. Translation

https://t.me/learningnets

- IPv6 – IPv4 (NAT64)

IPv6 Transition Mechanisms – Dual-Stack

- Many people state that IPv6 Dual Stack is the best transition method. Is Really Dual Stack best deployment method ?

- Many people would recommend it, before we try to answer this question, let’s understand how Dual-Stack works, what are the advantages and disadvantages, what are the challenges etc.

https://t.me/learningnets

IPv6 Transition Mechanisms – Dual-Stack

- Dual Stack is Native IPv6 and IPv4 Service, first was defined in RFC 2893
- Having IPv6 and IPv4 at the Hosts, network, operation/support tools, content and the application
- IPv4 applications use the IPv4 stack, and IPv6 applications use the IPv6 stack

https://t.me/learningnets

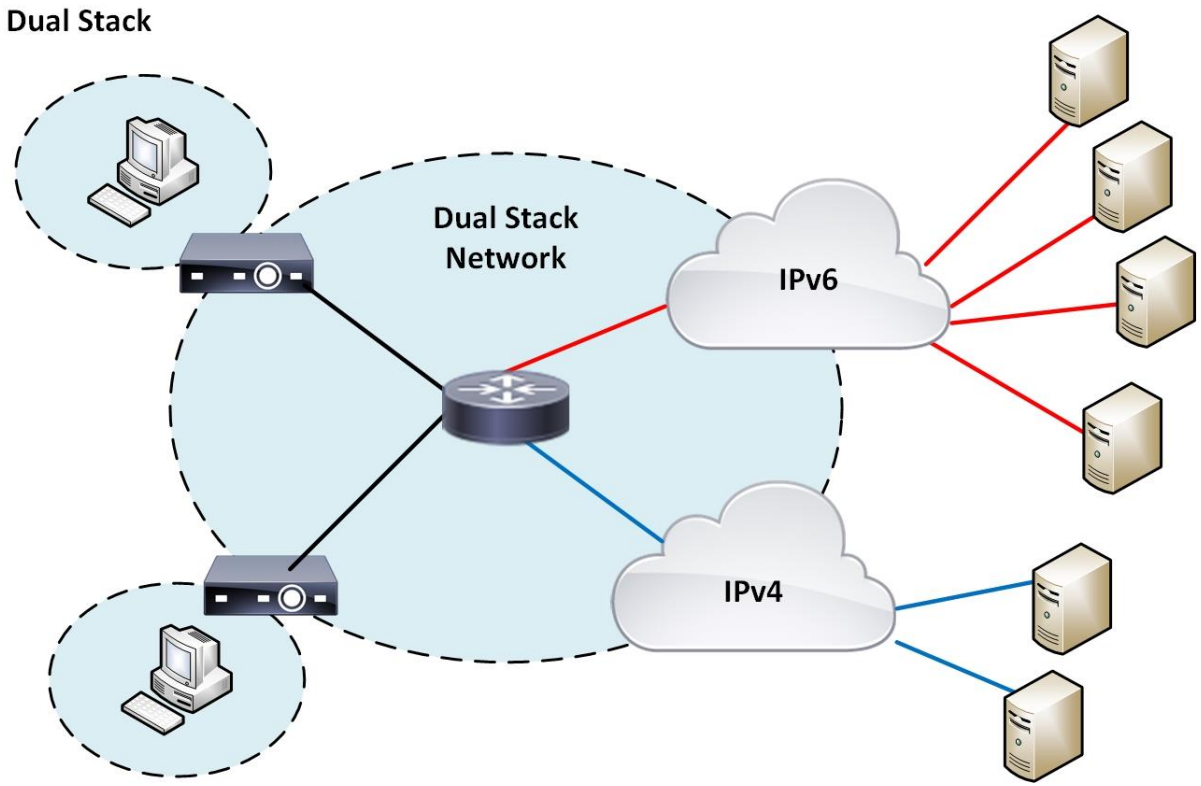
IPv6 Transition Mechanisms – Dual-Stack

- Routing protocols handle both IPv4 and IPv6

- Since entire network will have both IPv4 and IPv6, when it is needed IPv4 can be removed without causing down time

https://t.me/learningnets

IPv6 Transition Mechanisms – Dual-Stack



Network, Applications, Services, CPE and Access Networks needs to run Both IPv4 and IPv6

https://t.me/learningnets

IPv6 Transition Mechanisms – Dual-Stack

- Dual Stack is considered as Simplest solution , without any tunneling and translation mechanism (Most deployments will need translation, we will discuss)

- Every interface speaks both IPv4 and IPv6

- Communication is driven by DNS
  - If destination address in A record, communication is done via IPv4
  - If destination address in AAAA record, communication is done via IPv6
  - If both A and AAAA records are replied by DNS, then IPv6 is preferred

https://t.me/learningnets

Happy Eyeballs

- Happy Eyeballs has two versions, Version 1 defined in RFC 6555 , version 2 defined in RFC 8305
- Happy Eyeballs tries to prefer IPv6 connections to IPv4 connections, but will use an IPv4 connection if IPv6 isn’t working fast enough
- It is important to select IP address family
- Overall goal with the Happy Eyeballs is to improve end user performance in Dual Stack environment

https://t.me/learningnets

Happy Eyeballs

- When client receives both AAAA and A response from DNS server, before Happy Eyeballs, browsers preferred IPv6 over IPv4 and tried to setup TCP connection over IPv6. If the IPv6 routing , IPv6 Server have a problem or simply IPv6 is filtered on the path, browser waits TCP to timeout which can take a minute

- If there is second IPv6 address in DNS AAAA response, and if it has a problem as well, browser has to wait a minute more

- With Happy Eyeballs, if IPv6 connection somehow has a problem, failing back to IPv4 happens between 200 to 400 ms

https://t.me/learningnets

Happy Eyeballs

- With Happy Eyeballs, when there is a broken IPv6 path, failing back to IPv4 is much faster, RFC recommends 200 – 400 ms.

- Without Happy Eyeballs, first response when there is a broken IPv4 connectivity is to turn off IPv6 , which doesn't help for IPv6 adoption

- Thus Happy Eyeballs helps for transitioning to IPv6!

https://t.me/learningnets

Happy Eyeballs

- Both Operating Systems and the Browsers implement this algorithm
- Microsoft, Linux, Android , Apple IOS etc. comes with Happy Eyeballs
- Apple wrote Happy Eyeballs v2 RFC 8305

https://t.me/learningnets

Happy Eyeballs v1 vs. v2

https://t.me/learningnets

Dual-Stack Requirements

- Require sufficient amount of IPv4 addresses (Shouldn’t limit the growth of iPv6 deployment)

- If company doesn’t have an IPv4 address, they may need to purchase an IPv4 address from market

https://t.me/learningnets

Dual-Stack Requirements

- CPEs should support both IPv4 and IPv6

- Dual Stack also requires hardware and infrastructure which support IPv6

https://t.me/learningnets

Problems with Dual Stack

- How we can have Dual Stack if we don’t have enough IPv4 addresses?
  - Solution to this is CGN (Thus earlier I said that we will discuss)
- Having Dual Stack requires extra staff training
- Deploying both IPv6 and IPv4 requires extra device resources (RIB and FIB memory and CPU)

https://t.me/learningnets

Solution to IPv4 depletion with Dual Stack

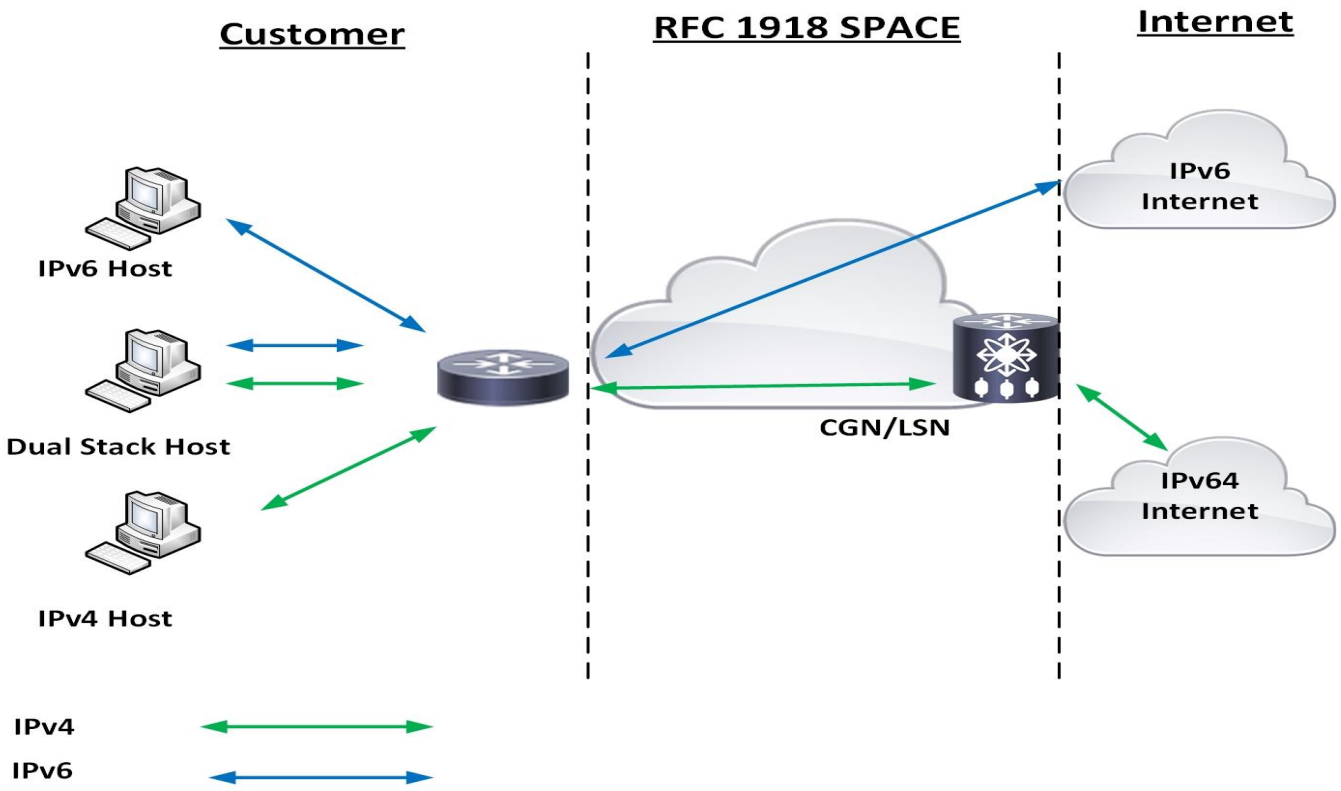
- Many Service Provider that want to deploy Dual Stack has IPv4 depletion problem

- Thus, in real life we see IPv6 deployment in the network and CGN for IPv4, this is called Dual Stack with SP NAT (CGN) deployment

https://t.me/learningnets

Solution to IPv4 depletion in Dual Stack Design

- IPv6 is available at the Host side
- But This solution requires CGN since Service Provider doesn't have enough IPv4 Public address and they don't purchase an IPv4 public address from market



Dual-Stack with CGN

https://t.me/learningnets

Solution to IPv4 depletion in Dual Stack Design

- Advantage of this design is company can have IPv6 everywhere
- Another advantage is amount of IPv4 Public address is low since there is NAT
- Disadvantage of this design is there is NAT, so all the possible problems of NAT (Will be discussed in detail) is applicable with this design option

https://t.me/learningnets

IPv6 Transition Mechanisms – Tunnels

- There are three different type of Tunnels :
  1. Manuel Tunnels
  2. Semi Automatic Tunnels
  3. Automatic Tunnels

- With Tunnels, two IPv6 islands communicate over IPv4 part of the network or two IPv4 islands communicate over IPv6 part of the network
  - IPV6 - IPv4 – IPv6
  - IPv4 – IPv6 – IPv4

https://t.me/learningnets

IPv6 Transition Mechanisms – Tunnels

- All tunneling mechanisms require that the endpoints of the tunnel run both IPv4 and IPv6 protocol stacks, that is, endpoints must run in dual-stack mode.

- The dual-stack routers run both IPv4 and IPv6 protocols simultaneously and thus can interoperate directly with both IPv4 and IPv6 end systems and routers

https://t.me/learningnets

IPv6 Transition Mechanisms – Tunnels

- It is possible to protect the IPv6 traffic over IPv4 tunnels using IPv4 IPSEC, by applying a crypto map to both the tunnel interface to encrypt outgoing traffic, and to the physical interface to decrypt the traffic flowing.

- Protecting tunnels in this way may negatively impact performance

- Last but not least, NAT is not allowed along the path of any tunneling mechanism

https://t.me/learningnets

Manuel/Configured IPv6 Tunnels

- Manuel Tunnels for IPv6 were explained in RFC 4213 (Basic Transition Mechanisms for IPv6 Hosts). It is known as Configured IPv6 Tunnels. Tunnel source and the destination manually need to be configured

- A technique for establishing point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.

https://t.me/learningnets

Manuel/Configured IPv6 Tunnels

- Requires Dual Stack Tunnel End Points, both IPv4 and IPv6 addresses are configured at each end of the Tunnel
- When there are so many sites, Manuel tunnels are not considered scalable
- 6PE and 6VPE are considered as Manuel/Configured Tunnels, both of these concepts will be explained later in detail

https://t.me/learningnets

Manuel/Configured IPv6 Tunnels

According to RC 4213, Tunneling can be used in a variety of ways:

- Router-to-Router. IPv6/IPv4 routers interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans one segment of the end-to-end path that the IPv6 packet takes

- Host-to-Router. IPv6/IPv4 hosts can tunnel IPv6 packets to an intermediary IPv6/IPv4 router that is reachable via an IPv4 infrastructure. This type of tunnel spans the first segment of the packet's end-to-end path

https://t.me/learningnets

Manuel/Configured IPv6 Tunnels

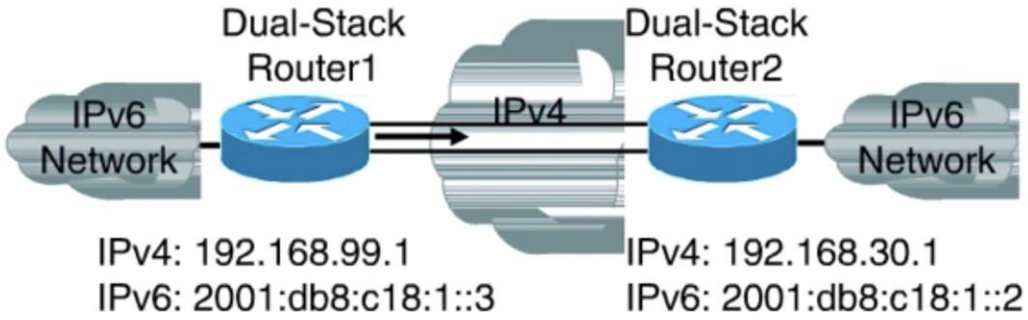
- Host-to-Host. IPv6/IPv4 hosts that are interconnected by an IPv4 infrastructure can tunnel IPv6 packets between themselves. In this case, the tunnel spans the entire end-to-end path that the packet takes

- Router-to-Host. IPv6/IPv4 routers can tunnel IPv6 packets to their final destination IPv6/IPv4 host. This tunnel spans only the last segment of the end-to-end path

https://t.me/learningnets

Manuel IPv6 Tunnels - How it works

Manually Configured Tunnel (RFC4213)




```
router1#

interface Tunnel0
 ipv6 address 2001:db8:c18:1::3/64
 tunnel source 192.168.99.1
 tunnel destination 192.168.30.1
 tunnel mode ipv6ip
```

```
router2#

interface Tunnel0
 ipv6 address 2001:db8:c18:1::2/64
 tunnel source 192.168.30.1
 tunnel destination 192.168.99.1
 tunnel mode ipv6ip
```

- Manually Configured tunnels require:
  - Dual stack end points
  - Both IPv4 and IPv6 addresses configured at each end

https://t.me/learningnets

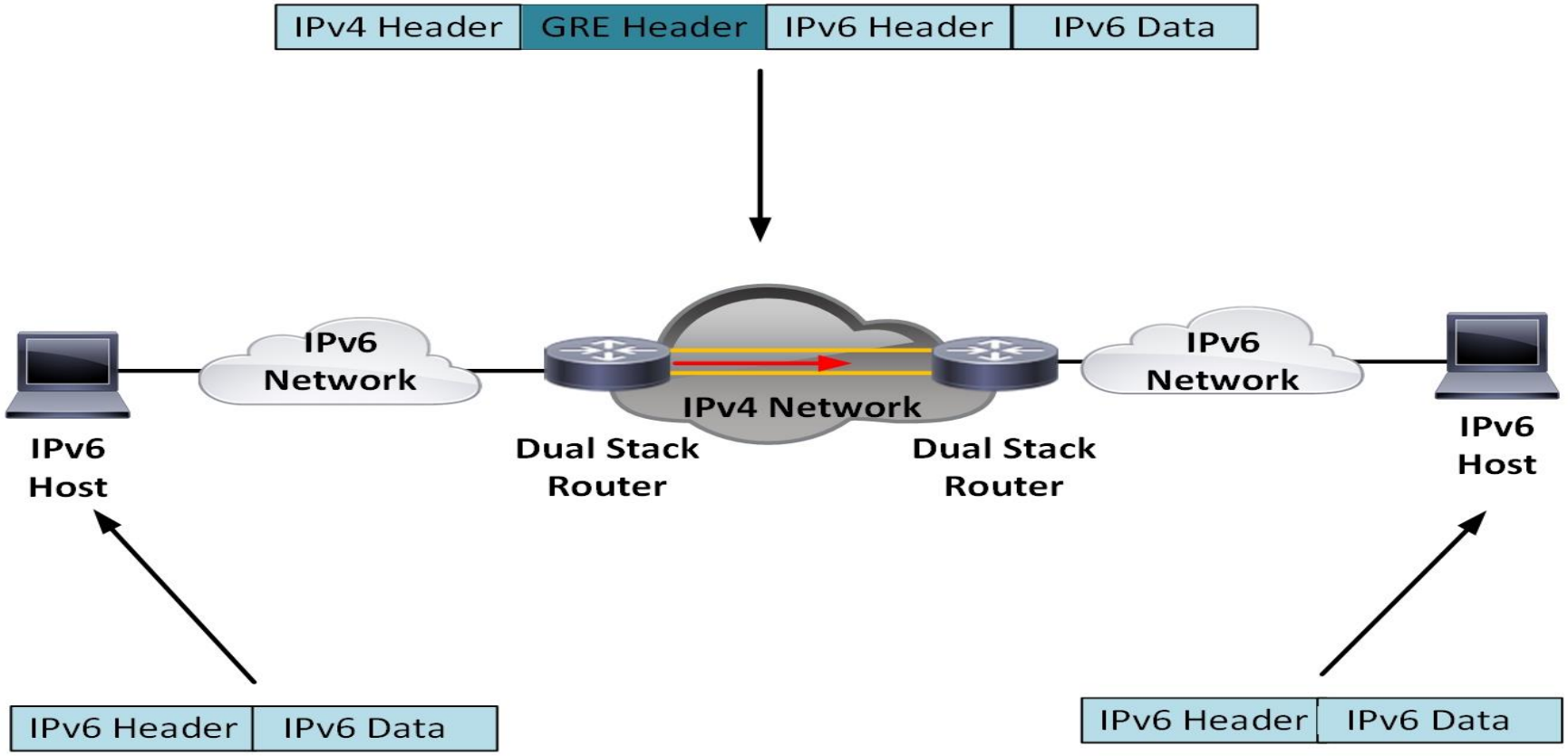
Manuel IPv6 Tunnels – GRE Tunnel

- GRE Tunnel is another Manuel/Configured Tunneling mechanism which can be used for transporting IPv6 packets over IPv4 infrastructure or vice versa

- The IPv6 over IPv4 GRE tunnel uses the standard GRE tunneling technique that is designed to provide the services necessary to implement any standard point-to-point encapsulation scheme

https://t.me/learningnets

Manuel IPv6 Tunnels – GRE Tunnel



https://t.me/learningnets

Semi Automatic IPv6 Tunnels – Tunnel Brokers

- With Semi-Automatic Tunnels, tunnel destination address is automatically learned , not manually configured

- Tunnel Brokers are Semi-Automatic Tunnels, explained in RFC 3053

- At the host side, tunnel can be initiated by the PC or Router which can serve to entire LAN

https://t.me/learningnets

Semi Automatic IPv6 Tunnels – Tunnel Brokers

- The Tunnel Broker idea is an alternative approach based on the provision of dedicated servers, called Tunnel Brokers, to automatically manage tunnel requests coming from the users

- Tunnel brokers can be seen as virtual IPv6 ISPs, providing IPv6 connectivity to users already connected to the IPv4 Internet

https://t.me/learningnets

Semi Automatic IPv6 Tunnels – Tunnel Brokers

- The IPv6 Tunnel Broker provides an automatic configuration service for IPv6 over IPv4 tunnels to users connected to the IPv4 Internet
- IPv4 connectivity between the user and the Service Provider is required
- Tunnel Broker can be considered as ‘Authoritative Server’ which provides the IP addresses and the parameters of the actual Tunnel endpoints to the IPv6 end users (Hosts or Routers)

https://t.me/learningnets

Elements of a Tunnel Broker

Tunnel Broker (TB)

- The TB is the place where the user connects to register and activate tunnels. The TB manages tunnel creation, modification and deletion on behalf of the user

- For scalability reasons the tunnel broker can share the load of network side tunnel end-points among several tunnel servers

https://t.me/learningnets

Elements of a Tunnel Broker

Tunnel Broker (TB)

- It sends configuration orders to the relevant tunnel server whenever a tunnel has to be created, modified or deleted

- The TB may also register the user IPv6 address and name in the DNS

https://t.me/learningnets

Elements of a Tunnel Broker

Tunnel server (TS)

- A Tunnel Server is a dual-stack (IPv4 & IPv6) router connected to the global Internet
- Upon receipt of a configuration order coming from the TB, it creates, modifies or deletes the server side of each tunnel
- It may also maintain usage statistics for every active tunnel

https://t.me/learningnets

How Tunnel Broker Mechanisms Works

- The client of the Tunnel Broker service is a dual-stack IPv6 node (host or router) which is connected to the IPv4 Internet

- Approaching the TB, the client should be asked first of all to provide its identity and credentials so that proper user authentication, authorization and (optionally) accounting can be carried out (e.g., relying on existing AAA facilities such as RADIUS)

- This means that the client and the TB have to share a pre-configured or automatically established security association to be used to prevent unauthorized use of the service

https://t.me/learningnets

How Tunnel Broker Mechanisms Works

- **When the host request to create IPv6 Tunnel, The Tunnel Broker manages the client requests as follows:**

- Tunnel Broker first designates (e.g., according to some load sharing criteria defined by the TB administrator) a Tunnel Server to be used as the actual tunnel end-point at the network side

- It chooses the IPv6 prefix to be allocated to the client; the prefix length can be anything between 0 and 128, most common values being 48 (site prefix), 64 (subnet prefix) or 128 (host prefix)

https://t.me/learningnets

How Tunnel Broker Mechanisms Works

- It fixes a lifetime for the tunnel; - it automatically registers in the DNS the global IPv6 addresses assigned to the tunnel end-points

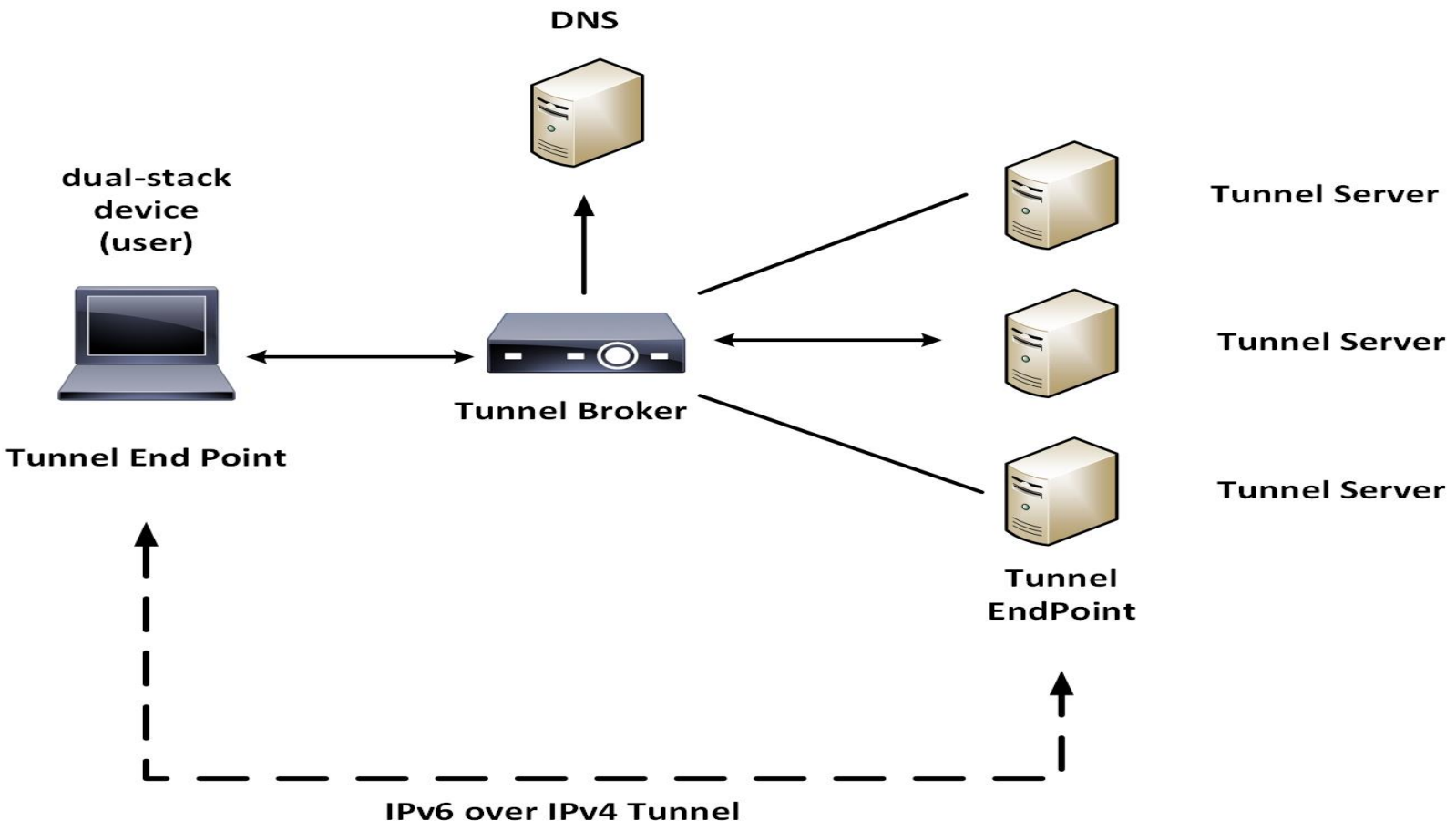
- It configures the server side of the tunnel

- It notifies the relevant configuration information to the client, including tunnel parameters and DNS names

After the above configuration steps have been carried out (including the configuration of the client), the IPv6 over IPv4 tunnel between the client host/router and the selected TS is up and working, thus allowing the tunnel broker user to get access to the IPv6 Internet

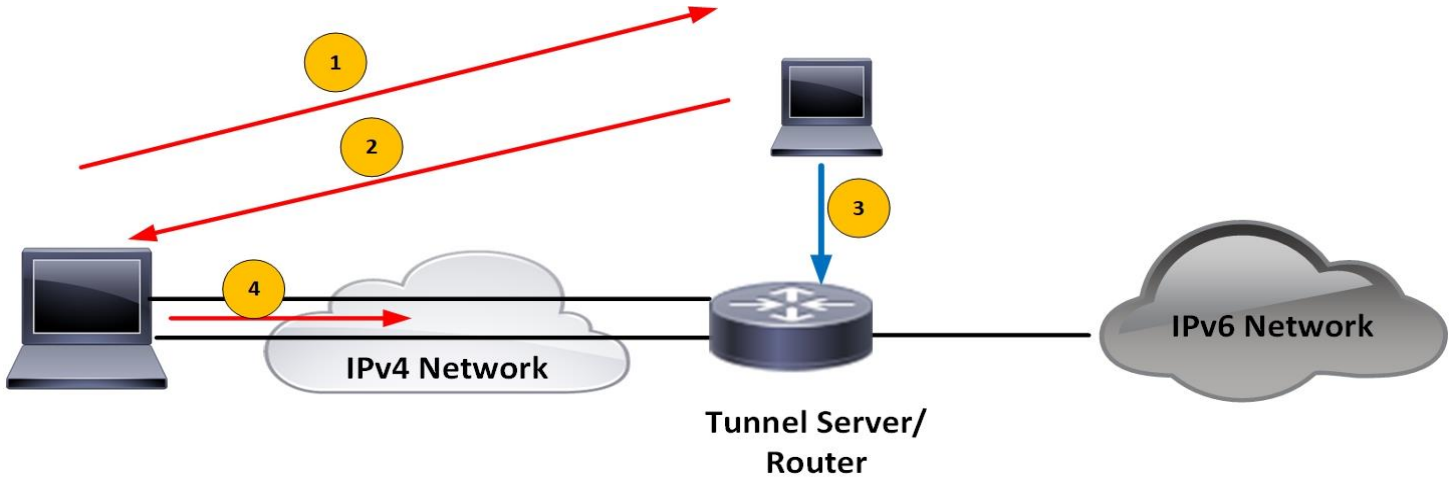
https://t.me/learningnets

How Tunnel Broker Works



https://t.me/learningnets

How Tunnel Broker Works



1. Tunnel request over HTTPS on IPv4
2. Tunnel information response on IPv4
3. Tunnel Broker configures the tunnel on the Tunnel Server
4. Client/End User established the Tunnel with the Tunnel Server

Tunnel Broker

https://t.me/learningnets

Who provides IPv6 Address to the Tunnel Broker Service End Users?

- The IPv6 addresses assigned to both sides of each tunnel must be global IPv6 addresses belonging to the IPv6 addressing space managed by the TB

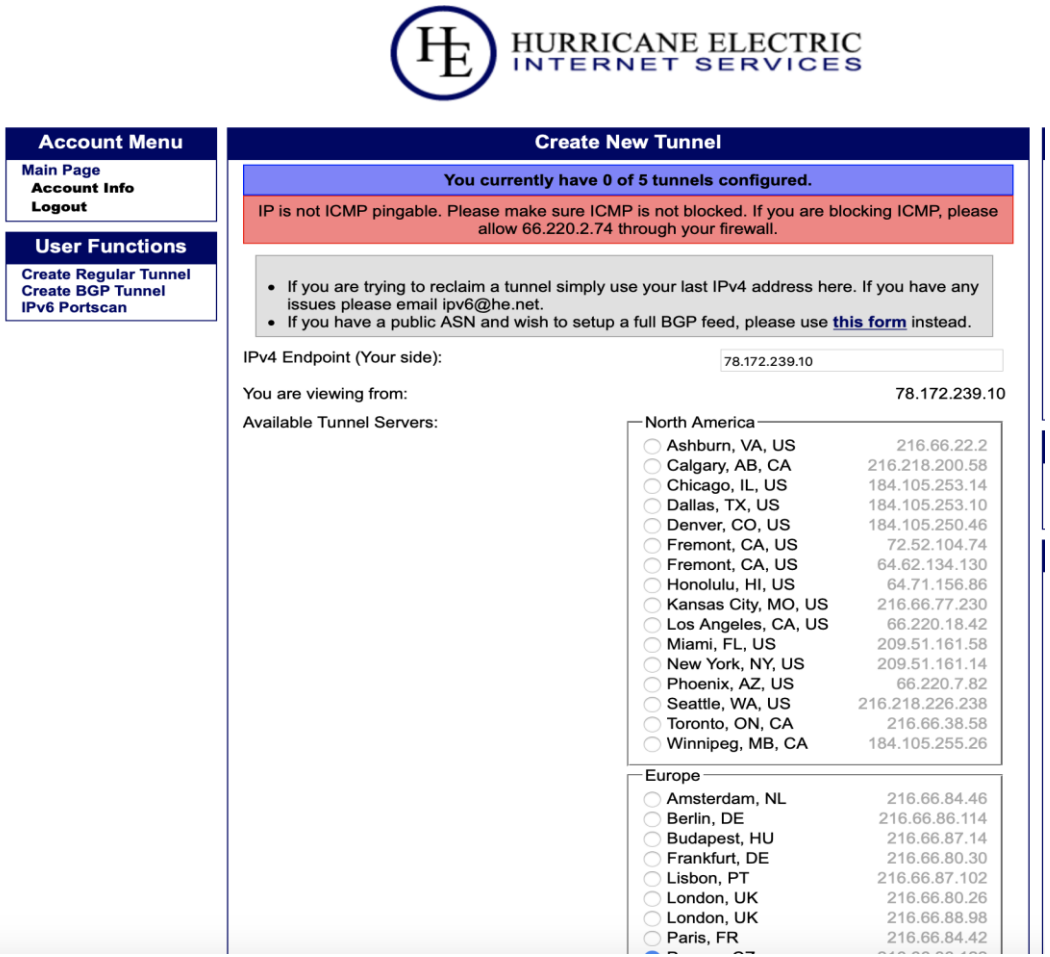
- You can find public FREE Ipv6 Tunnel Broker services from http://www.sixxs.net/ and http://tunnelbroker.net/

https://t.me/learningnets

Tunnel Broker – Hurricane Electric

- I created an account on HE to have IPv6 tunnel from my PC to HE Tunnel Servers as you can see from this figure

- I am a IPv6 requesting client, HE is a Tunnel Broker, communication between us was a Https portal of Hurricane Electric



https://t.me/learningnets

Automatic Tunnels for IPv6 Transition

- With Automatic Tunnels, Tunnel endpoints must be derived automatically , thus provides scalability in design
- IPv4 endpoint addresses are embedded in IPv6 address
- Automatic tunnels are generally suitable for temporary tunnels, transient connectivity : site to site or host to host VPNs

https://t.me/learningnets

6to4 Automatic Tunnel

- RFC 3056 is explained 6to4 Automatic Tunnels as “Connection of IPv6 Domains via IPv4 Clouds”

- Tunnel IPv4 endpoint addresses are embedded in the IPv6 address with this tunneling mechanism thus it is a stateless tunneling mechanism

- 6to4 Tunnels is used to connect two IPv6 islands over IPv4 network

https://t.me/learningnets

6to4 Automatic Tunnel

- It creates a block of IPv6 addresses from a locally configured IPv4 address by embedding that IPv4 address to the prefix 2002::/16, resulting in a /48 IPv6 prefix

- IPv6 packets are encapsulated by adding an IPv4 header with the Protocol field set to 41

https://t.me/learningnets

6to4 Automatic Tunnel

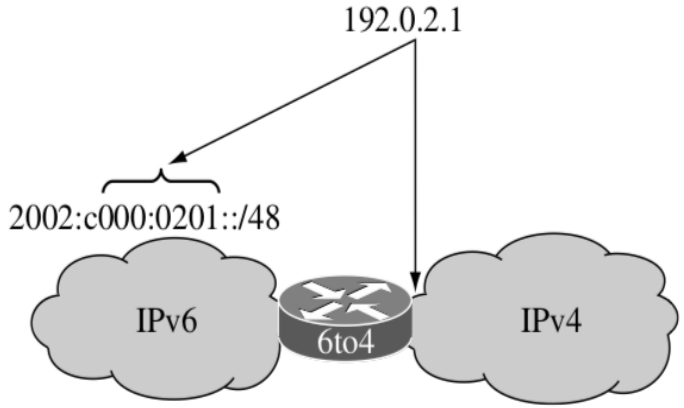
- The 6to4 IPv6 address space is built by the 2002::/16 prefix reserved for the 6to4 mechanism, followed by the 32 bits of the IPv4 external address of the border router of the site, giving the site a /48 prefix

https://t.me/learningnets

6to4 Automatic Tunnel

- The border router has an external IPv4 address (192.0.2.1). The IPv6 site behind the border router uses 2002:c000:0201::/48 to number its whole network.

- The address space is based on 2002:<ipv4 external address in hex>::/48, where the IPv4 address is the border router external IPv4 address (192.0.2.1), represented in hexadecimal as c000:0201

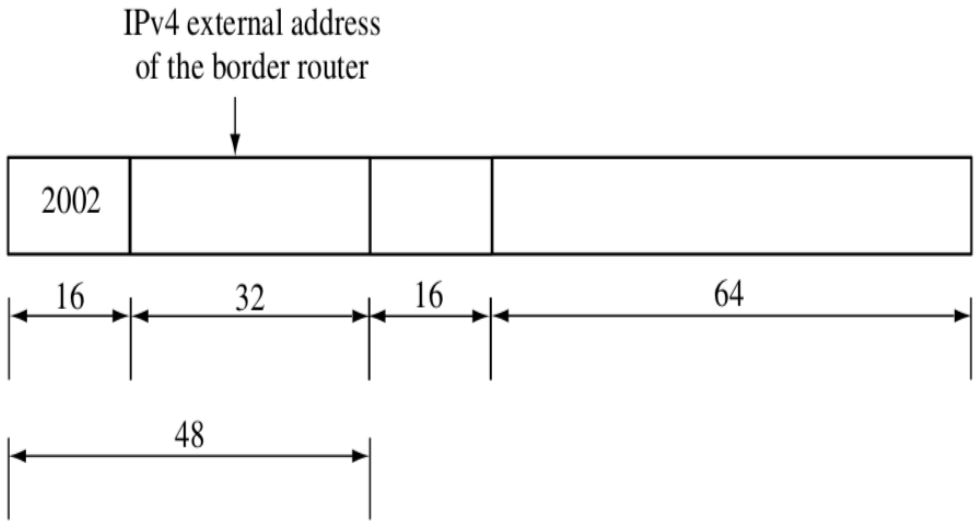


6to4 site IP address space is based on the border router IPv4 address

https://t.me/learningnets

6to4 Automatic Tunnel

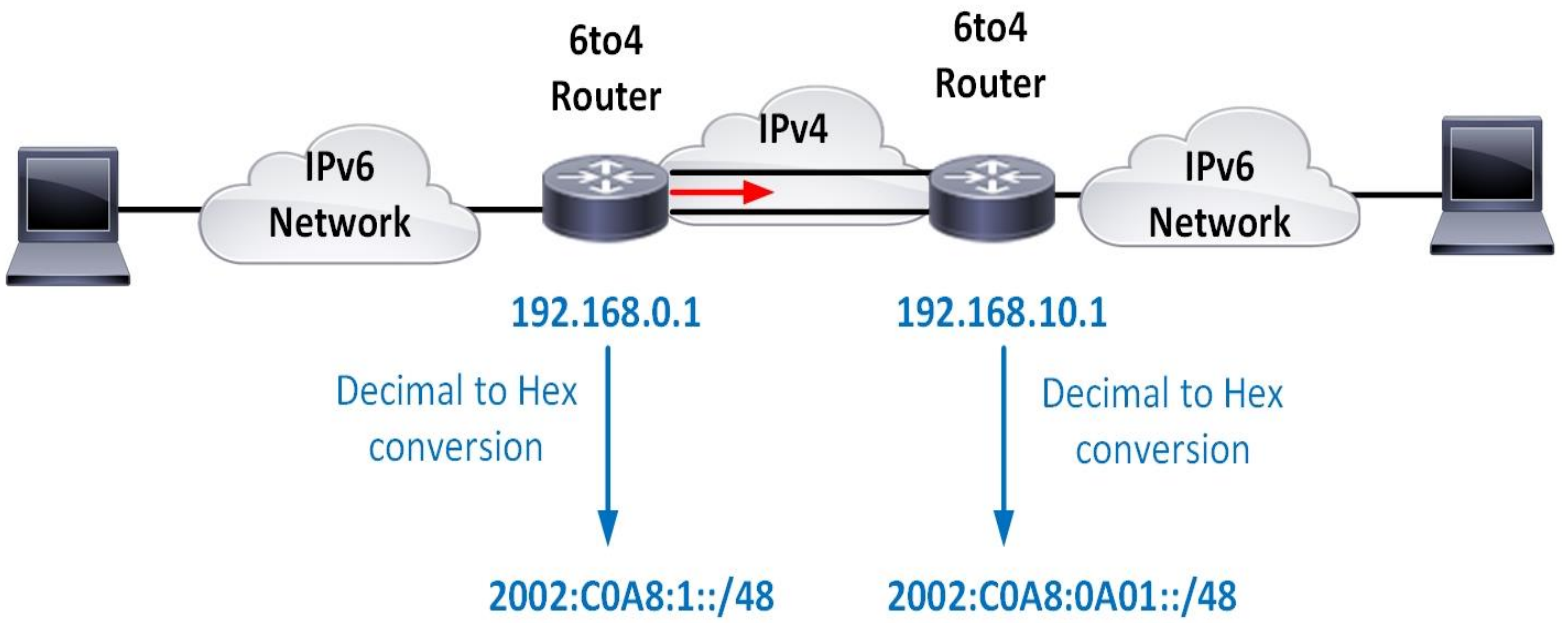
- 6to4 Address Structure



The 6to4 mechanism needs to be only implemented in border routers. Hosts inside the IPv6 site do not need to support 6to4

https://t.me/learningnets

6to4 Automatic Tunnel



- **2002::/16 is allocated for 6to4 tunnels**
- **Border Router IPv4 address is Public as well, not RFC 1918**

https://t.me/learningnets

6to4 Deployment/Configuration

- Below is the 6to4 Tunnel Configuration on the Cisco device

```
Router#
Interface loopback 0
    ip address 192.168.0.1  255.255.255.0
    ipv6 address 2002:C0A8:1:1::./64 eui-64
Interface Tunnel 0
    tunnel source Loopback 0
    tunnel mode ipv6ip 6to4
ipv6 route 2002::/16 Tunnel 0
```

https://t.me/learningnets

6to4 Tunnel Border Relay

- If host A sends a packet to C with a non-6to4 address such as 3ffe:b00:1::1, the R1 router, the border router of A's site, does not know where to route the packet since the destination address is not a 6to4 address. R1 needs a 6to4 relay to the non-6to4 IPv6 Internet

- A 6to4 relay is a 6to4 border router that has connectivity to the rest of the IPv6 networks

- It is used as a transit for the other 6to4 sites to reach the non-6to4 IPv6 networks.

https://t.me/learningnets

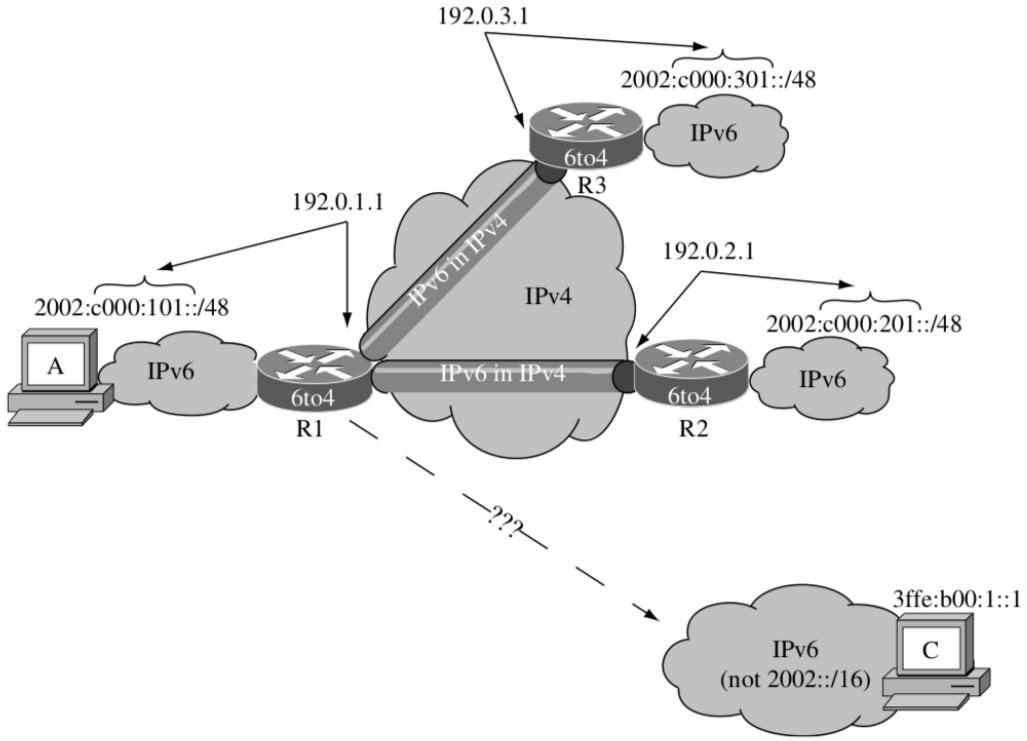
6to4 Tunnel Border Relay

- To enable the 6to4 relay, the 6to4 relay router is a 6to4 router with a default route to the IPv6 Internet
- The 6to4 relay should contain some ingress filtering
- A 6to4 site that is using a 6to4 relay installs in the 6to4 border router an IPv6 default route pointing to the 6to4 address of the relay
- 6to4 relay routers do not require specific features to act as 6to4 relays, just a static route entry

https://t.me/learningnets

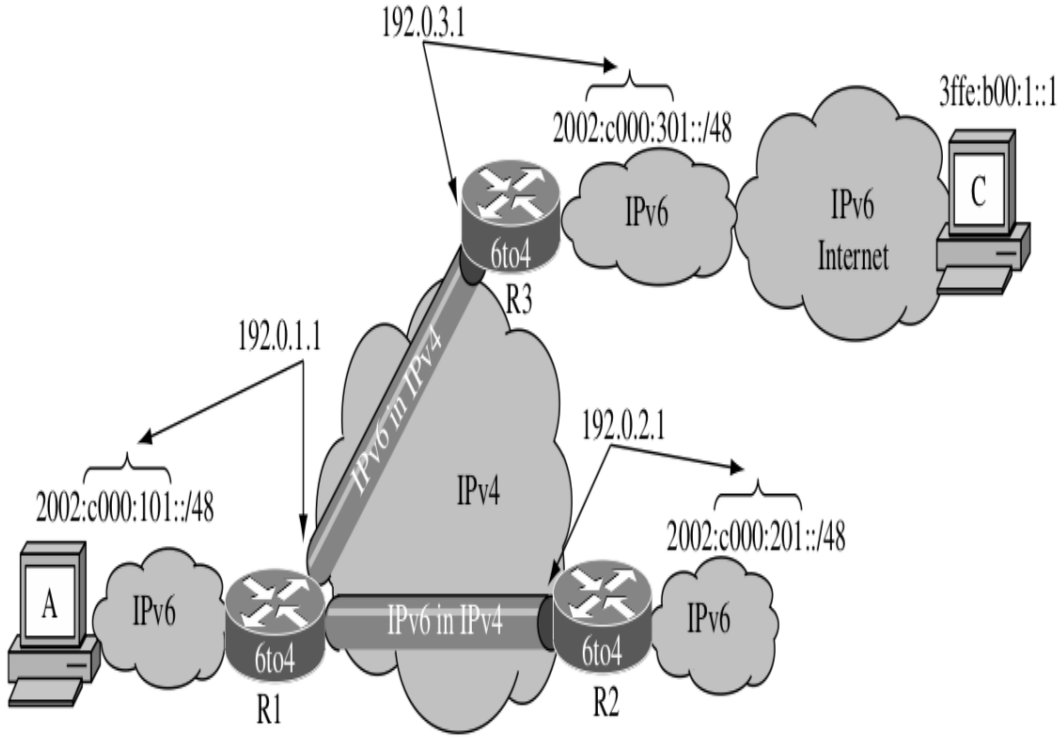
6to4 Tunnel Border Relay – Without Relay

- Without Border Relay, 6to4 site cannot communicate with non-6to4 site



https://t.me/learningnets

6to4 Tunnel Border Relay – With Relay



In the left figure, A sends a packet to C. R3 is the 6to4 relay for R1 and is connected to the non-6to4 IPv6 Internet. When R1 wants to forward the packet to a non-6to4 destination address (3ffe:b00:1::1), it cannot build an automatic tunnel to some other 6to4 router, since it cannot extract the IPv4 address from the IPv6 destination address. If R1 has a default route to go through R3 via the 6to4 mechanism, then R1 encapsulates the IPv6 packet to R3 and R3 decapsulates it and forwards it to the IPv6 network

https://t.me/learningnets

6to4 Tunnel Summary

- 6to4 is an Automatic Tunneling mechanism
- Assign a IPv6 prefix to the attached network
- The 6to4 mechanism uses the 2002::/16 prefix. Any 6to4 site has the following address space: 2002:<ipv4 external address in hex>::/48. Only the border router has to support 6to4
- 2002::/16 address is assigned to the customer network, not an address from Global Unique Address of the company, this is the limitation of 6to4 tunneling mechanism

https://t.me/learningnets

6to4 Tunnel Summary

- Border Routers run dual stack and support 6to4
- A 6to4 capable border router cannot use 6to4 if it is not assigned a public IPv4 address.
- All 6to4 sites are reachable through their IPv4 border router address
- All 6to4 sites have a 6to4 relay, statically configured on the site border router, to transit the non-6to4 IPv6 traffic
- Hosts do not need to support or know about 6to4

https://t.me/learningnets

6rd – IPv6 Rapid Deployment

- RFC 5569 is written for IPv6 Rapid Deployment on IPv4 Infrastructures
- 6rd is an extension of 6to4 tunnels
- It is an Automatic tunneling mechanism (IPv6 over IPv4 network)

https://t.me/learningnets

6rd – IPv6 Rapid Deployment

- With 6to4 tunnels, 2002::/16 reserved prefix need to be used as an IPv6 prefix

- With 6rd, this restriction is removed, IPv6 prefix can be used from the company's local address block (Global Unicast Block)

- 6rd consists of two main hardware components, the CE (Customer Equipment) router and the BR (Border Relay) router

https://t.me/learningnets

6rd - CE (Customer Edge) Router

- The CE router is positioned at the edge of the service provider IPv4 access infrastructure
- Provides IPv6 connectivity to this end user's network
- The native IPv6 traffic coming from the end user hosts is encapsulated in IPv4 by the CE router and tunneled to the Border Relay router or directly to other CE routers in the same 6rd domain
- Conversely, encapsulated 6rd traffic received from the Internet through the Border Relay router and 6rd traffic from other CE routers will be de-capsulated and forwarded to the end-user nodes

https://t.me/learningnets

6rd - Border Relay Router

- The BR router provides connectivity between the CE routers and the IPv6 Internet. Both the CE and BR routers are dual-stack devices, and the devices between the BR and CE routers can be IPv4 only

- At the CE router, if the packet IPv6 destination address matches the locally configured 6rd prefix, the packet is considered to be part of the local 6rd domain and needs to be forwarded to another CE router.

- In such a case, the IPv4 address embedded in the IPv6 destination address is used as the IPv4 destination address of the 6rd tunnel, and the local WAN interface IPv4 address is used as the source address for the 6rd tunnel, which is an IPv6 packet directly encapsulated in IPv4.

https://t.me/learningnets

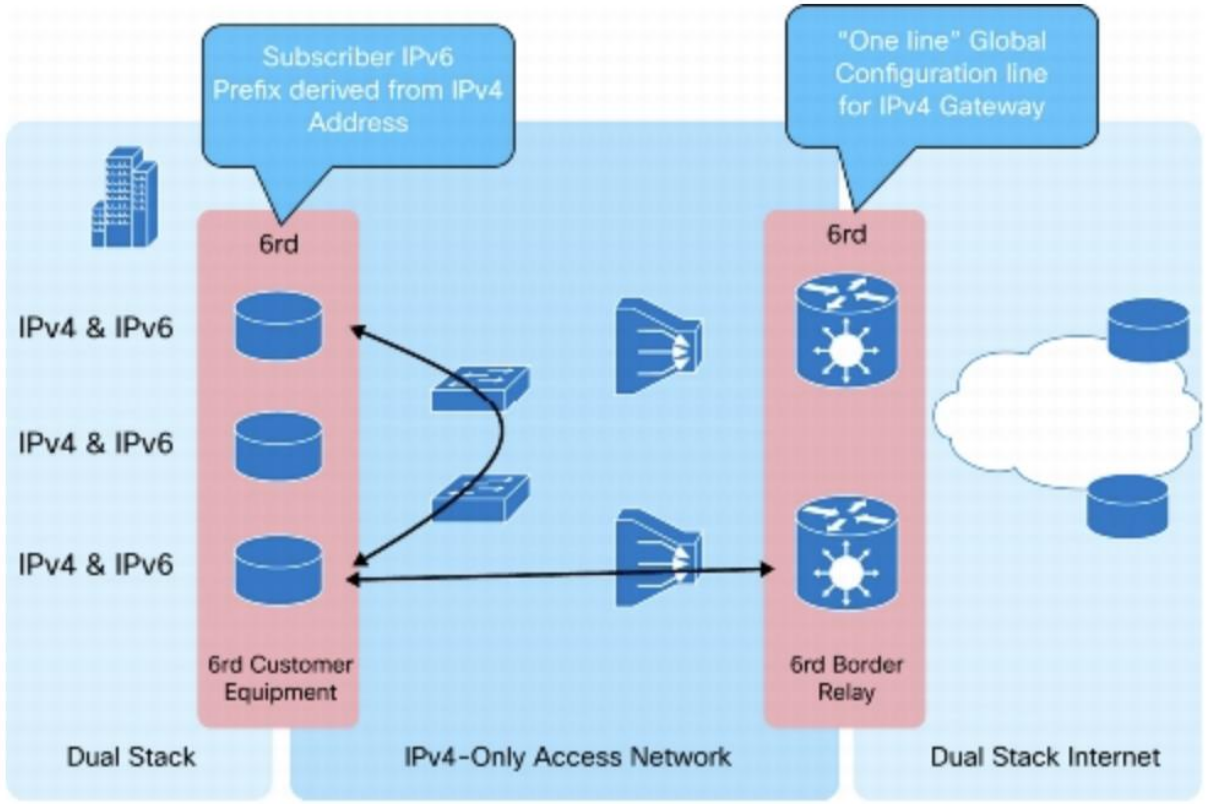
6rd - Border Relay Router

- If the IPv6 destination address does not match the locally configured 6rd prefix-in other words, if the packet does not belong to the local 6rd domain-the packet will be tunneled to the BR router by a 6rd tunnel

- In this case, the locally configured BR IPv4 address on the CE router is used as the destination address for the encapsulated packet.

https://t.me/learningnets

6rd - Border Relay Router



6rd consists of two main hardware components, the CE (Customer Equipment) rou

https://t.me/learningnets

6rd – IPv6 Rapid Deployment

- Similar to 6to4 IPv6 tunnels, 6rd is a standard based stateless tunneling mechanism.

- Since 6rd is Stateless, packets don’t have to go through the same BR (Border Relay) router

- Border Relay is required if the destination IPv6 address is outside the company network

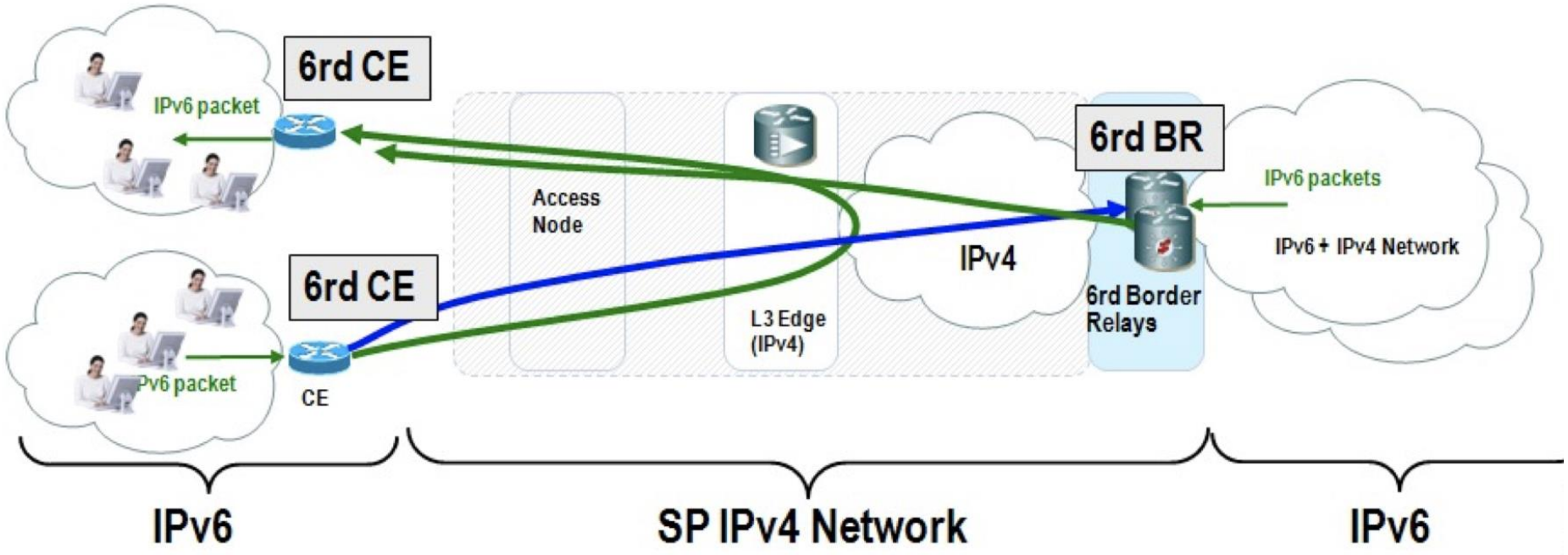
https://t.me/learningnets

6rd – IPv6 Rapid Deployment

- If two IPv6 customer sites talk to each other, traffic doesn’t go through Border Relay Routers
- For HA and Load Balancing, more than one Border Relay is used
- Each border relay router needs to be configured with the same IPv4 address (Anycast) so that CE routers are routed to the closest border relay.

https://t.me/learningnets

6rd – IPv66 Rapid Deployment Traffic Flow Within Domain and Outside Domain



https://t.me/learningnets

6rd Summary

- Extension of 6to4 Tunnel
- Used as a stateless tunneling mechanism as IPv6 Transition mechanism
- IPv6 networks can communicate over IPv4 network
- Removed the requirement of having 2002::/16 IPv6 prefix for tunneling, instead company local IPv6 prefix can be used for tunneling

https://t.me/learningnets

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

- It is a host to router or host to host Automatic tunneling mechanism, host can tunnel IPv6 traffic across IPv4 network

- Defined in RFC5214, so it is a standard based mechanism

- ISATAP enables unicast communication between IPv6/IPv4 hosts across the IPv4-only Intranet and Internet (If ISATAP router has an access to the IPv6 Internet), it doesn’t support Multicast

https://t.me/learningnets

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

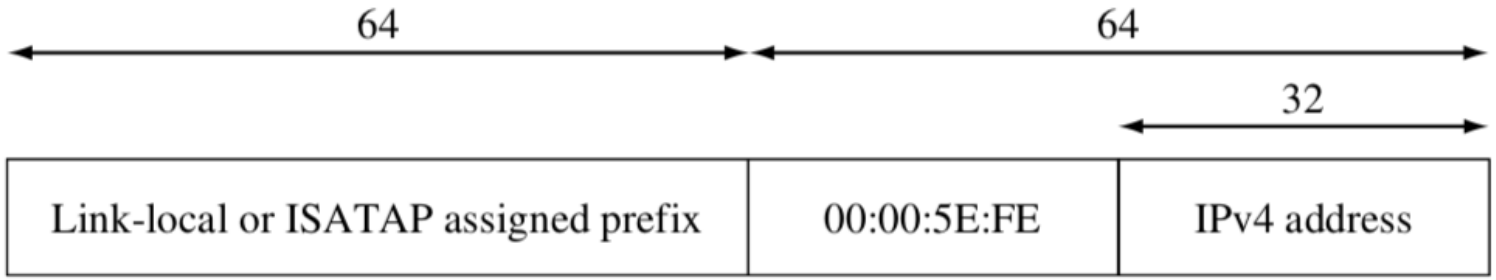
- Embeds the IPv4 address of the node in the last 32 bits of the interface identifier part of its IPv6 address

- It utilizes DNS to determine what prefix it is to assign and what gateway to use

https://t.me/learningnets

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

- Below figure shows the format of an ISATAP address. The first 32 bits of the interface identifier are ‘00:00:5E:FE’, reserved by IANA for ISATAP, and define the ISATAP interface identifier



https://t.me/learningnets

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

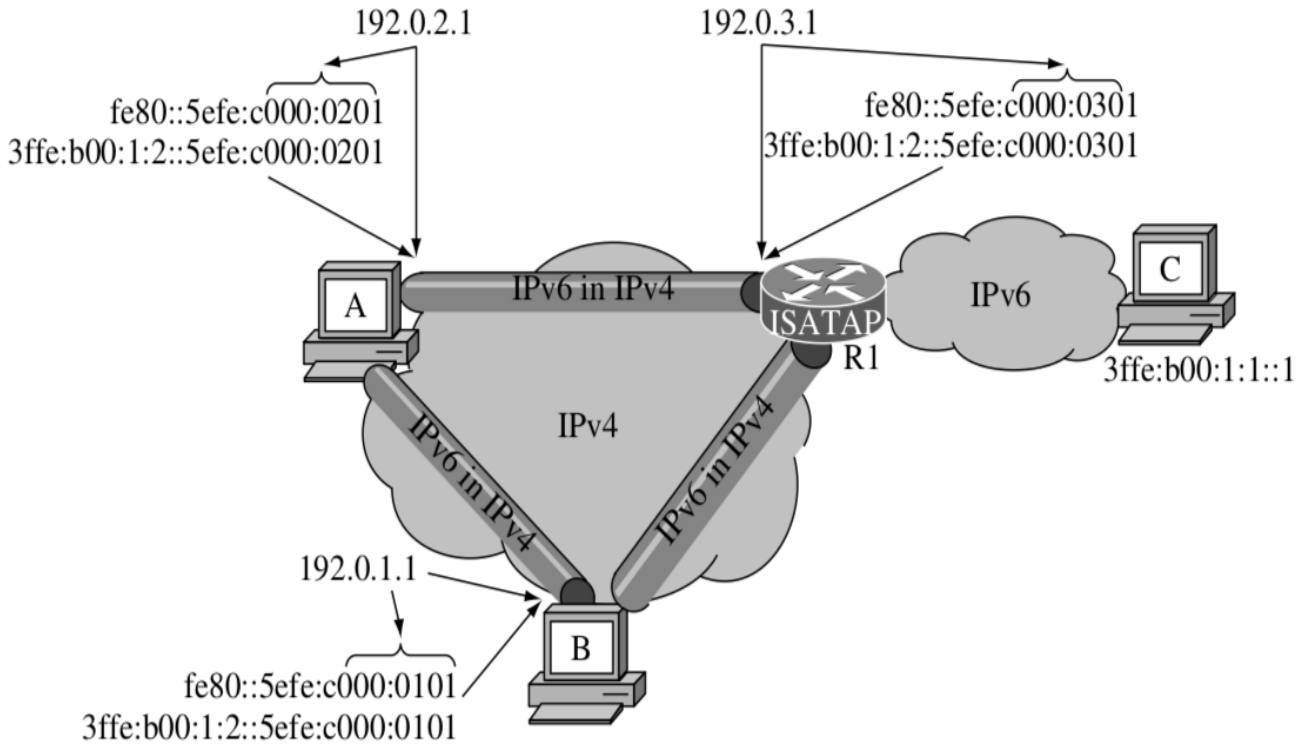
- ISATAP creates a virtual link over a full IPv4 site, thus enabling ISATAP on a host/router creates on them a virtual interface with an IPv6 address

- ISATAP implementation in an organization is designed to take your entire IPv4 network, and make it one big IPv6 logical link. You don't "subnet" ISATAP networks. So, all of your IPv4 becomes one large IPv6 subnet as far as ISATAP is concerned

- Link-local address (fe80::/64), unique-local, or global addresses can be used as IPv6 ISATAP addresses
- Hosts and the Router which will have IPv6 over IPv4 tunneling, needs to have Dual-Stack and ISATAP to be enabled

https://t.me/learningnets

ISATAP – Link Local and Global ISATAP Addressing

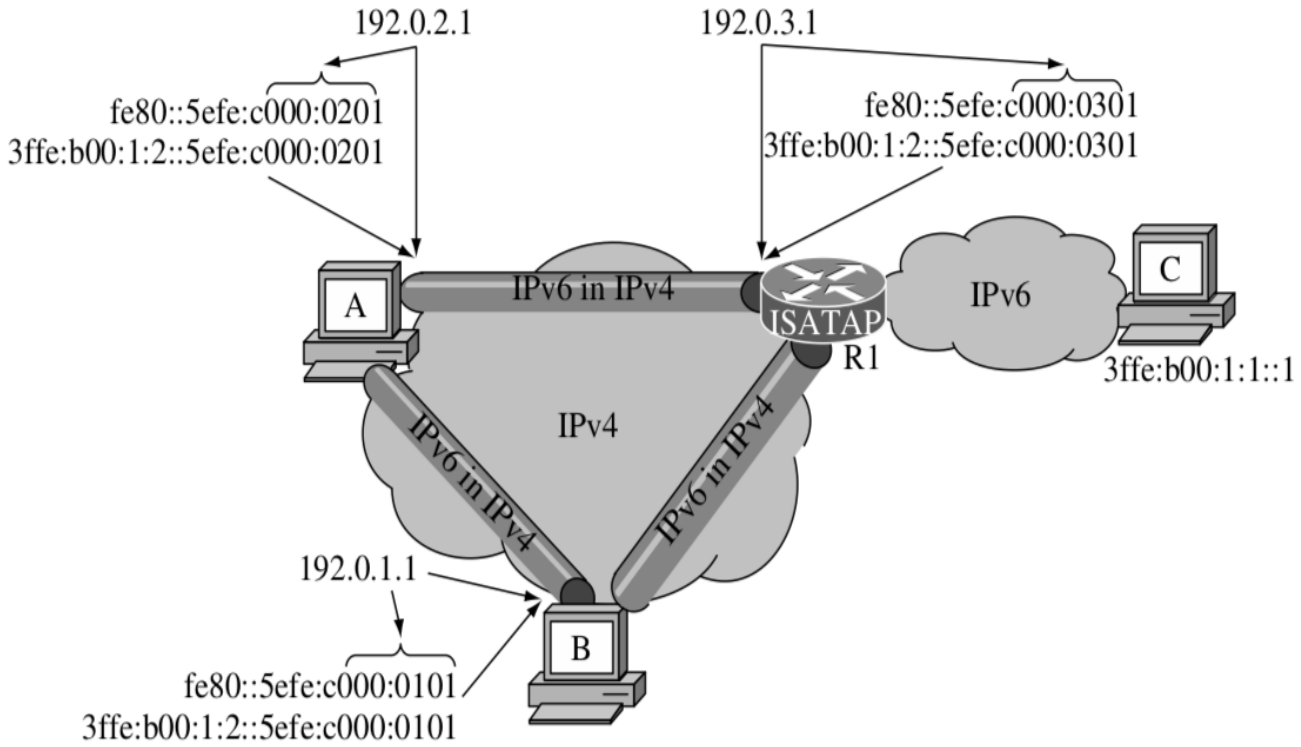


Host A, host B and router R1 are all dual-stack and have an enabled implementation of ISATAP

Host C is IPv6 without ISATAP. The network manager uses the 3ffe:b00:1::/48 for its site. It assigns 3ffe:b00:1:2::/64 to the ISATAP virtual link over the IPv4 network

https://t.me/learningnets

ISATAP – Link Local and Global ISATAP Addressing



Host A has the 192.0.2.1 IPv4 address and creates its link-local address based on the ISATAP format: fe80::5efe:c000:0201, computed using the ISATAP 32 bit interface identifier (0000:5efe) and the hexadecimal representation (c000:0201) of its IPv4 address (192.0.2.1). Host B and router R1 do the same respectively, which builds a virtual link , all are link local neighbor of each other

https://t.me/learningnets

ISATAP Router

- In ISATAP, when hosts are dual-stack and ISATAP enabled, they directly communicate via IPv6 with each other without ISATAP router
- ISATAP router is needed when there is ISATAP host communicate with non-ISATAP enabled IPv6 host and IPv6 Internet
- ISATAP Router is needed for publishing a prefix for ISATAP IPv6 auto-addressing on the hosts

https://t.me/learningnets

ISATAP Router

- When a host auto-configures it’s ISATAP address, it first contacts the ISATAP Router to learn it’s prefix

- The ISATAP Router is statically configured in all ISATAP nodes or hosts can discover the ISATAP router via DNS

https://t.me/learningnets

ISATAP Summary

- ISATAP is used within a site, or within one administrative domain
- ISATAP creates a virtual link over a potentially wide IPv4 network. Any broadcast-like packet, such as one sent to ff01::1, on the link will create a potentially large number of packets on the network. So the more ISATAP nodes that are deployed, the less it is scalable
- ISATAP does not traverse NAT
- ISATAP doesn’t support Multicast, so you cannot run routing protocols over ISATAP tunnels

https://t.me/learningnets

TEREDO

- Teredo enables nodes to tunnel IPv6 over IPv4 through NATs , similar to 6to4 and 6rd, it is an auto tunnel IPv6 over IPv4 protocol

- It provides automatic tunneling that allows IPv6/IPv4 (Dual stack) hosts to establish IPv6 connectivity with each other across the IPv4 Internet even when IPv4 network address translation (NAT) devices need to be traversed

- Because of this capability, Teredo is considered more suitable than 6to4 for small office/home office (SOHO) environments that use NATs to hide their private IPv4 addresses from the Internet

https://t.me/learningnets

- Similar to 6to4, Teredo uses it’s own address prefix , which is 2001:0::/32

- If the local network is behind an IPv4 NAT, and the NAT gateway does not support 6to4, Teredo can be used by the host to reach IPv6 network

https://t.me/learningnets

TEREDO

- Teredo encapsulates IPv6 packets over UDP over IPv4

- Teredo makes a lot of assumptions about the NAT behavior. This is based on experimental results from trying different vendors implementations at specific points in time. Not only were all vendors not tried, but there is no guarantee that the observed behaviors will remain in the subsequent releases of those NAT products.

- Teredo might not function because of some new or non-observed NAT behavior.

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

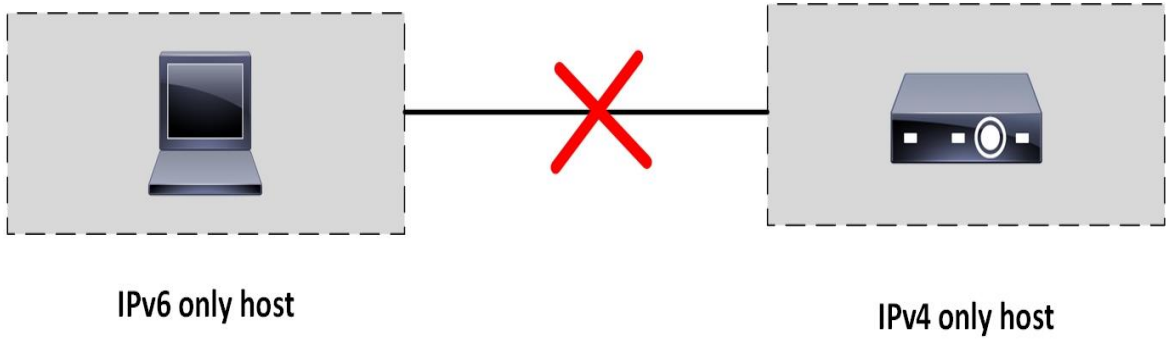
https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

NAT64

- IPv6 only host cannot communicate directly to IPv4 host



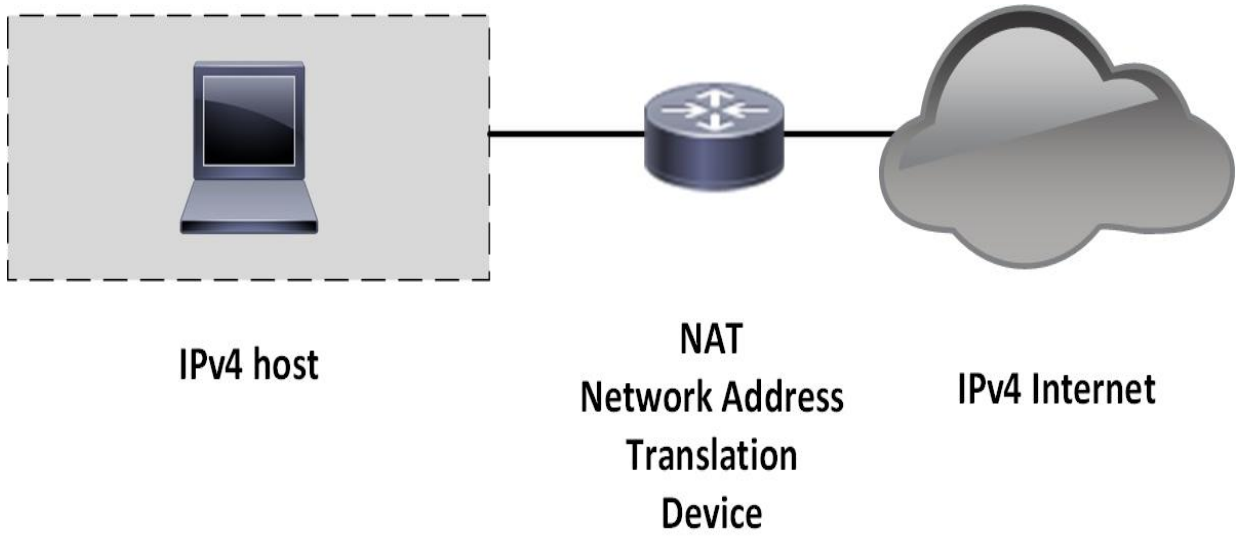
- For that reason several transition mechanisms developed

- Typical use case for NAT64 is IPv6 only Greenfield networks

https://t.me/learningnets

NAT44

- Regular NAT 44 is an operation to translate Private IPv4 address to a Public IPv4 address

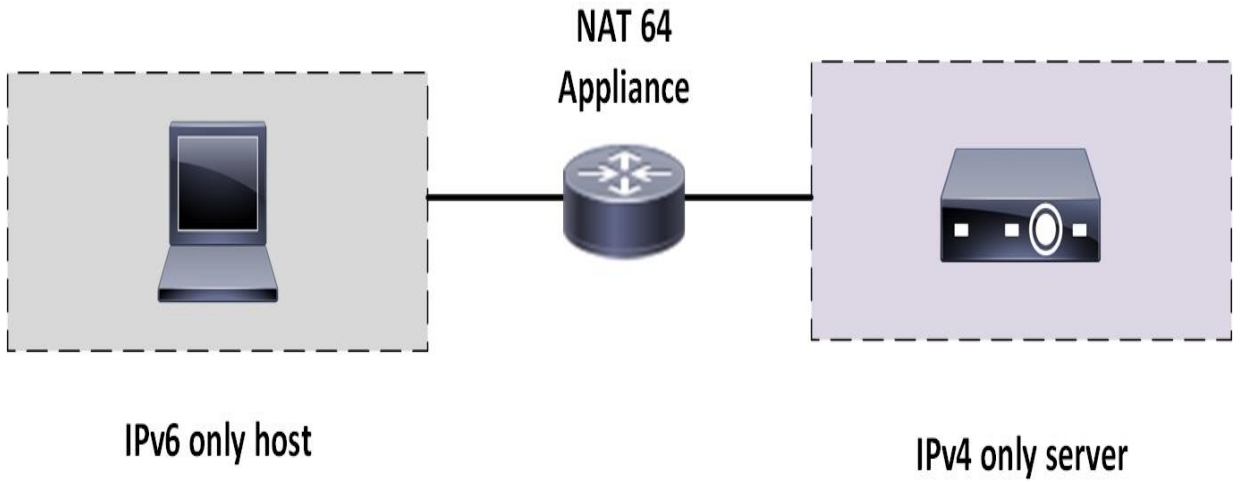


https://t.me/learningnets

NAT64

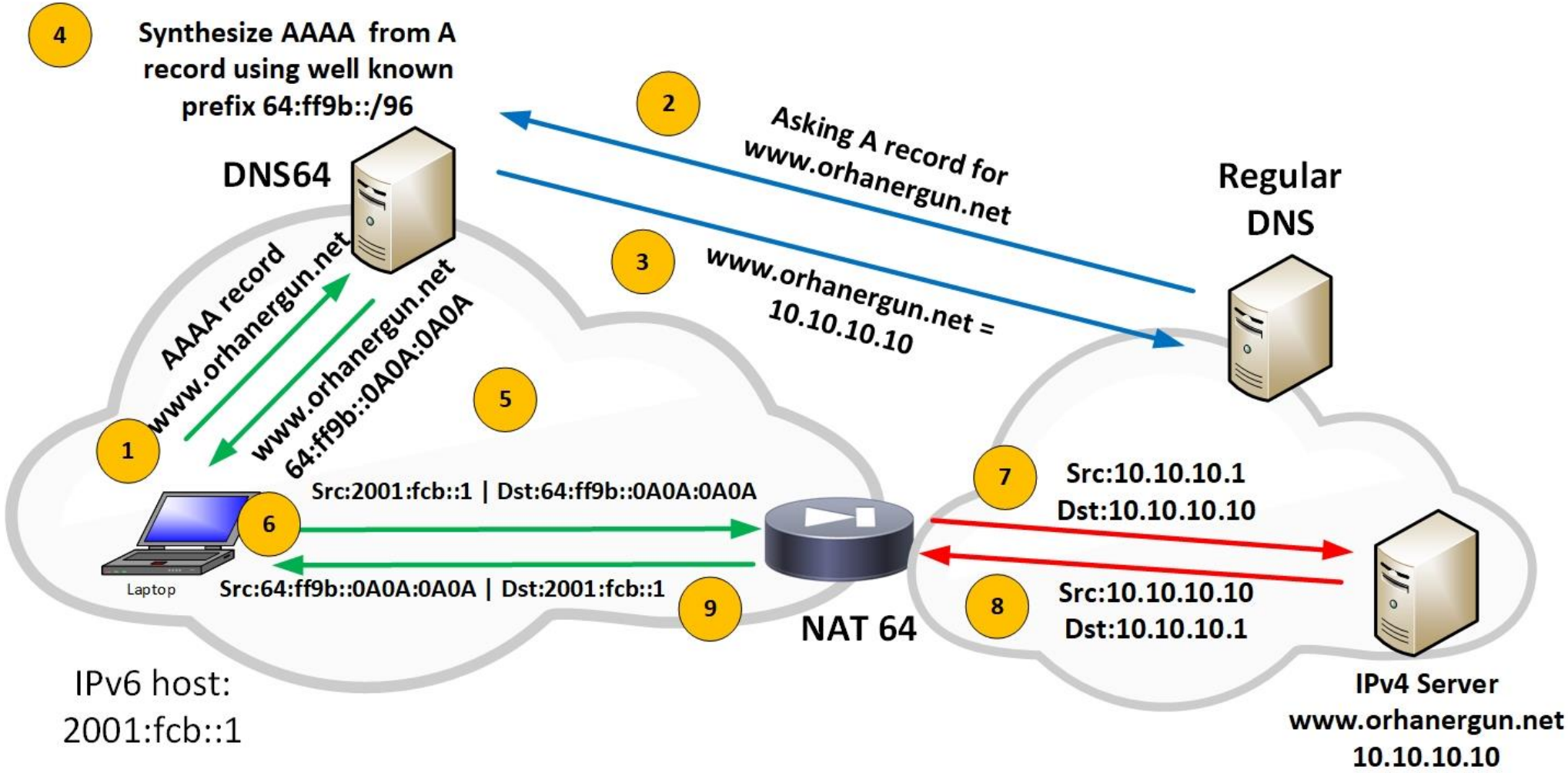
- In the case of NAT64, user doesn’t have an IPv4, It only has an IPv6 address

- NAT64 makes possible IPv6 only hosts to talk to IPv4 only server for example



https://t.me/learningnets

NAT64 – How it works



https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

CGN – Carrier Grade NAT

- CGN is commonly known as LSN (Large Scale NAT) in the operator community
- In CGN, IP addresses and the transport ports (TCP and UDP) are shared among the users
- CGN/LSN is commonly referred as NAT 444
- NAT444 , having two layer of NAT, first at he customer side, second layer of NAT in the SP network

https://t.me/learningnets

CGN – Carrier Grade NAT

- CGN moves Public IPv4 address pool from the customer edge to more centralized location

- It is Address + Port Translation solution (NAPT)

- Can be accomplished in multiple ways

1. NAT 444
2. NAT 464
3. DS-Lite

https://t.me/learningnets

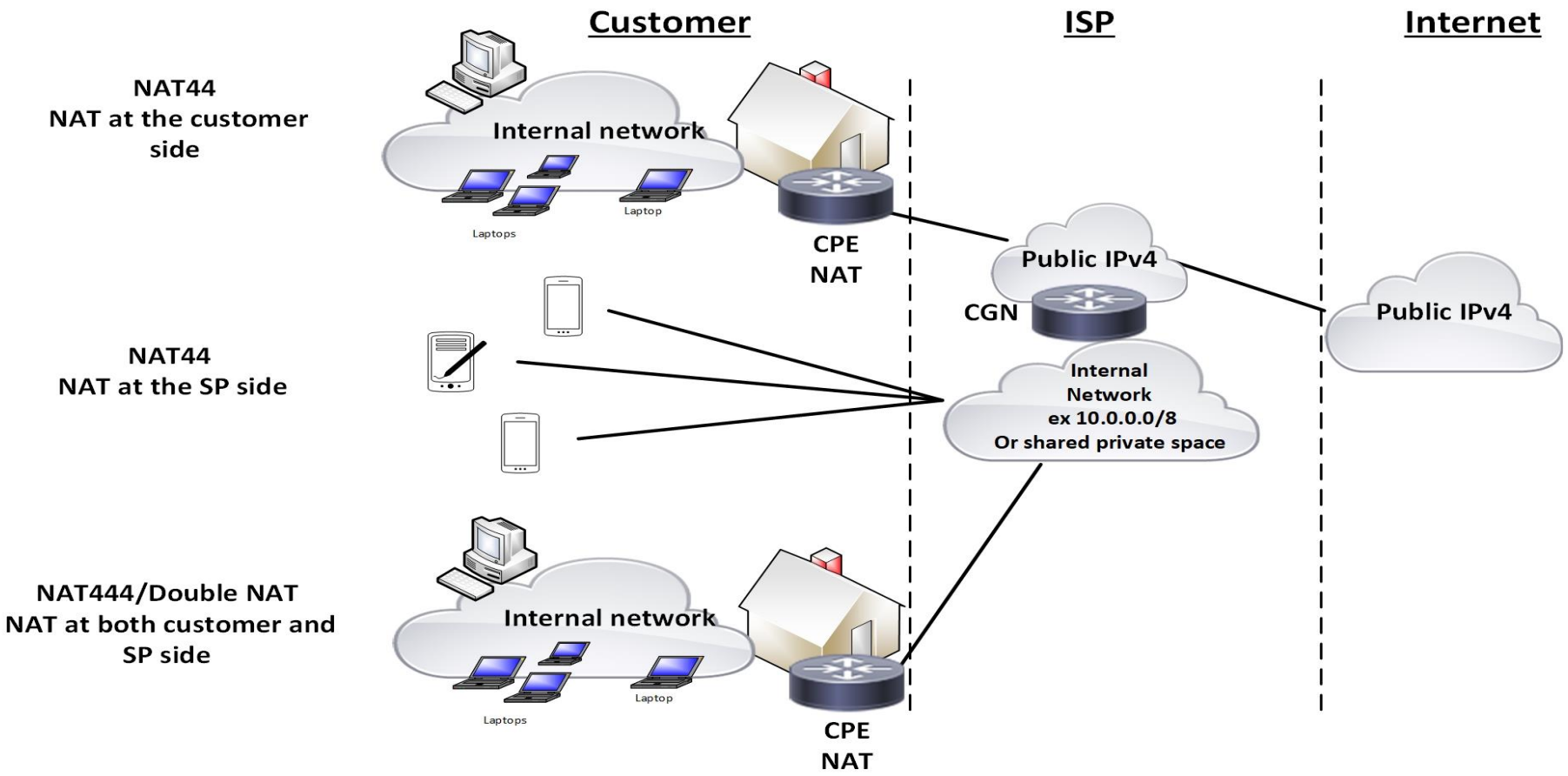
CGN – Carrier Grade NAT

- Difference between Customer NAT (Residential NAT) and SP NAT (CGN, LSN) is, with Residential NAT, single public IPv4 address represent one household, with SP NAT (CGN,LSN), single public IPv4 address is shared across multiple households

- With Residential NAT, 16 bit port space(65000 TCP and UDP ports) is for single household but with SP NAT, 16 bit port space of the IP address is shared among multiple households

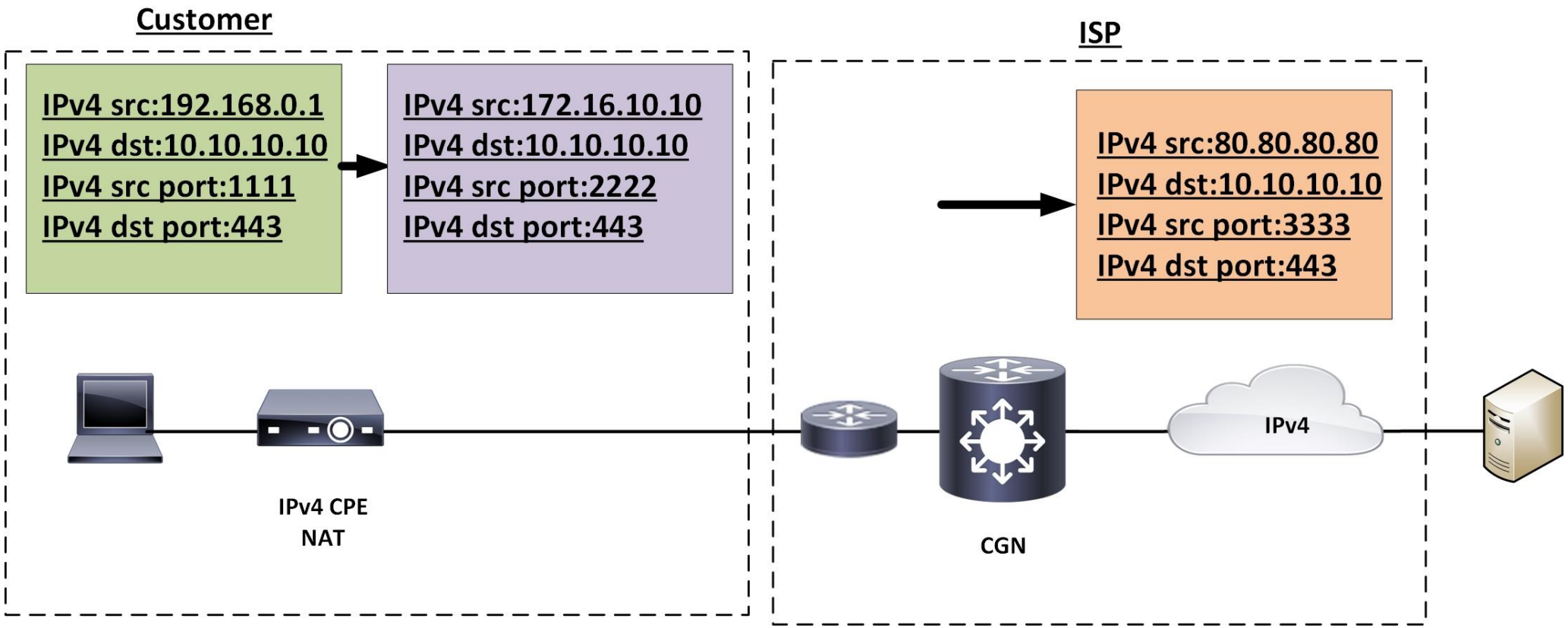
https://t.me/learningnets

How NAT (Network Address Translation) Wor*ks*



https://t.me/learningnets

CGN – How CGN Work



https://t.me/learningnets

CGN – Carrier Grade NAT, LSN – Large Scale NAT Deployment Options

- CGN can be deployed either as Inline or Offline
- Inline CGN deployment is more common in Enterprise and Residential networks as network traffic pass through the NAT box
- Offline CGN removes the NAT from the primary data path and utilizes source routing mechanisms to send the traffic to the NAT boxes
- Offline CGN is more common deployment model in the SP networks

https://t.me/learningnets

CGN Advantages

- It is well known NAT , two times NAT operation , customer and SP side, no IPv6 learning curve
- CPE – Customer NAT doesn’t need to change
- CPE doesn’t need to support IPv6

https://t.me/learningnets

CGN – Sharing Addresses Problems

- LCGN is an IP address sharing solution, many users share the same Public IP address, there are problems with it

  - Some applications break , applications which can work with single Layer of NAT may not work with two layers of NAT

- Sharing addresses makes operations/troubleshooting harder

  How many ports should be assigned to each user? It is called Port Spray

  Many websites open 80-100 TCP connection (Newspapers), some apps open hundreds of sessions (Google Map etc.)

https://t.me/learningnets

CGN – Sharing Address Problems

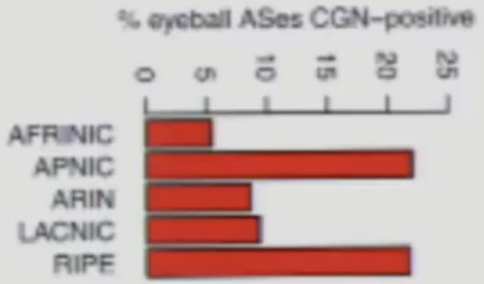
- Intense logging will be needed for the Lawful intercept
- Traceability of users behind CGN
- CGN in forwarding path (Inline deployment) becomes single point of failure
- Offline CGN deployment requires source routing which creates unnecessary complexity
- CGN IP address getting blacklisted due to address sharing (Not every user is innocent)

https://t.me/learningnets

CGN Current Deployment in SP networks

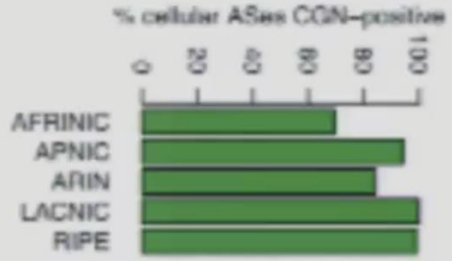
Eyeball Networks (Non-Cellular)

- CGN-positive: **17.1%**
  - particularly in the European and Asia-Pacific Region



Cellular Networks

- CGN-positive: **94%**
  - CGN is the norm for cellular



https://t.me/learningnets

464 XLAT

- T-Mobile is using 464 XLAT

https://t.me/learningnets

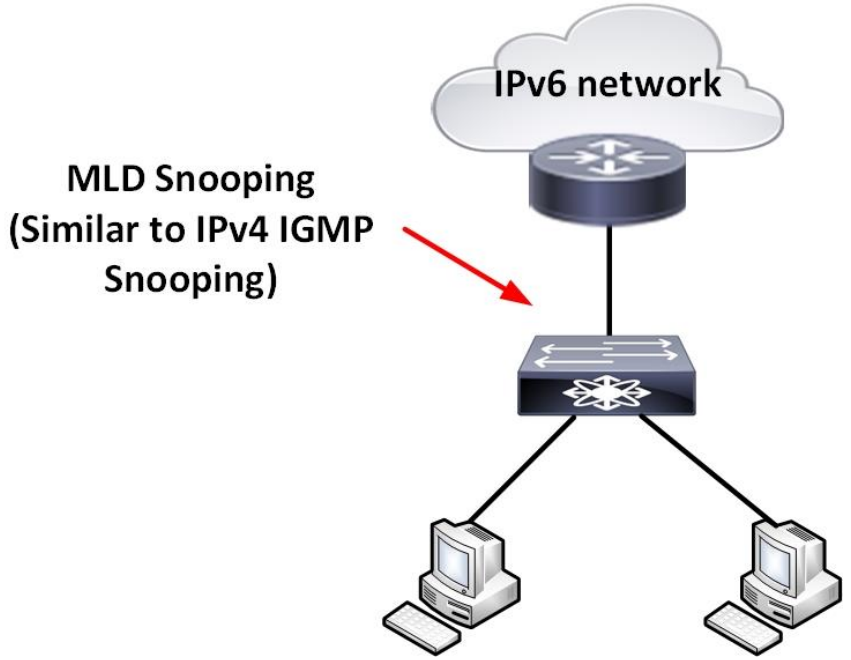
IPv6 Multicast

- Similar to IGMP – In IPv6 there is MLD
- MLD , Multicast Listener Discovery uses Link Local Source Addresses (Hop Count is 1)
- There are MLDv1 and MLDv2
- MLD v1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3

https://t.me/learningnets

IPv6 Multicast

- With MLDv1, host signal the interest to the (*,G) , With MLDv2, host can signal not only which multicast group but also individual source to group information to LHR -- (S,G)



https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

https://t.me/learningnets

IPv6 Discussions – Will IPv6 replace IPv4?

- Most of the mobile operators currently use LSN solutions

- Financially using IPv4 and NAT is more easier than deploying IPv6 as there is no new learning curve, new operations and potentially new hardware to support IPv6

https://t.me/learningnets

IPv6 Discussions – Does IPv6 have Better Security?

- IPv6 is not more secure than IPv4
- If encryption required, IPSEC is required for both cases
- With IPv6, address scanning/reconnaissance is harder due to longer addresses with IPv6

https://t.me/learningnets

IPv6 Discussions – IPv6 Space is infinite

- IPv6 addresses has two parts, network and host portion
- Host portion is 64 bits so for the network parts 64 bits remain
- RIRs are providing /32s usually but there are many ISPs which receive /29 and shorter prefixes such as /24s
- Some people already believe that in 10 to 15 years RIRs might have IPv6 address shortage

https://t.me/learningnets

IPv6 Discussions – Will IPv6 reduce NAT Deployment?

- IPv4 will be around for many years
- When IPv6 is deployed, IPv6 only sites cannot communicate with IPv4 only sites, translation (NAT) is required for those sites to communicate
- When there is no IPv4 anymore, and if networks don’t use ULA (Unique Local Address) then NAT can be removed

https://t.me/learningnets

IPv6 Discussions – Does IPv4 Running Out?

- RIRs don’t provide IPv4 anymore as it was mentioned before
- But companies purchase an IPv4 addresses from each other, so IPv4 public address can be purchased from the market (Problems with this were discussed earlier)
- As of 2019, IPv4 address is around $10 - $20 and all RIRs allow IPv4 address transfers
- Company in Saudi Arabia can purchase an IPv4 from U.S and register that IPv4 address to RIPE

https://t.me/learningnets

IPv6 Summary

- You don’t have to deploy IPv6 everywhere from day 1
- Assessment and planning is key for IPv6 design
- Stateful IPv6 translation mechanisms have many challenges such as asymmetric routing, logging issues, single point of failure and so on
- Dual stack still requires IPv4 address on the CPE ! It is against to IPv4 exhaustion issue

https://t.me/learningnets

- You can start core to edge (You have a time), Edge to core (rely on tunneling) or Internet edge (e-commerce)
- 6PE and 6VPE is best transition mechanisms for the MPLS networks
- Running IPv6 together with IPv4 doesn’t create a problem for IPv4 infrastructure but still memory and CPU of the devices need to be tracked.

https://t.me/learningnets