IPv4 to IPv6 Transition

Agenda

- IPv4 to IPv6 Transition
- Probable IPv6 adoption challenges in **AfgREN**

Why IPv6 ?

- in September 1981, IPv4 was described for the first time
- Ipv4 specification was first published as the IETF RFC 791 standard in 1981
- By 1992, the scalability and limited ipv4 address space became an issue

IPv4 Limitations

- Exhausted IPv4 address space
- Disproportionate IPv4 assignment (Almost 50% of addresses are reserved for USA)
- Weak protocol extensibility of IPv4 header
- Quality of Service (QoS)

IPv6 Benefits

- Larger address space
- Simplified Header
- End-to-End Connectivity
- Faster Forwarding/Routing
- Mobility
- **Enhanced Priority support**: ipv4 used 6 bits of DSCP (Differential Service Code point) and 2 bits of ECN (Explicit Congestion Notification) to provide QOS. In ipv6, traffic class and flow labels are used for efficient routing of the packets.
- **Extensibility**: ipv6 header is extensible to add more information in the option part. Ipv4 provides only 40 bytes for option, whereas, option in ipv6 can be as much as the size of ipv6 packet itself.
- Smooth transition

IPv4-to-IPv6 Transition Mechanisms

- Transition is means of connection between IPv4 & IPv6 as both protocols are incompatible
- Transition referring to initial state of IPv4 only network that IPv6 nodes are added or overlaid overtime.
- IETF transition working group
- Organizations with IPv4 infrastructure seeking transition to IPv6 is facing problems like identifying impacts, planning the transition and performing the migration.
- IPv6 has been designed for easing the transition and co-existence with IPv4
- Transition mechanisms divided into 3 categories:

  -- Dual Stack

  -- Tunneling

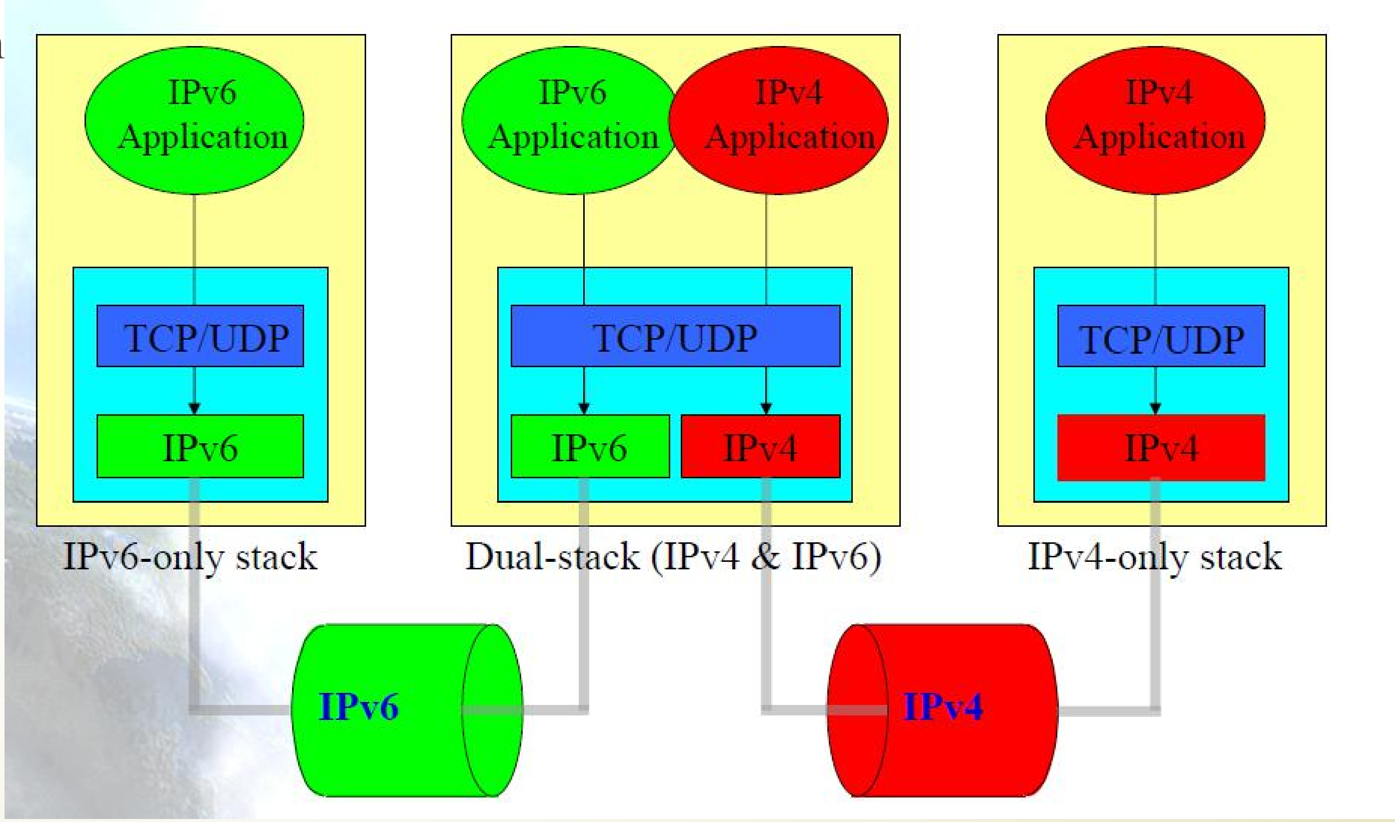
  -- Translation

Dual Stack =Dual IP Layer operation

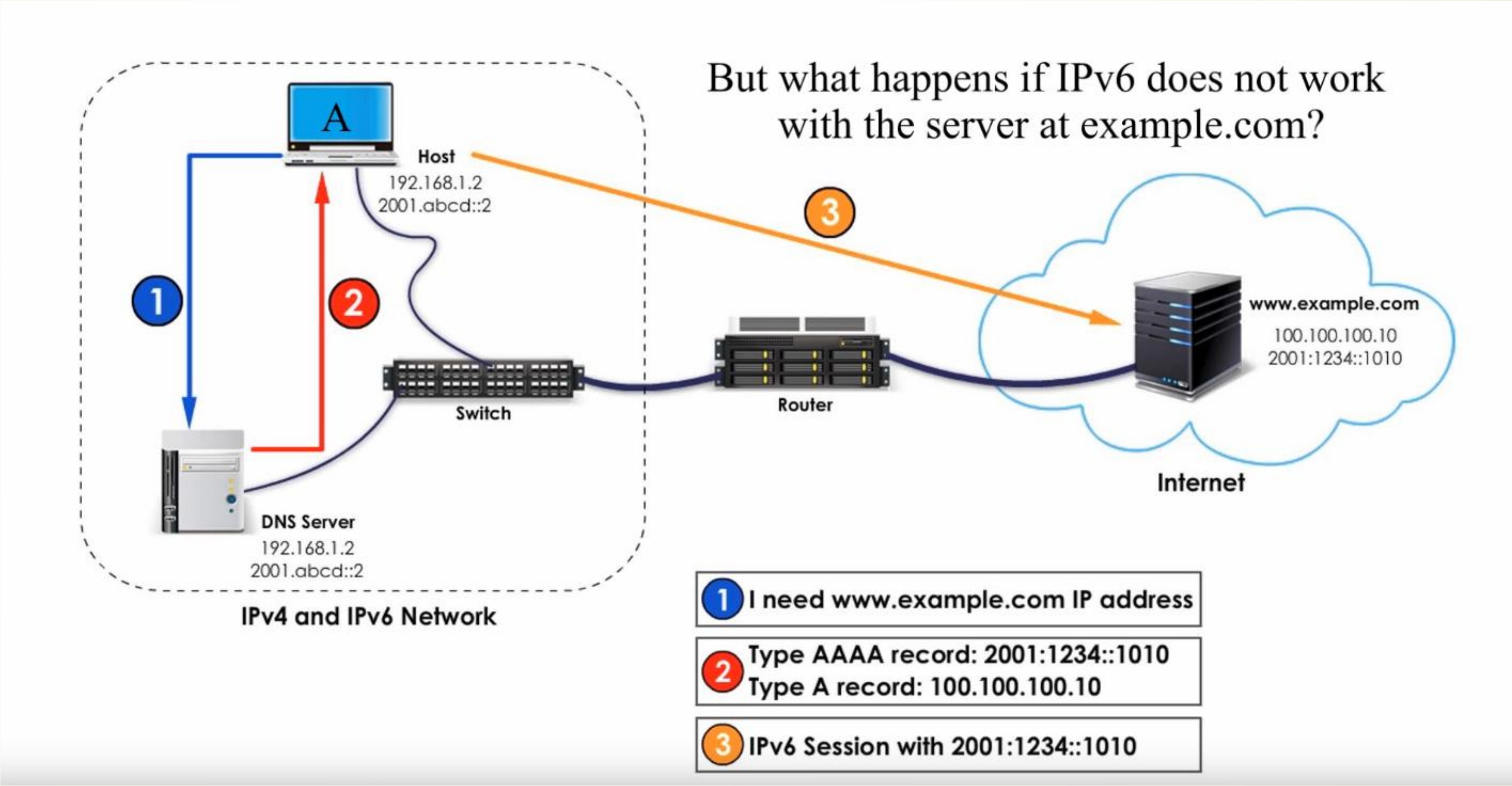
- Dual stack happens at network layer
- implementation of both IPv4 & IPv6 stacks on devices RFC2893
- Devices can be router, other infrastructure devices and end users
- Only network layer is dualized using common application, transport and data link layers.
- Dual stacked VLAN networks (RFC4554) based on VLAN tagging that enables layer 2 switches to broadcast or trunk the Ethernet frames containing IPv6 payloads to one or more IPv6 routers.
- DHCP Consideration
- DNS considerations

  -- A resource record for IPv4

  -- AAAA resource record for IPv6



Dual stack Example



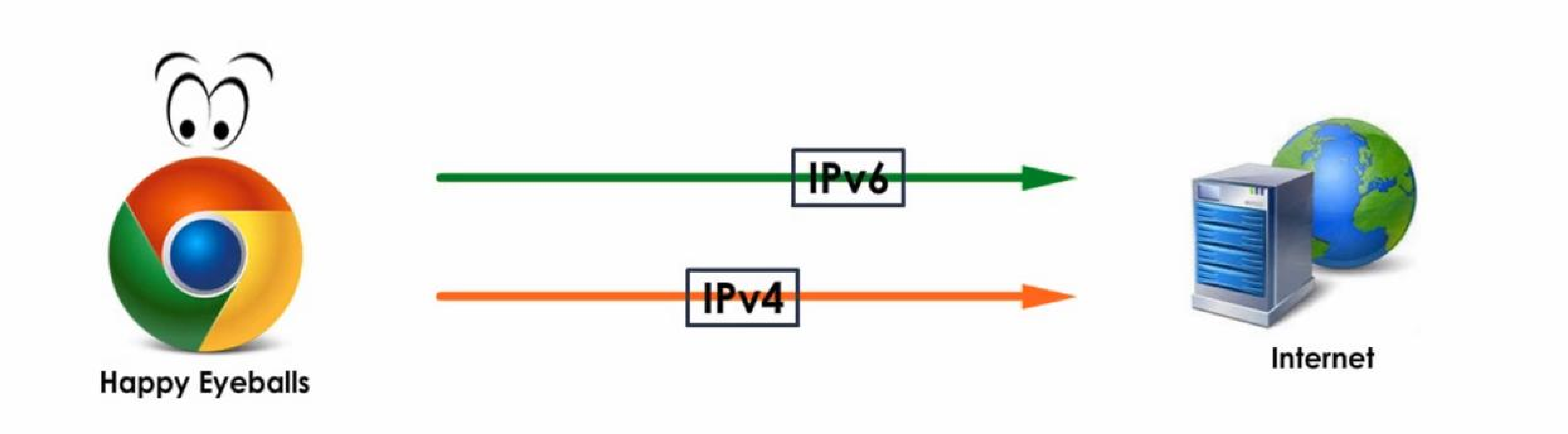
But what happens if IPv6 does not work with the server at example.com?

1 I need www.example.com IP address

2 Type AAAA record: 2001:1234::1010
Type A record: 100.100.100.10

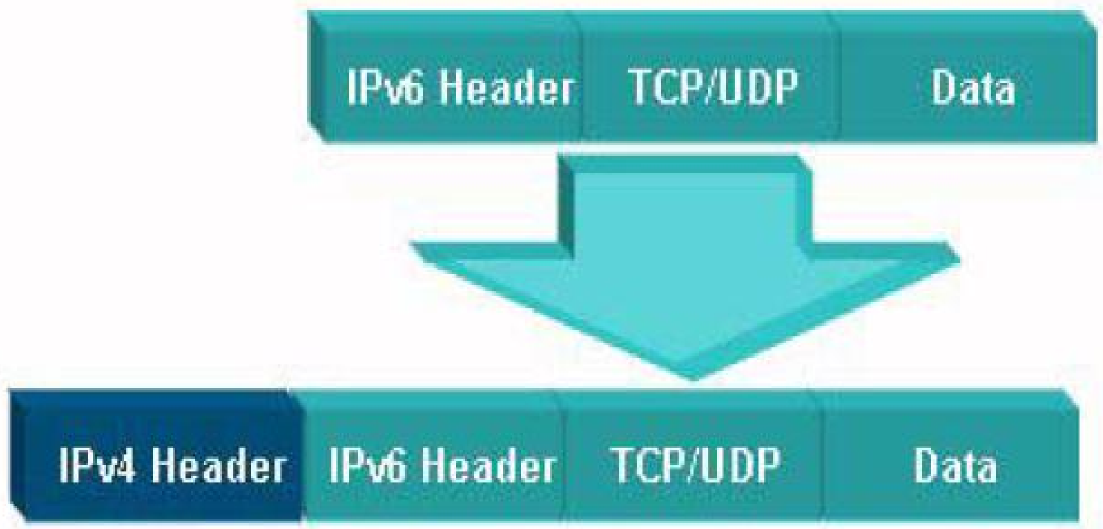
3 IPv6 Session with 2001:1234::1010

Happy Eyeballs



2. Tunneling

- A variety of tunneling exists to support ipv4 over ipv6 tunneling and vice versa
- Configured or predefined and Automatic
- Tunneling is to carry an ip packet into the payload of another ip packet
- to transfer data between two compatible network nodes over incompatible network
- Tunneling of IPv6 packet through IPv4 network entails prefixing each IPv6 packet with an IPv4 header and will enable tunneled packet to be routed over ipv4 infrastructure
- Protocol field of IPv4 is set to 41 decimal to indicate encapsulated packet
- Entry node of tunnel performs encapsulation
- Exit node of tunnel do de-capsulation

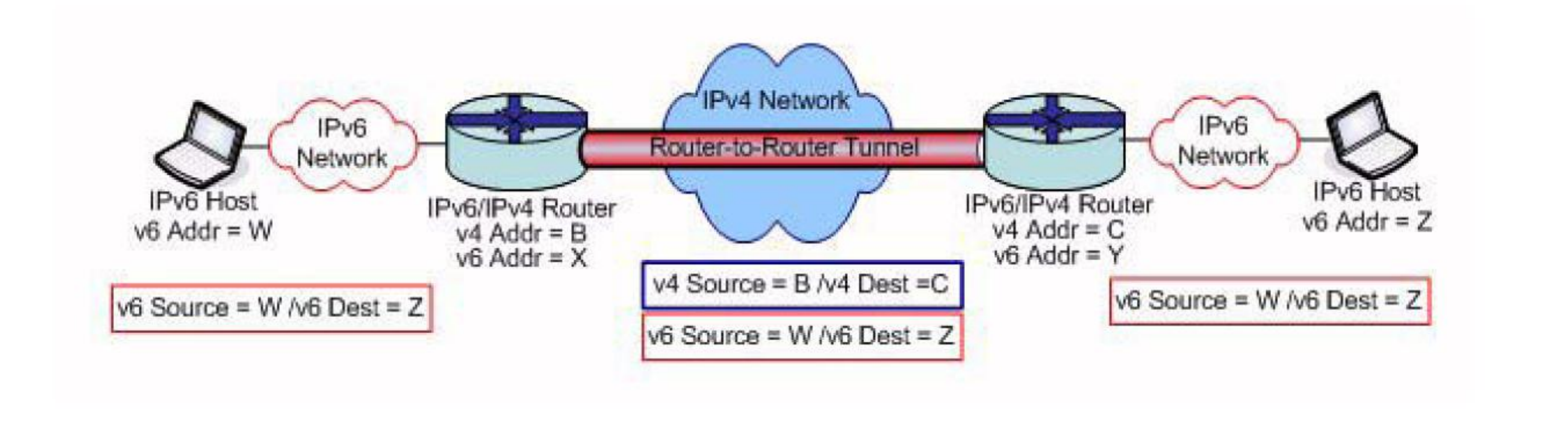


Types of tunneling

1. Manual tunneling (configured or predefined)

- ❑ Router to router
- ❑ Host to router
- ❑ Router to host
- ❑ Host to host

- ➢ Among all above manual tunneling probably **router to router** is commonly used that is shown bellow

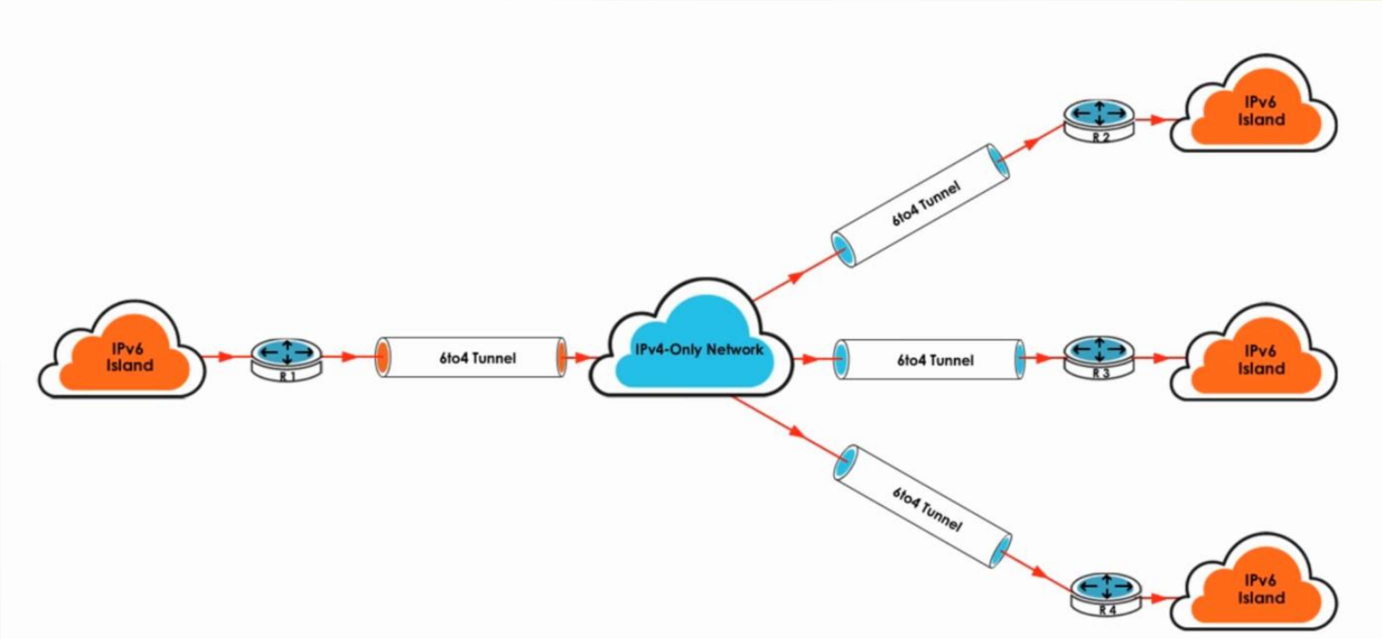


2. Automatic tunneling

- ❑ 6to4
- ❑ ISATAP
- ❑ 6RD
- ❑ Tunnel brokers
- ❑ Teredo
- ❑ DSTM

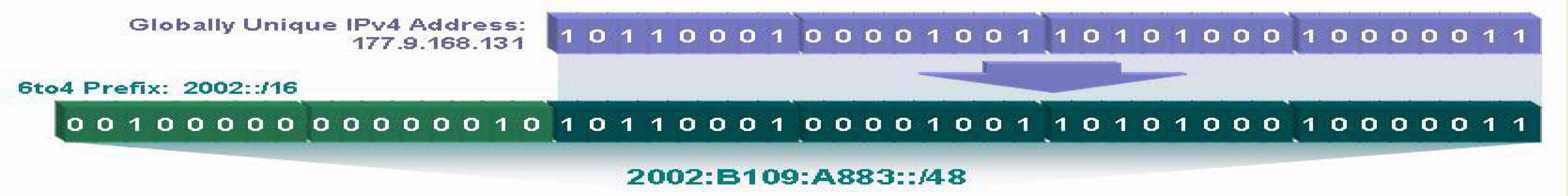
1. 6to4 tunneling (RFC3056)

- Relies on particular IPv6 format to identify 6to4 packets to tunnel them accordingly
- connect multiple IPv6 network over one tunnel
- Point to multi point connection
- Every 6to4 node has a unique 6to4 address
- 6to4 is a router to router mechanism
- 6to4 uses simple protocol=41 encapsulation (IPv6 in IPv4)

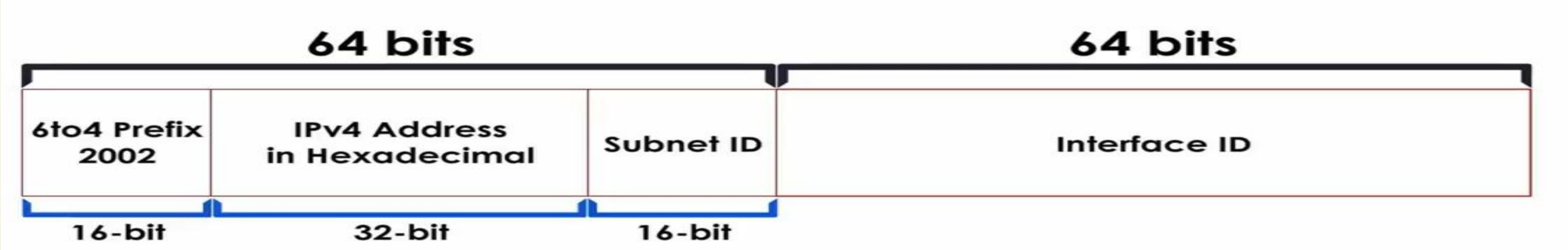


Structure of 6to4 IP address

- 6to4 prefix 2002::/16 (Global routing prefix)
- Ipv4 address in Hexadecimal (6to4 router terminating the tunnel)
- This concatenation forms a /48 prefix shown in the figure
- Unique ipv4 address represents ipv4 address of 6to4 router terminating 6to4 tunnel

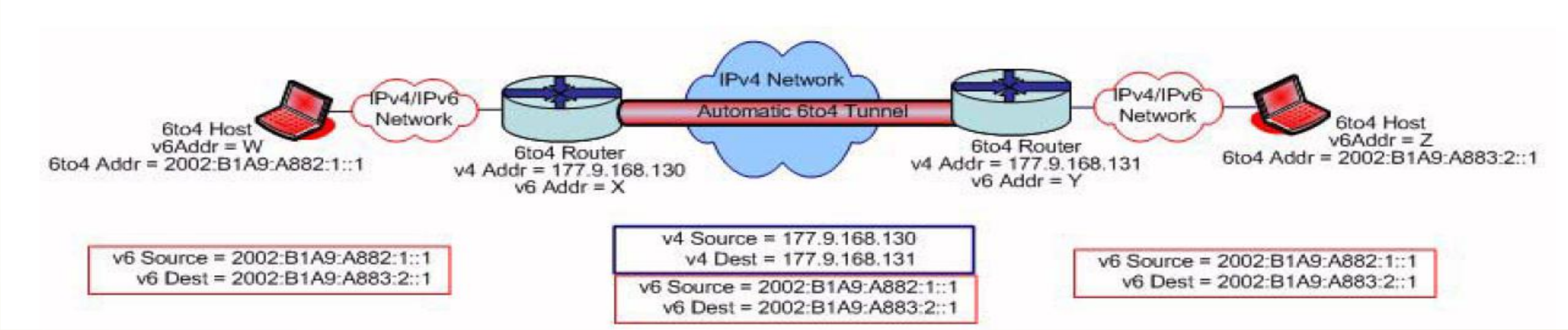


- Subnet ID
- Interface ID



6to4 tunneling Example

- Routers ipv4 interface are 177.9.168.130 and 177.9.168.131 respectively
- Transforming into 6to4 addresses, we arrive at **2002:B109:A882::/48:1::1** and **2002:B109:A883::/48:1::2**
- These prefixes now identify each site in terms of 6to4 reachability
- The AAAA and PTR resource records corresponding to these 6to4 addresses should be added to DNS within the appropriate domains.



IPv4 Network
Automatic 6to4 Tunnel
IPv4/IPv6 Network
IPv4/IPv6 Network
6to4 Host
v6Addr = W
6to4 Addr = 2002:B1A9:A882:1::1
6to4 Router
v4 Addr = 177.9.168.130
v6 Addr = X
6to4 Router
v4 Addr = 177.9.168.131
v6 Addr = Y
6to4 Host
v6Addr = Z
6to4 Addr = 2002:B1A9:A883:2::1
v6 Source = 2002:B1A9:A882:1::1
v6 Dest = 2002:B1A9:A883:2::1
v4 Source = 177.9.168.130
v4 Dest = 177.9.168.131
v6 Source = 2002:B1A9:A882:1::1
v6 Dest = 2002:B1A9:A883:2::1
v6 Source = 2002:B1A9:A882:1::1
v6 Dest = 2002:B1A9:A883:2::1

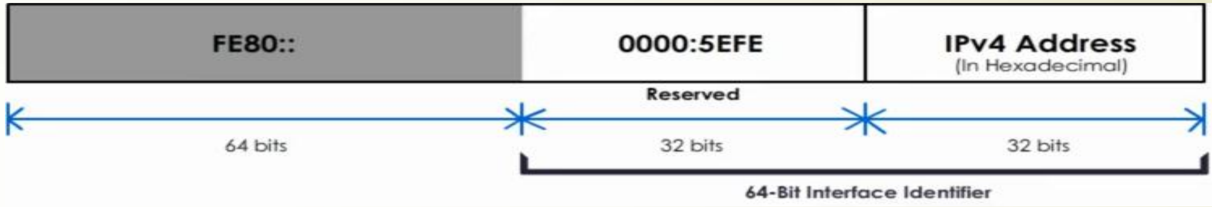
- As networks are incrementally migrated to ipv6, 6to4 relay routers can be used to relay packets form host on pure ipv6 networks to ipv6 host via ipv4 networks.

2. ISATAP (Intra-Site Automatic Tunneling Addressing Protocol)

- Experimental protocol for IPv6 to IPv4 tunneling for host to router, router to host and host to host configurations.
- Its point to point connection
- ISATAP IPv6 address formed using IPv4 address to define interface ID
- Interface ID=::5EFE:a.b.c.d
- Hosts supporting ISATAP are required to maintain a *potential router list* (PRL) containing the IPv4 address and associated address lifetime timer for each router advertising an ISATAP interface.
- ISATAP host encapsulates IPv6 packet with IPv4 header

How to Get ISATAP IPv6 from IPv4

- ISATAP uses a well defined IPv6 format
- ISATAP IPv6 address format-Link Local



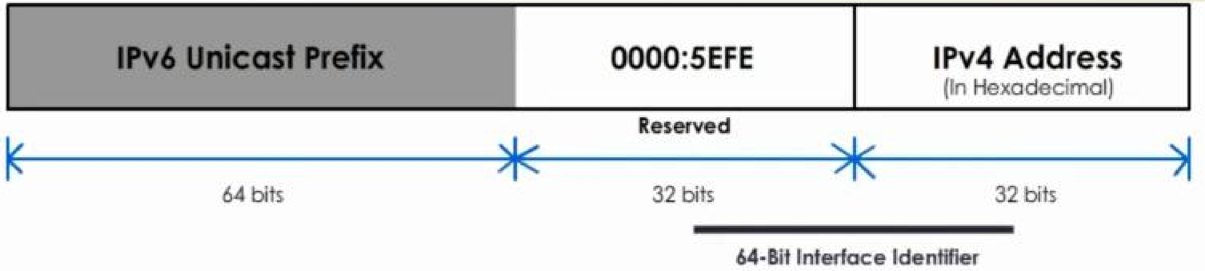
FE80:: | 0000:5EFE | IPv4 Address (In Hexadecimal)

Reserved

64 bits | 32 bits | 32 bits

64-Bit Interface Identifier

- ISATAP IPv6 address format-Global unicast

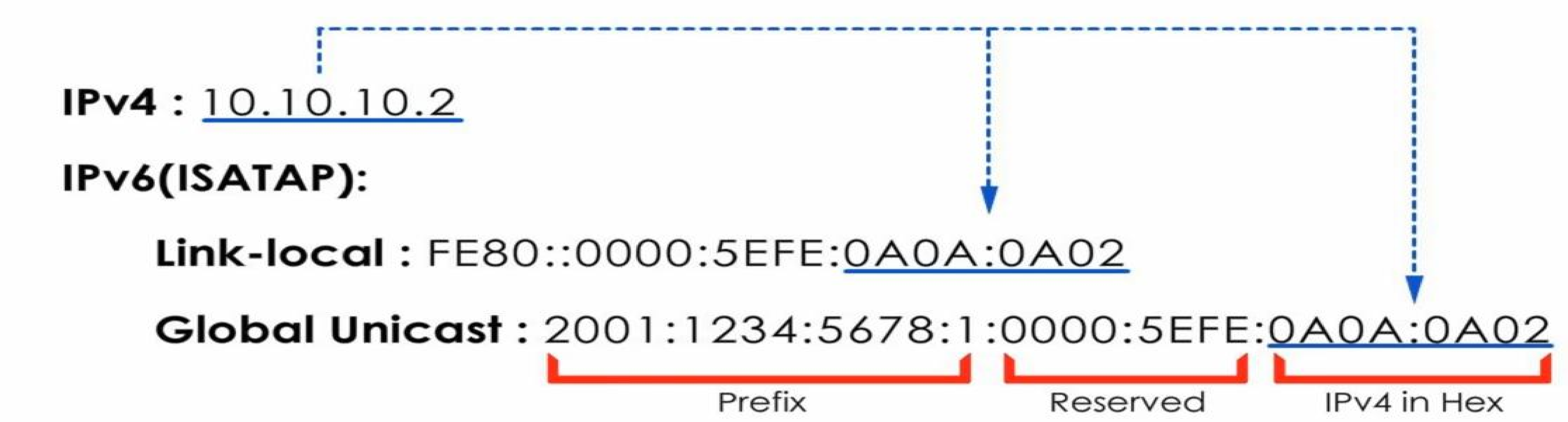


IPv6 Unicast Prefix | 0000:5EFE | IPv4 Address (In Hexadecimal)

Reserved

64 bits | 32 bits | 32 bits

64-Bit Interface Identifier



IPv4 : 10.10.10.2

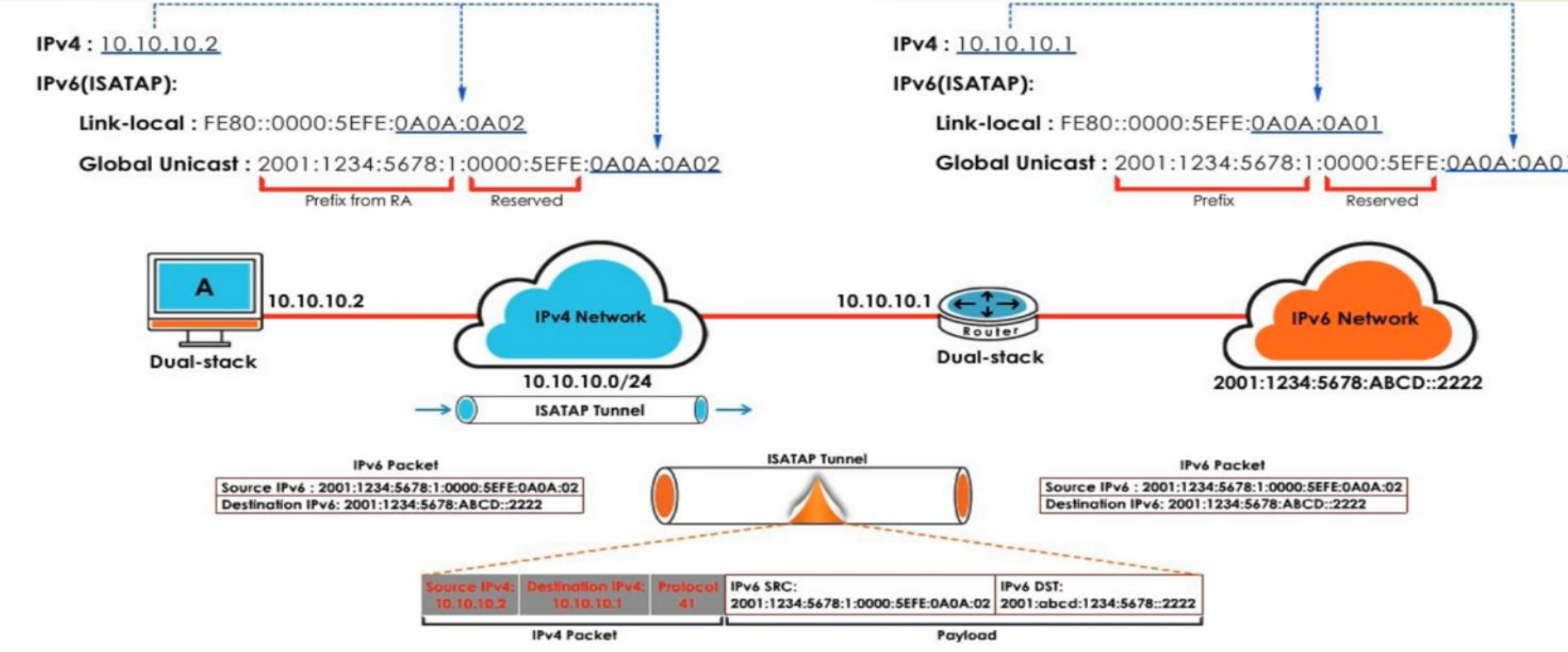
IPv6(ISATAP):

Link-local : FE80::0000:5EFE:0A0A:0A02

Global Unicast : 2001:1234:5678:1:0000:5EFE:0A0A:0A02

ISATAP operation

- An ISATAP tunnel can exist between any two dual stack device
- Provides dual stack hosts with access to the IPv6 network over an ipv4 only network


IPv4 : 10.10.10.2
IPv6(ISATAP):
Link-local : FE80::0000:5EFE:0A0A:0A02
Global Unicast : 2001:1234:5678:1:0000:5EFE:0A0A:0A02
Prefix from RA
Reserved
IPv4 : 10.10.10.1
IPv6(ISATAP):
Link-local : FE80::0000:5EFE:0A0A:0A01
Global Unicast : 2001:1234:5678:1:0000:5EFE:0A0A:0A0
Prefix
Reserved
A
10.10.10.2
Dual-stack
IPv4 Network
10.10.10.0/24
ISATAP Tunnel
10.10.10.1
Router
Dual-stack
IPv6 Network
2001:1234:5678:ABCD::2222
IPv6 Packet
Source IPv6 : 2001:1234:5678:1:0000:5EFE:0A0A:02
Destination IPv6: 2001:1234:5678:ABCD::2222
ISATAP Tunnel
IPv6 Packet
Source IPv6 : 2001:1234:5678:1:0000:5EFE:0A0A:02
Destination IPv6: 2001:1234:5678:ABCD::2222
Source IPv4: 10.10.10.2
Destination IPv4: 10.10.10.1
Protocol 41
IPv6 SRC: 2001:1234:5678:1:0000:5EFE:0A0A:02
IPv6 DST: 2001:abcd:1234:5678::2222
IPv4 Packet
Payload

3. 6RD (IPv6 Rapid Deployment)

- 6rd is stateless used to encapsulate ipv6 packets into ipv4 packet
- 6rd is driven from 6to4 tunneling and removes the following 2 drawbacks related to 6to4.

1. Packets from native IPv6 hosts have to traverse a 6to4 relay router so that IPv6 packets can be encapsulated in IPv4 packet.
2. Removes the dependency to **2002::/16** prefix and 6to4 prefix resulting into receiving packets from other ISP with same prefix (Dropping means we blackhole traffic, relaying it means we process traffic from both our customers and customers form other ISPs)

- With 6rd Every ISP can use its own unique IPv6 prefix that leads to the following advantages

1. All 6RD hosts are reachable from all native IPv6 hosts that can reach the ISP IPv6 network.
2. The relay **belongs to the ISP** and only does 6to4 tunneling for the customers of the ISP so they are completely responsible for the quality of service.
3. Anonymous traffic attacks are reduced since each ISP process the traffic from its own customers

- Operates entirely within the users ISPs network
- RFC5969
- Implemented originally by FREE (French ISP)

6rd example

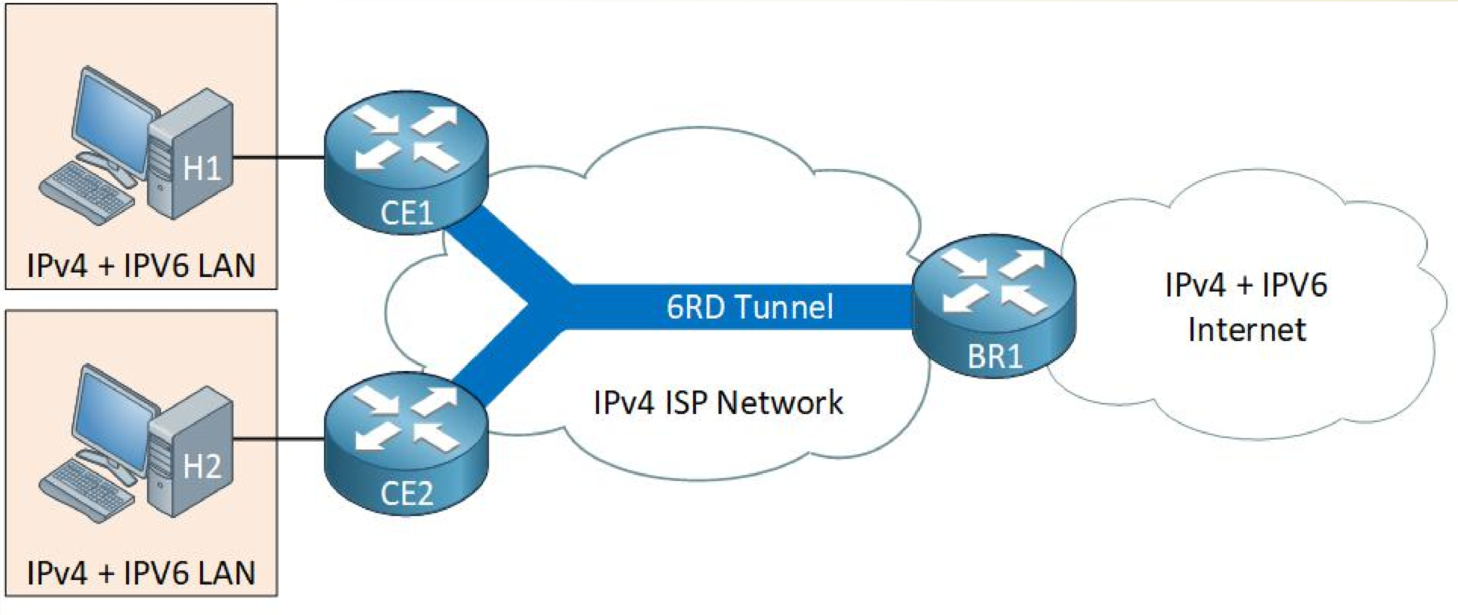
- The ISP has an internal ipv4 network
- Each customer has CE (customer Equipment) or RG (Residential Gateway) with WAN IP on ISP side and ipv4 and ipv6 hosts on the LAN side.
- CE router do encapsulation
- BR or border relay has ipv4 on ISP side and provide connection CE routers and IPv6 network and performs decapsualtion
- For high availability and load balancing we can have multiple BRs
- 6rd addressing and prefixes (IPv6 prefix & prefix length, embedded IPv4 address in IPv6 prefix and 6RD border relay IPv4) are decided

  by ISP with different options

  --TR-069

  -- DHCP option 212

  -- PPP PCP option



Translation

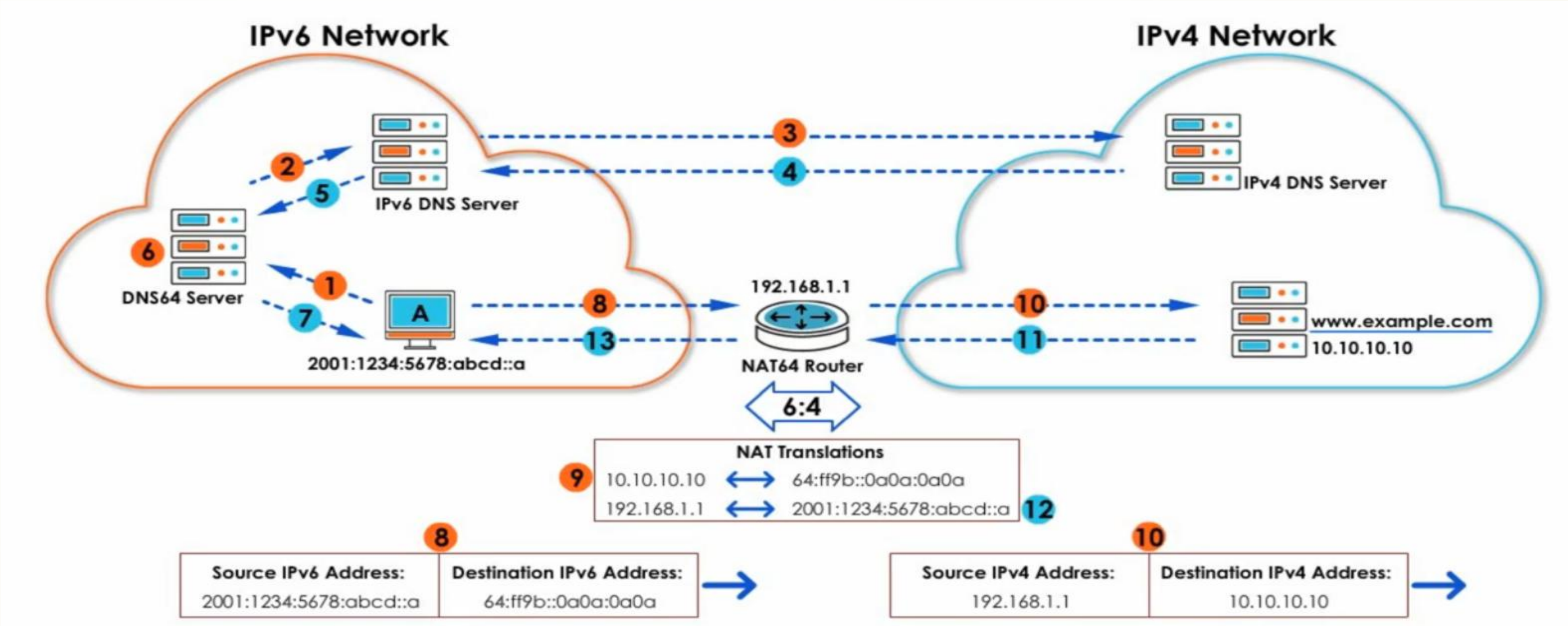
- Perform IPv4 to IPv6 translation and vice versa at particular layer of protocol stack, typically the network, transport or application layer.
- Unlike tunneling, translation modifies IP packets commutatively between IPv4 and IPv6
- IPv6 only nodes communicating IPv4 only nodes

❑ **Translation Categories**

- NAT64
- Dual Stack Lite
- BIS
- BIA
- ALG
- SIIT Algorithm

NAT64

- There are 3 Components of NAT64
- NAT64 prefix (Network specific Prefix or NSP and Well Known Prefix or WKP =64:FF9B::/96)
- DNS64 Server (DNS server for both IPv4 and IPv6)
- NAT64 Router



NAT Translations

10.10.10.10	⟷	64:ff9b::0a0a:0a0a
192.168.1.1	⟷	2001:1234:5678:abcd::a

8

Source IPv6 Address:	Destination IPv6 Address:
2001:1234:5678:abcd::a	64:ff9b::0a0a:0a0a

10

Source IPv4 Address:	Destination IPv4 Address:
192.168.1.1	10.10.10.10

Dual Stack Lite

- Dual stack lite is a promising approach that takes the best of NAT64 and avoiding its problem
- It uses ipv6 only links between the provider and customer
- Allow ISPs to provide IPv4 only network services for customers with native IPv6 without changing end-users software
- Tunneling IPv4 over IPv6 is far simpler than translation, so the performance and redundancy concerns are eliminated
- Sharing same IPv4 addresses among customers by combining:

--Tunneling

--NAT

- No need for multiple level of NAT

- Two Elements

-- DS-Lite Basic Bridging Broadband (B4)

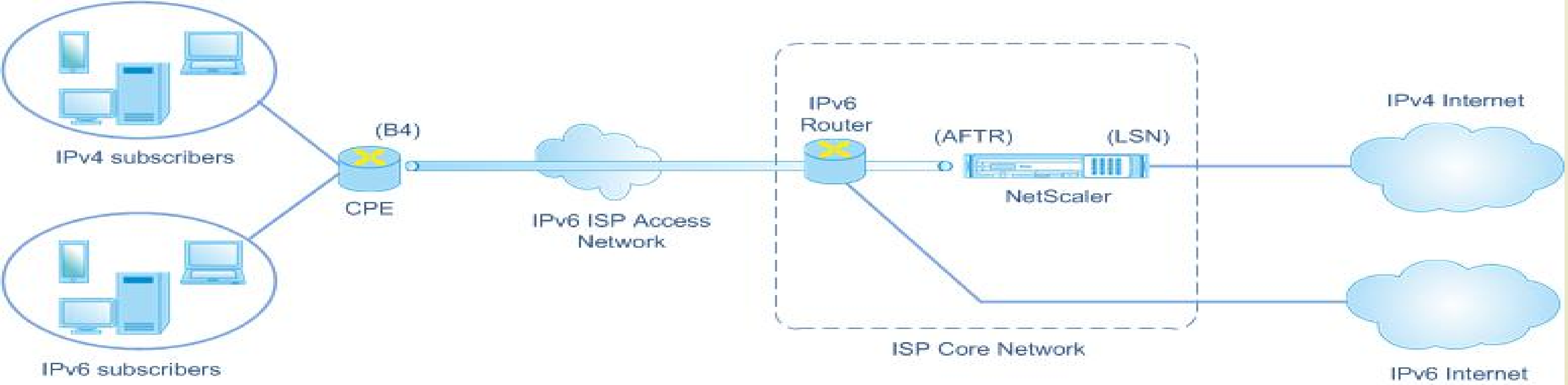
-- DS-Lite Address Family Transition Router (AFTR)

-- Also called CGN (Carrier Grade NAT) or LSN (Large Scale NAT)

DS–lite Architecture

Ds lite architecture is consist of following components

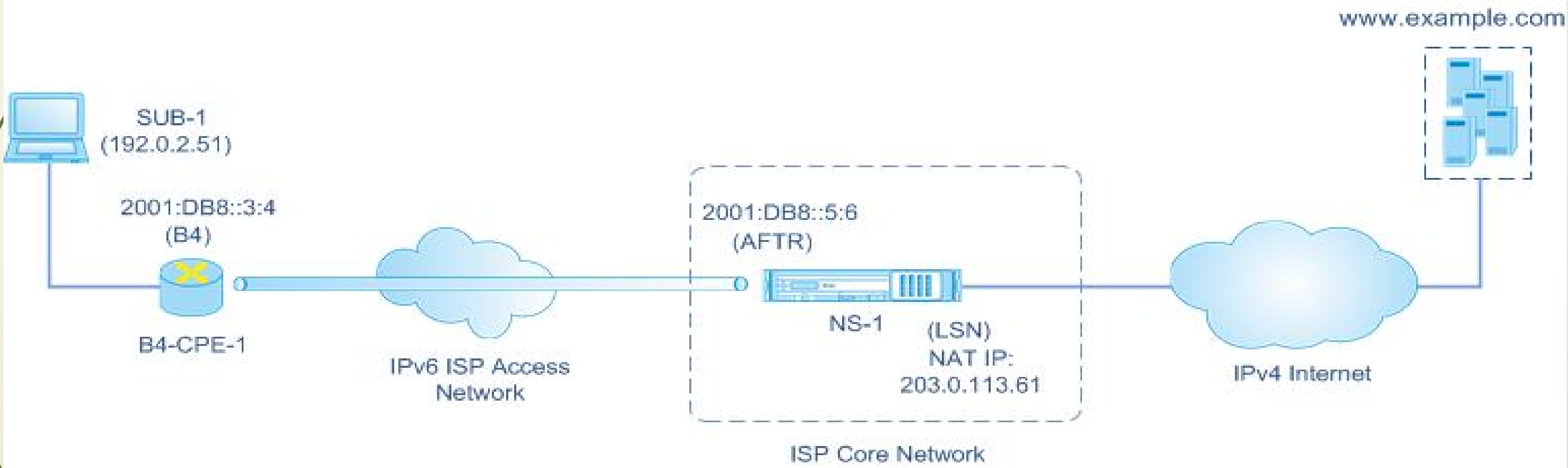
- **Basic Bridging Broadband (B4):** B4, is a device or component that resides in the subscriber premises.
- IPv4 subscribers are connected to the IPv6-only ISP access network through the CPE device containing the B4 component
- **Address family transition router (AFTR):**AFTR is a device or component residing in the ISP’s core network. AFTR terminates the IPv6 tunnel from the B4 device
- **Softwire.** The IPv6 tunnel created between B4 and AFTR is called a softwire.



Ds-lite example

- Following settings is used in this example

Entity	Details
IPv4 address of subscriber SUB–1	192.0.2.51
IPv6 address of softwire endpoint on the B4 device (B4–CPE–1)	2001:DB8::3:4
IPv6 address of the softwire endpoint on the AFTR device (NS–1)	2001:DB8::5:6



Transition challenges

- There are a number of well-known problems for transition techniques
- Tunneling can result in a decreasing of path-MTU
- Widespread drop of ICMP error messages “black holes” where packets are dropped without any reason reported
- Dual stack is facing long delay establishing TCP connection with dual stack nodes

Migration challenges at AfgREN

1. Core migration

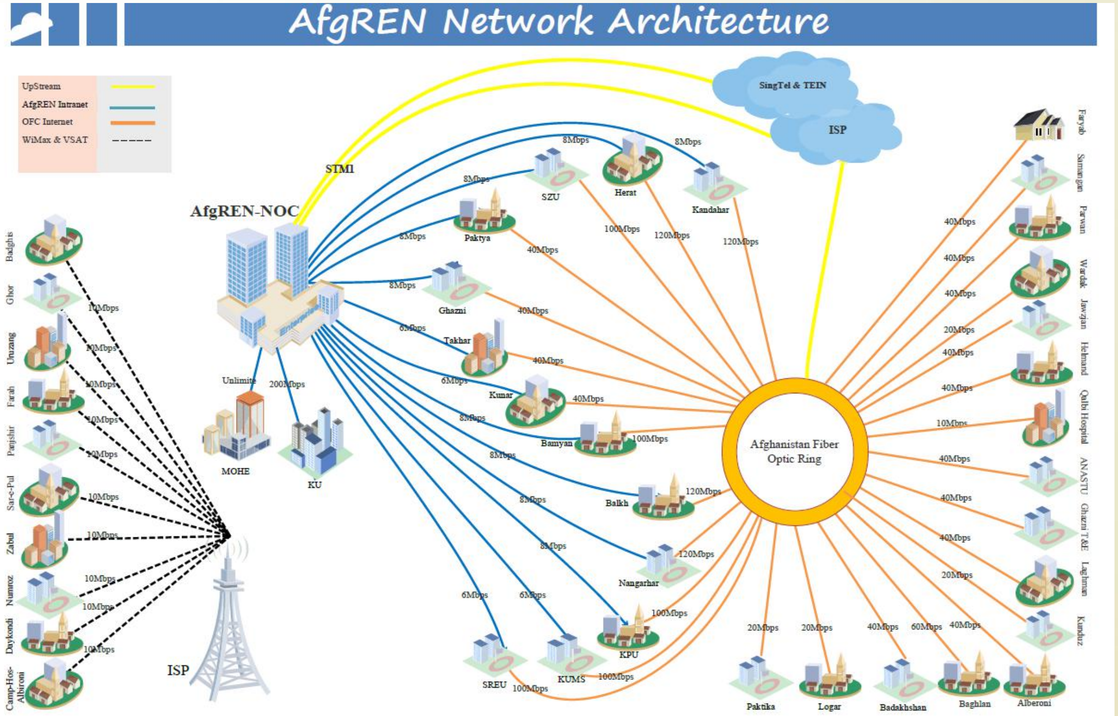
- Need to upgrade all core routers to support IPv6 routing, routing protocols and dual stack
- Transition mechanism needed :

○ for access-core boundary routers configured tunnel need to be applied between them.

○ Alternatively, translation gateways could be used at these boundary points

❑ Challenges

- AfgREN core network is not an internal backbone
- The core network is an ISP running only IPv4 networks



2. Client-server side migration

- Upgrading servers and hosts to dual stack implementation
- Servers should be able to fulfill the request of IPv6 clients too
- Dual stack for internet-facing IP applications such as web servers

❑ **Challenges**

- Dependency to ISP capabilities to run required transition mechanism
- Upgrading costs

Thank You