IPv6 in Broadband Networks

MR-244

January 2011

Agenda

1. Introduction to the Broadband Forum
2. Business drivers for IPv6 and IPv4 exhaustion
3. Key IPv6 attributes and deployment challenges
4. IPv6 strategies for broadband access to support Internet access and new services
5. Summary

IPv6 in Broadband Networks Tutorial Contributors

- Christophe Alter – France Telecom
- Salman Asadullah – Cisco
- David Allan – Ericsson
- Michel Borgne – France Telecom
- Dave Christophe – Alcatel-Lucent
- Guillaume Gottardi – Cisco
- Michael Hanrahan – Huawei
- Christian Jacquenet – France Telecom
- David Kessens – NSN
- Suresh Krishnan – Ericsson
- Roberta Maglione – Telecom Italia
- Drew Rexrode – Verizon

We are the Broadband Forum
http://www.broadband-forum.org

- The Broadband Forum is the central organization driving broadband solutions and empowering converged packet networks worldwide to better meet the needs of vendors, service providers and their customers.

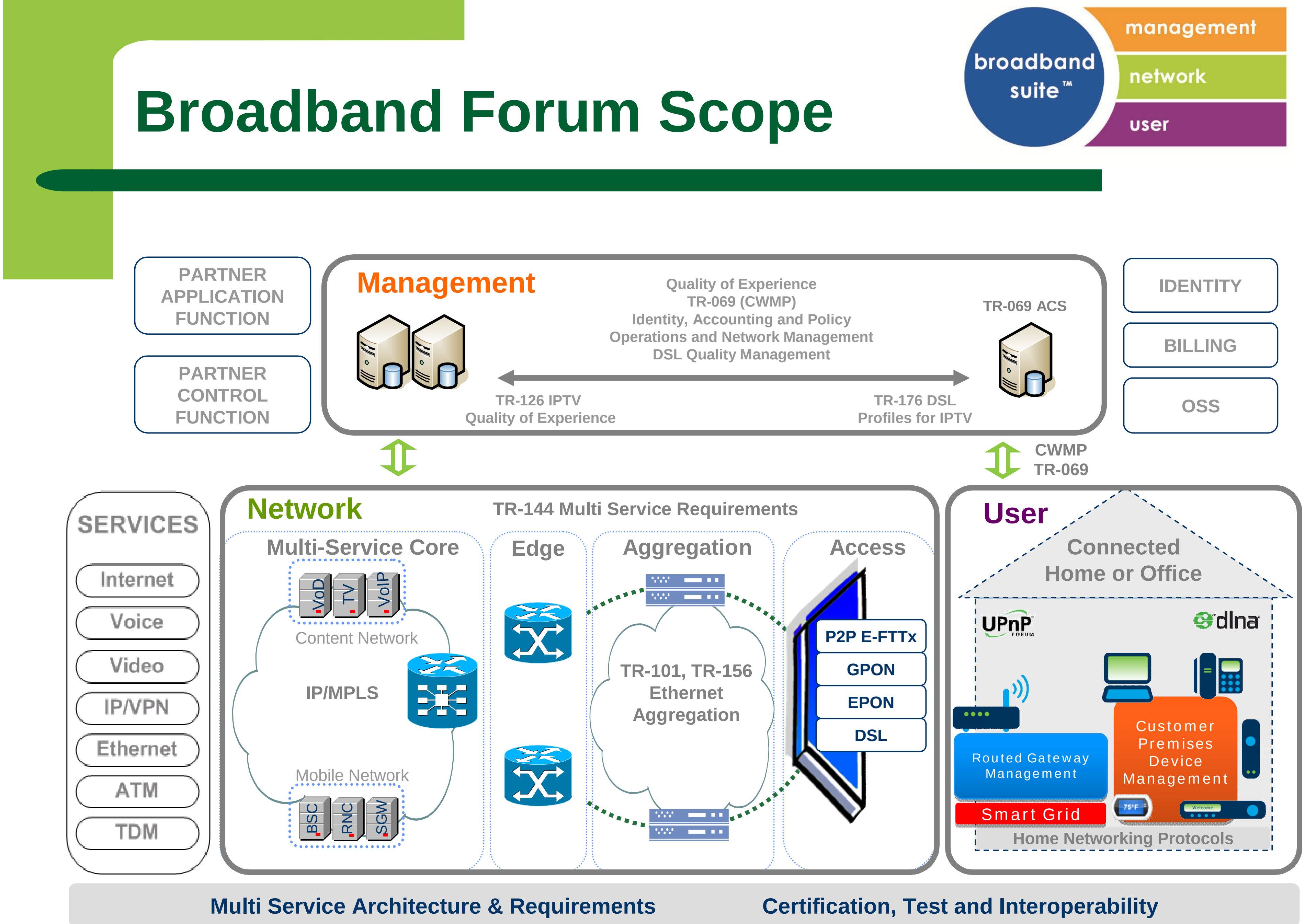
- We develop multi-service broadband packet networking specifications addressing interoperability, architecture and management. Our work enables home, business and converged broadband services, encompassing customer, access and backbone networks.

The BroadbandSuite
Goals and Focus

The BroadbandSuite is broken down into three major domains:

- **BroadbandManagement**
  - **Goal –** enhance network management capabilities and enable an intelligent, programmable control layer that unifies diverse networks
  - **Focus** - empower service providers to deliver and efficiently maintain personalized services that enhance the subscriber experience
- **BroadbandNetwork**
  - **Goal** - establish network architecture specifications to support current and emerging services and applications
  - **Focus** - deliver access, aggregation and core specifications that provide inherent interoperability, quality, scalability and resiliency capabilities from end-to-end
- **BroadbandUser**
  - **Goal** - Define unified networking standards by establishing a common set of CPE capabilities within the business, home and mobile environments
  - **Focus** - Simplify the service delivery process by developing common devices' identification, activation, configuration and maintenance specifications

Broadband Forum Scope



We don’t work alone

Coordinated industry efforts maximize value with minimum overlap

Drivers for IPv6 and IPv4 exhaustion

Why IPv6 is needed, state of IPv4 and conservation techniques, IPv6 support and benefits

broadband forum

Why do we need IPv6 ?

- The main reason is very simple: **To keep the Internet growing!**
- 4.3 billion addressable destinations is simply not enough to address the human population, let alone if people have more than one device permanently connected to the Internet
  - Many addresses are used for infrastructure and not users
  - Many addresses cannot be used due to technical limitations so the actual limit is much lower than 4.3 billion and more likely closer to around 1 billion

IPv4 Address Space Exhaustion

- The good news:

  IANA still has IPv4 addresses in stock

  (IANA holds a total of 7 “/8” blocks on 25-Nov-2010,
  a “/8” block is equivalent to 16,777,216 addresses)
  - 7 available /8 blocks

- The bad news:

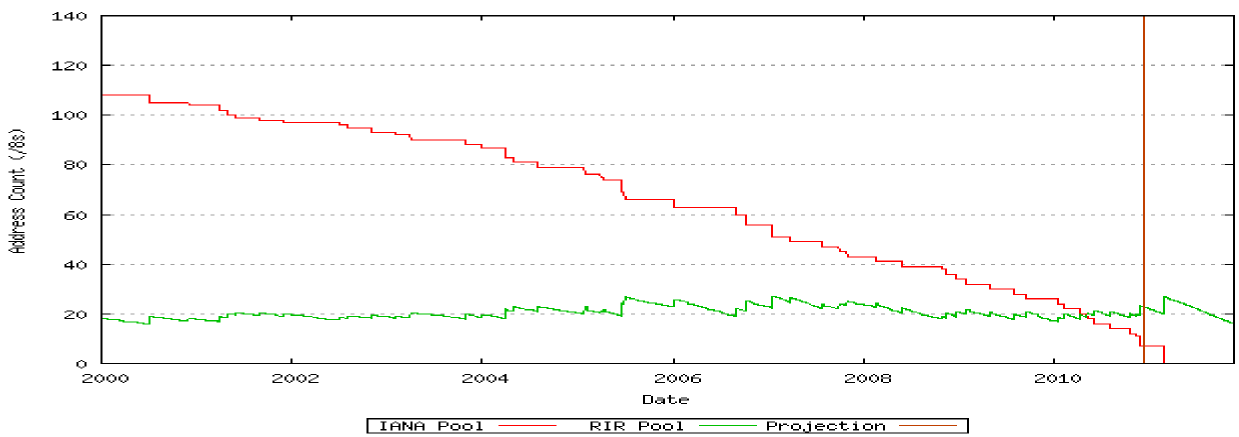
  Statistical analysis (14-Dec-2010) by Geoff Huston (chief scientist APNIC, one of the RIRs) predicts that IANA will run out of IPv4 addresses in February 2011

  Analysis (14-Dec-2010) by Stephan Lagerholm (Consultant - IPv6) predicts IANA unallocated IPv4 address depletion in January 2011

IANA: Internet Assigned Number Authority
RIR: Regional Internet Registry

Projection of IPv4 Address Space Exhaustion

- IANA's pool is decreasing by at least 10 /8's per year
- Geoff Huston projections (as of 14-Dec-2010):
  - IANA unallocated IPv4 Address Pool Exhaustion: **23-Feb-2011** (Red)
  - RIR unallocated IPv4 Address Pool Exhaustion: **20-Nov-2011** (Green)



Source: IPv4 Address Report, Figure 35, http://www.potaroo.net/tools/ipv4/

Human behavior might cause exhaustion sooner than what statistics predict!

IPv4 address conservation techniques

- The Internet technical community did not sit idle with IPv4 address exhaustion on the horizon
  - IPv6 was developed as the ultimate solution
  - Address saving technologies have been developed and deployed
  - Policies at the RIRs have been implemented to make it harder to get addresses
- Multiple approaches taken to preserve IPv4 address space
  - Classless Internet Domain Registry (CIDR)
  - Network Address Translation (NAT)
  - Application specific approaches

We are running out of options to extend the life of IPv4!

Side effects of assignment efficiency

Address use efficiency is not without complications - the higher the efficiency, the higher the cost

- Fragmented address space puts pressure on routing tables
- Management, administration and operations are much more complicated
- Deployment of new services becomes much harder

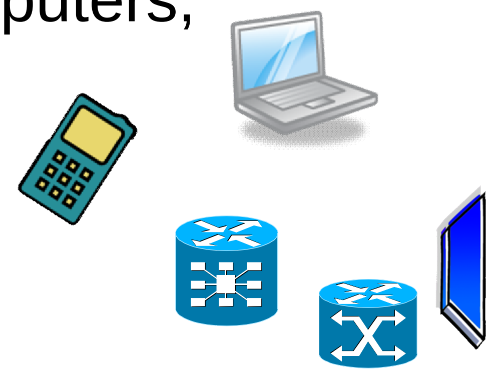
An important reason for the success of IPv4 was adequate address space and ubiquitous reachability

Benefits of large address space

- End-to-end connectivity; more innovation possible
- NAT no longer required
  - Operational benefits (less problems with unsupported applications)
  - Application friendly
  - Easier lawful interception and logging
  - Cost benefits (less packet processing and memory states required)
  - Increased energy efficiency
- Easier (=less costly) to do network planning and to add devices and services to existing deployments

Existing IPv6 support

- Operating systems on devices (computers, etc) found in the home and office
- Mobile devices
- Broadband network equipment
- Security equipment (firewalls, etc)
- Internet and Applications Service Providers
  - Many transit providers already support IPv6
  - Some application service providers have introduced support
    - For search, maps, etc
    - Movie/video downloads



Key drawbacks of having no IPv6 support

- There are not enough private addresses to address all customers (10.0.0.0/8 allows around 16.8M hosts)
- Multiple layers of NAT are hardly manageable and impact performance
- Competitive forces will compel the deployment of transition technologies to allow IPv6 hosts to reach the IPv4 only network and vice-versa

Can you afford not to support IPv6 host and access to IPv6 services?

Key IPv6 attributes and deployment challenges

Definition, how to configure and IPv6 routing in the home

IPv6 has much that you'd recognize…

ICMPv6

DHCPv6

BGP

OSPFv3

FTPv6

IS-IS

Prefix/Mask

But there is so much new as well…

SLAAC

Neighbor Discovery

Link Local Addresses

RS/RA

DAD

IPv6 is more than just a bigger address

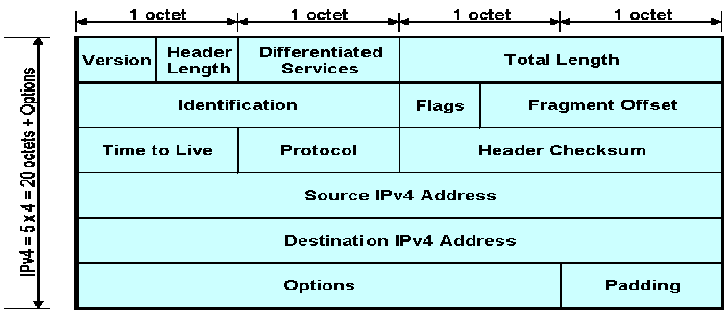
- The goals have been ambitious
  1. Avoid the fragmentation of routing prefixes inherent to IPv4 allocation
  2. Offer network level connectivity and service even when the network is isolated from the global v6 space
  3. Simplify the bootstrapping of a IPv6 host using IPv6 protocols
- Broadband Forum focuses on the impact of IPv6 over the network from the core to the user

Let's explore the addressing architecture

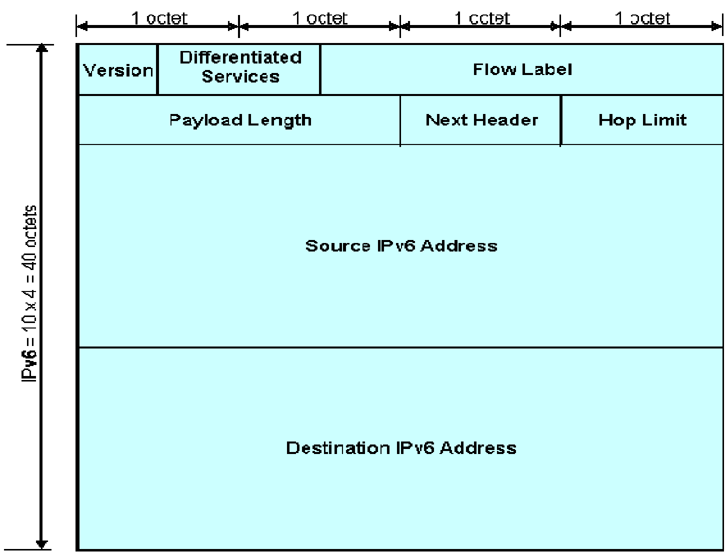
IPv6 Addressing

- IPv6 addresses are 128 bits long
  - 64 bits of “location” and 64 bits of “identity at that location”
  - Many orders of magnitude than IPv4 (4×10^9 to 3.4×10^{38})
- Three different types of addressed entities
  - Unicast: identifies a single interface
  - Multicast: identifies a set of interfaces
  - Anycast: identifies a set of interfaces but resolves to the nearest one
- IPv6 supports scoped addressing
  - Which can mean multiple addresses per interface
  - The scope of the address determines the reachability of the address

IPv4 Header



IPv6 Header



RFC 791, RFC 2460

Scoped addressing

Commonly used scopes

- Link local Address (LLA): Used only for on-link communication. Cannot be used across routers.
  - Used for bootstrapping connectivity
  - Used for node communication on same link and next hop resolution by IGP protocols
- Unique local Address (ULA): Unique within an organizational boundary

  This is for operation in private networks and when the global Internet is not available
- Global unique Address (GUA): Theoretically unique and routable globally
  – Globally unique and routable
  – RIR allocates prefixes to LIRs who assign them

RFC 4007

IPv6 addressing on nodes

- IPv6 addresses are assigned to interfaces, not to nodes
- Each interface has at least one address
  – Every interface MUST have a link-local address
- IPv6 is designed to work with multiple addresses assigned to each interface
  – E.g. Each interface might have a link-local, multiple unique-local and global addresses assigned

How to configure IPv6 addresses

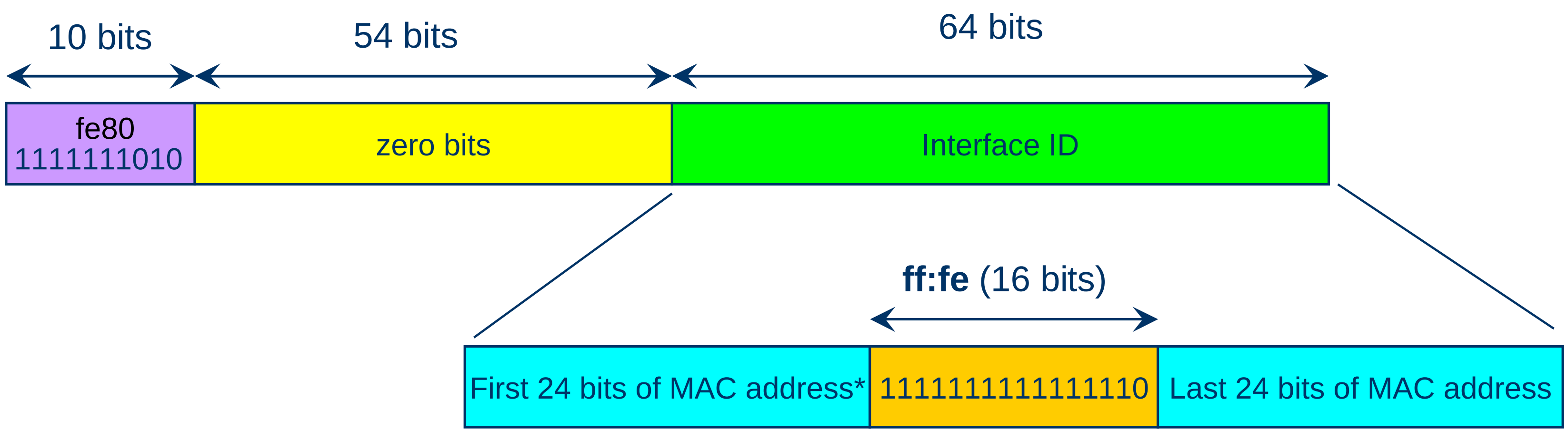
Lowest order 64-bit field of unicast address may be assigned in several different ways

- Self-configured from a 64-bit EUI (Extended Unique Identifier), or expanded from a 48-bit MAC address (*e.g*. Ethernet address)
- Self-generated pseudo-random number (to address privacy concerns)
- Assigned *via* DHCPv6 (IPv6 address assignment or prefix delegation)
- Generated using cryptographic algorithms (e.g. CGA, HBA)
- Manually configured

CGA: Cryptographically generated address
DHCP: Dynamic Host Configuration Protocol
HBA: Hash based address

Link Local Address formation

- The prefix fe80::/10 has been set aside for link-local unicast addresses in the IPv6 addressing architecture
- Every IPv6 host must have a link-local address on each interface
- The most common form of the link local address is based on the 48 bit MAC address of the interface



* Universal/local bit #7 of MAC address is flipped

Stateless address auto-configuration (SLAAC)

- Node forms an address from two pieces of information
  - The top 64 bits of the address are provided by a router using a Router Advertisement message… the location
  - The lower 64 bits are selected by the node; collectively referred to as the Interface Identifier (IID)… the identity
- Interface identifiers can be formed in several ways
  - Formed from the 48 bit MAC address of the interface with the universal/local bit flipped and 16 bits ff:fe inserted in the middle
  - Formed from the IEEE EUI-64 identifier of the interface with the universal/local bit flipped (No bits inserted in the middle)
  - Formed from the private/public keys of the node (CGA)
  - Manually assigned…

CGA – Cryptographically generated IPv6 addresses

Neighbor Discovery (ND) Protocol

- Integral part of the IPv6 protocol suite
- Protocol for solving a set of problems related to the interaction between nodes attached to the same link
  - Discovers presence of nodes on link and their link layer addresses
  - Finds routers to forward packets towards other sub-networks
- Built on top of ICMPv6
- Necessary for SLAAC to work
- Supports multiple link types
  - Multicast capable point-to-point and non-broadcast multiple-access (NBMA)

RFC 2461

ICMP: Internet Control Message Protocol

Neighbor Discovery Messages

- Five different message types
  - Router Solicitation (RS)
  - Router Advertisement (RA)
  - Neighbor Solicitation (NS)
  - Neighbor Advertisement (NA)
  - Redirect
- These messages are used as building blocks to provide multiple functions. E.g. NS is used for both address resolution and Duplicate Address Detection

broadband forum

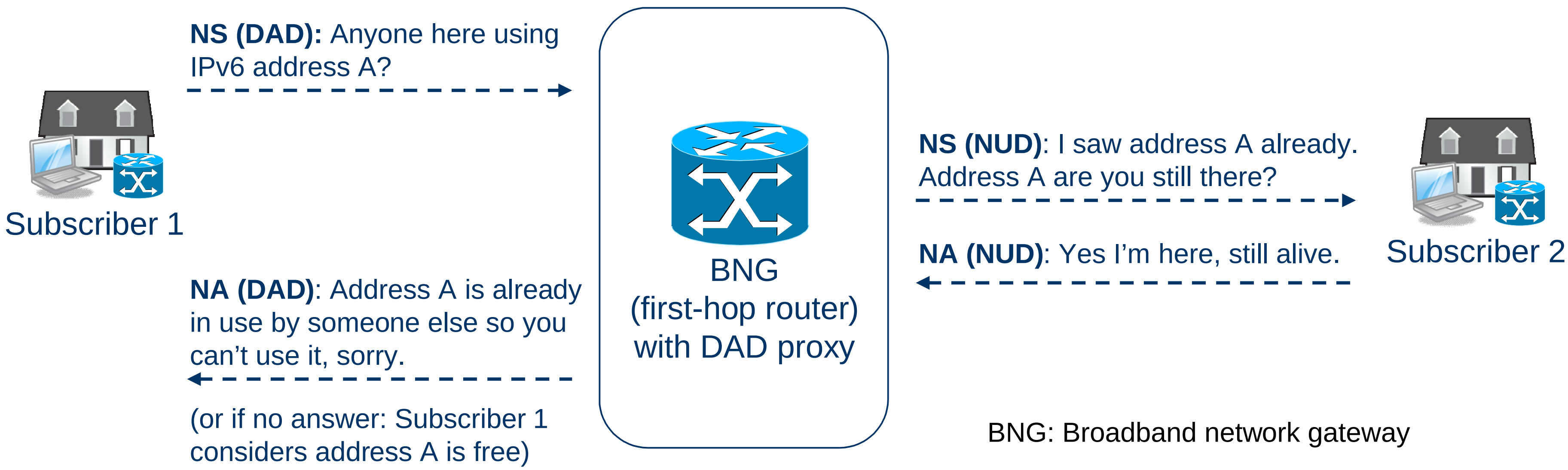
Neighbor Solicitation and Neighbor Advertisement (NS/NA)

NS/NA messages have multiple usages:

- Discover the Link-layer Address associated with a given IPv6 address
- Verify whether a given Link-local Address is still reachable (Neighbor Unreachability Detection - NUD)
- Detect duplicates for a given IPv6 address (Duplicate Address Detection - DAD)

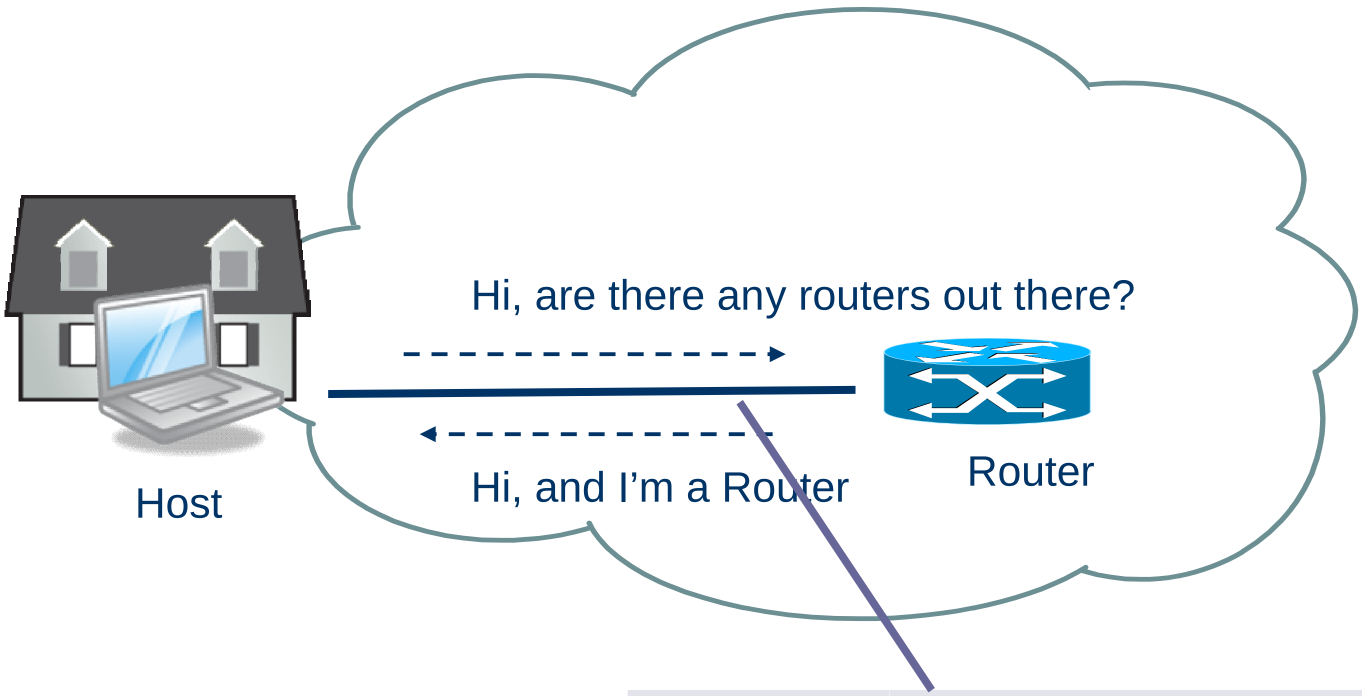
Duplicate Address Detection (DAD)

- When a new IPv6 address is formed, a NS is sent to detect any conflict with other nodes on the same link
  - If a node uses the same IPv6 address it replies with a NA
- In a multipoint to point (N:1 VLAN) architecture, a helper mechanism (DAD proxy) is required on the BNG



Broadband Forum TR-177, Annex B: *Duplicate Address Detection (DAD) Proxy*

SLAAC & Router Advertisements (RAs)



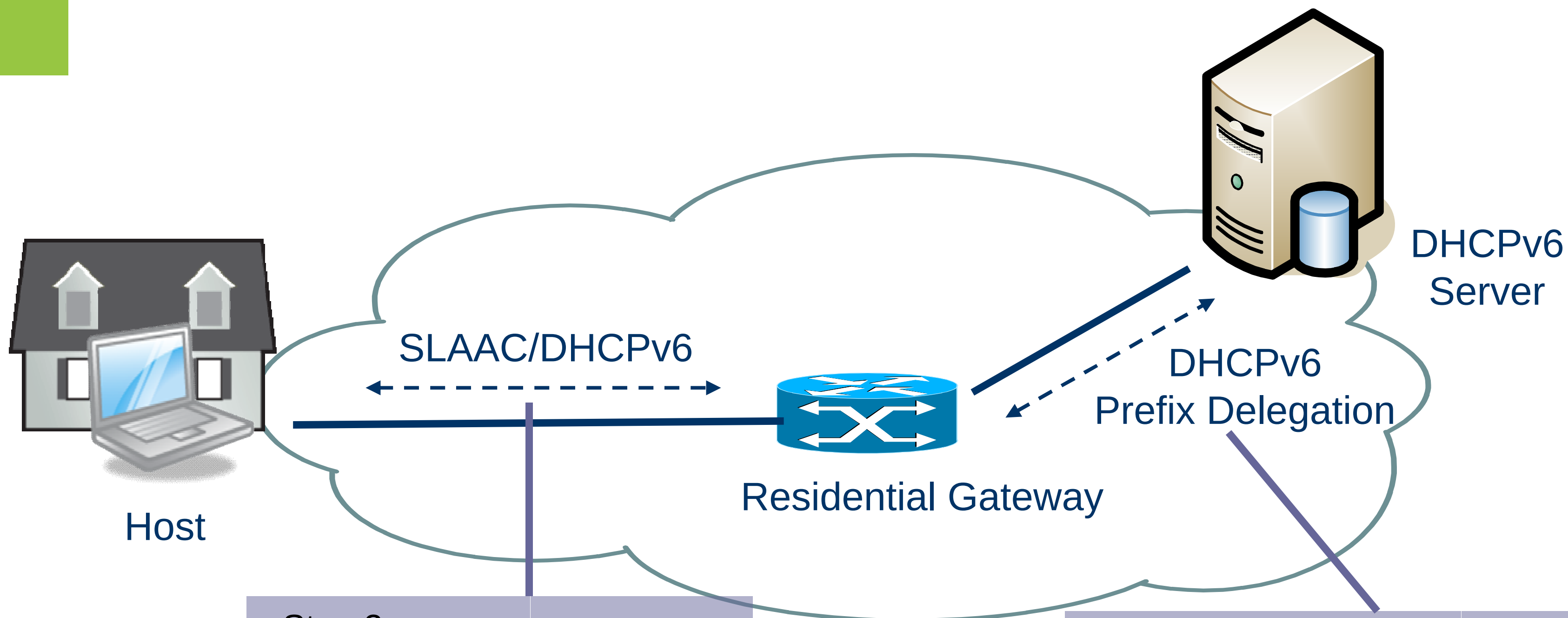
- I can be your default router
- Here's the link Prefix and the MTU
- There is a DNS server around in case you need more information

RA characteristics

- Efficient method of disseminating network wide information
  - Pieces of information the RA can convey are MTU, default route, hop limit and DNS server address
- Perfect fate sharing
  - If a router goes down, it does not advertise
- Inform hosts on whether on-link computations based on the prefix information are do-able or not
- Stateless address auto-configuration possible
  - Hosts form their own address without any overhead or state on the network
- But some hosts need more information and may use stateless DHCPv6 …

broadband forum

DHCPv6 Prefix Delegation



Step 2:
- Distribute complete/partial information received using DHCPv6 prefix delegation

Step 1:
- Here's some prefix(es) and configuration information
- Feel free to distribute downstream

DHCPv6 Characteristics

- Used for distributing client specific information such as addresses, delegated prefixes, and client specific configuration
- Provides centralized control of the IPv6 host configuration
  - For networks that desire this
  - Host address is known by the DHCP server
  - Allows providing additional parameters, such as the address of a TR-069 Auto-Configuration Server

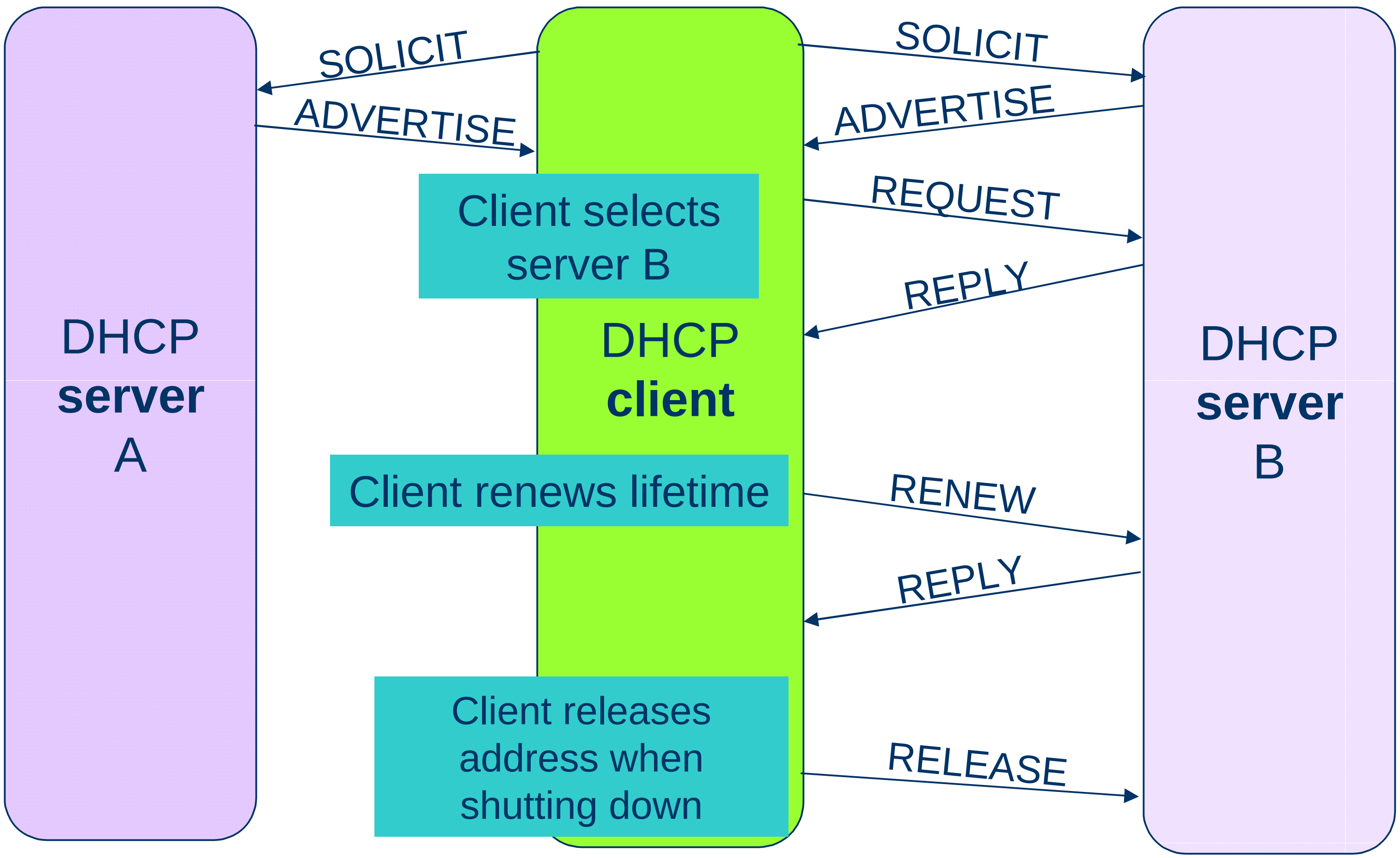
DHCPv6 Basics

- Client uses Link-Local address or addresses determined using other methods to transmit and receive DHCPv6 messages
- Server receives messages from clients using a reserved, Link-Scoped multicast address
  - All_DHCP_Relay_Agents_and_Servers (FF02::1:2)
    - Link-scoped multicast address used by a client to communicate with on-link relay agents and servers
  - All_DHCP_Servers (FF05::1:3)
    - Site-scoped multicast address used by a relay agent to communicate with servers

DHCPv6 (Major) Message Types

Message (Type)	Purpose
SOLICIT (1)	A client sends a SOLICIT message to locate servers.
ADVERTISE (2)	A server sends an ADVERTISE message to indicate that it is available for DHCP service, in response to a SOLICIT message received from a client.
REQUEST (3)	A client sends a REQUEST message to request configuration parameters, including IP addresses and prefixes from a specific server.
REPLY (4)	A server sends a REPLY message containing assigned addresses (or prefixes) and configuration parameters in response to a SOLICIT, REQUEST, RENEW, REBIND message received from a client.
RENEW (5)	A client sends a RENEW message to the server that originally provided the client's addresses and configuration parameters to extend the lifetimes on the addresses assigned to the client.
REBIND (6)	A client sends a REBIND message to any available server to extend the lifetimes on the addresses assigned to the client.

DHCPv6 Machinery



DHCPv6 Prefix Delegation

- New options for DHCPv6 for delegation of prefixes
  - Requesting Router indicates interest in obtaining prefixes
  - Delegating Router assigns prefixes to Requesting Router
- Requesting router indicates interest in prefix delegation by including an option (IA_PD) in Solicit message
  - Delegating router indicates availability of prefix(es) by including them in Advertise message
- Requesting router asks for prefix(es) in Request message
  - Delegating router delegates prefixes by including Prefix option in Reply message

IPv6 Routing in the Home

Topics

1. How much address space should ISP allocate to a home?
2. Prefix delegation
3. Security implications

How much address space should an ISP allocate to a home?

- Addressing should not be the limiting factor for the digital home
  - Strong desire to contain L2 broadcast/multicast to specific media - For example, Gigabit Ethernet multicast does not leak into bandwidth constrained wireless LAN
- Prefix length may vary across regions
  - ISPs should follow recommendations from respective RIRs
  - Most RIRs recommend a /56 to the home

Prefix delegation (PD)

- Prefix delegation is a means of transferring authority over a set of prefixes to a CPE
- Once an RG is up and running, it requests a prefix range for local use
- From this prefix range, the RG can assign prefixes/addresses to devices attached on its LAN interfaces using SLAAC or DHCPv6

Security

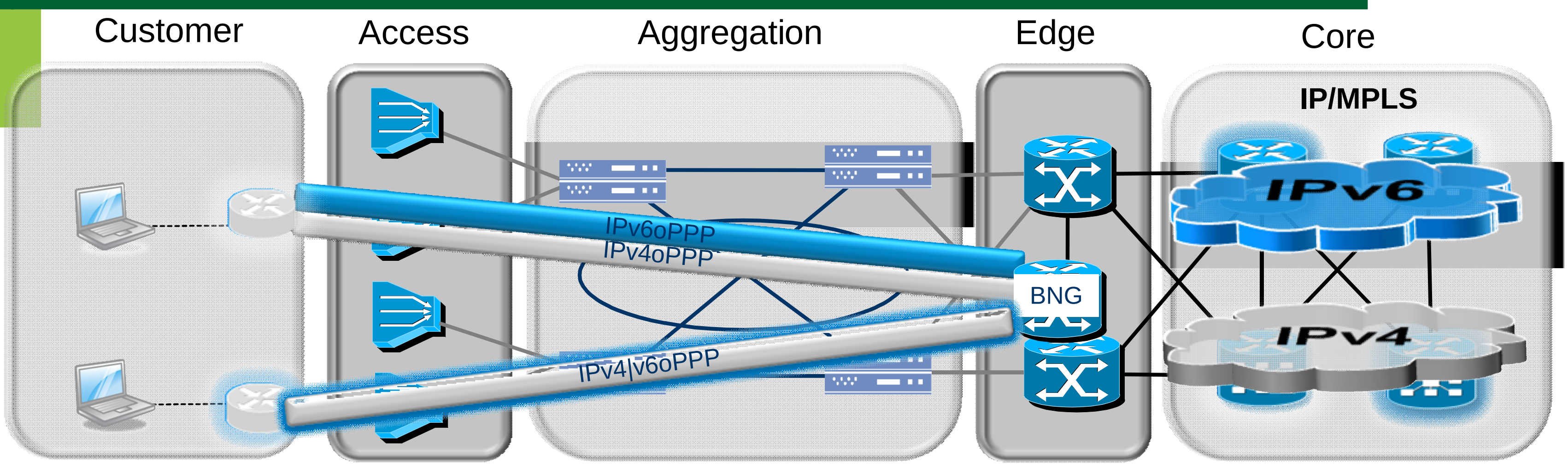
- In IPv4 deployments, network address translation protects home network devices/applications from communications initiated from the web
  - Outgoing transactions from the home create temporary pin holes in the NAT
- In IPv6, a stateful firewall on the RG can provide similar protection
  - UPnPv6 can be used to authorize selected communications initiated from the web

IPv6 strategies for broadband access to support Internet access and new services

Preparing for IPv6 integration: dual stack, dual stack with tunneling and IPv6-only to IPv4-only translation

PPP Model

PPP Session(s) with Dual-stack IPv4/IPv6

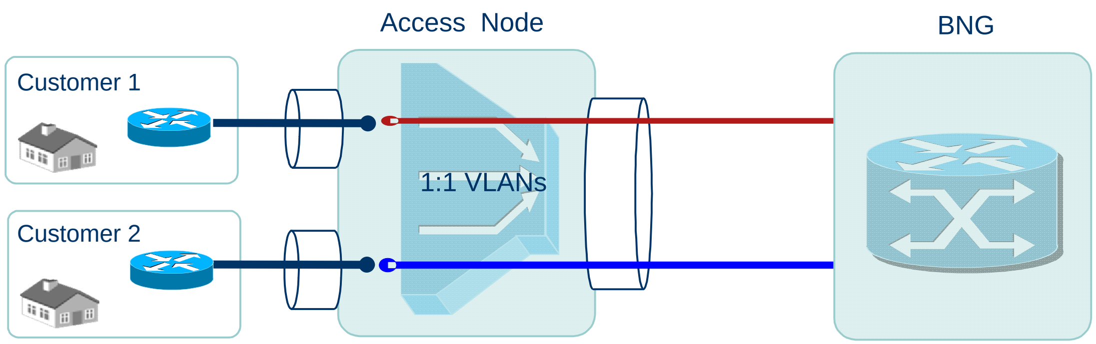


- Native Dual-Stack IPv4/IPv6 service on RG LAN side
- NO changes in existing Access/Aggregation Infrastructure
- One PPPoE session per Address Family (IPv4 or IPv6) or one PPPoE session carrying both IPv4 and IPv6 NCPs running as ships in the night
  - As an option, PPPoE session from Host and bridged on RG
- IPCPv6 for Link-Local address
- SLAAC or DHCPv6 can be used to number the WAN link with a Global address
- DHCPv6-PD is used to delegate a prefix for the Home Network

Broadband Forum TR-187: *IPv6 for PPP Broadband Access*

IPCP: IP Control Protocol
NCP: Network Control Protocol
RG: Residential Gateway

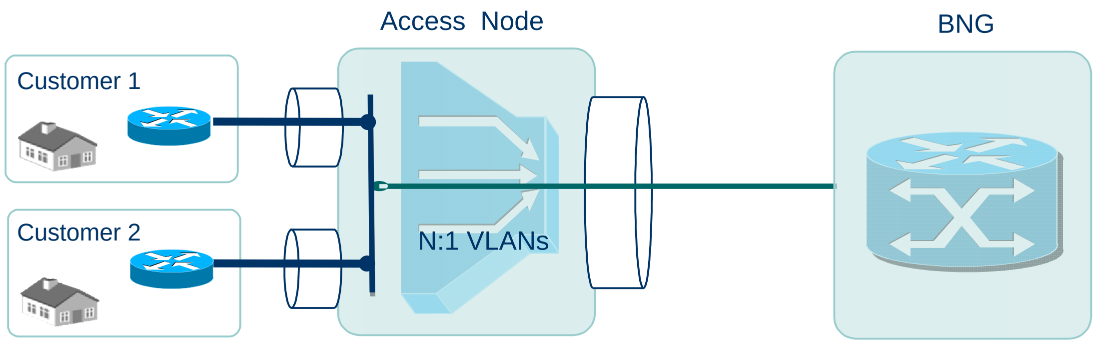
IPv6oE Model
IPv6 over Ethernet with 1:1 VLAN



- At L2, IPv6oE with 1:1 VLANs resembles PPPoE
  - No change to Access Node to support IPv6
  - Point-to-point broadcast domain does not require any special L2 forwarding constraints on Access Node, and SLAAC and Router Discovery work the same
  - Line-identifier used for 1:1 VLAN mapping= (S-TAG, C-TAG)
- However 1:1 VLANs and IPoE *do* require some extra BNG functionality
  - Need to run Neighbour Discovery
- DHCPv6-PD or DHCPv6 server capabilities could be used at BNG to delegate a prefix for the Home Network

IPv6oE Model

IPv6 over Ethernet with N:1 VLAN



- Requires IPv6 specific functions in Access Nodes
  - Security requirements: IPv6 anti-spoofing, router advertisement (RA) snooping, lightweight DHCPv6 relay, etc
  - Multicast requirements: MLDv2, MLDv2 filtering
- Subscriber line identification
  - VLAN does not provide a unique subscriber line identifier
  - Lightweight DHCP Relay Agent on the Access Node to convey subscriber line-identifier
- N:1 challenges due to non-broadcast multiple access (NBMA) nature of split horizon forwarding
  - DAD proxy in BNG allows DAD operation across N:1 VLAN

MLD: Multiple Listener Discovery

broadband forum

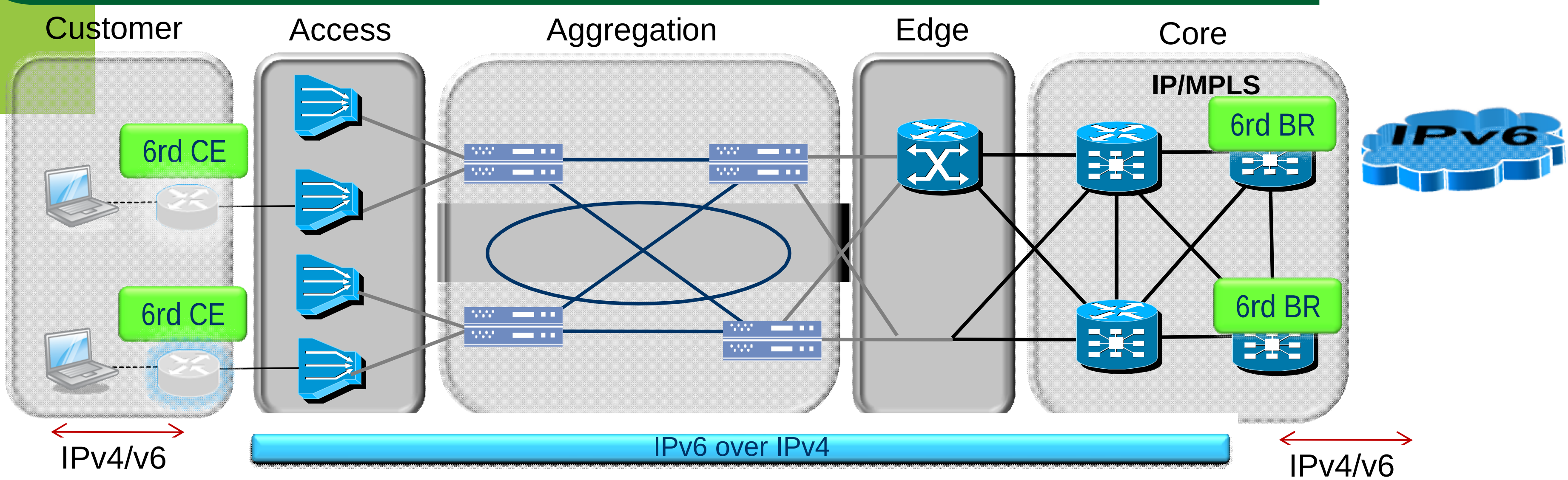
Agenda

Preparing Step: IPv6 Integration

- Dual-Stack IPv4 and IPv6
- Dual Stack with Tunneling
- IPv6-Only to IPv4-Only Translation

IPv6 Services over IPv4-only network

6rd: IPv6 connectivity using tunnels



- Introduction of two Components: 6rd CE (Customer Edge) and 6rd BR (Border Relay)
- Automatic Prefix Delegation on 6rd CE
- Simple, stateless, automatic IPv6-in-IPv4 encap and decap functions on 6rd (CE & BR)
- IPv6 traffic automatically follows IPv4 Routing
- 6rd BRs addressed with IPv4 anycast for load-balancing and resiliency
- No impact on existing access and aggregation networks

6rd: IPv6 rapid deployment

RFC 5969

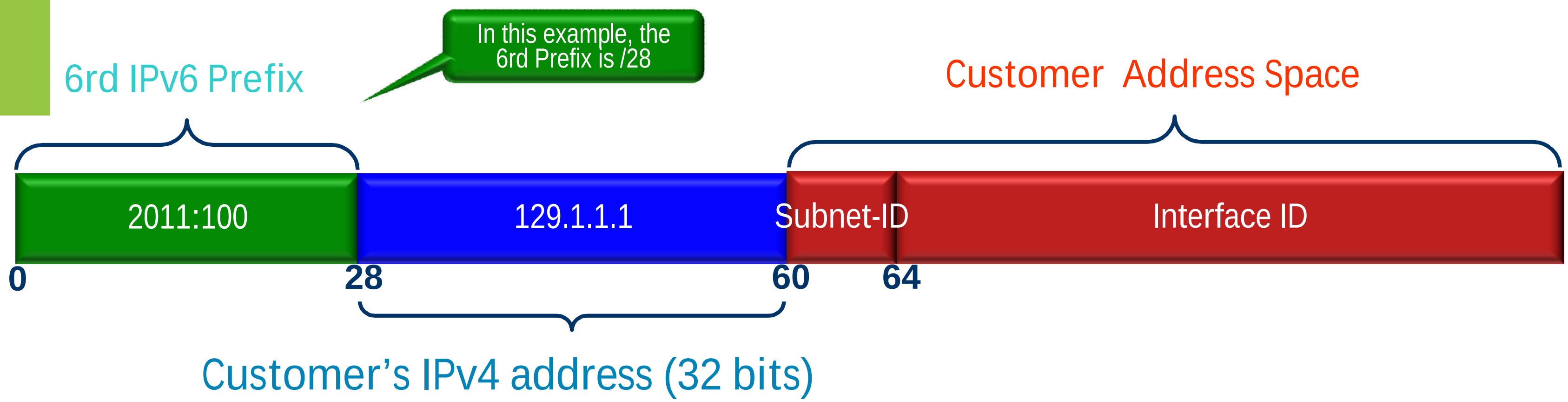
Broadband Forum TR-124 I2: ***Functional Requirements for Broadband Residential Gateway Devices***

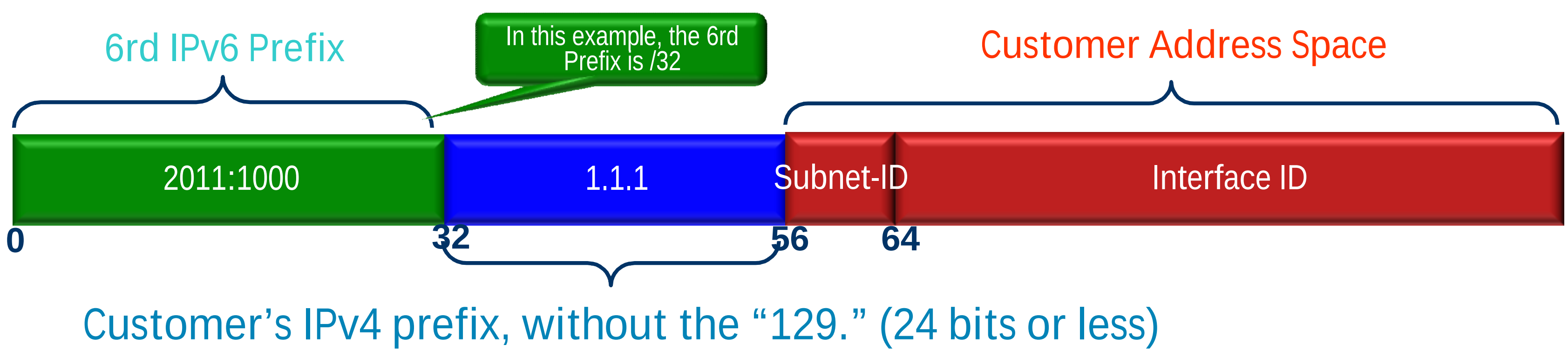
Broadband Forum WT-242: ***IPv6 Transition Mechanisms for Broadband Networks***

3 Key Components of 6rd

- IPv6 Prefix Delegation Derived from IPv4
  - No need for DHCPv6 on 6rd CE WAN interface
  - No need for DHCPv6 server in the network
  - Supports Global IPv4 or NATed IPv4 in same deployment
- Stateless Mapping and Encapsulation of IPv6 over IPv4 (RFC 4213)
  - IPv4 encapsulation automatically determined from each packet's IPv6 destination
  - No per-subscriber tunnel state or provisioning, hence single dimension scaling (data-plane) on 6rd BR
- IPv4 Anycast to Reach BR
  - Simplify network 6rd BR placement, load-balancing and/or redundancy across multiple 6rd BRs

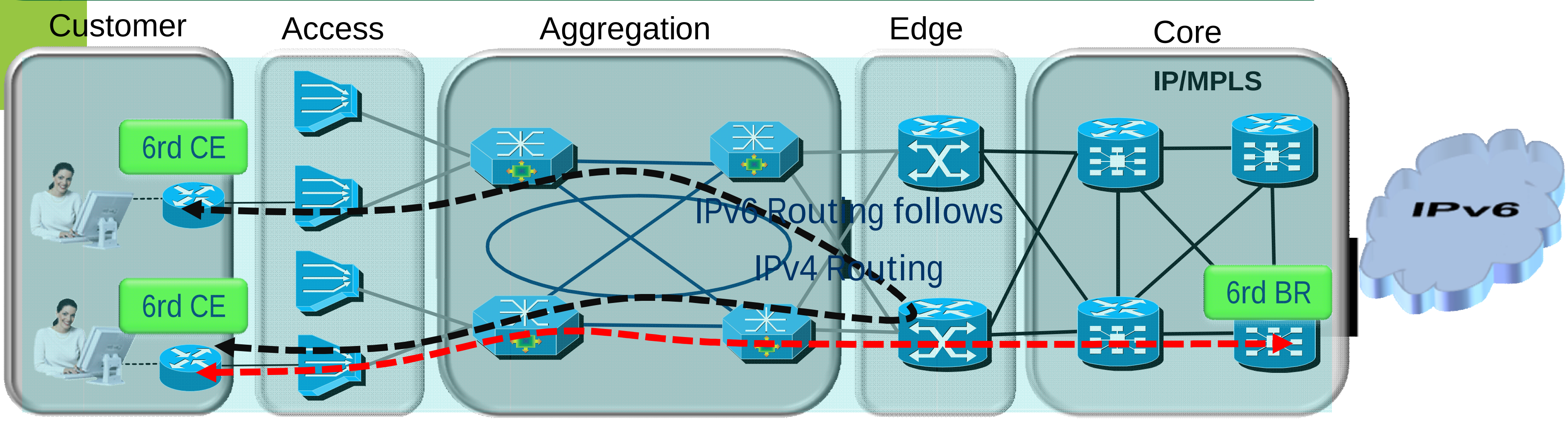
6rd Automatic Prefix Delegation





Any number of bits may be masked off, as long as they are common for the entire domain (applicable to aggregated global IPv4 space as well).

6rd Stateless mapping and encap/decap



IF 6rd IPv6 Prefix Positive Match

THEN Encap in IPv4 with embedded address

Destination Inside 6rd Domain

•2001:100	•8101:0101	•Interface ID

ELSE (6rd IPv6 Prefix Negative Match)

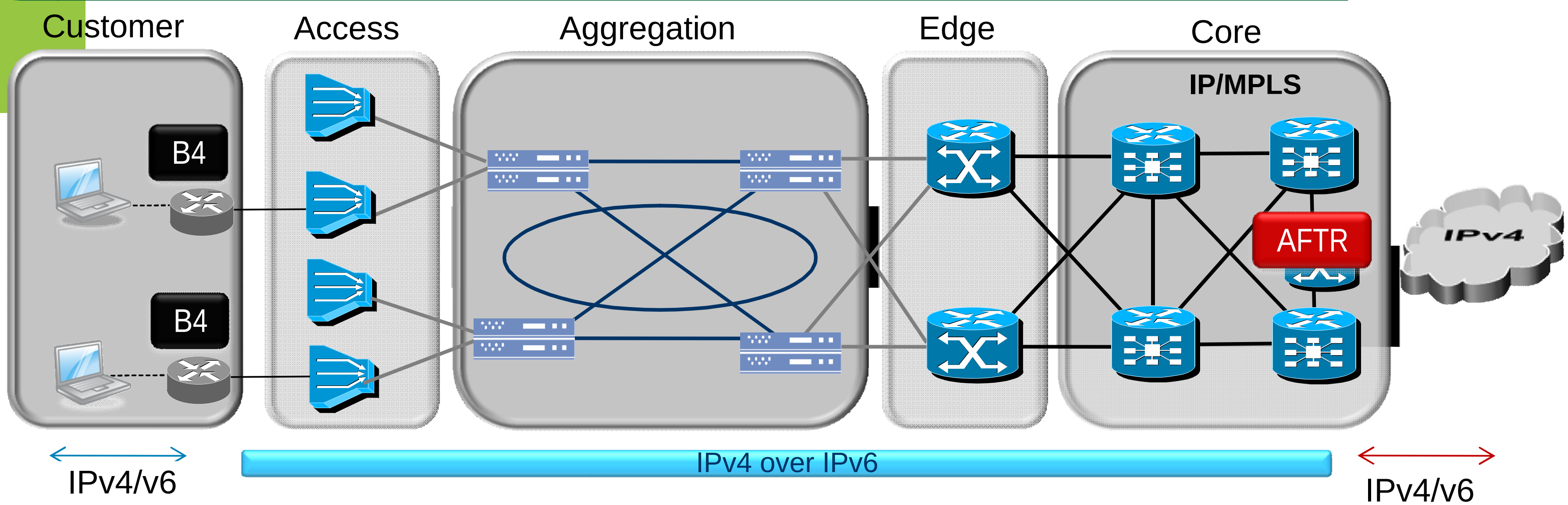
ENCAP with BR IPv4 Anycast Address

Destination Outside 6rd Domain

•"Not 2001:100…"	•Interface ID

IPv4 services over IPv6 network

Dual-Stack Lite (DS-Lite): IPv4 connectivity using tunnels

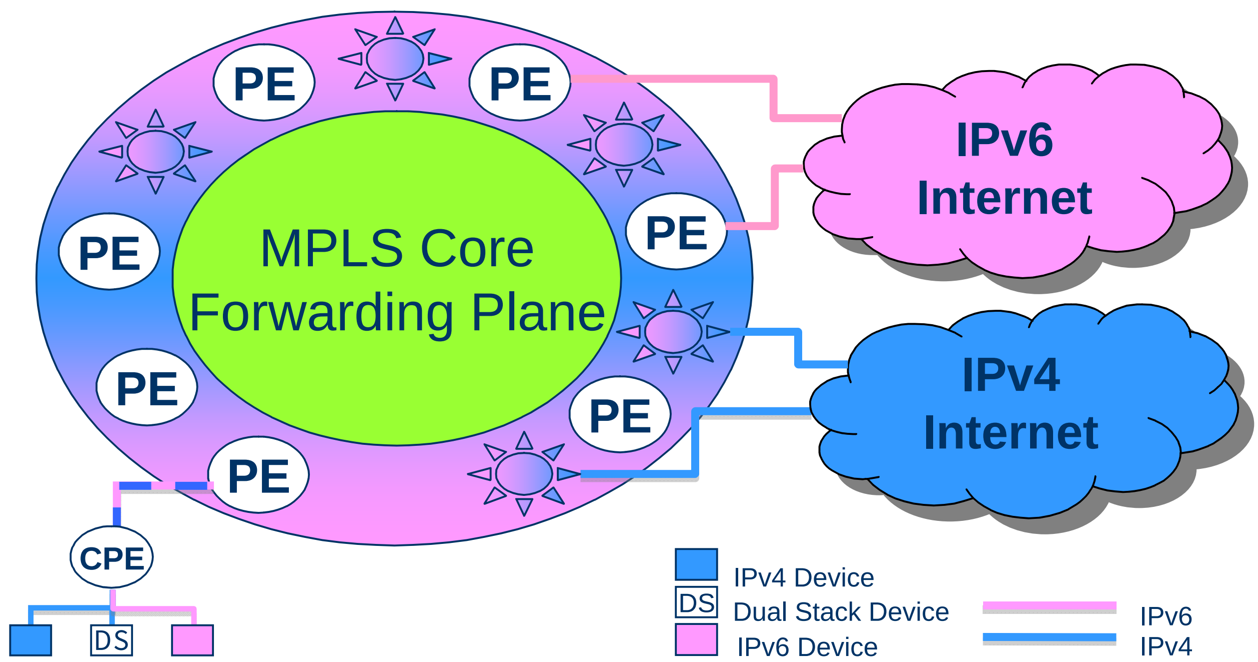


- Conserve IPv4 addresses by offering IPv4 services on top of a IPv6 network
- Access, Aggregation, Edge, Core and Network services (DNS and DHCP) support IPv6
- Introduction of two components initiating and terminating IPv4 over IPv6 tunnel:
  - Basic Bridging Broadband Element (B4) which typically sits in the RG
  - Address Family Translation Router (AFTR) performing NAT44 instead of RG
- Start DS-Lite deployment while some traffic remains native IPv4

Broadband Forum WT-242: ***IPv6 Transition Mechanisms for Broadband Networks***
Broadband Forum TR-124: ***Functional Requirements for Broadband Residential Gateway Devices***

MPLS 6PE/6VPE for IPv6 traffic transport

MPLS edge routers need to support 6PE/6VPE capabilities, allowing the MPLS core network to transport IPv6 traffic as ships in the night.



6PE: IPv6 Provider Edge

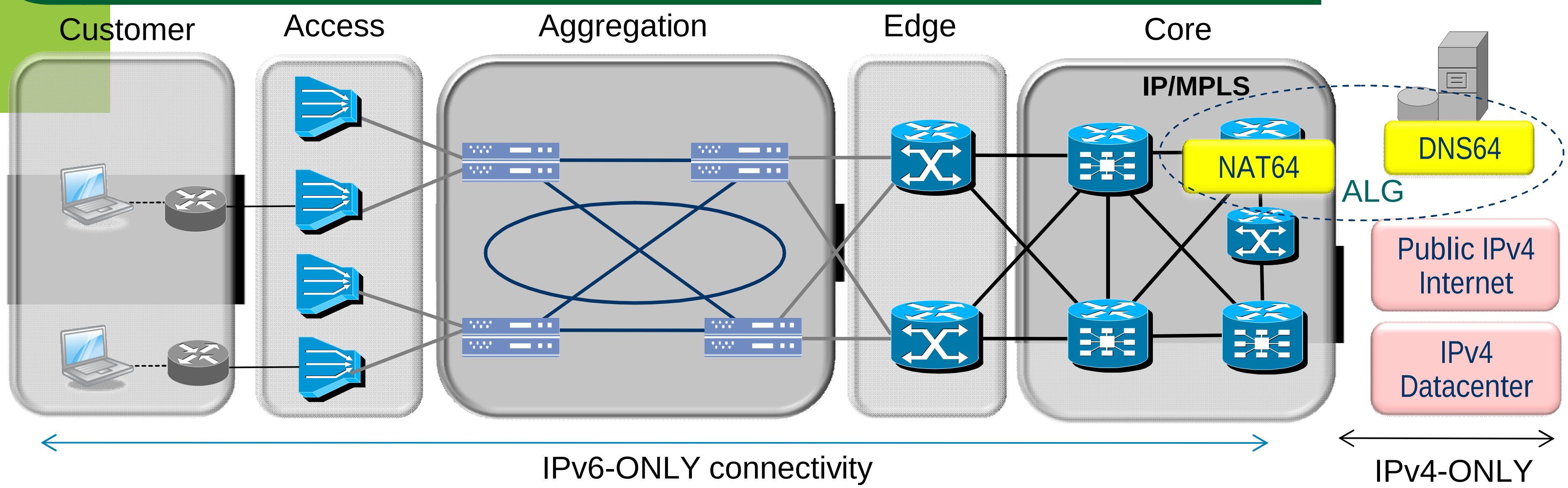
6VPE: IPv6 VPN Provider Edge

Agenda

Preparing Step: IPv6 Integration

- Dual-Stack IPv4 and IPv6
- Dual Stack with Tunneling
- IPv6-Only to IPv4-Only Translation

Connecting IPv6-only with IPv4-only: AFT64

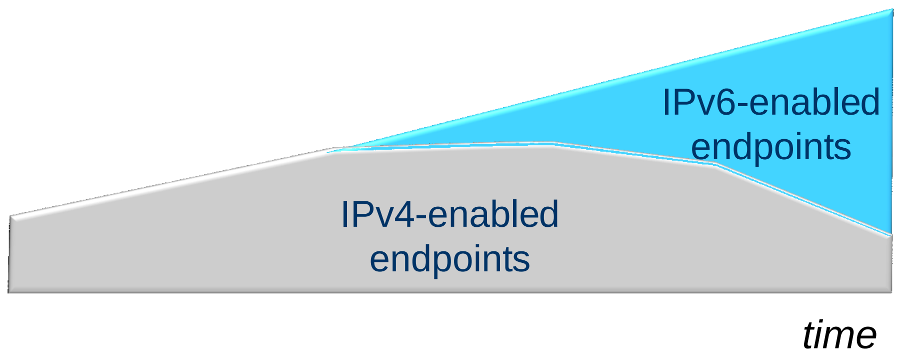


- AFT64 technology is only applicable in case where there are IPv6-only end-points that need to talk to IPv4-only end-points (AFT64 for going from IPv6 to IPv4)
- Application Layer Gateway (ALG) is required
- Key components includes NAT64 and DNS64 (can co-exist)
- <u>Assumption:</u> Network infrastructure supports IPv6 and some hosts have fully transitioned to IPv6

Conclusion

Multiple technologies are available to serve various IPv6 migration strategies:

- 6rd: start offering IPv6 services, over the top of an IPv4-only network
- Add IPv6 capabilities to the network: TR-187, WT-177, 6rd
- DS-Lite: save IPv4 addresses, maintain IPv4 services over the top of an IPv6 capable network
- Avoid any multiplication of NAT (i.e. NAT444)



Summary

Summary

- IPv4 address space likely to be exhausted by end of 2011
- More IP addresses required to connect growing number of users, devices, infrastructure, etc for Internet growth
- IPv6 is the solution for IPv4 address exhaustion
  - Helps eliminate addressing as a limiting factor in the digital home with a global address that allows the removal of NAT
- Several strategies to begin integrating IPv6 support into broadband access for Internet access and new services
  - Dual-stack IPv4 and IPv6, Tunneling IPv6 over IPv4 (6rd), Tunneling IPv4 over IPv6 (DS-Lite) and IPv6-Only to IPv4-Only translation
  - The Broadband Forum facilitates IPv6 deployments by specifying Routing Gateway, Access, Aggregation and Edge Node functional requirements enabling a smooth migration
- IPv4 and IPv6 will need to coexist for many years

Related Broadband Forum documents

- TR-124i2: *Functional Requirements for Broadband Residential Gateway Devices*
- TR-177: *IPv6 in the Context of TR-101*
- TR-187: *IPv6 for PPP Broadband Access*

Work in Progress

- WT-242: *IPv6 Transition Mechanisms for Broadband Networks*
- PD-193: *IPv6 updates to TR-069 related TRs*

Background:

- TR-101: *Migration to Ethernet Based DSL Aggregation*
- TR-069: *CPE WAN Management Protocol*

Related Standards Organizations and Consortiums

- **Broadband Forum:** http://www.broadband-forum.org
- **HGI:** http://www.homegatewayinitiative.org/
- **IETF:** http://www.ietf.org
- **IPv6 Forum:** http://www.ipv6forum.com/
- **UPnP Forum:** http://www.upnp.org/

Thank you for attending the IPv6 in Broadband Networks Tutorial

For more information, visit us at

http://www.broadband-forum.org

broadband forum

Abbreviations

6PE – IPv6 Provider Edge
6rd – IPv6 rapid deployment
6VPE – IPv6 VPN Provider Edge
AFTR – Address Family Translation Router
ALG – Application Layer Gateway
APNIC – Asia Pacific Network Information Center
B4 – Basic Bridging Broadband Element
BGP – Border Gateway Protocol
BNG – Broadband Network Gateway
BR – Border Router
CE – Customer edge
CGA – Cryptographically Generated Address
CIDR – Classless Internet Domain Registry
DAD – Duplicate Address Detection
DHCP – Dynamic Host Configuration Protocol
EUI – Extended Unique Identifier
FTP – File Transfer Protocol
GUA – Global Unique Address
HBA – Hash based address
HGI – Home Gateway Initiative
IANA – Internet Assigned Number Authority
ICMP – Internet Control Message Protocol
IID – Interface Identifier
IP – Internet Protocol
IPCP- Internet Protocol Control Protocol
IS-IS – Intermediate System to Intermediate System
LIR – Local Internet Registry
LLA – Link Local Address
LNS – L2TP Network Server
MAC – Media Access Control
MLD – Multicast Listener Discovery
NA – Neighbor Advertisement
NAT – Network Address Translation
NBMA – Non Broadcast Multiple Access
NCP – Network Control Protocol
NS – Neighbor Solicitation
OSPF – Open Shortest Path First
PD – Prefix Delegation
PPP – Point-to-Point Protocol
RA – Router Advertisement
RG – Residential Gateway
RIR – Regional Internet Registry
RS – Route Solicitation
SLAAC – Stateless Address Auto-Configuration
ULA – Unique Local Address
UPnP – Universal Plug & Play
v4 – Version 4
v6 – Version 6