IPv6

Internet Protocol Version 6

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

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
  3. ISATAP
  4. TEREDO
  5. DS-Lite – Dual Stack Lite

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

IPv6 Course Outline

- IPv6 in Internet of Things (IOT)
  - Requirements for IPv6 in IOT Networks
  - 6LOWPAN – IPv6 over Low Power Wireless Personal Area Networks
  - RPL – Routing over Low Power and Lossy Networks

- Segment Routing (SRv6) – SR IPv6 Dataplane
  - SR-MPLS vs SRv6
  - SRv6 Header
  - Locator and Functions
  - SRv6 Basic Functions
  - TI-LFA , MPLS L3VPN examples with SRv6

- IPv6 Discussions:
  - Will IPv6 replace IPv4?
  - Does IPv6 have Better Security?
  - Will IPv6 reduce NAT Deployment?

IPv6 Business Drivers

IPv6 Business Drivers

- **IPv4 address exhaustion**
- **Business Continuity (E-Commerce, Content Providers, Content Delivery Networks)**
- **Easier Network Mergers and Acquisitions (No overlap, NAT etc.)**

IPv6 Addressing

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

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

IPv6 Addressing

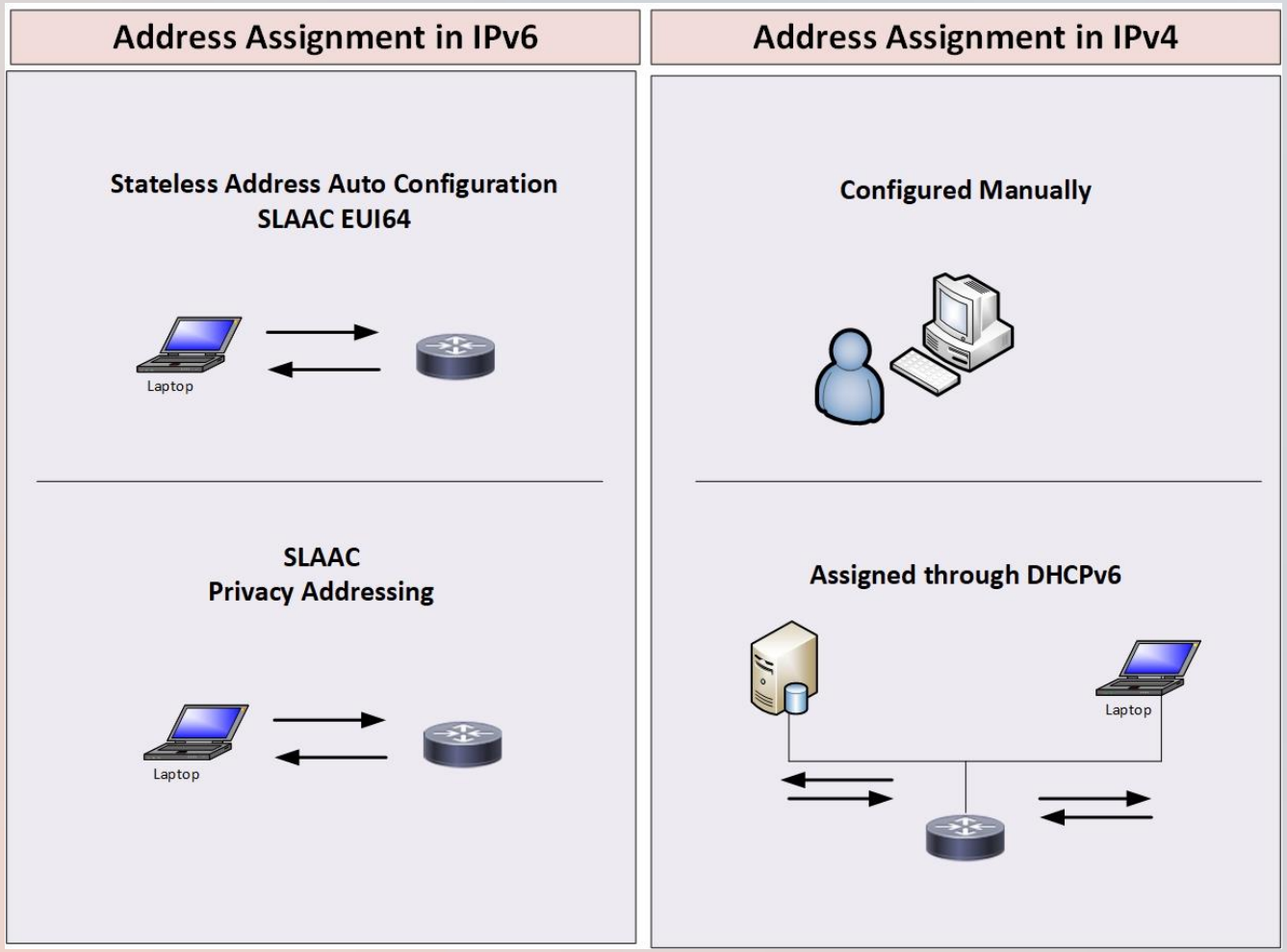
- 128 bit address has two portion. Network and Host
- Network (Sometimes called as Topology portion) is 64 bits
- Host Portion is 64 bits as well

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

Network Portion Host Portion

IPv6 Address Assignment to the Hosts

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



IPv6 Address Assignment to the Hosts

- Although there are two methods in IPv4 for obtaining an IP address, IPv6 has three methods
- Static configuration is basically the same in both protocols, although less relevant for IPv6, because of the length of the address
- DHCP is also there for both protocols, and IPv6 DHCPv6 is described in RFC 3315

IPv6 Address Assignment – SLAAC

- The new method that IPv6 introduces is called Stateless Address Autoconfiguration(SLAAC), and described in RFC 4862
- SLAAC works by combining part of the address from an interface's gateway, learned via Router Advertisements(RAs), and an interface's layer 2 address with "ff:fe" adding in the middle of it
- So, router announces it's own prefixes, host take prefix part and interface ID part is generated by using MAC address of the host (Different with Privacy Extensions, it will be explained)

IPv6 Address Assignment – SLAAC

- In practice, this generally means that using SLAAC an interface's address will be composed of; the first 64 bits of its gateway's address, plus the higher 24 bits of its Ethernet MAC, plus 16 hardcoded bits of "ff:fe", plus the lower 24 bits of its MAC address. IPv6 addresses are 128 bits, and 64 + 24 + 16 + 24 = 128

IPv6 Address Assignment – SLAAC

- As an example, let's say an interface's gateway had the address 2001:db8::1, and the interface's MAC address was 01:23:45:67:89:ab

This would result in an IPv6 address of 2001:db8::123:45ff:fe67:89ab

- It's easier to understand if you write it out in long form :

2001:db80:0000:0000:0000:0000:0000:0001 Gateway 0123:4567:89ab MAC
0123:45ff:fe67:89ab MAC after padding
2001:db80:0000:0000:0123:45ff:fe67:89ab Final IP address

IPv6 Address Assignment – SLAAC Privacy Extension

- If your operator is using SLAAC then you can be tracked using the last 48 bits of your IPv6 address because it's unique

- Websites that you visit can see that you have a new IP address, because you have roamed to a new operator, they can also see that the last 48 bits of the address stay the same every time. Hence, every website you visit will know your device regardless of what network you're on. You can be easily tracked across providers

IPv6 Address Assignment – SLAAC Privacy Extension

- This problem was resolved by issuing an update to the SLAAC protocol called “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, which is defined in RFC 4941

- Basically, your computer’s Ethernet interface no longer uses its MAC to fill in the last 48 of its IPv6 address. Instead it picks a series of bits randomly, and fills in the last 48 bits with the random bits.

IPv6 Address Assignment – SLAAC Privacy Extension

- But sometimes tracking might be required internally in the inside network , for example for troubleshooting or logging purposes

- Thus the recommendation for the Privacy extension is, use it for the external communication but not for internal network

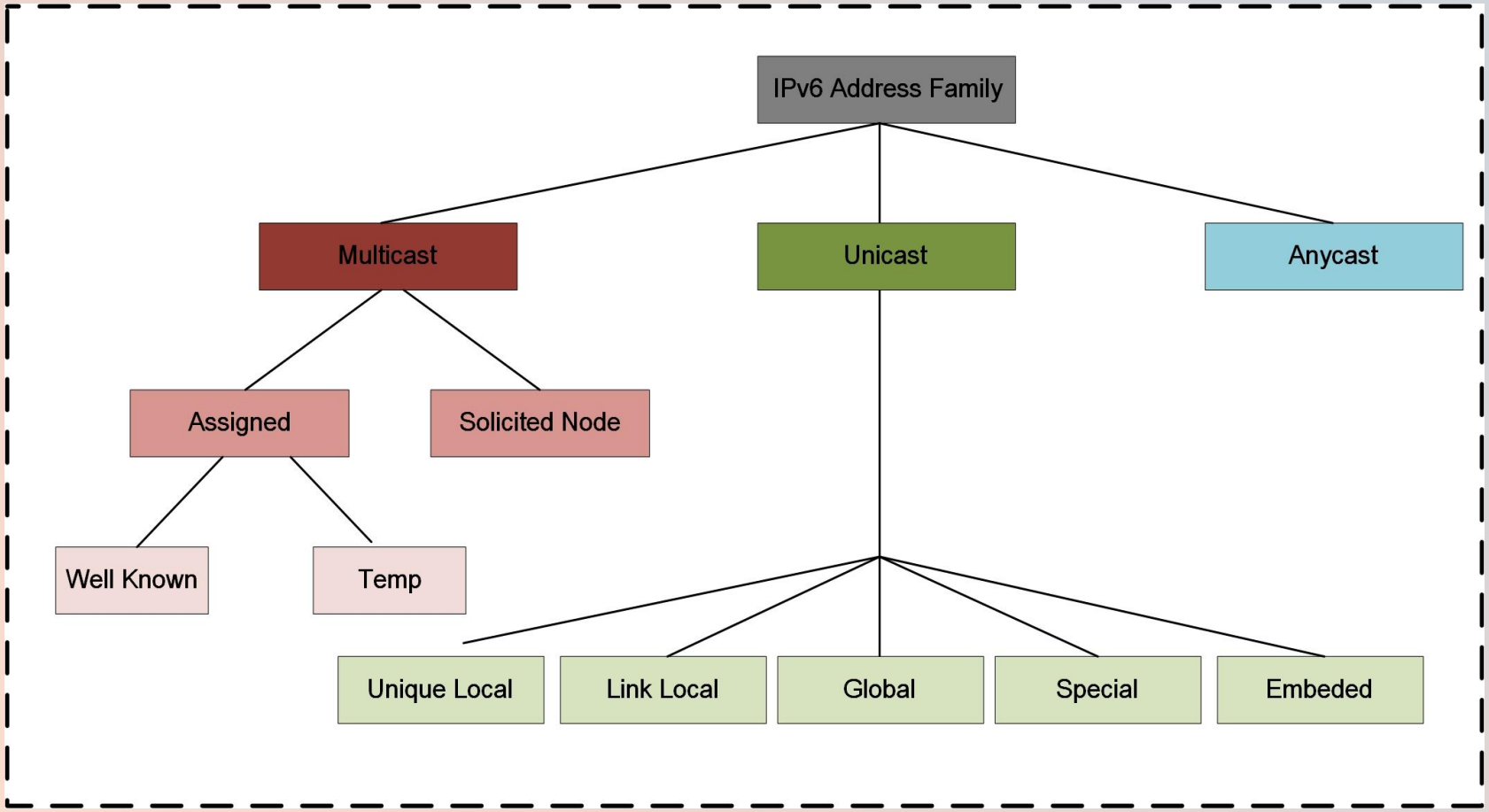
IPv6 Address Assignment – When to use DHCPv6?

- SLAAC can be used in production environment, but many organizations don’t like unpredictability, particularly with Privacy Extension
- DHCPv6 can be used when there is a requirement for predictability
- In fact, different place in the network have different requirement, SLAAC can be used for the customer address assignment in the SP but same organization generally use Static address assignment or DHCPv6 for servers in their Datacenter

IPv6 Address Assignment – When to use DHCPv6?

- If DHCPv6 will be used, network needs to stop announcing SLAAC prefixes and M bit needs to be set in the Router Advertisement messages (RA)

IPv6 Addressing



There is no Broadcast Addressing in IPv6

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)

Unicast IPv6 Address Types

- Three types of Unicast IPv6 Address Types:

1. Link-Local – Non-routable , exists on single layer 2 domain

fe80::/10

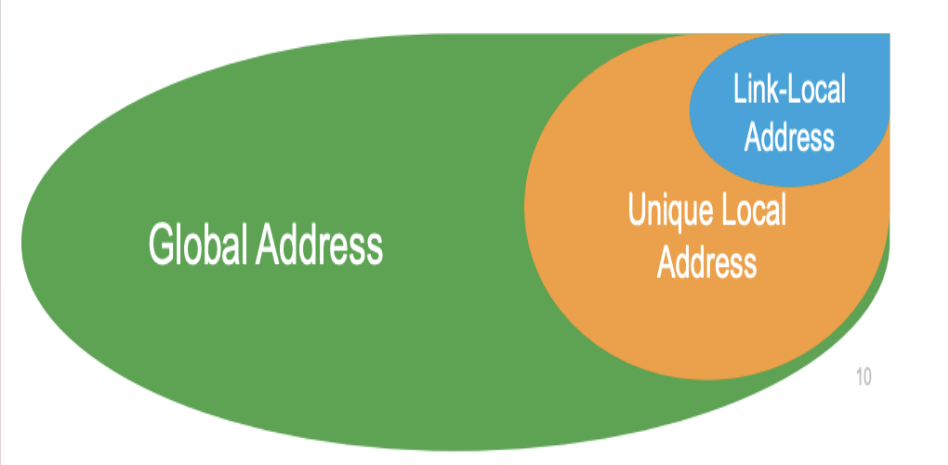
2. Unique-Local : Routable within AS

fc00::/7

3. Global Unicast Address – Routable across Inter domain

2000::/3

(Range is between 2000 – 3fff – First 2 byte)



Unicast IPv6 Address Types

- 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

IPv6 Address Recommendations

- First 64 bits are fixed of the Link Local Address. Interface identifier/Host Portion can be modified, Vlan number, IPv4 addresses can be encoded into IPv6 Link Local Address for easier troubleshooting

- IGP routing can run by just using Link Local Address, but in this case management of those interfaces cannot be possible since Link Local Address is not routable

IPv6 Address Recommendations

- 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)

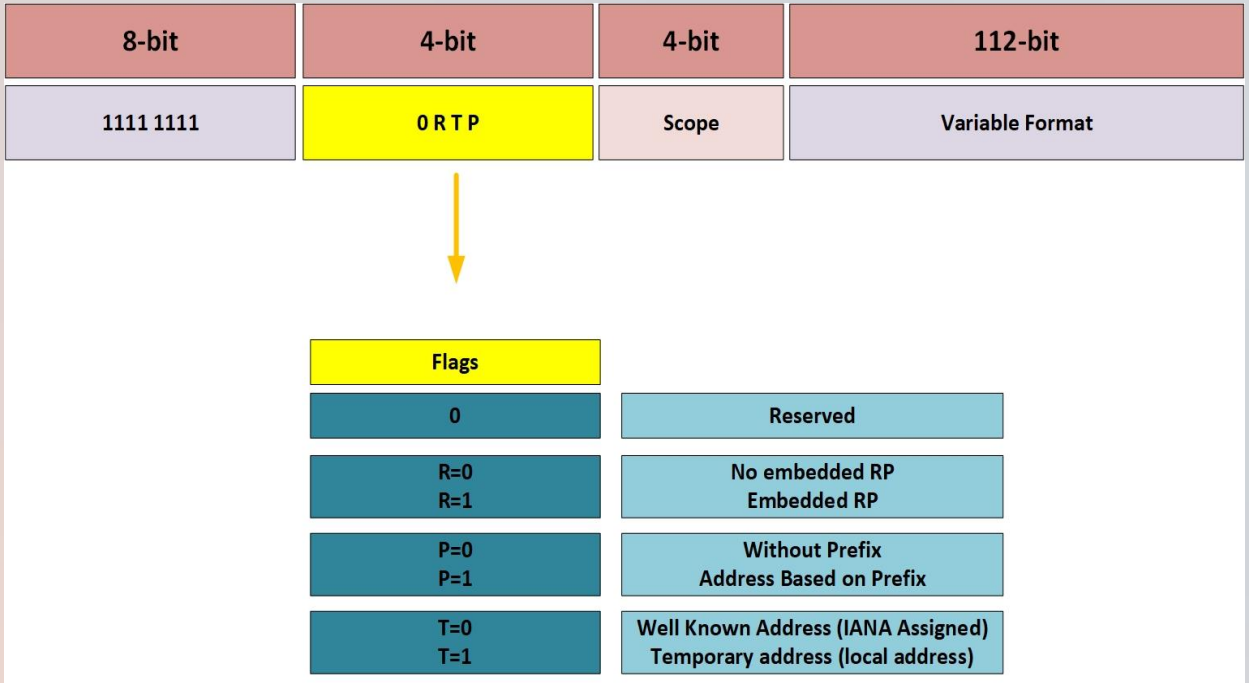
IPv6 Address Recommendations

- General recommendation to assign IP address for internal network is Global Unicast Address
- There are vast number of prefixes in Global Unicast Address space
- No need to manage NAT etc, just one address space for internal and external purposes

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



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

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 multicast address of the unicast address being checked for duplicates

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 multicast address which is generated from the remote router's unicast address

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

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

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

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

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

IPv6 Address Planning

IPv6 Address Plan

- We need to analyze the entire network, we need to know each Place In the Network where IPv6 will be deployed
- How many locations , countries, regions , cities , buildings etc.
- Which services, applications and the systems will be connected in each location
- For SP and Enterprises services and the number of locations are different (Fixed networks, mobile networks, datacenters , POP locations , branch offices, campus locations etc.)

IPv6 Address Plan

- IPv6 addresses can be received from Upstream ISP or one of the 5 different RIRs (LACNIC, AFRINIC, APNIC, ARIN , RIPE)

IPv6 Address Plan

- Some networks get IPv6 address from one of the 5 RIRs and use it in different regions, some networks get address from each RIR in each region, second approach is usually seen as better for traffic engineering but dealing with different RIRs can create more operational challenge

IPv6 Address Plan – Getting IPv6 space from RIR

- You can become a member of RIR and get your own allocation – Membership is available to all organizations who are operating a network
- RIRs list their address allocation policies on their website
- Minimum allocation is a /32 for Service Providers, if you need more than that you need to prove that you will more than 65k /48 assignments

IPv6 Address Plan – Getting IPv6 space from Upstream ISP

- Enterprises usually receive IPv6 address space from their Upstream ISPs
- They receive /48 from upstream
- If they will multihome , then better to receive from their IPv6 address space from RIR directly

IPv6 Address Plan – PI vs PA Discussion

- PI (Provider Independent) or PA (Provider Assigned/Aggregatable)?
- PI space is better for organizations who want to multihome to different SPs
- PA is okay if you are single homed or plan to do NAT for IPv6 in the network which is not recommended

IPv6 Address Plan – PI vs PA Discussion

- If Enterprise will terminate their business with one of their multihomed upstream ISPs, PA is challenging as Enterprise need to give their IPv6 address space back and re-address their network , thus many organizations are going down the PI path

IPv6 Address Plan Fundamentals

- In general we don’t worry about the number of hosts in IPv6 address planning , we have 2 to 64 IPv6 addresses for hosts
- Enterprises usually get /48 as a prefix length or multiple /48 based on their scalability requirements
- Service Providers should get /32 as minimum or multiple of them based on their scale

IPv6 Address Plan Fundamentals

- We need to have a methodology for writing an IPv6 Addressing Plan
- In General there are 5 rules to write an efficient, stable , scalable and secure IPv6 address plan
- Simplicity , Embedding Information , Reserving some addresses, Summarization and Involvement of other teams

IPv6 Address Plan – Simplicity

- IPv6 address plan should be simple, we don’t want to explain our addressing schema days or weeks

- Templates should be used as much as possible

IPv6 Address Plan – Simplicity

- Use nibble boundary, A nibble boundary means : subnetting address space based on the address numbering, each number in IPv6 represents 4 bits = 1 nibble , which means that IPv6 addressing can be done on 4-bit boundaries

IPv6 Address Plan – Simplicity

- Nibble boundary example:

- 2001:cafe:0:10::/61 is :

2001:cafe:0000:0010:0000:0000:0000:0000 to
2001:cafe:0000:0017:ffff:ffff:ffff:ffff

With /61, the address blocks don’t use the entire nibble range , BUT,

IPv6 Address Plan – Simplicity

- Nibble boundary example:

- 2001:cafe:0:10::/60 is :

2001:cafe:0000:0010:0000:0000:0000:0000 to 2001:cafe:0000:001F:ffff:ffff:ffff:ffff

With /60, this subnet uses the entire nibble range (0 to F)

This makes the numbering plan for IPv6 simpler, for example Service Provider can have a particular meaning for their particular POP infrastructure addressing

IPv6 Address Plan – Encoding some information

- Encoding/Embedding some information helps for operation people as well as help for easier troubleshooting

- Location information , country , city , Vlan number can be encoded in Link Local and Global Addresses

IPv6 Address Plan – Reserving some IP Space

- Designing networks for future growth is essential , same is true for IPv6 address plan
- New locations can be added, company can grow organic or inorganically, thus for better summarization , reserving some IP address in advance is clever decision
- You can reserve /64 but assign /126 or /127 for P2P addresses for example

IPv6 Address Plan – Summarizable

- Summarization reduces routing table size
- It reduces number of information to deal with
- It reduces convergence time in case of failure
- It reduces troubleshooting time thus increases high availability of the network
- Thus summarizable addresses will help for better network design

IPv6 Address Plan – Involvement of Other teams

- For example application and the security teams need to be involved in IPv6 deployment and Address planning

- Based on the IPv6 addresses assigned for each location, security team need to deploy accurate security policies

IPv6 Address Plan – Different PIN Addressing Suggestions

- Different Place in the Network requires special addressing requirements

- P2P links , Loopback addresses , Host/End User Addresses , Buildings , Campus Locations , Services (Broadband, Internet) etc.

IPv6 Address Plan – Different PIN Addressing Suggestions –ISP Network

- ISPs and Enterprise Networks have different requirements as the services, number of sites etc. are different, let's look at ISP Address Plan suggestions based on their PINs and the services

- All ISPs should get minimum /32 from their RIR (Larger ones and more serious ones get /29)

- Loopback Address: Numbering all loopbacks out of one /64 block and assign /128 per loopback

IPv6 Address Plan – Different PIN Addressing Suggestions –ISP Network

Infrastructure Addressing:

- /48 per region, /48 allows 65k subnets
- /48 for the whole backbone

- General recommendation for the Infrastructure addressing is, summarize between the sites

IPv6 Address Plan – Different PIN Addressing Suggestions –ISP Network

- LAN subnets : /64 per LAN
- P2P links should be assigned either /64 or /127 (RFC 6164)
- You can see Link local addresses are recommended for the P2P infrastructure link by some documents , it is good for having less address (No Global IPv6 address required in this case) but link local address are not routable so NOC cannot reach to these addresses

IPv6 Address Plan – Different PIN Addressing Suggestions –ISP Network

- NOC – Network Operation Center is considered as part of the network infrastructure, usually /60 within the infrastructure /48 block is seen as enough

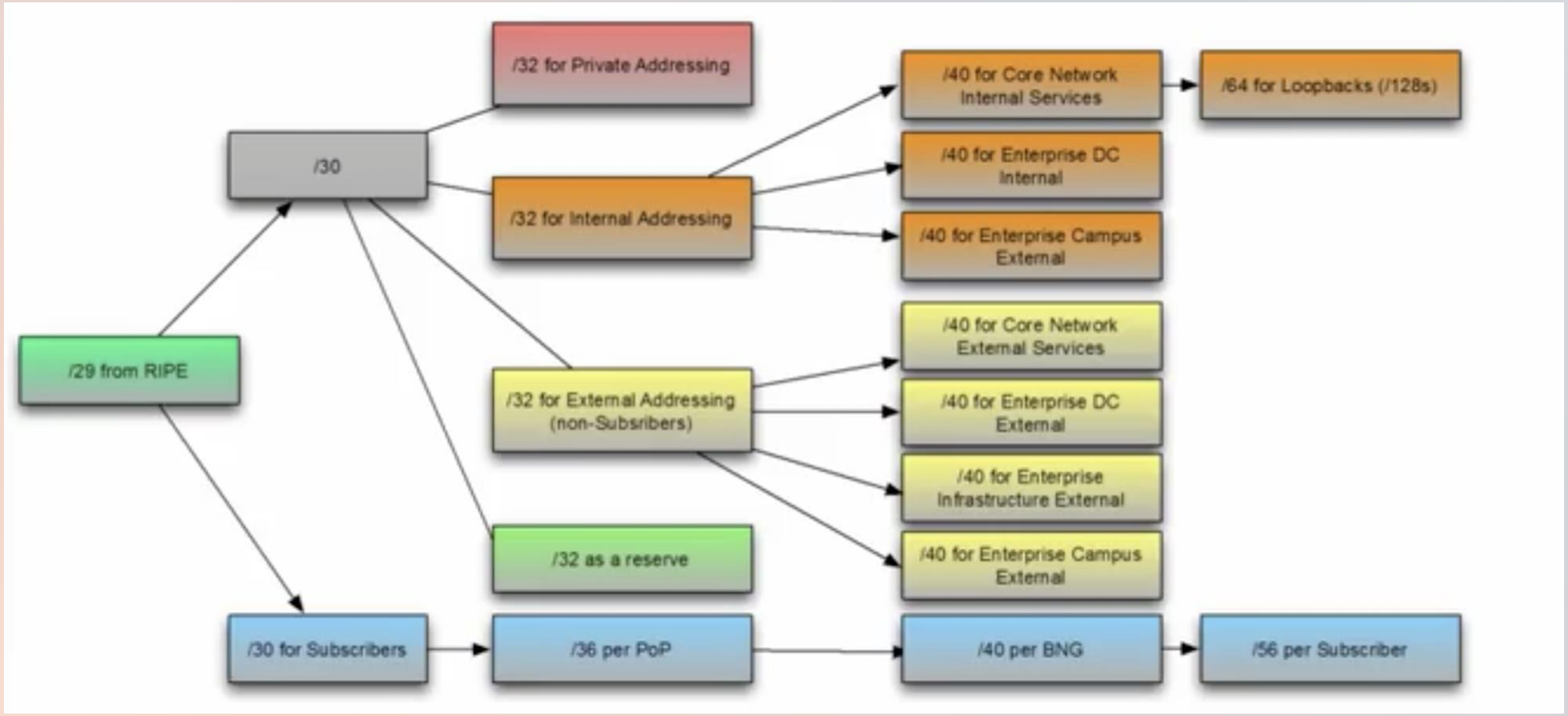
- Shared/Critical services such as DNS , SMTP , POP3/IMAP etc. also considered as part of the infrastructure and one /64 is enough for these addresses

IPv6 Address Plan – Different PIN Addressing Suggestions –ISP Network

- ISP to Customer Link : /48 should be allocated for this, between the POPs /48 should be divided

- And customer should get one /48 for large scale networks, /56 for small scale and if it is LAN , then /64

ISP IPv4 Address Assignment Example



IPv6 Transition Mechanisms

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

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

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

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

- 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.

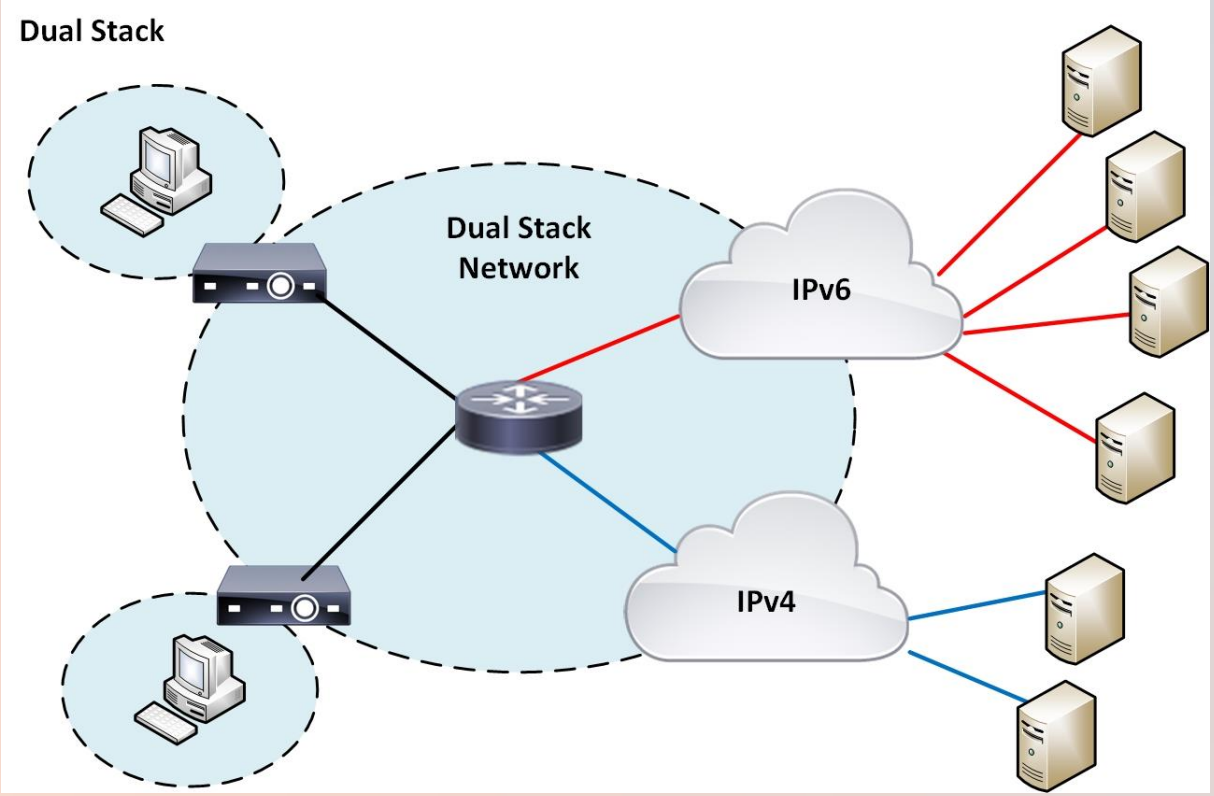
IPv6 Transition Mechanisms – Dual-Stack

- 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

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

IPv6 Transition Mechanisms – Dual-Stack



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

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

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

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 (Very bad user experience thus users usually turn off IPv6)

Happy Eyeballs

- 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

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!

Happy Eyeballs

Device	DNS query sending style	IPv6 broken, time until fallback to IPv4			Comments
	Dual-stack destination	Black hole	No route	Address unreachable	
Symbian^3 on Nokia N8 (11.012)	**A** first and used if possible. **AAAA** if no IPv4.	N/A	N/A	N/A	Symbian^3 prefers IPv4 hence tested fallback scenarios are N/A. The DNS query order is a configuration parameter.
Windows 7 Starter Edition on HP *IE 8.0.7600 & Google Chrome 8.0.552.224 & Safari 5.0.2*	**A** and after reply **AAAA**. Uses IPv6 if both available.	**~21s**	**~21s** (after 3 SYN & ICMPv6 errors)	**~21s** (after 3 SYN & ICMPv6 errors)	Same initial delay with those browsers. **The 21 seconds is TCP timeout after 3rd SYN failed.**
iOS4 4.2.1 on Apple iPhone4 *Safari*	**A** first and **AAAA** immediately after. Uses IPv6 if both available.	**No fallback**	**~4s** (After 5 SYN & ICMPv6)	**~4s** (After 5 SYN & ICMPv6)	Lucky observation: waits ~350 ms for AAAA to arrive after A is received before going for IPv4
Apple OS/X 10.6.6 on iMac *Safari 5.0.3* *Firefox 3.6.13*	**A** first and **AAAA** immediately after. Uses IPv6 if both available.	**~75s**	**~4s** (After 5 SYN & ICMPv6)	**~4s** (After 5 SYN & ICMPv6) **Firefox:** no fallback at all!	Special note that Firefox did not fallback on address unreachable error.
Android 2.3.1 on Samsung Nexus S *Native browser*	**AAAA** and after reply **A**. Uses IPv6 if both available.	**~21s**	**~0s** (acts on first ICMPv6)	**~0s** (acts on first ICMPv6)	**The 21 seconds is TCP timeout after 3rd SYN failed.**
Maemo5 IPv6 enabled version on Nokia N900 *Firefox & native*	**AAAA** and after reply **A**. Uses IPv6 if both available.	**~189s**	**~0s** (acts on first ICMPv6)	**~0s** (acts on first ICMPv6)	189s is after 6th SYN failed. Kernel: 2.6.28-based
Ubuntu 10.04 /10.10 on "PC" *Firefox 3.6.13*	**AAAA** and after reply **A**. Uses IPv6 if both available.	**~21s**	**~0s** (acts on first ICMPv6)	**~0s** (acts on first ICMPv6)	Note: immediate fallback to IPv4 happens also during complex page load (i.e. minimizes damage when IPv6 is always preferred) Kernel (10.04): 2.6.32-27, (10.10): 2.6.35-24

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

Happy Eyeballs v1 vs. v2

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

Dual-Stack Requirements

- CPEs should support both IPv4 and IPv6
- Dual Stack also requires hardware and infrastructure which support IPv6

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)

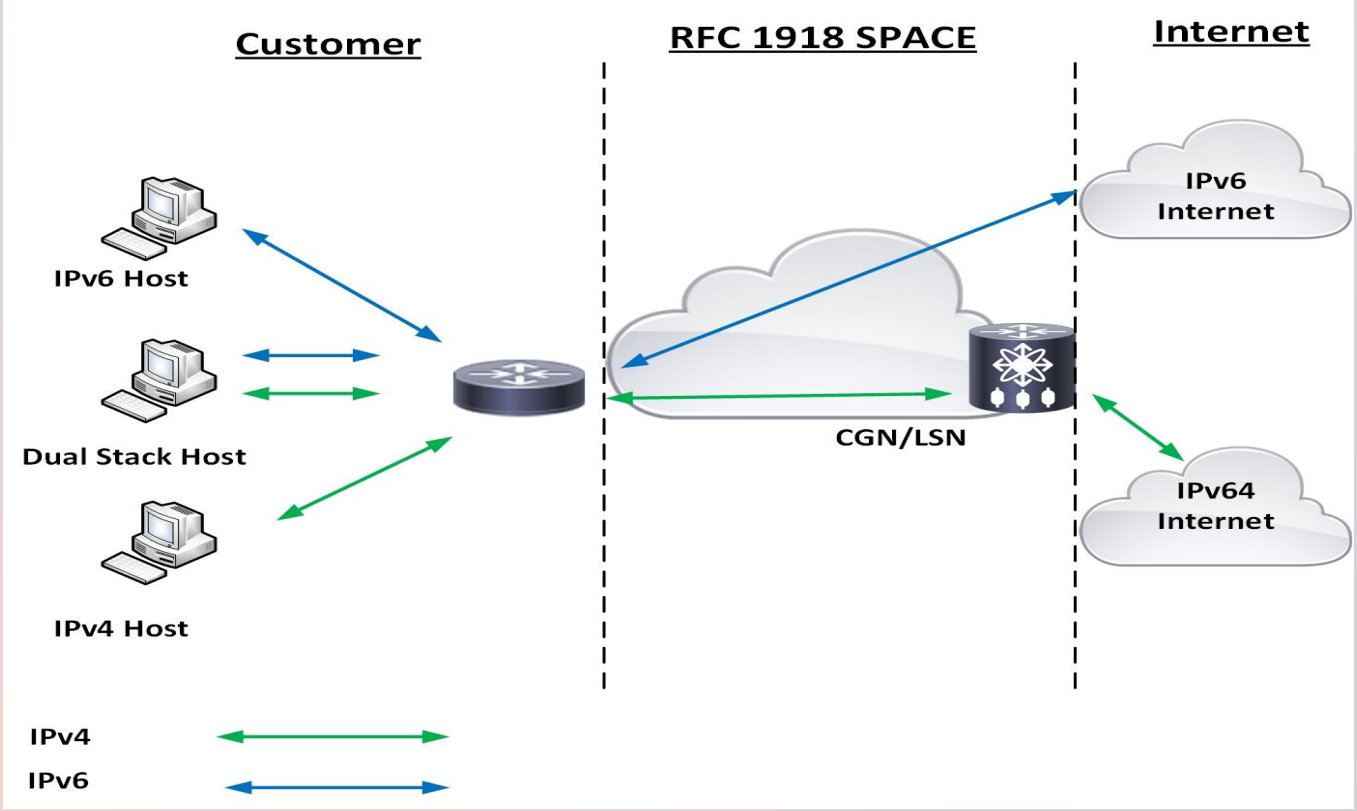
Solution to IPv4 depletion with Dual Stack

- 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

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

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

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

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

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

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.

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

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

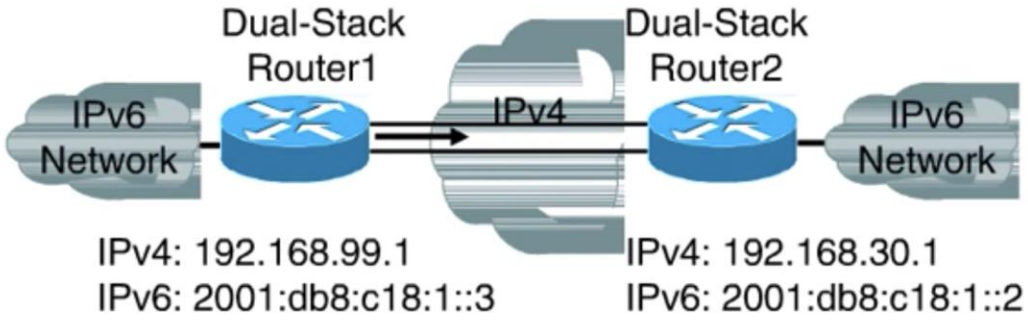
Manuel/Configured IPv6 Tunnels

- 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

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
```

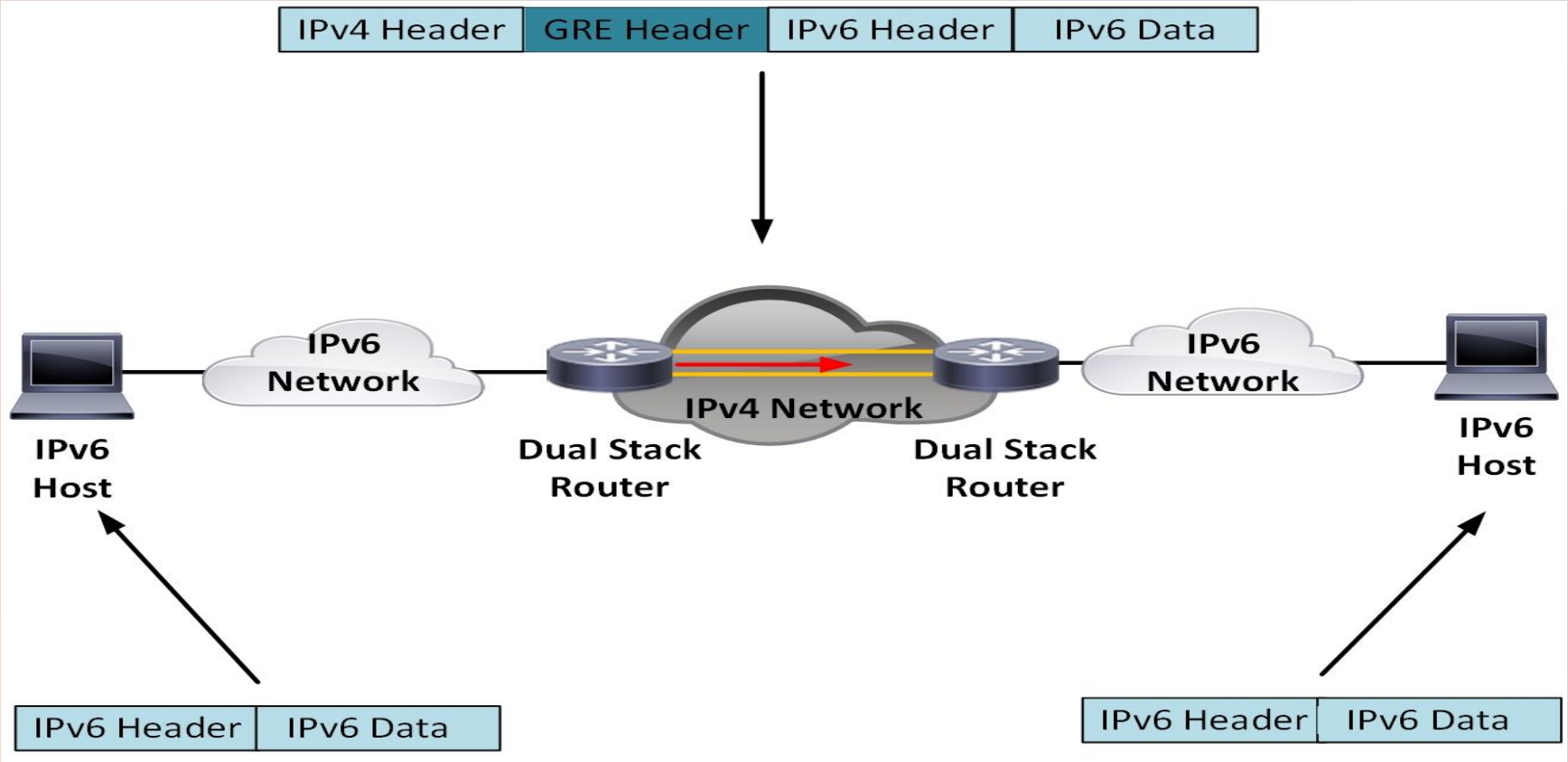
- Manually Configured tunnels require:
  - Dual stack end points
  - Both IPv4 and IPv6 addresses configured at each end

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

Manuel IPv6 Tunnels – GRE Tunnel



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

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

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)

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

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

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

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

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)

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

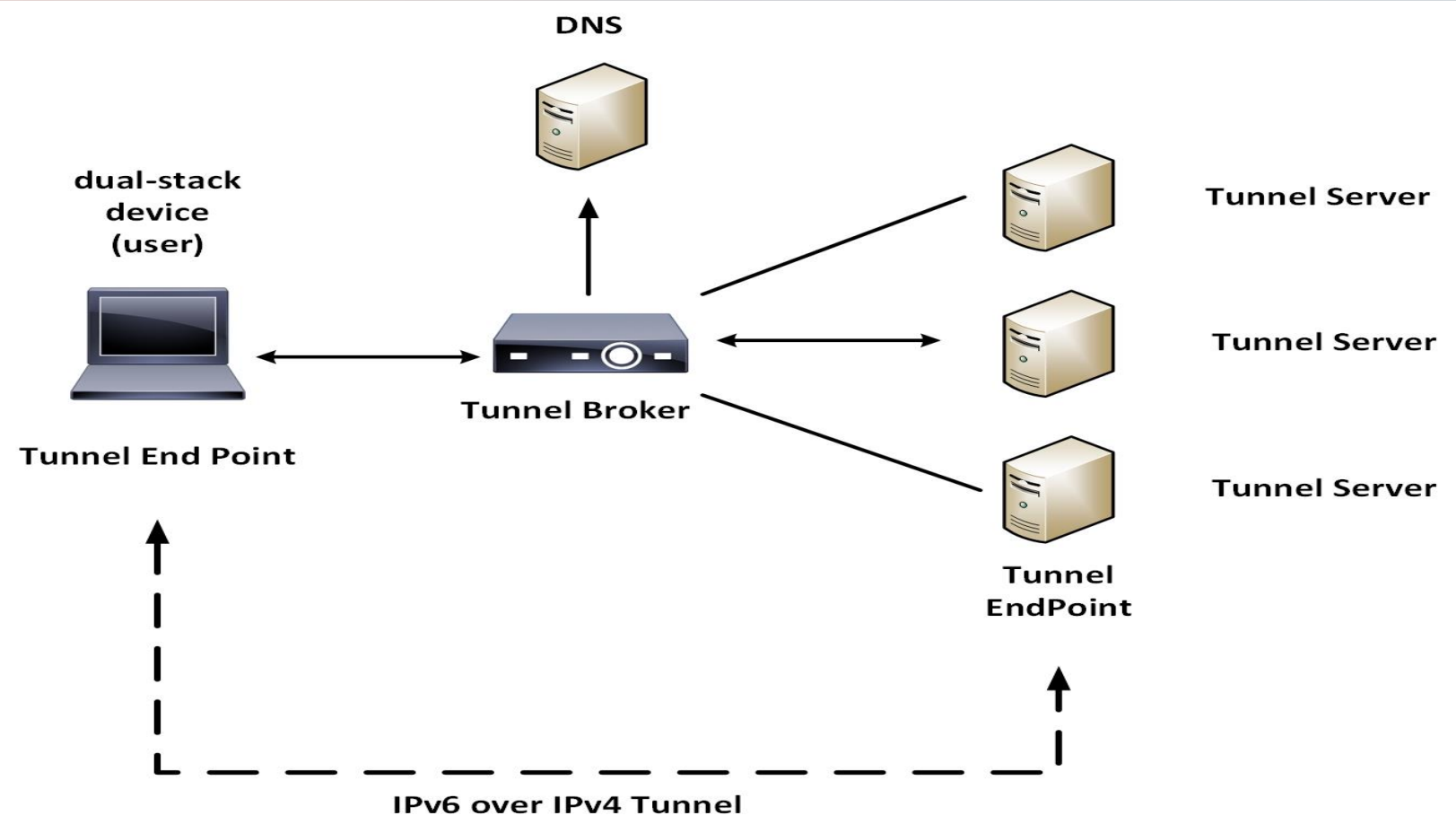
- It configures the server side of the tunnel

How Tunnel Broker Mechanisms Works

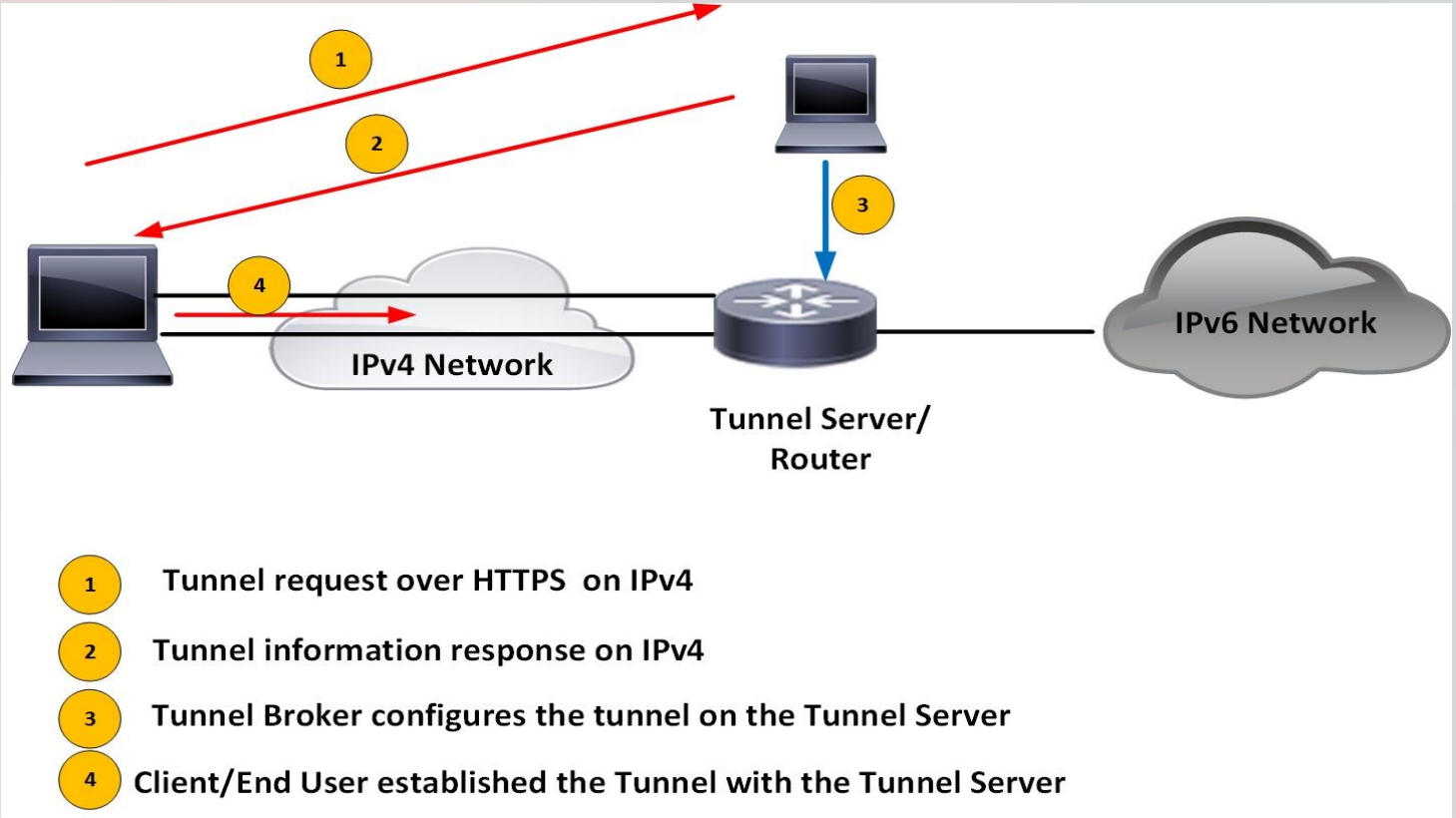
- It notifies the relevant configuration information to the client, including tunnel parameters and DNS names

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

How Tunnel Broker Works



How Tunnel Broker Works



Tunnel Broker

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

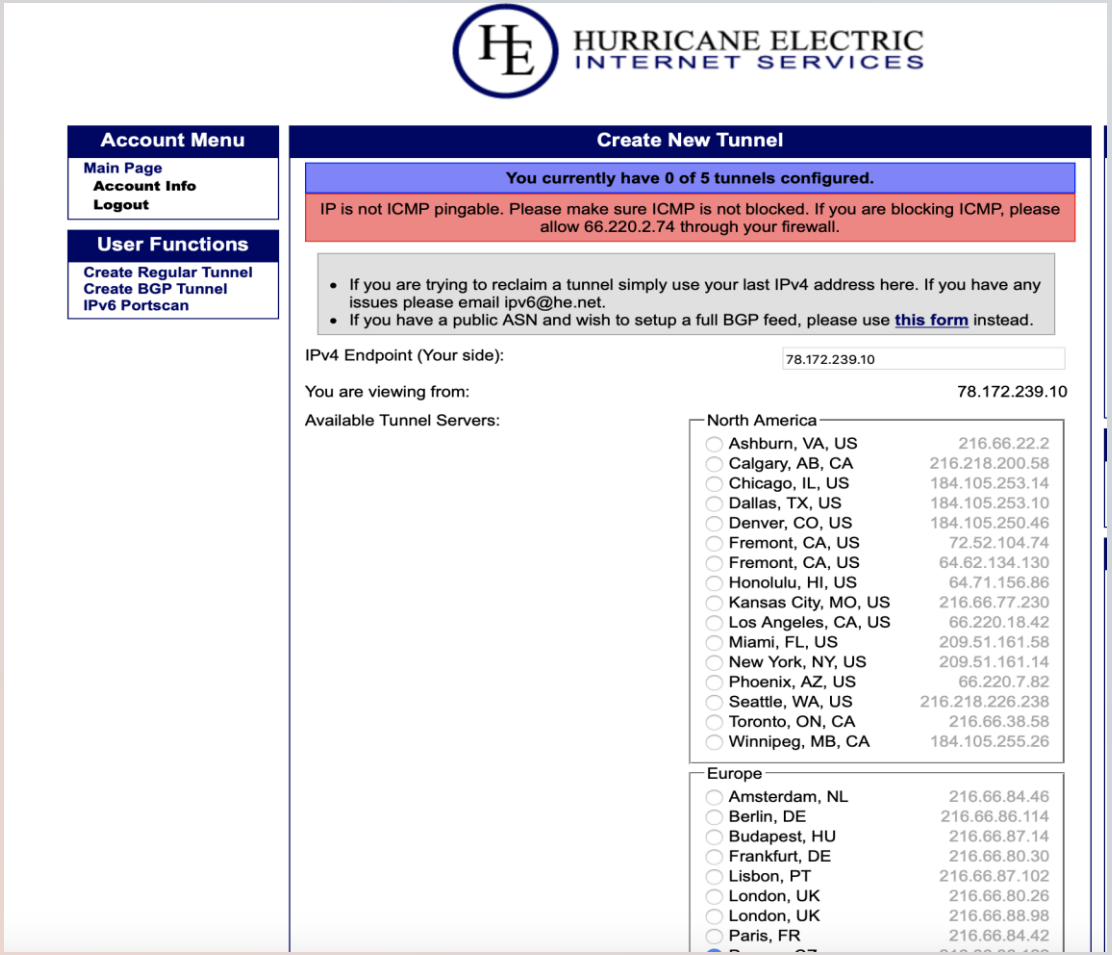
- The IPv6 addresses assigned to both sides of each tunnel must be global IPv6 addresses belonging to the IPv6 addressing space managed by the TB

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

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



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

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

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

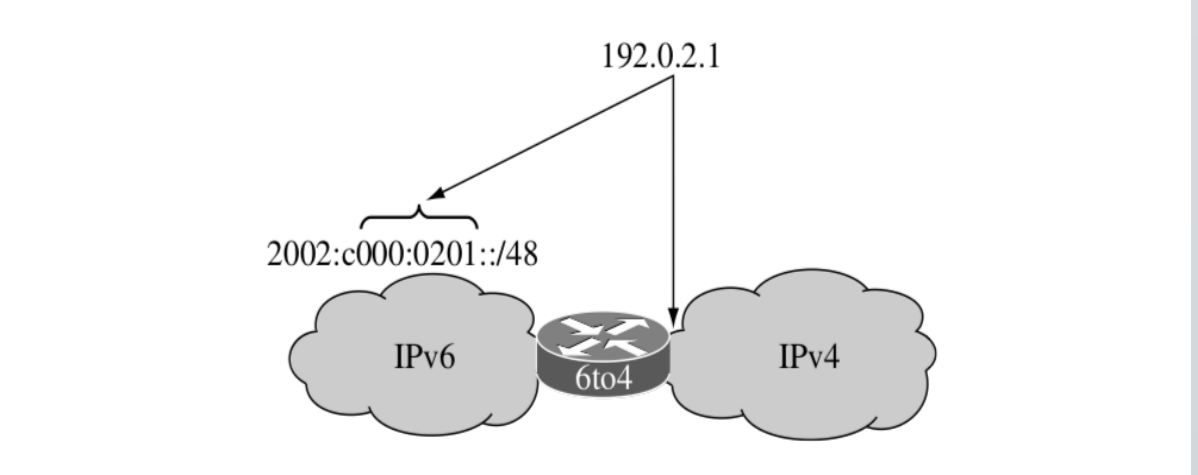
6to4 Automatic Tunnel

- 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

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.

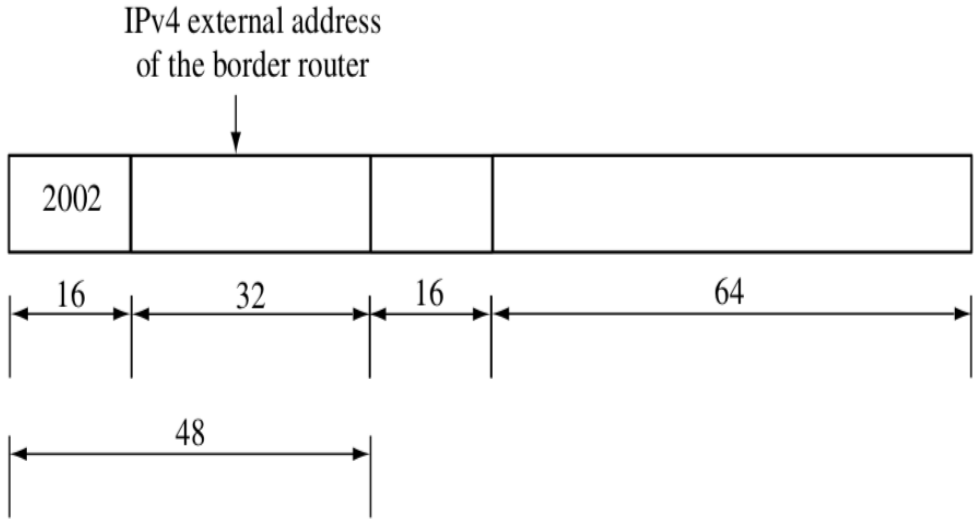
- The address space is based on 2002:<ipv4 external address in hex>::/48, where the IPv4 address is the border router external IPv4 address (192.0.2.1), represented in hexadecimal as c000:0201



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

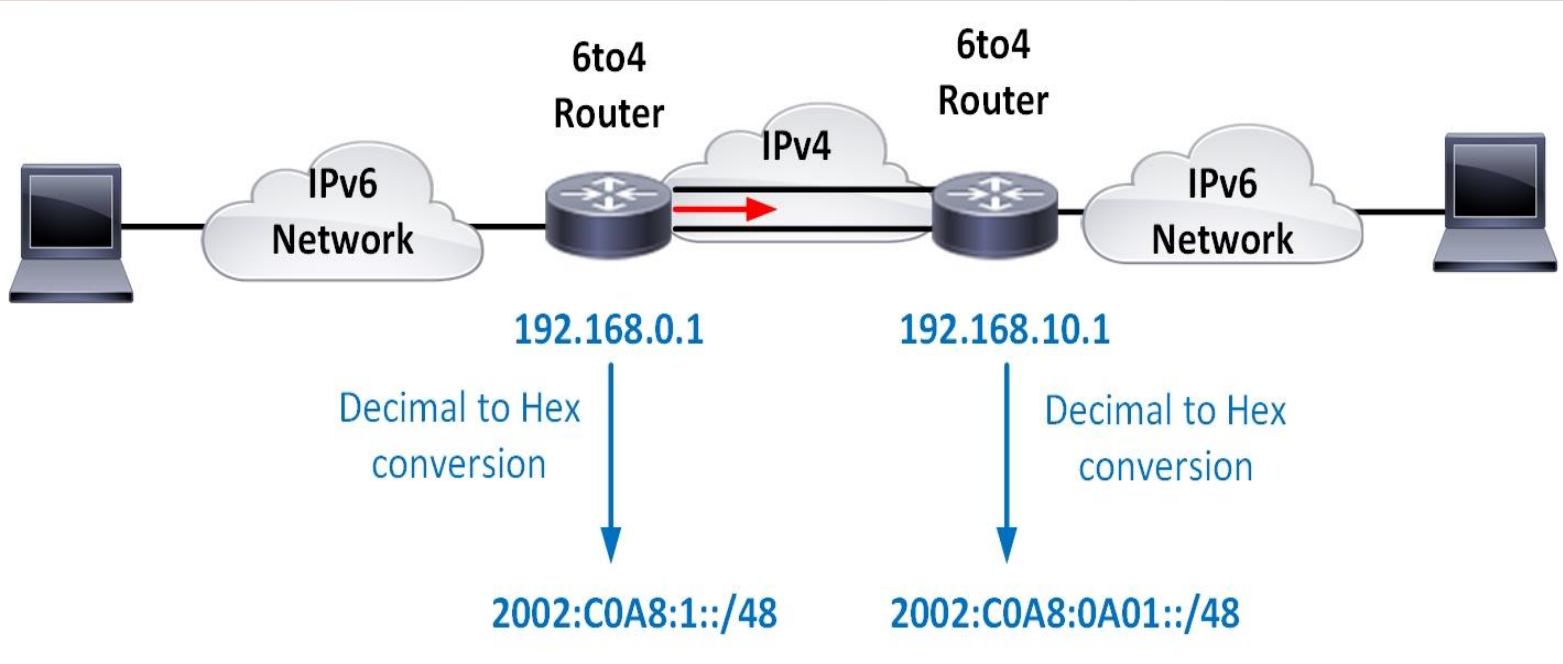
6to4 Automatic Tunnel

- 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

6to4 Automatic Tunnel



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

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
```

6to4 Tunnel Border Relay

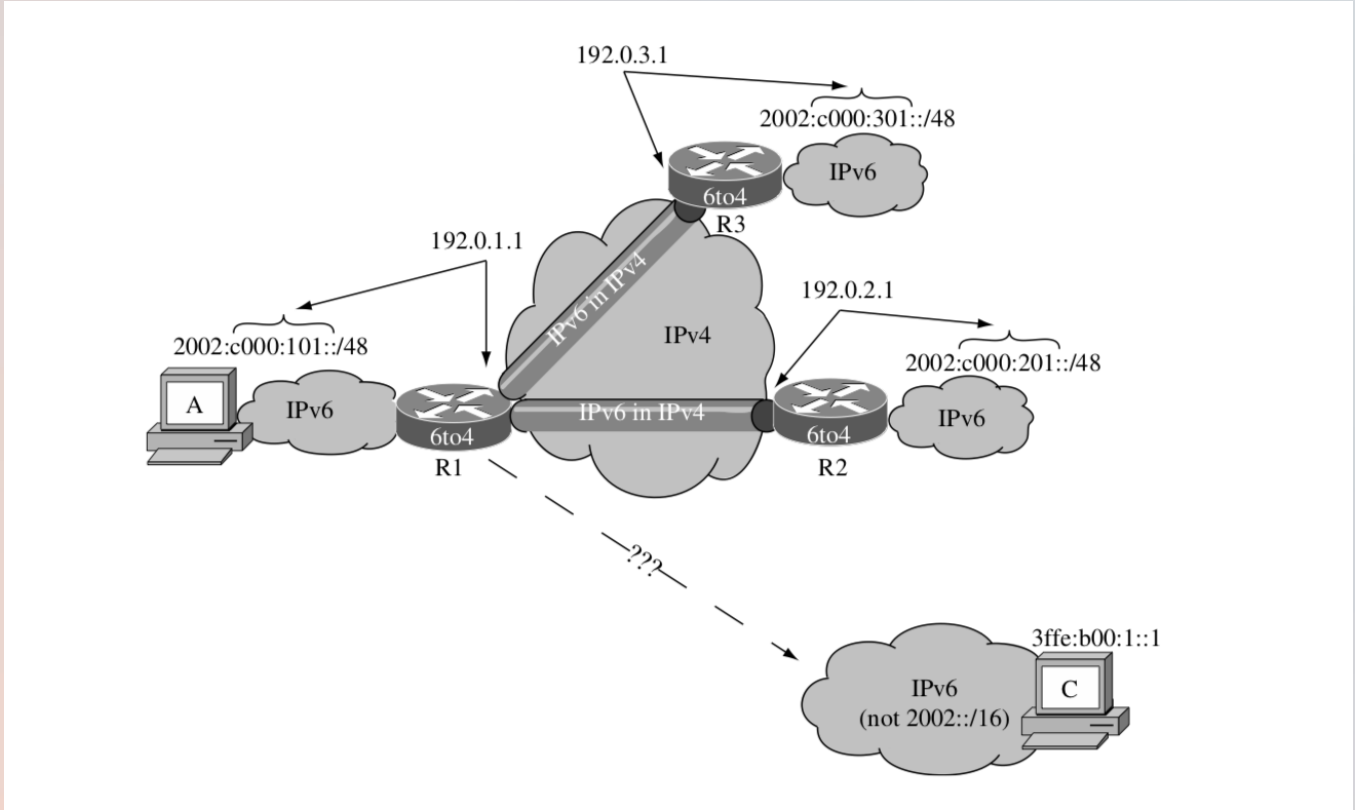
- If host A sends a packet to C with a non-6to4 address such as 3ffe:b00:1::1, the R1 router, the border router of A's site, does not know where to route the packet since the destination address is not a 6to4 address. R1 needs a 6to4 relay to the non-6to4 IPv6 Internet
- A 6to4 relay is a 6to4 border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

6to4 Tunnel Border Relay

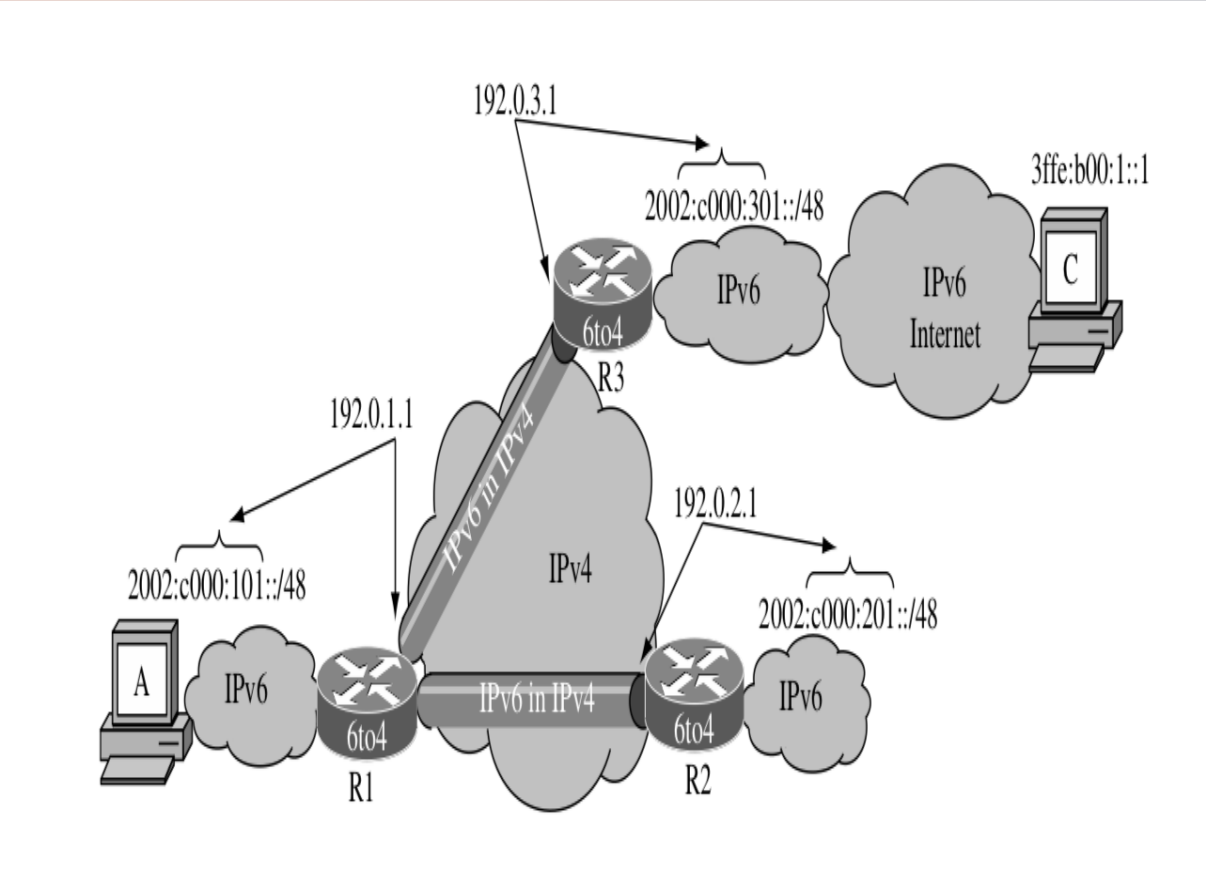
- To enable the 6to4 relay, the 6to4 relay router is a 6to4 router with a default route to the IPv6 Internet
- The 6to4 relay should contain some ingress filtering
- A 6to4 site that is using a 6to4 relay installs in the 6to4 border router an IPv6 default route pointing to the 6to4 address of the relay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

6to4 Tunnel Border Relay – Without Relay

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



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

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

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

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)

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

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

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

6rd - Border Relay Router

- 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

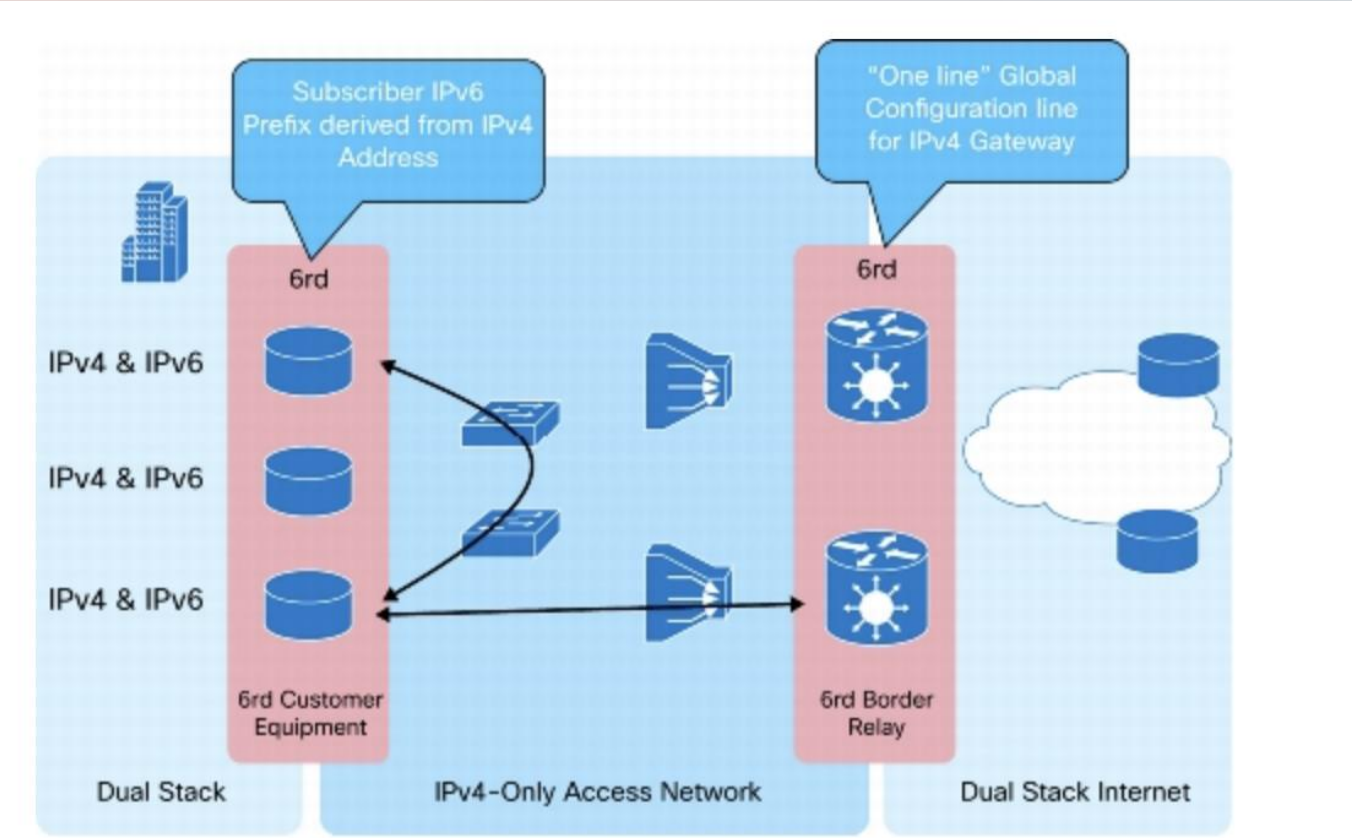
- In such a case, the IPv4 address embedded in the IPv6 destination address is used as the IPv4 destination address of the 6rd tunnel, and the local WAN interface IPv4 address is used as the source address for the 6rd tunnel, which is an IPv6 packet directly encapsulated in IPv4.

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

6rd - Border Relay Router



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

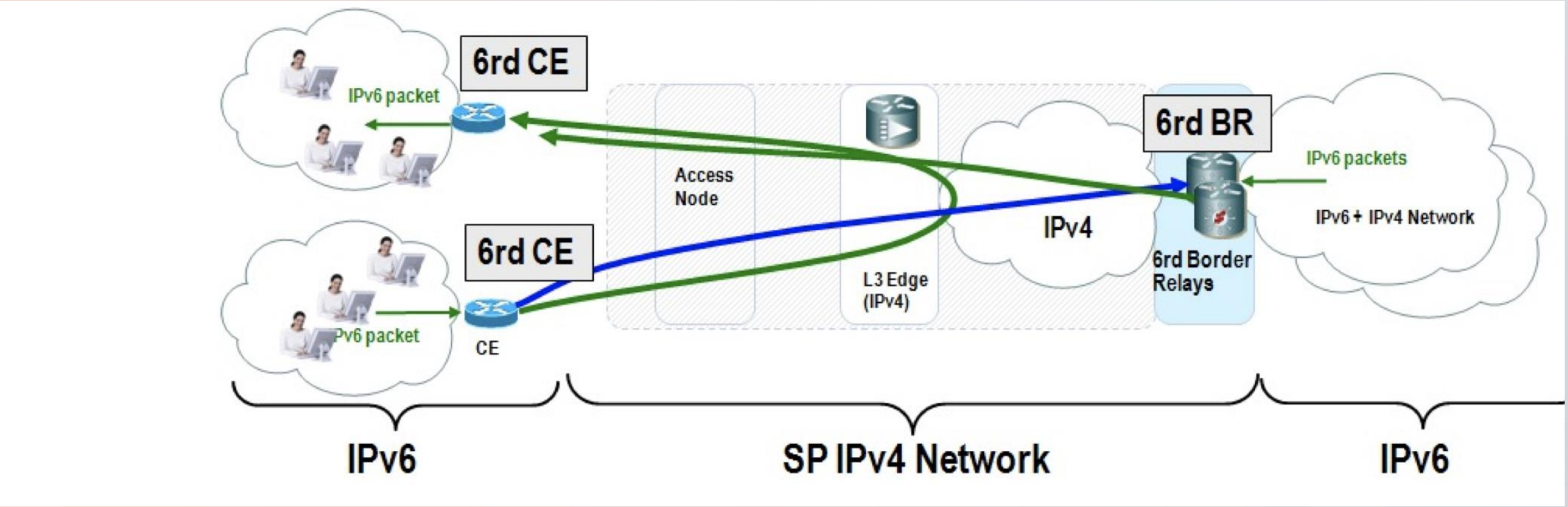
6rd – IPv6 Rapid Deployment

- 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

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.

6rd – IPv6 Rapid Deployment Traffic Flow Within Domain and Outside Domain



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

ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

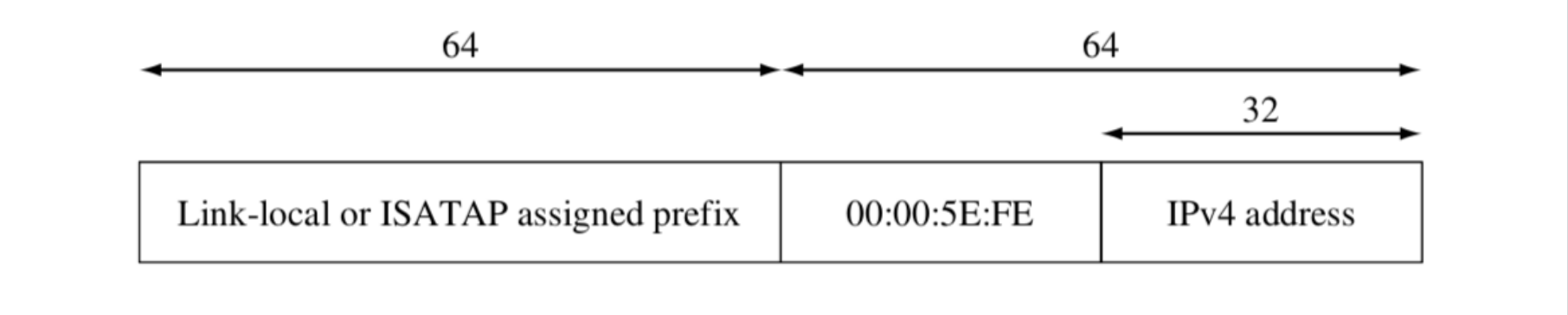
- It is a host to router or host to host Automatic tunneling mechanism, host can tunnel IPv6 traffic across IPv4 network
- Defined in RFC5214, so it is a standard based mechanism
- ISATAP enables unicast communication between IPv6/IPv4 hosts across the IPv4-only Intranet and Internet (If ISATAP router has an access to the IPv6 Internet), it doesn’t support Multicast

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

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



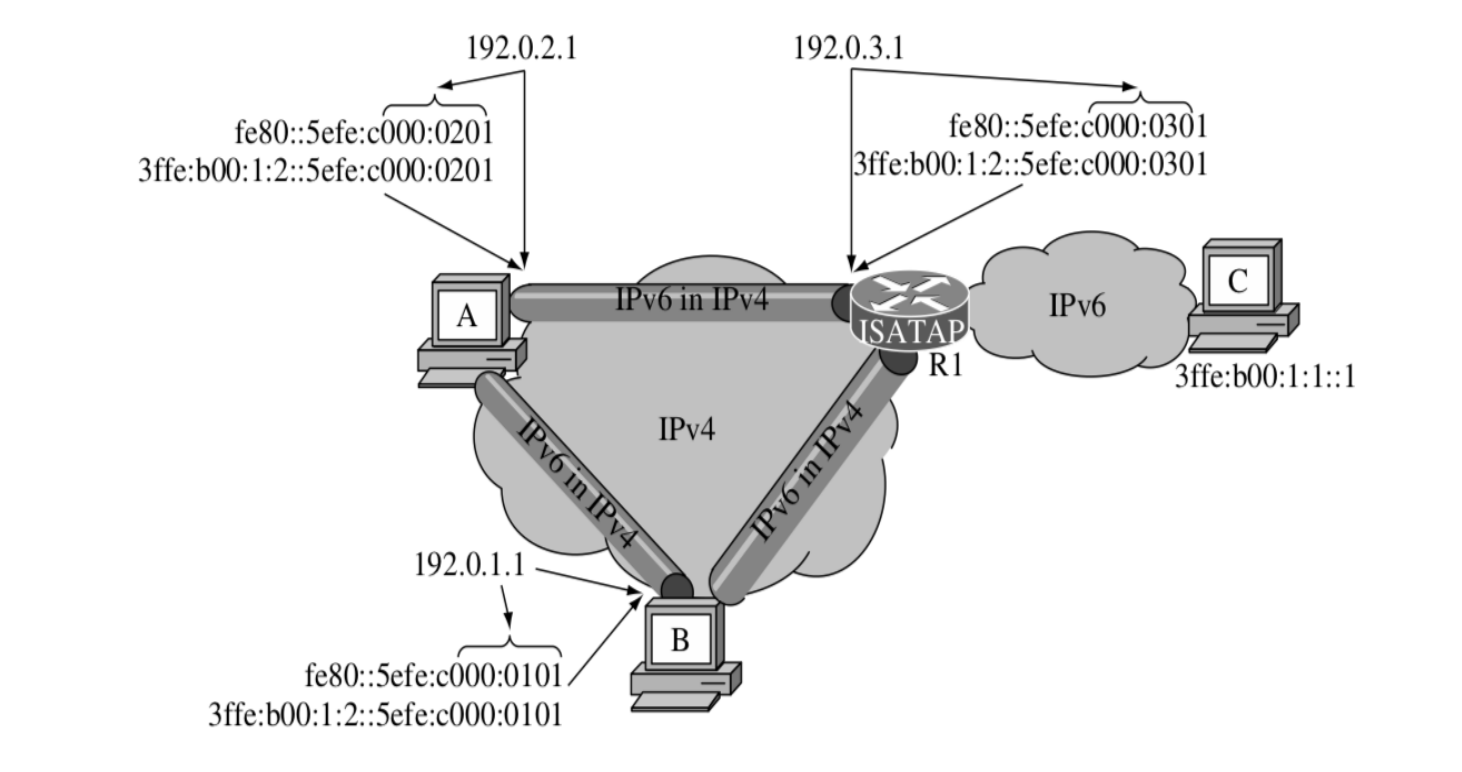
ISATAP - Intra-Site Automatic Tunnel Addressing Protocol

- 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

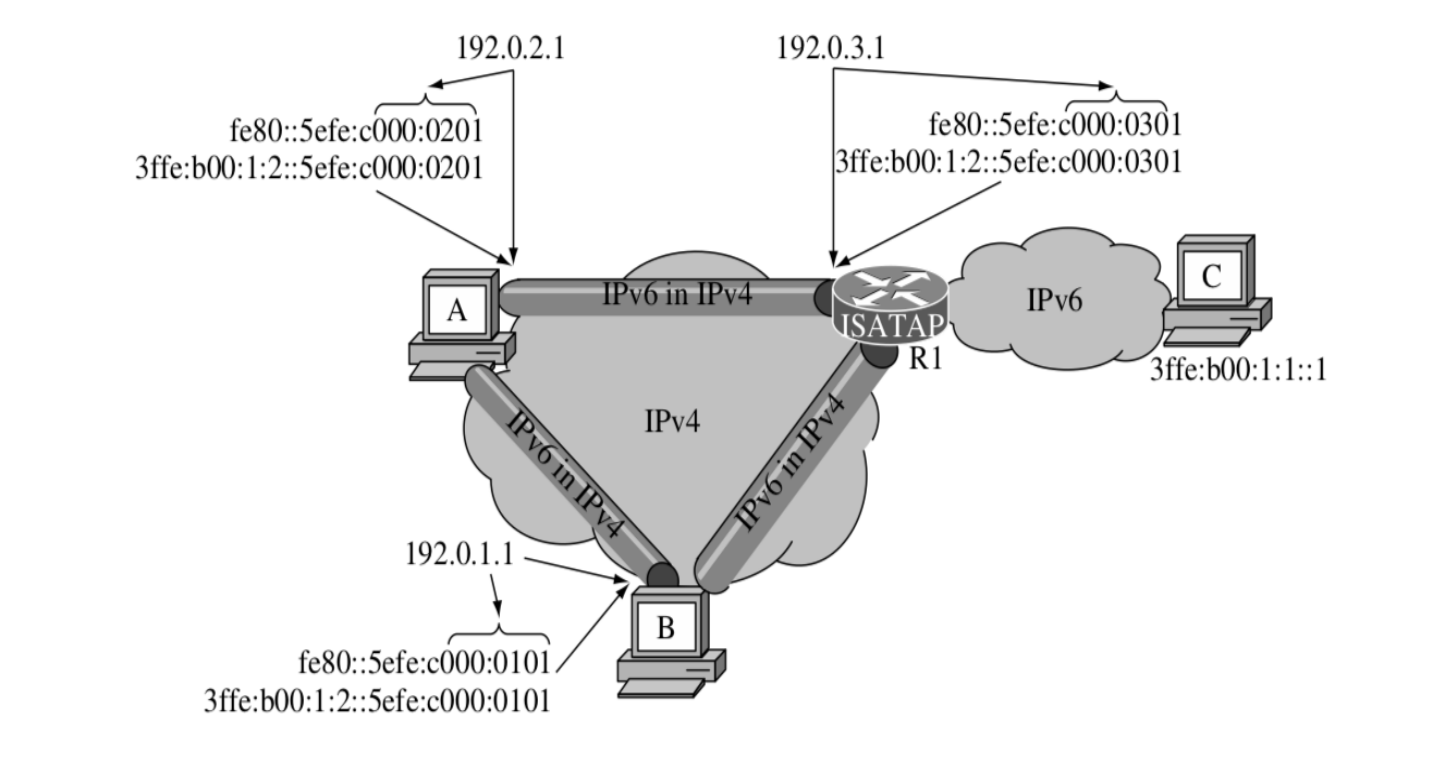
ISATAP – Link Local and Global ISATAP Addressing



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

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

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

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

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

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

TEREDO

- 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

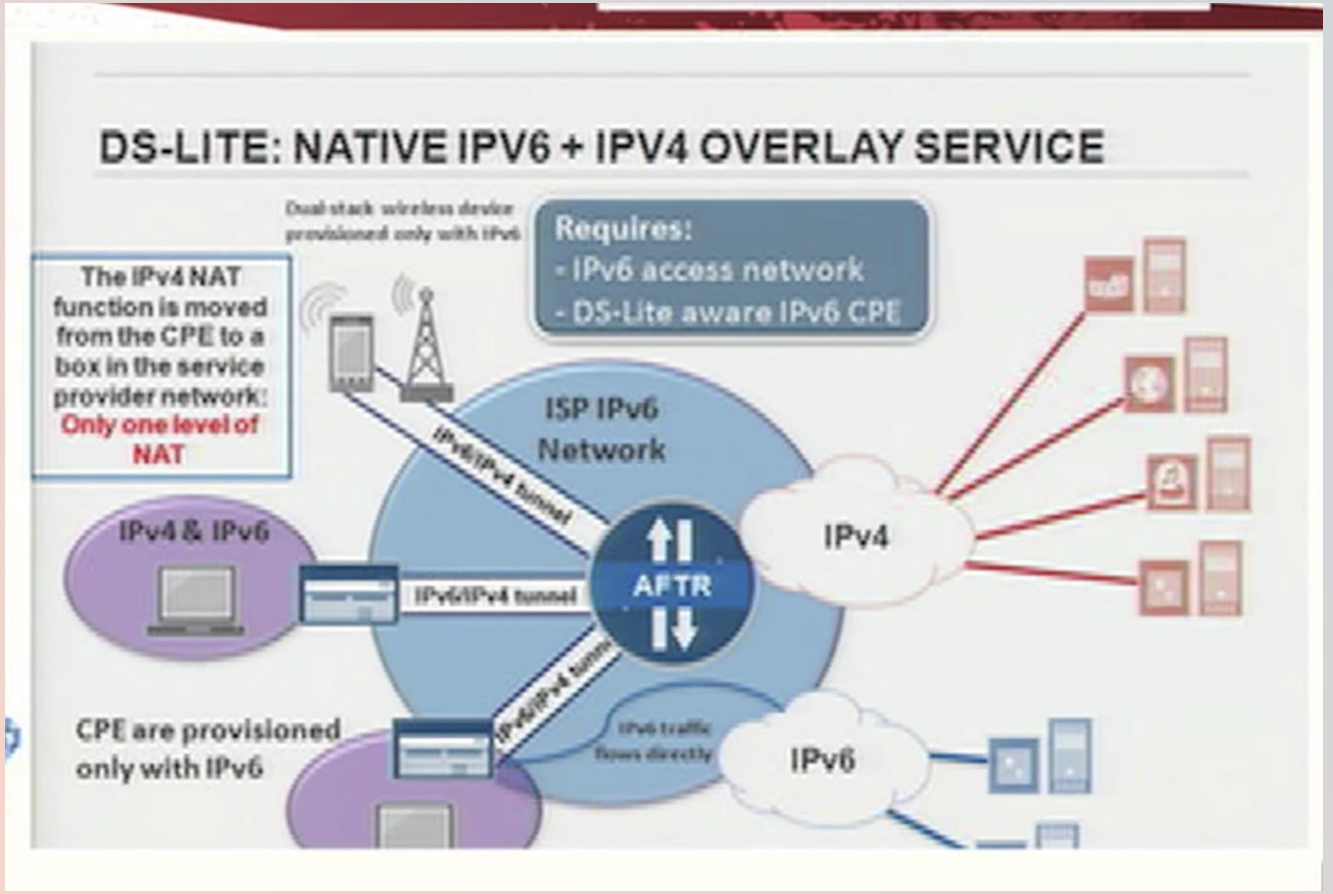
TEREDO

- 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.

DS-LITE

- It is an IPv4 overlay on top of an IPv6 infrastructure
- Similar to 6rd, DS-Lite is stateless , if there is NAT in the network for CGN purpose, that part is only stateful
- Access network needs to be IPv6 and CPE needs to be DS-Lite aware IPv6 node

DS-LITE



DS-LITE

- When Service Provider use DS-LITE, link between the provider and the customer (access network) is IPv6, this is considered as an advantage because network doesn’t have to run dual-stack
- Dual stack requires more resources on the device and management of it is more costly compare to IPv6 only infrastructure
- With DS-LITE only one layer of NAT is necessary , this is for connecting IPv6 only host to IPv4 content or IPv4 private addresses to be NATed to public address

DS-LITE

- It requires CPE to support DS-LITE, this is considered as disadvantage as there might be millions of CPEs and legacy devices may not be upgradable to support DS-LITE

- Some Operators deployed DS-LITE already

IPv6 Translation Techniques

- Translation techniques allow IPv6 only devices to communicate with IPv4 only devices (NAT64, 464XLAT)

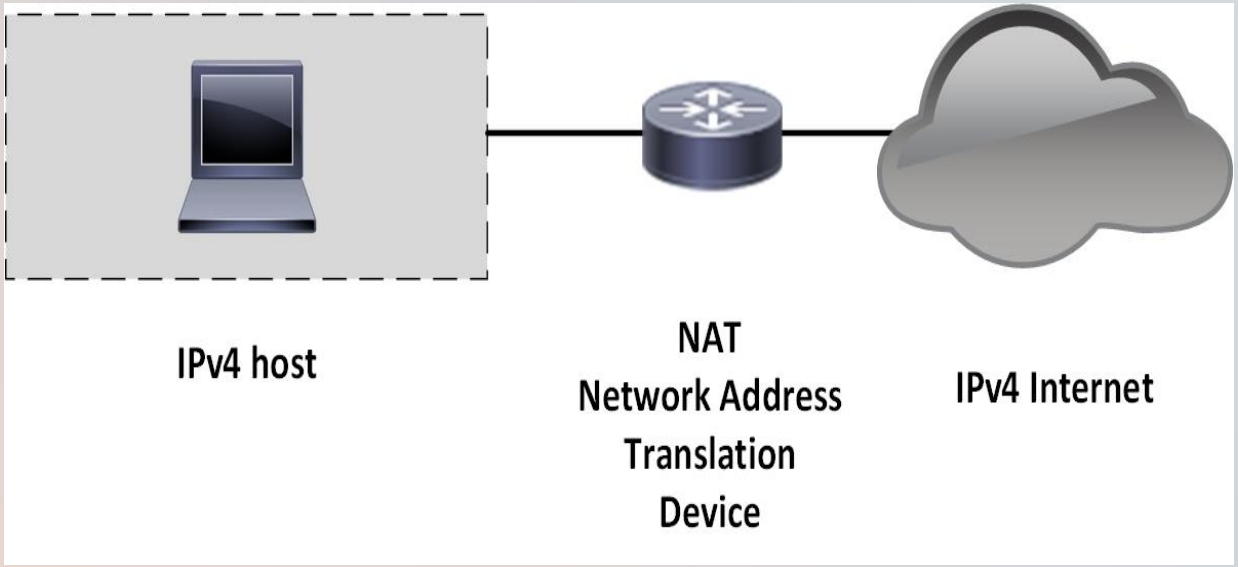
- Also they are used to extend the life of IPv4 (NAT – CGN/LSN)

IPv6 Translation Techniques

- NAT 44
- NAT64 and DNS 64
- CGN (aka LSN)
- 464XLAT

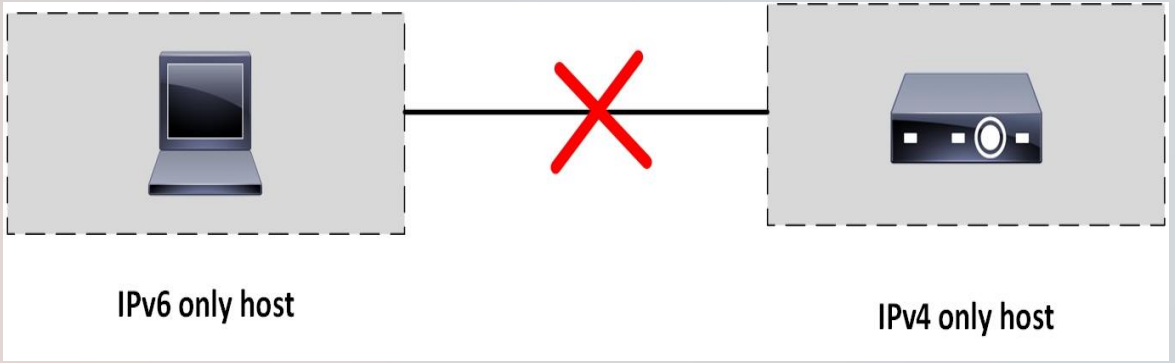
NAT44

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



NAT64

- IPv6 only host cannot communicate directly to IPv4 host



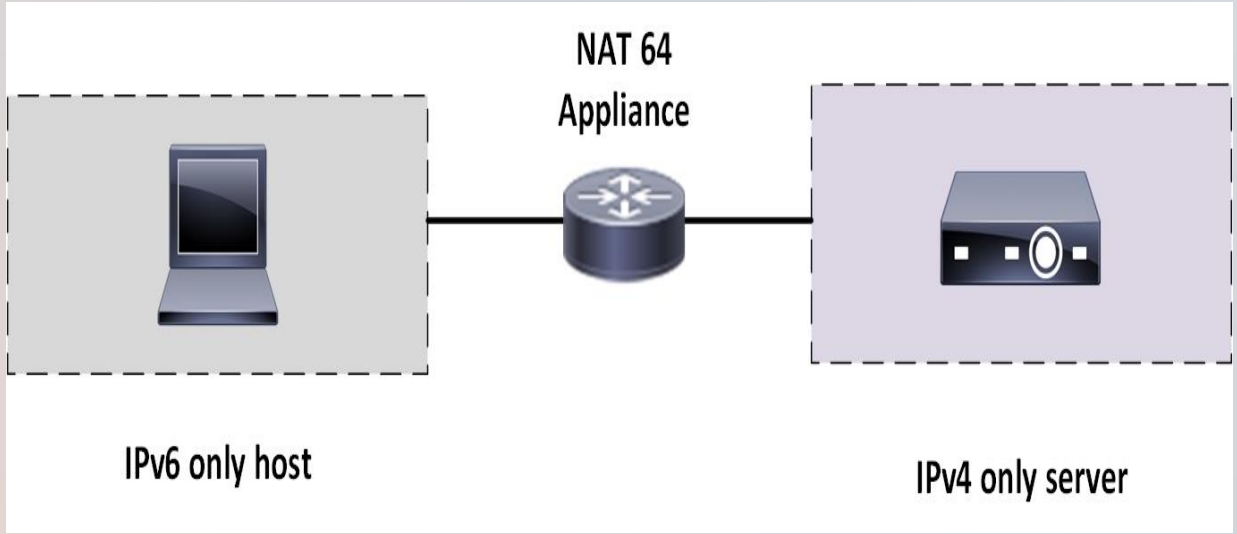
- For that reason several transition mechanisms developed

- Typical use case for NAT64 is IPv6 only Greenfield networks

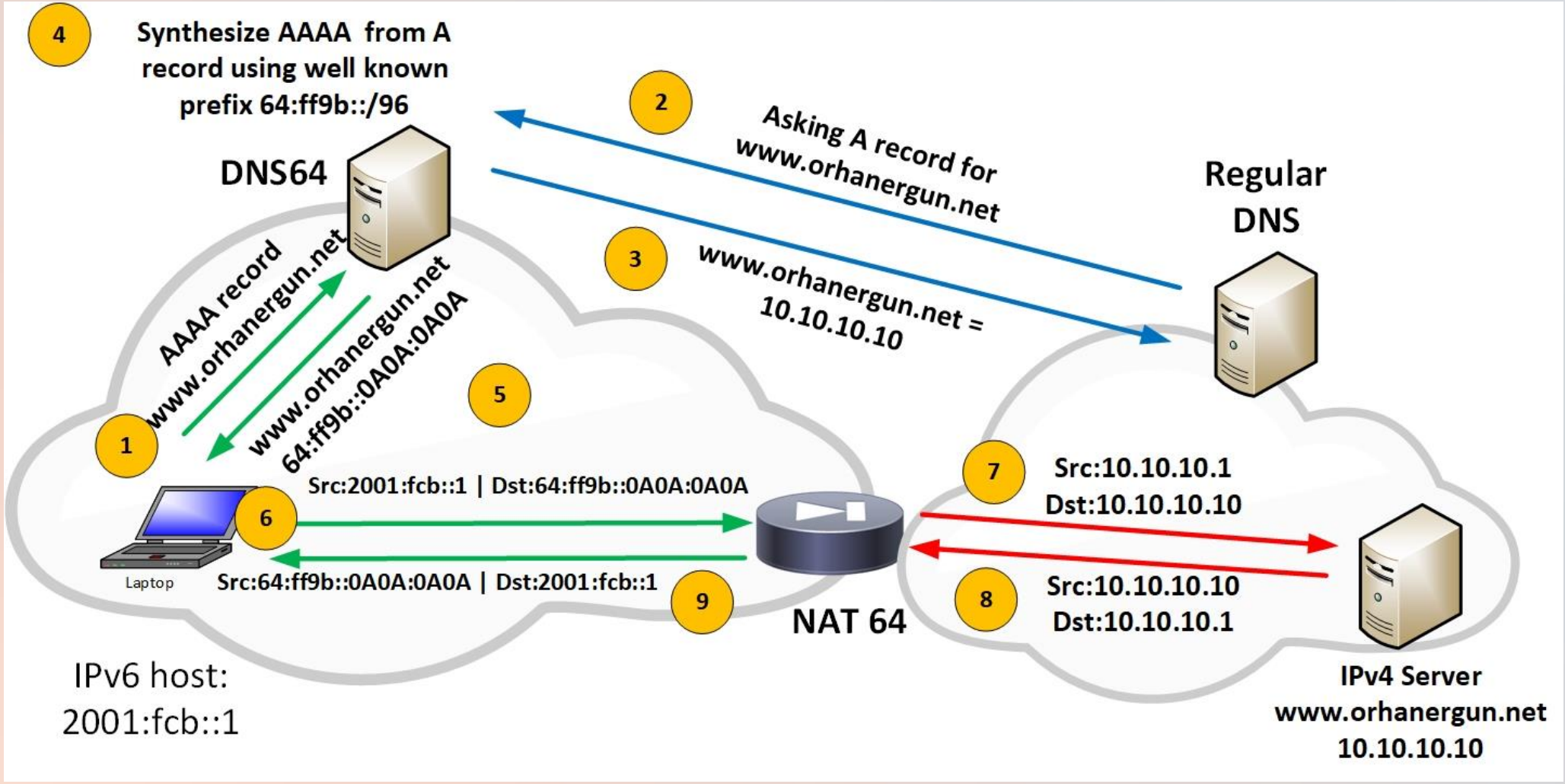
NAT64

- 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



NAT64 – How it works



NAT 44 and NAT64 Difference

- Translation of IP address into another IP address is known as Network Address Translation (NAT44 , NAT-PT)

- Translation of IP address from one address family into another address family is known as AFT (Address Family Translation), example is NAT 64, NAT46

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

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

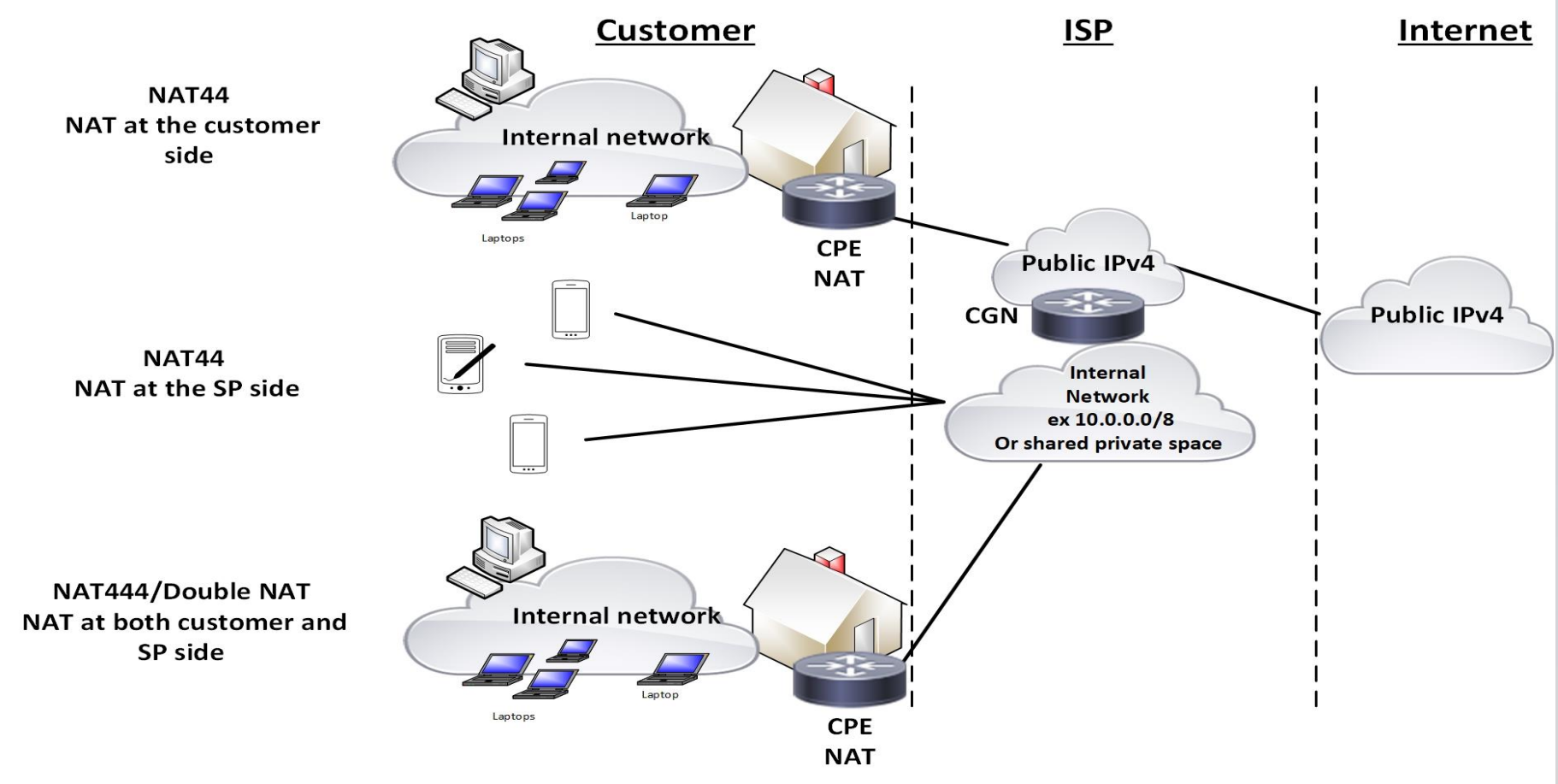
1. NAT 444 (Two layer of NAT44)
2. NAT 464
3. DS-LITE (It is a tunneling solution but mostly used together with CGN)

CGN – Carrier Grade NAT

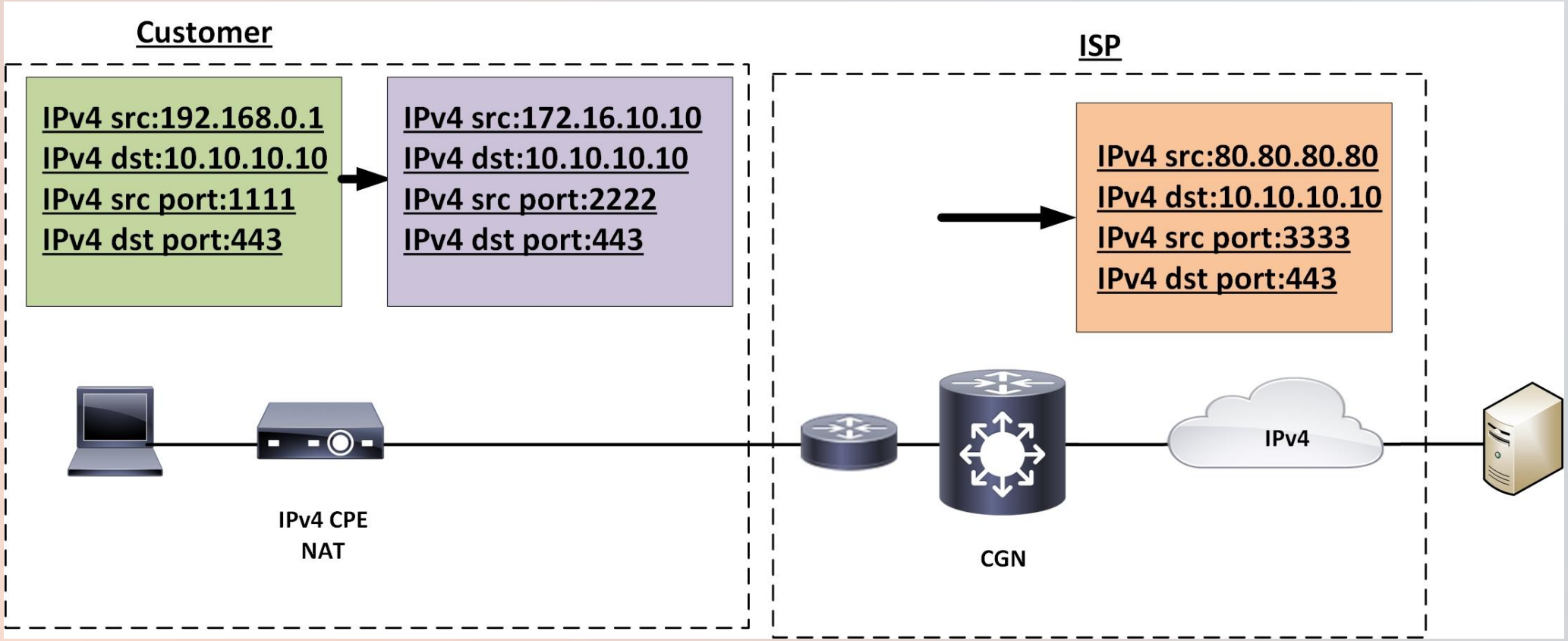
- Difference between Customer NAT (Residential NAT) and SP NAT (CGN, LSN) is, with Residential NAT, single public IPv4 address represent one household, with SP NAT (CGN,LSN), single public IPv4 address is shared across multiple households

- 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

How NAT (Network Address Translation) Wor*ks*



CGN – How CGN Work



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

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

- 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

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

CGN – Sharing Addresses Problems

- CGN 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

CGN – Sharing Addresses Problems

- 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.)

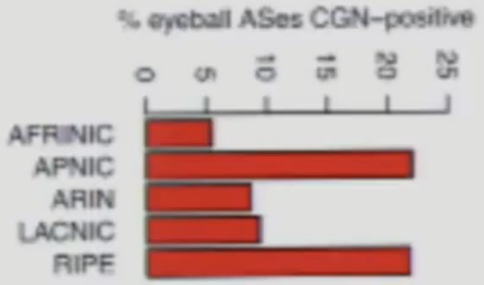
CGN – Sharing Address Problems

- 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)

CGN Current Deployment in SP networks

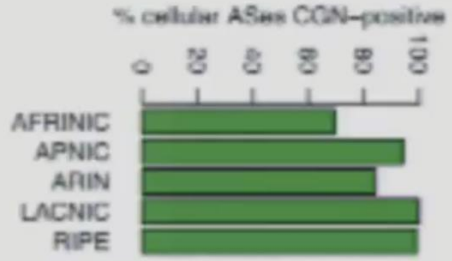
Eyeball Networks (Non-Cellular)

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



Cellular Networks

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



464 XLAT

- Some applications don’t work over IPv6 only network, they don’t support IPv6, such as Spotify, Skype, Whatsapp, Netflix etc.
- For IPv6 only network, NAT64/DNS64 is a good solution because it doesn’t require IPv4 on the host but above applications fail to work on IPv6 only networks
- Thus RFC 6877 – 464XLAT – Combination of Stateful and Stateless Translation was defined in IETF

464XLAT

- It is essentially an extension of NAT64
- Stateless NAT 46 at the Client side, Stateful NAT 64 at the network side
- Clients are assigned IPv6 address from the Service Provider NAT64 address pool

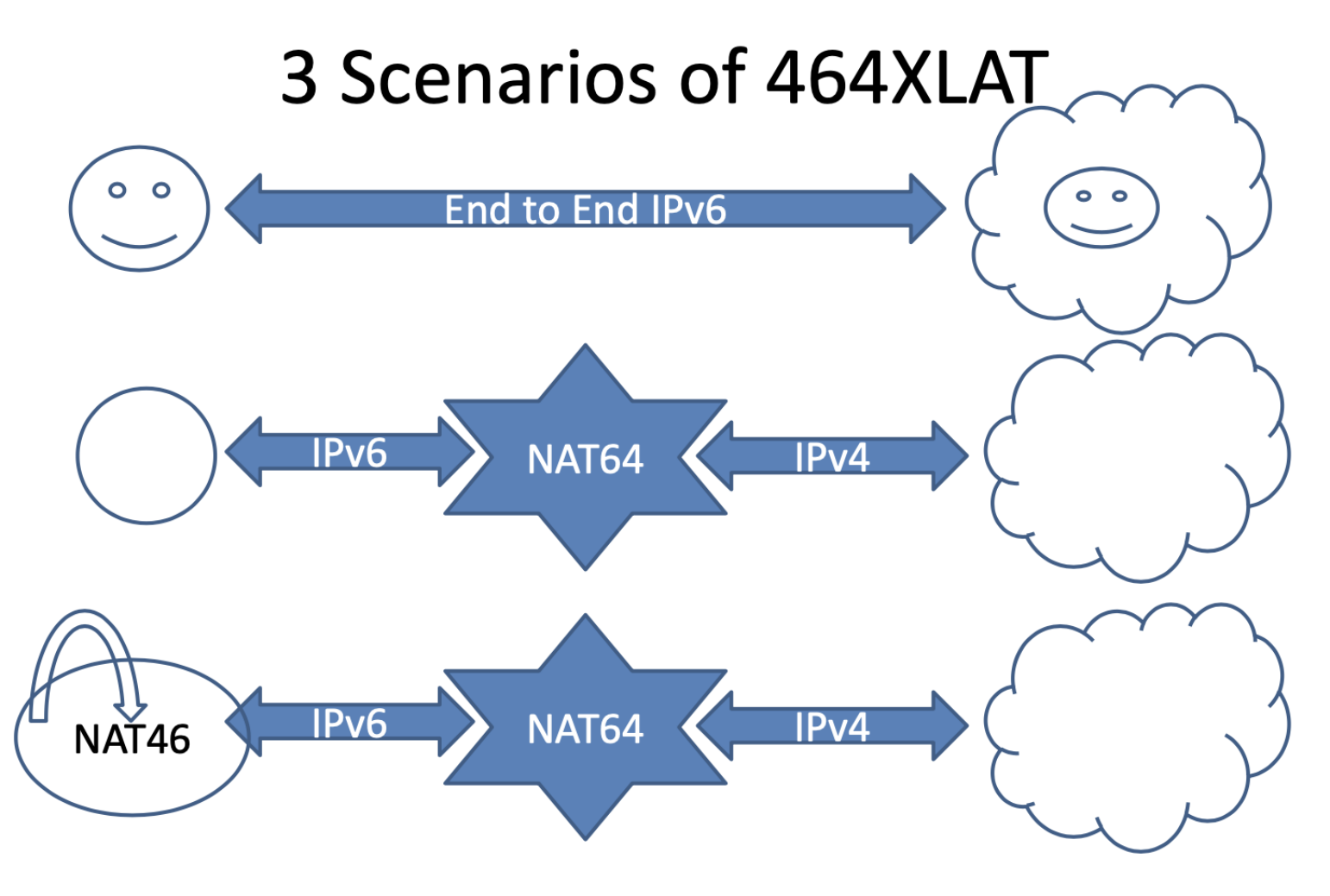
464XLAT

- IPv6 content is reachable without any CLAT or PLAT translation (For example Facebook , Google, Wikipedia etc.) because both Web browsers and the above content servers support IPv6 end to end

- If application supports IPv6 (for example web browsers) but the server is IPv4 only (www.amazon.com) then NAT64/DNS translates IPv6 from the client to IPv6 address to IPv4

- If application doesn’t support IPv6 (Skype, WhatsApp, Spotify), then client performs CLAT to translate IPv4 to IPv6 and network translate IPv6 address to IPv6 , thus IPv4> IPv6> IPv4 translation happens

464XLAT



464XLAT Summary

- 464XLAT is just a set of building blocks:

- Stateless NAT64 (RFC6145)

Client side translation CLAT (NAT4->6)

- Stateful NAT64 (RFC6146)

Provider site translation PLAT (NAT6>4)

- DNS64 (RFC 6147)

When the FQDN does not have a AAAA record, DNS64 dynamically creates one that allows the client to use IPv6 and the network translates from IPv6 to IPv4 at the NAT64

Used by many Mobile Operators today

IPv6 Routing Protocols

IPV6 Routing Protocols

- When IPv6 routing is enabled together with IPv4 routing protocol, we need to make sure sufficient device resources on the networking devices
- IPv6 Routing Protocols (General Purpose routing protocols at least – Not RPL etc.), they are very similar to their IPv4 counterpart
- There will be some differences which will be covered next

IPv4 and IPv4 Routing Protocols Side by Side

IPv4 Routing Protocols	IPv6 Routing Protocols
RIPv2	RIPnG – Next Generation
OSPFv2	OSPFv3
ISIS	ISIS for IPv6
EIGRP	EIGRP for IPv6
BGPv4	MP-BGP
PIM	PIM for IPv6

OSPF for IPv6 (OSPFv3)

- Operates very similar to OSPFv2 , both are link state protocols also other things are similar such as the LSA flooding rules, the LSA aging mechanisms, and the interface types (broadcast, point-to-point, point-to-multipoint, among others)
- Both OSPFv2 and OSPFv3 have two level of hierarchy (Backbone and Non-Backbone Areas)
- OSPFv2 only supports IPv4 but OSPFv3 supports both IPv4 and IPv6

OSPF for IPv6 (OSPFv3)

- But in OSPFv3, topology and reachability information are carried in different LSA
- Thus, adding a loopback interface for example doesn’t trigger full SPF run as it doesn’t change the topology of the network
- New LSA Type defined for OSPFv3

OSPF for IPv6 (OSPFv3)

- If you make a simple change, like changing the IP address on one of your routers then the topology itself doesn't change
- In OSPFv2, a new type 1 LSA and perhaps a type 2 LSA have to be flooded. Other routers that receive the new LSA(s) have to recalculate the SPT even though the topology did not change
- In OSPFv3, they changed this by creating a *separation* between prefixes and the topology

OSPF for IPv6 (OSPFv3)

- There is no prefix information in LSA type 1 and 2, you only find topology information in these LSAs, you don’t find any IPv6 prefixes in them!
- Prefixes are now advertised in type 9 LSAs and the link-local addresses that are used for next hops are advertised in type 8 LSA
- Type 8 LSAs are only flooded on the local link, type 9 LSAs are flooded within the area.

OSPF for IPv6 (OSPFv3)

- Type 1 and Type 2 LSA repurposed , Type 8 and Type 9 LSA are added in OSPFv3 (Link and Intra-Area Prefix Respectively)
- Type 8 LSA is link local only, Type 9 is Area wide
- LS Types indicates Scope as well (E is domain wide, 0x4005)

OSPFv3 LSAs		OSPFv2 LSAs	
LS Type	**Name**	**Type**	**Name**
0x2001	Router LSA	1	Router LSA
0x2002	Network LSA	2	Network LSA
0x2003	Inter-Area Prefix LSA	3	Network Summary LSA
0x2004	Inter-Area Router LSA	4	ASBR Summary LSA
0x4005	AS-External LSA	5	AS-External LSA
0x2006	Group Membership LSA	6	Group Membership LSA
0x2007	Type-7 LSA	7	NSSA External LSA
0x0008	Link LSA		*No Corresponding LSA*
0x2009	Intra-Area Prefix LSA		*No Corresponding LSA*

OSPF for IPv6 (OSPFv3)

- **Inter-Area Prefix LSA:**

  These LSAs are IPv6 equivalent of IPv4's Type-3 Summary LSAs. These LSAs are originated by the ABR to specify IPv6 prefixes that belong to other areas. A separate LSA is originated for each address prefix

- **Inter-Area Router LSA:**

  These LSAs are IPv6 equivalent of IPv4's Type-4 Summary LSAs. Originated by the ABR, the Inter-Area Router LSA describes the route to the ASBR. Each LSA describes a route to a single router

OSPFv3 LSAs		OSPFv2 LSAs	
LS Type	**Name**	**Type**	**Name**
0x2001	Router LSA	1	Router LSA
0x2002	Network LSA	2	Network LSA
0x2003	Inter-Area Prefix LSA	3	Network Summary LSA
0x2004	Inter-Area Router LSA	4	ASBR Summary LSA
0x4005	AS-External LSA	5	AS-External LSA
0x2006	Group Membership LSA	6	Group Membership LSA
0x2007	Type-7 LSA	7	NSSA External LSA
0x0008	Link LSA		*No Corresponding LSA*
0x2009	Intra-Area Prefix LSA		*No Corresponding LSA*

OSPF for IPv6 (OSPFv3)

- An OSPFv2 router forms adjacencies using its configured IPv4 interface address

- OSPFv3, however, makes use of IPv6's link-local address scope (FE80::/10). All OSPFv3 adjacencies are formed using link-local addresses

OSPF for IPv6 (OSPFv3)

- Neighboring routers are referred to not by IP address, but by OSPF ID, demonstrating OSPFv3's fundamental separation of the SPF tree and IP addressing

- OSPFv3 router IDs *are not IPv4 addresses*; they are merely unique 32-bit identifiers expressed in the familiar dotted-decimal notation

OSPF for IPv6 (OSPFv3)

- Unknown LSA Type Handling : OSPFv2 routers simple discard LSAs of an unknown type. OSPFv3 LSAs may be discarded, or optionally stored and flooded as though they were understood.

OSPF v2 vs. OSPFv3

Design Concern	OSPFv2	OSPFv3
Scalability	Good	Better since Router and Network LSA doesn't contain prefix information but only topology information
Working on Full Mesh	Works well with mesh group	Works well with mesh group
Working on Hub and Spoke	Works poorly, require a lot of tuning	Works bad requires tuning
Fast Reroute Support	Yes - IP FRR	Yes - IP FRR but limited platform support
Suitable on WAN	Yes	Yes
Suitable on Datacenter	DCs are full mesh. So, Not well	DCs are full mesh so Not well
Suitable on Internet Edge	No it is designed as an IGP	No it is designed as an IGP
Standard Protocol	Yes IETF Standard	Yes IETF Standard
New LSAs	None	Links LSA (Type 8) is used for adjaceny formation and link local scope only, Inter-Area-Prefix LSA (Type9) which is one of the biggest enhancement since it is used to carry prefix information only,inside an area
LSA Types	Router(Type1),Network(Type2),Summary(Type3),ASBR External(Type4),AS External(Type5),NSSA(Type7)	Router(Type1),Network(Type2),Inter-Area Prefix(Type3),Inter-Area Router(Type4),AS External(Type5),NSSA(Type7),Link LSA(Type8),Intra-Area-Prefix-LSA(Type9)
Transport	Multicast, 224.0.0.5 and 224.0.0.6	Same but with IPv6 addresses. Multicast. FF02::5 and FF02::6
Reachability info handeling	Inside an Area, Router and Network LSA carries the reachability information,between areas reachability info is carried in Summary(Type3) LSA	Inside an area reachability information is carried in Intra Area Prefix LSA (Type9) which is new LSA type, inter area prefixes are still carried in Type 3 LSA but name is changed as Inter-Area prefix LSA
Topology info handeling	Inside an Area Router and Network LSA carries the topology information,topology info is not carried beyond an area	Same.Inside an Area Router and Network LSA carries the topology information,topology info is not carried beyond an area
Stuff Experince	Very well known	Not well known, especially topology and reachability information handling,Multi Area Adjaceny and new LSA types should be understood better
Overlay Tunnel Support	Yes it supports	Yes it supports
MPLS Traffic Engineering Support	Yes with CSPF or external controller	Yes, with CSPF or external controller
Security	MD5 Authentication	Authentication is removed since it runs on top of IPv6, IPv6 supports IPSEC and Authentication, this simplifies the OSPF header
Suitable as Enterprise IGP	Yes	Yes
Suitable as Service Provider IGP	Yes	Definitely
Complexity	Easy	Moderate
Resource Requirement	Full SPF runs on prefix or topology change so it is worse than OSPFv3	If topology doesn't change, full SPF is not needed. Prefix information is carried in new LSA, not in Router LSA anymore
IPv6 Support	No	Yes
IPv4 Support	Yes	Yes
Default Convergece	Slow	Even slower if multiple address families are used
Troubleshooting	Easy	Harder,requires understanding IPv6 addressing, after that it is same packet types, LSA, LSU, DBD
Routing Loop	Inter area prefixes should be received from ABR,all non-backbone areas should be connected to the backbone area	Same as OSPFv2. Inter area prefixes should be received from ABR,all non-backbone areas should be connected to the backbone area

IS-IS for IPv6

- RFC5308 adds IPv6 address family support to IS-IS
- IS-IS can be deployed for IPv4 and IPv6 as Single Topology and Multi Topology
- With Single Topology IS-IS, IPv4 and IPv6 shares same link state topology and same SPF calculation for both IPv4 and IPv6
- Separate link state topology for IPv4 and IPv6 IS-IS in Multi Topology Routing IS-IS , Separate SPF Calculation for IPv4 and IPv6 in MTR IS-IS

IS-IS for IPv6

- Single Topology better for resource usage but Multi Topology might be good for resilience based on the network topology
- In order to have IPv6 support in IS-IS, unlike OSPF , we don’t need to have separate version of the protocol, instead new TLVs (Type, Length, Value Encoding) are simply added
- Thus, IS-IS is considered as extendible protocol when it is compared with other link state routing protocol which is OSPF

IS-IS for IPv6

2 Type/Length/Values (TLV) added to support IPv6 routing in IS-IS:

1. IPv6 Reachability TLV (0xEC) : Describes network reachability such as IPv6 routing prefix, metric information and some option bits

2. IPv6 Interface Address TLV (0xE8) : Contains a 128 bit address For Hello PDUs, must contain the link-local address (FE80::/10). For LSP, must only contain the non link-local address

EIGRP for IPv6

- EIGRP is a Cisco propriety protocol which supports IP routing, there is an Informational RFC 7868 , no stub feature
- EIGRP, similar to IS-IS, has a TLV based encoding schema, thus, it is considered as extendible protocol
- EIGRP has been extended to support IPv6 routing , new TLVs have been added

EIGRP for IPv6

- IPv6_REQUEST_TYPE
- IPv6_METRIC_TYPE
- IPv6_EXTERIOR_TYPE are the new TLVs.

- Hellos are sourced from the link-local address and destined to FF02::A (all EIGRP routers). This means that neighbors do not have to share the same global prefix (with the exception of explicitly specified neighbors where traffic is unicasted)

EIGRP for IPv6

- Automatic summarization is disabled by default for IPv6 (unlike IPv4)
- No split-horizon in the case of EIGRP for IPv6 (because IPv6 supports multiple prefixes per interface)
- No need to have new version of the protocol to have IPv6 with EIGRP, similar to IS-IS

IPv6 in BGP

- BGP4 is used for IPv6, IPv4 and many address family
- When BGP is used any address family other than IPv4 Unicast, we call it MP-BGP (Multi Protocol BGP)
- Single protocol (BGPv4) is used to carry both IPv4 and IPv6

IPv6 in BGP

- IPv6 behavior is similar as the IPv4 behavior
- IPv4 routes can be exchanged over an IPv6 TCP session and vice versa
- There may be two next-hop addresses in the next-hop attribute

IPv6 in BGP

Address Family Information (AFI) for IPv6:

- AFI = 2 (RFC 1700)
  - Sub-AFI = 1 Unicast
  - Sub-AFI = 2 (Multicast for RPF check)
  - Sub-AFI = 3 for both Unicast and Multicast
  - Sub-AFI = 4 Label
  - Sub-AFI= 128 VPN

IPv6 in BGP

To make BGP-4 available for other network layer protocols, RFC2858 defines multi-protocol extensions for BGP-4:

1. Enables BGP-4 to carry information of other protocols (e.g MPLS,IPv6)
2. New BGP-4 optional and non-transitive attributes:
    1. MP_REACH_NLRI
    2. MP_UNREACH_NLRI
3. Protocol independent NEXT_HOP attribute
4. Protocol independent NLRI attribute

IPv6 in BGP

New optional and non-transitive BGP attributes:

- MP_REACH_NLRI (Attribute code: 14)

  Carry the set of reachable destinations together with the next-hop information to be used for forwarding to these destinations

- MP_UNREACH_NLRI (Attribute code: 15)

  Carry the set of unreachable destinations

IPv6 in BGP - IPv6 over IPv4 or IPv4 over IPv6 Sessions

- BGP routers that support IPv6 allow BGP sessions to be set up using IPv6 addresses. MP-BGP speakers tell their neighbors which AFI+SAFI combinations they want to use in the OPEN message at the beginning of a BGP session

- This can lead to the situation where IPv6 routing information is exchanged over IPv4, or IPv4 routing information is exchanged over IPv6.

IPv6 in BGP - IPv6 over IPv4 or IPv4 over IPv6 Sessions

- Actually nothing wrong with that, but it can create problem:

How does the router know what IPv6 next hop address to include in its updates towards an IPv4 neighbor? To avoid this situation, it’s considered best practice to only exchange IPv4 prefixes over an IPv4 external BGP (EBGP) session and only exchange IPv6 prefixes over an IPv6 EBGP session.

IPv6 in BGP - IPv6 over IPv4 or IPv4 over IPv6 Sessions

- However, internal BGP (IBGP) doesn’t update the next hop address, so there are no problems exchanging both IPv4 and IPv6 prefixes over the same IBGP session

- So most networks use the existing IPv4 IBGP sessions to exchange IPv6 prefixes rather than set up a whole new set of IPv6 IBGP sessions.

IPv6 in BGP - IPv6 over IPv4 or IPv4 over IPv6 Sessions

- The only downside of this approach is that if then something bad happens to IPv4, the IPv4 IBGP sessions go down and IPv6 is also affected

- If IPv6 had its own IBGP sessions, it may have continued to operate independently from IPv4.

IPv6 MPLS

IPv6 in MPLS

- If IPv6 will be transported over MPLS network, two possible approaches can be used , either Dual-stack or tunneling
- We have seen dual stack
- IPv6 IGP , MP-BGP and IPv6 for LDP should be deployed for dual-stack on the network , comes with the complexity , resource usage , security (two protocols vs one) and scalability problems with dual-stack comes into the picture

IPv6 in MPLS

- LDPv6 is defined in RFC 7552
- LDP is a transport protocol, services run op top it, for example 6PE and 6VPE doesn’t require LDPv6 as LDPv4 is enough to provide transport for these services
- But for the IPv6 only network, LDP specification (RFC 5036) has lack of details, thus LDPv6 RFC defined the new rules for IPv6 only and dual stack networks in regards to LDP label distribution, LSP Mapping , LDP TTL Security and so on.

6PE

- RFC 4798 defined 6PE procedure as Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)
- PE routers are dual stack routers (Supports both IPv4 and IPv6) and MP-BGP capable devices
- With 6PE approach, core network is just an IPv4 MPLS network, doesn’t have to support IPv6

6PE

- If provider is using Route Reflector to send IPv6 address reachability between 6PE routers, then RR needs to support dual-stack as well, if full mesh IBGP between the 6PE routers, then no need dual-stack on RRs

- Between CE and PE , it is IPv6 connectivity

- 6PE is used for Global IPv6 connectivity, IPv6 Internet, if customer is looking to connect their side within their VPN, then solution is called 6VPE

6PE

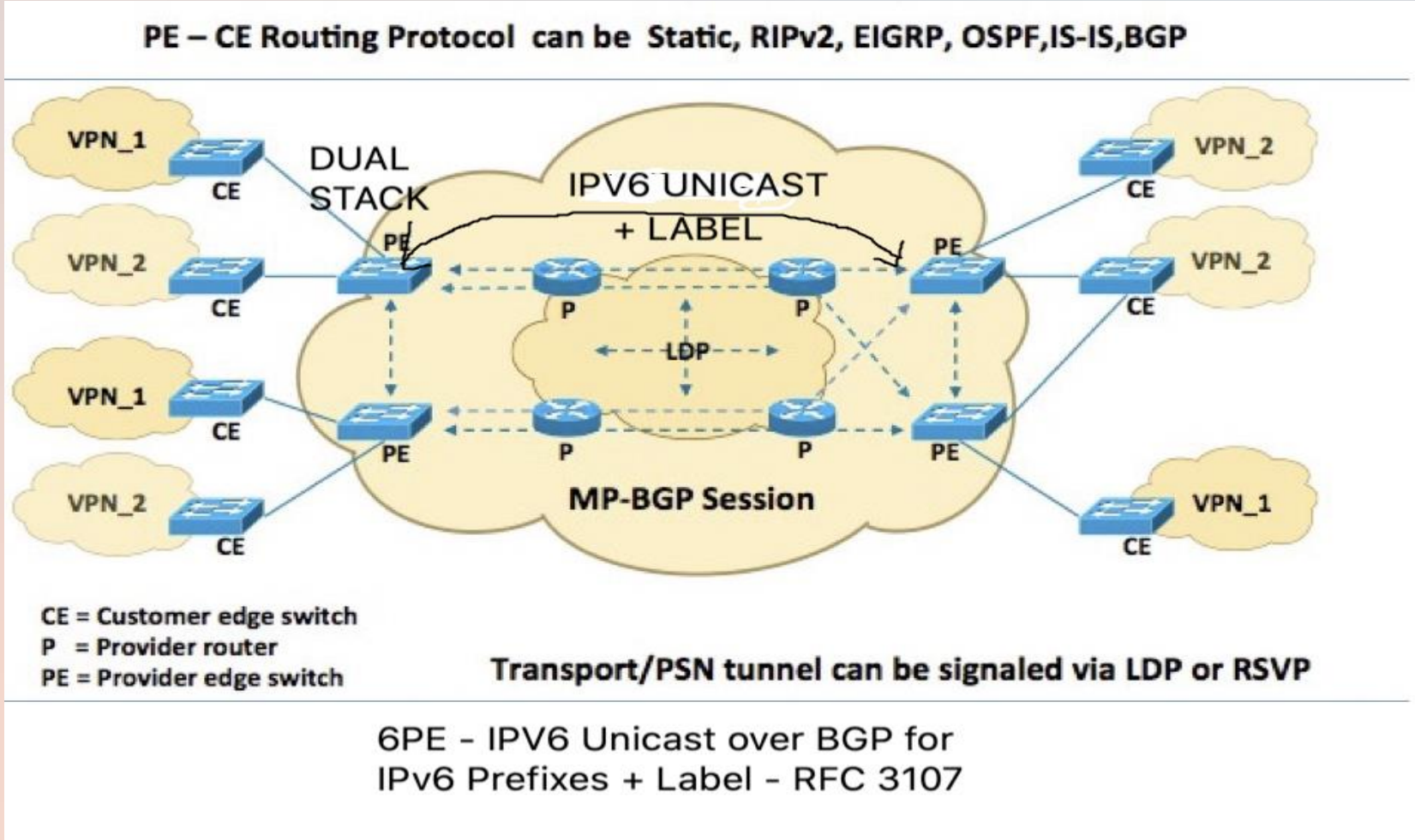
- When using 6PE, a CE router is connected to an interface on the PE router that’s in the global IPv6 routing table

- Between PE routers there’s an MPLS network with BGP, an IGP (IPv4) and LDP (IPv4).

6PE

- The IGP and LDP only needs to be IPv4 capable, and BGP only needs to have an IPv4 session
- That BGP session do however need to activated for the IPv6 unicast address family to make it possible to advertise IPv6 prefixes from PE to PE. Additionally, BGP needs to attach a label to each IPv6 prefix with the ‘send label’ command on Cisco devices.
- IPv6 routes pointing to the CE router should be redistributed into BGP

6PE



6PE - IPV6 Unicast over BGP for
IPv6 Prefixes + Label - RFC 3107

6VPE

- The difference between 6PE and 6VPE is whether the IPv6 routes are in the global routing table or in VRFs

- 6PE serves the same role as plain IPv4 over MPLS, and 6VPE is the equivalent of an MPLS VPN

6VPE

- Both 6PE and 6VPE exploit the fact that as long as a packet somehow can be forwarded through LSP from ingress PE to egress PE, P routers do not care about anything but the transport label

6VPE

- With 6VPE, the CE facing interface on the PE router is in a VRF

- This makes 6VPE pretty much exactly like an MPLS VPN, except that the transport label is derived from an IPv4 address instead of IPv6, if dual-stack (IPv4 and IPv6) would be deployed on MPLS core, IPv6 address of the Egress PE would be used as next-hop and transport label would be assigned for that IPv6 next-hop address

6VPE

- Required Protocols for 6VPE (Similar to traditional MPLS VPN) :

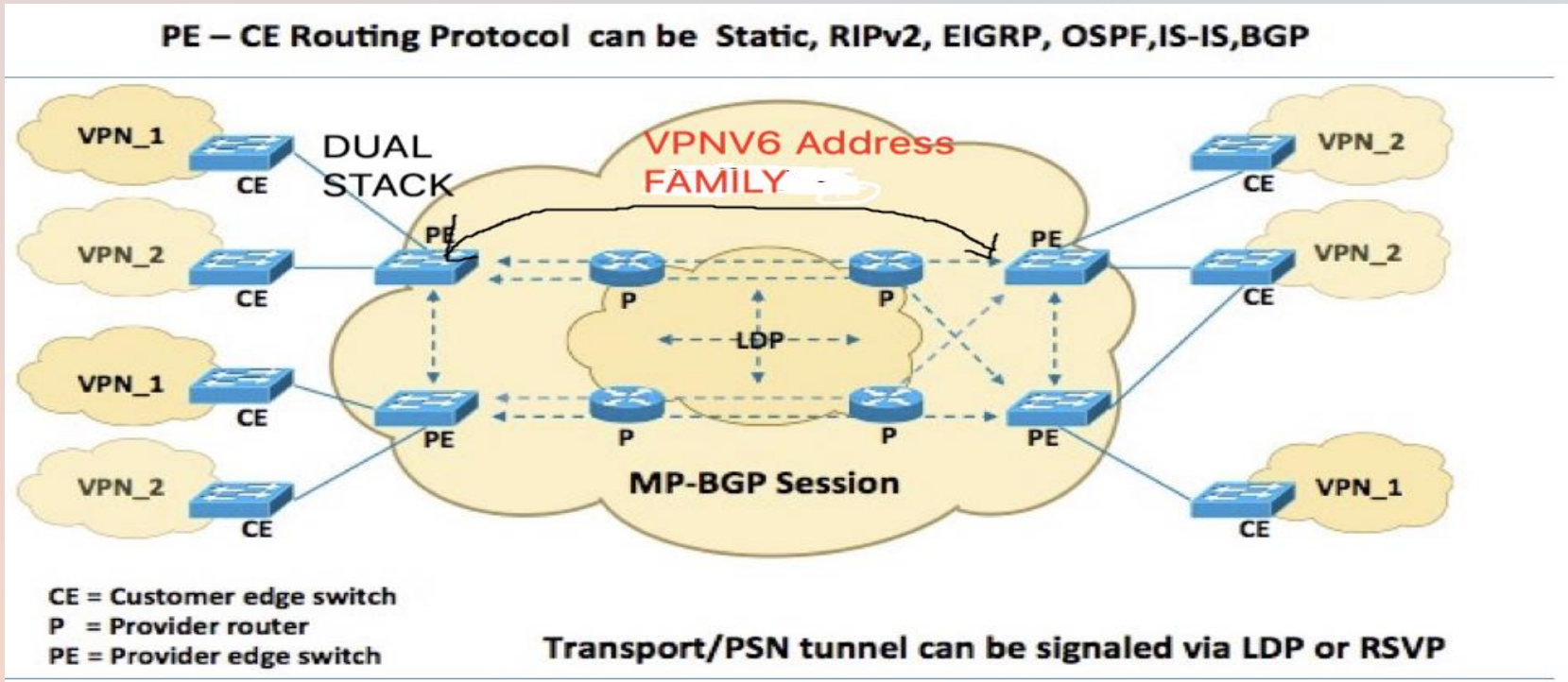
- An MPLS core with IPv4 IGP and IPv4 LDP and/or TE.
- The PE routers are IPv6 capable.
- The PE routers have IPv6 VRFs on interfaces towards CEs.
- BGP advertises VPNv6 prefixes between PEs and they are imported into VRFs based on route targets.

6VPE

- Required Protocols for 6VPE (Similar to traditional MPLS VPN) :

- The data plane uses a transport label and a VPN label.
- There’s some kind of IPv6 routing between CE and PE.
- BGP next hop on ingress PE is an IPv4-mapped IPv6 address.
- You can run MPLS VPN for IPv4 and 6VPE at the same time, and even on the same interface.

6VPE



6VPE - IPv6 Prefixes in VRFs, VPNv6 Address Family Between PEs
No IPv6 , No LDPv6 in the Core
Core is IPv6 , LDPV4 , Only MP-BGP is for VPNv6 session

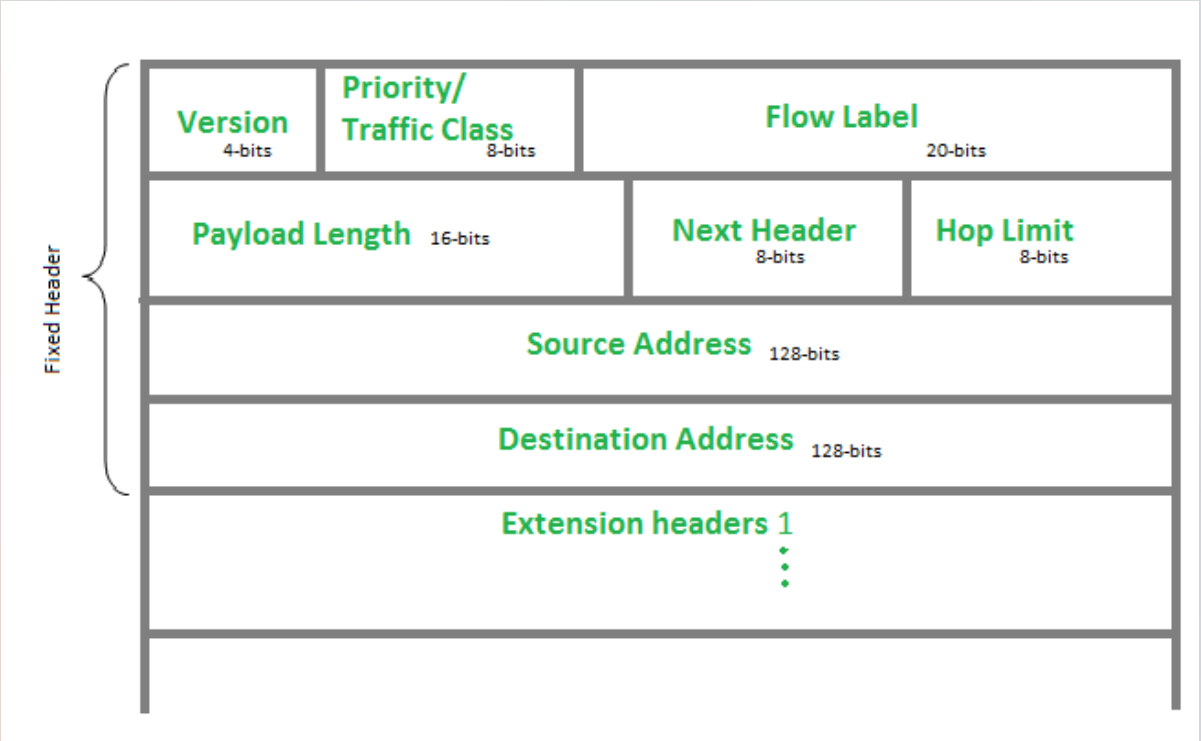
IPv6 in MPLS Summary

- Core doesn’t run IPv6 , LDPv6 with 6PE and 6VPE
- Only IPv4 and LDPv4 with 6PE and 6VPE
- Provides scalability , less complexity , better security and easier troubleshooting as there is single protocol only in the Core with 6PE and 6VPE
- Less resource usage in the core with 6PE and 6VPE but more on the Edge (PE) routers
- It could be designed as Dual Stack in the core, in that case opposite of the above advantages

IPv6 Quality of Service - QoS

IPv6 QoS

- There are two fields that can help IPv6 QoS : Traffic Class and Flow Label
- Traffic Class is 8 bit field which is used to distinguish packets from different classes or priorities
- IPv4 TOS byte is renamed with IPV6 Traffic Class , it is same as IPv4 8 bits TOS byte



IPv6 QoS

- Both IPv4 and IPv6 use DSCP for the PHB
- First 6 bits of the Traffic Class Field is DSCP and 2 bits for ECN , same as IPv4 TOS byte
- The intended use case with Flow Label is QoS - I.e. the source might want to ask for special handling for packets associated with a certain flow

IPv6 QoS

- IPv6 classification can be done based on IP Precedence, DSCP or EXP values which are already defined for IPv4

- Same type of services can be given by the Provider to the customers (Gold, Bronze , Silver , Best Effort service classes for QoS)

IPv6 QoS

IPv6 Marking , Queening , Shaping , Rate-Limiting etc. all are same as IPv4 and on the Cisco devices can be configured under MQC , match ip protocol IPv6 vs match ip protocol IPv4

There is Flow Label field in IPv6 header

IPv6 QoS

- Flow label is 20 bit field which is defining the packet of the field
- It is selected by the source randomly and never modified in the network
- Flow label is a value given to a flow of packets, and that value is the same across that flow.

IPv6 QoS

- There's no information that actually assists with ordering of that flow, its simply to identify them as part of that flow
- Flow label can help routers to hash packets in a given flow, some vendors already support that (Ex: Arista, If IP hashing is enabled, flow label by default is part of hash fields)

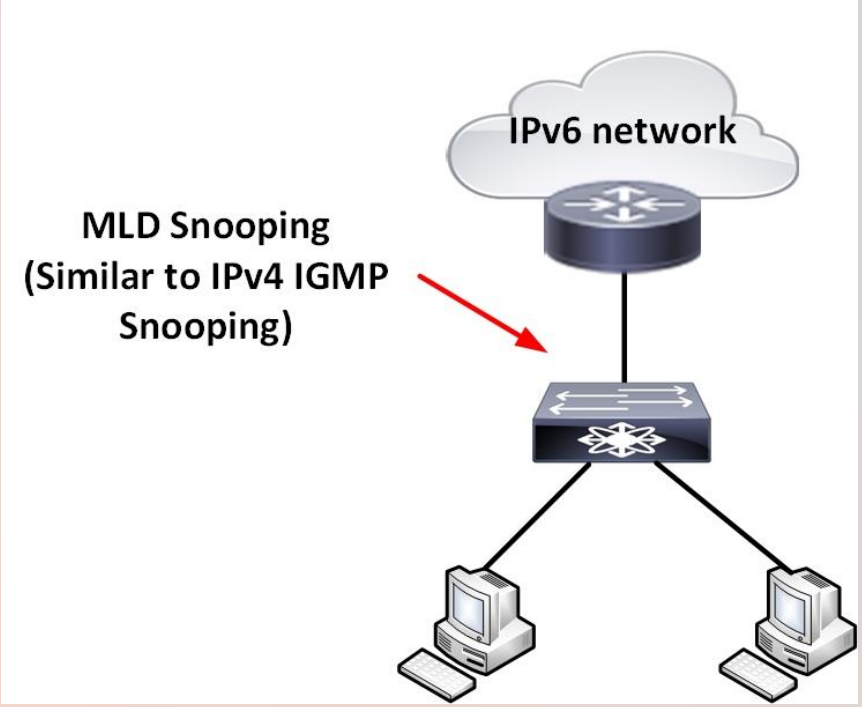
IPv6 Multicast

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

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)



IPv6 Security

IPv6 Security

- Most of the IPv6 attacks are similar to IPv4
- Application Layer Attacks, Roque devices in the network such as DHCP server, Man-in-the-Middle Attacks (MITM) , sniffing etc.
- The mechanism which is used to prevent this attacks in IPv6 are used to protect IPv6 as well

IPv6 Security – IPSEC

- IPSEC can encrypt IPv6 packets similar to IPv4
- Network engineers believe that IPSEC usage is mandatory in IPv6 but this is not true
- Original IPv6 RFC mandated IPv6 implementation to support IPSEC, implementation means, code has to support but usage by network administrators is not mandatory

IPv6 Security – IPSEC

- For many reason IPSEC may not be wanted to be used, for example it prevents network telemetry information so monitoring of the flows would be impossible, thus newer RFC recommendation is : IPSEC should be supported by all IPv6 nodes (Not must)

- IPSEC still can be used for site to site or remote access based VPN purposes

IPv6 Security – Routing Security

- Preventing IPv6 Routing Attacks is important as IPv4 counter part
- MD5 authentication for BGP , IS-IS and EIGRP is still supported in IPv6
- Beware that OSPFv3 removed MD5 authentication but replaced with transport mode IPSEC
- Thus use MD5 to authenticate neighbors in EIGRP , IS-IS and BGP and use IPSEC to secure OSPFv3

IPv6 Security – ARP Spoofing

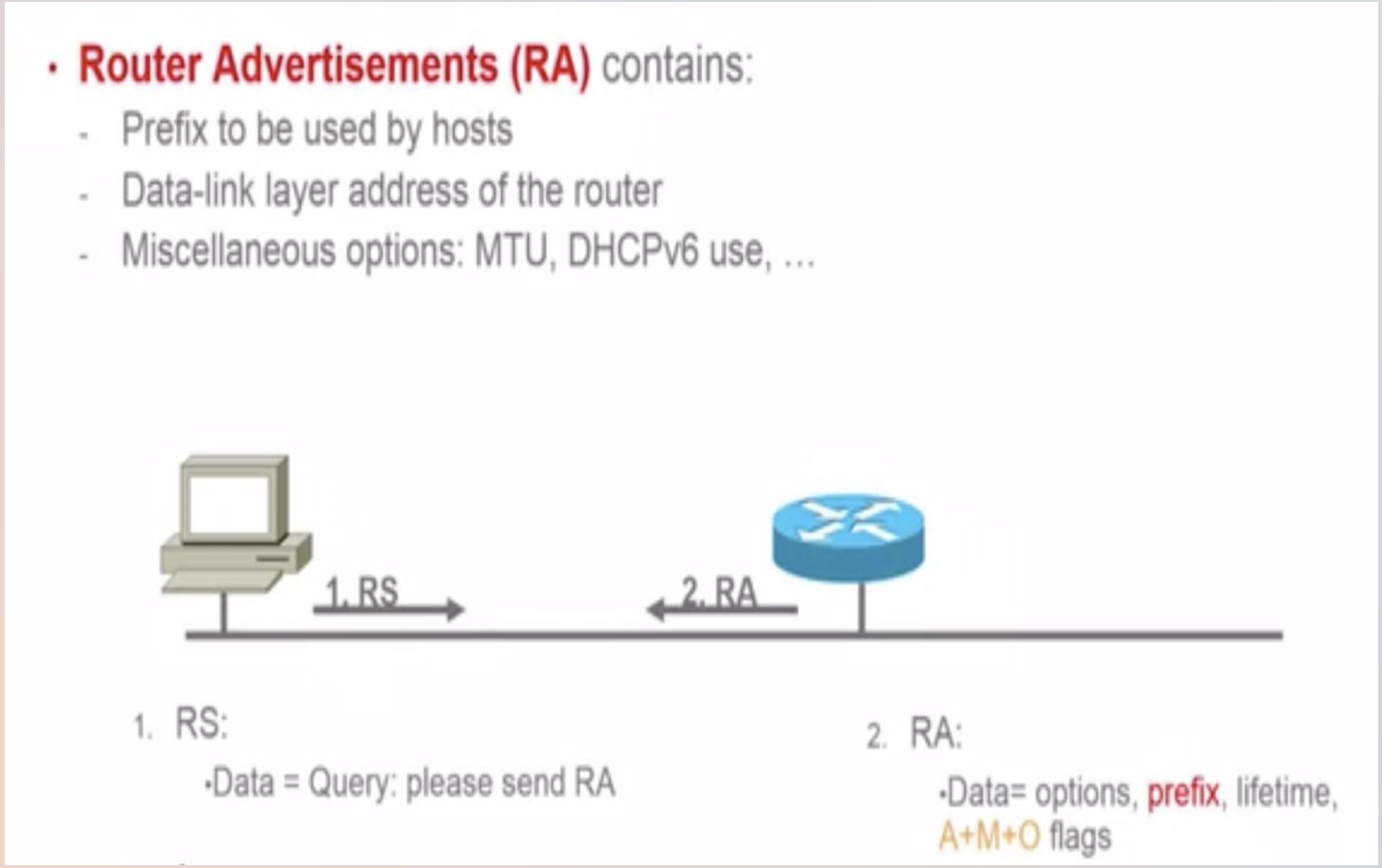
- ARP Spoofing is possible with IPv6 as well , prevention mechanism such as NDP which is similar to DHCP snooping is available

- Also some platforms have SEND technology , SEND is encrypting NDP packets

IPv6 Security – Roque RA (Router Advertisement)

- In an IPv6 deployment, routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network

- ”RA guard feature” protect malicious attacks against Roque RA



IPv6 Security – Roque RA (Router Advertisement)

- RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses
- To protect your network from rogue RAs, a device may implement RA Guard , a feature similar to DHCP Snooping
- RA Guard will only forward RAs, if they are received on a port known to be connected to an authorized router. Additional filtering may happen based on the MAC address of the router.

IPv6 Security – IPv6 Privacy Extensions

- One of the ways of assigning IPv6 address is Stateless Address Autoconfiguration(SLAAC) as it was explained earlier

- SLAAC works by combining part of the address from an interface's gateway, learned via Router Advertisements(RAs), and an interface's layer 2 address with "ff:fe" shoved in the middle of it

IPv6 Security – IPv6 Privacy Extensions

- If your operator is using SLAAC then you can be tracked using the last 48 bits of your IPv6 address because it’s unique

- Websites that you visit can see that you have a new IP address, because you have roamed to a new operator, they can also see that the last 48 bits of the address stay the same every time. Hence, every website you visit will know your device regardless of what network you’re on. You can be easily tracked across providers

IPv6 Security – IPv6 Privacy Extensions

- This problem was resolved by issuing an update to the SLAAC protocol called “Privacy Extensions for Stateless Address Autoconfiguration in IPv6”, which is defined in RFC 4941

- Basically, your computer’s Ethernet interface no longer uses its MAC to fill in the last 48 of its IPv6 address. Instead it picks a series of bits randomly, and fills in the last 48 bits with the random bits.

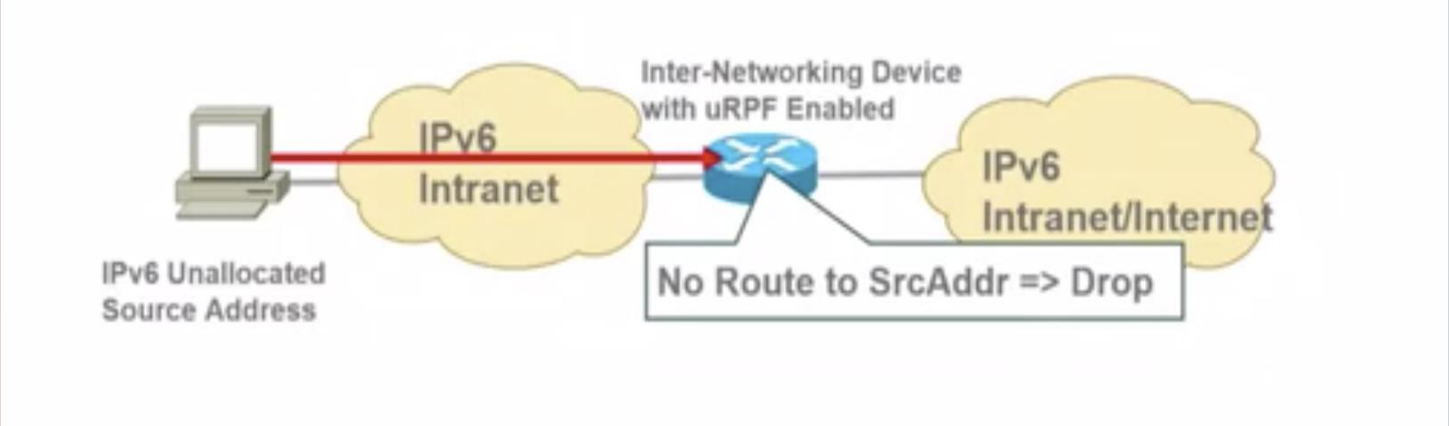
IPv6 Security – IPv6 Privacy Extensions

- But sometimes tracking might be required internally in the inside network , for example for troubleshooting or logging purposes

- Thus the recommendation for the Privacy extension is, use it for the external communication but not for internal network

IPv6 Security – Anti Spoofing

- IP address spoofing is possible with IPv6 as well
- Similar to IPv4, uRPF is the method to prevent spoofing



IPv6 Security - uRPF

- uRPF is Unicast Reverse Path Forwarding (Not Filtering☺) is defined in RFC 3704

- It is designed to limit the impact of DDOS attacks, by denying traffic with spoofed addresses access to the network

IPv6 Security - uRPF

- Routers make their forwarding decisions based on Destination IP Address
- With uRPF, router looks at the Source IP address as well
- There are four types of uRPF : Strict, Loose , Feasible Path and VRF mode

IPv6 Security - Strict and Loose Mode uRPF

- Routers look at Source IP and then the Routing Table
- If source is reachable via the input interface , then it is forwarded, otherwise packet is dropped , this mode is called Strict mode uRPF
- If source is reachable via any route in the routing table then it is forwarded, otherwise packet is dropped, this mode is called Loose mode uRPF

IPv6 Security - Strict and Loose Mode uRPF

- uRPF Strict mode is generally used for Single Homed Customers

- For Multihomed customers, traffic can come from different interfaces, thus uRPF Loose mode should be used

IPv6 Security - RTBH (Remotely Triggered Blackholing)

- Remotely triggered blackholing is used for DDOS prevention for a long time
- DDOS attacks have an economical impact
- According to NBC News article, More than 40% of DDOS Attacks cost $1 million per day

IPv6 Security - RTBH (Remotely Triggered Blackholing)

- Remote Triggered Blackhole is a technique which is used to mitigate DDOS attack dynamically
- Before RTBH, customer used to call Operator when there is an attack, Operator NOC engineer used to connect to the attacked network, trace the source of the attack, place the filters accordingly and attack goes away
- Manual operation is open to configuration mistakes, cannot scale in large networks and between the attack and the required action, services stay down

IPv6 Security - RTBH (Remotely Triggered Blackholing)

There are two types of RTBH

- Destination based RTBH
- Source based RTBH

IPv6 Security - Destination Based RTBH (Remotely Triggered Blackholing)

- First RTBH idea was Destination based RTBH

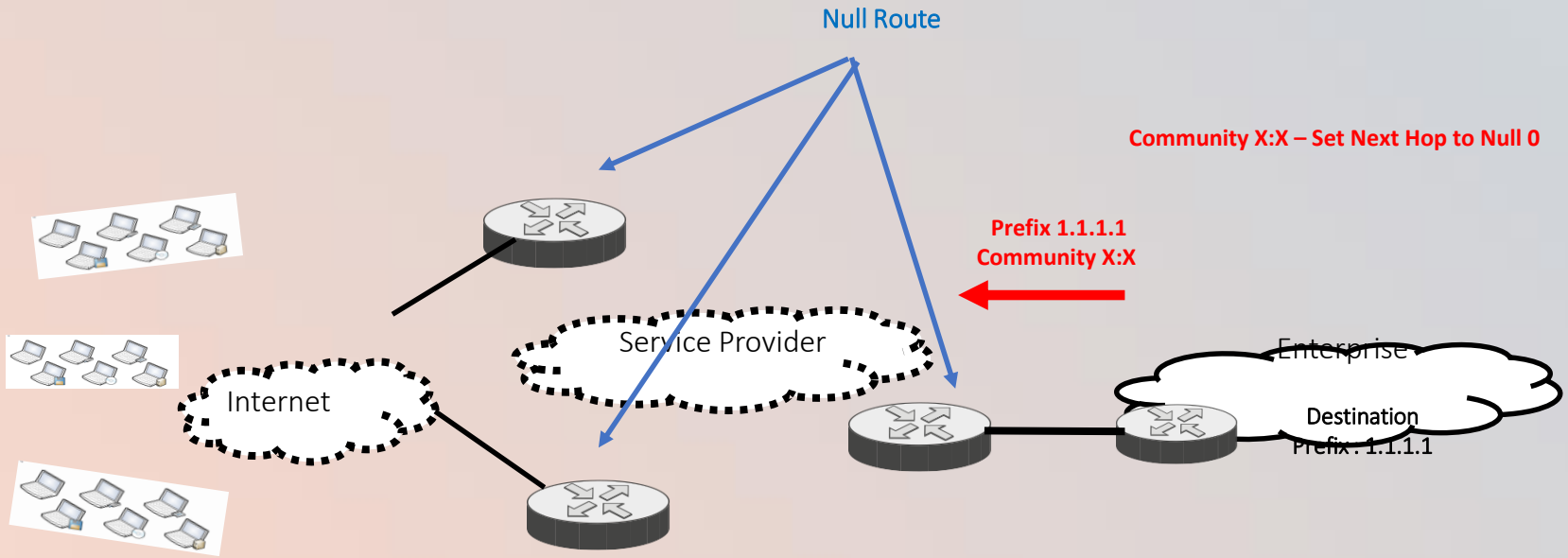
- With this technique, SP and the Customer agree on the discard community

IPv6 Security - Destination Based RTBH (Remotely Triggered Blackholing)

- When there is an attack to the server, victim (customer) send the server prefix with the previously agreed community value

- When SP receives the update with that community, action is set to next hop to null, so packet is dropped before reaching to the customer link

IPv6 Security - Destination Based RTBH (Remotely Triggered Blackholing)



IPv6 Security - Destination Based RTBH (Remotely Triggered Blackholing)

- Problem with this attack, server will not be reachable from the legitimate sources too
- Attack is completed but at least the other services might stay up
- Also customer might change the IP address of the attacked server in DNS, which might take time to propagate this though

IPv6 Security - Destination Based RTBH (Remotely Triggered Blackholing)

- RFC 3882 covers Destination based RTBH
- Better than manual processing
- Requires pre-configuration of null route on all edge routers in the SP network

IPv6 Security - Source Based RTBH (Remotely Triggered Blackholing)

- RFC 5635 brings the idea of Source RTBH
- Instead of customer specifying the attacked system IP address to the SP, customer calls SP that they are under attack
- By combining uRPF and discard route (null route) configuration, based on the attack source, DDOS is mitigated (In theory)

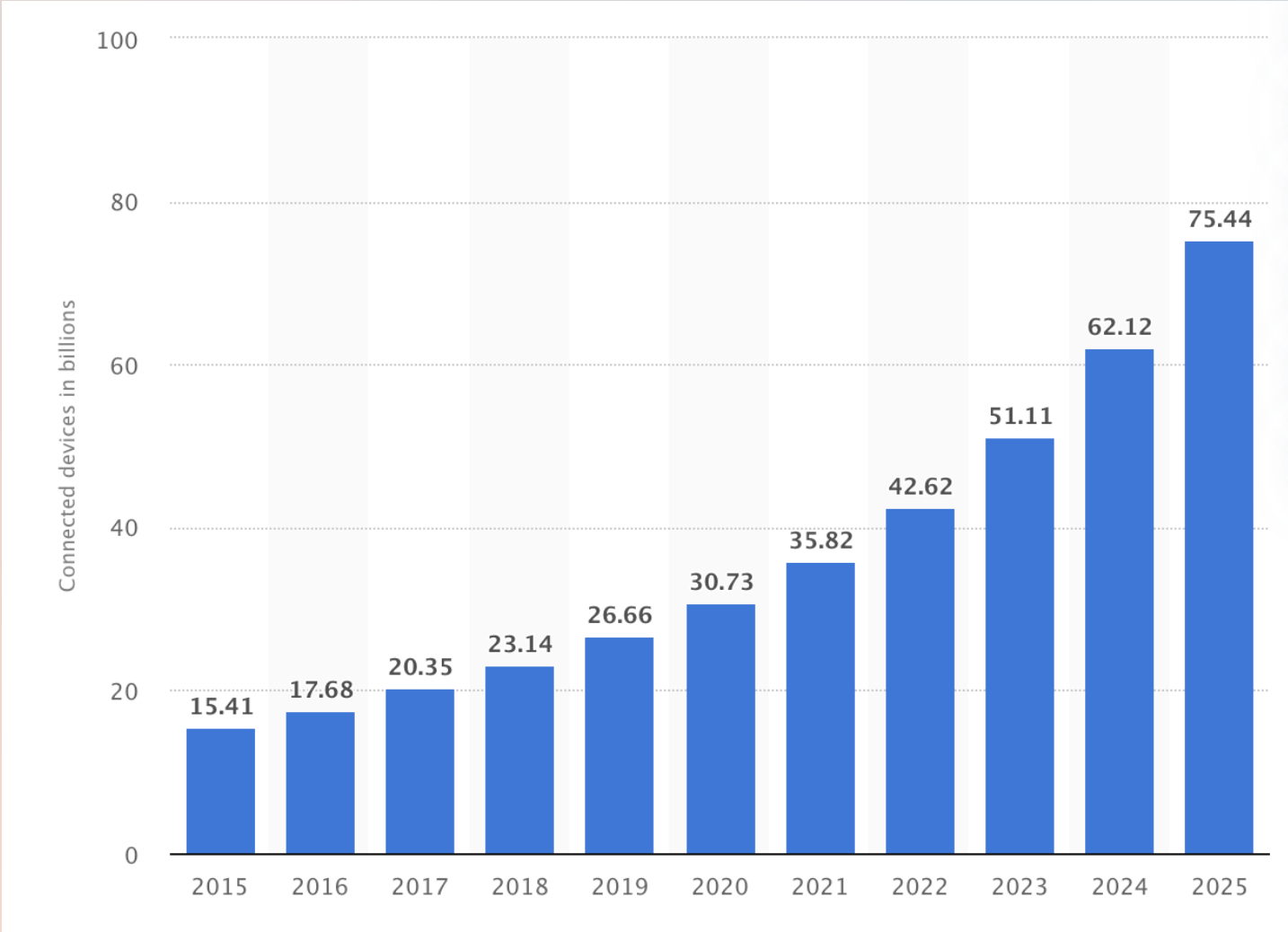
IPv6 in Internet of Things (IOT)

IPv6 in Internet of Things (IoT)

- The IoT describes the network of devices that are connected via the Internet.

- Being connected, such smart devices, which include smart home devices such as smart meters and smart locks, are able to share data among each other, providing benefits such as better quality of life and greater insight into business.

IPv6 in Internet of Things (IoT) – Number of Expected IOT Devices

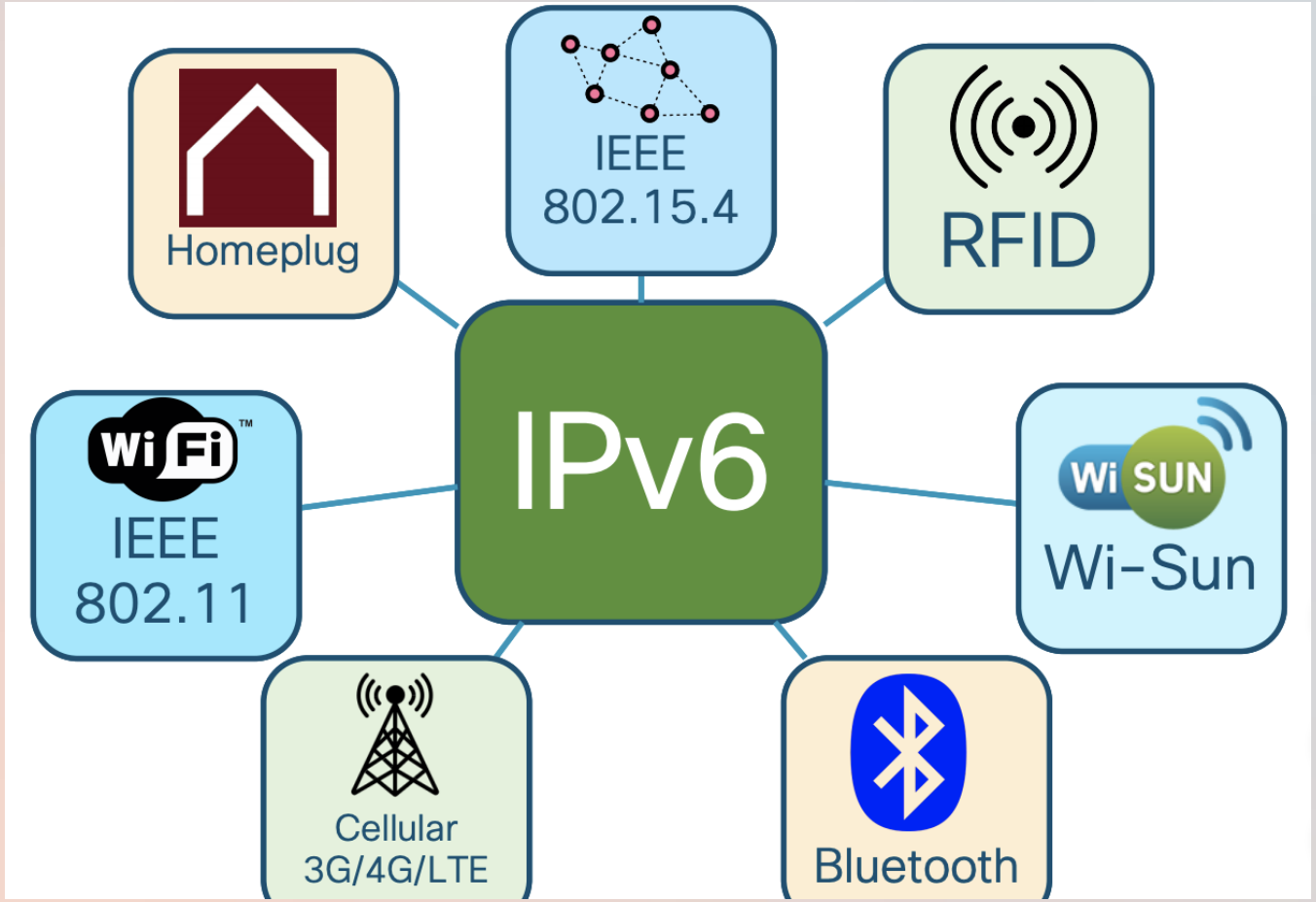


IPv6 in Internet of Things (IoT)

- IoT devices and smart objects can connect using a myriad of protocols that do not directly “talk” to one another

- IPv6 has become the common thread that allows for the interoperability of IoT devices using different connectivity (link layer) protocols

IPv6 in Internet of Things (IOT)



Reasons to have IPv6 in IOT Networks

- Depends on the application of IOT , range , power requirement , amount of data being transferred , bandwidth, reliability of the protocols are chosen.

- Some protocols may work with IP address , some doesn’t require IP address or routing protocol (For example LORA/LORAWAN doesn’t require IP Address or any routing protocol to establish topology)

Reasons to have IPv6 in IOT Networks

- IPv6 supports around 340 undecillion addresses or 340 trillion trillion trillion, which is enough to give universally unique IP addresses to each IoT device. Thus, scalability is one reason why IPv6 would be better for IOT networks

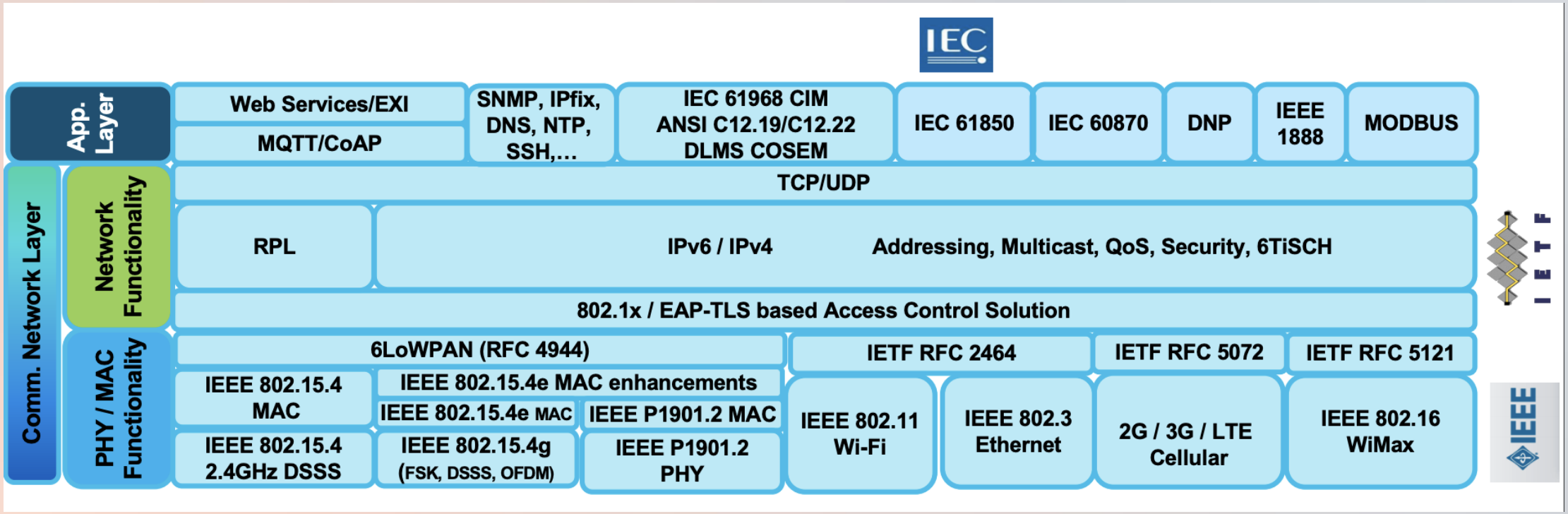
- With IPv6, investment in NAT is not necessary, each node can have GUA, without NAT they can communicate with IOT Cloud (Internet)

Reasons to have IPv6 in IOT Networks

- IPv6 allows IoT products to be uniquely addressable without having to work around all of the traditional NAT and firewall issues.

- Larger and more advanced host devices have all sorts of tools to make working with firewalls and NAT routers easier, but small IoT endpoints do not.

IPv6 in IOT - IoT Use of Open Standards



IPv6 in Internet of Things (IOT) – 6LOWPAN

- Generally, two main categories of networks are deployed in the IoT: short-range and long-range, low-power networks

- The short-range, low-power networks, sometimes called ‘last 100 meters of connectivity’ represent a large fraction of the potential number of things, e.g. IPv6 over low-power wireless personal area networks (6LoWPAN), radio frequency identification (RFID), near-field communication (NFC) and Bluetooth low energy (BLE)

IPv6 in Internet of Things (IOT) – 6LOWPAN

- IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) defines the transmission of IPv6 over IEEE 802.15.4 (RFC 4944)

- 6LOWPAN is an Adaption Layer and has two major function to enable usage of IPv6 over 802.15.4 based IOT networks
  - Fragmentation and Header Compression

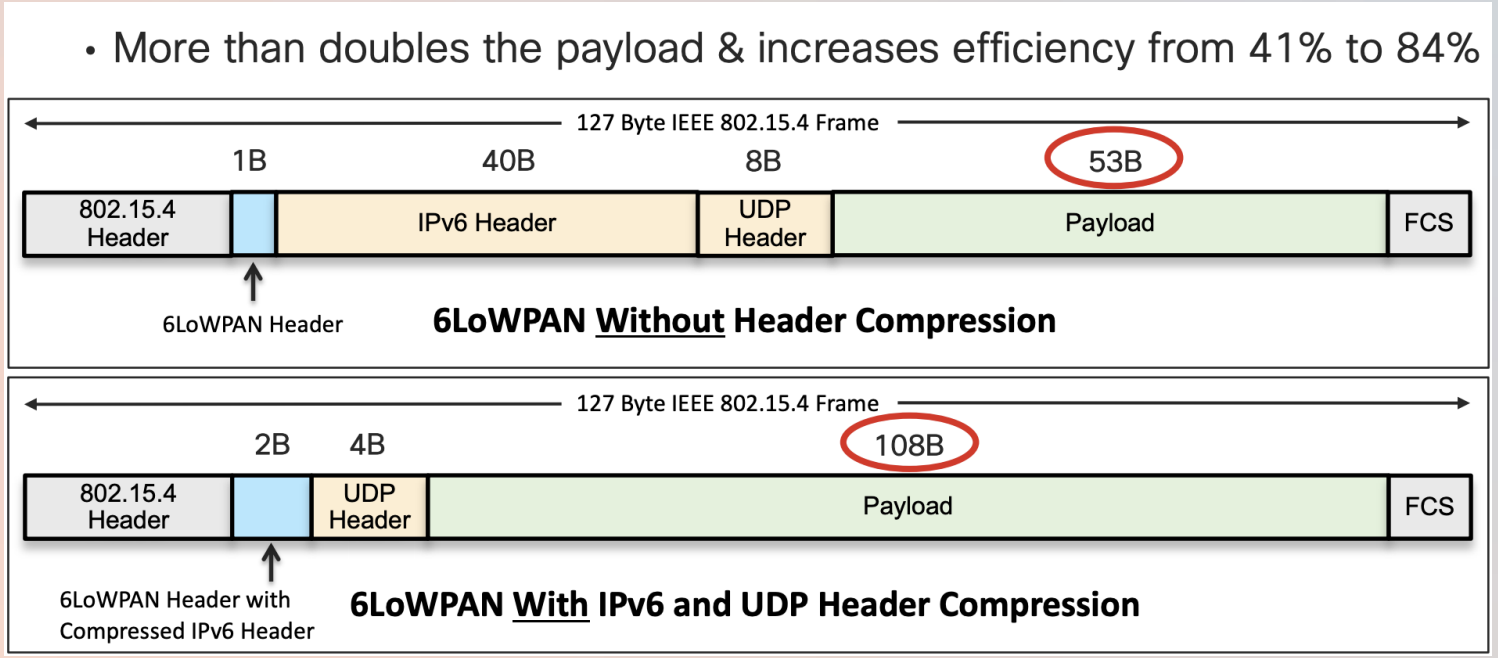
IPv6 in Internet of Things (IOT) – 6LOWPAN

- IEEE 802.15.4 has an MTU of only 127 bytes!

- But IPv6 minimum MTU is 1280 byte, 1280 byte IPv6 packet cannot fit in 127 byte 802.15.4 based 6LOWPAN packets, thus IPv6 packet is fragmented

IPv6 in Internet of Things (IOT)

- Also, IPv6 header size is 40 Byte and without header compression, this occupies big amount of portion of 6LOWPAN packets



IPv6 in Internet of Things (IOT) – 6LOWPAN

- The 6LoWPAN network architecture contains three elements: host node, router node and edge router

- The hosts can sense the physical environment and actuate devices
-
- The routers are intermediate nodes that forward data packets from the hosts to the edge routers or to a destination inside the 6LoWPAN network.

IPv6 in Internet of Things (IOT) – 6LOWPAN

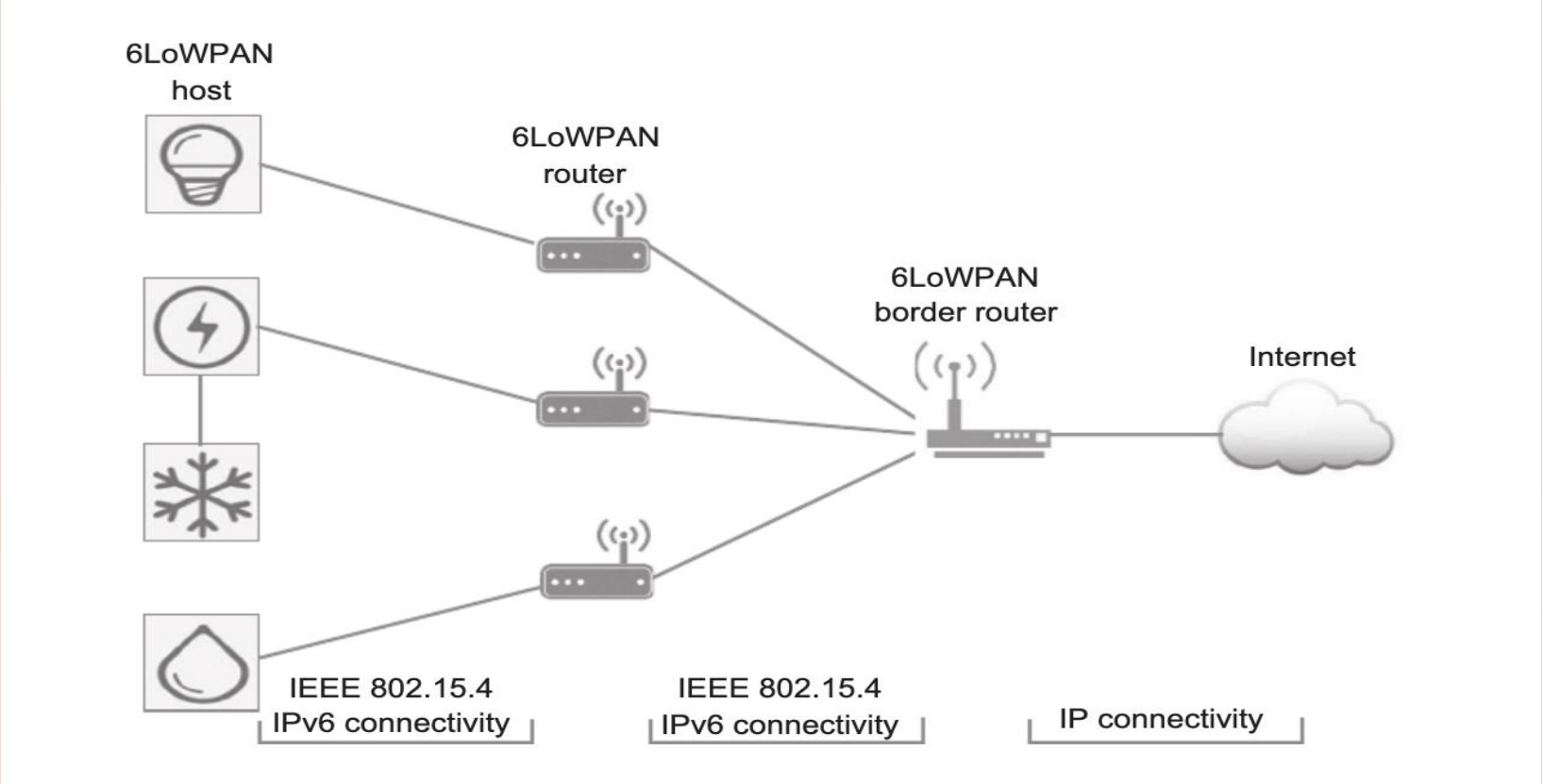
- The connection among 6LoWPAN elements is implemented via IPv6 over IEEE 802.15.4

- The edge routers provide interconnection and traffic management (e.g. Neighbor Discovery (ND) and handling IPv6 interconnectivity) between 6LoWPAN network and other IP networks (typically the Internet)

IPv6 in Internet of Things (IOT) – 6LOWPAN

- Sending and receiving packets between 6LoWPAN elements and IP nodes in other networks occur in an end-to-end scheme similar to any IP nodes where each 6LoWPAN element is identified by a unique IPv6 address

IPv6 in Internet of Things (IOT) – 6LOWPAN Network Architecture



6LOWPAN Network Architecture

IPv6 in Internet of Things (IOT) – 6LOWPAN

- Generally, routing protocols in 6LoWPAN can be divided into two categories: ‘mesh-under’ and ‘route-over’

- With the mesh-under scheme, the adaptation layer performs the packet routing and forwarding over multiple hops based on the 6LoWPAN header or the IEEE 802.15.4 link layer address.

IPv6 in Internet of Things (IOT)

- In the route-over, all routing decisions are taken in the network layer and packets are forwarded to the final destination using IPv6 addresses.

- One of the important routing protocols for 6LoWPAN networks is the IPv6 routing protocol for low-power and lossy networks (RPL) which was developed by the RoLL working group to meet the requirements and challenges of low-power and lossy networks (LLNs)

IPv6 in Internet of Things (IOT) – RPL (Routing over Low Power and Lossy Links)

- RPL is a distance vector routing protocol which organizes the network as a Directed Acyclic Graph (DAG) routed at the IOT Gateway/Sink

- It constructs the network topology by using an objective function which defines how routing metrics are computed to obtain a Rank value

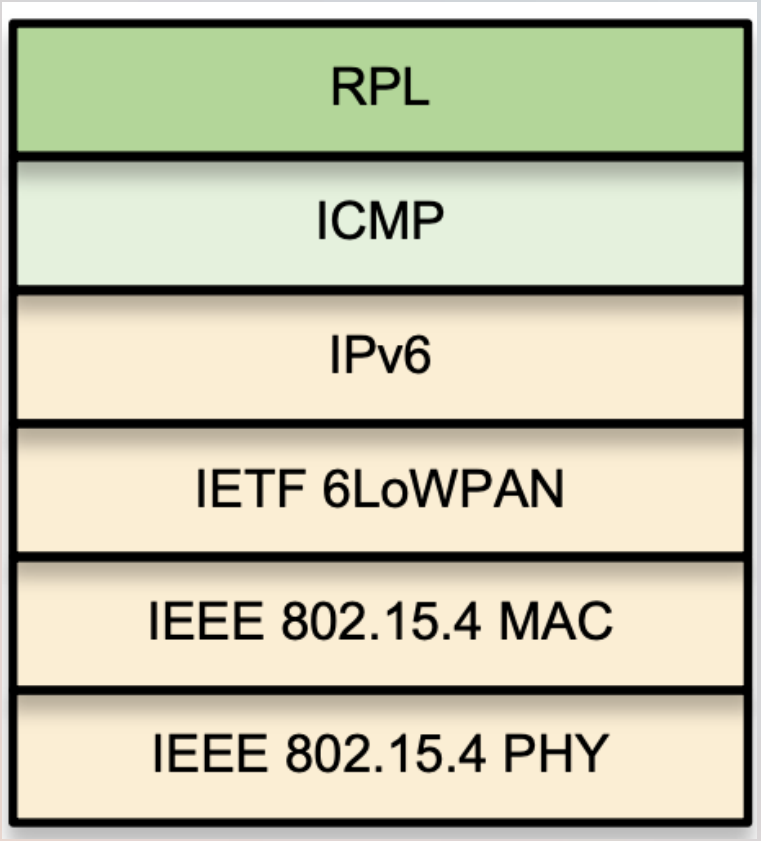
IPv6 in Internet of Things (IOT) – RPL (Routing over Low Power and Lossy Links)

- The Rank value represents a nodes' position in the graph and the node selects its parent based on the Rank. RPL is expected to be the standard routing protocol for 6LoWPAN networks

IPv6 in Internet of Things (IOT) – RPL (Routing over Low Power and Lossy Links)

Existing IP routing protocols are poorly suited for IoT :

1. Lossy connections and will lose state too easily
2. Only consider link cost, not node type or other constraints
3. Lack of routing flexibility when different objective functions are required



Routing over Low Power Lossy Networks (RPL)

- Existing IP routing protocols are poorly suited for IOT
  - Lossy connections, thus routing churn
  - They only consider link cost (Bandwidth and Delay Staticly) not other type of constraints
  - When different objective functions exist lack of flexibility

Routing over Low Power Lossy Networks (RPL)

- RFC 6550 defines RPL : IPV6 Routing protocol for Low Power and Lossy Networks

- RPL is a Distance Vector Routing Protocol
  - New routing attributes (Objective Functions) : Energy, Latency , Link Reliability (ETX Value) , link color etc.

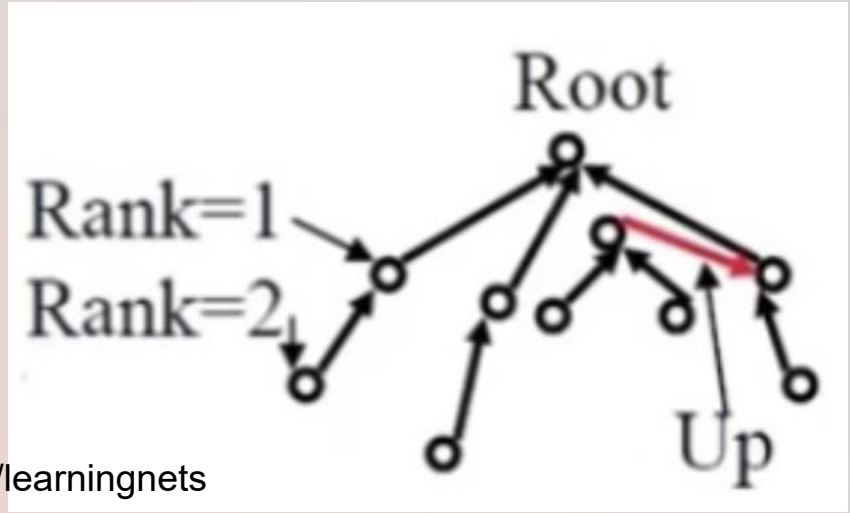
Routing over Low Power Lossy Networks (RPL)

- RPL can run op top of IEEE 802.15.4 , BLE etc.

- With RPL, routing is based on Destination Oriented Directed Acyclic Graph (DODAG)

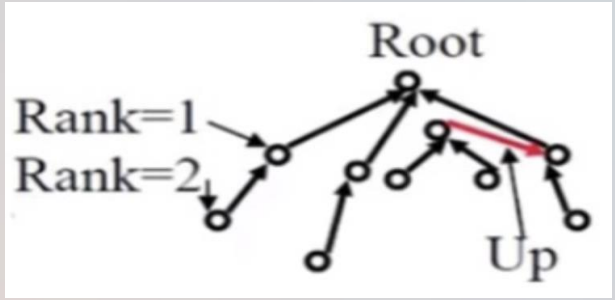
Routing over Low Power Lossy Networks (RPL) – Terminology

- Directed Acyclic Graph: It is a spanning tree without cycle
- Root: Destination of the nodes in DAG
- Up: it is any edge that is directed towards to the root
- Down: It is any edge that is directed away the root

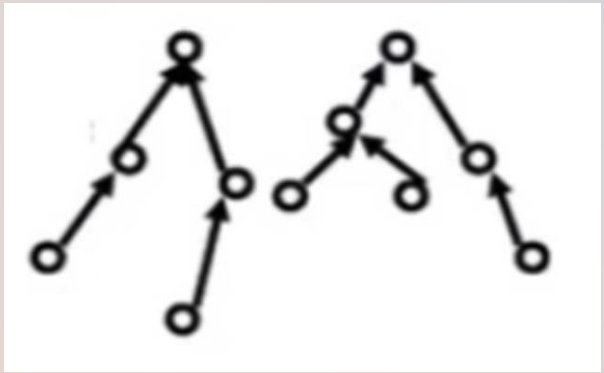


Routing over Low Power Lossy Networks (RPL) – Terminology

- DODAG: Special kind of DAG where each node wants to reach a single destination
- Objective Function: This can be energy, latency, reliability etc. Minimum objective function path is considered as best
- Rank: It is the distance from the root
- RPL instance: When there is one or more DODAG, each DODAG is an instance



RANK

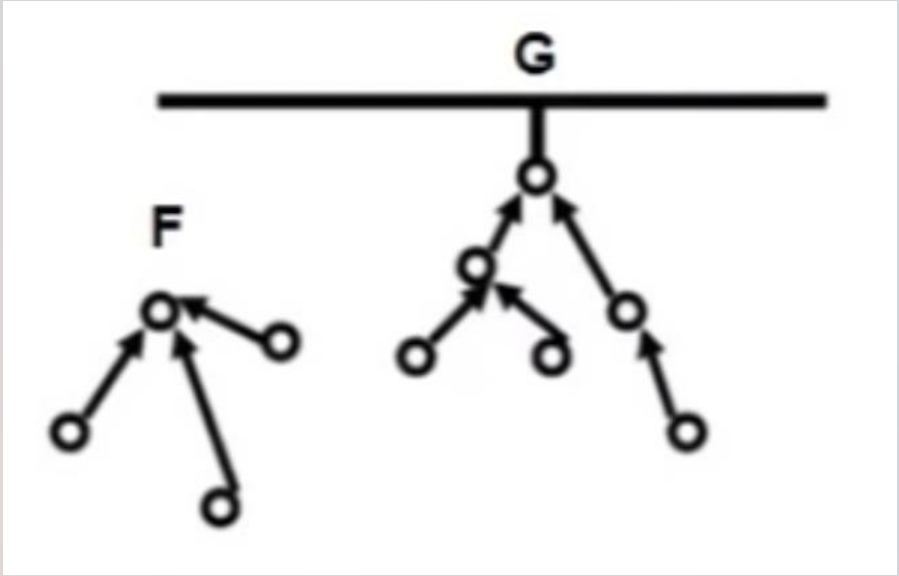


Two Root, Two DODAG
Thus, Two RPL Instances

Routing over Low Power Lossy Networks (RPL) – Terminology

- Grounded: When DODAG reaches it to the Root it is considered as Grounded, through root is connected to backhaul network

- Floating : When a DODAG isn't connected to backhaul via Root, it is Floating DODAG

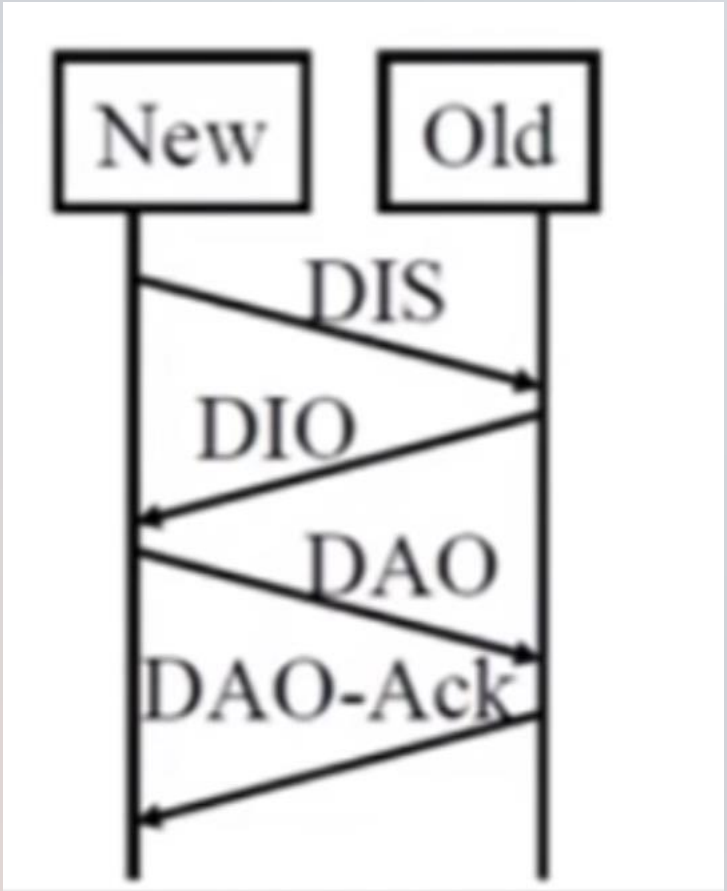


Routing over Low Power Lossy Networks (RPL) – Terminology

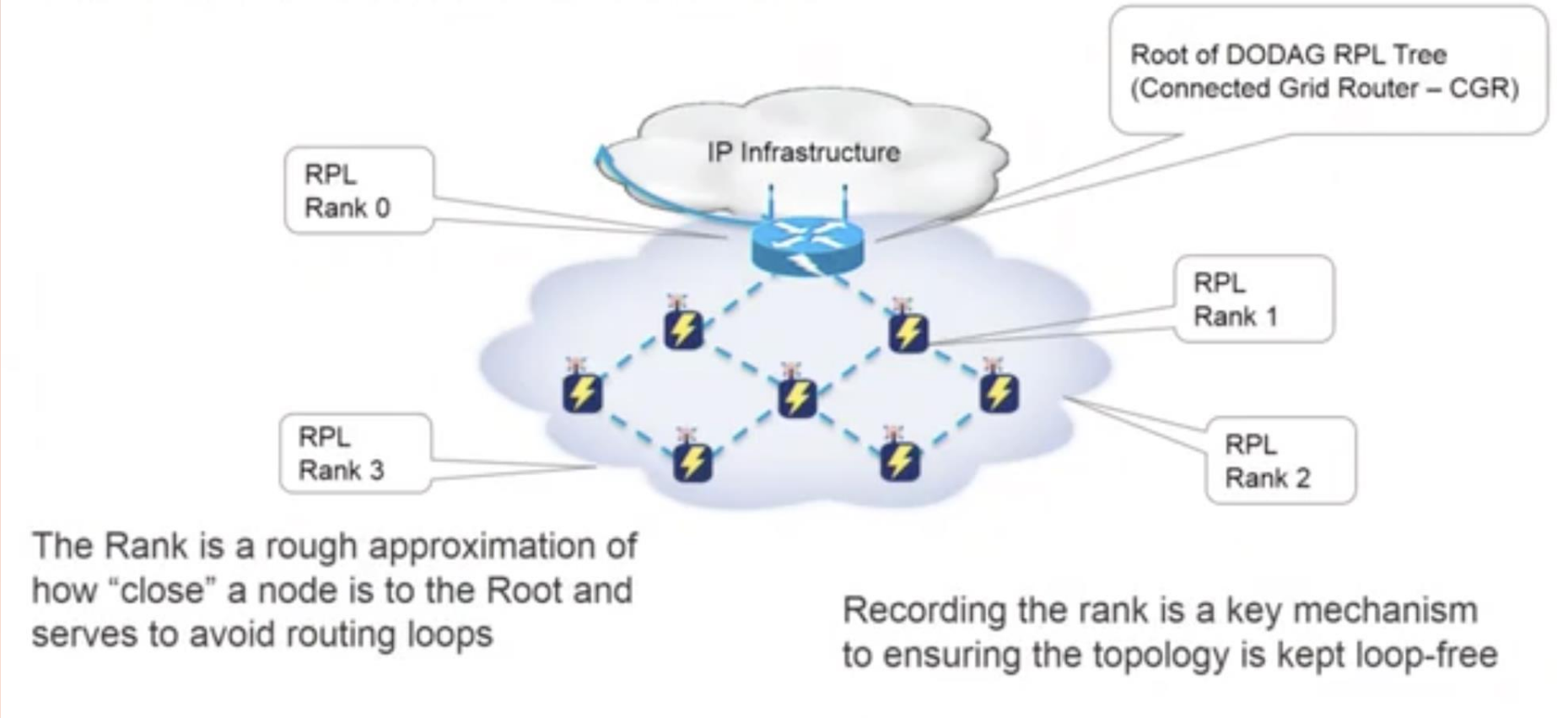
- Parent: where the arrow is pointing towards, child is where the arrow comes from. Parents can have multiple children and children can have multiple parents
- Sub-DODAG : It is any subtree of a given DODAG
- Storing Node : Keeps whole routing table
- Non-Storing Node : Keeps routing info only about their parent
- Note: Root is always storing node !

IPV6 Routing Protocol RPL Control Plane Messages

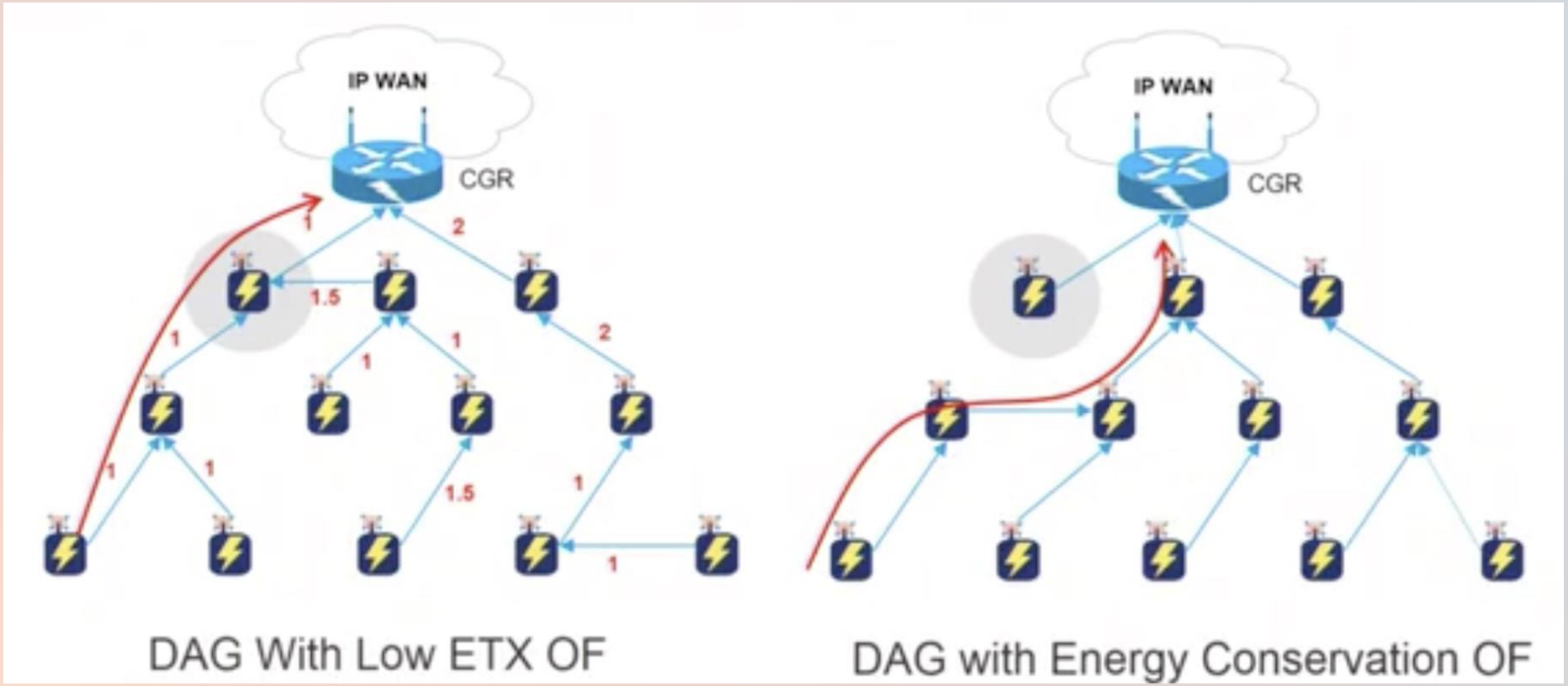
- DIS : DODAG Information Solicitation: When node first initialize, send this message to tell others if any DODAG exists or not
- DIO – DODAG Information Object- This message is advertised by any nodes in multicast manner to downstream nodes
- DAO : When DODAG is found, child sends this to parent or to the root to request joining to the DODAG
- DAO-ACK : It is a response by the parent , saying Yes or No



RPL – Cisco CGR as a Root



RPL – Objective Function Example – Cisco



Segment Routing (SRv6)
SR IPv6 Dataplane

Segment Routing (SRv6) – SR IPv6 Dataplane

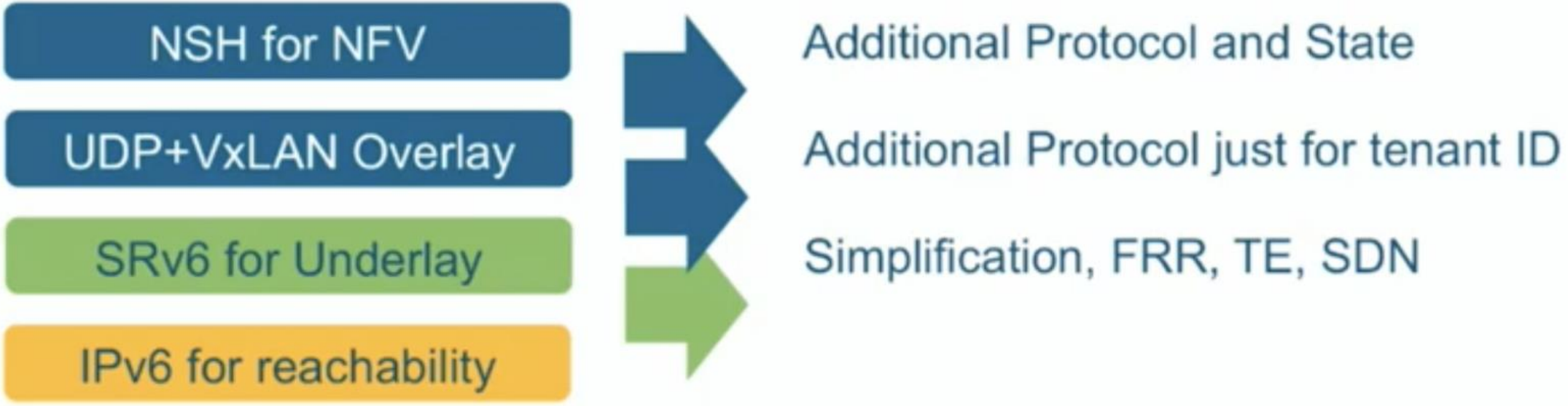
- Segment Routing works based on Source Routing
- Two dataplane is defined for Segment Routing : MPLS andIPv6
- MPLS has been deployed in many networks
- Segment routing is applied to an IPv6 data plane by encoding IPv6 segments into new routing extension header (SRH)

Segment Routing (SRv6) – SR IPv6 Dataplane

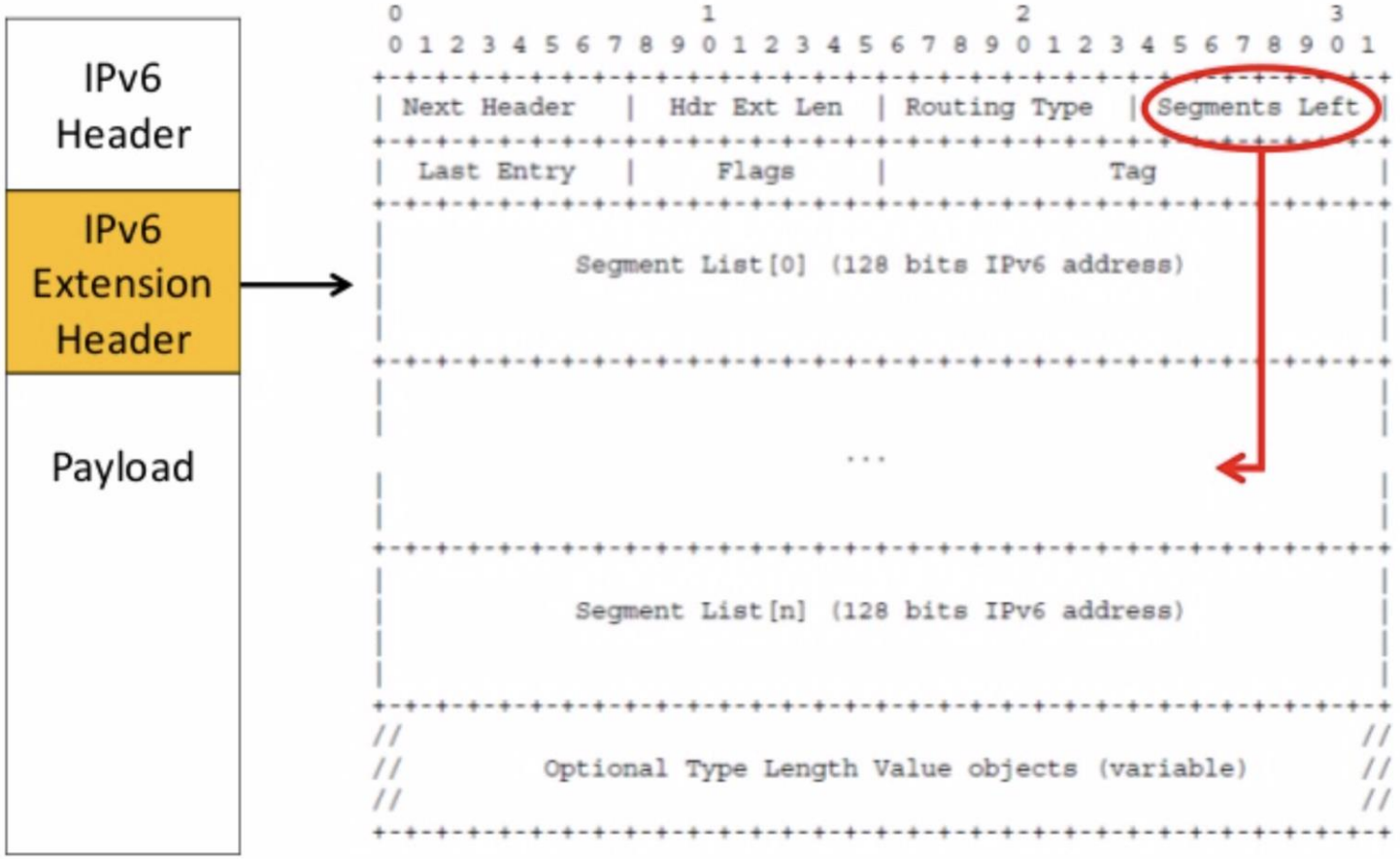
- SR brings Scalability , removes some protocol requirements such as LDP, RSVP , NSH
- Can provide 50msec FRR coverage in any topology with TI-LFA
- Can be used as unified control plane for DC, WAN and Metro Networks
- SR MPLS in DC can be used but generally hosts don’t deploy MPLS, thus SRv6 is seen as better candidate to be deployed towards up to the Host as IPv6 in the host is supported by every vendor

Segment Routing (SRv6) – SR IPv6 Dataplane

- SR MPLS is used for Transport purpose , SRv6 can be used not only for Transport, but also for Service signaling, so much more protocol can be eliminated in the network



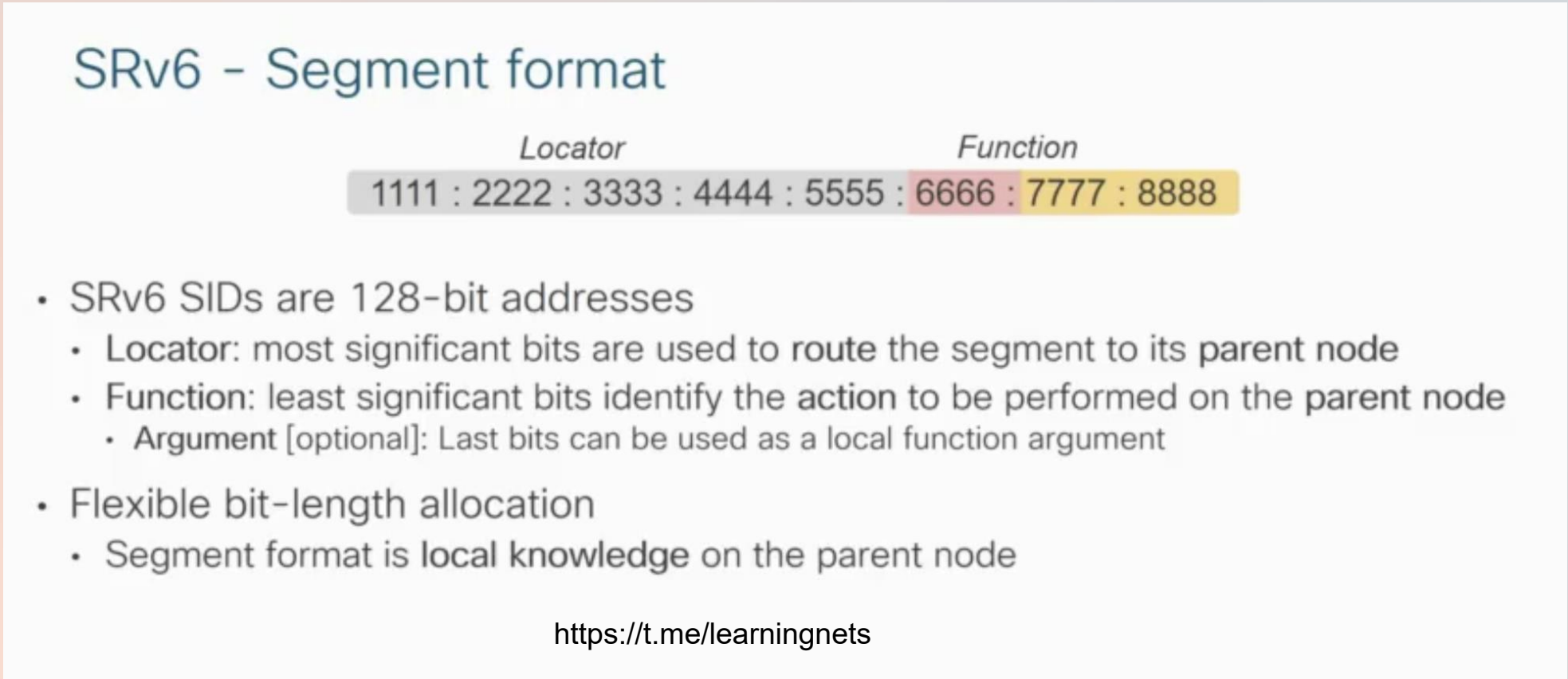
Segment Routing Header in IPv6



- Routing Type
  - 4 (Segment Routing)
- Segments Left
  - Index to the next segment in the Segment List
  - Decremented on Endpoint node
- Last Entry
  - Index to the first segment in the Segment List
- Segment List
  - Encoded starting from the last segment of the path (Segment List [0] contains the last segment)

Segment Routing (SRv6) – SR IPv6 Dataplane

- When SRv6 is deployed, only the nodes that have to process the packet header must have SRv6 dataplane support, all other nodes in the network are just plain IPv6 nodes



Segment Routing (SRv6) – SR IPv6 Dataplane

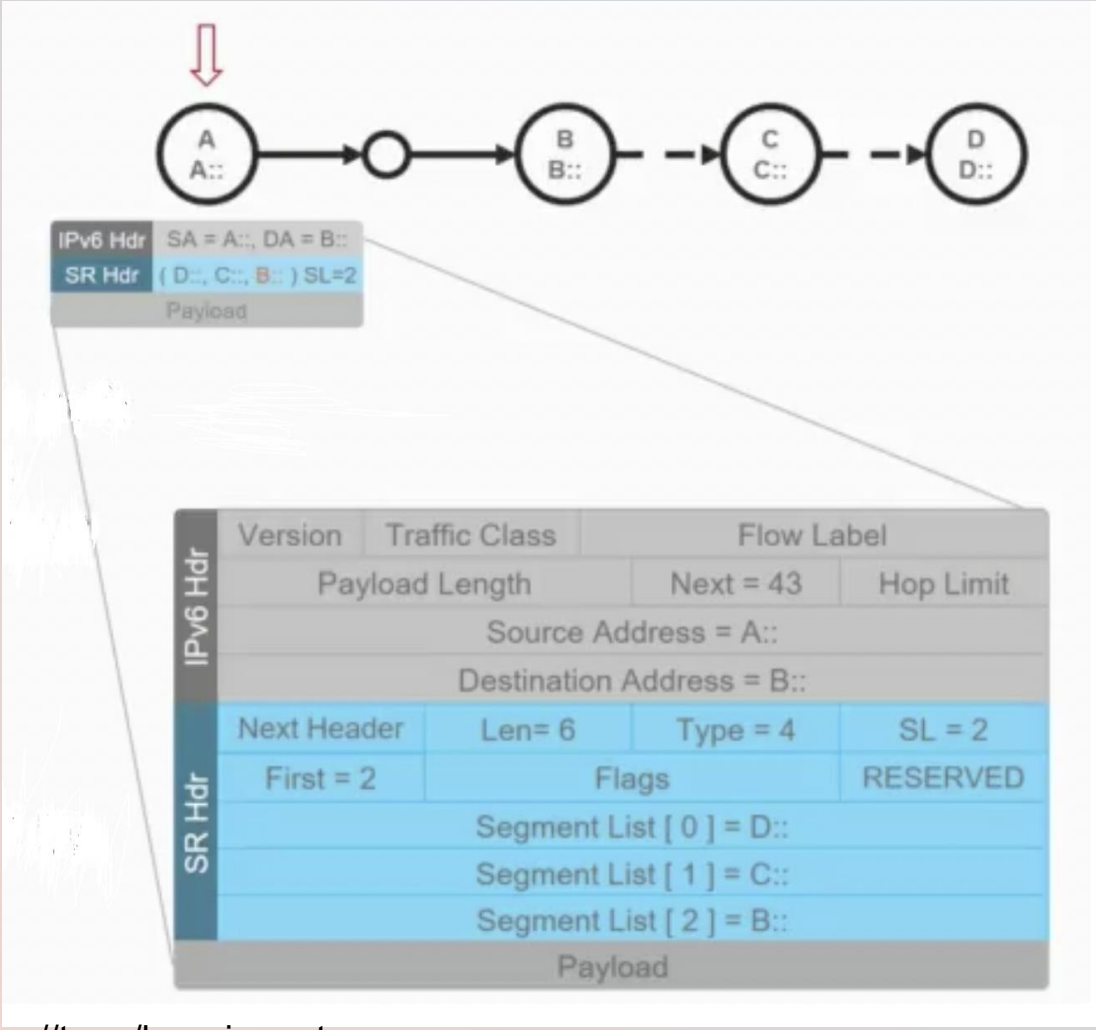
- 128 bit segment ID is broken into three fields: Locator, Function and Arguments
- These represent the forwarding information (Locator) and any actions to be performed at that destination (Function), plus any information required by the individual SID (Arguments)
- The Argument field of the SID could carry the QoS Flow Identifier (QFI), for example

Segment Routing (SRv6) – SR IPv6 Dataplane

- Locator part is routable in an IPv6 network
- Locator information is distributed by IGP and all other nodes install this information to their IPv6 routing table. Even it is not a real address, the other nodes will be able to route packets to the this address (aka SRv6 SID)
- Segment Left (which is decremented at every SRv6 hop) is copied to the IPv6 Destination field, allowing standard routing practices to be applied to SRv6 packets when traversing non-SRv6 capable network elements

Segment Routing (SRv6) – Non-SRv6 Capable Nodes

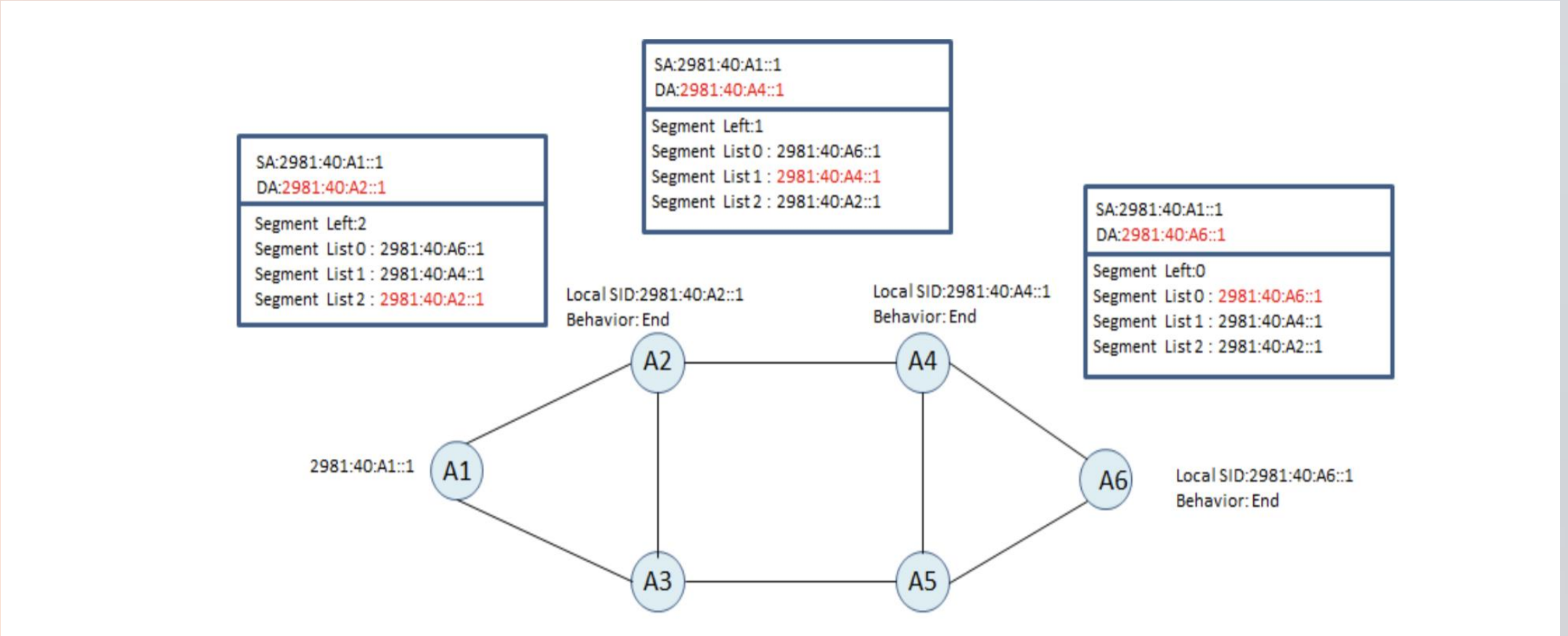
- Non-SRv6 capable nodes just perform IPv6 routing, they don’t have to understand or take any action on SRH



SRv6 Basic Functions - END Function

- This is corresponding to a Node SID in SR-MPLS
- When the node receive the packet with End Function (Function 0) it decrements the Segments Left field, update the Destination Address field in the IPv6 header and forward the packet to next node along the shortest path route (Node SID in SR-MPLS uses shortest path tree as well)
- If Segment Left is 0, it means final node is reached, thus IPv6 and SRH headers are removed and payload is processed

SRv6 Basic Functions - END Function



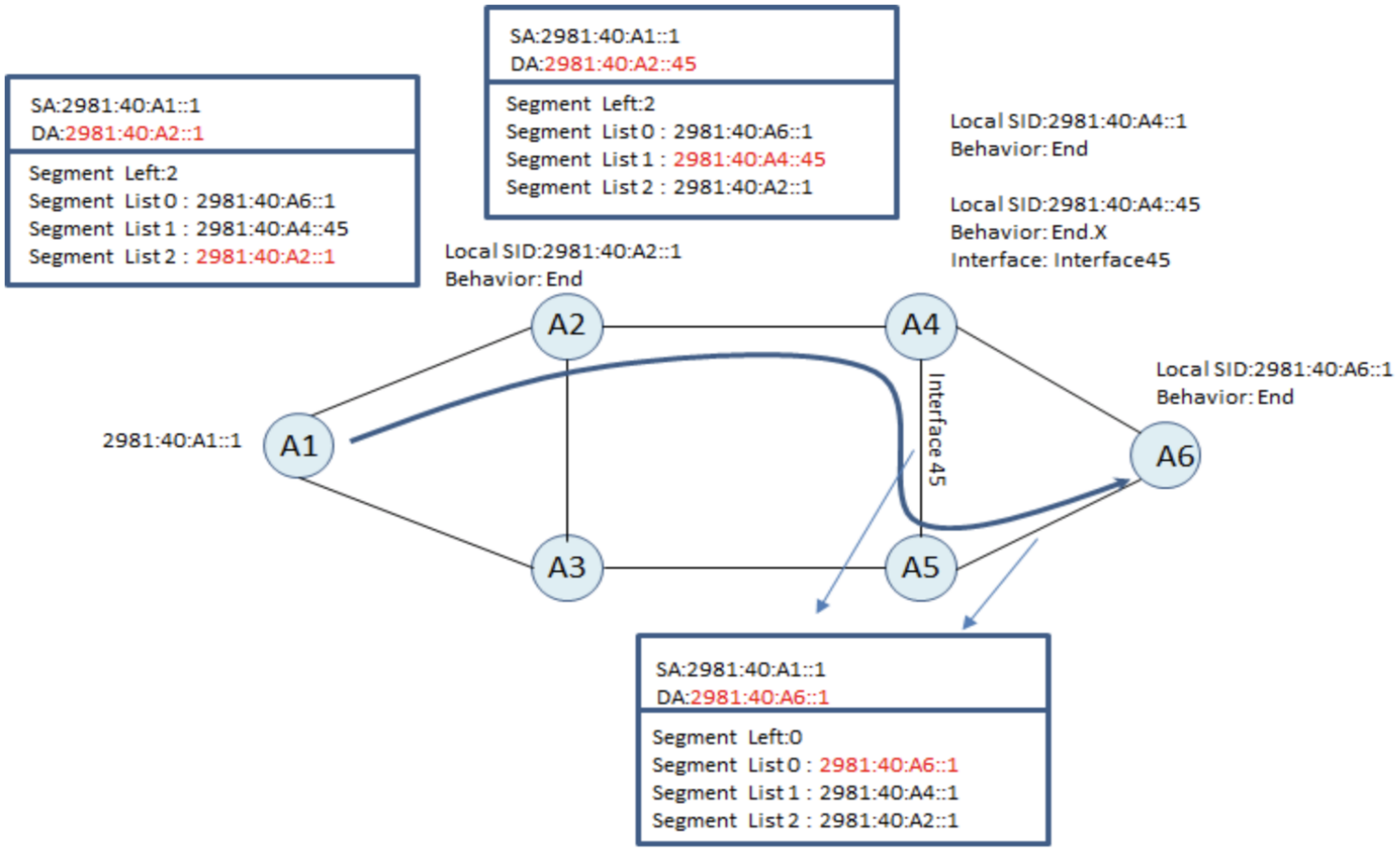
SRv6 Basic Functions - END.X Function

- End.X function is defined locally and it points an outgoing interface. Official definition for End.X function is Endpoint with cross-connect to layer-3 adjacencies

- It is similar to Adjacency-SID in SR-MPLS

- When traffic needs to be pushed to a certain interface, END.X function is used , Example use case for this function is TI-LFA

SRv6 Basic Functions - END.X Function



SRv6 Functions List

Functoins Defined in Net Programming

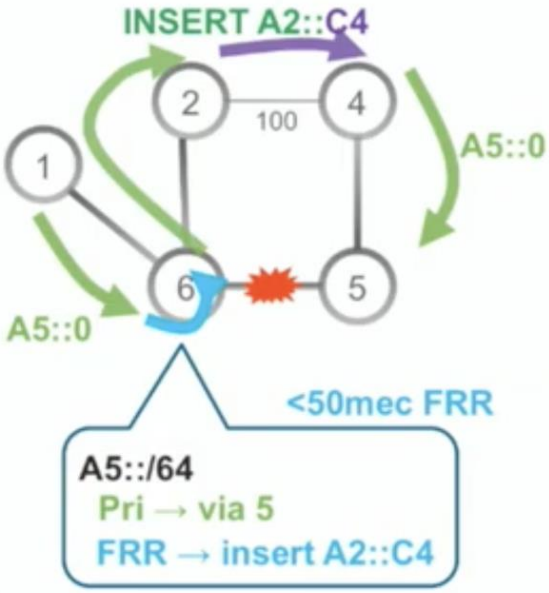
- **End** Endpoint function The SRv6 instantiation of a prefix SID
- **End.X** Endpoint function with Layer-3 cross-connect The SRv6 instantiation of a Adj SID
- **End.T** Endpoint function with specific IPv6 table lookup
- **End.DX2** Endpoint with decapsulation and Layer-2 cross-connect L2VPN use-case
- **End.DX2V** Endpoint with decapsulation and VLAN L2 table lookup EVPN Flexible cross-connect use-cases
- **End.DT2U** Endpoint with decaps and unicast MAC L2 table lookup EVPN Bridging unicast use-cases
- **End.DT2M** Endpoint with decapsulation and L2 table flooding EVPN Bridging BUM use-cases with ESI filtering
- **End.DX6** Endpoint with decapsulation and IPv6 cross-connect IPv6 L3VPN use (equivalent of a per-CE VPN label)
- **End.DX4** Endpoint with decapsulation and IPv4 cross-connect IPv4 L3VPN use (equivalent of a per-CE VPN label)
- **End.DT6** Endpoint with decapsulation and IPv6 table lookup IPv6 L3VPN use (equivalent of a per-VRF VPN label)
- **End.DT4** Endpoint with decapsulation and IPv4 table lookup IPv4 L3VPN use (equivalent of a per-VRF VPN label)
- **End.DT46** Endpoint with decapsulation and IP table lookup IP L3VPN use (equivalent of a per-VRF VPN label)
- **End.B6** Endpoint bound to an SRv6 policy SRv6 instantiation of a Binding SID
- **End.B6.Encaps** Endpoint bound to an SRv6 encapsulation Policy SRv6 instantiation of a Binding SID
- **End.BM** Endpoint bound to an SR-MPLS Policy SRv6/SR-MPLS instantiation of a Binding SID
- **End.S** Endpoint in search of a target in table T

- **T.Insert** Transit behavior with insertion of an SRv6 policy
- **T.Insert.Red** Transit behavior with reduced insert of an SRv6 policy
- **T.Encaps** Transit behavior with encapsulation in an SRv6 policy
- **T.Encaps.Red** Transit behavior with reduced encaps in an SRv6 policy
- **T.Encaps.L2** T.Encaps behavior of the received L2 frame
- **T.Encaps.L2.Red** Transit with reduce encaps of received L2 frame

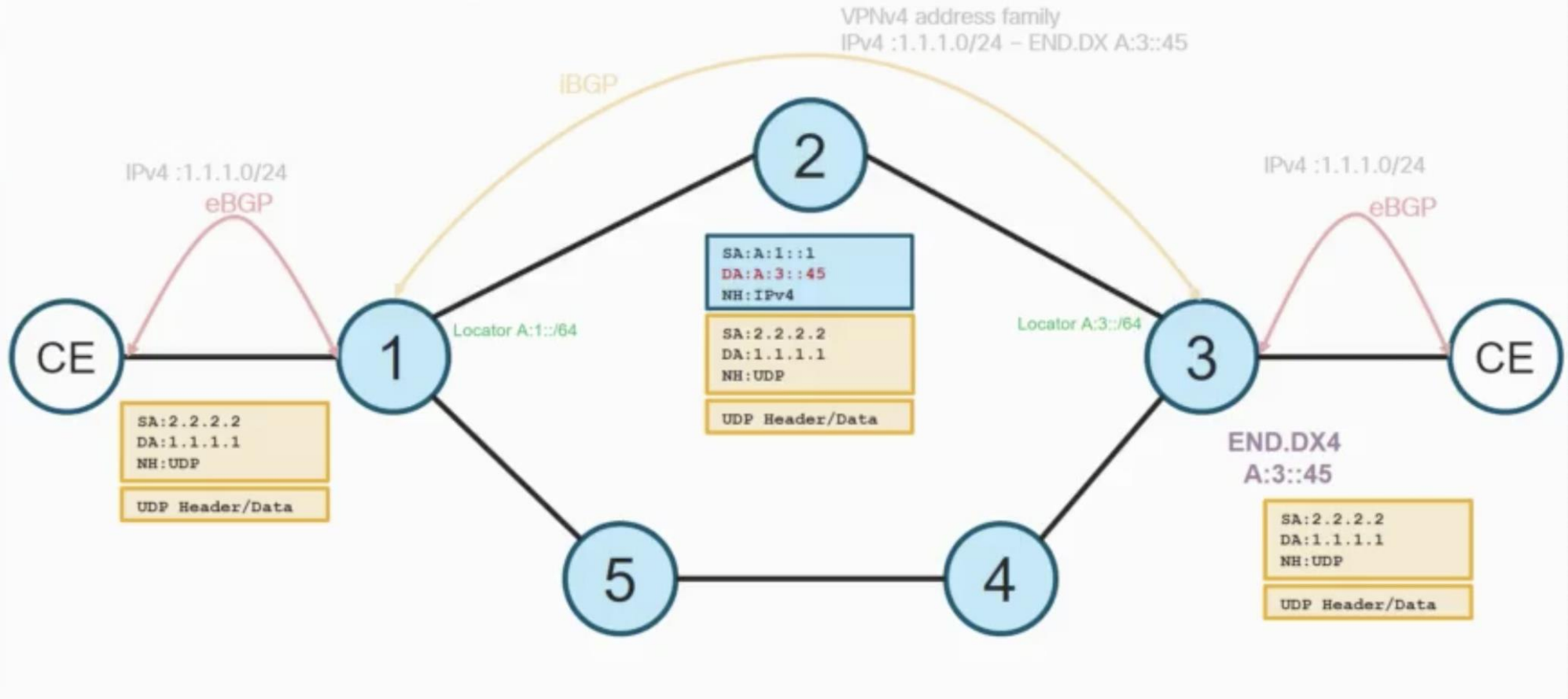
TI-LFA with SRv6 Use Case

TILFA

- 50msec Protection upon
  local link, node or SRLG failure
- Simple to operate and understand
  - automatically computed by the router's IGP process
  - 100% coverage across any topology
  - predictable (backup = post convergence)
- Optimum backup path
  - leverages the post-convergence path, planned to carry the traffic
  - avoid any intermediate flap via alternate path
- Incremental deployment
- Distributed and Automated Intelligence



VPNv4 example with SRv6 Dataplane



IPv6 Discussions

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

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

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

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

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

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

- You can start core to edge (You have a time), Edge to core (rely on tunneling) or Internet edge (e-commerce, it is done for business continuity)
- 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.

IPv6 Quiz

Questions and the Answers

Question-1

Fictitious Service Provider company has been planning IPv6 access for their residential broadband customers. Which solutions below don’t require access node changes in the Service Provider domain? (Choose Three)

A. CGN

B. 6rd

C .6to4

D. IPSEC

E. DS-Lite

F. Dual Stack

Answer-1

- IPSEC is not an option. Dual Stack requires IPv6 support in addition
- to IPv4 everywhere.
- DS-Lite require IPv6 access nodes.
- 6rd and 6to4 are the IPv6 tunneling mechanisms over IPv4 Service Provider infrastructure.

Answer-1

- 6rd and 6to4 don’t require access node upgrade such as DSLAM, in the case of residential broadband upgrade.
- But both 6to4 and 6rd still require CPE upgrade on the customer site.
- CGN (LSN) doesn’t require access node upgrade as well; most of the residential equipment already supports NAT44.
- Thus the answer of this question is A, B and C.

Question-2

- Which below mechanisms allow asymmetric IPv6 routing design?

- **A.** 6rd
- **B.** 6to4
- **C.** NAT 64 +DNS 64
- **D.** D. DS-Lite

Answer-2

- Asymmetric routing is possible with the stateless mechanisms only.
- 6rd is the stateless tunneling mechanisms.
- NAT64 + DNS 64 can be stateful or stateless, thus they are not the correct answer. DS-Lite has CGN component, which is always stateful.
- That’s why answer of this question is A, 6rd.

Question-3

What is the biggest cost component during IPv6 transition design?

A. CPE

B. Access Nodes

C. Core Nodes

D. Training

E. Application Development

Answer-3

- Biggest cost component is CPE (Customer Premises Equipment).
- In case IPv6 is not supported on the CPE, enabling it on software
- requires operational expenses, changing the hardware requires both operational and capital expenses.
- If Service Provider needs to change CPE for 10 Million customers and every CPE cost only 50$, 500million $ is required only for CAPEX.
- That’s why answer of this question is A, CPE.

Question-4

Which below options might be a possible problems with NAT 64 + DNS 64 design? (Choose Three)

A. It may not support IPv4 only applications such as Skype

B. Duplicate DNS entries can come if company has more than one DNS

C. It doesn’t support DNSSEC

D. It doesn’t translate IPv4 to IPv6

E. Stateful NAT 64 + DNS 64 makes routing design harder

Answer-4

- As they have been explained in the IPv6 chapter, NAT64+DNS64
- may not support IPv4 only applications such as Skype. Duplicate DNS entries can come if company has more than one DNS and Stateful NAT 64 + DNS 64 makes routing design harder.
- Thus the correct answer of this question is A, B and E.

Question-5

If IPv6 only node will reach to IPv4 only content, which below mechanism is used?

A. 6rd tunneling

B. Dual Stack

C. Translation

D. Host to Host tunneling

Answer-5

- Translation mechanism is needed. Tunneling cannot solve this problem.

Question-6

- Which below options are used as IPv6 transition mechanisms? (Choose Three)

A. Dual-Stack

B. Edge to Core Ipv6 design approach

C. Tunneling

D. Translation

D. E. IPv6 Neighbor Discovery

Answer-6

- As it is explained in detail in the IPv6 Transition Mechanisms; Dual-Stack, Tunneling and the Translation are the IPv6 transition mechanisms.

- That’s why, answer of this question is A, C and D.

Question-7

Which subnet mask length is used in IPv6 on point-to-point links for consistency?

A. /56
B. /64
C. /96
D. /126
E. /127

Answer-7

- /64 is used in IPv6 on point-to-point links for consistency
- Although there was discussions around its usage and some people
- considered initially that it was wasting of address space, general design recommendation is using /64 or /127 for point to point links and using /64 everywhere including point to point link provides consistency.

Question-8

Which IPv6 design method consumes more resources on the network nodes?

A. Dual-Stack
B. Tunneling mechanisms
C. Translation mechanisms
D. IPv6 only network
E. Carrier Grade NAT

Answer-8

- Dual Stack on the network nodes consumes more CPU and more memory compare to tunneling and the translation mechanisms, which are used for IPv6 transition

- That’s why; the answer of this question is A, Dual-stack

Question-9

What does Dual-Stack mean?

A. Enabling IPv6 and IPv4 on all the networking nodes

B. Enabling IPv6 and IPv4 on all the networking nodes and the links

C. Enabling IPv6 and IPv4 on all the networking nodes, links, hosts and applications

D. Enabling IPv6 and IPv4 on the core, aggregation and access network nodes.

Answer-9

- Dual stack is providing both IPv4 and IPv6 connectivity to all the networking nodes, links, hosts and applications. That’s why; answer of this question is C.

Question-10

Fictitious Service Provider company requires more Public IPv4 addresses but due to IPv4 exhaustion they couldn’t receive from the RIRs. What is the option for them to continue providing IPv4 services without enabling IPv6 on CPE, access and core network?

A. Carrier Grade NAT

B. DS-Lite

C. NAT64 + DNS64

D. 6rd

E. 6to4

Answer-10

- IPv4 exhaustion problem requires Carrier Grade NAT solution, which share public IPv4 addresses among multiple users by using NAT 44 on the CPE and NAT 44 on the SP domain. It is also called double NAT, Large Scale NAT, Dual NAT 44 or NAT444

- That’s why answer of this question is A, Carrier Grade NAT.

Question-11

Which below terms are used interchangeably for Carrier Grade NAT (CGN)? (Choose Three)

A. LSN

B. Double NAT

C. Service Provider NAT

D. CPE NAT

E. NAT 444

Answer-11

- LSN (Large Scale NAT), Double NAT, NAT 444 are used interchangeably for CGN. Thus, the answer of this question is A, B and E.

Question-12

Which below options are used as an IPv6 over IPv4 tunneling mechanism? (Choose Two).

A. 6to4
B. 6rd
C. NAT 64 + DNS64
D. DS-Lite
E. MAP-E
F. 464xlat

Answer-12

- Out of given options, IPv6 tunneling mechanisms are 6to4 and 6rd. Remaining ones is used for IPv4 tunneling. IPv4 service is tunneled over IPv6.

- That’s why; answer of this question is A and B.

Question-13

What are the problems with Carrier Grade NAT IPv6 design? (Choose four)

A. Some applications doesn’t work behind CGN

B. If the users behind same LSN, stateful devices might drop traffic, thus require traffic go through CGN node even if the traffic between nodes which are behind same LSN

C. IP address overlapping if Customer uses same private address range with the Service Provider

D. It requires IPv6 on the CPE nodes, thus CPEs have to be upgraded

E. Since it is stateful, asymmetric traffic is not allowed.

F. Since it is stateless, asymmetric traffic is not allowed.

Answer-13

- Some applications doesn’t work behind CGN If the users behind same LSN, stateful devices might drop traffic, thus require traffic go through CGN node even if the traffic between nodes which are behind same LSN IP address overlapping if Customer uses same private address range with the Service Provider . Since it is stateful, asymmetric traffic is not allowed.

- Correct answer of this question is A, B, C and E.

Question-14

What are the problems with dual stack IPv6 design? (Choose Three)

A. It consumes more memory and CPU on the networking nodes compare to tunneling and translation mechanisms

B. It doesn’t solve IPv4 address exhaustion problems

C. It requires IPv6 support on all the CPE and Access nodes

which are the most cost associated components

D. Troubleshooting wise it is harder compare to tunnelling and translation mechanisms

E. All of the above

Answer-14

- It consumes more memory and CPU on the networking nodes compare to tunneling and translation mechanisms. It doesn’t solve IPv4 address exhaustion problems. CPEs and hosts still require IPv4 address. Host private address is NATed to the CPE public IPv4 address (NAT44) It requires IPv6 support on all the CPE and Access nodes, which are the most cost associated components

- That’s why; answer of this question is A, B and C.

Question-15

What is the best IPv6 design method for MPLS Layer 3 VPN service?

A. Dual Stack

B. NAT 64 + DNS 64

C. 6rd

D. 6VPE

E. 6PE

Answer-15

- Best IPv6 design method for MPLS Layer 3 VPN service is 6VPE.

Question-16

Which options are the IPv6 Automated Tunneling mechanisms? (Choose Three)

A. 6rd

B. 6over4

C. 6to4

D. Tunnel Brokers

E. NAT-PT

F. GRE Tunnels

Answer-16

- 6rd, 6to4 and 6over4 are the automated IPv6 tunneling mechanisms. 6over4 requires multicast on the network thus it is deprecated.
  In all three mechanisms IPv4 addresses embedded in the IPv6 address.

Answer-16

- Tunnel broker is a semi-automated mechanism. The Authoritative server provides tunnel destination address. NAT-PT is a translation mechanism and because of security issues it is deprecated

- GRE Tunnels are manual tunneling mechanism. That’s why the answer of this question is; A, B and C

Question-17

Service Provider Company wants to implement DPI (Deep Packet Inspection) node in the network. Which below method would create a problem?

A. Tunneling

B. Dual-Stack

C. Native IPv4

D. Translation

Answer-17

- Most of the DPI devices cannot work with the IPv6 tunneling mechanisms. Thus using them with the DPI element can create a problem. There is no problem with the other options. Correct answer is Option A.

Question-18

Enterprise Company implemented QoS on their network. Which below IPv6 design option method doesn’t work well with QoS?

A. Dual Stack

B. Translation

C. IPv6 only

D. Tunneling

Answer-18

- Ipv6 tunneling mechanisms don’t work well with the QoS.

Question-19

Which below options are used for host to host IPv6 tunneling?

A. ISATAP

B. 6to4

C. 6rd

D. Teredo

E. IPv6 DAD

Answer-19

- ISATAP and the Teredo are used for host to host or host to router tunneling.

Question-20

Enterprise Company wants to have an experience with the IPv6. They have 50 IT Lab facilities and want to access IPv6 application in the datacenter. They don't have currently IPv6 on their network and they want to have an access immediately from the labs to the applications

Where would they start enabling IPv6?

A. Network Core first and IT labs should enable IPv6
B. No need for IPv6 on the network, they can use translation
C. IT labs should be enabled IPv6 and tunnel to the DC
D. Placing CGN box at the central place solves is best design options for them

Answer-20

- As it is explained in the IPv6 chapter, they are looking for Edge to the Core model. IT labs should be enabled IPv6 and tunnel to the DC. Answer of this question is C.

Question-21

Which mechanism can be used to deploy IPv6 services in an IPv4 only backbone?

A. NAT64 at the edge of the network

B. 6PE in the backbone network

C. 6RD on CPEs and 6RD BRs at the Edge of the network

D. DS-Lite at the Edge of the network

Answer-21

- Since in the requirement it is said that, IPv4 only backbone, NAT64, 6PE and DS-Lite cannot be a solution

- Because NAT64 requires IPv6 only network or Dual Stack, 6PE requires MPLS network and DS-Lite requires IPv6 only network

- Yes, NAT64 could be place at the Internet edge and the best place for NAT64 deployment is Internet edge according to RFC 7269, in this question, requirement says that IPv4 only network. That’s why; answer of this question is C.

Question-22

E-commerce company want to enable IPv6 on their network as soon as possible. Where would be the best place for them to start and which solution would you recommend?

A. All DC infrastructure, running dual stack is best option.

B. At the internet edge, NAT 64 + DNS 64 is a best solution

C. At the internet edge and dual stack is best solution

D. All over the network and dual stack is best solution

Answer-22

- In the requirement it is said that E-commerce Company and they want to enable IPv6 as fast as possible. Dual stack is very time consuming if not impossible

- Also, since the business is E-commerce, in general, IPv6 business case for the E-commerce companies is IPv6 presence

Answer-22

- If Happy Eye balls enabled at the customer sites, or IPv6 only users will reach to their site, it is important to have IPv6 presence for E-commerce companies. Thus Starting from the Internet Edge and enabling NAT 64 + DNS 64 is the best for the given company and the requirements

- Thus, answer of this question is B

Question-23

Which below options are critical as an IPv6 First Hop Security features? (Choose Three)

A. Suppressing excessive Multicast neighbor discovery messages

B. ARP Inspection

C. Limiting IPv6 Router advertisement

D. Preventing rogue DHCPv6 assignments

E. Broadcast control mechanism

Answer-23

- There is no ARP in IPv6. So ARP inspection is unrelated
- There is no Broadcast in IPv6 as it is explained in the IPv6 chapter, thus Option E is wrong as well. Remaining all three features are critical IPv6 First Hop Security features
- That’s why; answer of this question is A, C and D.

Question-24

Enterprise Company implemented dual stack network. It took a lot of time them to implement dual stack on all their networking nodes, links, applications, hosts and operating system. Although their network is 100 % dual stack, they only see 25 % IPv6 Internet traffic on their network.

What might be the possible problem?

A. Some of their link for the Internet may not be IPv6 enabled

B. Content which their users try to access is not enabled IPv6

C. Operating system of their users might prefer IPv4 over IPv6

D. They might have Happy Eye Balls enabled and IPv6 might have priority

Answer-24

- Because either content, which their users try to access, is not enabled IPv6 or Operating system of their users might prefer IPv4 to IPv6. Answer of this question is B and C

Question-25

Which below protocols are used in IPv6 Multicast?

A. MLD

B. Auto-RP

C. MSDP

D. Embedded RP

E. Anycast RP

Answer-25

- MSDP and Auto-RP is not supported in IPv6 Multicast. MLD, Embedded RP and Anycast RP are the IPv6 Multicast features.

- MLD is equivalent of IGMP Snooping in IPv4 and whenever there are layer 2 switches in IPv6 Multicast design, MLD should be enabled for optimal resource usage.