RIPE NCC

RIPE NETWORK COORDINATION CENTRE

IPv6 Advanced Training

Training Course

RIPE NCC Learning & Development

Schedule

Day Planning:

09:00 - 09:30	Coffee, Tea
11:00 - 11:15	Break
13:00 - 14:00	Lunch
15:30 - 15:45	Break
17:30	End

Introduction

- What's your name?
- What's your job?
- Experience with IPv6?
- What do you want to learn from this training?

IPv6 Advanced: Course Overview

Introduction

Get Approval

- Get the green light
- Project planning

Get Ready

- Create an addressing plan
- Get IPv6 training
- Build a test environment
- Adopt a transition strategy

Deploy

- Backbone network
- Access network
- Enterprise network
- Datacenter network
- Cloud networks

Manage

- Troubleshooting
- Monitoring

Tips and Tricks

Poll!

Where is **your organisation** at with IPv6 deployment?

https://ripe-ncc.typeform.com/ipv6a1

Check the **results**

Introduction

How Do You Expand Your Networks Today?

No Action / I don’t care

No longer a choice

Competitors are already implementing IPv6.

Extend life of IPv4

You've already done this

Concerns regarding NAT

Is it feasible to acquire IPv4 address space from the marketplace?

Deploy IPv6

That's where we are now!

The ultimate goal is 

IPv6

Guarantee continuity, growth and innovation/new services

How to Start Deployment of IPv6?

There is no right or wrong way!

We propose a **phased** approach

Which is **systematic** and **holistic.**

1. Get approval	2. Get Ready	3. Deploy	4. Manage
Management's decision and sign-off, project planning	Preparations for the deployment including addressing plans	The actual deployment phase full of technical changes and configurations	Keeping your IPv6 network up and running, and up-to-date

Detailed Overview of the Four Phases

1. Get Approval	2. Get Ready	3. Deploy	4. Manage

• Getting the green light from decision makers
• Create a project plan:
  - Identifying the scope of the project
  - Identify the involved teams, services, equipment and the required skills
	• Create an addressing plan:
	  - Address allocation
	  - Addressing structure and best practices
	  - IP Address Management Tools
	• Get training
	• Build a test environment
	• Adopt a transition strategy
		• Deploy in backbone networks:
		  - IPv6 in IGPs & BGP & MPLS
		• Deploy in access networks:
		  - Fixed and Mobile access networks
		  - Transition mechanisms
		• Deploy in enterprise networks:
		  - IPv6 in enterprise host networks
		  - Multihoming
		• Deploy in datacenter networks
		• Deploy in cloud networks
			• Troubleshooting IPv6 networks:
			  - Tools for troubleshooting
			• Monitoring IPv6 networks:
			  - RIPE Atlas as a monitoring tool

Get Approval

Tasks in This Phase

1. Getting the **green light** from decision makers
2. Create a **project plan:**
   - Identify the scope of the project
   - Identify the involved teams, services, equipment and the required skills

Get the Green Light

IPv6 Has Technical Advantages

- No more IP scarcity
- End-to-end communication without NAT/CGN/LSN
- Numbering flexibility
- IPv6 deployment is unavoidable for sustainable growth, it is better to act early

But they're not enough to convince decision makers

Poll

How **supportive** is your management of IPv6 deployment?

https://ripe-ncc.typeform.com/ipv6a2

Check the **results**

Convincing Decision Makers

Show potential areas of cost savings:

- **Price of IPv4 addresses** needed for new projects (network expansion) compared to IPv6
- Cost of acquiring and operating **NAT** and hidden costs (troubleshooting, keeping logs)
- Cost of **postponing the unavoidable transition**
- Potential profits by **selling of existing IPv4** addresses
- **High IPv4 cost on major Cloud Networks** (Google, AWS, etc.)

Convincing Decision Makers - More Reasons

1. Compliance - laws and regulations

2. Industry pressure / customer demands

   - Not offering IPv6 causes sub-optimal service offering, creates a competitive disadvantage

3. Innovation

4. Prestige/image

What Might be Affected by Deploying IPv6?

You need a comprehensive **analysis** of the **impact** of:

Hardware in your network

routers, firewalls, switches, servers, etc.

Services you provide

broadband network service - mobile and fixed, IMS service, zero touch provisioning service, web service, etc.

Applications and **software** you use

billing software, CRM software, etc.

Network protocols you use

OSPF, IS-IS, BGP, DNS, DHCP, etc.

Your **staff**

Training your staff and using their man hours.

Questions

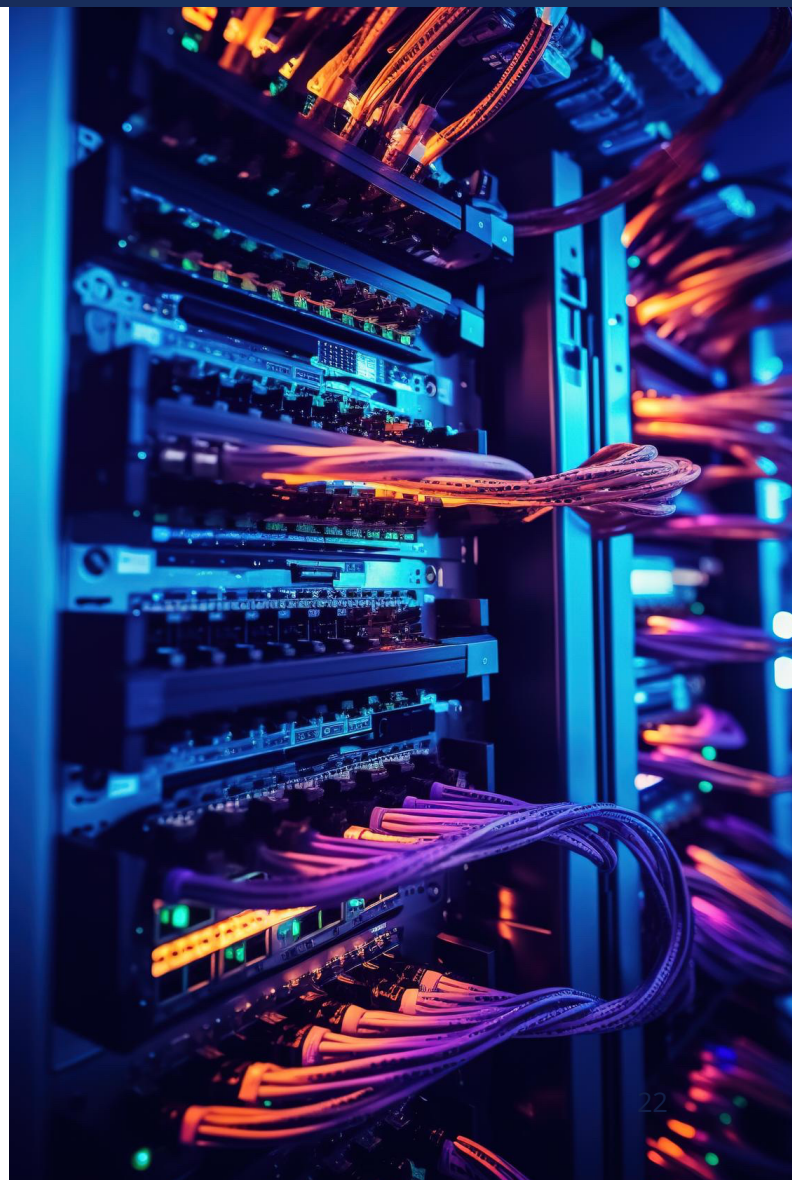
Project Planning

Nine critical elements of a good project plan:

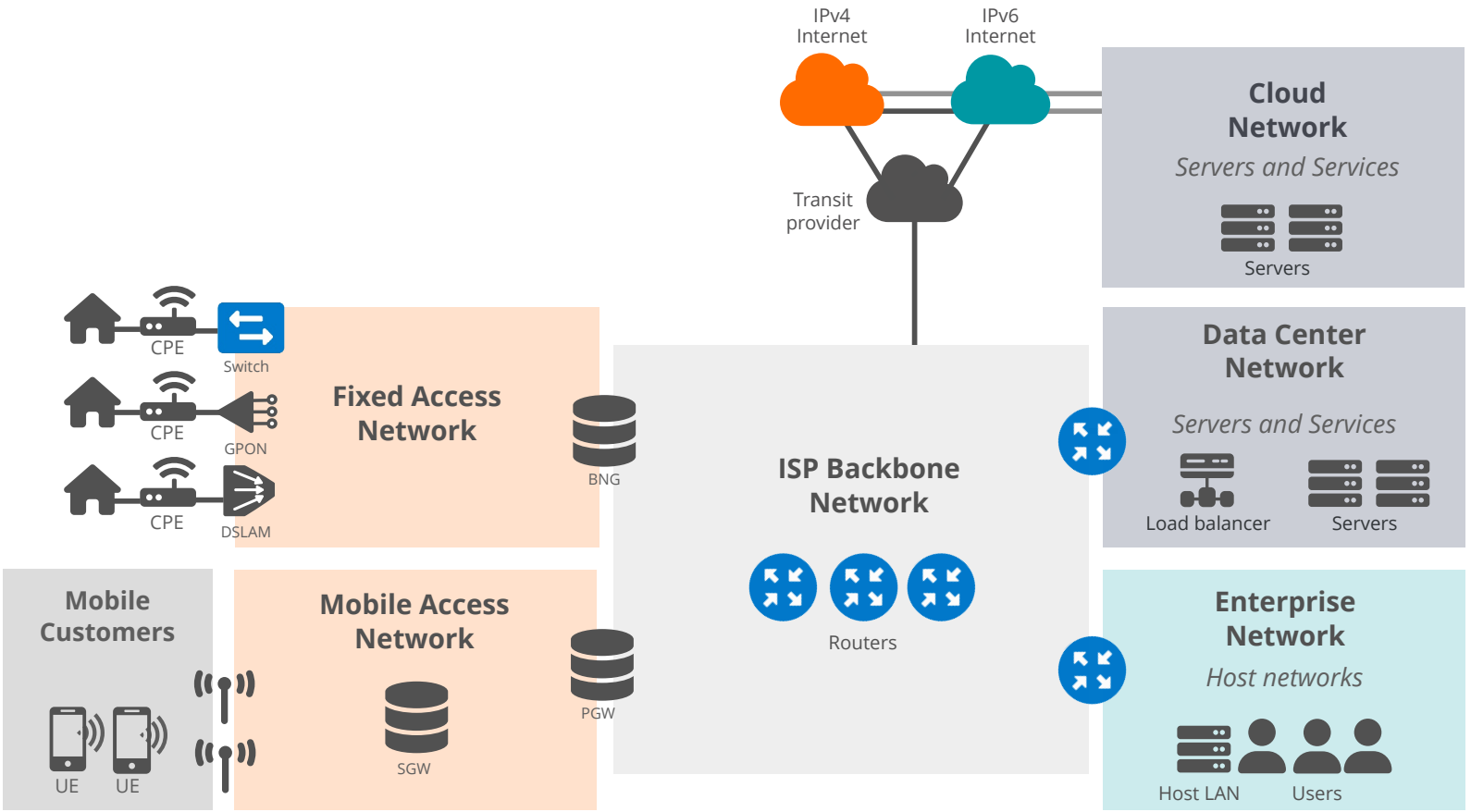
- Goals
- Scope (parts of network / priorities)
- Cost
- Schedule
- Stakeholders
- Communications
- Risks
- Requirements & dependencies
- Human resources

Scope: Parts and Types of Your Network

- Backbone Network
- Access Network(s)
- Data Center Network
- Host LAN
- Enterprise Network
- Cloud Network



Reference Architecture



Scope: Assess Your Network and Prioritisation

Decide where to start based on:

- Hardware readiness
- Software readiness
- Customer needs and demands
- Providers constraints
- Dependencies
- Skills of human resources
- Regulatory needs

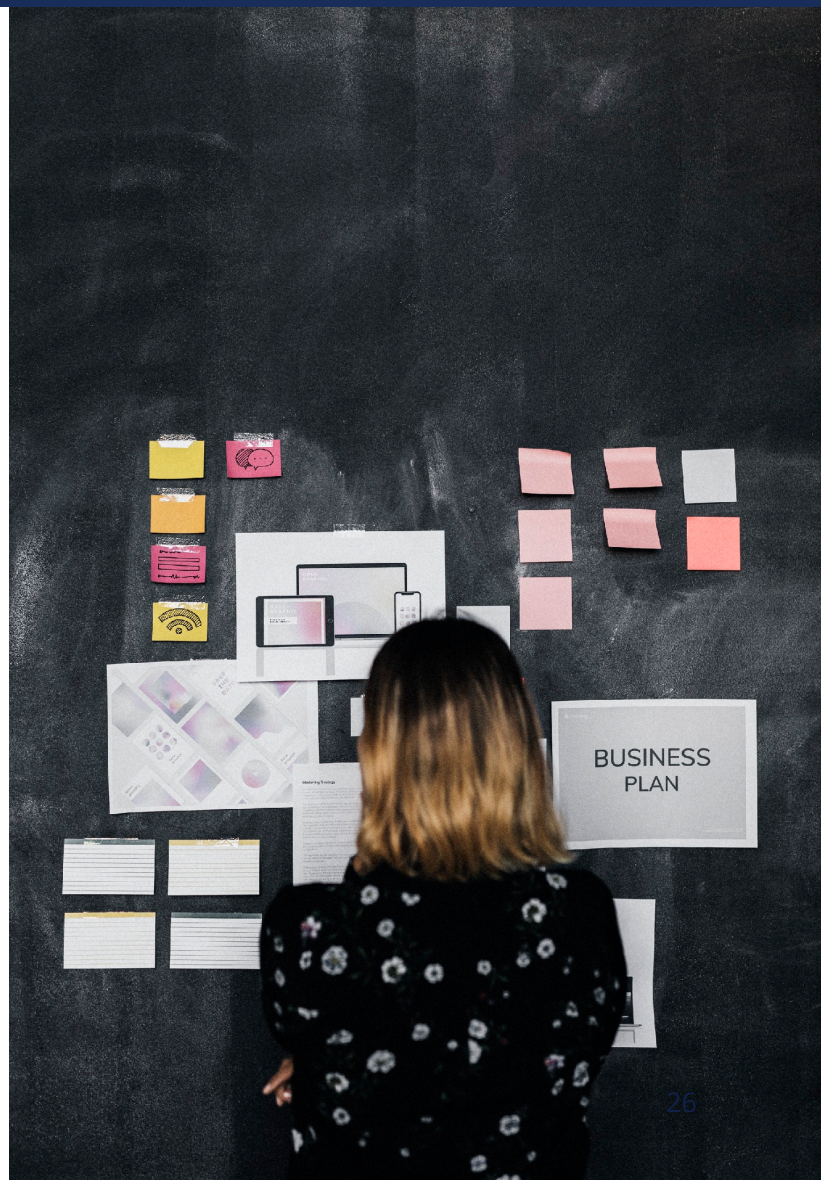
Sample Template: Assessing the Installed Base

Equipment Hostname	Features Required	Missing Features	Solutions	Equipment End-of-life Date
Aggregate Network Region 1 Layer-2 Switch Software version: 15.1(4)M7	• MLDv2 snooping [RFC4541] • IPv6 Basic specification [RFC8200/STD86] * • IPv6 Addressing Architecture [RFC4291] * • Default Address Selection for IPv6 [RFC6724] • ICMPv6 [RFC4443/STD89] * • SLAAC [RFC4862] * • Neighbor Discovery [RFC4861] [RFC6980] * • SNMP protocol [RFC3411] • SNMP capabilities [RFC3412, RFC3413, RFC3414] • SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289] • Transmission of IPv6 Packets over Ethernet Networks [RFC2464]	• SNMP protocol [RFC3411] • SNMP capabilities [RFC3412, RFC3413, RFC3414] • SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]	• Transfer functionality to another switch	10-2027
Backbone Network Region 1 Router Software version: 17.3.1a	• IPv6 Basic specification [RFC8200/STD86] * • Transmission of IPv6 Packets over Ethernet Networks [RFC2464] • IPv6 Addressing Architecture [RFC4291] * • Default Address Selection for IPv6 [RFC6724] • Unique Local IPv6 Unicast Addresses (ULA) [RFC4193] • DHCPv6 client/server/relay [RFC8415] * • DHCPv6 Relay Agent Remote-ID Option [RFC4649] • DHCPv6 Relay Agent Subscriber-ID Option [RFC4580] • DHCPv6 Client Link-Layer Address Option [RFC6939] • ICMPv6 [RFC4443/STD89] * • SLAAC [RFC4862] * • IPv6 Router Advertisement Options for DNS Configuration [RFC8106] *	• DHCPv6 Client Link-Layer Address Option [RFC6939] • ICMPv6 [RFC4443/STD89] * • SLAAC [RFC4862] *	• Wait until the end of the life cycle	05-2026
Backbone Network Region 2 Router Software version: 17.2.9d	• DHCPv6 Relay Agent Remote-ID Option [RFC4649] • DHCPv6 Relay Agent Subscriber-ID Option [RFC4580] • DHCPv6 Client Link-Layer Address Option [RFC6939] • ICMPv6 [RFC4443/STD89] * • SLAAC [RFC4862] * • IPv6 Router Advertisement Options for DNS Configuration [RFC8106] *	• DHCPv6 Client Link-Layer Address Option [RFC6939] • ICMPv6 [RFC4443/STD89] * • SLAAC [RFC4862] *	• Wait until the end of the life cycle	05-2026

Consider Dependencies

Before making the final decision on prioritisation, consider:

- Network service dependencies
- Vertical dependencies - customers and providers
- Priority conflicts
- Long term strategy



Costs

- Infrastructure investments
- Employee hours
- Training costs

Human Resources: Skills Needed

Solid understanding of the **IPv6 protocol**

Strong knowledge about existing network **equipment, services** and **configuration**

Knowledge about the fundamentals of **IPv6 security**

Knowledge about **transition mechanisms**

Strong **troubleshooting** capability

Efficient and responsive **project management**

Poll!

In your opinion, what are the skills currently **missing** in your organisation?

https://ripe-ncc.typeform.com/ipv6a3

Check how **other course participants answered**

Teams Involved

Project management team

Network architecture team

Network planning teams

may include sub-teams depending on the organisation's size

Network security teams

Network operations teams

may include sub-teams depending on the organisation's size

Network help desks

Customer management and **billing** teams

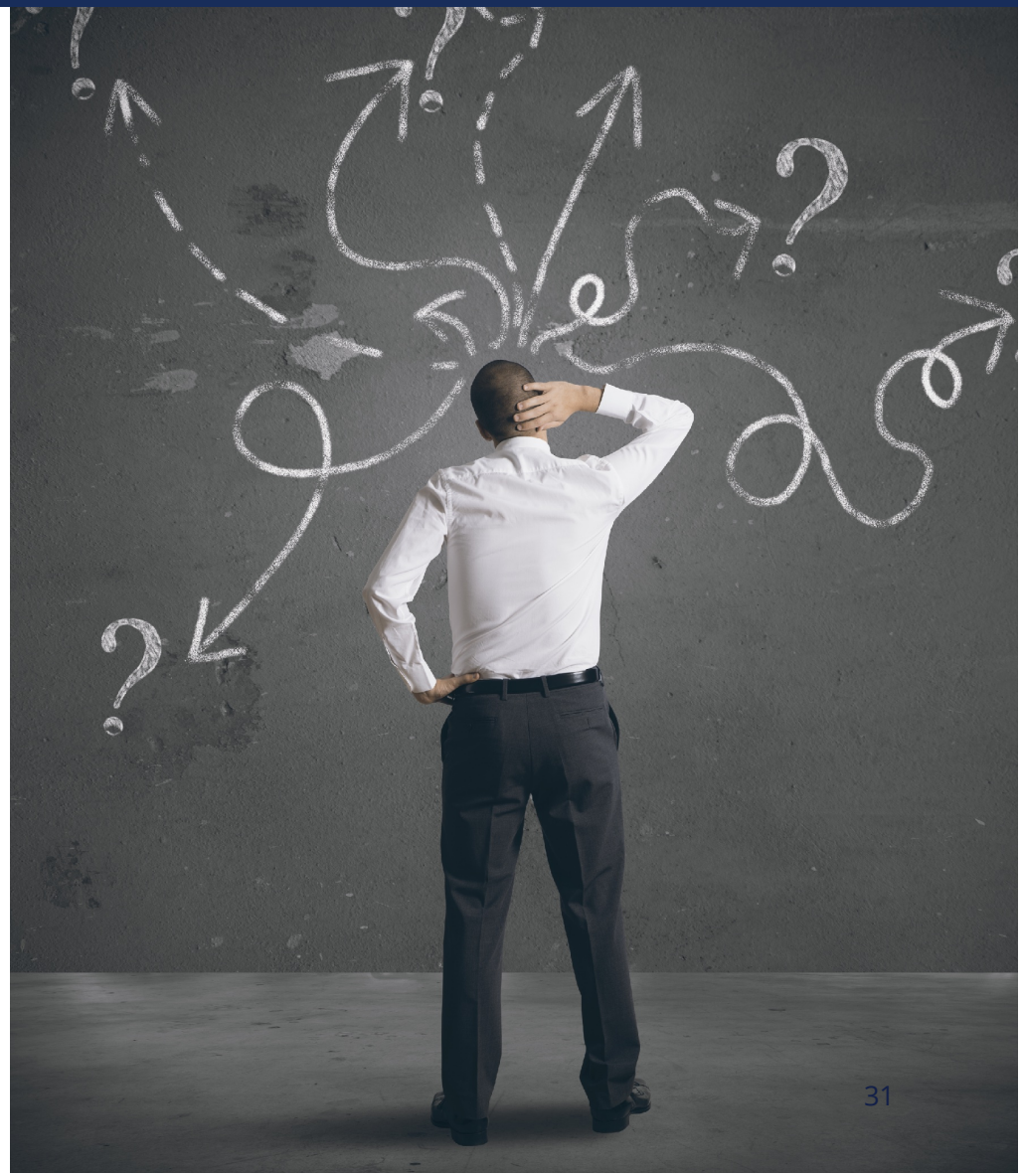
Software development teams

Legal team

Procurement team

Challenges for an IPv6 Deployment Project

- Difficult to **estimate deadlines**
- Beware of **proprietary features** and technologies
- **Resistance** to the change
- IPv6 deployment involves **complexity** and **uncertainty**



‘Get Approval’ Phase - Summary

1. Justify IPv6 deployment and get the **green light**

2. Have an informed **project plan** by:

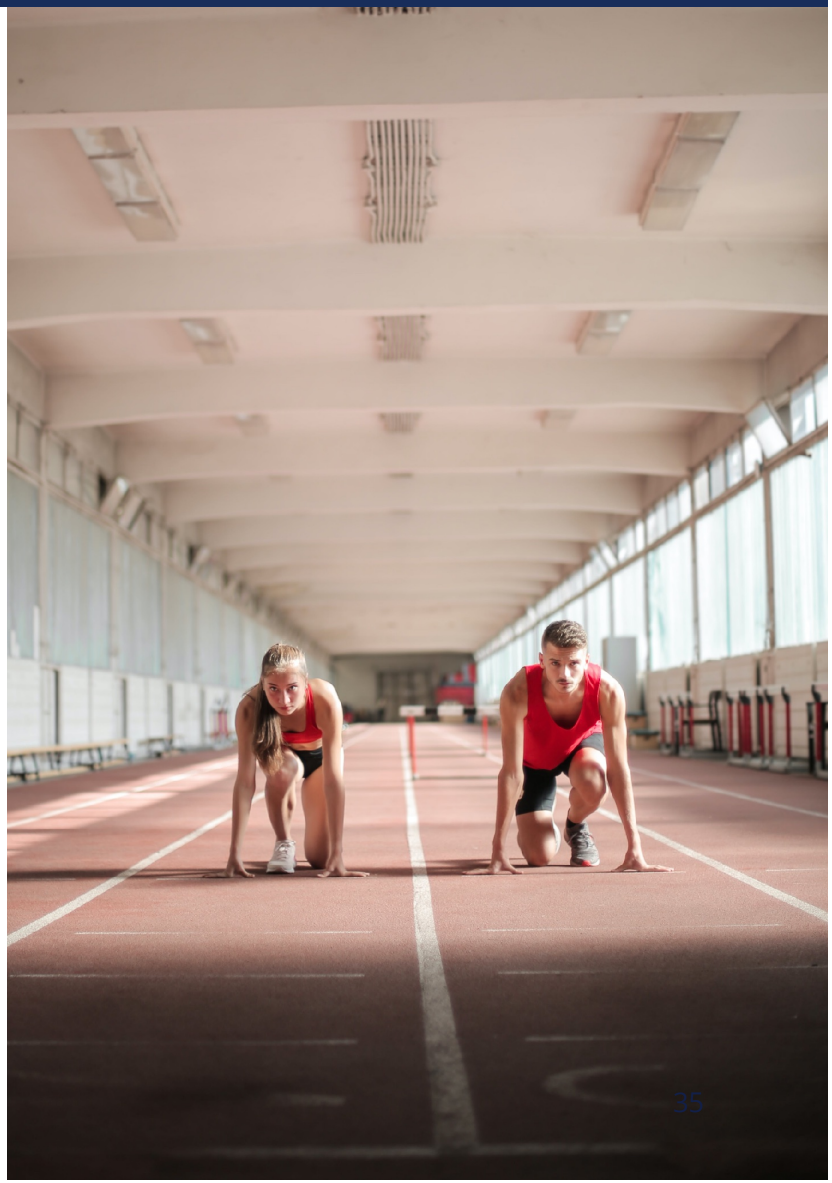
   - Prioritising and identifying the **scope** of the project
   - Knowing the **skills** needed with the teams and human resources involved
   - Being aware of the IPv6 deployment **challenges**
   - Adopt an approach that can help with **uncertainty** and **complexity**

Questions

Get Ready

Tasks in this Phase

1. Create an addressing plan
2. Get IPv6 training
3. Build a test environment
4. Adopt a transition strategy



Create an Addressing Plan

Address Allocation

IPv6 Address Allocation Criteria

For allocations and extensions up to a /29:

- Be a **member** of the RIPE NCC
- Have a **plan** for making sub-allocations and/or end site assignments within two years.

Need more than a /29? Also provide documentation on: *

- Amount of **users** and extent of **infrastructure**
- Hierarchical and geographical **structure / planned longevity**
- Segmentation of infrastructure for **security**

Already have IPv6, but need more than a /29: *

- **Utilise enough** of the initial allocation
- Justify **new needs**

* *When requesting more than a /29, you also need to provide additional documentation to justify the size.*

Link to RIPE NCC Assessment Criteria:

https://www.ripe.net/manage-ips-and-asns/ipv6/request-ipv6/assessment-criteria-for-ipv6-allocations

Additional Documentation Needed for Allocations Larger than /29

Need more than a /29? Also provide documentation on:

- Addressing/subnetting plan
- Network topology diagram
- Size and scope of end sites covered by request
- Statistics for past network growth (where applicable)
- Deployment plan (where applicable)

Already have IPv6, but need more than a /29:

For quite a while the RIPE NCC reserves some bits more for each allocation to the LIRs and try to keep some space available for the future expansions!

Link to RIPE-NCC Assessment Criteria:
https://www.ripe.net/manage-ips-and-asns/ipv6/request-ipv6/assessment-criteria-for-ipv6-allocations

PI Addresses

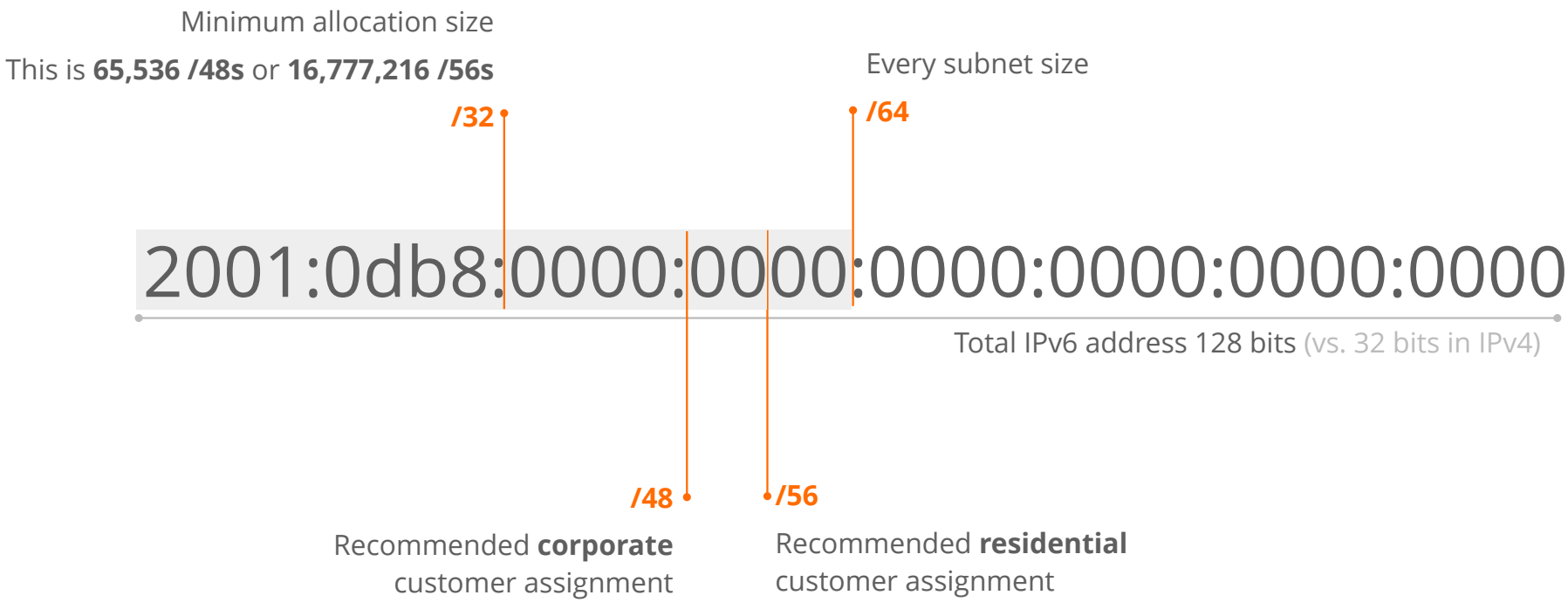
You don’t need to be an LIR to use your own IPv6 address space!

- To qualify, an organisation must:
  - Have a sponsoring LIR
  - **Meet** the contractual **requirements** for provider independent resources
  - LIRs must demonstrate special **routing requirements**
- Minimum assignment size: **/48**
- PI space **cannot** be used for sub-assignments

Create an Addressing Plan

Addressing Structure and Best Practices

IPv6 Addressing Refresher



Choosing which prefix size to use is your choice in the end!

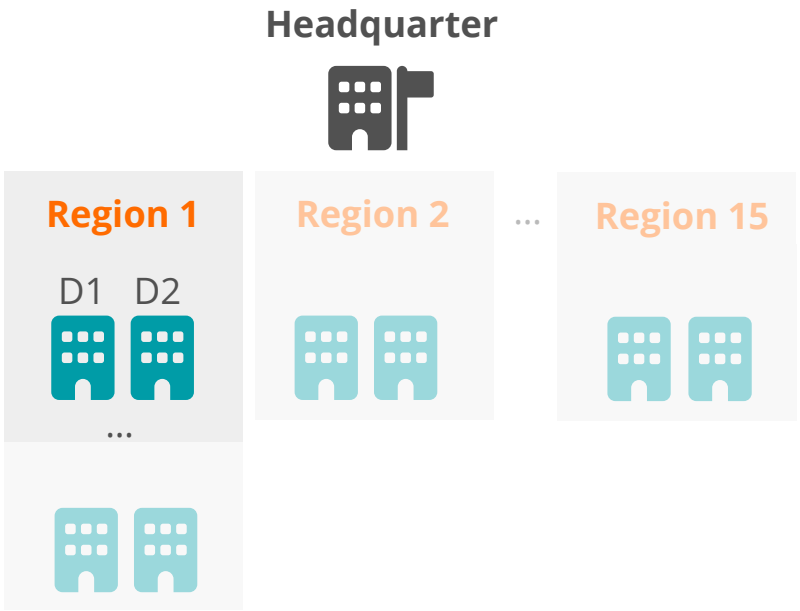
Best Practices for IPv6 Address Plans

- Priorities are **aggregation** and **scalability**
- /127 for p2p (still reserve /64)
- Single /64 for loopbacks per site
- Auto link-local address usage
- Avoid using trailing leading-zero addresses

Link to RIPE-690:
https://www.ripe.net/publications/docs/ripe-690

Why Does the Four-bit Boundary Rule Matter?

If you stick to the four-bit boundary rule then you can easily assign **functions** to the digits in the hex notation of IPv6.



Company Allocation 2001:0db8::/32
Split it into 16 and we'll have /36s to be used for the regions

2001:0db8:0000::/36 - Headquarter	2001:0db8:8000::/36 - Future Reserve
2001:0db8:1000::/36 - Region 1	2001:0db8:9000::/36 - Future Reserve
2001:0db8:2000::/36 - Region 2	2001:0db8:a000::/36 - Future Reserve
2001:0db8:3000::/36 - Future Reserve	2001:0db8:b000::/36 - Future Reserve
2001:0db8:4000::/36 - Future Reserve	2001:0db8:c000::/36 - Future Reserve
2001:0db8:5000::/36 - Future Reserve	2001:0db8:d000::/36 - Future Reserve
2001:0db8:6000::/36 - Future Reserve	2001:0db8:e000::/36 - Future Reserve
2001:0db8:7000::/36 - Future Reserve	2001:0db8:f000::/36 - Future Reserve

Now we will split the sub-allocation for Region 1 into 16 and assign them to different departments

2001:0db8:1000::/40 - Department 1	2001:0db8:1800::/40 - Future Reserve
2001:0db8:1100::/40 - Department 2	2001:0db8:1900::/40 - Future Reserve
2001:0db8:1200::/40 - Future Reserve	2001:0db8:1a00::/40 - Future Reserve
2001:0db8:1300::/40 - Future Reserve	2001:0db8:1b00::/40 - Future Reserve
2001:0db8:1400::/40 - Future Reserve	2001:0db8:1c00::/40 - Future Reserve
2001:0db8:1500::/40 - Future Reserve	2001:0db8:1d00::/40 - Future Reserve
2001:0db8:1600::/40 - Future Reserve	2001:0db8:1e00::/40 - Future Reserve
2001:0db8:1700::/40 - Future Reserve	2001:0db8:1f00::/40 - Future Reserve

Sometimes We Can’t Avoid Exceeding the Four-bit Boundary

- It especially happens for large prefixes such as /32 or even /36
- RIPE NCC allocates /29s and it is not on a four-bit boundary.
- Try to keep it at an administrative level and avoid using it on network device level

Using Unique Local Addresses (ULAs)

- **ULA Range:** fc00::/8 and **fd00::/8**
- ULAs are not routable on the Internet
- Pseudo-randomisation of ULA Global IDs (40 bits)
- ULAs and Dual-Stack - ULAs are less preferred than IPv4
- **Simply leverage Global Unicast Addresses!**

Assign Persistent Addresses to Customers. Why?

Example: Service hosting, incoming connections

Example: A power outage can cause IPv6 to break

Global Unicast Addresses (GUA) on P2P links

- Link-local addresses are usually enough, but to **monitor links, use GUAs**
- A prefix per POP
- IGP - *if you already use it inside the network*

Create an Addressing Plan

IP Address Management Tools

Why IP Address Management?

How do you currently keep track?

- There are many subnets in IPv6
- Your spreadsheet might not scale
- And you want to take care of (reverse) DNS

- There are **524288 /48s** in a **/29**
- That is **34359738368 /64s**!

Benefits of Using an IPAM Tool

- Repository of assignable IP addresses stays up-to-date
- Prevents duplicates in the networks - reduce human error
- Assists troubleshooting
- For regulatory or legal compliance

What Are the Functionalities of an IPAM Tool?

- IP search functionality
- IP address/device discovery
- Allocations and making reservations
- Connection to RIR Databases (pull and/or push information)
- Easy auditing, logging, historical view
- Task creation and assignment
- Multiple access profile support (admin, operator, user/read-only)
- Import and export of files
- Native VRF support
- DNS/DHCP Integration

What Should You Compare?

- Scale of the product? -F*or "ISP" or "small/ medium enterprise"?*
- Easy to learn?
- Cleaner graphical user interface
- Paid vs Free - *Customer support?*
- Licensed vs Open-source

Comparison of Open Source IPAMs

	{php}IPAM v1.6.0	NetBox v3.7.4	NetDot v1.0.8	GestioIP v3.5.7	NOC Project v23.1.4	NIPAP v0.29.6
Device Auto Discovery	Supported	Supported	Not Supported	Supported	Supported	Not Supported
Role Based Access Control	Supported	Supported	Supported	Supported	Supported	Supported
IPAM Centric	Yes	IPAM is a feature	IPAM is a feature	Yes	IPAM is a feature	Yes
API Support	Supported	Supported	Not Supported	Supported	Supported	Supported
VRF Support	Supported	Supported	Not Supported	Supported	Supported	Supported
DHCP Integration	Not Supported *work in progress for Kea DHCP (open-source DHCP server)*	Supported	Supported *Supported - generate configurations for ISC DHCPD*	Supported *SC DHCPD, ISC KEA, Microsoft DHCP server and a generic leases file formats*	Unknown	Supported *Supported - generate configurations for ISC DHCPD*
DNS Integration	Supported *Get data from Power DNS*	Not Supported	Supported *Only ISC BIND zone file exporting*	Supported *Microsoft DNS, BIND or other DNS server products and GestióIP*	Supported	Not Supported
Support	Community Support *more active*	Community and Commercial Support *for (paid) Cloud version*	Community Support	Community and Commercial Support	Community Support	Community Support

Questions

Lab Activity 1

IPv6 addressing plan using phpIPAM

Lab Activity 1 - IPv6 addressing plan using phpIPAM

- **Description**: Create and register IPv6 addressing plan in one of the most known and used IPAM tools; phpIPAM
- **Goal**: Implement an IPv6 addressing plan using IPAM tools
- **Time:** 20 minutes
- **Tasks:**

1. Creating a subnet in phpIPAM for your new allocation
2. Creating nested subnets for different parts of your network
3. Creating IP addresses inside the subnets & searching them
4. Checking the availability of smaller subnets

Lab Activity 1 - IPv6 addressing plan using phpIPAM

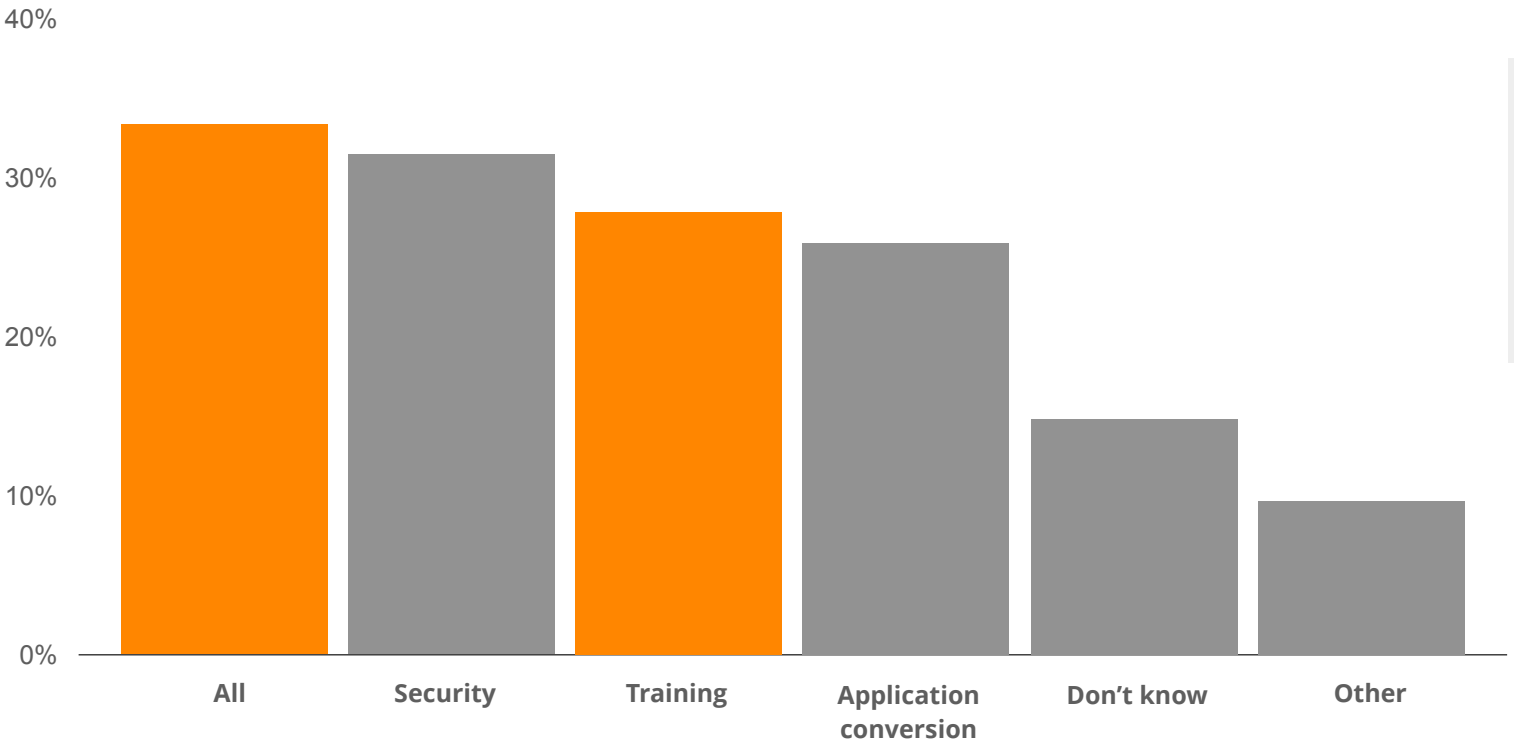
- **What have you learned?**
  - You created different types of subnets in the IPAM tool
  - You registered IP addresses and learned to search them
  - You learned how to check the availability of a certain size of subnets

{php}IPAM
Open-source IP address management

Get IPv6 Training

Is Training Really Needed?

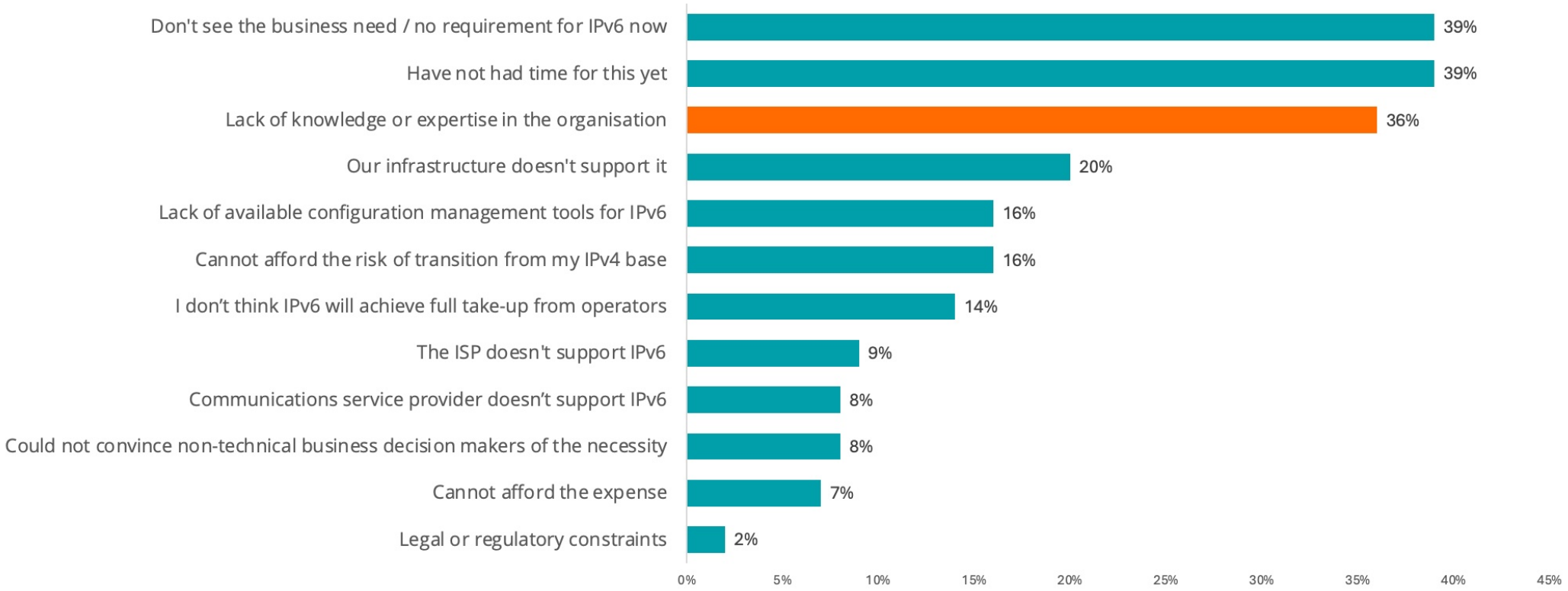
As you begin to think about the implementation of IPv6 at your organisation, **what areas do you feel are of concern**?



The survey chart as referenced in the informational RFC 9386 is from the **Industry Network Technology Council**

Source: Informational RFC9386
https://datatracker.ietf.org/doc/html/rfc9386#name-summary-of-questionnaire-and

Main Reasons For Not Deploying IPv6 (1709 responses)



Source: RIPE NCC Survey 2023
https://www.ripe.net/media/documents/RIPE_NCC_2023_Survey_Report.pdf

IPv6 Training for Different Roles

Network planning and architecture engineers

IPv6 Fundamentals & Advanced

Network operations engineers

IPv6 Fundamentals & Advanced

Network help desks

IPv6 Fundamentals

Project managers

Basic knowledge about networks and IPv6 protocol & First phase of IPv6 Adv. training

Network security engineers

IPv6 Fundamentals & Security, and related topics of IPv6 Advanced

Legal and compliance experts

Legal and regulatory aspects of IPv6

Software developers

IPv6 Fundamentals

Procurement team

Basic knowledge about the IPv6 protocol, IPv6 Fundamentals

RIPE NCC IPv6 Training and Certifications - Learning Path

IPv6

IPv6 Fundamentals

Get started with IPv6. You will learn how IPv6 addresses work, how to subnet, best-practices and IPv6-related RFCs among other topics.

Self-Paced E-Learning

IPv6 Fundamentals E-Learning Course 15h

Live Sessions

IPv6 Fundamentals in-Person Course	8h
Introduction to IPv6 Webinar	2h
IPv6 in the RIPE Database Webinar	1h

On Demand Certified Professionals Exam

IPv6 Fundamentals - Analyst 1h

IPv6 Advanced

Currently under development

Self-Paced E-Learning

IPv6 Advanced E-Learning Course 22h

Live Sessions

IPv6 Advanced in-Person Course	16h
IPv6 Addressing Plan Webinar	2h

On Demand Certified Professionals Exam

IPv6 Advanced - Associate 1h

The e-learning course and exam are currently being developed

IPv6 Security

Keep your IPv6 network secure. Learn to design a high-level strategy to protect your IPv6 infrastructure against common threats.

Self-Paced E-Learning

IPv6 Security E-Learning Course 25h

Live Sessions

IPv6 Security in-Person Course	8h
Basic IPv6 Protocol Security Webinar	2h
IPv6 Security Myths, Filtering & Tips Webinar	2h
IPv6 Associated Protocols Security Webinar	2h

On Demand Certified Professionals Exam

IPv6 Security - Expert 1h

Training Resources

ARIN

IPv6 case studies from specific companies

https://www.arin.net/blog/ipv6/

AFRINIC

Online courses on IPv6 Fundamentals, NDP, Address planning, transition mechanisms, IPv6 routing

https://learn.afrinic.net/elearning

lacnic

Online courses on IPv6 basics (English/Spanish), and IPv6 in campus and data center networks (Spanish)

https://campus.lacnic.net/

APNIC

Tutorials, online courses and virtual labs related to IPv6 fundamentals, deployment and security

https://academy.apnic.net/

IETF Informational RFCs

Comparisons and best practices about the industry implementations of IPv6.

Examples:
https://www.rfc-editor.org/info/rfc9386
https://www.rfc-editor.org/info/rfc9313

Industry Network Technology Council

Webinars on variety of IPv6 topics

https://industrynetcouncil.org/ipv6-webinars/

Vendors

Improvements in the technology and the features

Your own lab and network!

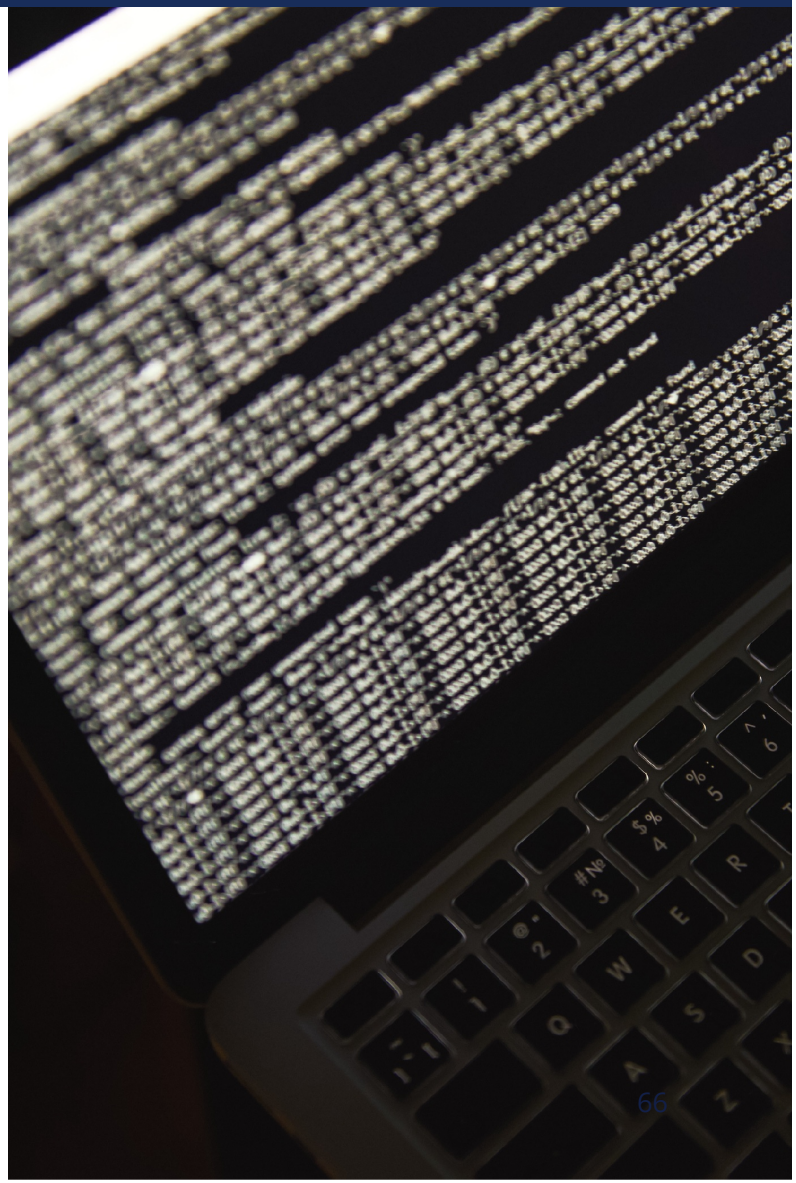
For testing new configuration and the compatibility/ interoperability of the devices

Questions

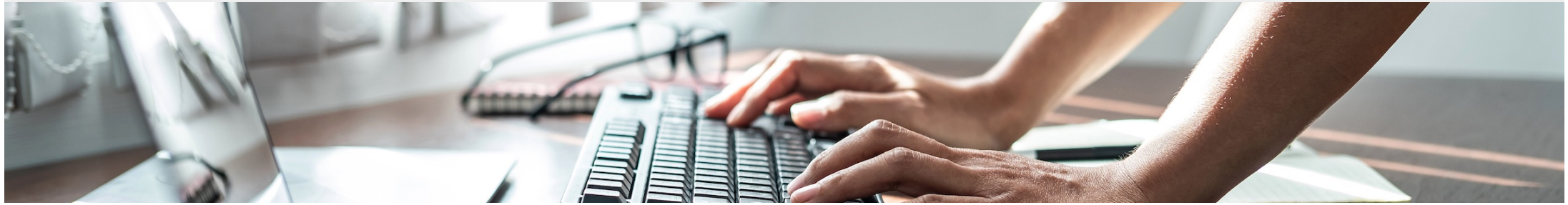
Build a Test Environment

Why Do You Need an IPv6 Test Lab?

- Choosing the new solution - **Proof of concept (PoC)**
- Testing the **new configuration**
- Testing the IPv6 **compatibility** and **interoperability** of the devices
- **Documenting** the solution/design
- Assessing **migration strategies**
- Learning tool!



A good lab environment should be a small replica of your live and future network



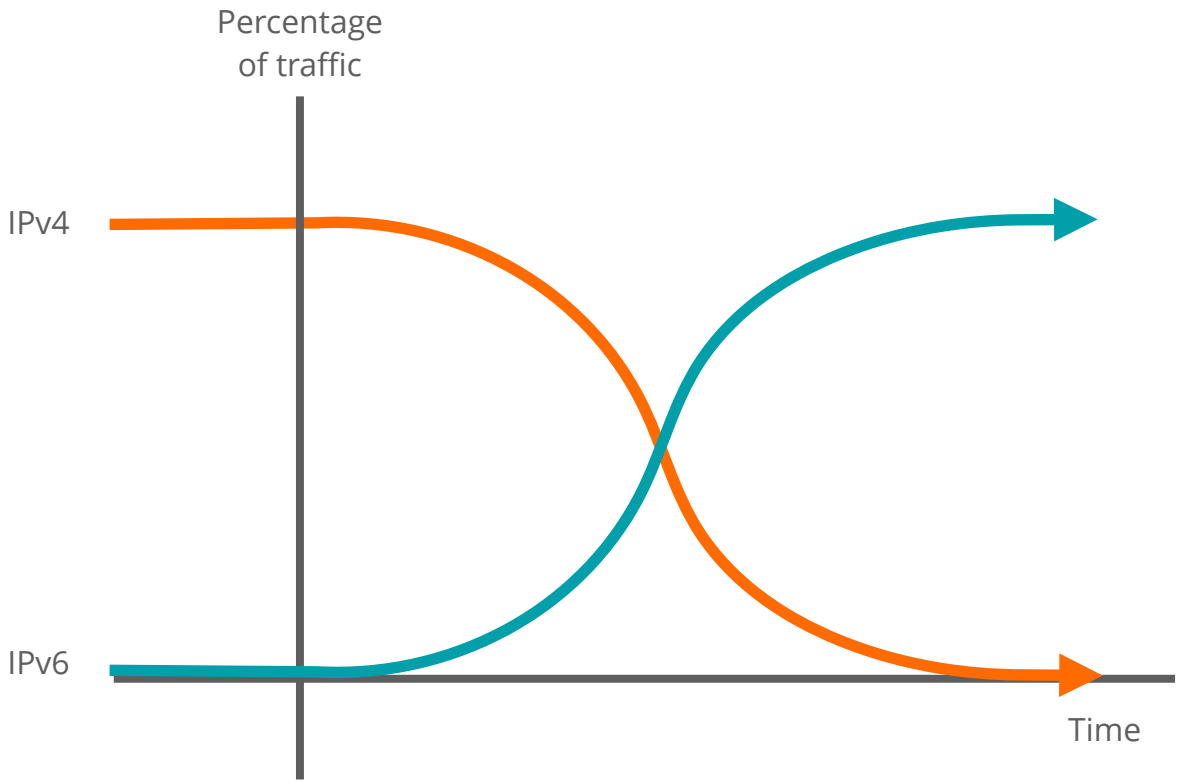
Components of a good IPv6 lab

- **Network equipments**
  router, switch, NAT, CPE, BNG, GGSN etc.
- **Security devices**
  firewall, IDS/IPS, etc.
- **Peripheral devices and systems**
  RADIUS, DNS, PCRF etc.
- **Monitoring and logging systems**
- **Customer end devices**
  with different OSes
- **Network testers**
- **Application servers**
- **Packet generator and analyser tools**
  scapy, Wireshark, termshark etc.

Questions

Adopt a Transition Strategy

IPv6 Transition Will Take Time!



With more IPv6 deployment:

- IPv4 traffic
- IPv6 traffic

Both IPv6 and IPv4 should be accessible

Transition Strategy

- Explains a broader concept
- Includes “Transition Mechanisms”
- Decisions for many different parts of the same network

Transition Mechanisms

- Explains the mechanisms for transition to IPv6
- Part of “Transition Strategy”
- Technical means and protocols of implementing your transition strategy
- Dual-stack, 6RD, 464XLAT, etc.

Which Network Type Do You Have?

Greenfield Network		Brownfield Network
You start with blank state		***Build on your existing IPv4 network***
New ISPs/Mobile Operators, New IoT Networks, Smart Grids		Existing Datacenters Existing Broadband networks
IPv6-only (or IPv4aaS) solution will be easier to use		Dual-stack easier to implement IPv6-only is future proof
Transition Mechanisms are NOT required (for closed networks)		Transition Mechanisms or Dual-Stack will be required.
Easy to deploy *(with good upfront planning)*		Not as easy as implementing in a Greenfield solution

Options for Backbone Networks

- IPv4-only backbone - *is not a future proof strategy*
- Dual-stack
- IPv6-only backbone *(can be considered for green-field deployments)*
- 6PE/6VPE - *for MPLS networks*

Options Comparison - Backbone Network

Main Advantage(s)	Strategies	Main Drawback(s)
- Single protocol to be managed inside the backbone - No major change in the backbone	**IPv4 only with tunnelling**	- No IPv6 capability in the backbone - Difficulty to apply security measures against IPv6 traffic inside the tunnels. - Possible suboptimal routing problems as the traffic will be diverted to the tunnel end-points in the backbone. - Possible MTU problems
- Native communication for both protocols - SRv6 can be enabled later	**Dual stack**	- Two different protocols to be managed - Does not solve IPv4 scarcity problem
- Single protocol to be managed inside the backbone - Future proof network deployment - SRv6 can be enabled later	**IPv6-Only**	- All nodes should support IPv6. - Another solution is needed for IPv4 destinations (ie. AFTR or tunnel broker) *For a closed network with the greenfield implementation these issues will not pose a problem*

** We will discuss the MPLS scenario later on in the course*

Options for Access Network(s)

Dual-Stack

Translation

Tunnelling

IPv6 packets within IPv4

IPv4 packets within IPv6

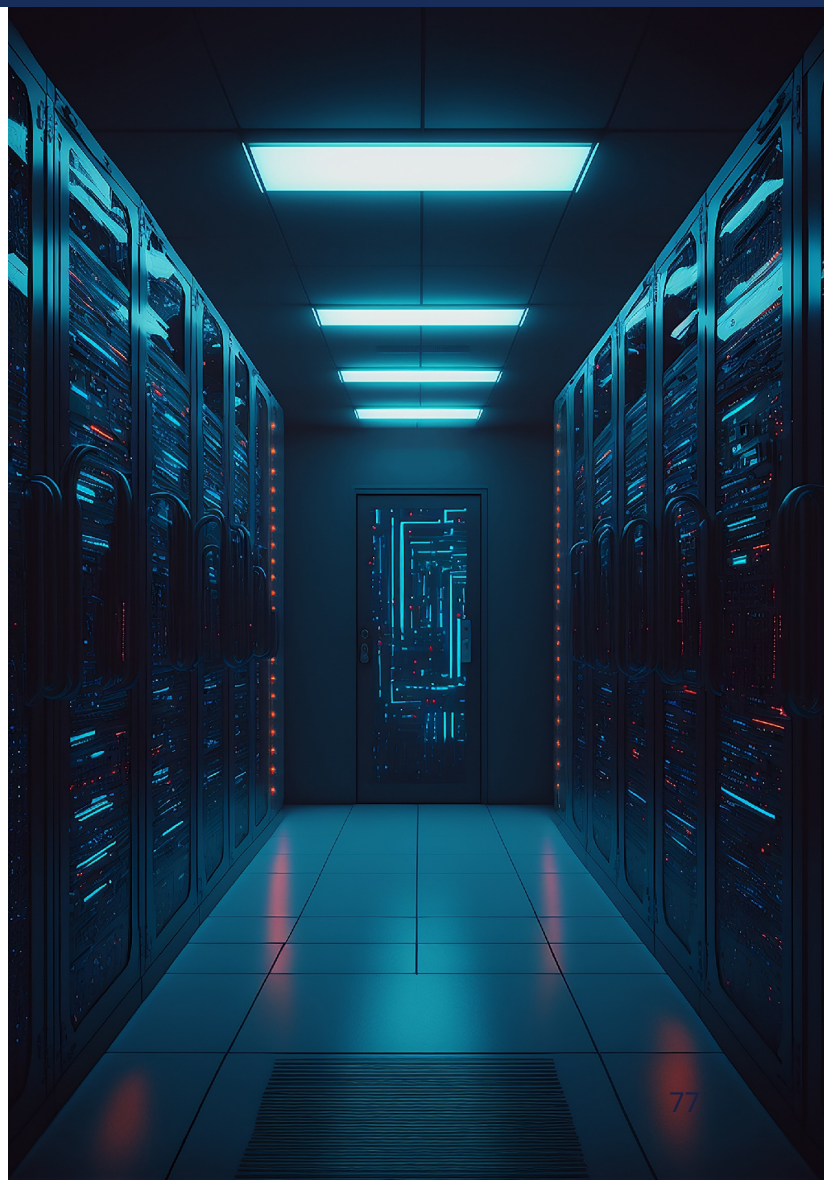
Options Comparison - Access Network

Main Advantage(s)	Strategies	Main Drawback(s)
- Native communication for both protocols	**Dual Stack**	- Two different protocols to be managed - Does not solve IPv4 scarcity problem
- Single protocol to be managed in the access network. - In case of “IPv6-only” scenario the access network will be future proof.	**Translation**	- Possible suboptimal routing problems as the traffic will be diverted to the address translators in the backbone. - Risk of loosing packet header details because of translation. - Additional devices to be configured - AFTRs - Possible scalability issues.
- Single protocol to be managed in the access network. - In case of “IPv6-only” scenario the access network will be future proof.	**Tunneling**	- Possible suboptimal routing problems as the traffic will be diverted to the tunnel end-points in the backbone. - Possible MTU problems. - Difficulty to apply security measures against IPv6 traffic inside the tunnels. - Additional devices to be configured - Tunnel end-points. - Possible scalability issues. - Not supported widely in mobile broadband scenarios

Options for Data Center Networks

- **Dual-Stack** - on the servers
- **IPv6-only** - with SIIT-DC
- **6/4 Proxy** - for the IPv6-only **clients**

- DNS Updates
- Security Updates
- Application Compatibility



Options Comparison - Data center Network

Main Advantage(s)	Strategies	Main Drawback(s)
- Native communication for both protocols	**Dual Stack**	- Two different protocols to be managed - Does not solve IPv4 scarcity problem - (a less severe issue in a datacenter when compared to access networks)
- Single protocol to be managed in the data center - Easiness of scalability with stateless solutions - Future proof solution	**IPv6-only**	- The need for all infrastructure to support IPv6. - The need for making the content available for IPv4 customers as well
- Single protocol to be managed in the data center	**6/4 Proxy**	- Setting up a proxy device in front of the servers. - The need for workaround solutions (such as X-Forwarded-For) for the session based applications - Not a future proof solution

Considerations For Other Network Parts and Types

Host LAN

Similar to access networks

Enterprise Network

VPN, SD-WAN

Cloud Network

*Cloud services **

* *This will be discussed later on in the course*

Transition Strategy Question

In the context of IPv6 migration, what is the **key difference** between a transition strategy and transition mechanisms?

a. A **transition strategy** outlines the specific methods used for migrating to IPv6, while **transition mechanisms** provide the overarching plan and objectives.

b. A **transition strategy** covers the high-level approach for migrating to IPv6, while **transition mechanisms** refer to the specific mechanisms used within that strategy.

c. A **transition strategy** involves testing and validation of IPv6 functionality, while **transition mechanisms** involve upgrading network equipment for IPv6.

d. A **transition strategy** includes monitoring and optimisation of IPv6 deployment, while **transition mechanisms** involve configuring devices to support both IPv4 and IPv6.

Transition Strategy Answer

In the context of IPv6 migration, what is the **key difference** between a transition strategy and transition mechanisms?

a. A **transition strategy** outlines the specific methods used for migrating to IPv6, while **transition mechanisms** provide the overarching plan and objectives.

✓ A **transition strategy** covers the high-level approach for migrating to IPv6, while **transition mechanisms** refer to the specific mechanisms used within that strategy.

c. A **transition strategy** involves testing and validation of IPv6 functionality, while **transition mechanisms** involve upgrading network equipment for IPv6.

d. A **transition strategy** includes monitoring and optimisation of IPv6 deployment, while **transition mechanisms** involve configuring devices to support both IPv4 and IPv6.

Needed Features For Your Strategy

- Your design will require **specific features**
- Check which features are available with your vendors and operators
- Non-exhaustive list of requirements can be found in RIPE-772

Link to RIPE-772:

For example: *For requirements for "router or layer-3 switch" equipment*

https://www.ripe.net/publications/docs/ripe-772/

Design Documents Creation

High Level Design (HLD) document

- Include **a structured format** of your ideas
- What to include?
  - Scope of your project
  - Objectives
  - Solution alternatives
  - Chosen solution and reasoning

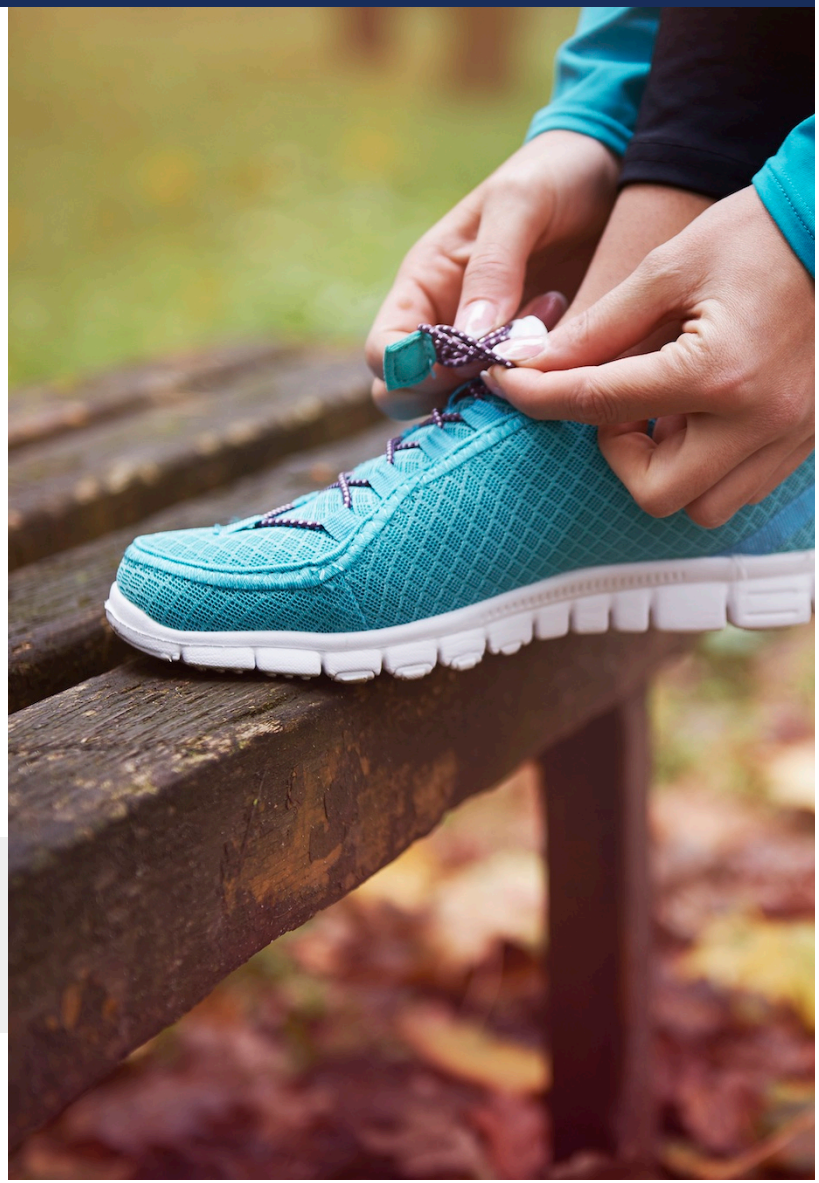
Low Level Design (LLD) document

- Holds **more information** than HLD
- What to include?
  - Configuration changes
  - Port numbers, IPv6 addresses, POP names etc. *as soon as they become available*

Get Ready Phase - Summary

1. Create an addressing plan
2. Get IPv6 training
3. Build a test environment
4. Adopt a transition strategy

The outcome of this phase is your design!

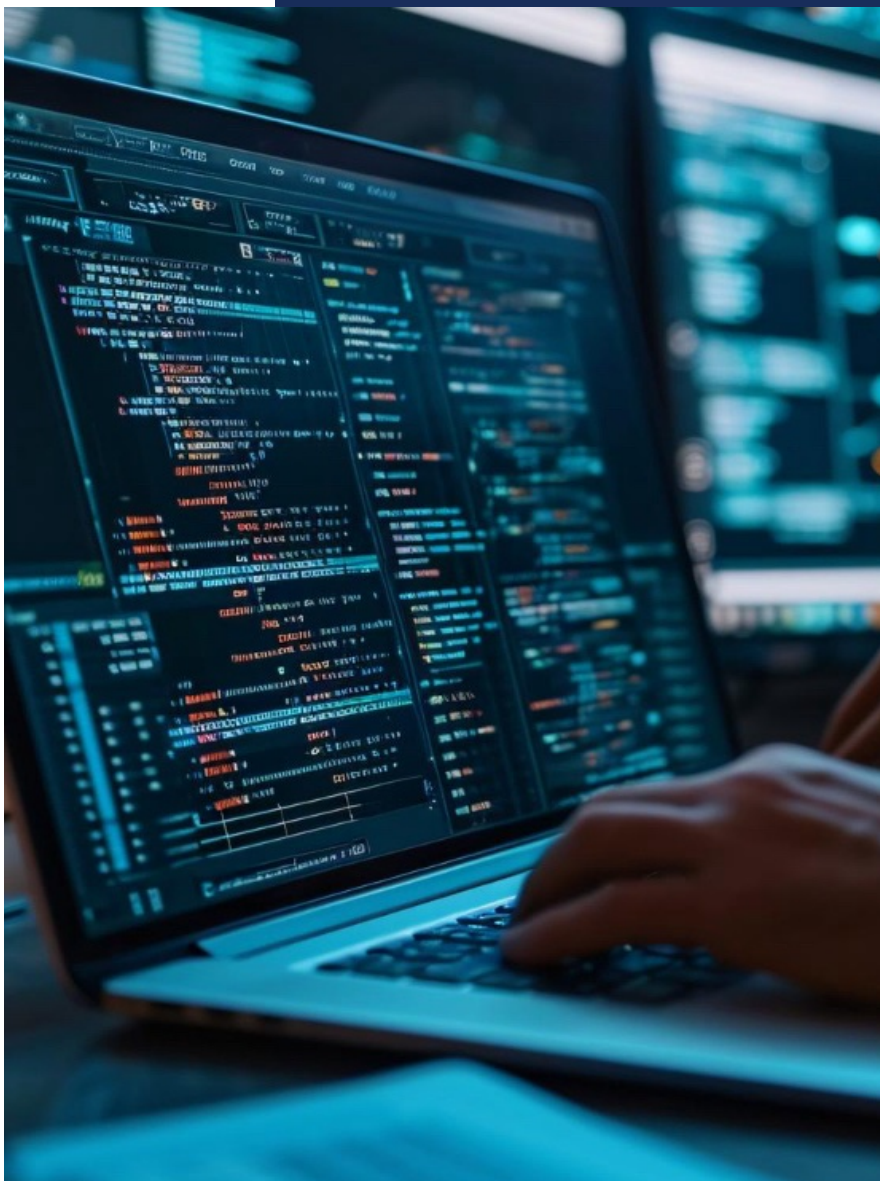


Questions

Deploy

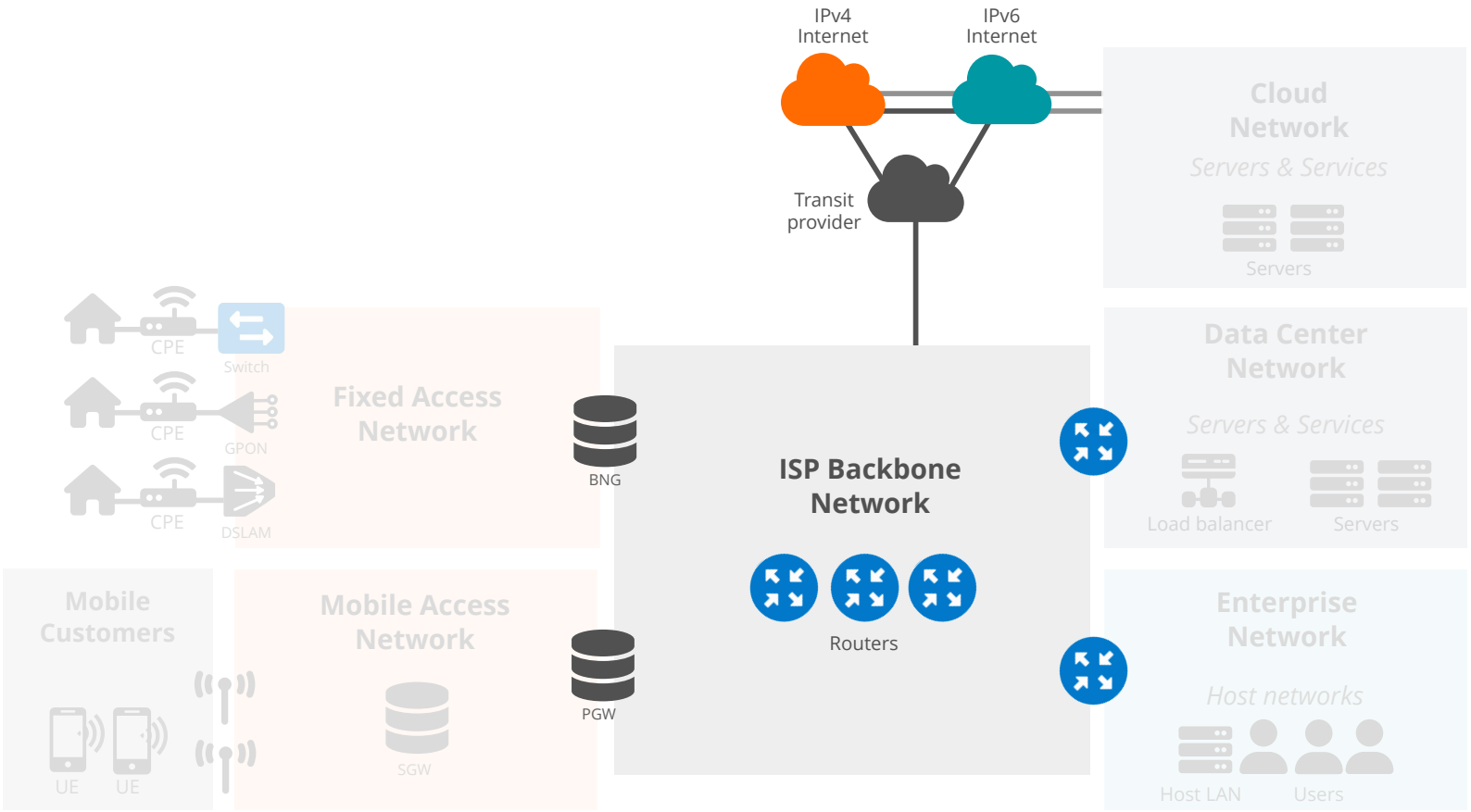
Tasks in This Phase

1. Deploy IPv6 in/for your:
   - Backbone network
   - Access network and Broadband Customers
   - Enterprise network & Different OSes
   - Datacenter network
   - Cloud Networks
2. Pilot tests



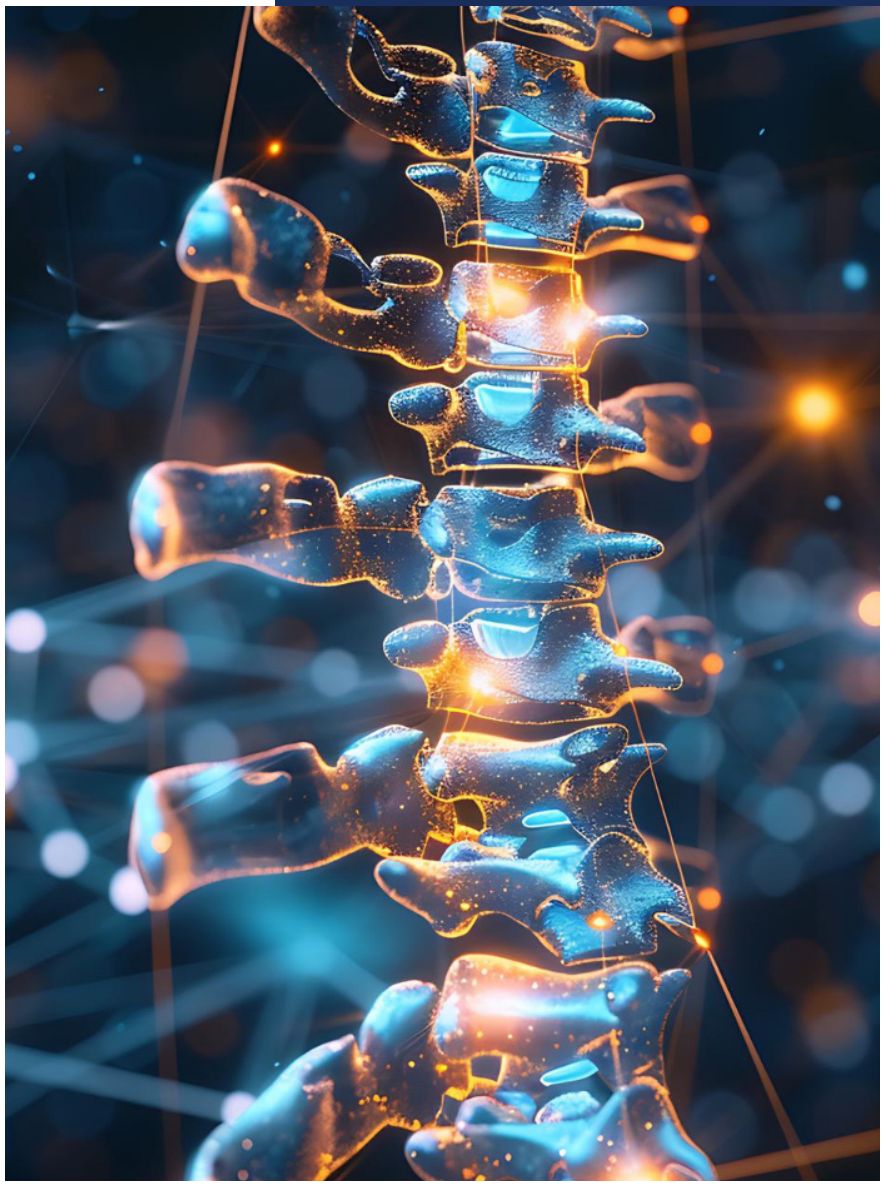
Backbone Networks

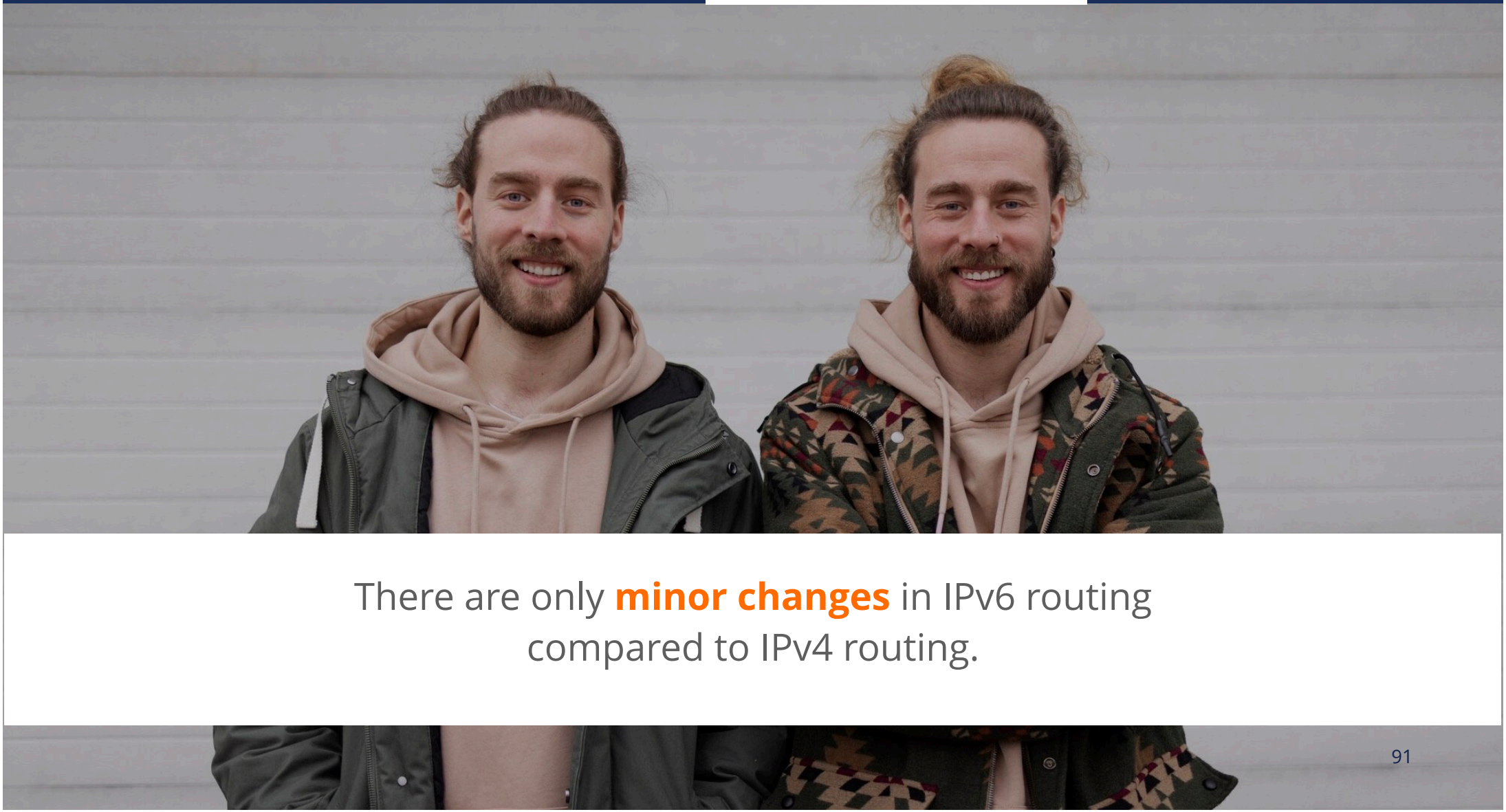
Reference Architecture - Backbone



IPv6 Introduction to the Backbone Network

- Upstream connection
- Transition strategies
  - Dual-stack
  - IPv4-only backbone
  - 6PE
  - IPv6-only backbone *(can be considered for green-field deployments)*
- Protocols - IGP, BGP, MPLS, SR





There are only **minor changes** in IPv6 routing compared to IPv4 routing.

Basics of Routing in IPv6 Question

According to the route table below, what is the next-hop address of the packet with the destination IP address **2001:db8:1001:1a2b:02ab:92ff:fe01:f8b2**?

Route	Next-hop
::/0	2001:db8:aaa:bbb::cdef:1
2001:db8::/32	2001:db8:bcd:aaa::1
2001:db8::/48	2001:db8:cde:bbb::1
2001:db8:1000::/36	2001:db8:ffff:eeee::1
2001:db8:1000::/48	2001:db8:def:bbb::1
2001:db8:2000::/48	2001:db8:def:bbb::2

a. 2001:db8:aaa:bbb::cdef:1

b. 2001:db8:bcd:aaa::1

c. 2001:db8:ffff:eeee::1

d. 2001:db8:def:bbb::1

Basics of Routing in IPv6 Answer

According to the route table below, what is the next-hop address of the packet with the destination IP address **2001:db8:1001:1a2b:02ab:92ff:fe01:f8b2**?

Route	Next-hop
::/0	2001:db8:aaa:bbb::cdef:1
2001:db8::/32	2001:db8:bcd:aaa::1
2001:db8::/48	2001:db8:cde:bbb::1
2001:db8:1000::/36	2001:db8:ffff:eeee::1
2001:db8:1000::/48	2001:db8:def:bbb::1
2001:db8:2000::/48	2001:db8:def:bbb::2

a. 2001:db8:aaa:bbb::cdef:1

b. 2001:db8:bcd:aaa::1

✓ 2001:db8:ffff:eeee::1

d. 2001:db8:def:bbb::1

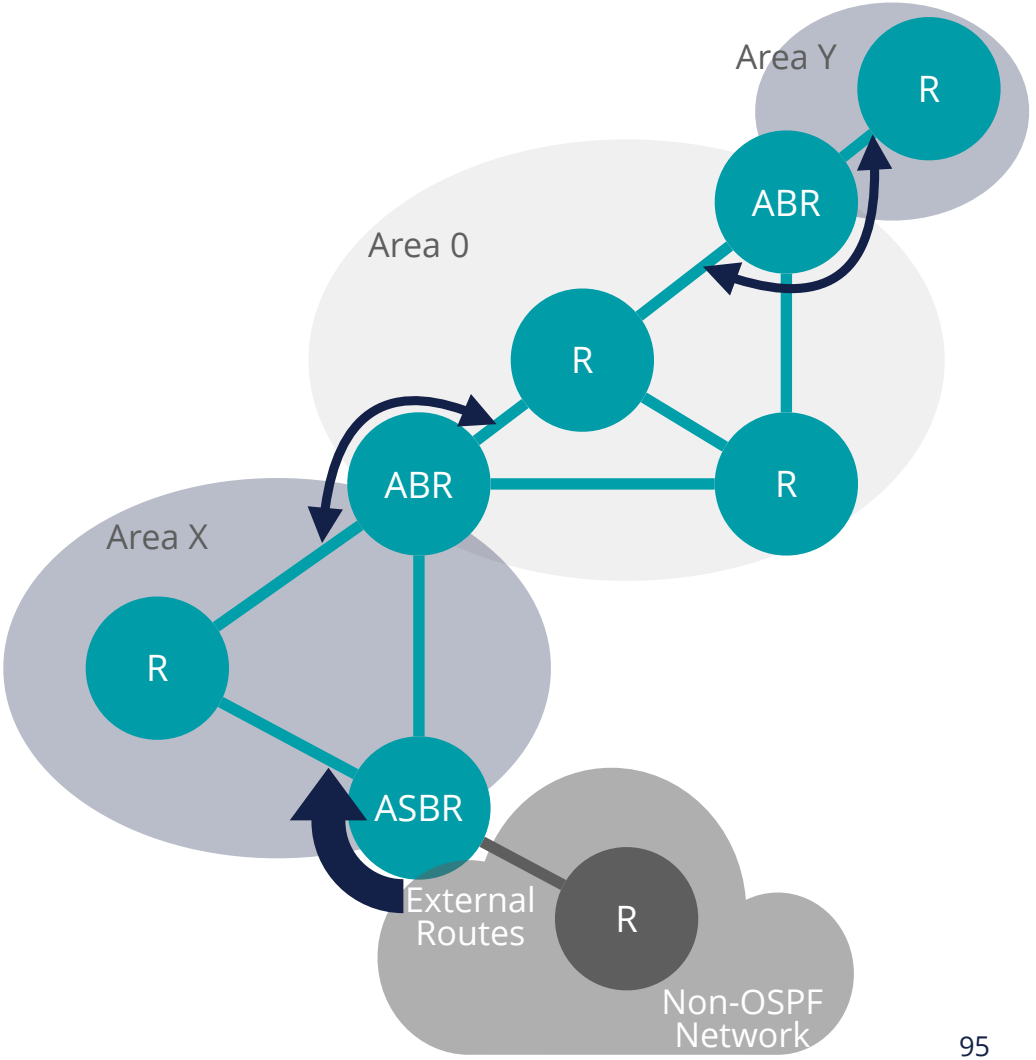
Backbone Networks

OSPFv3

OSPF Refresher

Open **S**hortest **P**ath **F**irst protocol

- Link-state protocol
  - Every router has full insight into network topology of the area
  - Routes are sent to other routers using Link State Advertisements (LSAs)
- Areas in OSPF and Area 0
- ABR/ASBR Roles
- Designated Router (DR) / Backup Designated Router (BDR) selection

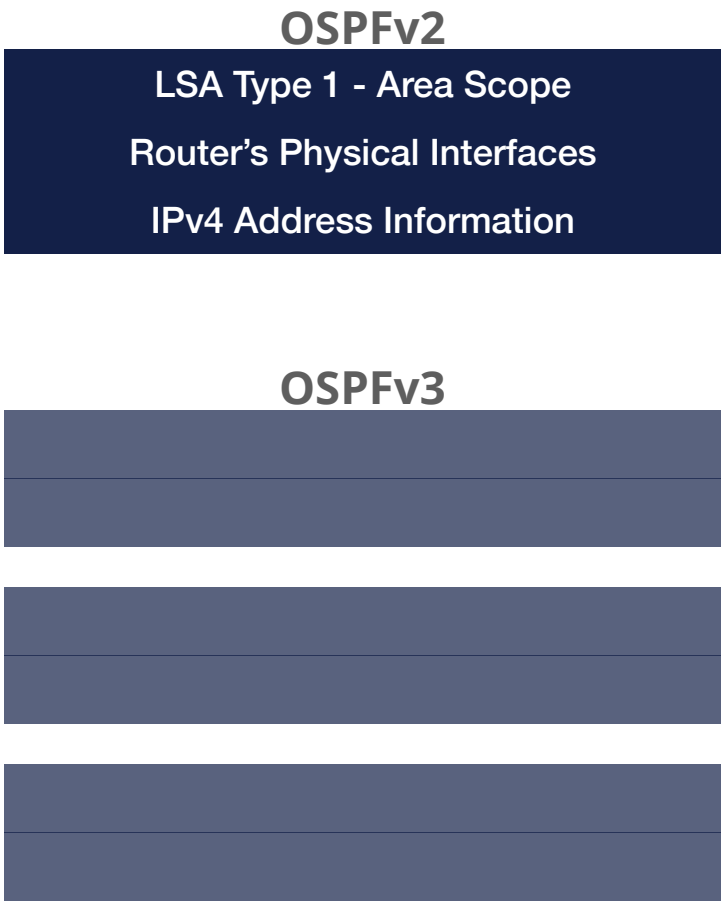


OSPFv3

- OSPFv3 is an implementation of OSPF for IPv6
- OSPFv3 runs directly over IPv6
- Most OSPFv3 functions are the same as OSPFv2
  - Neighbour discovery and adjacency formation mechanisms are identical
  - Router-ID lengths are same - 32 bits
- OSPFv3 and OSPFv2 are independent processes

What is New in OSPFv3?

- The **physical link and IPv6 address separation**
  - New LSA types - LSA 8 & 9
  - Various packet and LSA format changes (including removal of addressing semantics).
- Support for multiple instances of OSPF per link
  - to provide flexibility and segmentation in routing
- Addition of flooding scope
- Removal of opaque LSAs
- Using link-local addresses for adjacencies



New LSAs: Type-8 and Type-9

- Router-LSAs in OSPFv2
- Inefficient SPF calculations
- Separation of topology and IP information
- Link-LSAs - Type-8
- Intra-Area-Prefix LSA - Type-9

```
⊟ LS Update Packet
    Number of LSAs: 5
  ⊞ Router-LSA (Type: 0x2001)
  ⊞ Router-LSA (Type: 0x2001)
  ⊞ Network-LSA (Type: 0x2002)
  ⊟ Intra-Area-Prefix-LSA (Type: 0x2009)
      LS Age: 289 seconds
      Do Not Age: False
      LSA Type: 0x2009 (Intra-Area-Prefix-LSA)
      Link State ID: 0.0.0.2
      Advertising Router: 1.1.1.1 (1.1.1.1)
      LS Sequence Number: 0x80000001
      LS Checksum: 0x7226
      Length: 44
      # prefixes: 1
      Referenced LS type 0x2002 (Network-LSA)
      Referenced Link State ID: 0.0.0.2
      Referenced Advertising Router: 1.1.1.1
      PrefixLength: 64
    ⊞ PrefixOptions: 0x00
      Metric: 0
      Address Prefix: 2001::
  ⊟ Intra-Area-Prefix-LSA (Type: 0x2009)
      LS Age: 5 seconds
      Do Not Age: False
      LSA Type: 0x2009 (Intra-Area-Prefix-LSA)
      Link State ID: 0.0.0.0
      Advertising Router: 3.3.3.3 (3.3.3.3)
      LS Sequence Number: 0x80000001
      LS Checksum: 0x493a
      Length: 44
      # prefixes: 1
      Referenced LS type 0x2001 (Router-LSA)
      Referenced Link State ID: 0.0.0.0
      Referenced Advertising Router: 3.3.3.3
      PrefixLength: 64
    ⊞ PrefixOptions: 0x00
      Metric: 10
      Address Prefix: 2001::
```

OSPFv3 Question

What **remains the same** in OSPFv3 compared to OSPFv2?

a. Number of LSA types used
b. The length of the Router-ID
c. The separation of the physical topology and the IPv6 addresses
d. Usage of multicast addresses

OSPFv3 Answer

What **remains the same** in OSPFv3 compared to OSPFv2?

a. Number of LSA types used

The length of the Router-ID

c. The separation of the physical topology and the IPv6 addresses

d. Usage of multicast addresses

Backbone Networks

IS-IS

IS-IS Refresher

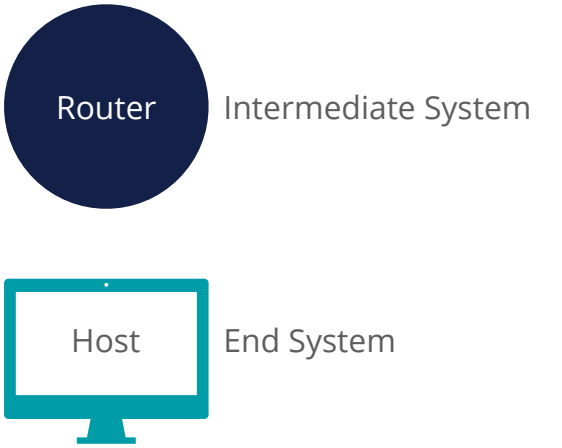
Intermediate **S**ystem to **I**ntermediate **S**ystem protocol

- Link-state protocol (just like OSPF)
  - Every router has full insight into network topology
  - Routes are sent to other routers using link-state-PDUs (LSPs)
  - Uses areas
  - Calculations based on Dijkstra algorithm (Shortest Path First - SPF)

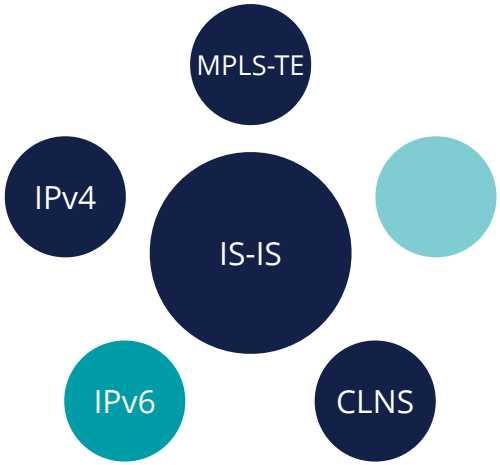
- LSPs use **T**ype-**L**ength-**V**alue fields (TLVs) to carry information

IS-IS Refresher

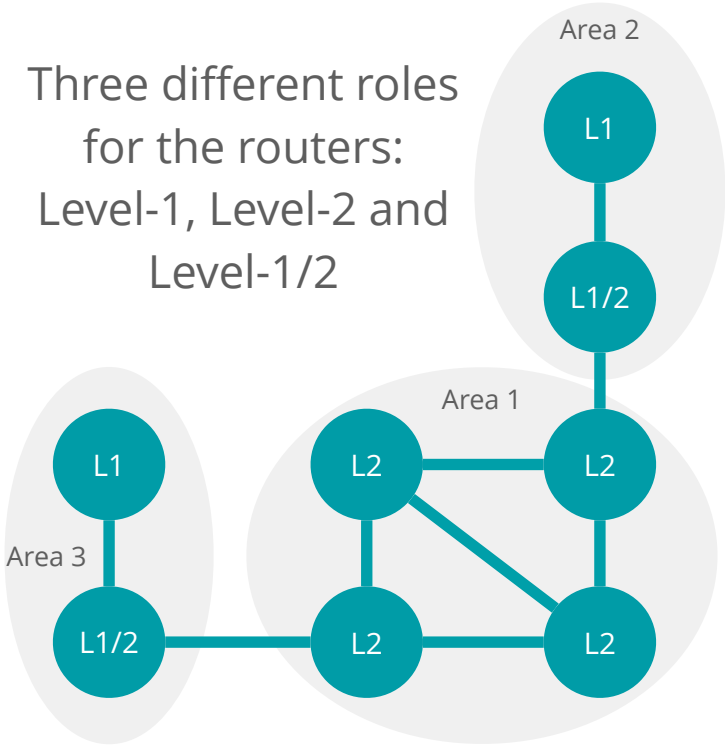
"Intermediate" and "End Systems" are basically routers and hosts



Thanks to the TLV structure **IS-IS is neutral to the network addresses**

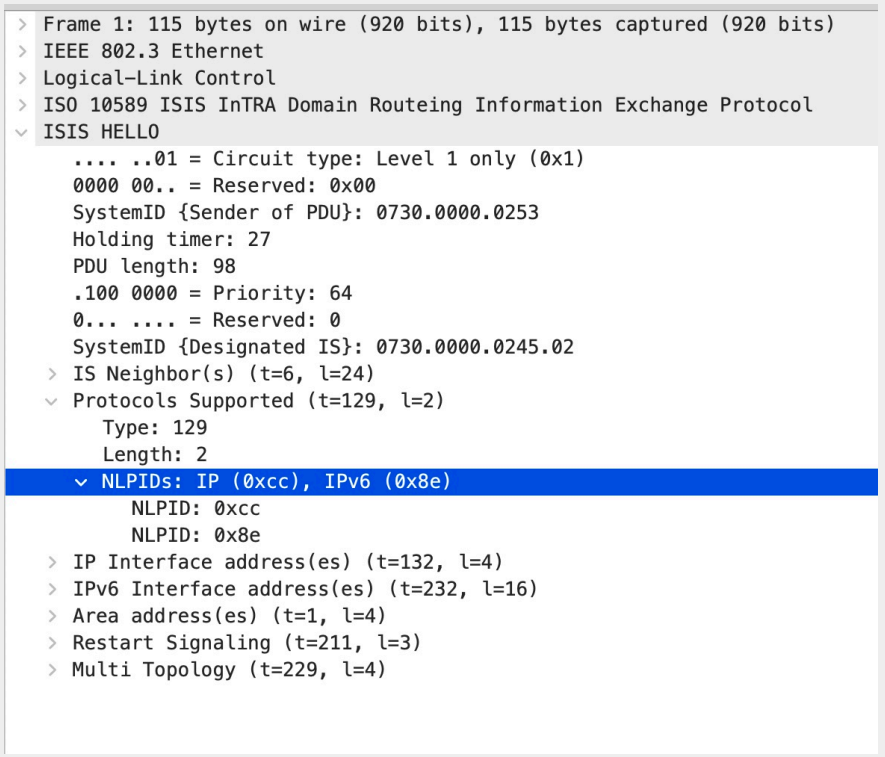


Three different roles for the routers: Level-1, Level-2 and Level-1/2



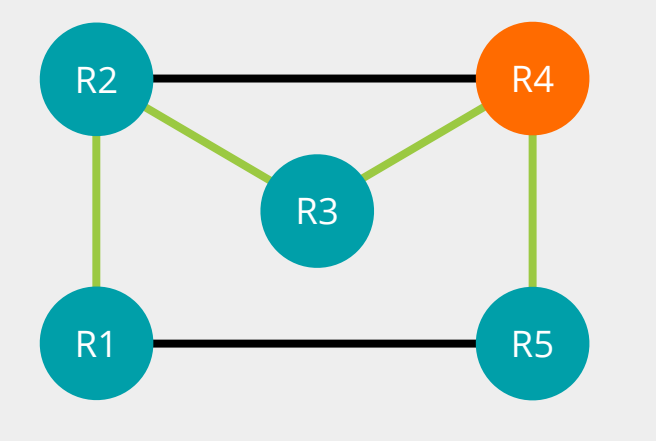
How Does IS-IS Carry IPv6 Information?

- LSP structure of IS-IS
- New TLVs for IPv6 (RFC 5308)
  - IPv6 Reachability TLV - type 236
  - IPv6 Interface Address TLV - type 232
- IPv6 NLPID (0x8E) is advertised by IPv6 enabled routers in the TLV 129 - *see the image on the right*



Multi Address Family Problem

Physical Topology



Routers supporting IPv4 and IPv6

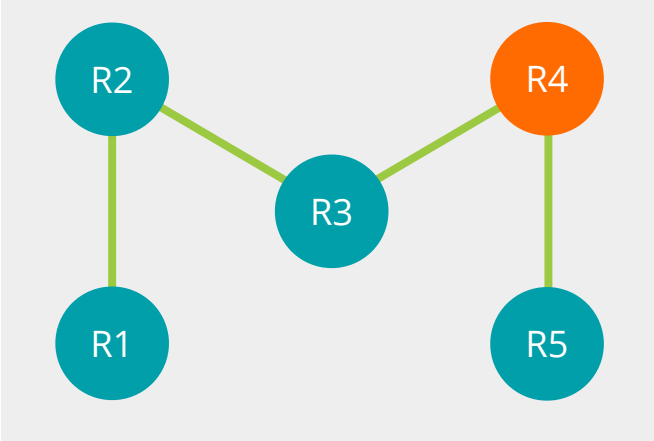
Routers supporting IPv4 only

High-cost links

Low-cost links

- Mismatching physical topologies for two different protocols (IPv4 and IPV6)
- By default, IS-IS runs a single SPF and calculates a single best-path
- Consider a scenario where R1 needs to send a IPv4 packet to R5 in the given topology

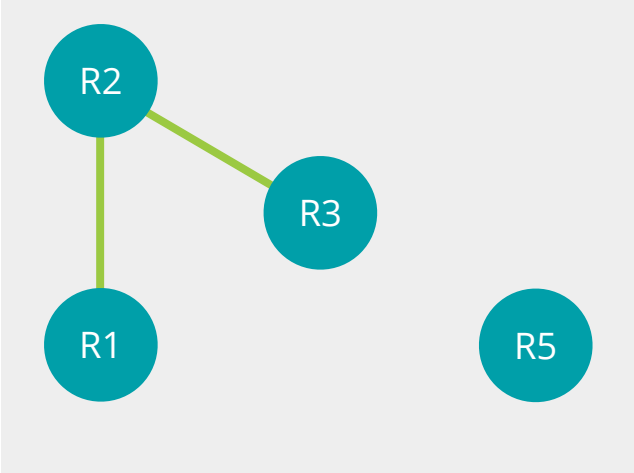
Best Path Calculated by IS-IS



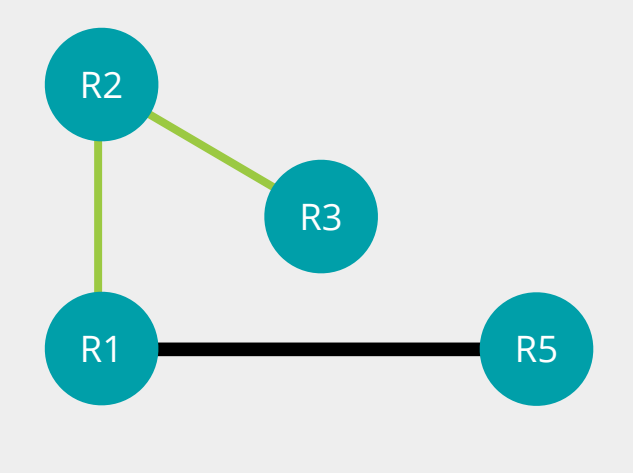
Multi-topology IS-IS

- **Now, consider the same for IPv6!**
- Multi-topology support for IS-IS (RFC 5120)
- New TLVs defined to enable;
  - Forming adjacencies
  - Advertisement of prefixes and reachable systems

Broken IPv6 Path



IPv6 Topology with MT enabled



Single vs. Multi Topology IS-IS

IS-IS Single Topology	IS-IS Multitopology
Same topology for all address families	Different topologies for different address families
One SPF for all address families	Individual SPFs for each address family
Requires less resources	Requires more resources
Old TLVs used	Multitopology TLVs used
Useful when the topologies are identical or congruent	Useful in the transition period

IS-IS Question

What advantage(s) of IS-IS allows it to be easily extended to carry other Layer-3 Protocols like IPv6?

a. Non-IP dependency
b. TLV structure in LSPs
c. Neutrality to the network addresses
d. All of the above

IS-IS Answer

What advantage of IS-IS allows it to be easily extended to carry other Layer-3 Protocols like IPv6?

a. Non-IP dependency

b. TLV structure in LSPs

c. Neutrality to the network addresses

✓ All of the above

Backbone Networks

IS-IS vs OSPFv3

Which protocol should we choose?

OSPFv3 or IS-IS?

The better one! For YOU!

Some Thoughts

- Both of the protocols are **comparable** and **open standard**
- OSPF is broadly deployed in enterprise market where IS-IS is the choice of ISPs as they need to build very large, flat networks
- You can choose either of them based on **your knowledge** about each protocol
- Another important factor to consider is the **vendor implementation**
- One more consideration: **SRv6**
  - Both protocols have proper extensions for SRv6.
  - For the deployment of SRv6 market mostly chooses IS-IS

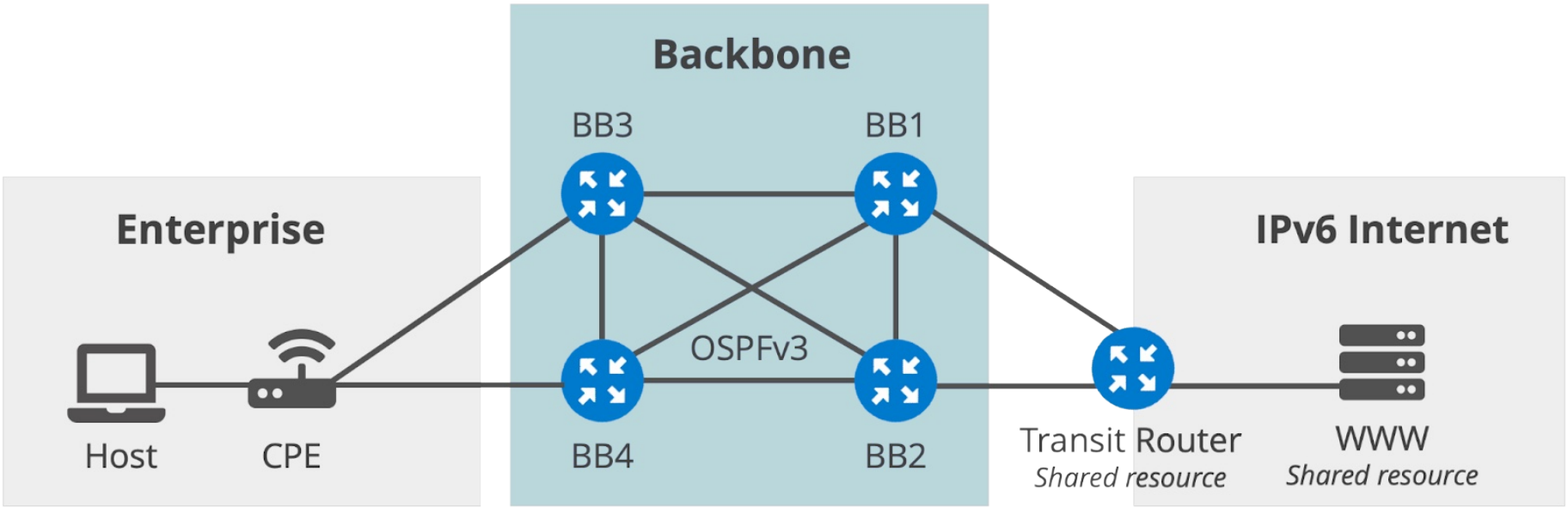
In the end, it is your design decision!

Questions

Lab Activity 2

Configuring OSPFv3 inside the backbone network

Lab Activity 2 - Configuring OSPFv3 inside the backbone network



In this LAB activity you'll work on the routers **BB1, BB2, BB3 and BB4 only**.

Lab Activity 2 - Configuring OSPFv3 inside the backbone network

- **Description**: In this lab activity you'll be configuring OSPFv3 among the backbone routers BB1, BB2, BB3 and BB4.
- **Goal**: Configure OSPFv3 in an IPv6 topology
- **Time:** 30 minutes
- **Tasks:**

  1. Check existing OSPFv2 configuration
  2. Configure OSPFv3 among the backbone routers
  3. Compare OSPFv2 and OSPFv3 Databases

Lab Activity 2 - Configuring OSPFv3 inside the backbone network

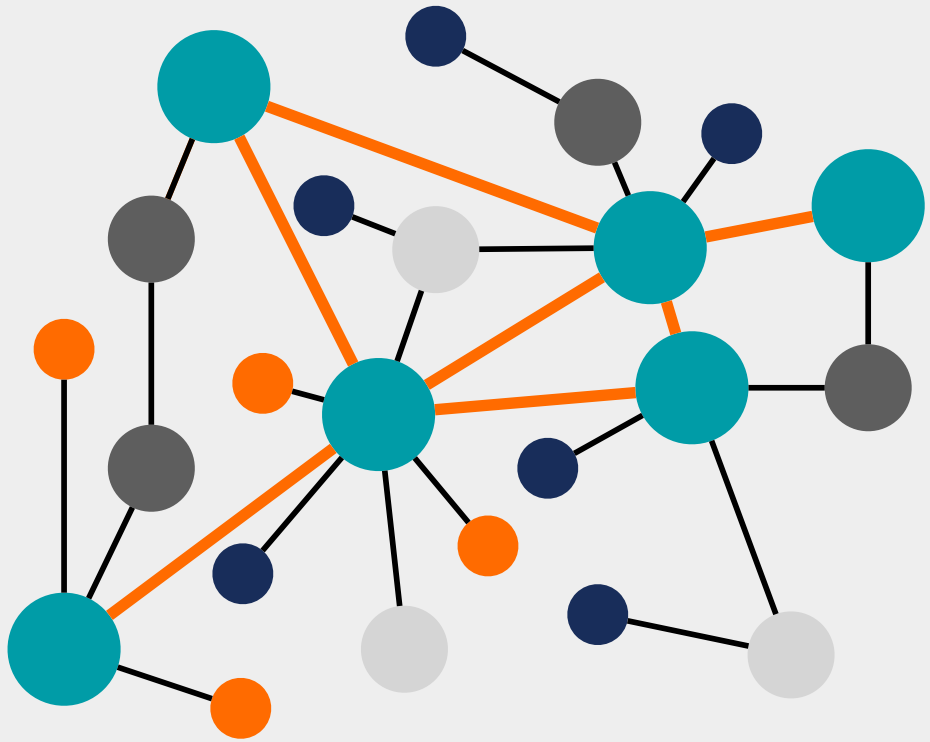
- **What have you learned?**
  - You checked the existing lab setup for OSPFv2 in the backbone network
  - You configured OSPFv3 between the backbone routers
  - You checked the routing tables for IPv6 to see the populated OSPF routes
  - You verified the connectivity with the ping tool
  - And you compared the OSPFv2 and OSPFv3 databases to see the difference between the ways how IP information is distributed.

Backbone Networks

BGP

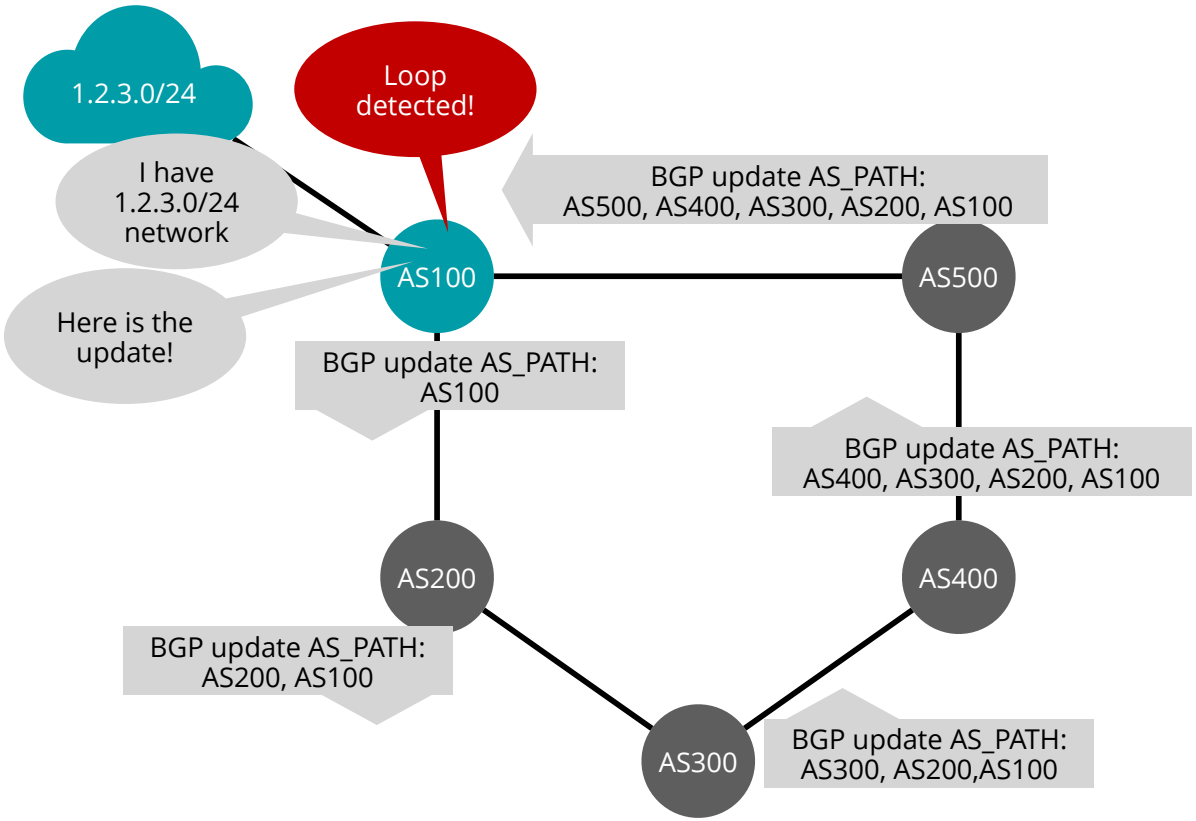
BGP Refresher

- Postal service of the Internet
- Exterior gateway protocol
- Path vector protocol
- Autonomous system
  - AS numbers; 16 or 32 bits
- Multiple attributes are supported



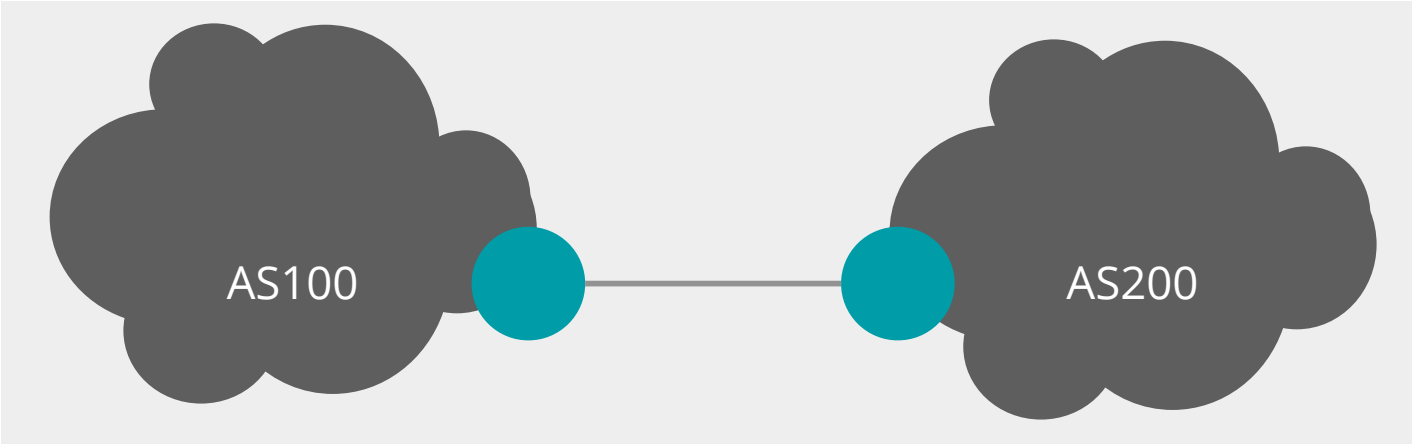
BGP Refresher - AS Path

- It is a **sequence of ASes** a route has traversed
- It is used for **loop detection** and in the algorithm of **best path selection**

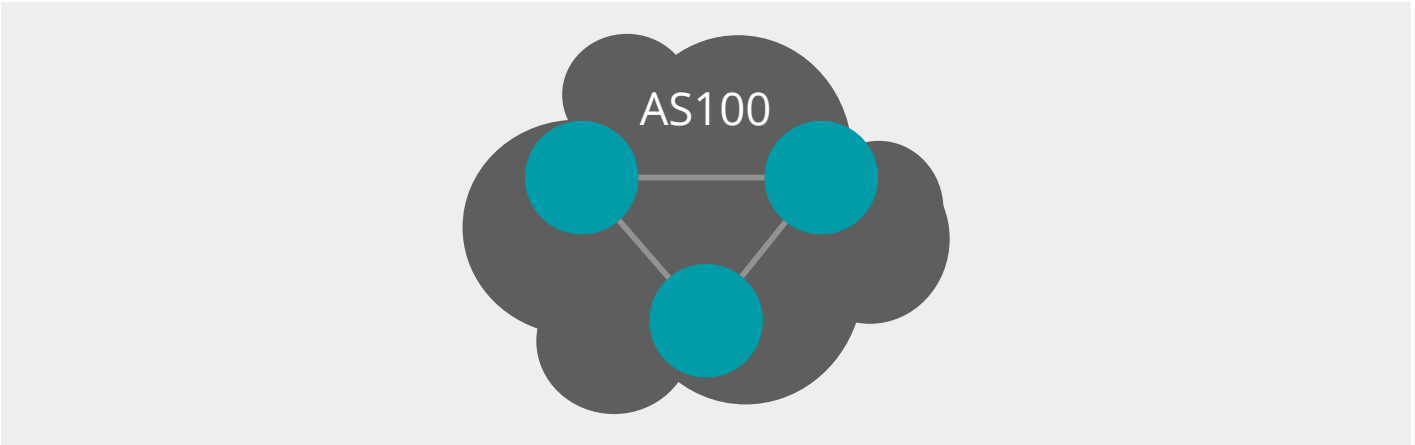


BGP Refresher - BGP Modes

eBGP



iBGP



BGP Refresher - BGP Messages

OPEN

opens the tcp session and capabilities exchange

NOTIFICATION

error handling

KEEPALIVE

keeps the session running

UPDATE

actual route updates (**NLRI**, AS-path, AS-path attributes)

BGP Update Message

- Message structure
- NLRI
  - Prefix
  - Mask

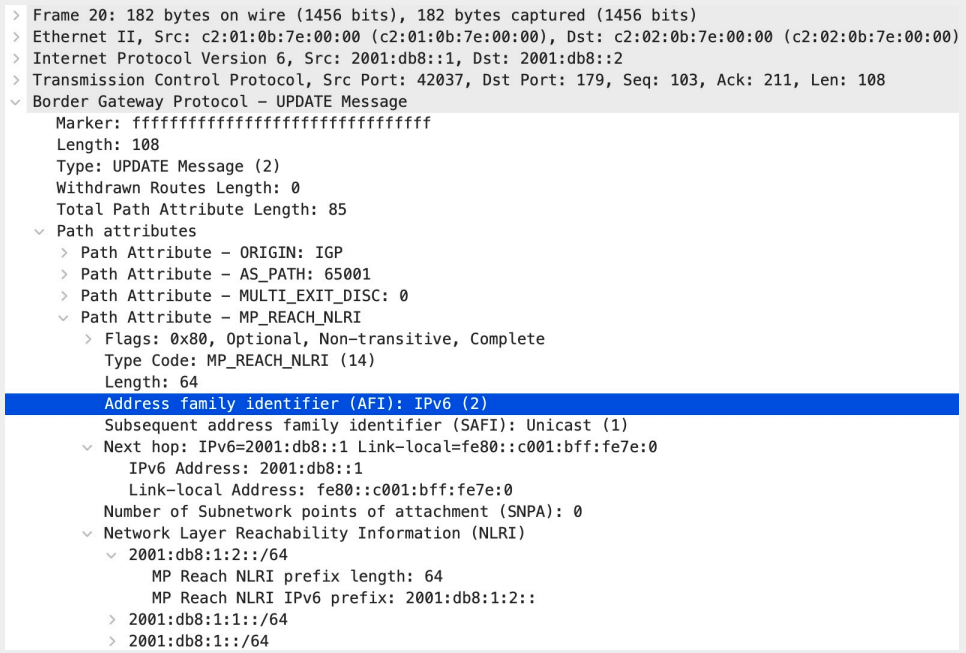
```
> Frame 1: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface -, id 0
> Frame Relay
> Internet Protocol Version 4, Src: 10.1.12.2, Dst: 10.1.12.1
> Transmission Control Protocol, Src Port: 179, Dst Port: 56516, Seq: 1, Ack: 1, Len: 102
v Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 52
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 25
  > Path attributes
  > Network Layer Reachability Information (NLRI)
v Border Gateway Protocol - UPDATE Message
    Marker: ffffffffffffffffffffffffffffffff
    Length: 50
    Type: UPDATE Message (2)
    Withdrawn Routes Length: 0
    Total Path Attribute Length: 25
  v Path attributes
    > Path Attribute - ORIGIN: IGP
    > Path Attribute - AS_PATH: 200
    > Path Attribute - NEXT_HOP: 10.1.12.2
    > Path Attribute - MULTI_EXIT_DISC: 242
  v Network Layer Reachability Information (NLRI)
    > 2.0.0.0/8
```

Multiprotocol BGP (MP-BGP)

- Multiprotocol Extensions for BGP-4 - RFC 2283
- Some of the protocols supported by MP-BGP
  - IPv4 unicast
  - IPv4 multicast
  - IPv6 unicast
  - IPv6 multicast
  - L2-VPN

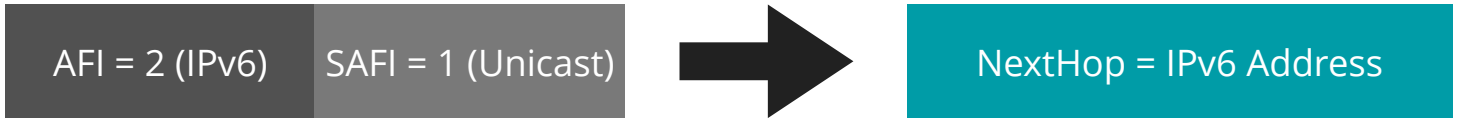
Multiprotocol BGP (MP-BGP)

- New capabilities in OPEN message (RFC 2842)
  - AFI - Address family identifier
  - SAFI - Subsequent address family identifier
- In RFC 2283 two things to be added to BGP-4
  - (a) the ability to associate a particular Network Layer protocol with the **next hop information**, and
  - (b) the ability to associate a particular Network Layer protocol with **NLRI**

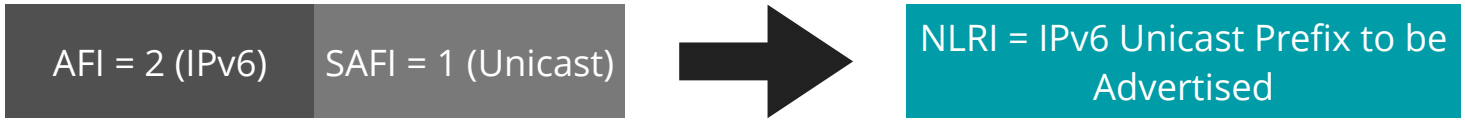


Multiprotocol BGP (MP-BGP)

- The ability to associate a particular Network Layer protocol with the **next hop information**, and



- The ability to associate a particular Network Layer protocol with **NLRI**



Examples of AFI and SAFI

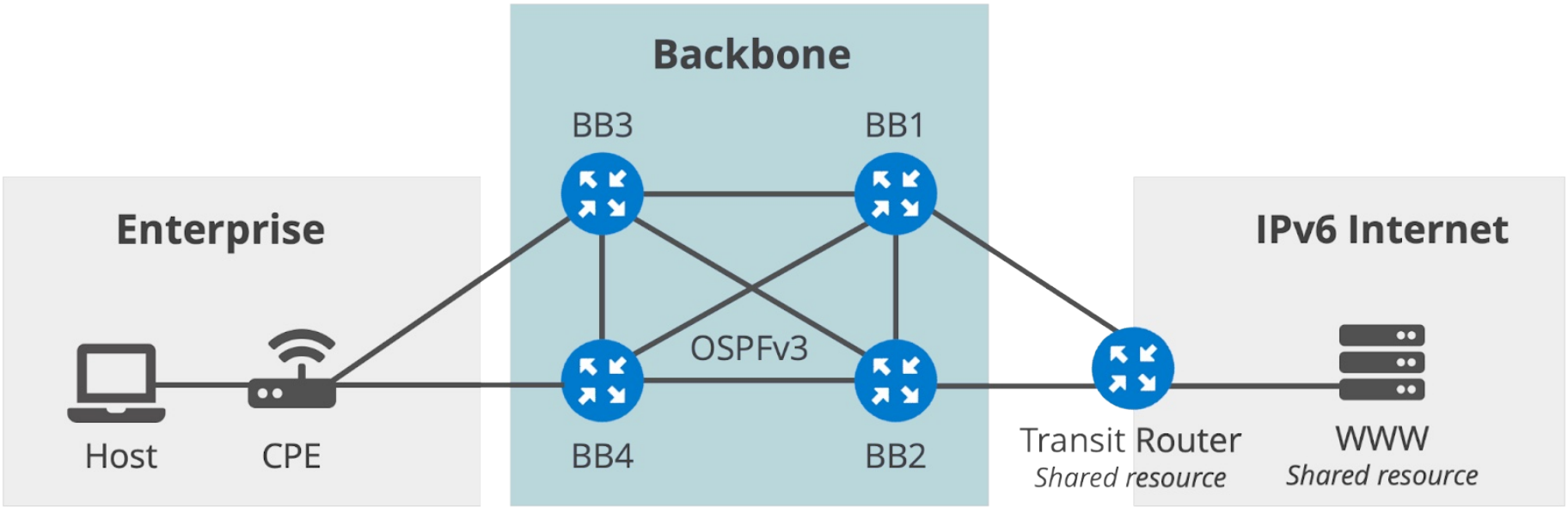
- Address Family Identifier (AFI) - Identifies address type
  - AFI = 1 (IPv4)
  - AFI = 2 (IPv6)
- Subsequent Address Family Identifier (SAFI) - Identifies sub category of address type
  - Sub-AFI = 1 (NLRI is used for unicast)
  - Sub-AFI = 2 (NLRI is used for multicast RPF check)
  - Sub-AFI = 3 (NLRI is used for both unicast and multicast RPF check)
  - Sub-AFI = 4 (label)
  - Sub-AFI = 128 (VPN)

Questions

Lab Activity 3

Configuring BGP in the backbone network

Lab Activity 3 - Configuring BGP in the backbone network



In this LAB activity you'll work on the routers **BB1, BB2, BB3 and BB4 only**.

Lab Activity 3 - Configuring BGP in the backbone network

- **Description**: You'll configure eBGP with the transit router and iBGP with the other routers inside the backbone network over IPv6 connections.
- **Goal**: Configure BGP in an IPv6 topology
- **Time:** 30 minutes
- **Tasks:**
  1. Configuring eBGP with the transit router
  2. Configuring iBGP within the backbone

Lab Activity 3 - Configuring BGP in the backbone network

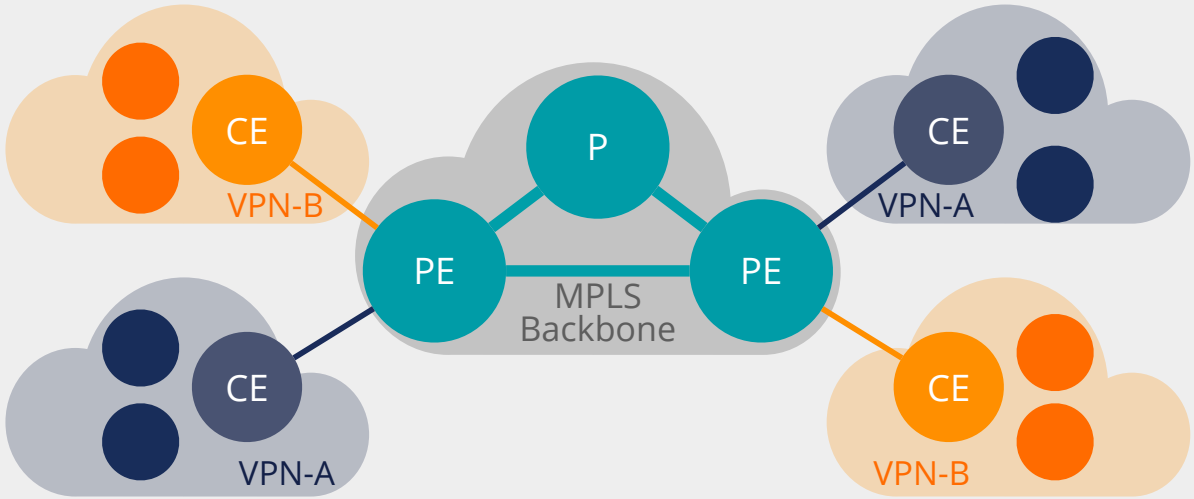
- **What have you learned?**
  - You checked the existing eBGP connections between the transit router and the 2 of the backbone routers; BB1 and BB2.
  - You configured eBGP over IPv6 between the transit router and the backbone routers BB1
  - You configured the required policies to receive and send the routes
  - You configured iBGP over IPv6 within the backbone network.
  - You compared the address family attributes (AFIs) of IPv4 and IPv6 routes

Backbone Networks

MPLS

MPLS Refresher

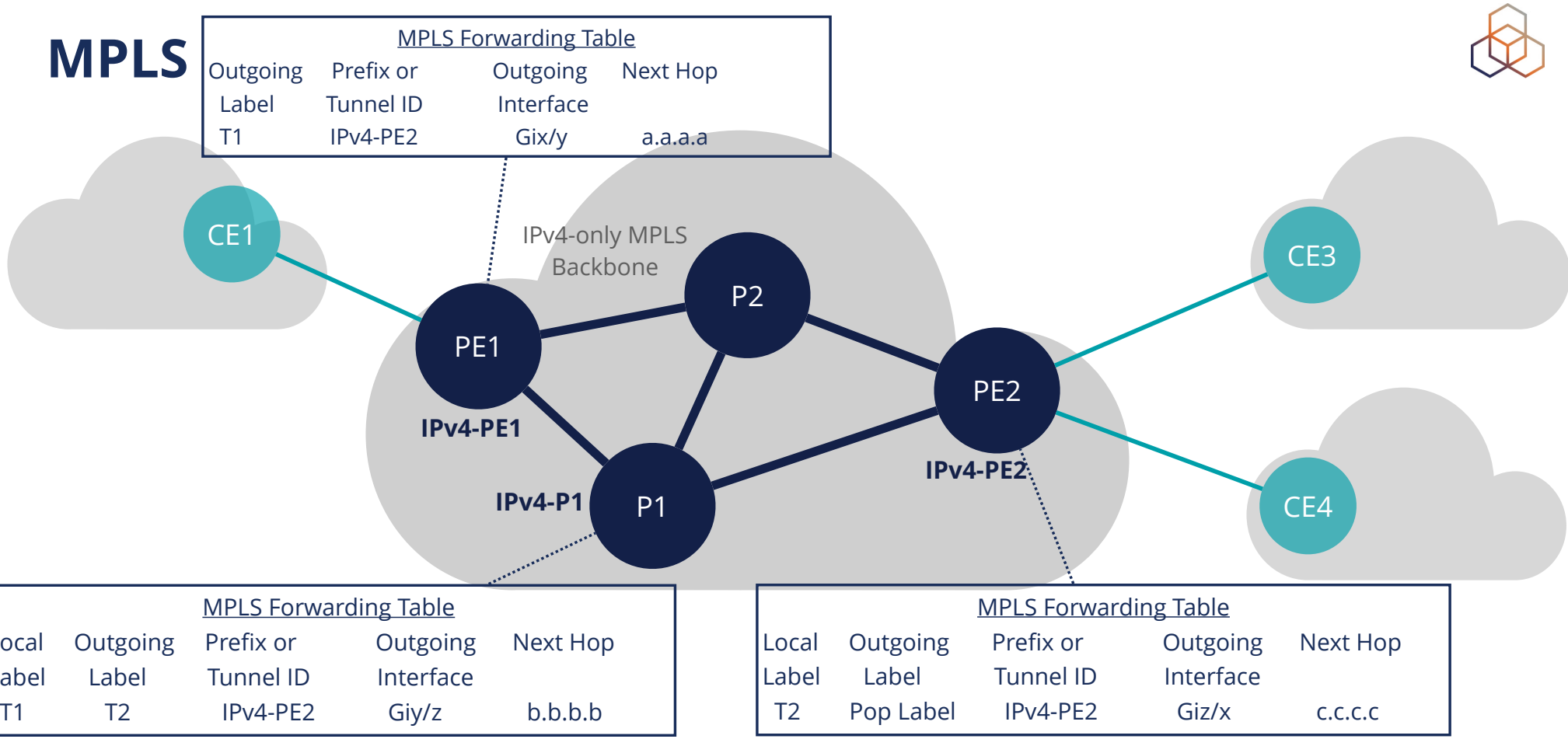
- Label Switching (instead of routing)
- Layer 2.5
- Efficiency in the data path
- Enables VPNs
- PE, P, LSR
- IGP, LDP, BGP



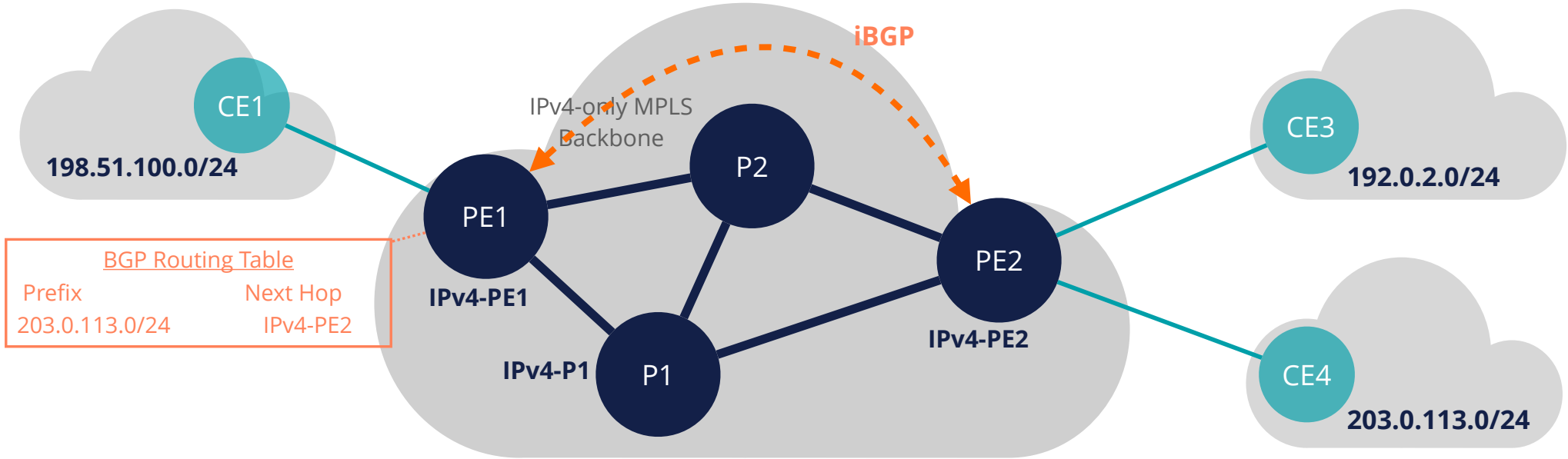
S Label — Service label indicates which service this packet belongs to

T Label — Transport label indicates how to reach the next hop

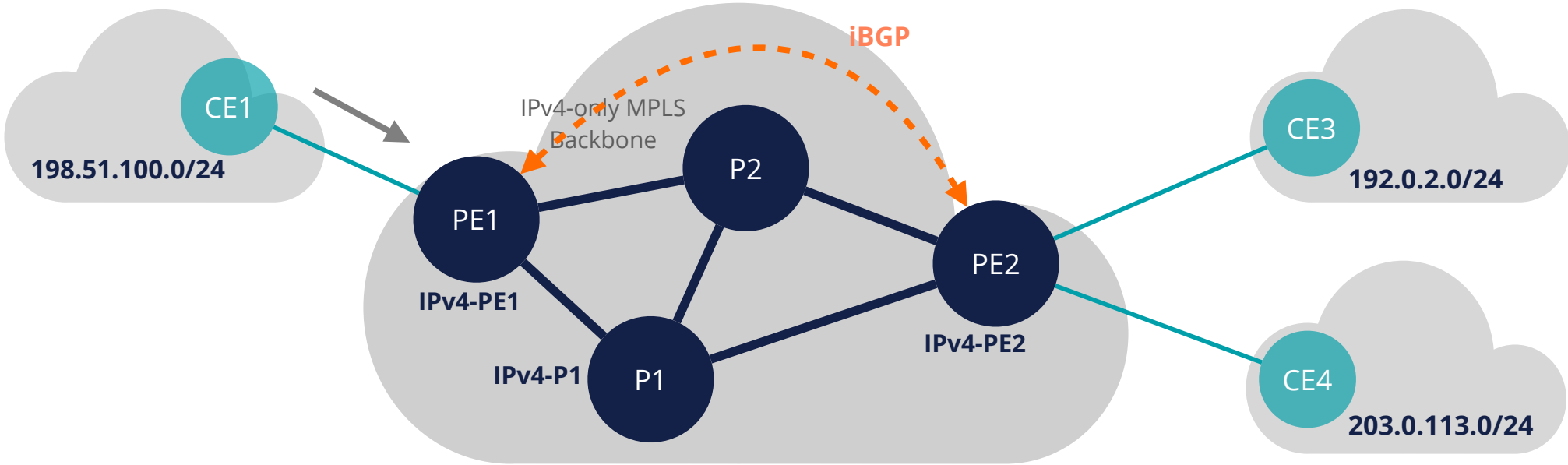
MPLS


MPLS Forwarding Table
Outgoing Label
Prefix or Tunnel ID
Outgoing Interface
Next Hop
T1
IPv4-PE2
Gix/y
a.a.a.a
CE1
IPv4-only MPLS Backbone
P2
PE1
IPv4-PE1
IPv4-P1
P1
PE2
IPv4-PE2
CE3
CE4
MPLS Forwarding Table
Local Label
Outgoing Label
Prefix or Tunnel ID
Outgoing Interface
Next Hop
T1
T2
IPv4-PE2
Giy/z
b.b.b.b
MPLS Forwarding Table
Local Label
Outgoing Label
Prefix or Tunnel ID
Outgoing Interface
Next Hop
T2
Pop Label
IPv4-PE2
Giz/x
c.c.c.c

MPLS


iBGP
IPv4-only MPLS Backbone
CE1
198.51.100.0/24
PE1
IPv4-PE1
P2
P1
IPv4-P1
PE2
IPv4-PE2
CE3
192.0.2.0/24
CE4
203.0.113.0/24
BGP Routing Table
Prefix
Next Hop
203.0.113.0/24
IPv4-PE2

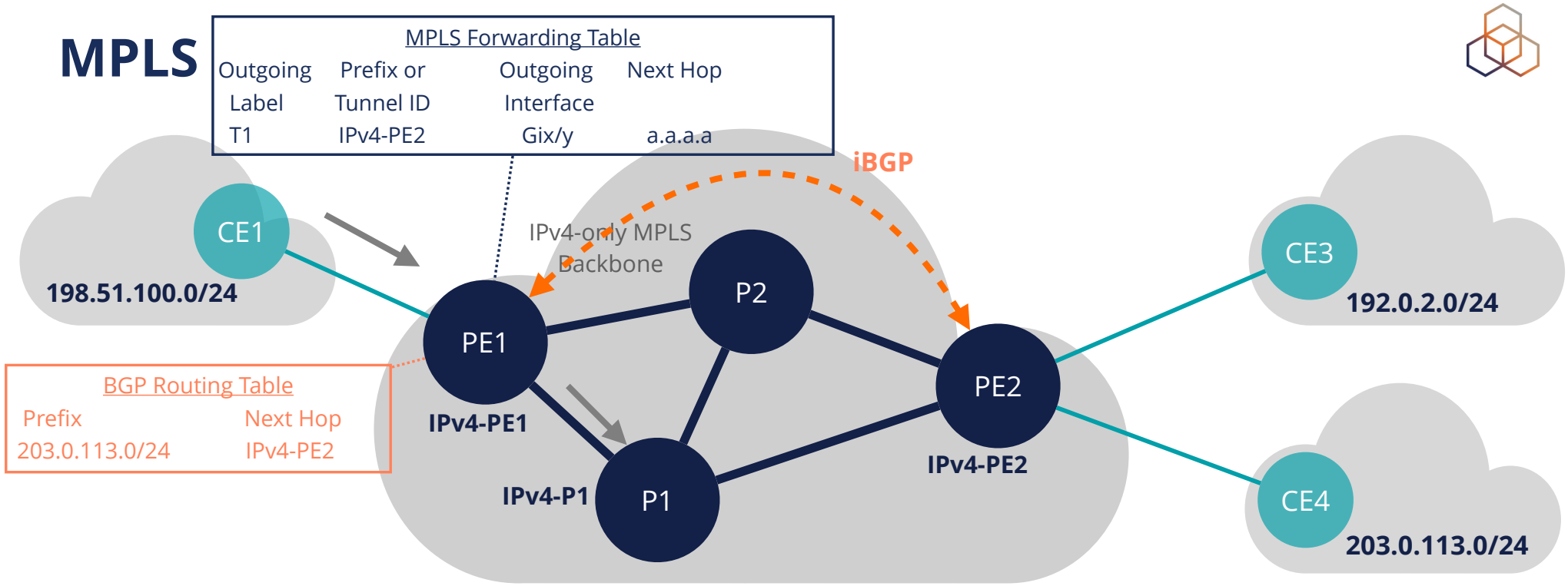
MPLS



IPv4 Destination = **203.0.113.4**

IPv4 →

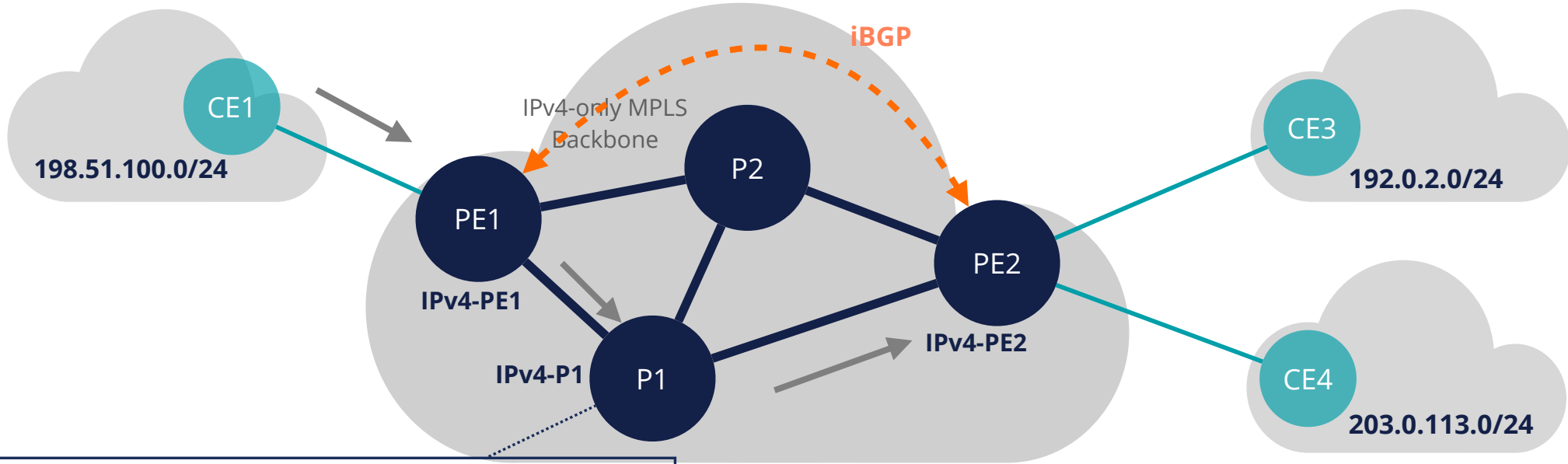
MPLS



IPv4 Destination = **203.0.113.4**

IPv4 → T1 Label | IPv4

MPLS

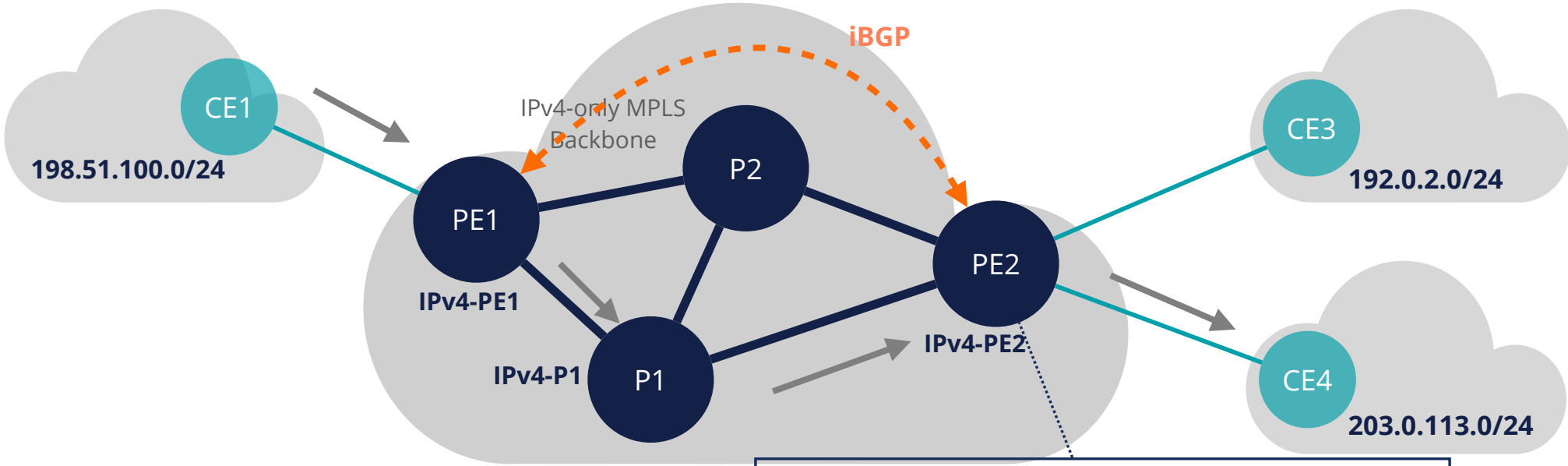


MPLS Forwarding Table

Local Label	Outgoing Label	Prefix or Tunnel ID	Outgoing Interface	Next Hop
T1	T2	IPv4-PE2	Giy/z	b.b.b.b

IPv4 Destination = **203.0.113.4**

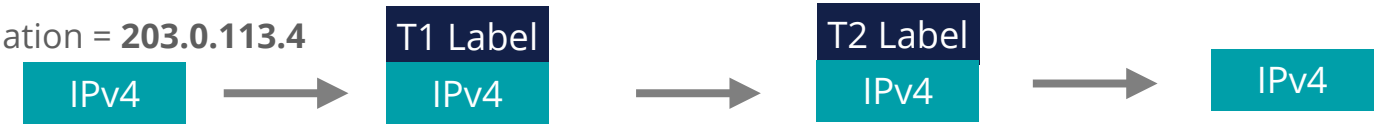
MPLS



MPLS Forwarding Table

Local Label	Outgoing Label	Prefix or Tunnel ID	Outgoing Interface	Next Hop
T2	Pop Label	IPv4-PE2	Giz/x	c.c.c.c

IPv4 Destination = **203.0.113.4**



Enabling IPv6 on MPLS Backbone - Two Approaches

Approach 1
6PE & 6VPE

Use **existing MPLS labelling**

Approach 2
LDPv6

Enable **dual-stack or**

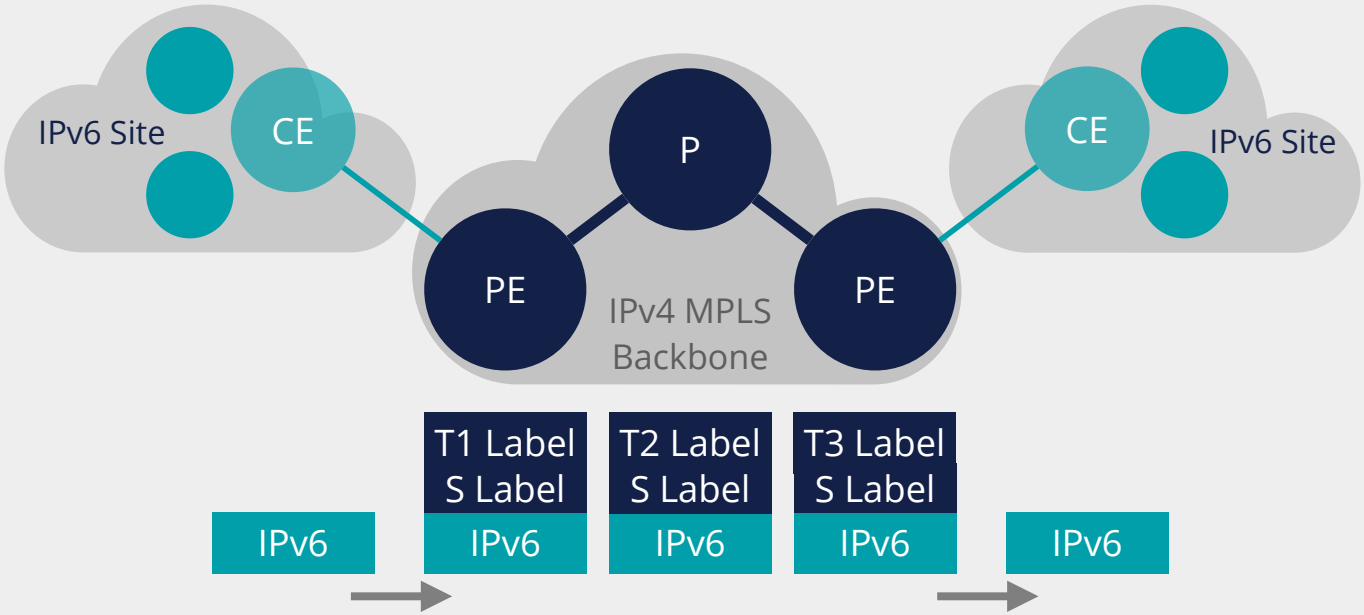
IPv6-only

On all backbone routers

6PE

- MPLS Tunnelling IPv6 over IPv4
- IPv4 IGP and LDP
- Dual-stack PEs
- IPv4 only P routers
- MP-BGP IPv6 sites' routes
- One IPv6 routing space
- Packet delivery
  - IPv6 lookups
  - Label pushing

Approach 1



6PE

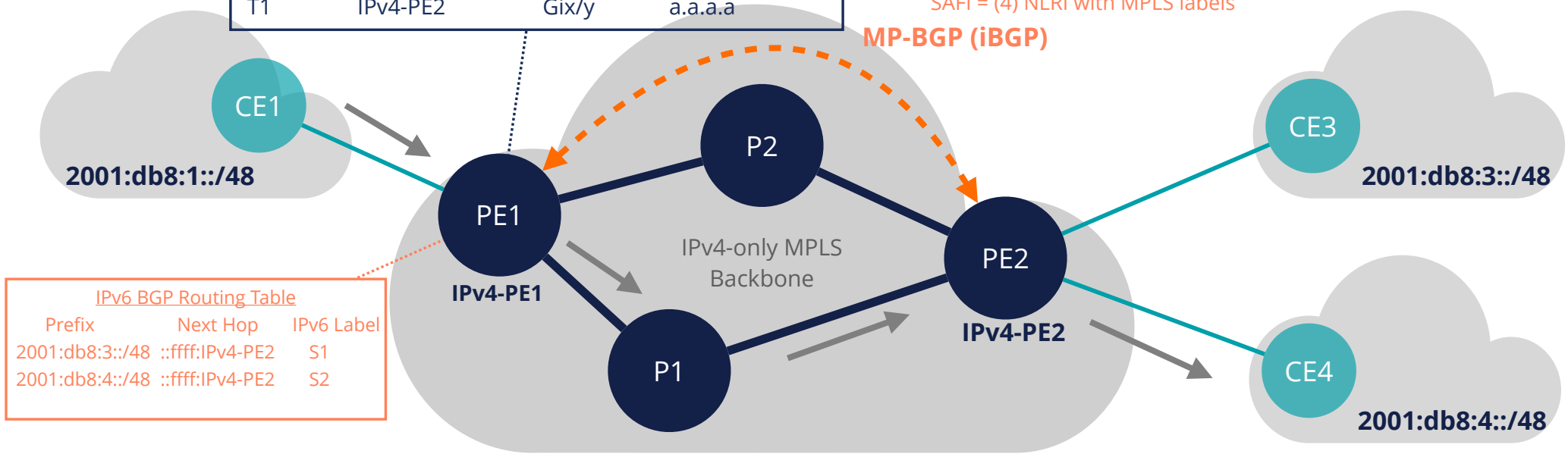
MPLS Forwarding Table

Outgoing Label	Prefix or Tunnel ID	Outgoing Interface	Next Hop
T1	IPv4-PE2	Gix/y	a.a.a.a

AFI = (2) IPv6

SAFI = (4) NLRI with MPLS labels

MP-BGP (iBGP)



IPv6 BGP Routing Table

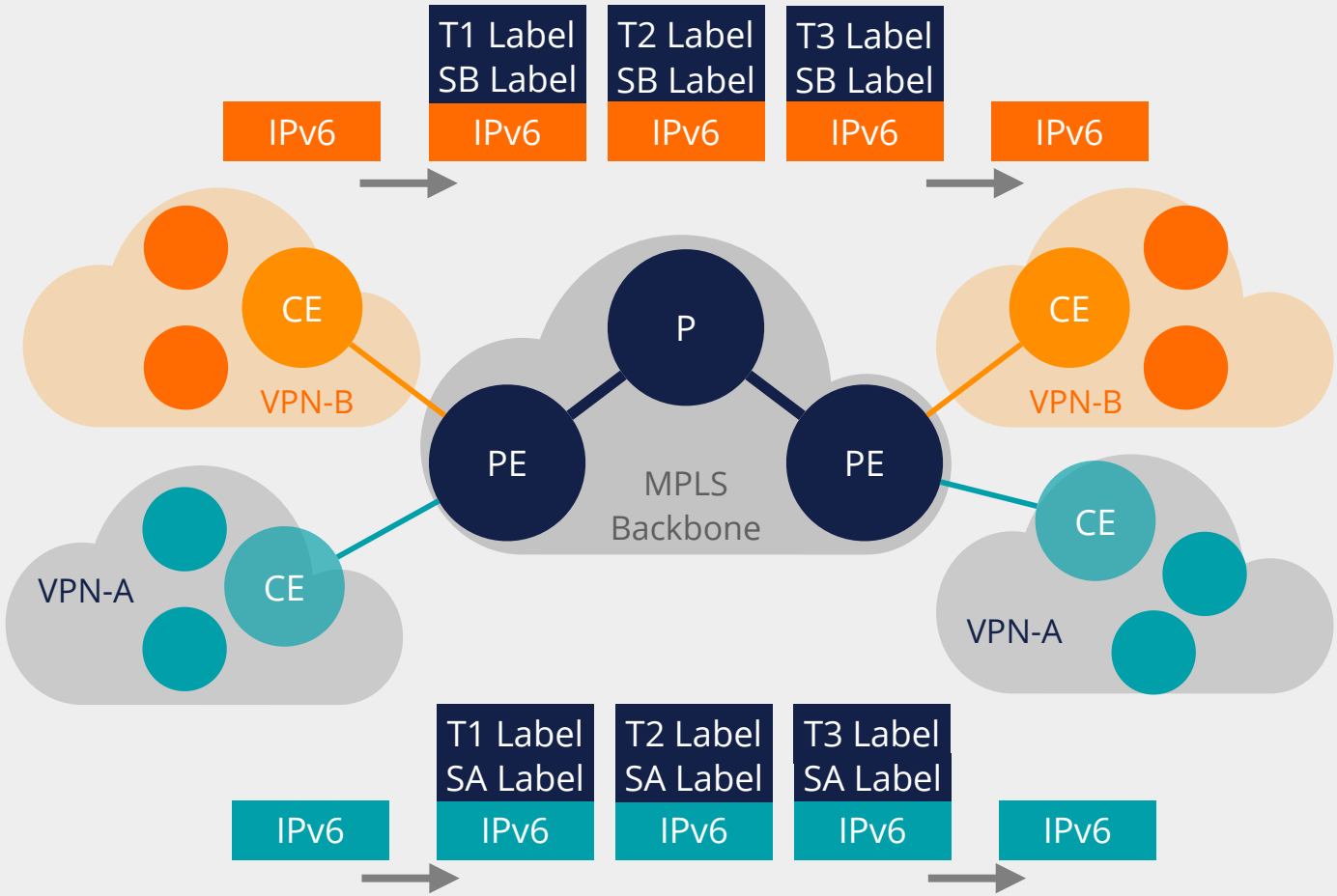
Prefix	Next Hop	IPv6 Label
2001:db8:3::/48	::ffff:IPv4-PE2	S1
2001:db8:4::/48	::ffff:IPv4-PE2	S2

IPv6 Destination = **2001:db8:4::1**

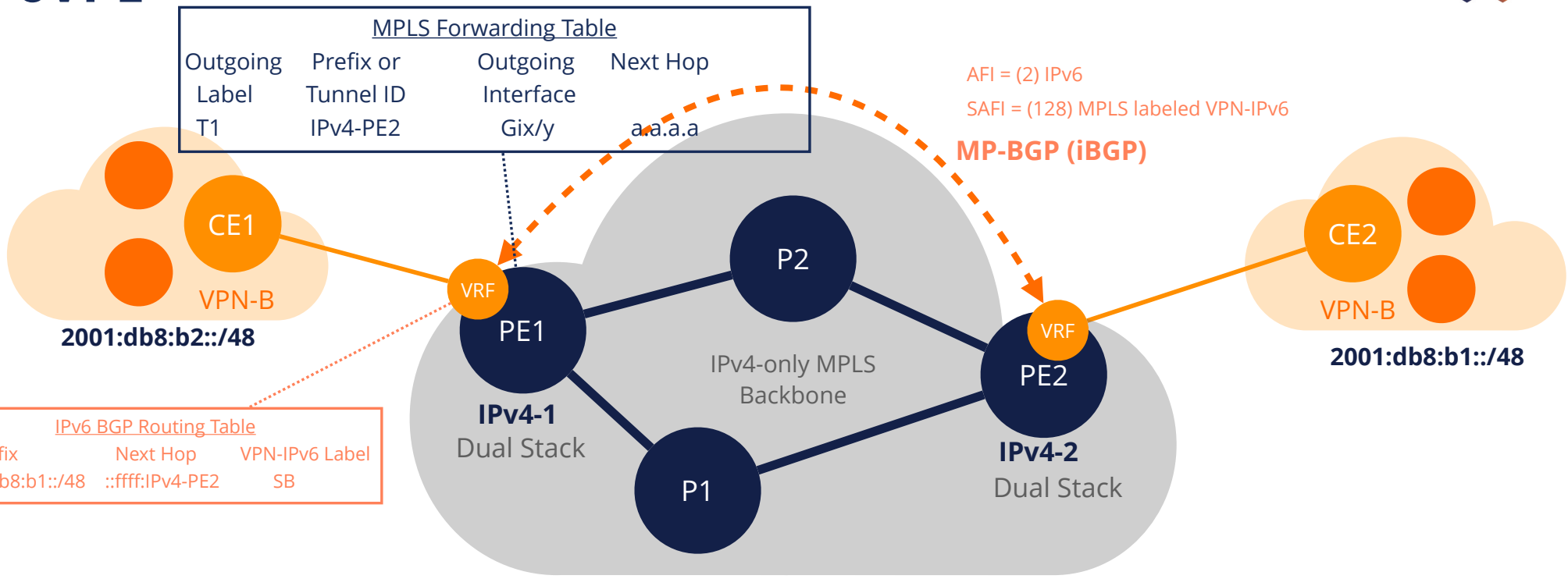
6VPE

- Enables IPv6 VPN service isolation
- IPv4 IGP and LDP
- Dual-stack PEs
- IPv4 only P routers
- MP-BGP IPv6 sites' routes
- Per-VPN IPv6 routing space
- Packet delivery
  - IPv6 lookups
  - Label pushing

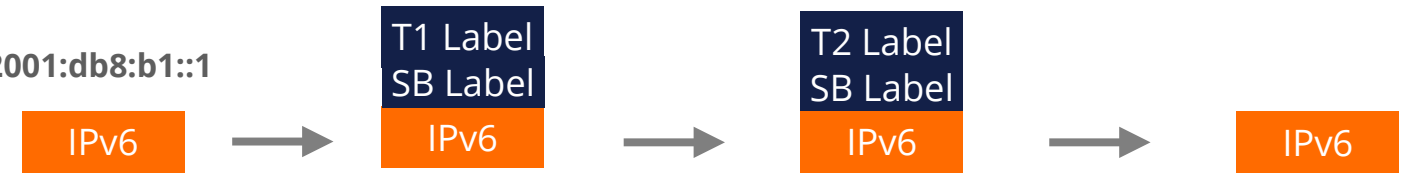
Approach 1



6VPE



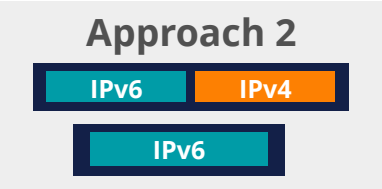
IPv6 Destination = **2001:db8:b1::1**



LDPv6

- Alternative approach for enabling IPv6 for services
- Enables MPLS functionality over IPv6 networks

- Label distribution for MPLS in IPv6 networks
  - RFC 7552 - in 2015



6PE and 6VPE or LDPv6 or SRv6?

6PE or 6VPE  For existing IPv4-only MPLS networks

LDPv6*  For greenfield networks

SRv6  For greenfield networks

* For greenfield networks, SRv6 is a viable alternative for LDPv6, if it is supported by the platforms you use as it simplifies the protocol stack.

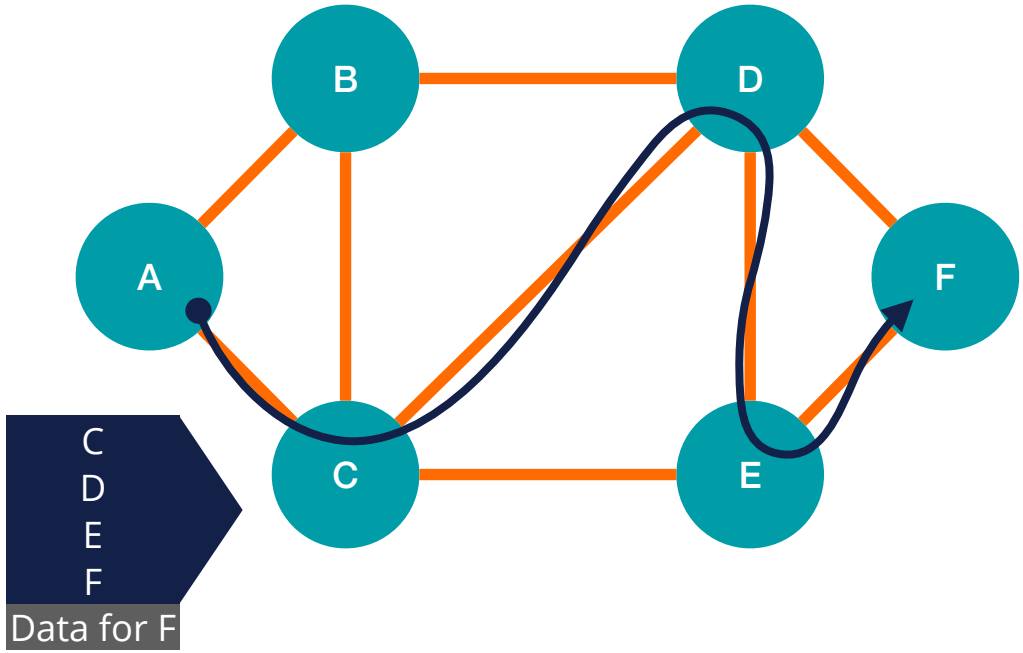
Questions

Backbone Networks

SRv6

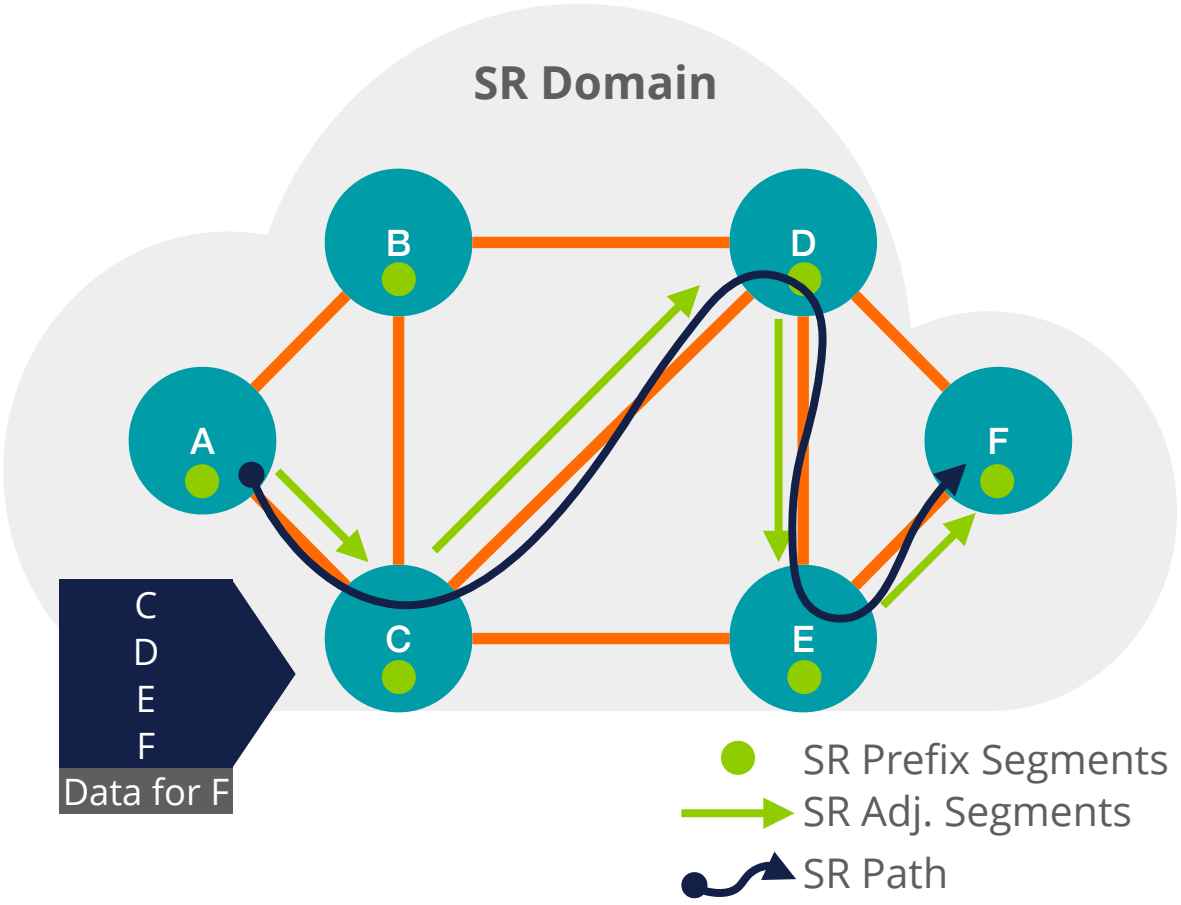
What is Segment Routing?

- Source-based routing
- Two different types:
  - SR-MPLS
  - SRv6



Elements of SR

- SR Domain
- SR Path
- SR Segments
  - Adjacency segment
  - Prefix segment



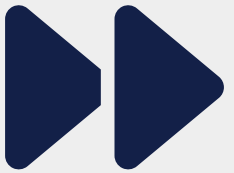
Operations in SR Domain

PUSH

Adding a new segment to the beginning of the list. For SRv6, it is the first segment in the SRv6 extension header (SRH)

NEXT

Moving on to the next segment in the list. For SRv6, copying the next segment from the SRH to the destination address of the IPv6 header



CONTINUE

Current segment stays active. For SRv6, the normal IPv6 forwarding action

SRv6

- Segment Routing Extension Header (SRH)
- SID structure

128-bit SRv6 SID

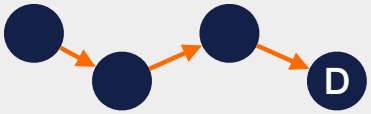
Locator: the route to the node performing the function

Function: the forwarding behaviour to be executed by the node

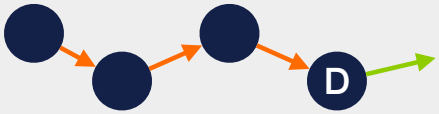
Arguments (optional): if the function needs (not shown in the drawing)

SRv6 Network Programming - Endpoint Behaviours

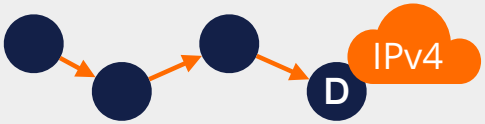
End Instruction
the shortest path to a given node



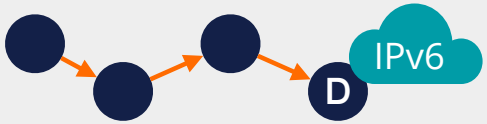
End.X Instruction
the shortest path to a given node followed by a forwarding over a specific link



End.DT4
the shortest-path to a selected egress node followed by a IPv4-VPN table lookup

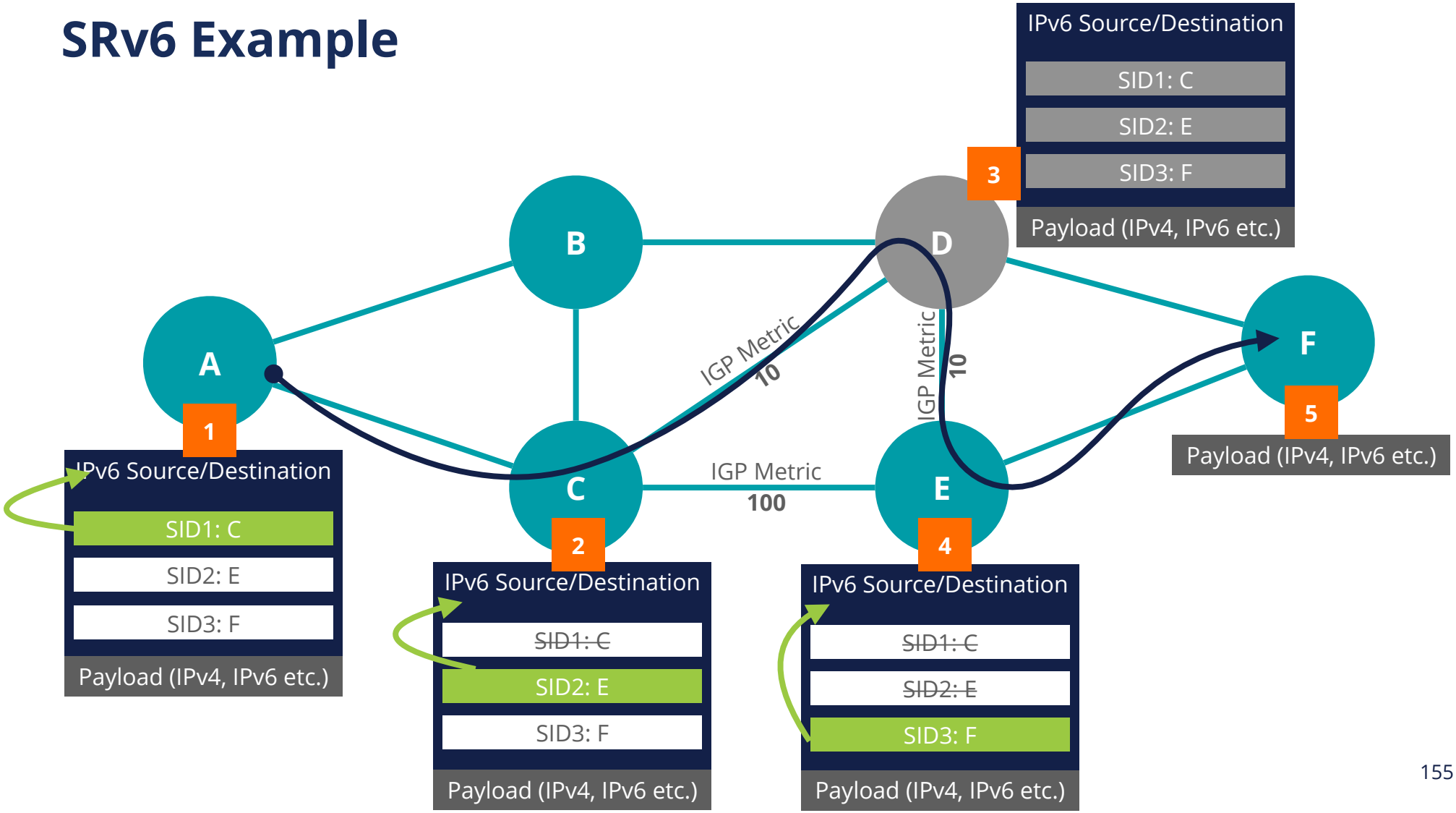


End.DT6
the shortest-path to a selected egress node followed by a IPv6-VPN table lookup



- Some of the most frequently used instructions
- For non-SRv6 devices it is normal IPv6 operation!

SRv6 Example



Role of IGPs and BGP in SRv6

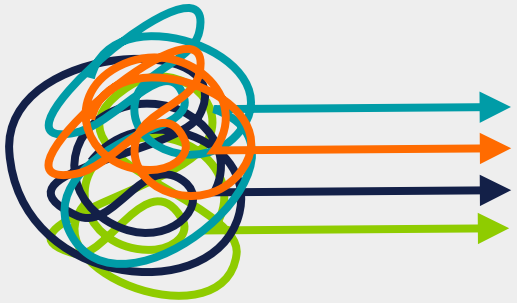
Distributing the SR information - SIDs

IS-IS extensions - RFC 9352
https://datatracker.ietf.org/doc/html/rfc9352

OSPF extensions - RFC 9513
https://datatracker.ietf.org/doc/html/rfc9513

BGP extensions - RFC 9514
https://datatracker.ietf.org/doc/html/rfc9514

Why Opt for SR?



Simplicity

Flexibility

Resiliency

Scalability

Backbone Networks Summary

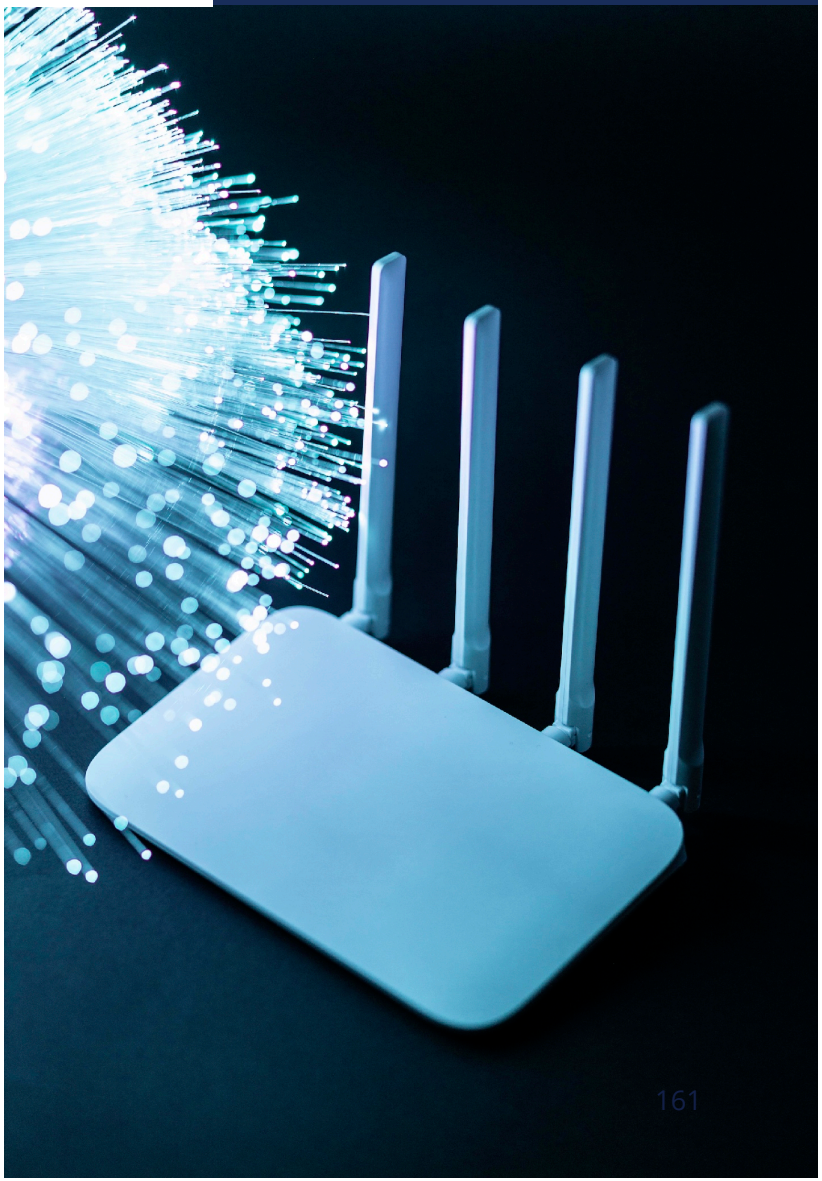
- IGP Protocols
  - OSPFv3
  - IS-IS
- BGP
- MPLS Networks and Services (VPNs)
  - 6PE/6VPE
  - LDPv6
- Segment Routing and SRv6

Questions

Access Networks

IPv6 Introduction to the Access Network

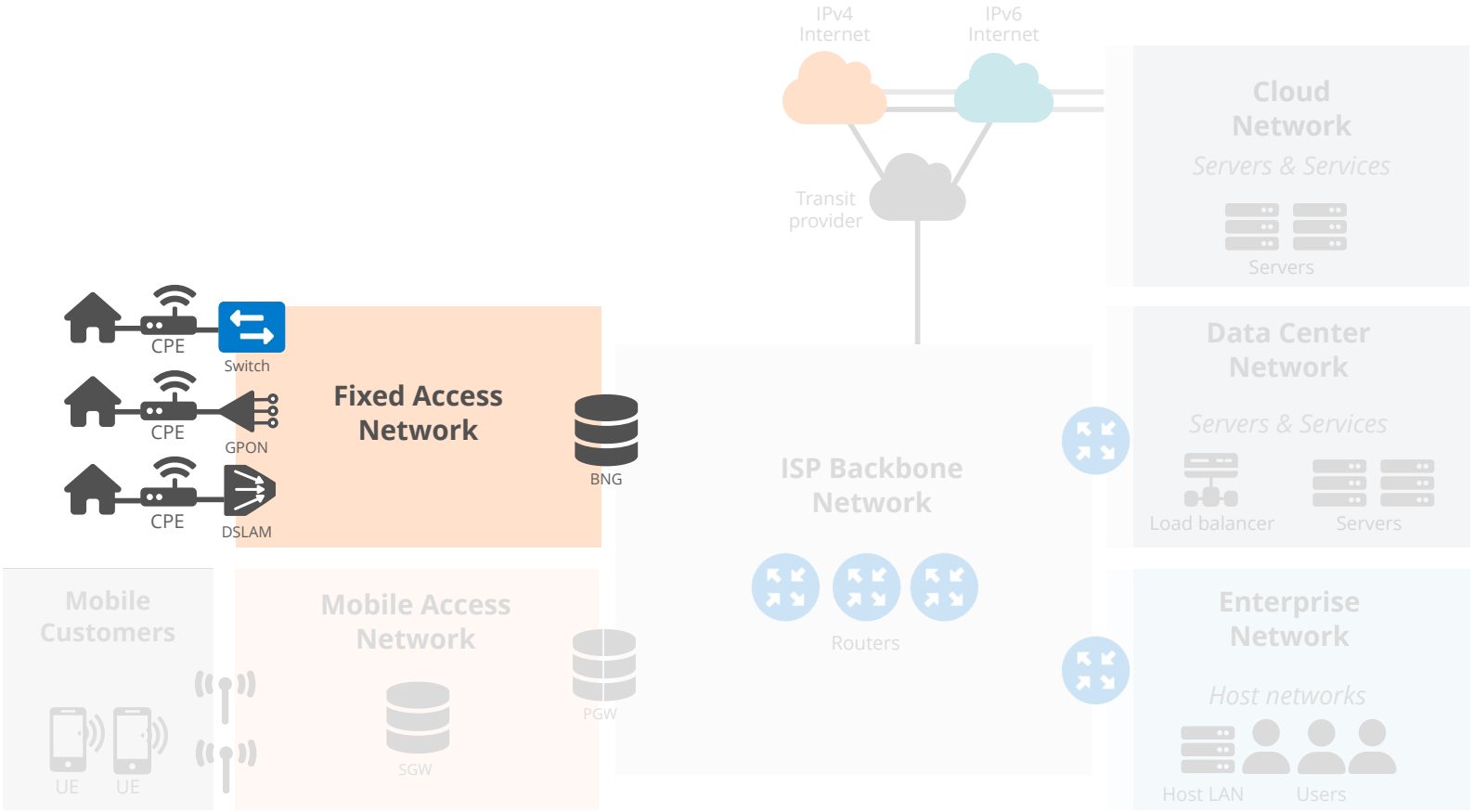
- **Internet traffic shifts to IPv6** and the status quo is no longer an option!
- Challenges for Access Networks
  - Dependency on user-equipments and CPEs
  - Country regulations (logging of users, lawful intercept, etc.)



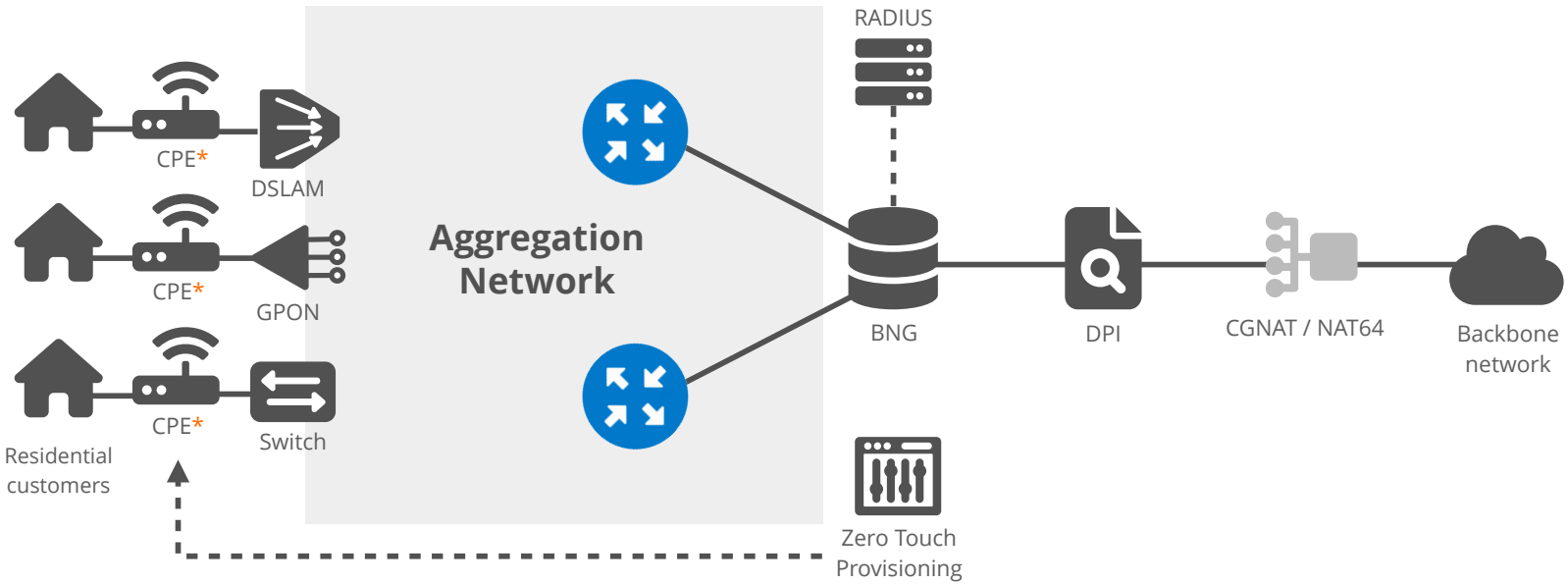
Access Networks

Fixed Access

Reference Architecture - Fixed Access Networks



Elements of a Fixed Access Network



* In the current design of the IPv4 fixed broadband access networks another layer of NAT functionality can be found on the CPEs as well.

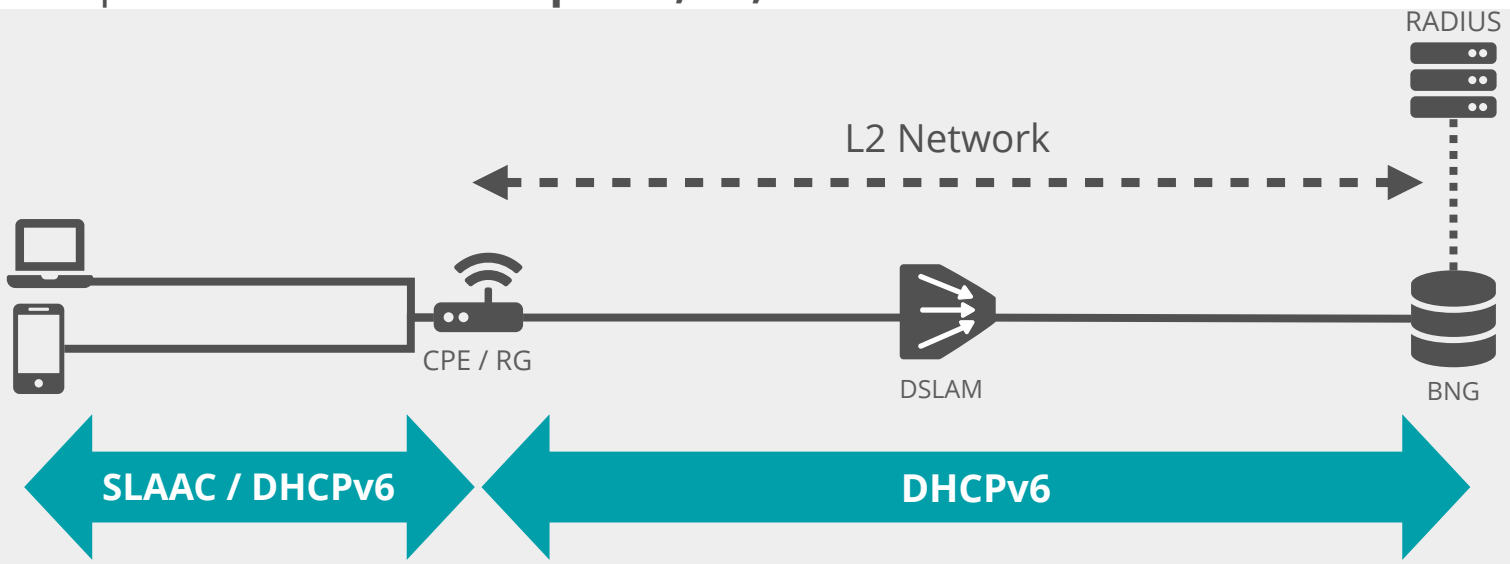
Two Connection Types

IPoE

PPPoE

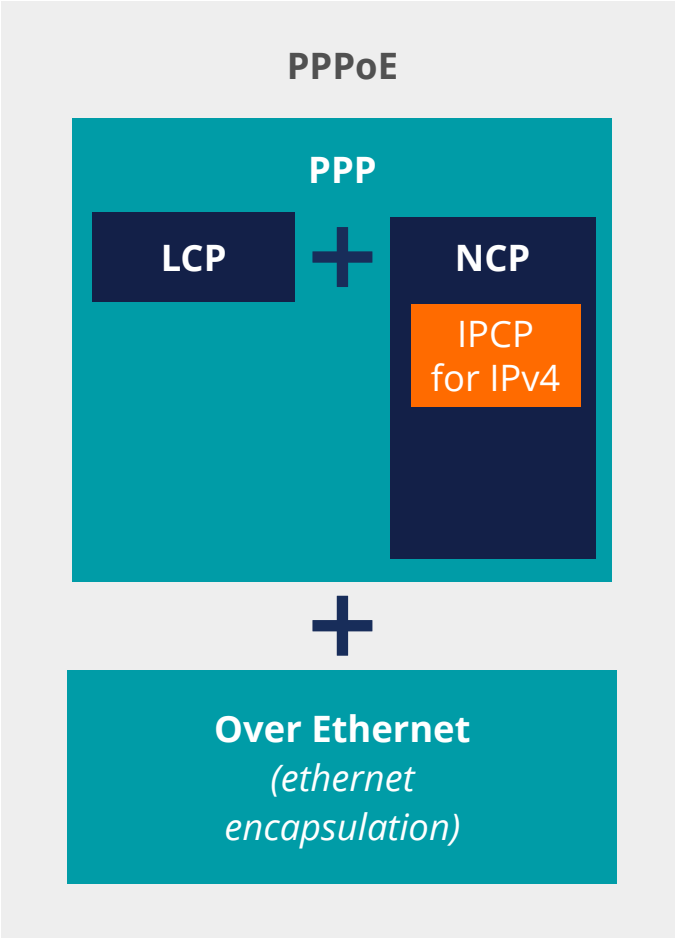
Connection Types - IPoE

- IPoE- encapsulating IP packets into Ethernet frames
- Straightforward connection
- **Uses DHCPv6 messages and options** - lack of integrated authentication and authorisation mechanism
- DHCP Opt. 82 and **DHCPv6 Opt. 37, 18, 16**



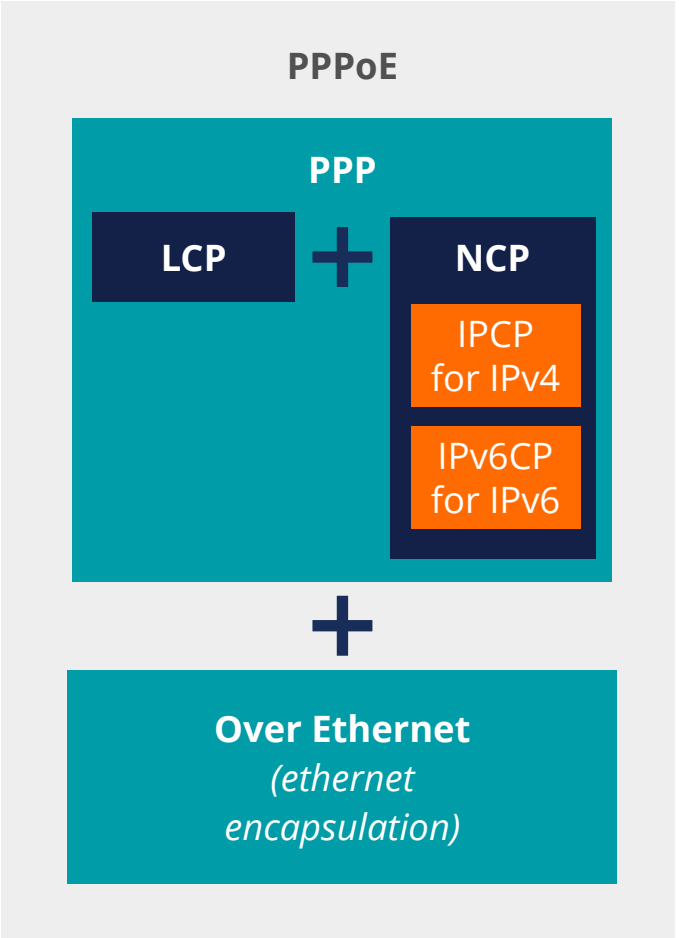
Connection Types - PPPoE

- PPP to facilitate communication between two end-points
- PPPoE - same benefits inside the ethernet encapsulation
- PPP phases - LCP and NCP (and optionally authentication in between)



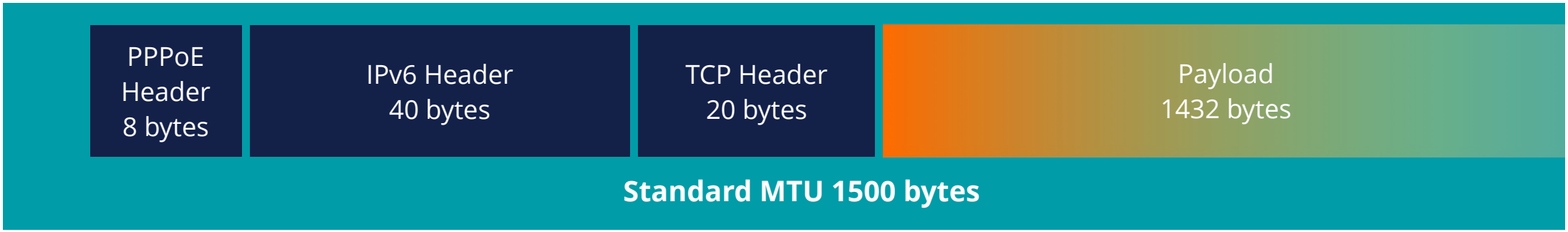
Connection Types - PPPoE

- **NCP for IPv6 = IPv6CP**
- IPCP - direct negotiation of IP addresses
- IPv6CP - other protocols (such as DHCPv6 or SLAAC) are responsible for IPv6 address assignment



PPPoE and MSS Adjustment

- Path MTU Discovery Problem - ICMPv6 filters
- TCP MSS
- 1452 bytes for IPv4
- **1432 bytes for IPv6**
- Optional MTU parameter in RA



DHCPv6 Prefix Delegation

- Addressing the hosts behind the CPE
- It is **new** and **only needed for IPv6**
- It is **stateful**

IPv4 deployments:

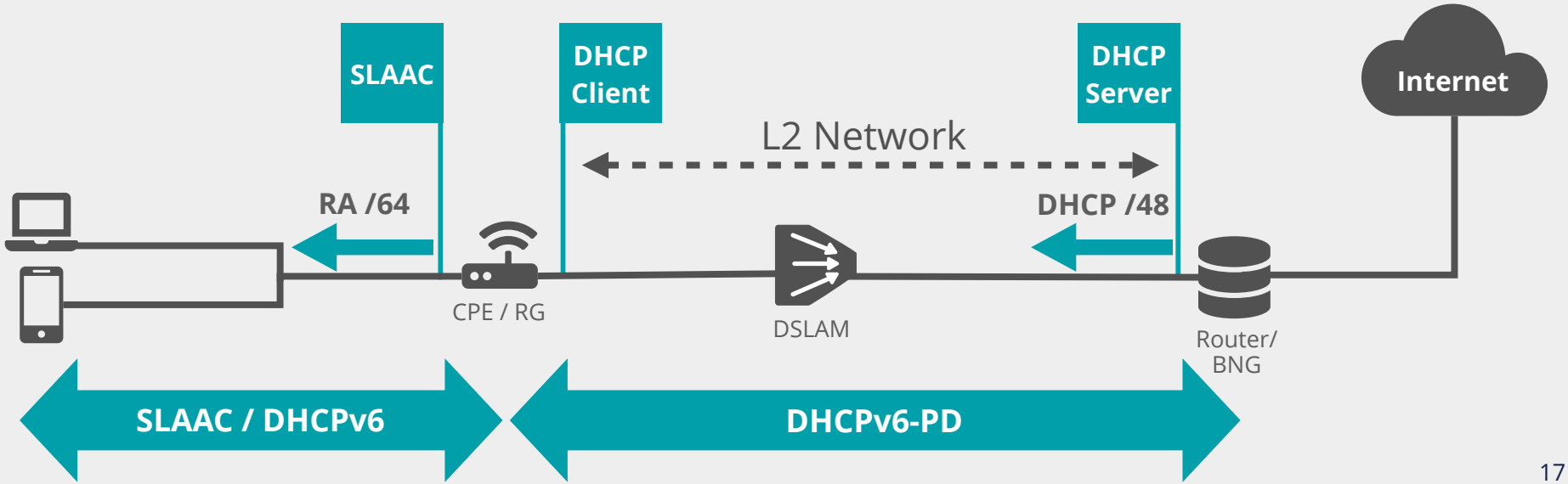
- ISP only has to deliver a **public** IPv4 address
- **NAT** is used for **translation** using RFC1918

IPv6 deployments:

- IPv6 **end-to-end** reachability:
- Home network gets its **own IPv6 prefix** (public address)
- **No NAT**

DHCPv6 Prefix Delegation

- ISP assigns a block of addresses for delegation to customers (e.g. /48, /56)
- Customer assigns /64 prefixes to LAN interfaces
- Can be used in combination with both IPoE and PPPoE.



DHCPv6-PD Question

Why do we need **DHCP-PD** in IPv6? Because we need…

a. a mechanism for the automation of assigning GUAs to the devices on the subscriber LAN
b. a mechanism for translation of the address used on the subscriber LAN
c. to use NDP over Internet for the devices behind the CPE
d. a low latency mechanism for IPv6 subscribers

DHCPv6-PD Answer

Why do we need **DHCP-PD** in IPv6? Because we need...

a. a mechanism for the automation of assigning GUAs to the devices on the subscriber LAN

b. a mechanism for translation of the address used on the subscriber LAN

c. to use NDP over Internet for the devices behind the CPE

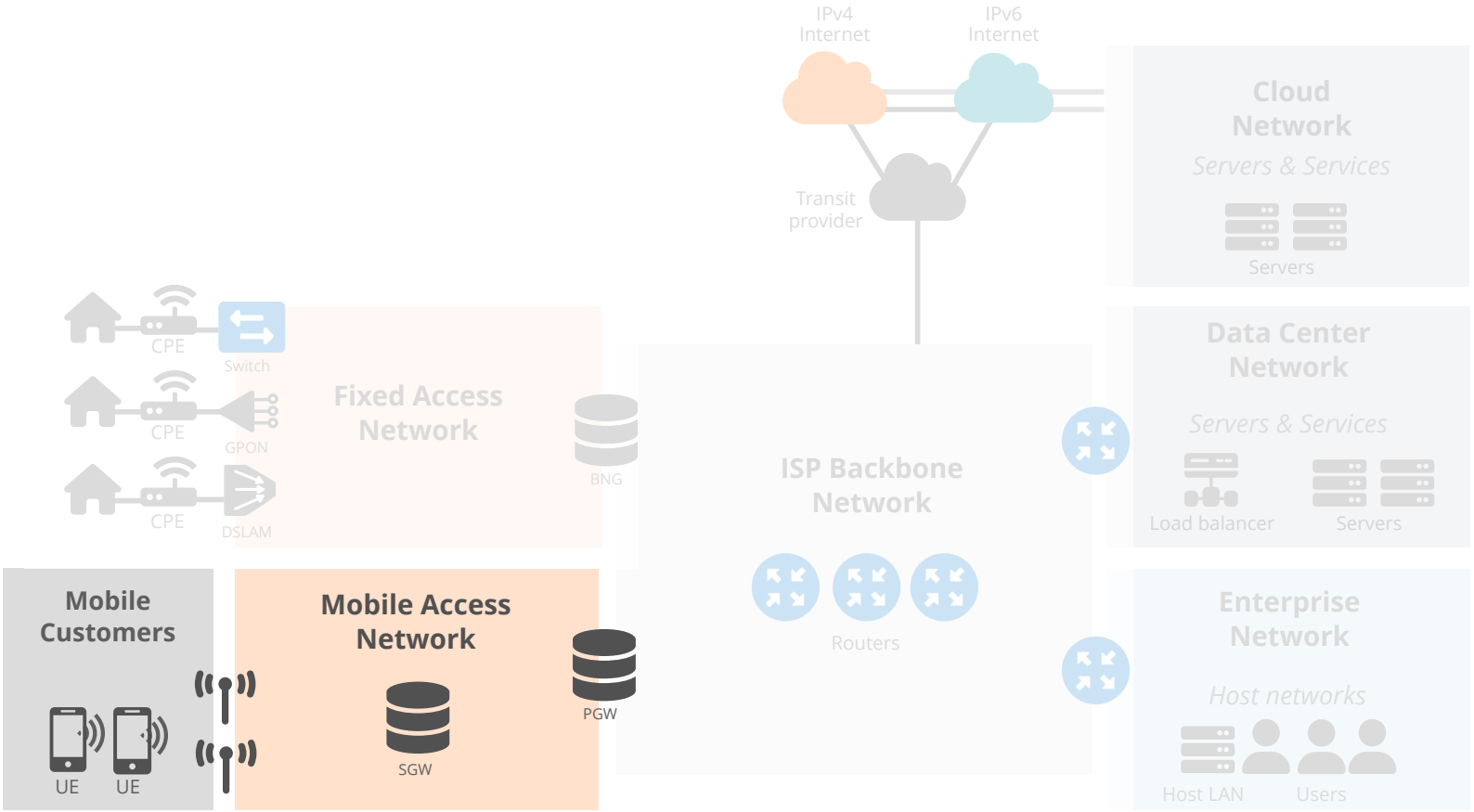
d. a low latency mechanism for IPv6 subscribers

Questions

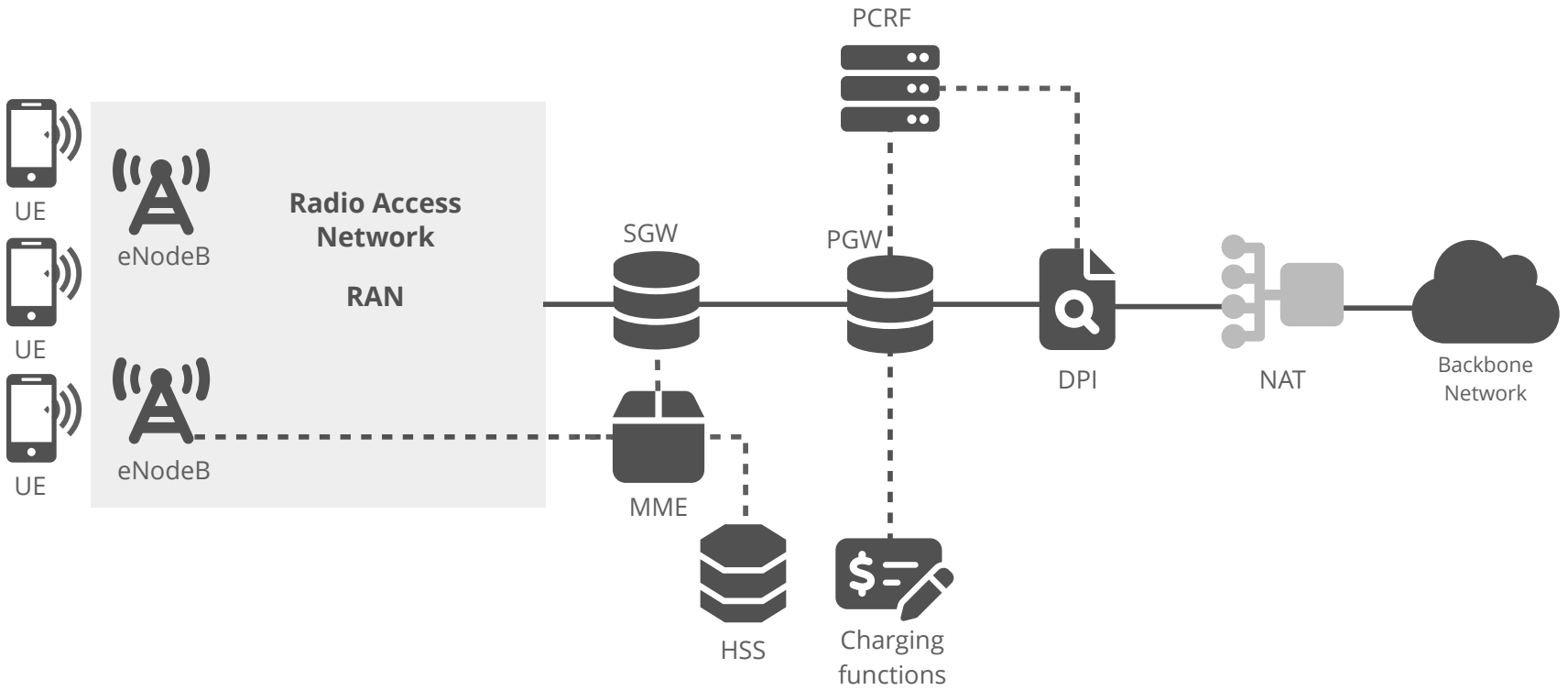
Access Networks

Mobile Access

Reference Architecture - Mobile Access Networks



Elements of a 4G Mobile Access Network



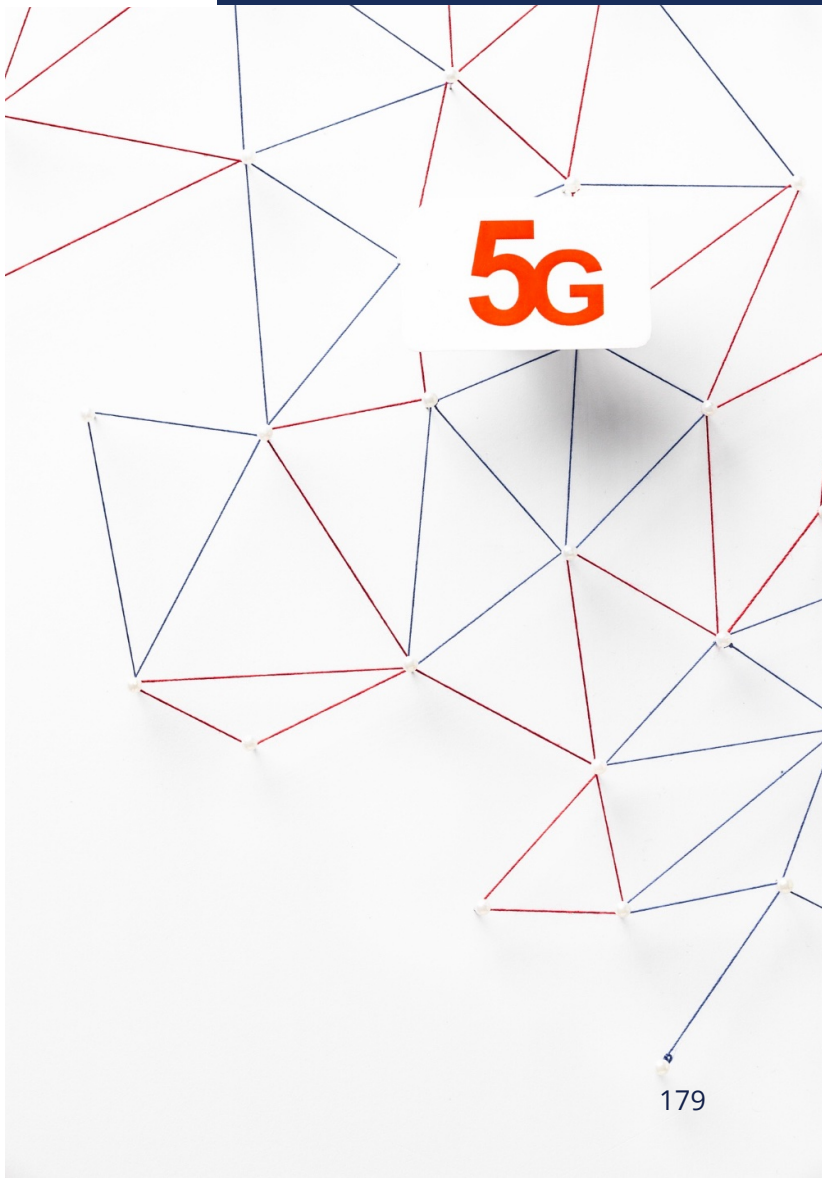
User Equipments

- 3GPP allows a single prefix assignment over the mobile link. - (3GPP TS 23.401 V18.5.0 - 2024-03, section 5.3.1.1 General)
  - Prefix delegation problem
  - Workaround: OPTION_PD_EXCLUDE in DHCPv6 (RFC 6603)

- No 464XLAT support on the iPhone (except tethering)
- Coordination with Apple for IPv6 integration within your mobile network

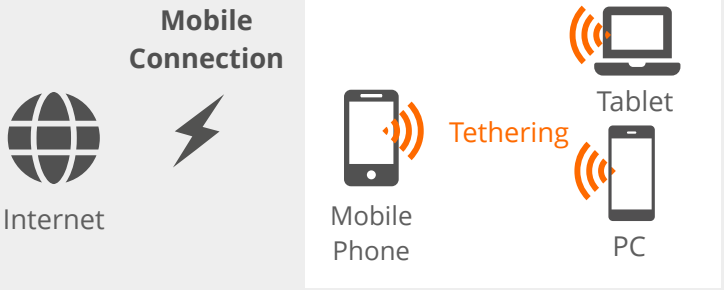
5G Networks

- **IPv6 is a key enabler for 5G** use cases as they bring massive amount of connections with Massive Machine Type Communication (**mMTC)** and low latency with Ultra-Reliable Low Latency Communications **(URLLC)**
- 5G is helps industries to achieve **IoT vision** (with IPv6)
- Dual-Stack should still be supported - due to the mixed nature of current networks



Tethering and IPv6

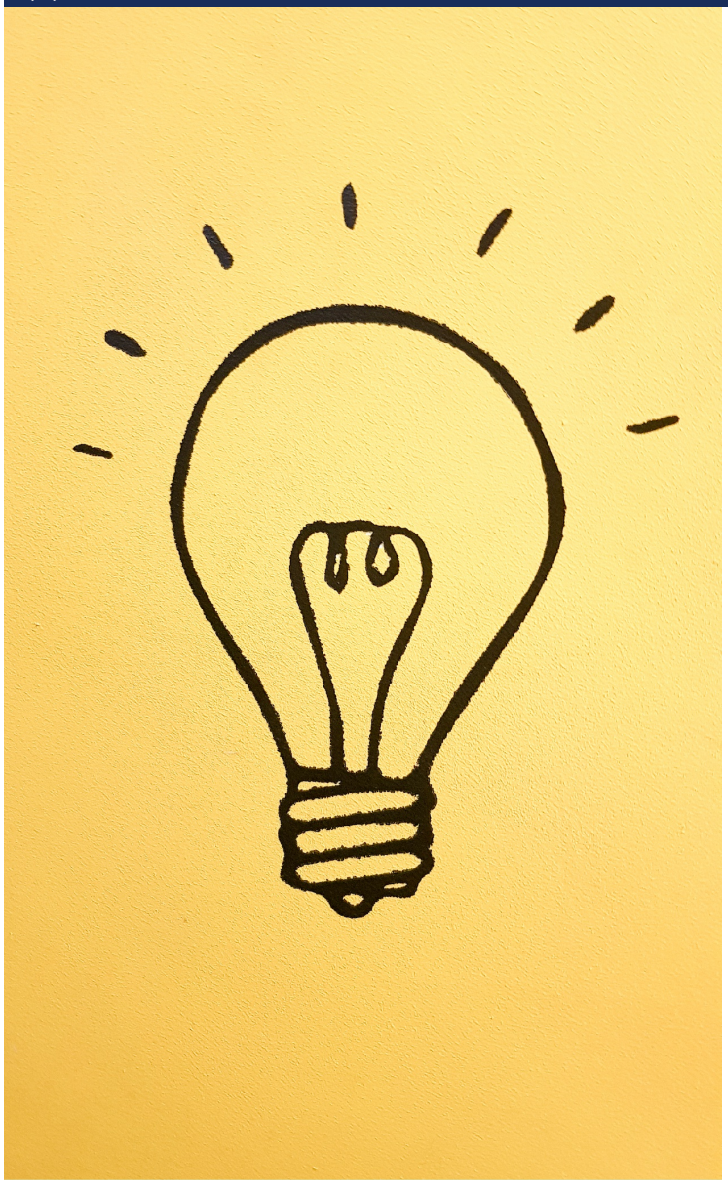
- A /64 prefix is received through an router advertisement (RA) to the phone
- An /128 from that /64 is used for the own WAN
- The same /64 is used for the LAN (and for tethering)
  - Tethering is done through RA
  - DAD is used to avoid duplicate addresses
- If the UE supports CLAT, using IPv4 addresses on tethered devices is also possible



Roaming Challenges

- Home and visited networks and the equipment should be **tested** for various types of mobile phones and scenarios

Roaming problems are extensively discussed in **informational RFC 7445:**
https://tools.ietf.org/html/rfc7445



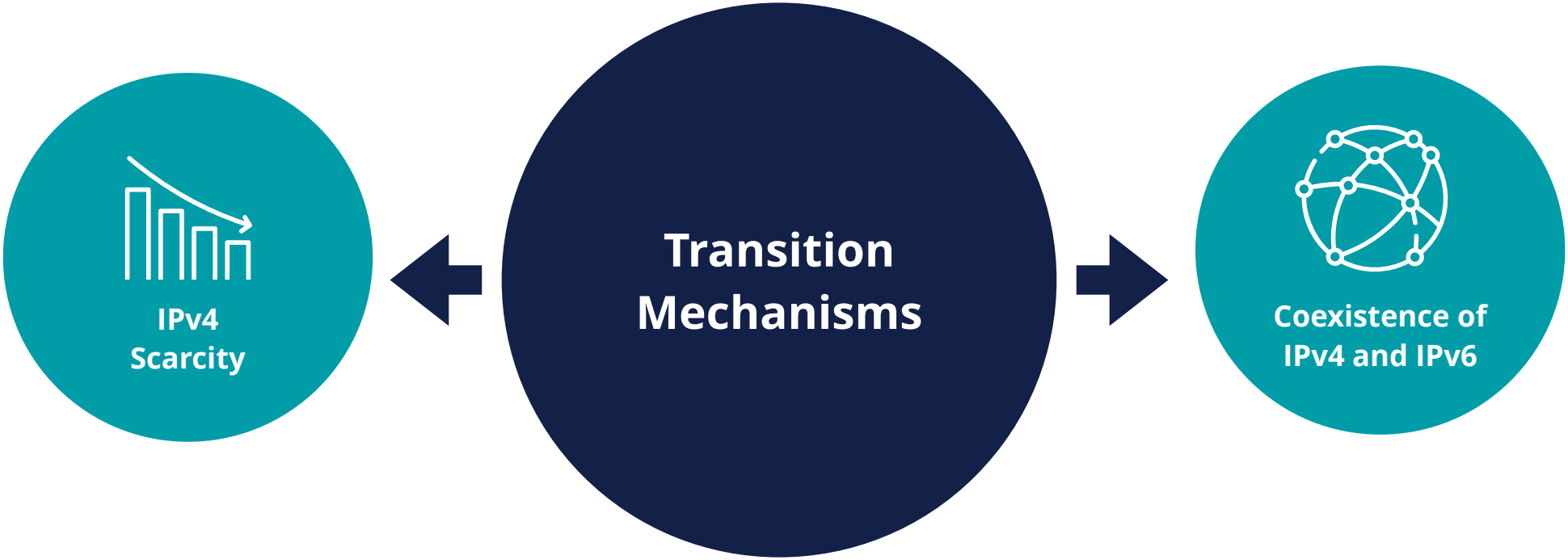
More Tips on Access Networks

- Backup IPv6 pools
- Static IPv6 prefix delegation - in fixed access networks
- Provisioning systems
- Alarm and monitoring systems
- Call-center tools and staff
- Applications and services in the ISP network
  - TV, Video on Demand or Instant Messaging services

Questions

Transition Mechanisms

Transition Mechanisms Solve Two Problems



Three Different Types of Transition

Tunnelling

IPv6 packets within IPv4

IPv4 packets within IPv6

v6-in-v4	v4-in-v6
6RD	DS-LITE
	LW4o6
	MAP-E

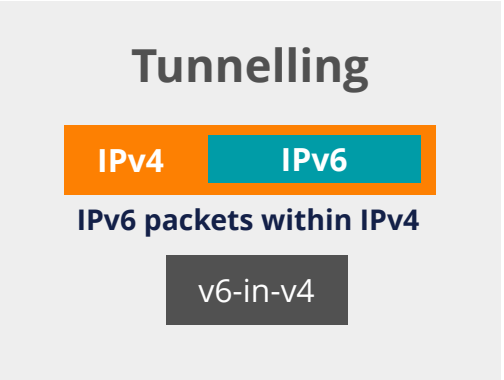
Translation

v6-to-v4	v4-to-v6
MAP-T	NOT USED
NAT64	
464XLAT	

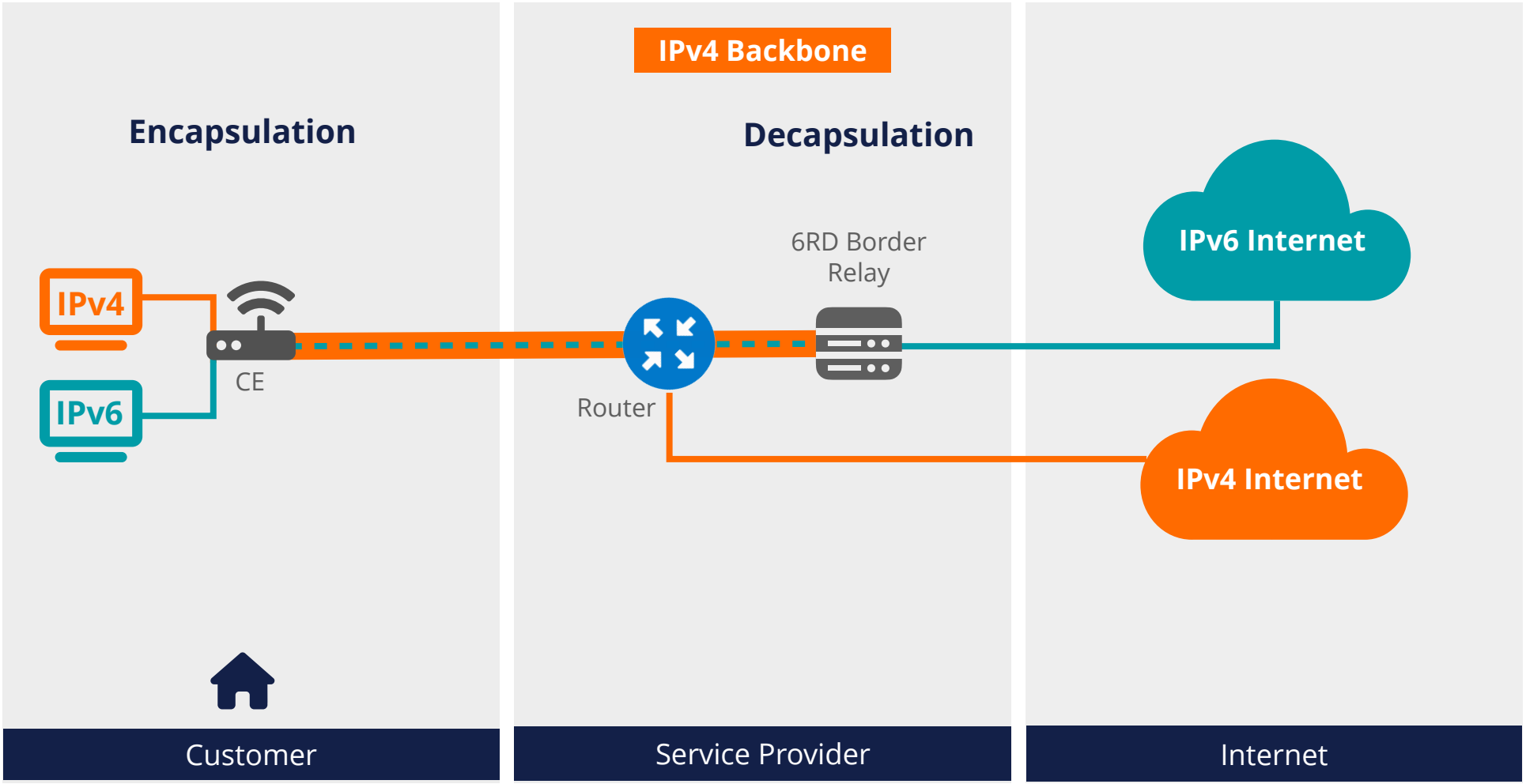
Dual-Stack

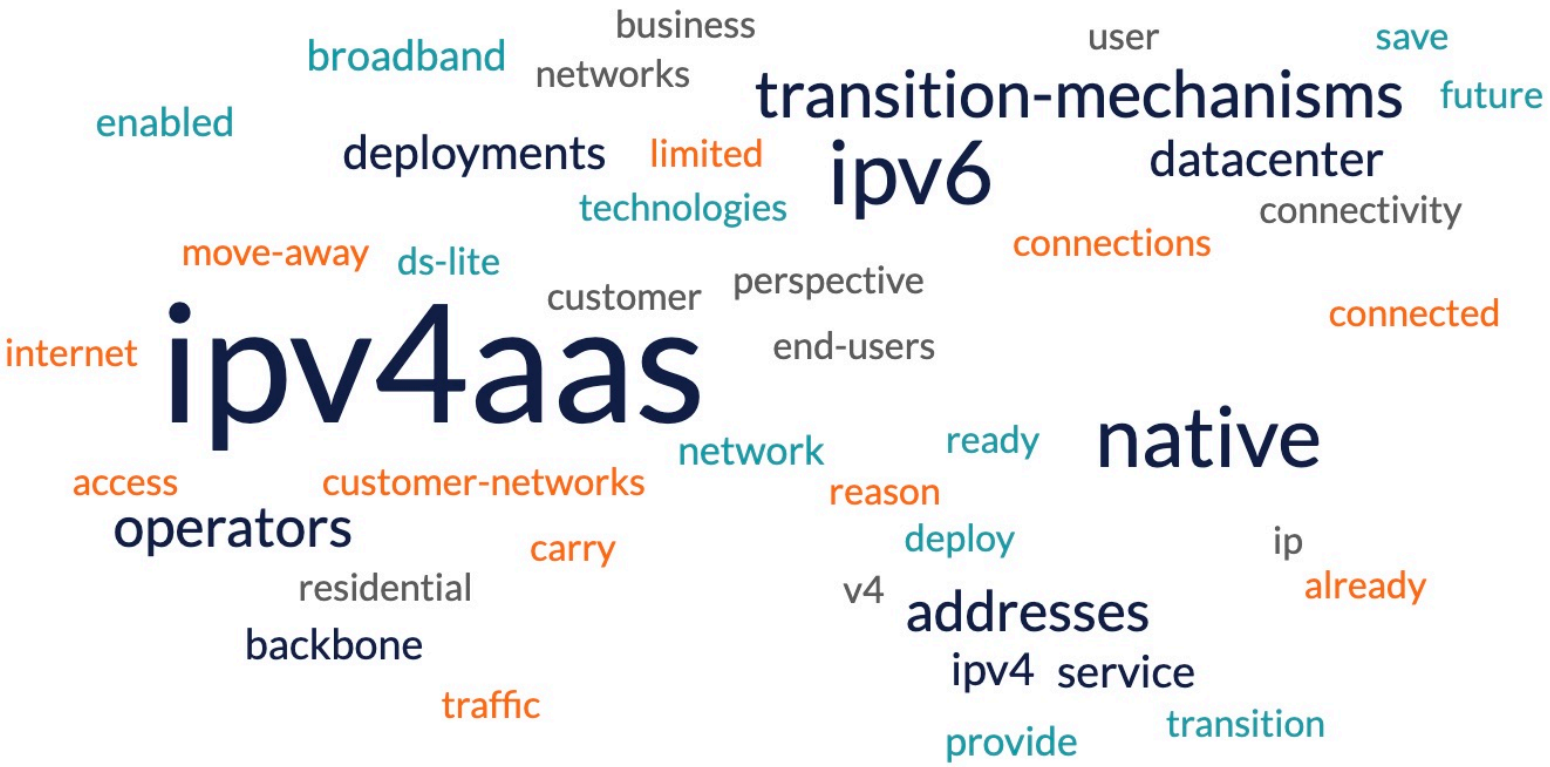
6RD

- Tunnelling mechanism for IPv6 over service providers' IPv4 infrastructure and IP resources
- Idea explained in RFC 5569 - Standardised in RFC 5969
- Algorithmic mapping between the IPv6 and IPv4 addresses
- Provides **stateless operation** and anycast resiliency for BRs
- The operator has full control over the relay
- 6RD prefix may be sent to the customer equipment (CE) by DHCP v4 options
- CPE should also support 6RD



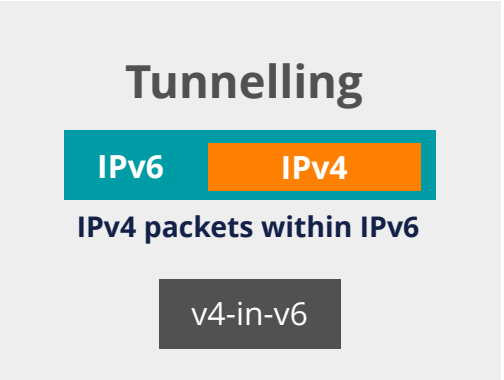
6RD


IPv4 Backbone
Encapsulation
Decapsulation
6RD Border Relay
IPv6 Internet
IPv4
IPv6
CE
Router
IPv4 Internet
Customer
Service Provider
Internet

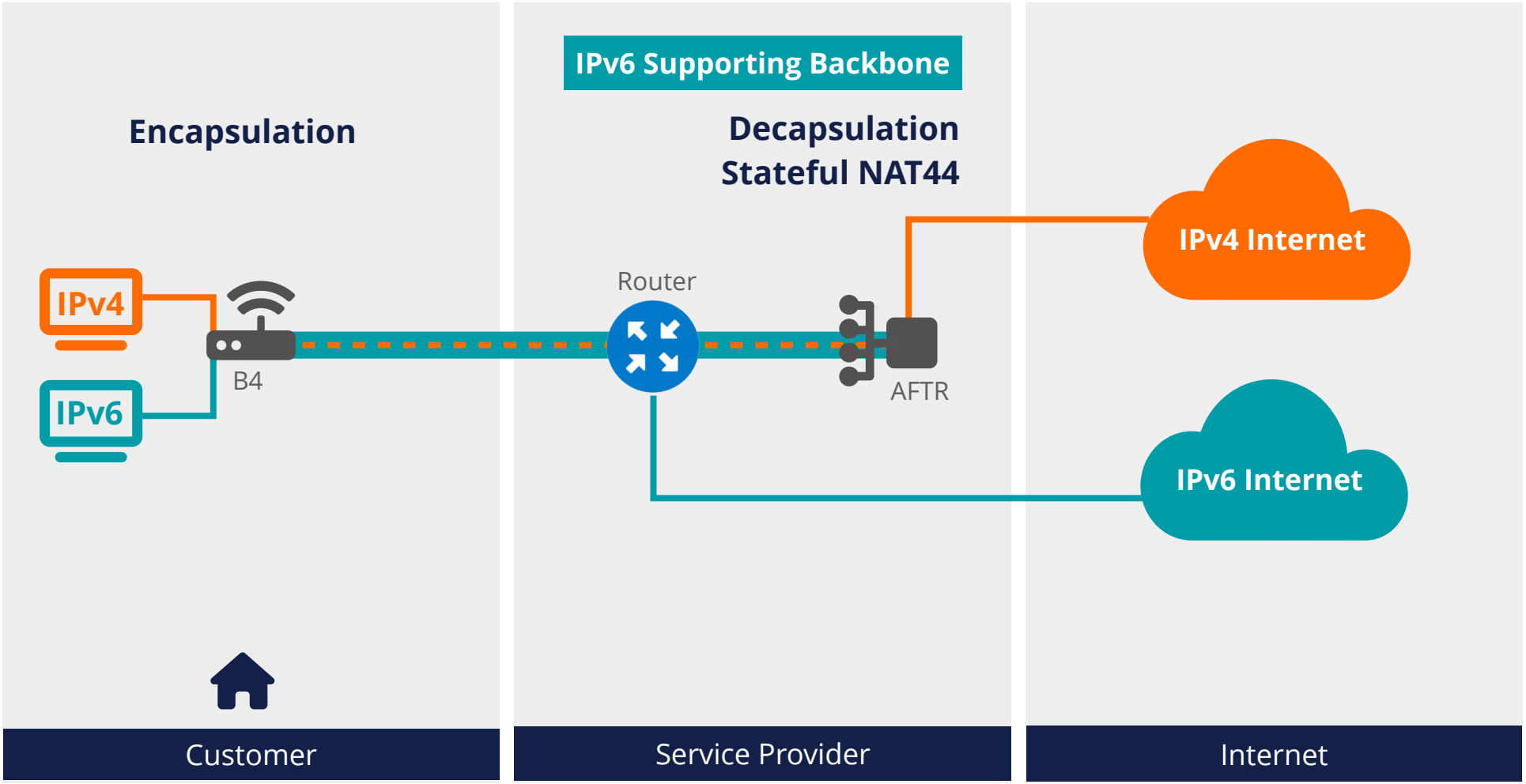

business
broadband
networks
user
save
transition-mechanisms
future
enabled
deployments
limited
ipv6
datacenter
technologies
connectivity
move-away
ds-lite
connections
customer
perspective
connected
internet
ipv4aas
end-users
native
network
ready
access
customer-networks
reason
operators
deploy
ip
carry
already
residential
v4
addresses
backbone
ipv4
service
traffic
transition
provide

DS-LITE

- Tunnelling IPv4 over IPv6
- Customer networks use private IPv4 addresses without NAT on CPE
- **NAT is centrally located** at the provider
- **Client's IPv6 address is used to maintain state and to keep clients apart**
  - Allows for duplicate IPv4 ranges
- Basic Bridging BroadBand (B4) and Address Family Transition Router (AFTR)
- CPE should support DS-LITE

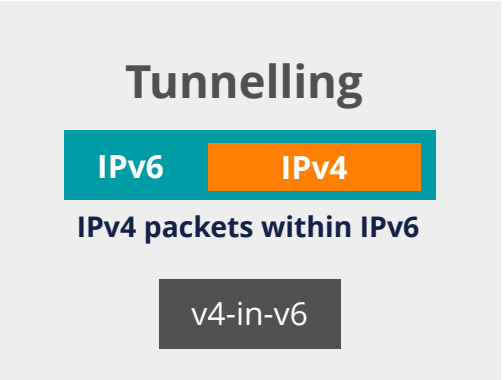


DS-LITE

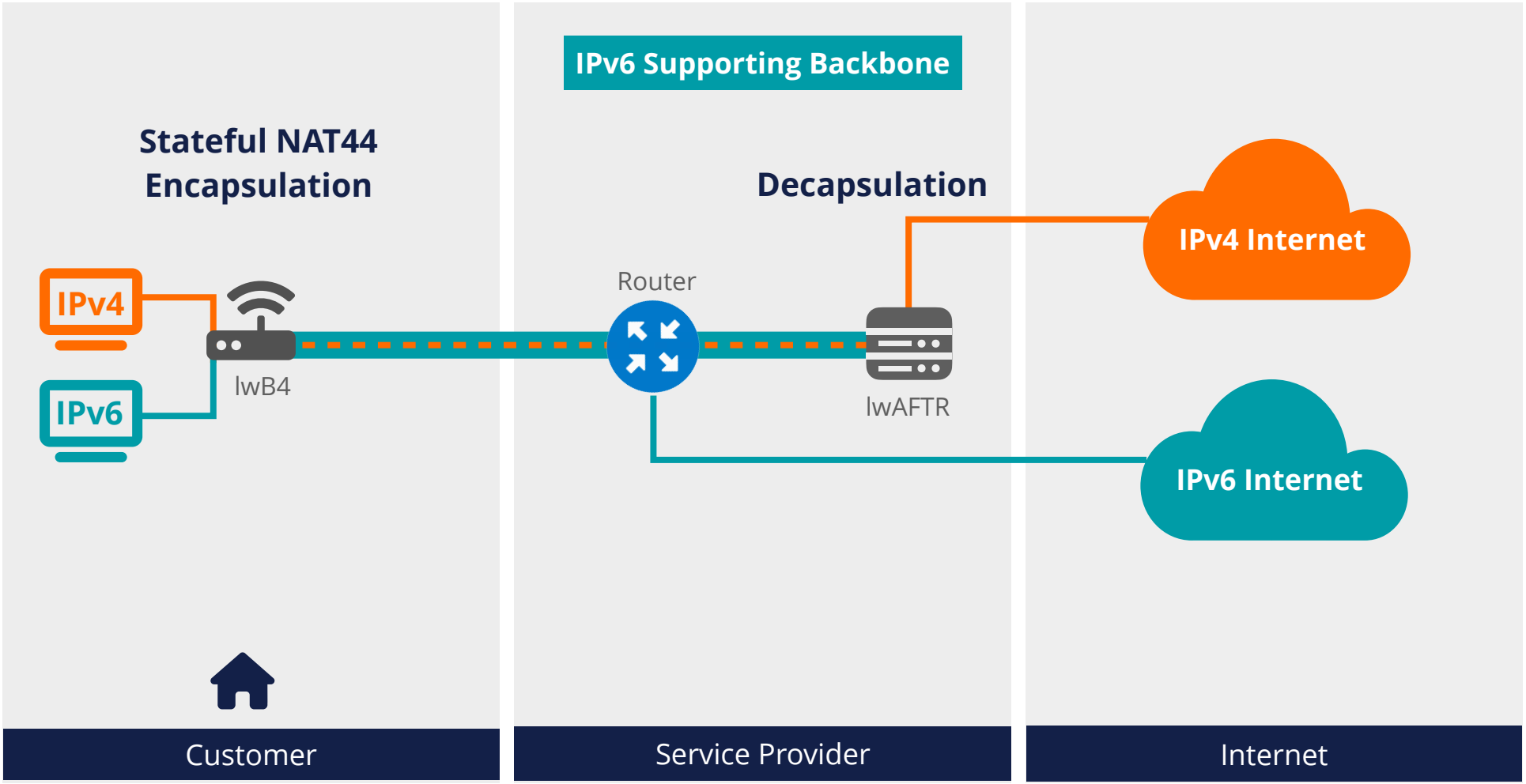

Encapsulation
IPv6 Supporting Backbone
Decapsulation
Stateful NAT44
IPv4
IPv6
B4
Router
AFTR
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

Lightweight 4 over 6

- Tunnelling IPv4 over IPv6
- Extension to DS-LITE
- Same tunnelling mechanism as DS-LITE
- **Moves NAPT function back to customer equipment**
  - In another name; lightweight B4 (lwB4)
- **Removes the need for central NAT**
  - Reduces the amount of states on lwAFTR
  - Per-subscriber state is still held in lwAFTR
- **Port-restricted IPv4 addresses allocated to the CPEs**
  - DHCP, TR-69 or port control protocol (PCP) can be used

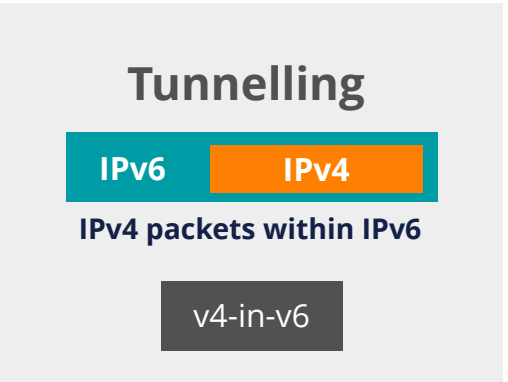


Lightweight 4 over 6

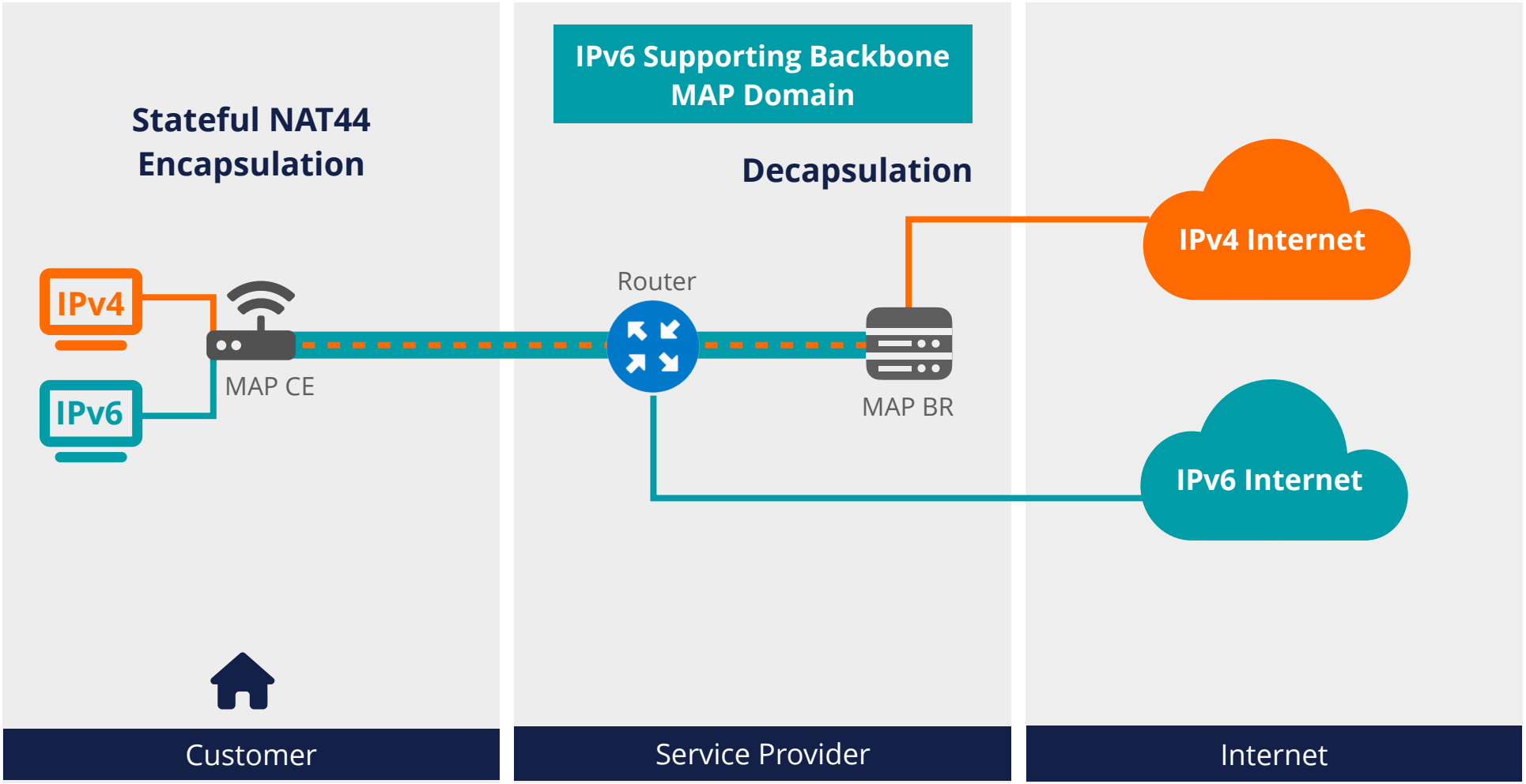


MAP-E

- Tunnelling IPv4 over IPv6
- **M**apping of **A**ddress and **P**ort w/ **Encapsulation** - RFC 7597
- Stateless Border Relay (BR) & Stateful CE Operation
- **Shared IPv4 addresses & Different ports**
- CEs are assigned a Port Set Identifier (PSID)
- “DHCP auto-configuration options for MAP-E” allows auto-configuration - RFC 7598
- **Stateless NAT on the central devices allows asymmetrical traffic and easy scaling**

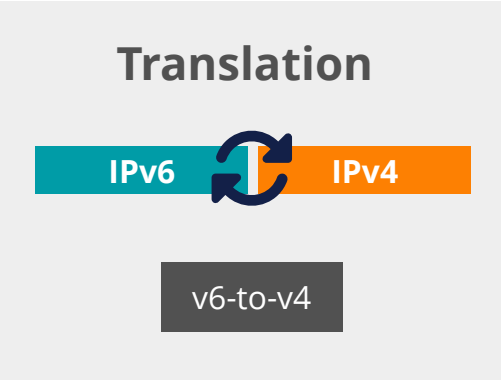


MAP-E

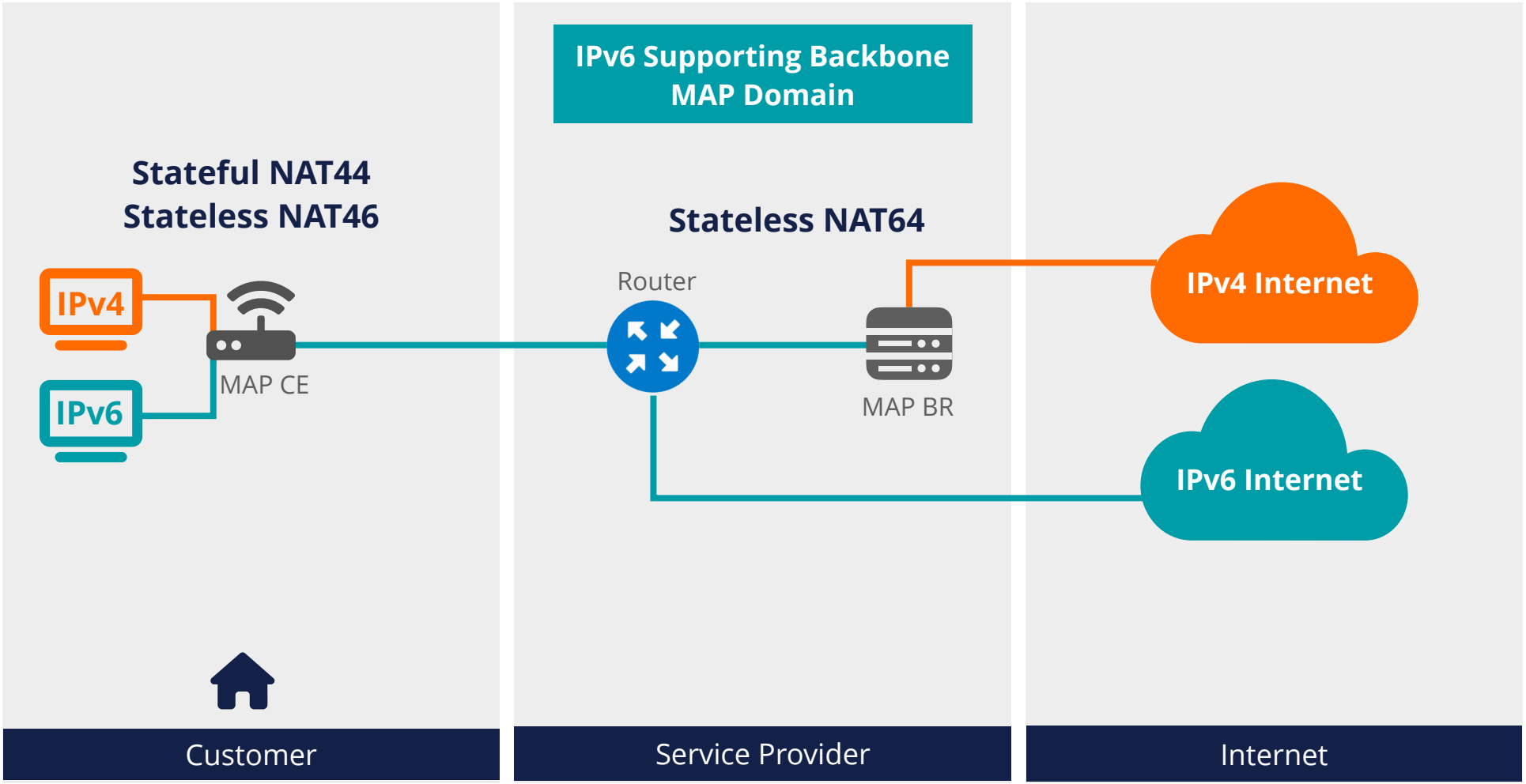

Stateful NAT44
Encapsulation
IPv6 Supporting Backbone
MAP Domain
Decapsulation
IPv4
IPv6
MAP CE
Router
MAP BR
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

MAP-T

- Translation mechanism for connecting IPv4 islands over service providers' IPv6 infrastructure
- **M**apping of **A**ddress and **P**ort using **T**ranslation - RFC 7599
- Stateless BR and Stateful CE Operation
- **Shared IPv4 addresses and Different ports**
- Two key differences with MAP-E:
  - Translation (instead of Tunnelling)
  - Special BR address in MAP-E **vs.** routed IPv6 prefix in MAP-T
- **MTU is a less concern as there is no extra header**

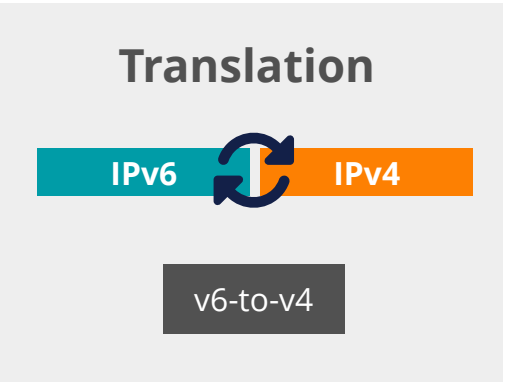


MAP-T

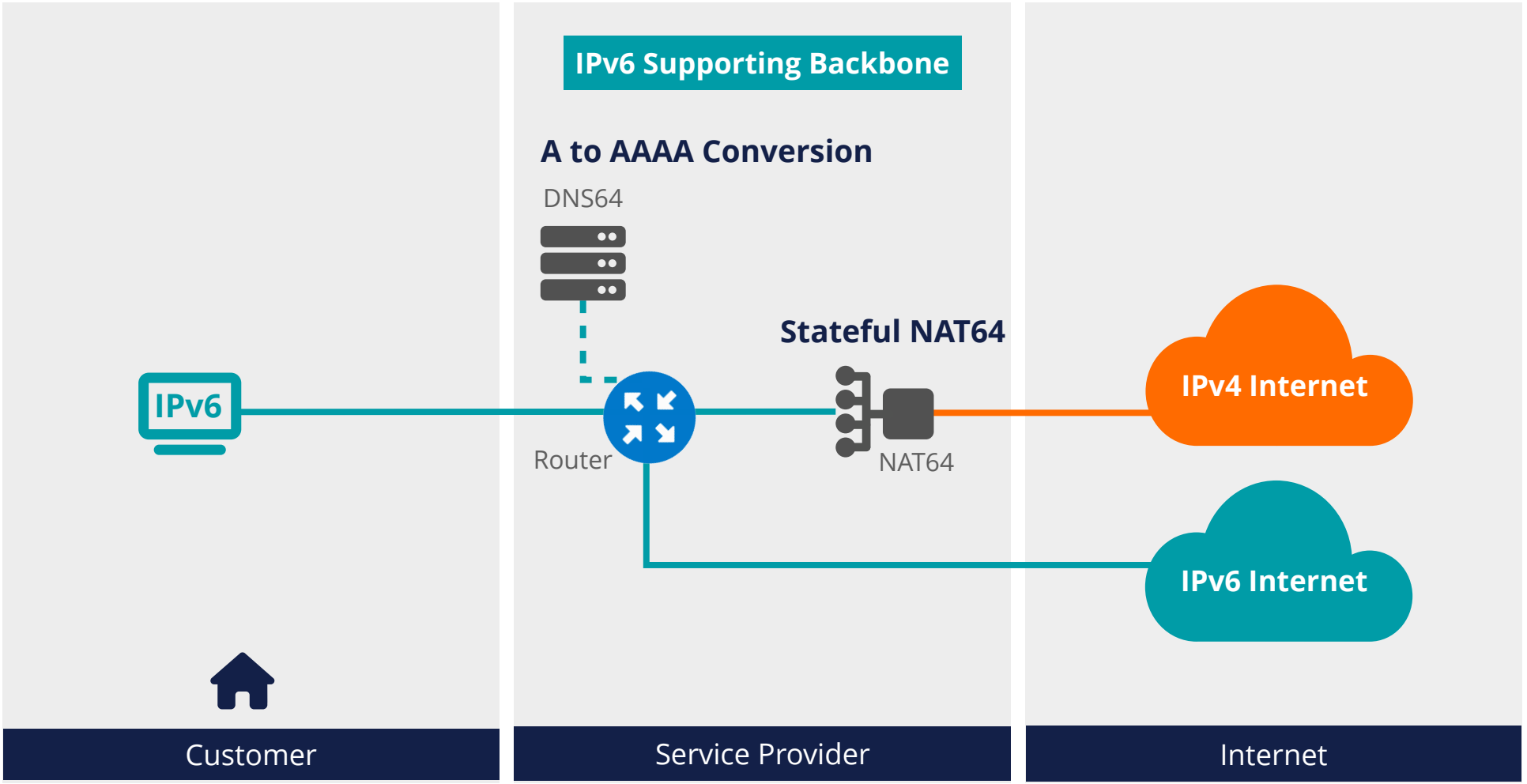

IPv6 Supporting Backbone
MAP Domain
Stateful NAT44
Stateless NAT46
Stateless NAT64
IPv4
IPv6
MAP CE
Router
MAP BR
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

NAT64 / DNS64

- Translation transition mechanism from IPv6 to IPv4
- **IPv6-only hosts can access IPv4 services/internet**
- Works in conjunction with **DNS64**
  - Capture responses and replace A with AAAA
  - Response is crafted based on target IPv4 address
- NAT64 box can be reached with **well known prefix** or **network specific prefix**
- IPv4 address sharing is possible



NAT64 / DNS64

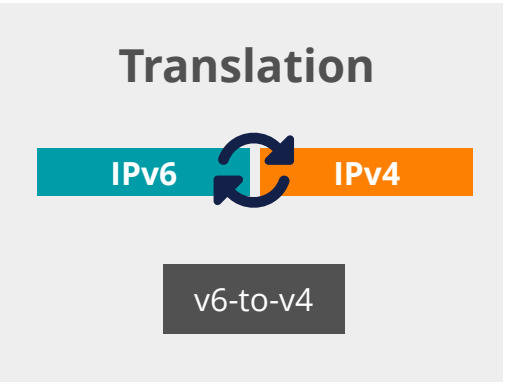

IPv6 Supporting Backbone
A to AAAA Conversion
DNS64
Stateful NAT64
IPv6
Router
NAT64
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

Challenges with NAT64

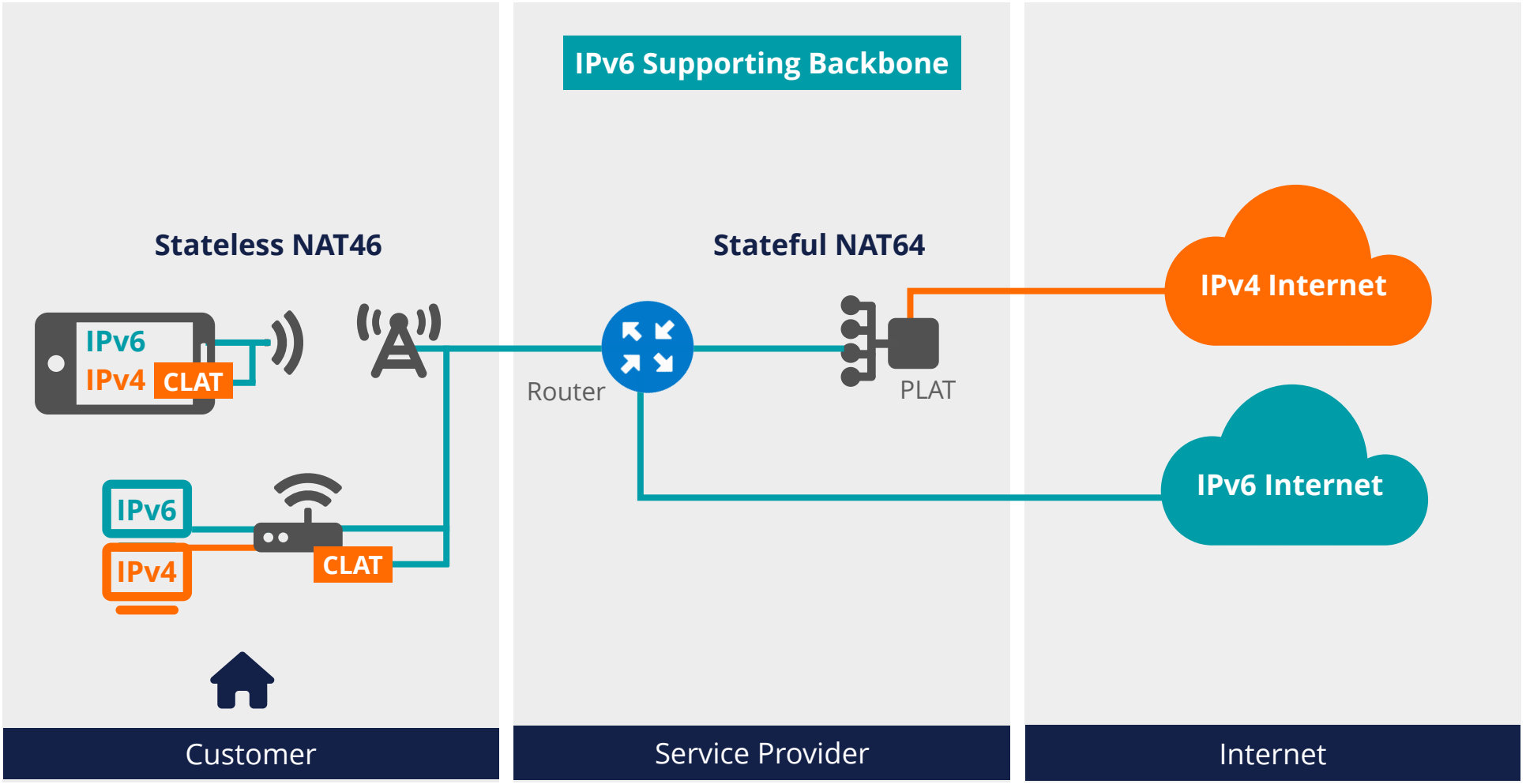
- DNSSEC
- IPv4 Literals
- Broken IPv6 Servers
- IPv4-only Apps

464XLAT

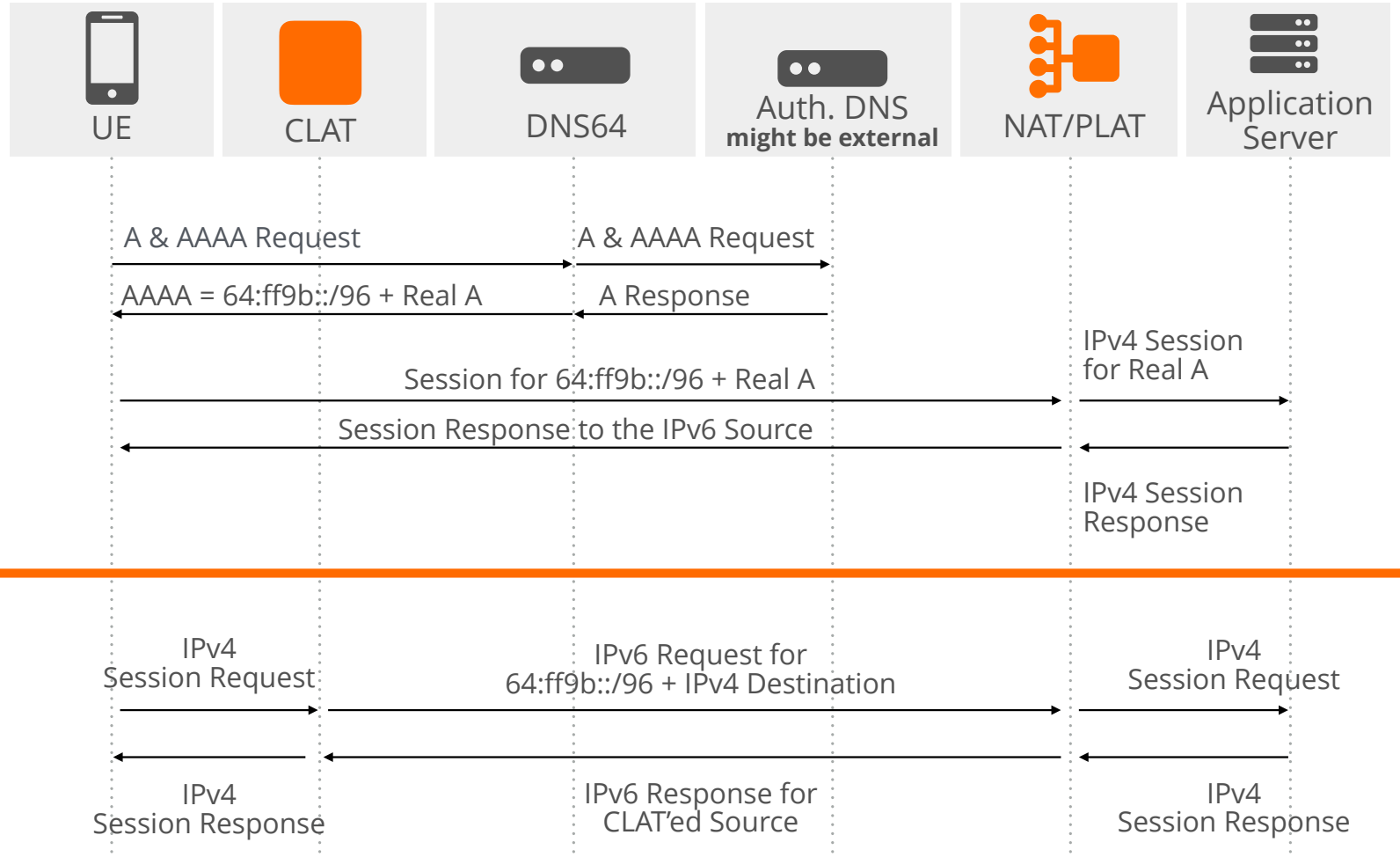
- Extension to NAT64 to access IPv4-only applications (legacy applications)
- Requires **CLAT function on the client**
- NAT46 - **CLAT** creates a virtual IPv4 interface inside the client and translates received IPv4 packets to IPv6
- NAT64 - **PLAT** inside the provider network applies translation from IPv6 to IPv4



464XLAT

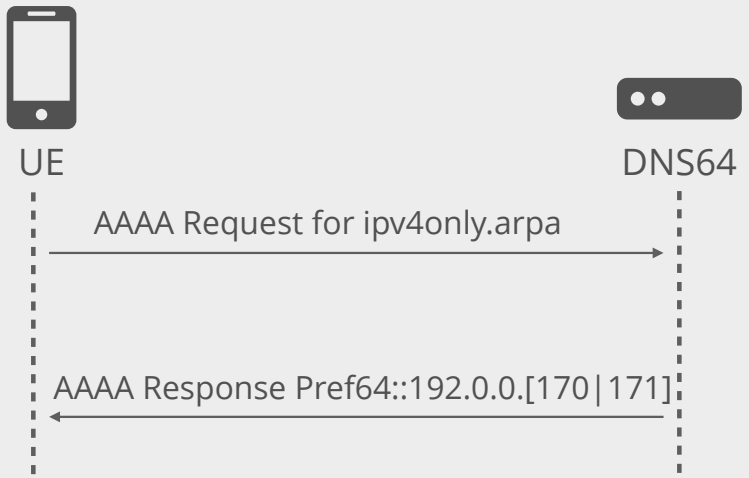

IPv6 Supporting Backbone
Stateless NAT46
Stateful NAT64
IPv6
IPv4
CLAT
IPv6
IPv4
CLAT
Router
PLAT
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

NAT64 vs. 464XLAT



Discovering the PLAT prefix

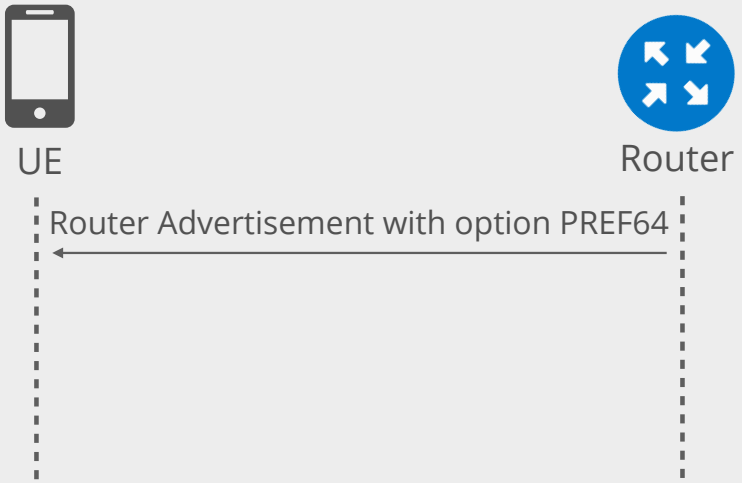
RFC 7050

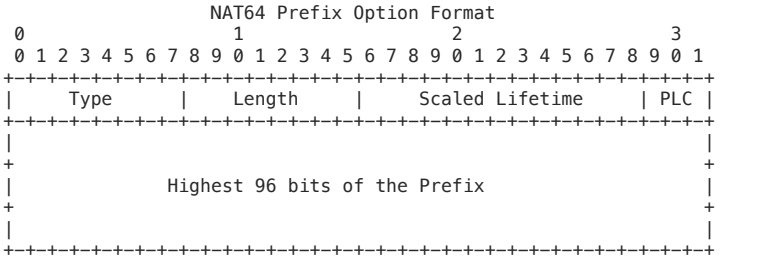



```
; <<>> DiG 9.10.6 <<>>
ipv4only.arpa AAAA @dns64.dns.google
;; QUESTION SECTION:
;ipv4only.arpa.       IN AAAA

;; ANSWER SECTION:
ipv4only.arpa.     21600 IN AAAA  64:ff9b::c000:aa
ipv4only.arpa.     21600 IN AAAA  64:ff9b::c000:ab
```

RFC 8781



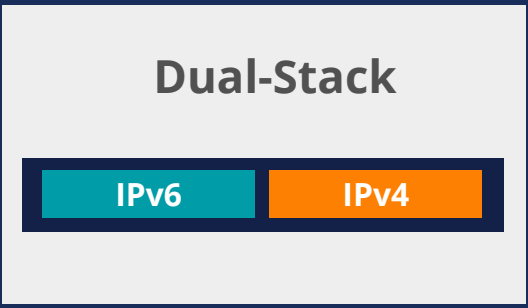


Dual-Stack

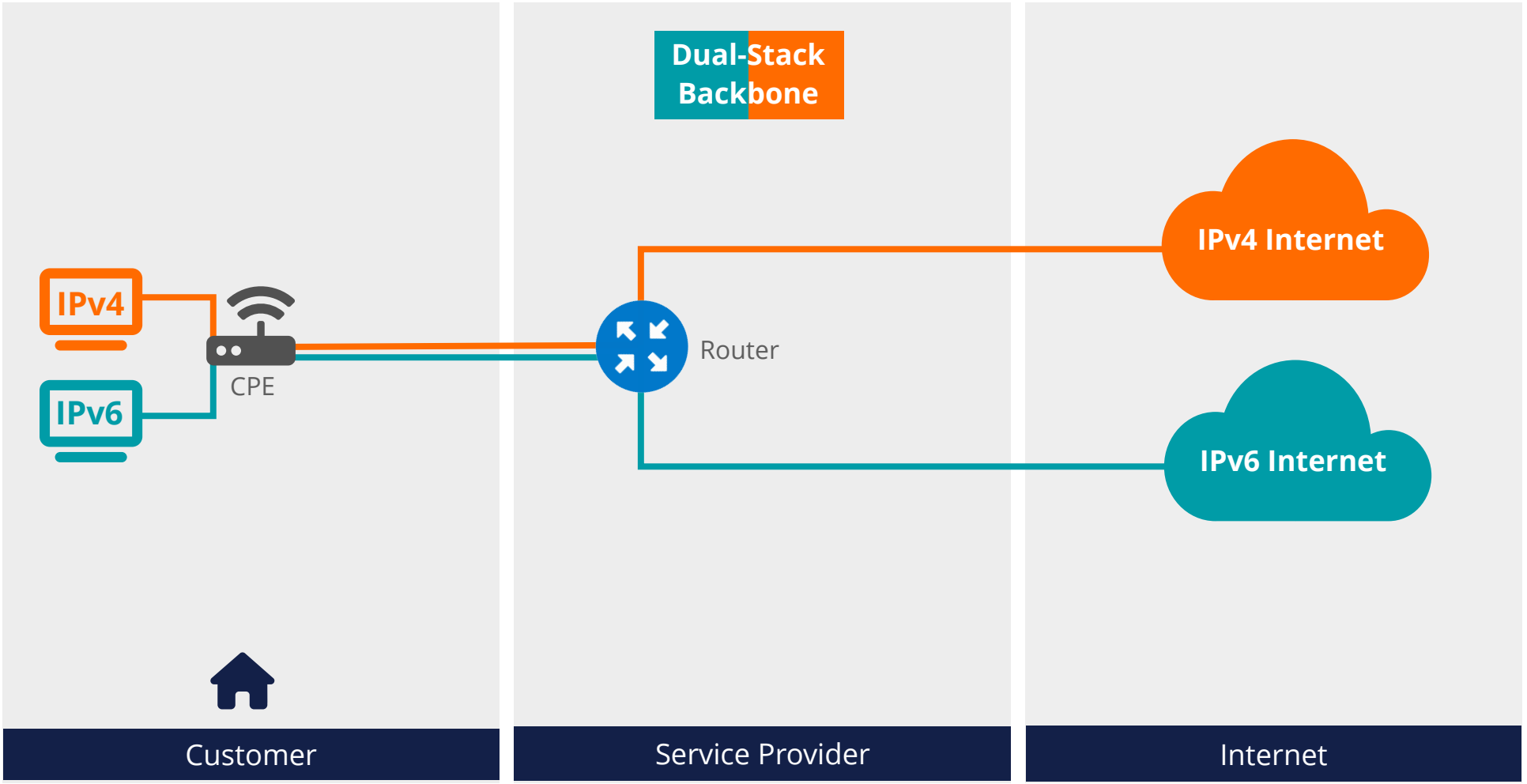
- **Native communication** on both protocols
- Relatively **easy to implement**
- **Hard to maintain** and has some challenges;
  - Increase complexity in the network (double firewall rules, routing tables, routing protocols)
  - Does not solve the IPv4 scarcity problem
  - Introduces a larger attack surface
  - Needs additional effort and expertise in the operation teams

"We are moving to IPv6-only, because we know that running a dual-stack network makes it more complex including troubleshooting time, security and QoS policies"

Veronika McKillop – Network Architect, Microsoft CSEO



Dual-Stack


Dual-Stack Backbone
IPv4
IPv6
CPE
Router
IPv4 Internet
IPv6 Internet
Customer
Service Provider
Internet

Transition Mechanisms Question

Which match is **NOT** correct?

a. 6RD; Tunnelling - v6-in-v4
b. NAT64; Translation - v6-to-v4
c. DS-LITE; Tunnelling - v4-in-v6
d. MAP-E; Translation - v4-to-v6

Transition Mechanisms Answer

Which match is **NOT** correct?

a. 6RD: Tunnelling - v6-in-v4
b. NAT64: Translation - v6-to-v4
c. DS-LITE: Tunnelling - v4-in-v6
✓ MAP-E: Translation - v4-to-v6

What to Compare? How to Choose?

- Device support
- Backbone network type - IPv6-Only, IPv4-only, Dual-stack
- Scalability
- Traffic flow efficiency - overhead of packets
- Operational complexity
- Logging regulations/needs
- Is it a “long-term” solution?
- IPv4 address sharing efficiency

Comparison of Different IPv6 Transition Mechanisms

	Dual-Stack	6RD	DS-LITE	LW4o6	MAP-E	MAP-T	NAT64 464XLAT
Mechanism	Double IP	Tunnelling	Tunnelling	Tunnelling	Tunnelling	Translation	Translation
Provider backbone	Dual-Stack	IPv4	IPv6	IPv6	IPv6	IPv6	IPv6
On customer equipment	Routing	IPv4 En/Decapsulation	IPv6 En/Decapsulation	Stateful NAT44 + En/Decapsulation	Stateful NAT44 + En/Decapsulation	Stateful NAT44 + Stateless NAT46	Stateless NAT46 (if CLAT in use)
On provider equipment	Routing	De/Encapsulation	De/Encapsulation + Stateful NAT44	De/Encapsulation	De/Encapsulation	Stateless NAT64	Stateful NAT64
Scalability	Medium - requires scaling both	High	Low - due to central NAT	Medium - still requires per subs states	High	High	Low - due to stateful NAT
IPv6-only host support	N/A	No	Yes (theoretically)	Yes (theoretically)	Yes (theoretically)	Yes (theoretically)	Yes
Popularity	High (decreasing)	Low	High (especially for fixed broadband)	Low	Low	Low (increasing)	High (especially for mobile broadband)

Comparison of Different IPv6 Transition Mechanisms

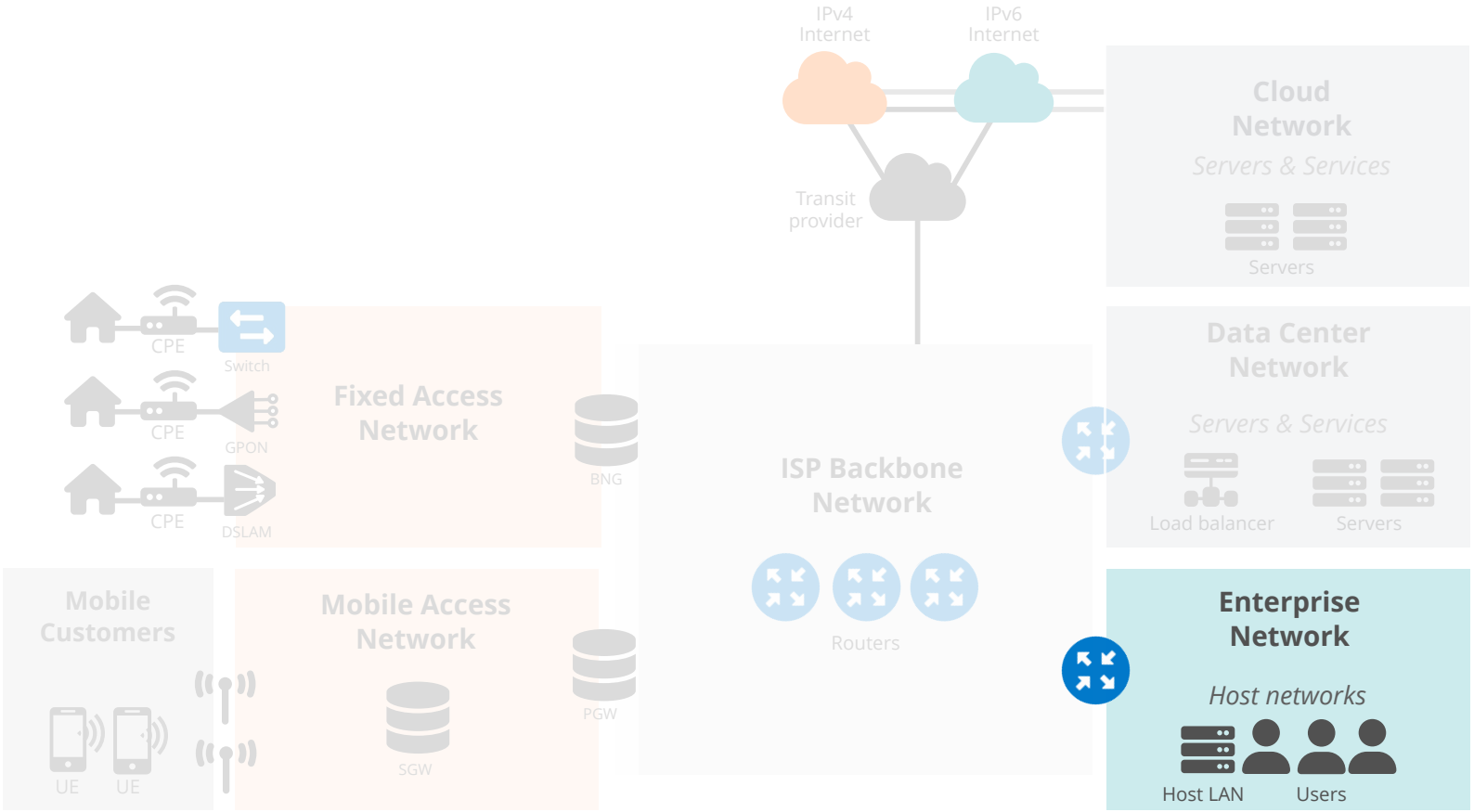
	Dual-Stack	6RD	DS-LITE	LW4o6	MAP-E	MAP-T	NAT64 464XLAT
MTU and traffic efficiency	No Overhead	20 byte (New IPv4 Header)	40 byte (New IPv6 Header)	40 byte (New IPv6 Header)	40 byte (New IPv6 Header)	20 byte Header difference	20 byte Header difference
Operational complexity	Medium (2 protocols)	Medium (Tunnel Maintenance)	Medium (Tunnel Maintenance)	Medium (Tunnel Maintenance)	Medium (Tunnel Maintenance)	Low to Medium	Low to Medium
Logging needs	Based CGN usage for NAT44	Based CGN usage for NAT44	High - fixed NAT can be considered to reduce	Medium - requires logging "per-subs states"	Low	Low	High
Asymmetric traffic support	Yes	Yes	No	No	Yes	Yes	No
IPv4 Address sharing efficiency	Based on CGN usage for NAT44	Based on CGN usage for NAT44	High - central NAT44 (dynamic port allocation is possible)	Low*	Low*	Low*	High - central NAT44 (dynamic port allocation is possible)

**Requires careful planning for provisioning as NAT44 is on CE*

Questions

Enterprise Networks

Reference Architecture - Enterprise Networks



What is an enterprise network?

Interconnected communication infrastructure for **hosts** and **users**

Enables **information sharing** and **resource access including cloud services**

In a **large** or **mid-scale** organisation

Reasons for Deploying IPv6 in Enterprises

For business growth

- Enables innovation and opportunities
  Take full advantage of new Internet-based areas such as IoT
- Enables easier acquisitions
  Get rid of overlapping private IPv4 addresses
- Enables better user experience
  Allowing smooth access to the IPv6 enabled services
- Simplifies your internal network
  Take advantage of easier administration
- Compliance with the regulations
  Governments enforce usage of IPv6

For the public sector

- Information should be available for everyone
  IPv4 and IPv6 are not compatible

The sooner enterprises deploy IPv6, the better!

The move to IPv6 is **inevitable**, there is **no alternative** plan at this time.

IPv6 is the cornerstone of our connected society.

Source: IPv6 Deployment in the Enterprise - ETSI GR IP6 001
https://www.etsi.org/deliver/etsi_gr/IP6/001_099/001/01.01.01_60/gr_ip6001v010101p.pdf

General Guidance for IPv6 Deployment in Enterprises

- Assess the **network requirements** for different services, applications and different components, including security
- Check different **transition technology** options and impacts
- Build a cross functional **team** including a skilled project manager
- Assess the existing **IT components including the cloud providers and contractors** for IPv6 readiness
- Prepare an IPv6 **addressing plan**
- Compare and choose the appropriate **routing** protocol
- **Execute** the plans starting **from upstream down to the core network, End Users and applications**

Specific Enterprise Questions for IPv6 Deployment

How can I achieve **multihoming** IPv6 connection to my upstream provider in a SOHO network?

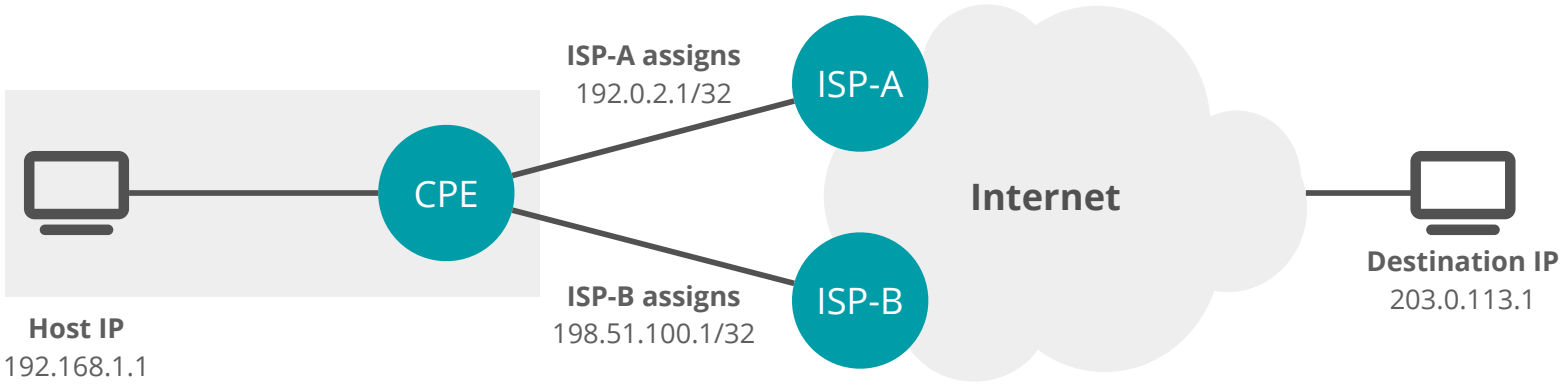
What should be supported in my **SD-WAN solution** to be able to deploy IPv6?

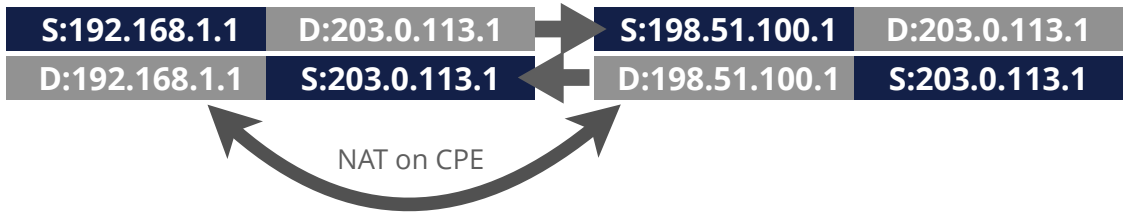
How will my **VPN solution** be affected during IPv6 deployment?

How is IPv6 supported in different **operating systems**?

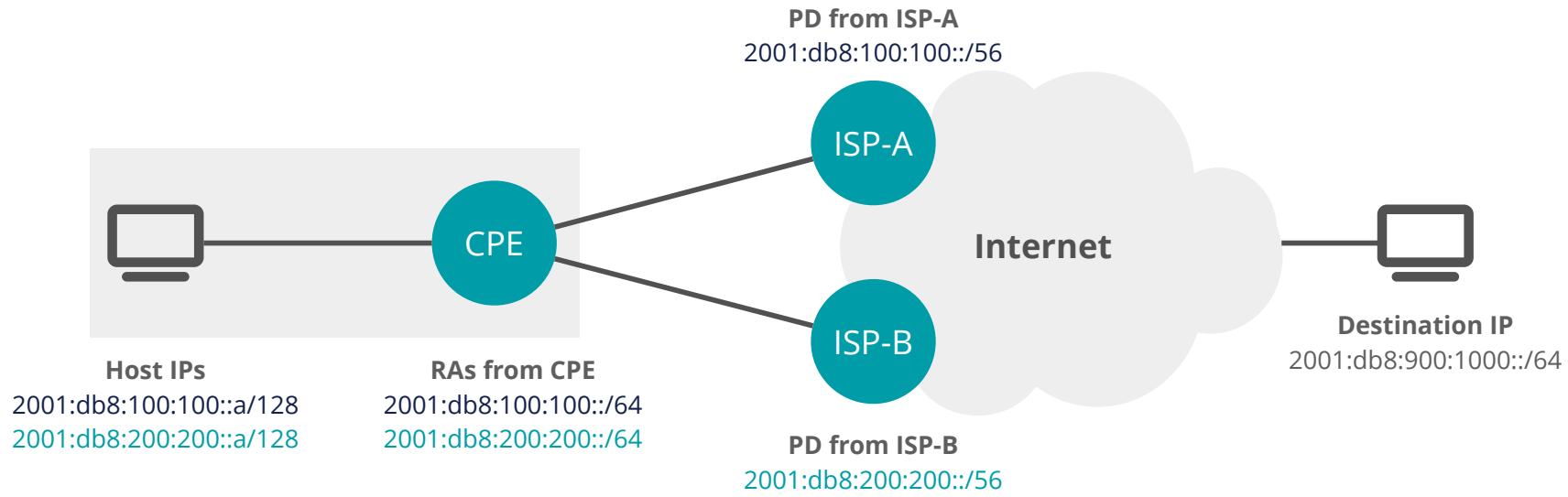
Multihoming

Multihoming With IPv4 and NAT





Multihoming With IPv6



- Each ISP assigns different IPv6 prefixes
- Host will have multiple GUAs

- Problems that might arise:
  - Asymmetrical routing
  - Packet drops

Proposed Solutions

SHIMv6

- New layer between L3 and L4
- Complex and potential impact on existing internet infrastructure
- Not widely adopted

LISP

- A map system decoupling the location information from the end-host id
- Works as an encapsulation layer
- Not widely adopted
- Address space RFC moved to **historic**

NPTv6

- Introduces NAT into IPv6
- Describes a stateless v6 to v6 translation
- RFC is still in “experimental” status
- Wide vendor support is available

RFC 7157 & RFC 8678

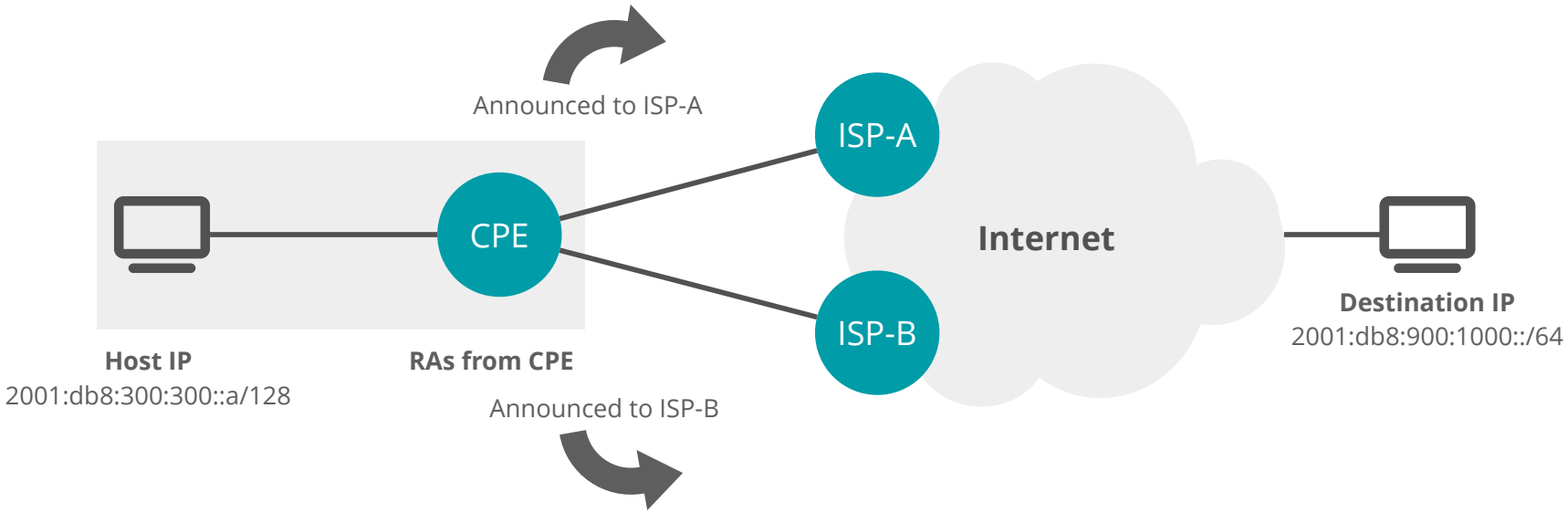
- Avoids the NAT solution
- Lists the goals needed to be achieved for a successful multihoming without NAT

Solution with Own Address Space

- ✅ Every end-site (which has its own address) can use current IPv4 best practices for IPv6 multihoming
- ✅ Can be implemented quickly

- ⚠️ Benefits to PI Address holders only
- ⚠️ Increases the size of Internet routing tables
- ⚠️ Cost implications for PI Address space
- ⚠️ Cost implications for scalability

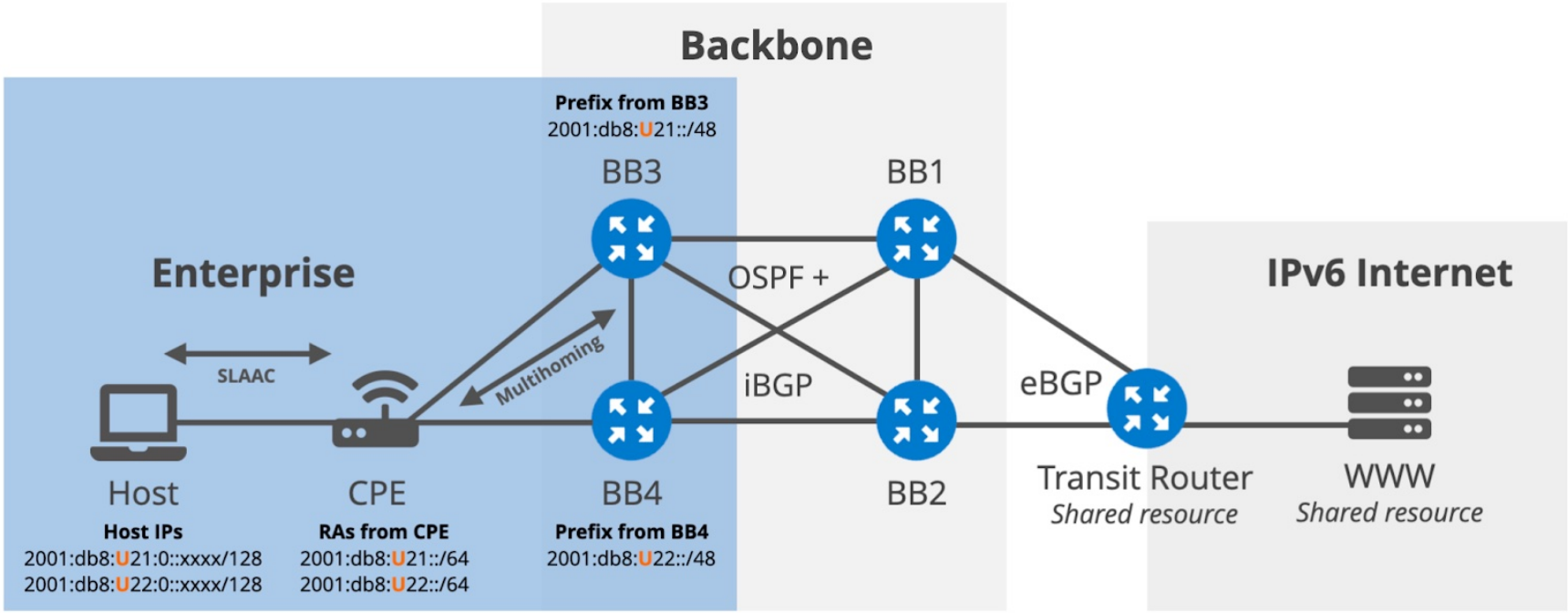
Multihoming with PI Address Space



Lab Activity 4

Multihoming for SOHO Networks

Lab Activity 4 - Multihoming for SOHO Networks



In this LAB activity you'll work on the routers **BB3, BB4, CPE and Host only**.

Lab Activity 4 - Multihoming for SOHO Networks

- **Description**: You'll first simulate this multihoming problem for SOHOs which do not have their own IPv6 address allocation and use ISPs addresses. Later, you'll solve this problem with one of the most viable methods.
- **Goal**: Configure IPv6 multihoming for Small Office Home Office (SOHO) enterprises without BGP
- **Time:** 30 minutes
- **Tasks:**

  1. Configuring a single homed SOHO network without own address space
  2. Configuring the redundant uplink
  3. Shutting down the main uplink and simulating the problem
  4. Using your own address space

Lab Activity 4 - Multihoming for SOHO Networks

- **What have you learned?**
  - You configured a single homed SOHO network with a single host behind a CPE.
  - You configured the redundant uplink for the CPE simulating a connection to another ISP and making CPE multihomed.
  - You checked and verified the connectivity from the host over both uplinks of CPE with two different IPv6 prefixes assumed to be assigned by the ISPs.
  - You triggered and verified the problem by shutting down one of the uplinks
  - You configured the same physical setup and solved the problem by using a single IPv6 prefix allocated to SOHO company instead of ISPs.

Operating Systems and IPv6

Modern Operating Systems with IPv6

Good News

IPv6 happens automatically

Bad News

IPv6 happens automatically

For better control in your host network, you may want to
disable SLAAC or Temporary Address Extensions!

Windows

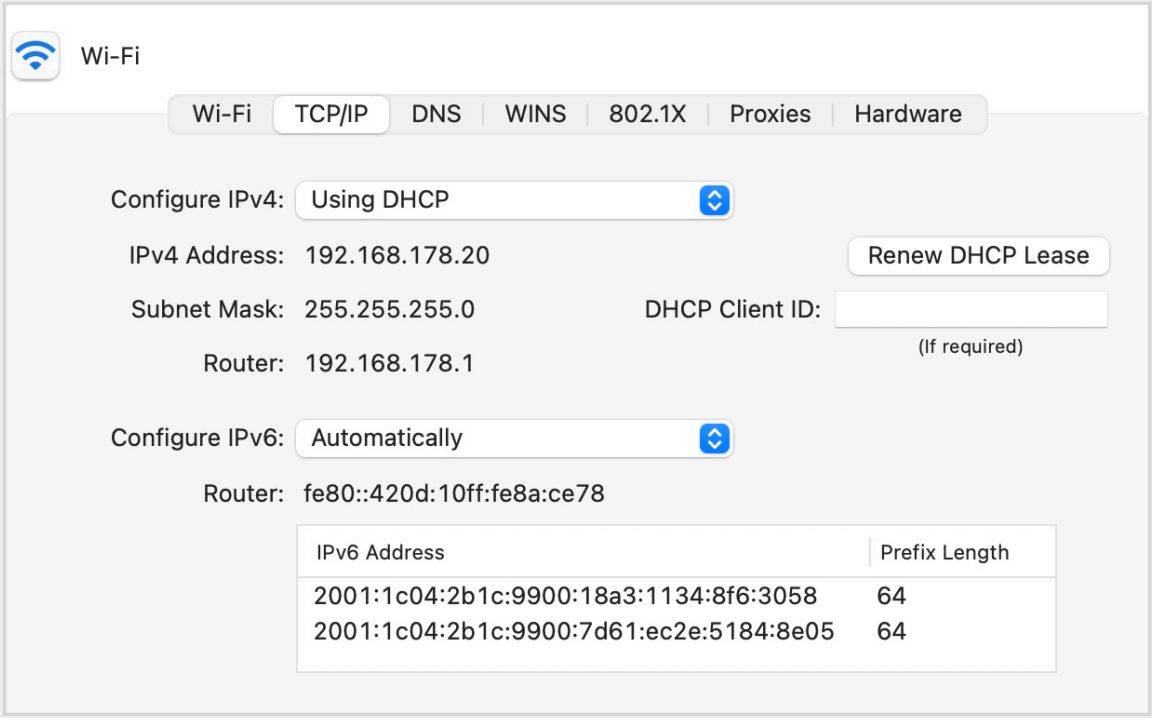
- Supports IPv6 natively
- On recent versions of Windows 10 and 11 DHCPv6 works off the shelf
- RDNSS is supported in Windows 10 since build 1703 - March 20, 2017
- You can check and disable/enable dhcpv6 with the commands:

`netsh interface ipv6 show interfaces`	Check the interface ID
`netsh interface ipv6 set interface XX advertise=enabled managed=enabled`	Change the status
`netsh interface ipv6 show interface XX`	Check the status on a specific interface

- Be careful with **Windows 7**, as old protocols such as “Privacy extensions”, “Teredo”, “ISATAP” or “6to4” might be enabled by default.

MacOS

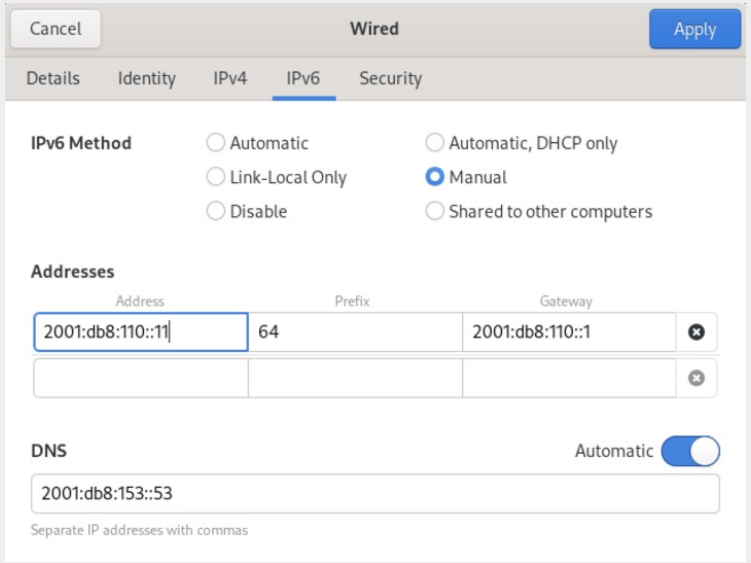
- Supports IPv6 natively
- As well as DHCPv6
- You can't disable IPv6 from the GUI by default




```
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether f8:4d:89:81:56:c6
        inet6 fe80::14f0:2563:da5d:cddc%en0 prefixlen 64 secured scopeid 0xe
        inet6 2001:1c04:2b1c:9900:18a3:1134:8f6:3058 prefixlen 64 autoconf secured
        inet6 2001:1c04:2b1c:9900:7d61:ec2e:5184:8e05 prefixlen 64 autoconf temporary
        inet 192.168.178.20 netmask 0xffffff00 broadcast 192.168.178.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
```

Linux

- Supports IPv6 and DHCPv6 off the shelf
- As a server, static configuration is preferred
- Manual configuration example from CENTOS/RHEL9

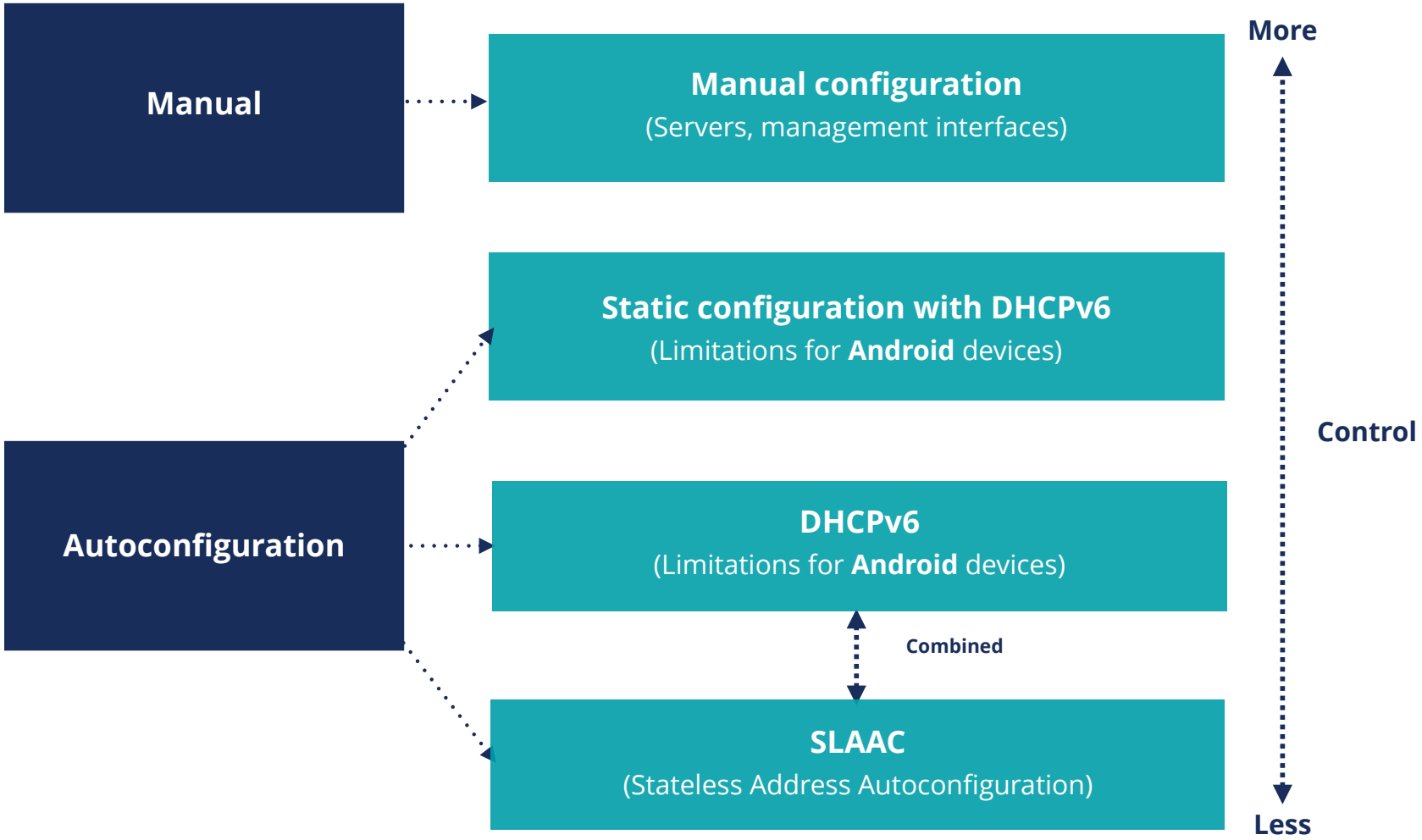



```
[user@localhost ~]$ nmcli connection show enp0s1 | egrep '(IP|ipv)6'
ipv6.method:                            manual
ipv6.dns:                               2001:db8:153::53
ipv6.dns-search:                        --
ipv6.dns-options:                       --
ipv6.dns-priority:                      0
ipv6.addresses:                         2001:db8:110::11/64
ipv6.gateway:                           2001:db8:110::1
--------------------omitted-----------------------
IP6.ADDRESS[1]:                         fe80::f4e4:feff:fe0f:e8d6/64
IP6.ADDRESS[2]:                         2001:db8:110::11/64
IP6.GATEWAY:                            2001:db8:110::1
IP6.ROUTE[1]:                           dst = 2001:db8:110::/64, nh = ::, mt = 100
IP6.ROUTE[2]:                           dst = ::/0, nh = 2001:db8:110::1, mt = 100
IP6.ROUTE[3]:                           dst = fe80::/64, nh = ::, mt = 1024
IP6.DNS[1]:                             2001:db8:153::53
```

Mobile OSes on LAN

- Both Apple and Android OSes support SLAAC and RDNSS
- DHCPv6 incapability on Android devices
- Effects of not using DHCPv6
- Recent updates and discussions
  - RFC9663
  - /64 assignment per device

Choosing the Address Configuration Method



Happy Eyeballs Question

What is **Happy Eyeballs**?

a. An algorithm for determining which protocol is better to reach a network
b. A method for deploying IPv6 servers
c. A new protocol used instead of dual-stack
d. A medical term for the eye disorder

Happy Eyeballs Answer

What is **Happy Eyeballs**?

- ✓ An algorithm for determining which protocol is better to reach a network
- b. A method for deploying IPv6 servers
- c. A new protocol used instead of dual-stack
- d. A medical term for the eye disorder

Happy Eyeballs

Why use it?

Makes dual-stacked websites more responsive to users

How does it work?

If there is both A and AAAA

- First IPv6 is used with a 300 ms head start
- If that fails, IPv4 is used

Implemented by almost all browsers and operating systems

Unstable connections can cause problems with session cookies

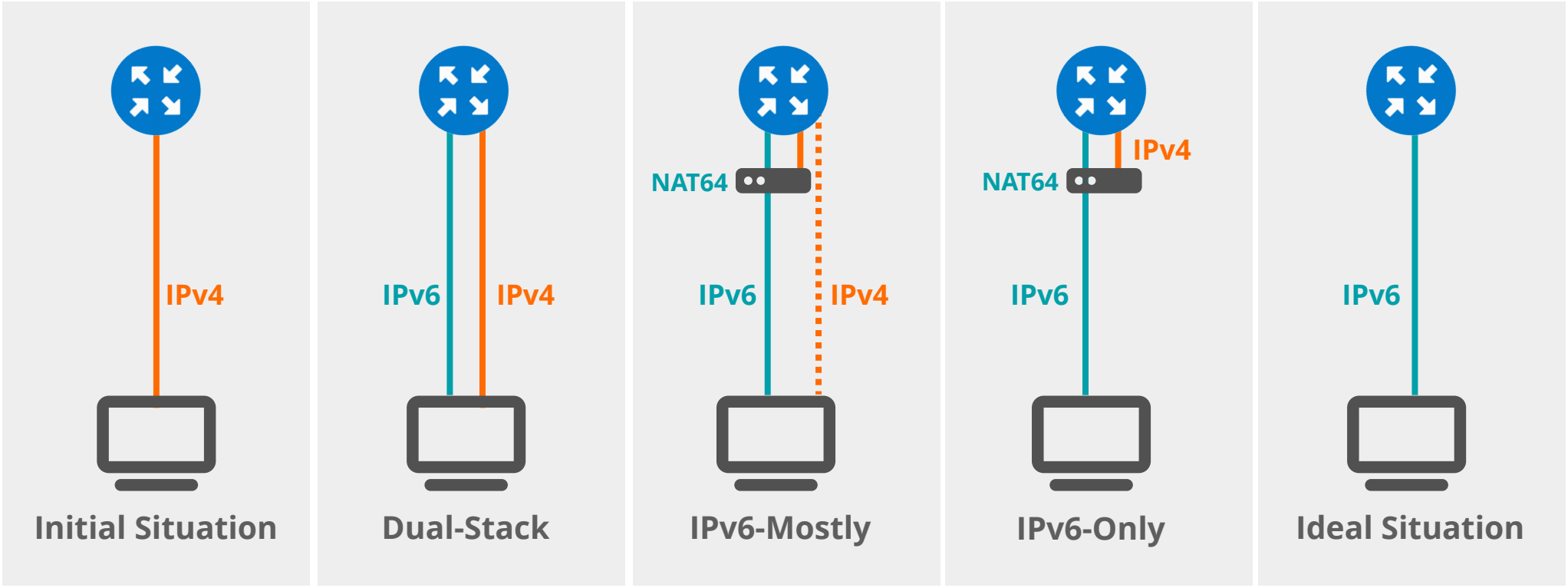
Long living sessions like “SSH” or “remote desktop” can still encounter problems

Happy Eyeballs v2

New enhancements over Happy Eyeballs v1:

- Asynchronous DNS queries
- Sorting of resolved destination addresses
- Asynchronous connection attempts
- **IPv4 Literals and Broken IPv6 Destination Addresses for IPv6-only networks**

IPv6 Mostly Networks

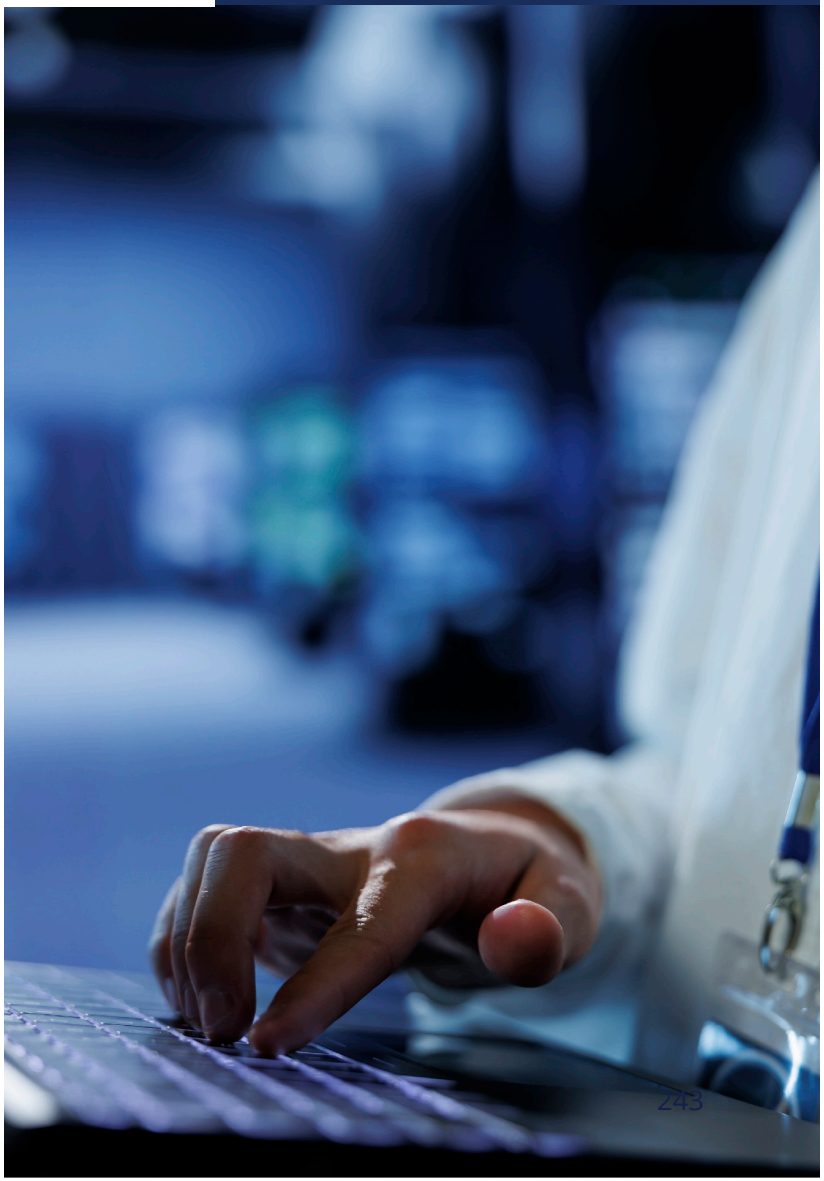


Options to Achieve IPv6-only in Heterogeneous Networks

Address assignment on nodes without an IPv4 address	Not scalable
Two different networks one with dual-stack and the other one is IPv6-only	Operational complexity Placing a host in the correct network segment is problematic
DHCP Option 108 (RFC 8925)	The IPv6-Only Preferred Option for DHCPv4 specifies a method to use a DHCP option

OSes Support DHCP option 108

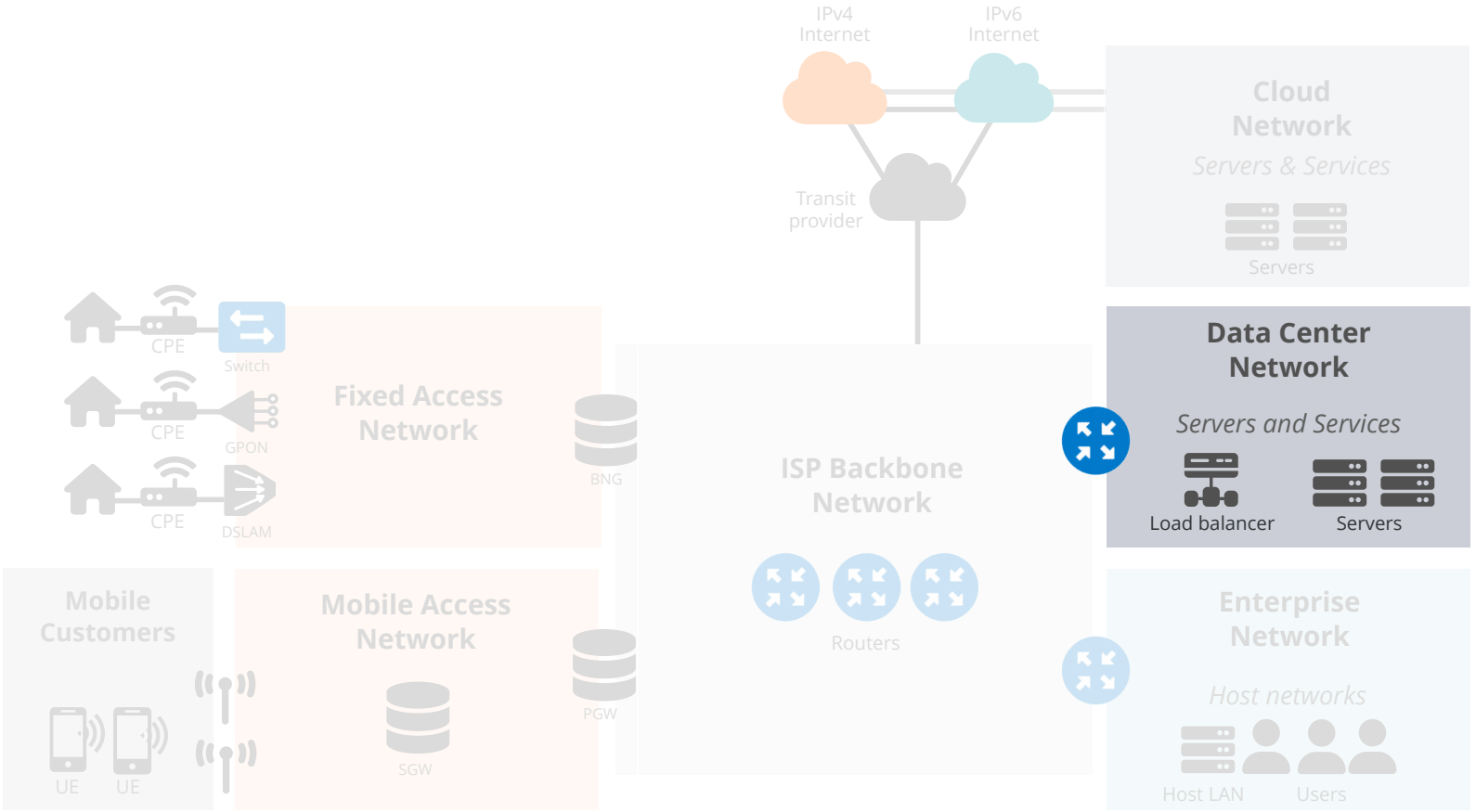
- All recent Android and iOS devices
- MacOS - 12.0.1 and newer
- Windows support is on its way - Announced on 7th of March 2024
- Linux - optional support on “systemd-networkd” - (no CLAT support yet)

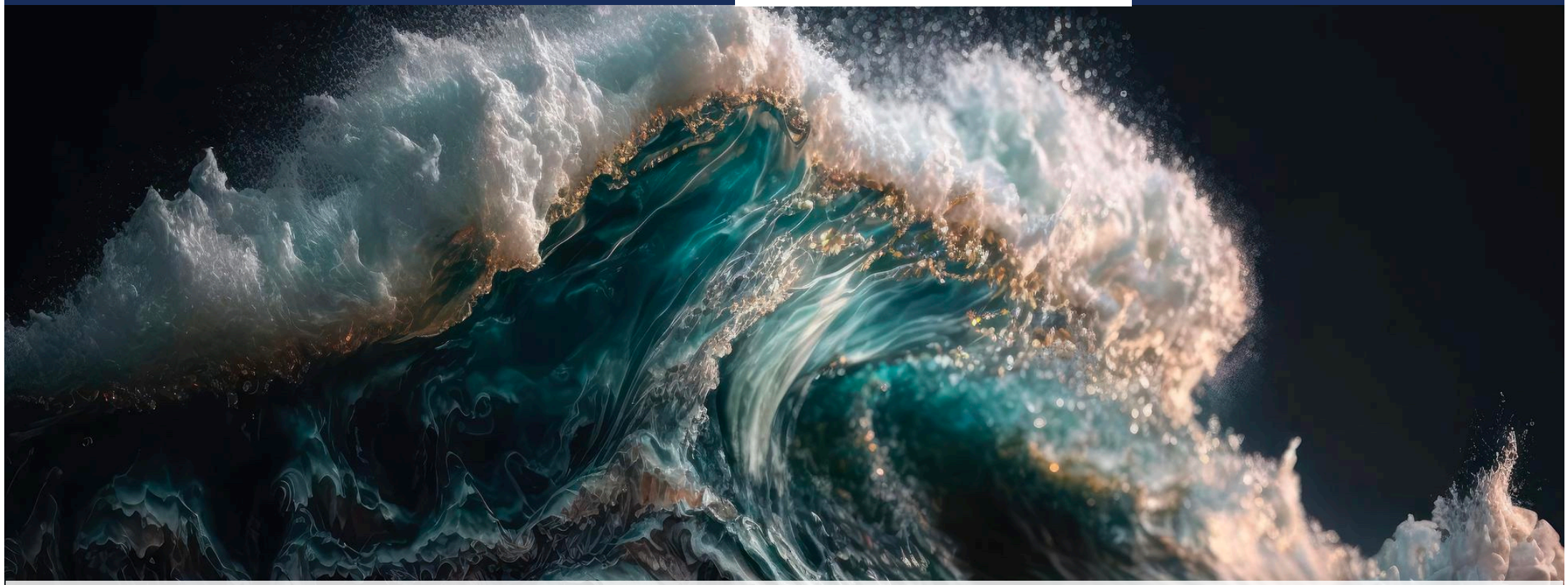


Questions

Data Center Networks

Reference Architecture - Data Center Networks





IPv6 Adoption: A Virtual Surge

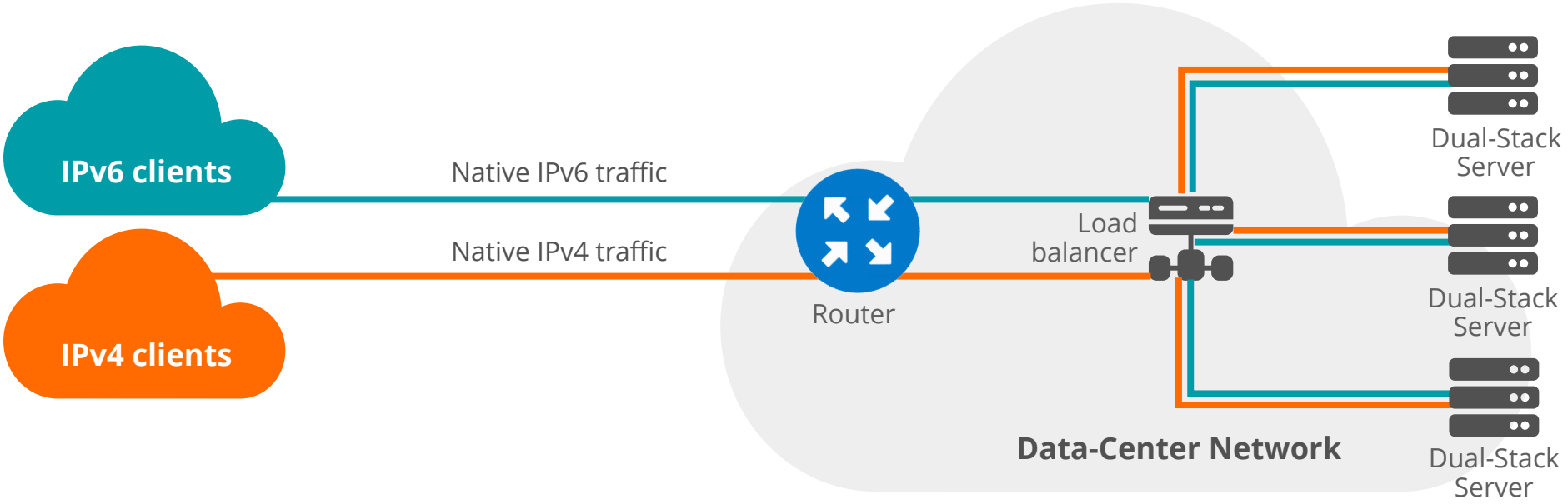
As virtualisation is **expanding the capacity** beyond what physical hardware permits, many data centers have already been forced to adopt IPv6

IPv6 Introduction in The Data Center Network

1. List your infrastructure and verify their IPv6 support and requirements
   - your applications and services
   - your servers, VMs and containers
   - your network and network security equipment
2. Choose a strategy
   - Dual-Stack Servers
   - Connection Proxying
   - Native IPv6 Servers (with SIIT-DC)
3. Make an address plan
4. Build a test environment - if possible
5. Enable and check IPv6 connectivity at your WAN connection
6. Configure your security infrastructure
7. Configure your routers and switches
8. Configure your servers and VMs accordingly
9. Configure your DNS servers
   (IPv6 AAAA and PTR records)

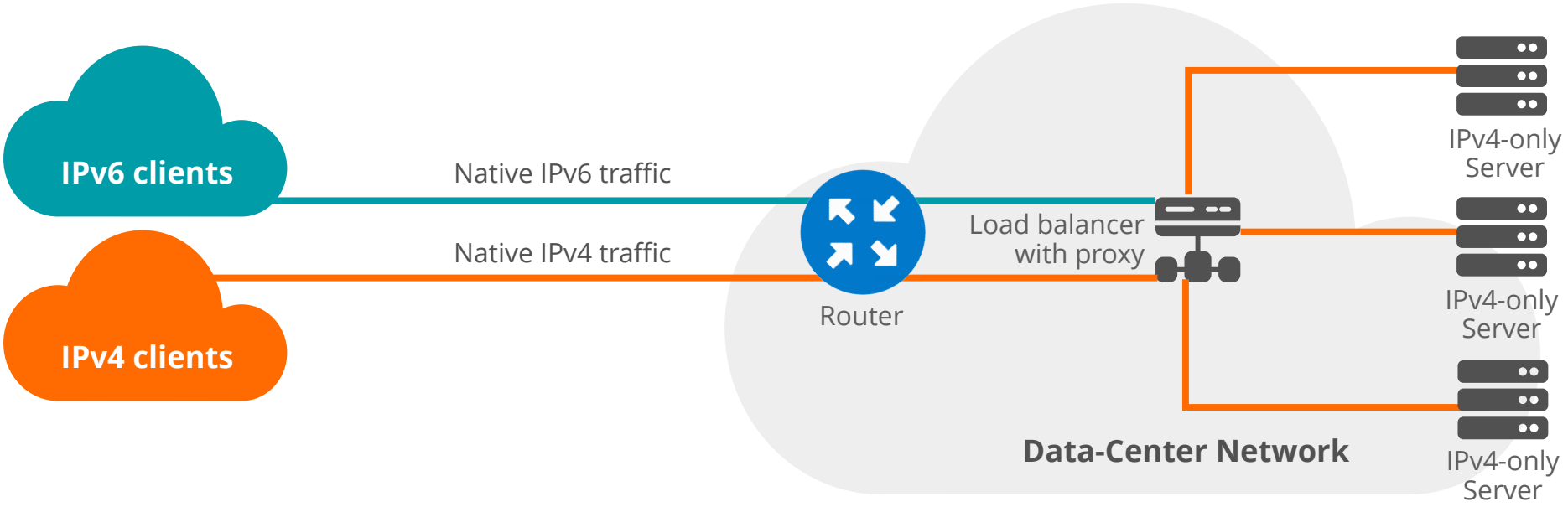
IPv6 Deployment
DC Strategies

Dual-Stack Servers



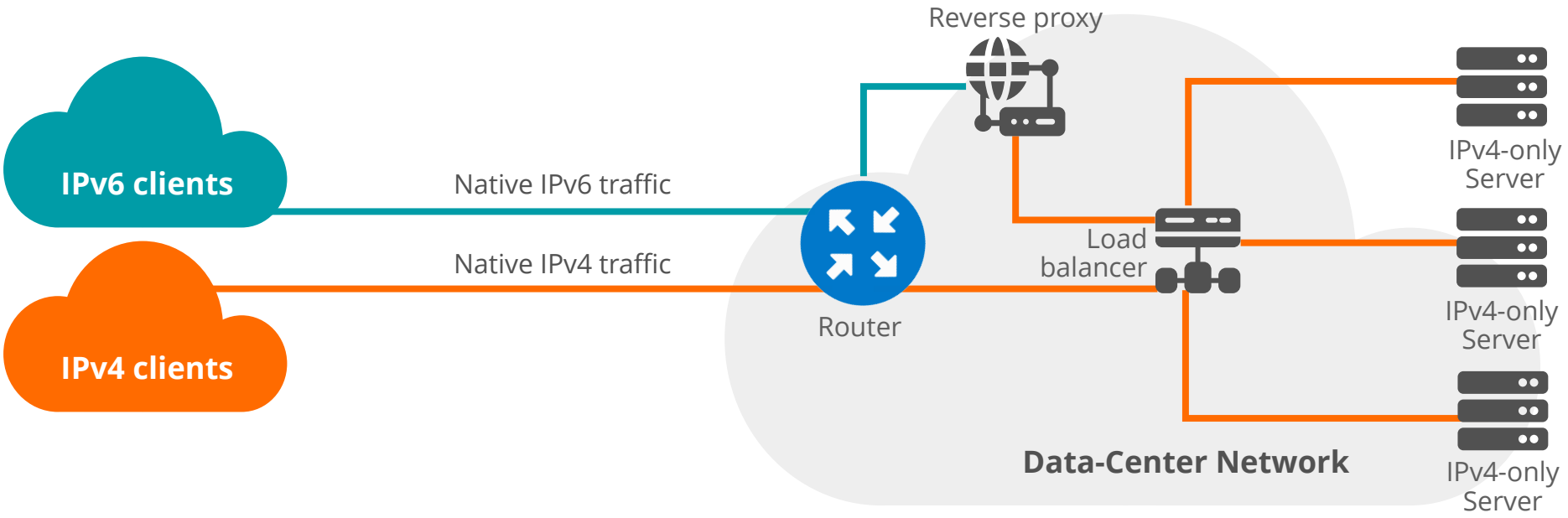
- Needs servers to support IPv6 natively
- Needs a fully dual stacked network
- All addresses fully visible where possible

Load Balancer with proxy



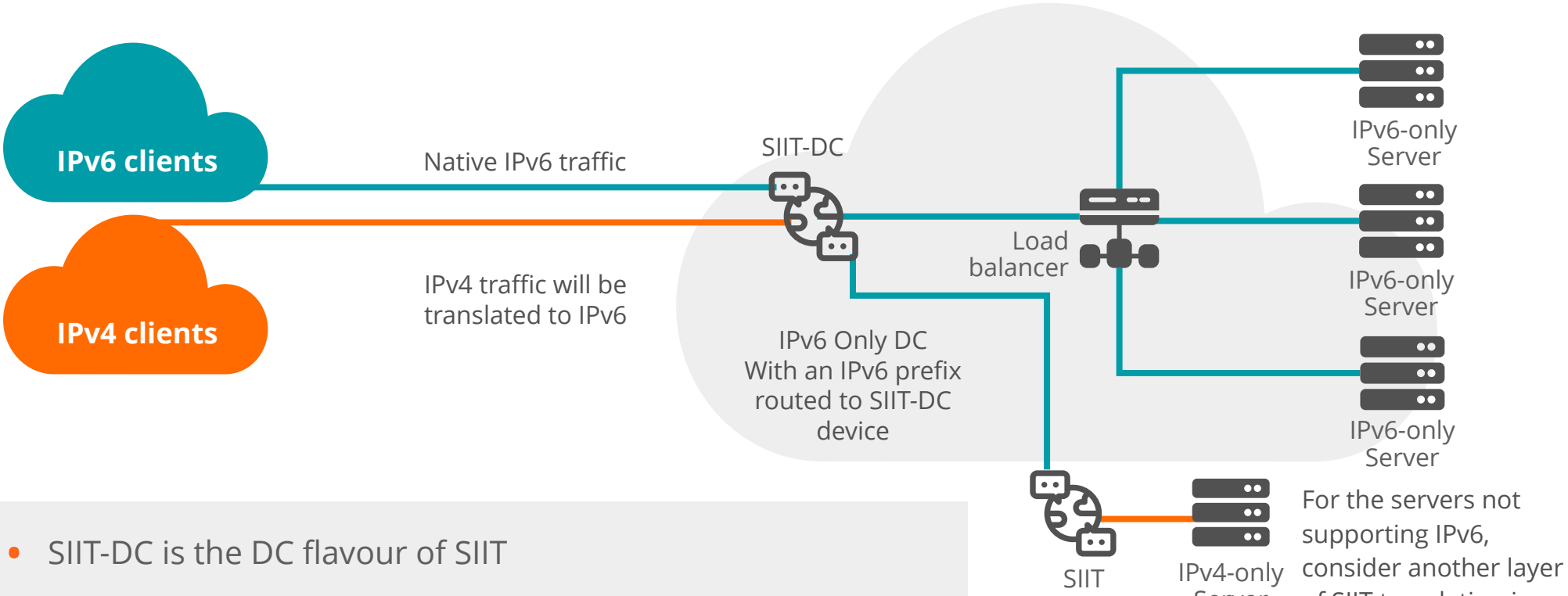
- Load-balancer will support dual-stack
- Proxy function runs on the load-balancer & AAAA DNS records for the services
- HTTP X-Forwarded-For feature

Reverse Proxy



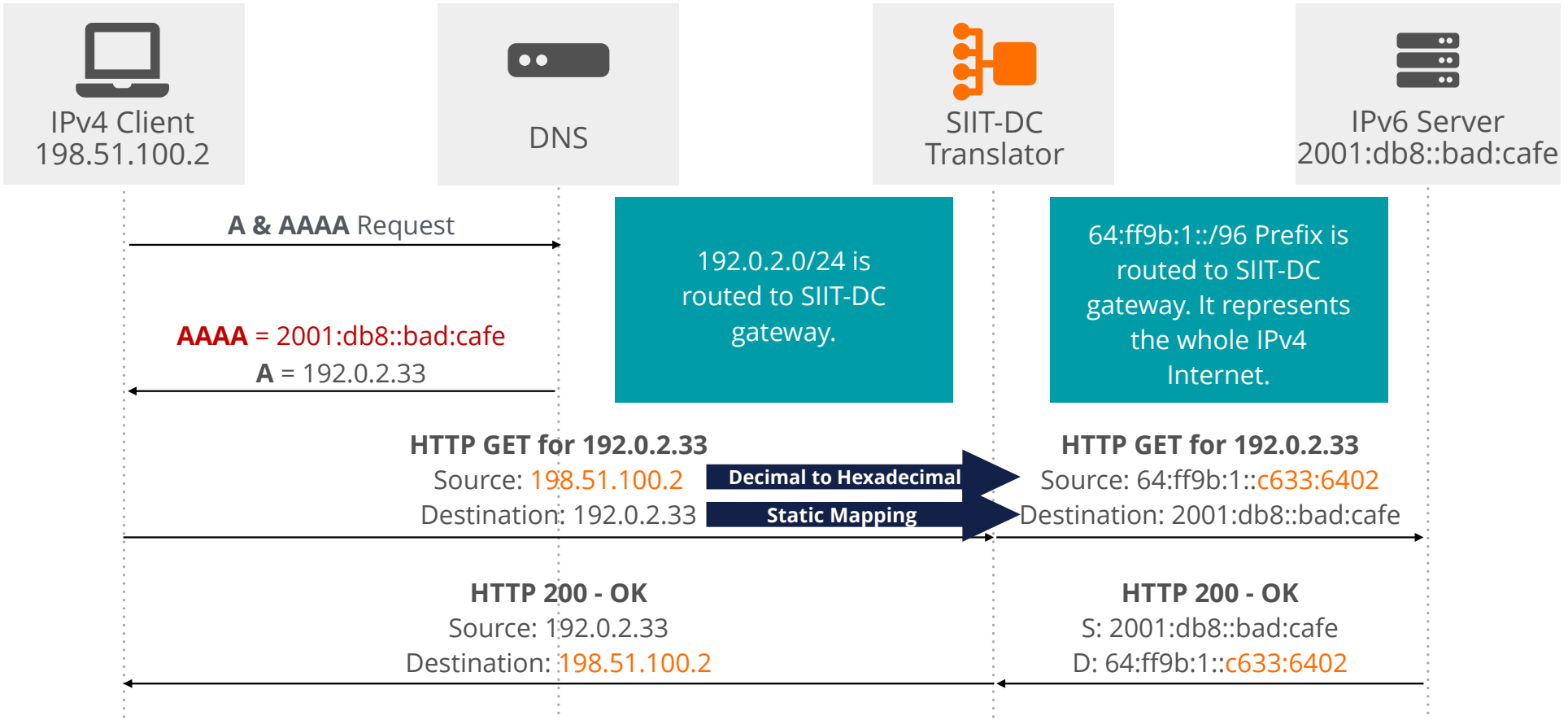
- Reverse proxy + AAAA records for matching IPv6 addresses
- Web servers might not see IPv6 addresses
- Load on Proxy? - increasing by time as the clients move to IPv6

Native IPv6 - SIIT-DC Scenario - SIIT defined in RFC 6145



- SIIT-DC is the DC flavour of SIIT
- Enables access to IPv6 servers from IPv4 clients, statelessly
- A prefix in the range of 64:ff9b:1::/48 can be used to represent IPv4 internet inside the DC network

SIIT-DC Scenario - Packet Flow



DNS in IPv6

Is DNS in IPv6 Difficult?

- **DNS** is not IP layer dependent
  - **A** record for **IPv4**
  - **AAAA** record for **IPv6**
- DNS does not answer based on the incoming protocol
- Only challenges are for translations
  - NAT64, proxies
- **Reverse DNS:** Mapping an IPv6 address to a hostname
- **ip6.arpa** domain

RFC 3596 is created to support the storage of IPv6 addresses in the DNS
Link: https://datatracker.ietf.org/doc/html/rfc3596

How to Create AAAA Records?

To create a AAAA (Quad-A) record generally you need to configure 3 parameters:

Host Name	Target IPv6 Address	TTL

An example in generic resource record format:

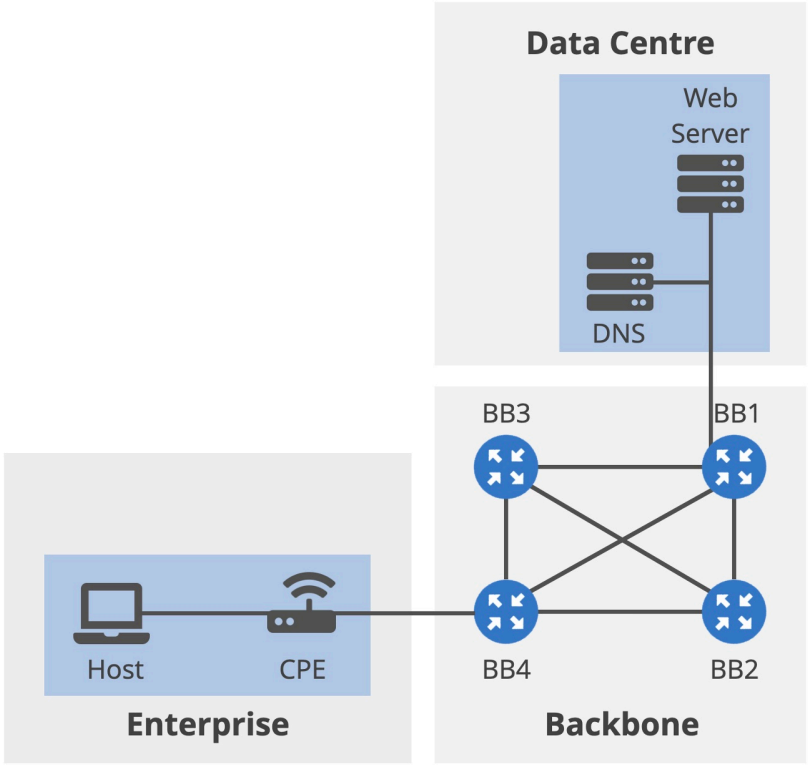
```
www.example.com. 86400 IN AAAA 2001:db8::123
```

After creating the AAAA record, you can check it with the **host** command. It should look like:

```
(base) admin@system ~ % host ripe.net
ripe.net has address 193.0.11.51
ripe.net has IPv6 address 2001:67c:2e8:25::c100:b33
```

Lab Activity 5

Lab Activity 5 - DNS Configuration



In this LAB activity you'll work on the **CPE router, host2 and DNS server only**.

Lab Activity 5 - DNS Configuration

- **Description**: You'll configure RDNSS option on the CPE device to send DNS information to the host device. You'll check the DNS zone file on the DNS server and then you'll configure a AAAA record in the zone file. You'll test web server reachability with the curl command
- **Goal**: Configure RDNSS on the CPE and DNS zone file for the AAAA records on the DNS server
- **Time:** 20 minutes
- **Tasks:**
  1. Configuring RDNSS option on CPE
  2. Configuring DNS Server for AAAA Record

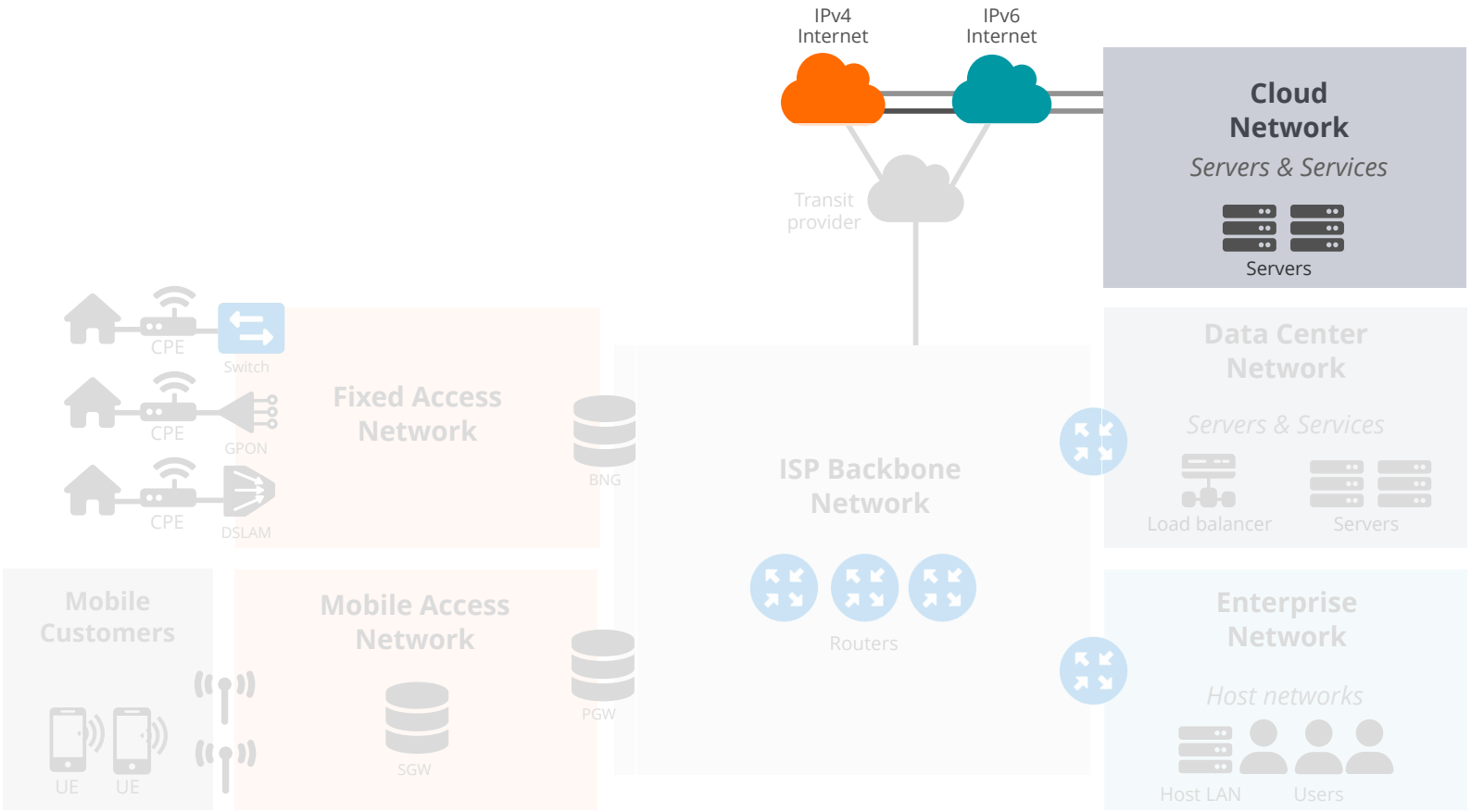
Lab Activity 5 - DNS Configuration

- **What have you learned?**
  - You configured RDNSS option on the CPE device and passed the DNS information to the host via RA messages
  - You checked the DNS records for a specific domain
  - You configured the AAAA record on the DNS server
  - You verified the same DNS information on the host and was able to reach the WEB server with this DNS record available.

Questions

Cloud Networks

Reference Architecture - Cloud Networks



There is no cloud

It's just someone else's computer

Cloud Networks

- IT services such as:
  - Compute-power
  - Data storage
  - Databases
- Scalable
- On-demand
- Over Internet
- On-demand services vs. Physical servers and data centers.

Drivers for IPv6 Deployment in Cloud Based Services

- Public IPv4 exhaustion
- Private IPv4 exhaustion
- Cost of IPv4 addresses
- Interoperability with IPv6 networks and IPv6-enabled end-users
- Elimination of workaround solutions (such as NAT, VRF or Overlays)
- Better and easier address management - accelerate the mergers and acquisitions
- Regulations

Questions for the Cloud Service Provider

Do you support IPv6 on:

Cloud network infrastructure?
to be able to create IPv6 network on cloud

VPN services?
to be able to reach IPv6 cloud network from on-premises DC

DNS services?
to be able to create IPv6 DNS records and access our resources

Compute services?
(VM, Containerised or Serverless) to be able to access compute resources over IPv6

Load-balancer services?
to be able to have a proper load-balancing to the resources over IPv6

Storage services?
to be able to access stored data over IPv6

Database services?
to be able to access DB over IPv6

Security services?
to protect resources against threats over IPv6

Steps to take

1. List the services and features you use
2. Check where you need IPv6 support and if it supported on your cloud provider network
3. Decide on the size of the services that need IPv6 support
   - Number of the services and subnets
   - Consider scaling
   - Check the number of data centers you need (availability zones etc.)
4. Check if bringing your own IPv6 address is supported (BYOIP)
5. Have an addressing plan (some cloud providers provide IPAM tools for IP address inventory management and tracking)
6. Build security rules to be implemented

Questions

Pilot and User Tests

First Steps in the Live Network

1. Select a small portion of the network for implementation
2. Pause maintenance work in that part of the network
3. Create a list of users to test the new protocol in end-user network segments
4. Create a direct communication channel between users and the project team
5. Test most used applications and websites
   - Make a list of top-25/50 apps on smart phones
   - Make a list of top-100 websites in your country or region
6. Encourage users to test a variety of devices
7. Monitor network performance during user tests
8. Keep track of reported issues

Deploy Phase - Summary - You Learned:

- How to deploy IPv6 in:
  - Backbone Networks
  - Access Networks
  - Enterprise Networks
  - Data Centers
  - Cloud Networks
- How to conduct user tests

Questions

Manage IPv6 Networks

Troubleshooting IPv6

Common Faults in IPv6 Networks

- Typos
- Misconfigured ACL or FW rules
- Devices running IPv6 without your explicit awareness
- Different routing/ECMP/link-aggregation behaviour than IPv4
- MTU problems
- NDP interoperability issues
- Transition mechanism problems

The best tool that you can use in IPv6 troubleshooting is:

Your knowledge

ICMPv6

Transition Mechanisms

OSPFv3/IS-IS

NDP

Addressing Plans

BGP

Prefix Delegation

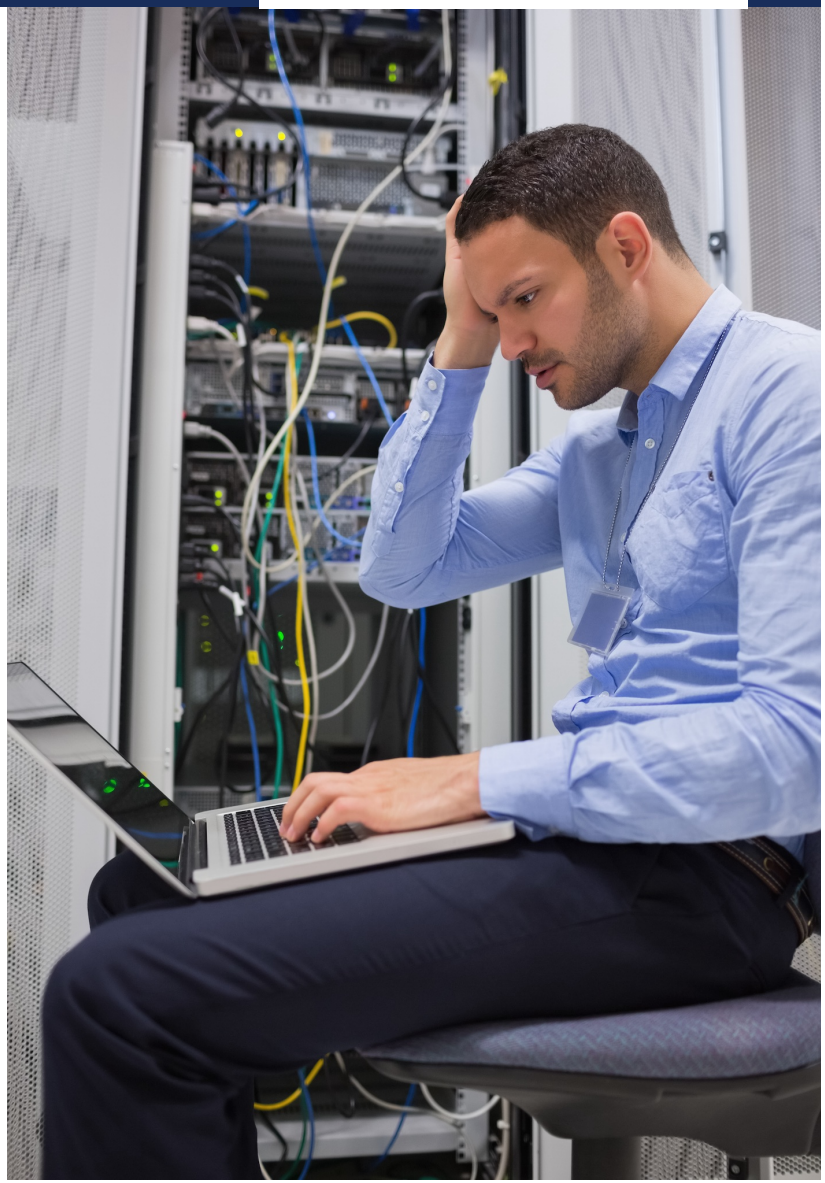
DHCPv6

Network Topology

Other Tools for Troubleshooting IPv6 Connectivity

- **ping(6)** - *connectivity check*
- **traceroute(6) & mtr** - *connectivity check*
- **dig, nslookup, host** - *DNS query*
- **Wireshark, tcpdump & termshark** - *Packet capture and analysis tools*
- **Scapy, Nmap** - *Packet generation and manipulation tools*

- And online tools...



Online Tools to Check IPv6 Connectivity

isp.test-ipv6.com

Codes for help-desks to interpret (RIPE-631 document)

ipv6-test.com

IPv4 and IPv6 connectivity tests & DNS information

doesnotwork.eu

Server, which does not work over IPv4

Offers e-mail IPv6 capability test

v6.de

Basic IPv4 and IPv6 connectivity information

bgp.tools

Latency comparison information for IPv4 and IPv6 in addition to connectivity information

ip6.me

Options for ipv4-only and ipv6-only tests and API for test automatisation

Demo time!

Demo test-ipv6.com

General Approach for IPv6 Troubleshooting

1. Online IPv6 connectivity tools
2. Recent changes in the network and monitoring tools
3. Local network communication
4. “ping” and “traceroute” for detecting broken IPv6 paths
5. IPv6 associated protocols - DNS, NDP, DHCPv6, SLAAC...
6. Routing paths and protocols - OSPFv3, IS-IS, BGP, static routes etc.
7. IPv6 security settings

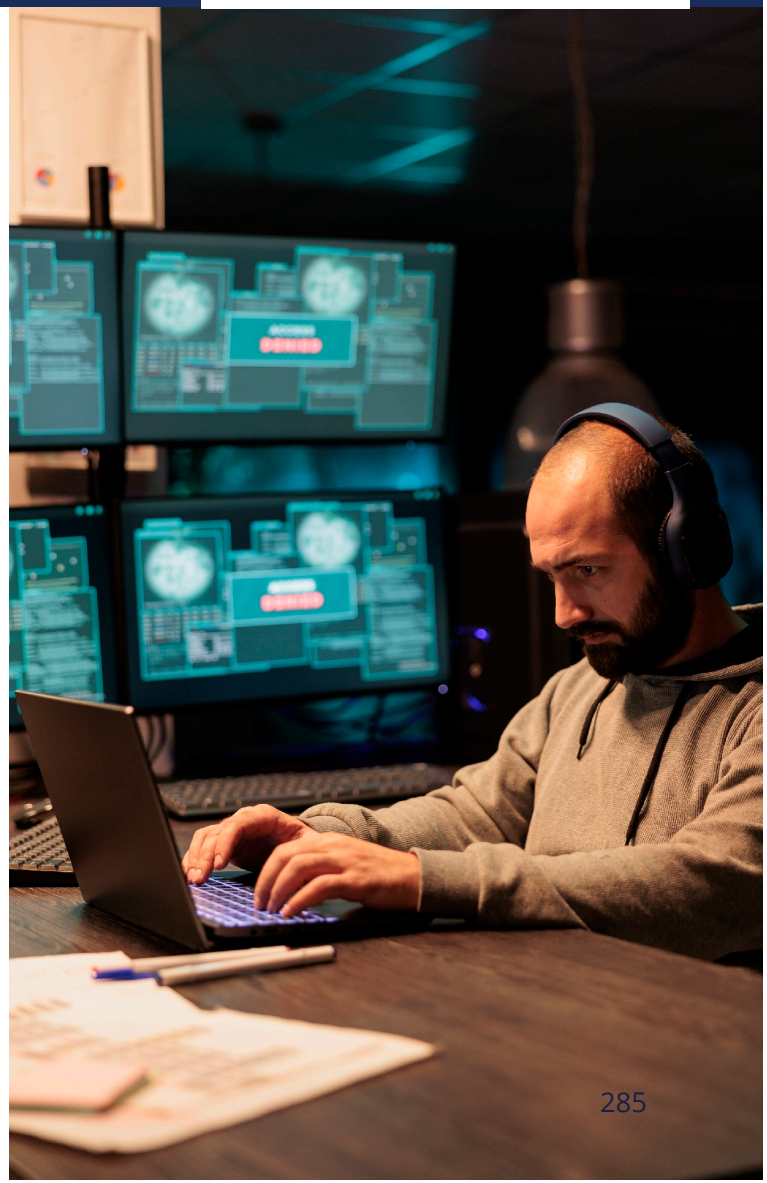
Questions

Monitoring IPv6 Networks

Benefits of monitoring tools

In the context of IPv6 deployment, you can:

- Track the **progress of IPv6 deployment** in your network.
- **Compare IPv6 statistics with IPv4 statistics** for performance optimisation.
- **Receive notifications** for unusual traffic patterns, enabling quicker troubleshooting.
- Easily **correlate events** with the deployment steps.
- **Take proactive actions** to enhance the customer experience.
- **Identify issues** that might be hidden due to "**happy eyeballs**".
- Detect and **respond to IPv6 specific threats**.



Network Monitoring

Logging

- Syslog
- SNMP traps

Performance Monitoring

Pull-Model

- SNMP
- RestAPI
- ICMP(v6)

Push-Model

- Telemetry
- NetFlow, sFlow & other “flow”s

Security Monitoring

- OpenVAS
- nMap
- THC-IPV6

IPv6 Security e-learning Course:

https://academy.ripe.net/enrol/index.php?id=12

Performance Monitoring

With performance monitoring tools you can:

- Track bandwidth usage and link utilisation
- Follow the changes in delay of the packets
- Check the reachability of specific targets
- Monitor your hardware metrics such as CPU/memory usages or error counters

Performance monitoring - Tools

Cacti

- Performance, fault management & graph data tool
- **SNMP polling** is the default source
- Plug-ins enable fault management, log management, device discovery, **NetFlow** data collection and more

Grafana

- A multi-platform open source visualisation web application
- Can be also fed through telemetry data (gRPC)

Iperf.fr

- A tool for active measurements of the maximum achievable bandwidth on IP networks
- Reports MSS/MTU size
- Measures delay jitter

smokeping

- Lightweight latency measurement tool
- It can measure, store and display latency, latency distribution and packet loss
- Supports different probes such as ping or web requests

Performance monitoring - Platforms

OpenNMS

- A free and open-source network monitoring and management platform
- Supports:
  - Route monitoring
  - Traffic analysis
  - Topology discovery

Nagios CORE

- Monitoring and alerting engine
- Extendible with add-on projects
- Front end is also customisable

ICINGA

- Network monitoring tool with enhanced visualisation capabilities
- It can be integrated with the other open source tools for better visualisation of their data
- Provides customisable dashboards

ZABBIX

- Another monitoring tool offering capabilities like monitoring network bandwidth usage, tracking configuration changes, and automatically discovering devices
- It provides trend-prediction for taking proactive actions

Using RIPE Atlas

Measuring latency and reachability from/to your network to/from random or specific destinations all over the world.

Checking the path from your network out via specific IP protocol.

IPv4/IPv6

Measuring reachability to your network (or to one of your Internet facing servers) **over a specific protocol**.

Measurement data can be **processed offline** or by the help of the Streaming API **in real-time.**

Link to RIPE Atlas: https://atlas.ripe.net

Tips & Tricks

Tips for “Get Approval” Phase

- Try to convince managers by showing the **cost reduction and possible revenues**.
- Prepare a detailed project plan, but don't think that you can cover **every detail** at the beginning.
- **Communication throughout the organisation** is the key, try to get your project announced to the whole organisation. Let people know what is coming and support you.
- Especially at the beginning of the project try to **have a core team** and don’t ask everybody to join your meetings.
- Adopt iterative approach with **short feedback loops** where in each iteration you’ll be fixing a different issue!
- **Document lessons learned** for the future feedback loops

Tips for “Get Ready” Phase

- Spend time on your **addressing plan**!
- Don’t forget your **backup pools** in your addressing plans!
- Having a LAB is very important, try to **test and analyse the results** in your LAB environment first.
- Try to plan your **training sessions just before the actual work** otherwise it will be forgotten!
- Ensure all new network equipment **purchases support IPv6 features**, regardless of current IPv6 usage, to future-proof the infrastructure.

Tips for “Deploy” Phase - I

- **Avoid vendor proprietary features** as much as possible.
- **Start the deployment from the internet connection point** (check with your service provider first) and expand it to the backbone and access networks respectively!
- Be careful with the **feature set of CPE devices**!
- **Lawful intercept** can be a pain, think ahead!
- For the fixed access customers, try to use **persistent prefix** assignments!
- Test **in-house developed applications**! Request product owners’ involvement.
- Don’t forget **network management systems**!
- Don’t forget **customer provisioning services** and software (CRM)!

Tips for “Deploy” Phase - II

- While deciding on the transition mechanisms **aim for IPv6-only** to make things smoother in the future.
- RFC6052 restricts the usage of well-known prefix if access to RFC1918 destinations (private IPv4 addresses) is needed.
- While using **NAT64** be careful about **fragmentation**. IPv6 packets will always be bigger than the IPv4 packets
- **Android** (still) **does not support DHCPv6**, don’t forget this in your plans!
- If you are using **ECMP** together with any-cast scenario make use of **flow-labels** for load-balancing.
- Avoid counting on deprecated or **old-fashioned mechanisms**. (TEREDO, ISATAP etc.)

We want your feedback!

What did you think about this session? Take our survey at:

https://www.ripe.net/feedback/av6/

What's Next in IPv6

Webinars

Attend another webinar live wherever you are.

- Introduction to IPv6 (2 hrs)
- IPv6 Addressing Plan (1 hr)
- Basic IPv6 Protocol Security (2 hrs)
- IPv6 Associated Protocols (2 hrs)
- IPv6 Security Myths, Filtering and Tips (2 hrs)

For more info click the link below

learning.ripe.net

Face-to-face

Meet us at a location near you for a training session delivered in person.

- IPv6 Fundamentals (8.5 hrs)
- IPv6 Advanced (17 hrs)
- IPv6 Security (8.5 hrs)

E-learning

Learn at your own pace at our online Academy.

- IPv6 Fundamentals (15 hrs)
- IPv6 Security (24 hrs)

For more info click the link below

academy.ripe.net

Examinations

Learnt everything you needed? Get certified!

- IPv6 Fundamentals - Analyst
- IPv6 Security - Expert

For more info click the link below

getcertified.ripe.net


RIPE NCC
Academy
Learn something new today!
academy.ripe.net

RIPE NCC Certified Professionals

https://getcertified.ripe.net/


Ënn
Соңы
An Críoch
پایان
Ende
Y Diwedd
Vége
Endir
Finvezh
վերջ
Koniec
Son
დასასრული
הסוף
Кінець
Finis
Lõpp
Amaia
Loppu
Tmiem
Liðugt
Kpaj
Slutt
Kraj
Sfârşit
النهاية
Конец
Konec
Fund
Fine
Fin
Einde
Fí
Край
Beigas
Τέλος
Fim
Slut
Pabaiga
E1
N1
D2

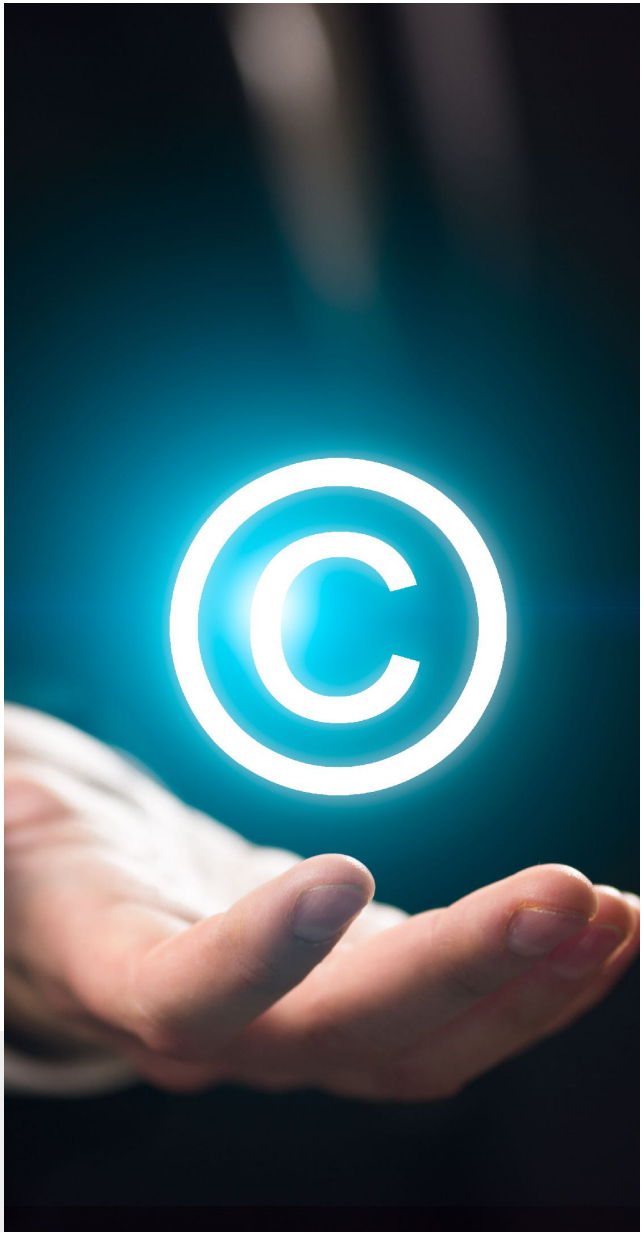
Copyright Statement

[...]

The RIPE NCC Materials may be used for **private purposes, for public non-commercial purpose, for research, for educational or demonstration purposes**, or if the materials in question specifically state that use of the material is permissible, and provided the RIPE NCC Materials are not modified and are properly identified as RIPE NCC documents. Unless authorised by the RIPE NCC in writing, any use of the RIPE NCC Materials for advertising or marketing purposes is strictly forbidden and may be prosecuted. The RIPE NCC should be notified of any such activities or suspicions thereof.

[...]

Find the full copyright statement here:
https://www.ripe.net/about-us/legal/copyright-statement



Annex

Enterprise VPN Solutions

IPv6 Support for Enterprise VPN Solutions

Most of the modern enterprise VPN solutions support IPv6 both as:

The traffic inside the tunnel

The underlying transport protocol

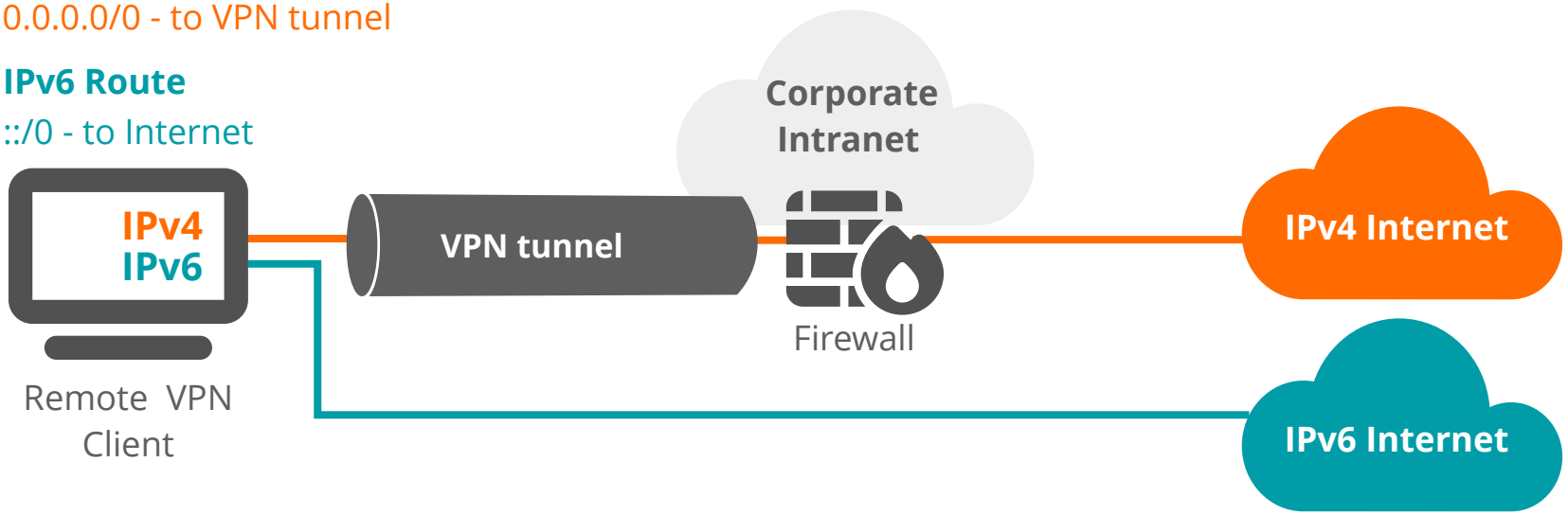
Examples:

- OpenVPN (TLS/SSL)
- Cisco AnyConnect/ASA (IPSec and TLS modes)
- Palo Alto Networks GlobalProtect VPN (IPSec & TLS modes)
- Fortinet VPN FortiClient (IPSec and TLS modes)
- F5 Big-IP Access (IPSec and TLS modes)
- Microsoft Always-On VPN (IPSec and SSTP/ TLS modes)

VPN Breakout Threat for IPv6

IPv4 Route
0.0.0.0/0 - to VPN tunnel

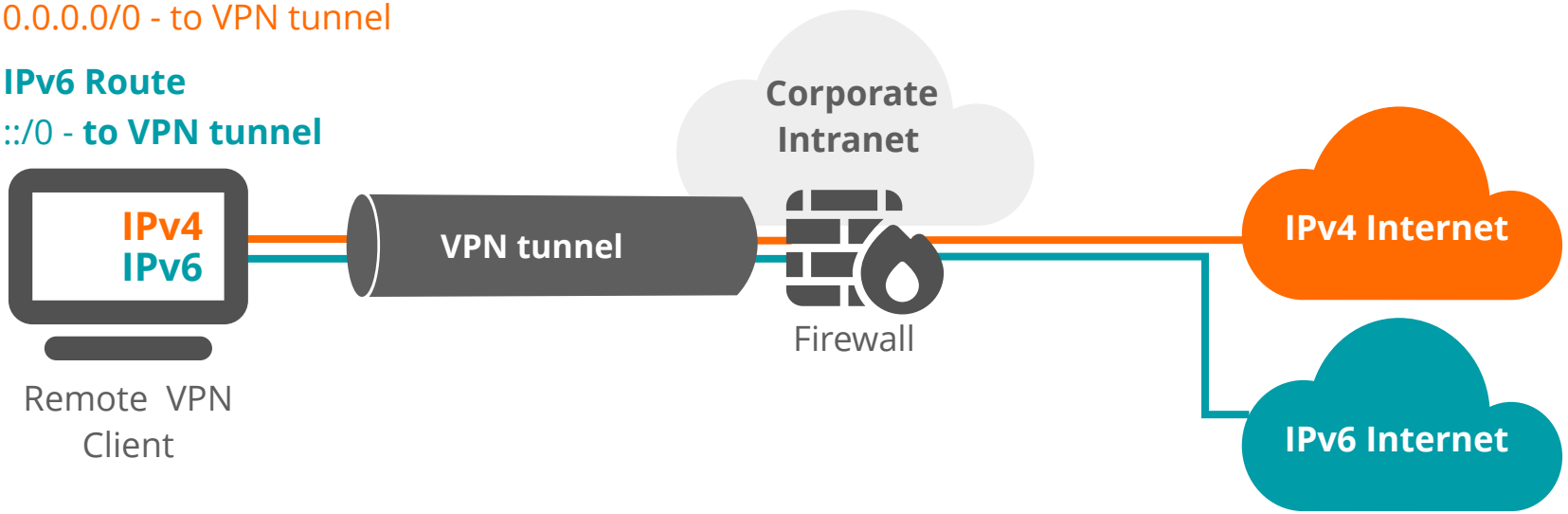
IPv6 Route
::/0 - to Internet



VPN Breakout Threat for IPv6

IPv4 Route
0.0.0.0/0 - to VPN tunnel

IPv6 Route
::/0 - **to VPN tunnel**



Don't consider disabling IPv6 on the clients as some of the commercial (private use) VPNs offer.

How to configure IPv6 for Enterprise IPSec VPNs?

1. **Assign an IPv6 address**

2. **On the VPN Server:**
   Define a range or a pool for the clients to be addressed

2. **On the client:**
   Configure the server's FQDN (or IP address)

3. **Configure IPsec Policies**
   (including Security Associations (SAs), authentication, encryption, and integrity protocols)

4. **Define the traffic** that needs to be encrypted (by using an ACL) and associate this with the policy defined

5. **Apply the policy**

How to configure IPv6 for Enterprise IPSec VPNs?

On the VPN Server

1. Assign an IPv6 address
2. **Define a range or a pool for the clients to be addressed**
3. Configure IPsec Policies (including Security Associations (SAs), authentication, encryption, and integrity protocols)
4. Define the traffic that needs to be encrypted (by using an ACL) and associate this with the policy defined
5. Apply the policy

On the Client

1. Assign an IPv6 address
2. **Configure the server's FQDN (or IP address)**
3. Configure IPsec Policies (including Security Associations (SAs), authentication, encryption, and integrity protocols)
4. Define the traffic that needs to be encrypted (by using an ACL) and associate this with the policy defined
5. Apply the policy

Configure **AAAA records on DNS servers** if you're using hostnames instead of IP addresses!

What to Consider for Deploying IPv6 with Enterprise VPNS?

- IPv4 vs IPv6 VPN: Similar for TLS and IPSec
  - Configure IPv6 addresses and pools accordingly
  - Adjust your ACLs to include IPv6 addresses
  - Be sure to configure AAAA records for your IPv6 VPN servers
  - For split tunnel: Review tunnelled prefixes carefully
- Consider clients with/without native IPv6
- Remote DNS impact on DNS64/NAT64 networks

How to configure IPv6 for Enterprise IPSec VPNs?

Server Configuration

IPv6 Addressing:
Assign outer IPv6 to server
Define inner IPv6 pool for clients

Set-up Authentication:
IPSec: Configure pre-shared keys/certificates
TLS: Install CA and server certificates

Configure Security Policies:
IPSec: Define SAs, encryption, integrity
TLS: Set TLS version, cipher suites

Define Traffic Rules:
IPSec: Configure ACLs for traffic selection
TLS: Configure split-tunneling

Apply policies

Client Configuration

Set server FQDN/IPv6 address

IPv6 Addressing:
Use existing outer IPv6 assigned by ISP/local network
Receive inner IPv6 from server

Set-up Authentication:
IPSec: Configure pre-shared key/certificate
TLS: Install client certificates

Configure Security Policies:
IPSec: Define set SAs (often server-pushed)
TLS: Ensure compatibility

Define Traffic Rules:
Specify which traffic should be tunnelled (server-pushed)
Set split-tunnelling if applicable

Apply settings

Configure **AAAA records on DNS servers** if you're using hostnames instead of IP addresses!

How to configure IPv6 for Enterprise VPNs?

On the VPN Server

1. Assign a IPv6 address
2. **Define a range or a pool for the clients to be addressed**
3. Configure IPsec Policies (including Security Associations (SAs), authentication, encryption, and integrity protocols)
4. Define the traffic that needs to be encrypted (by using an ACL) and associate this with the policy defined
5. Apply the policy

On the Client

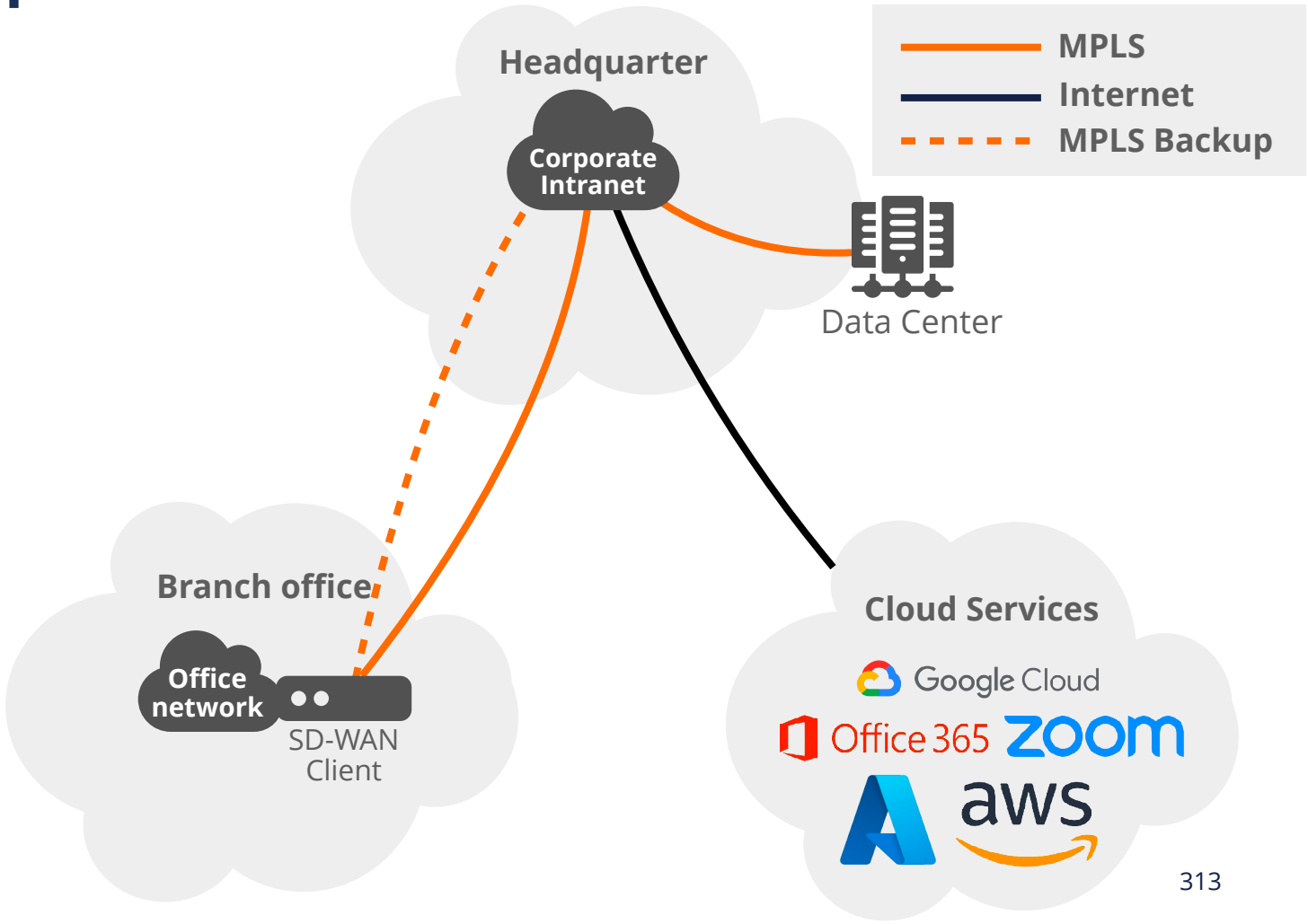
1. Assign a IPv6 address
2. **Configure the server's FQDN (or IP address)**
3. Configure IPsec Policies (including Security Associations (SAs), authentication, encryption, and integrity protocols)
4. Define the traffic that needs to be encrypted (by using an ACL) and associate this with the policy defined
5. Apply the policy

SD-WAN

Traditional Enterprise Branch Office Connections

Traditional Architecture:

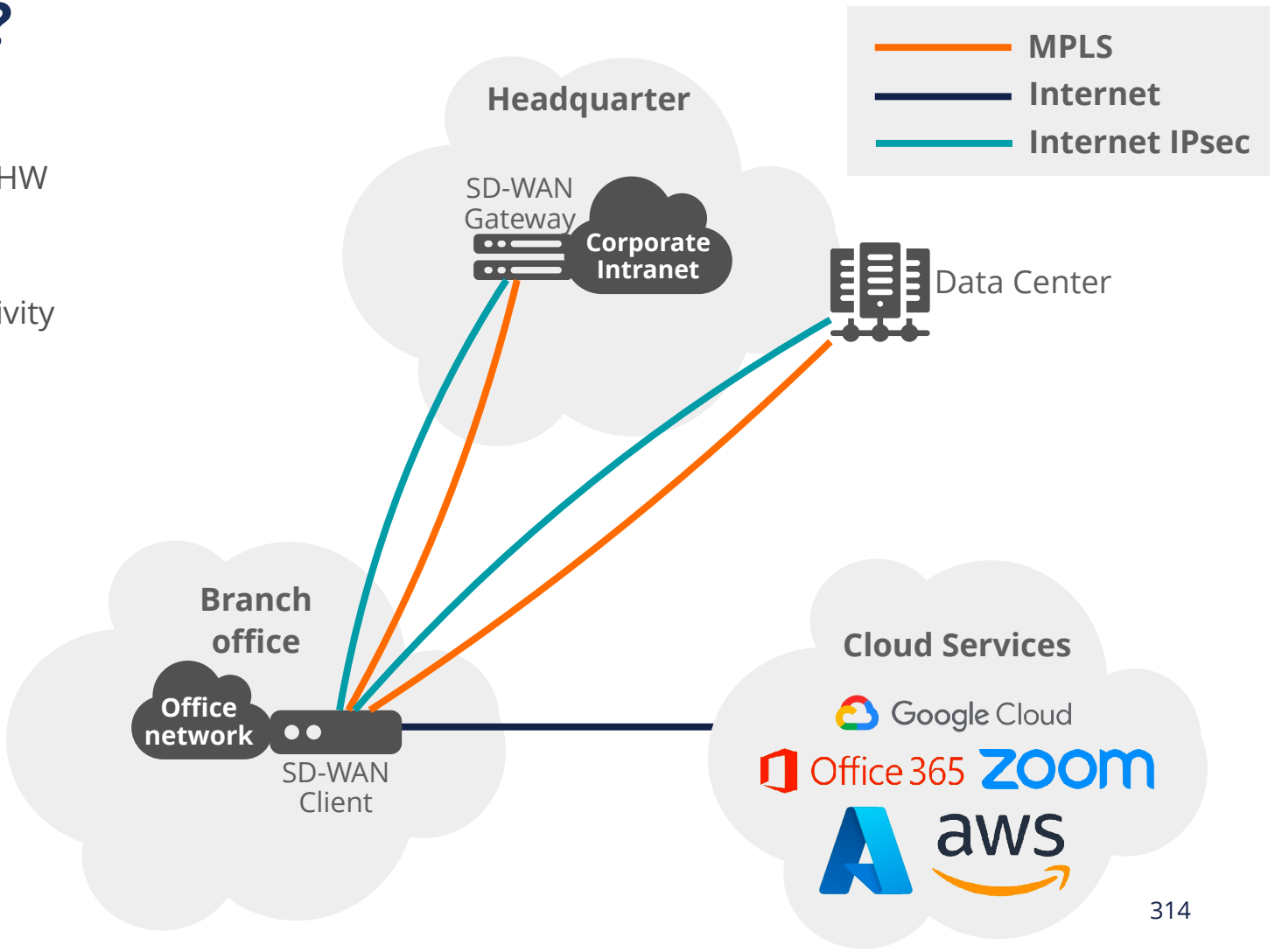
- Inflexible and costly MPLS connections
- Geographical limitations of MPLS availability
- Dedicated paths



What is SD-WAN?

SD-WAN Architecture:

- Separates network from its HW
- Forms a virtualised overlay
- Provides optimised connectivity & cost saving



SD-WAN Challenges for IPv6 Deployment - I

Feature parity control for SDWAN solution

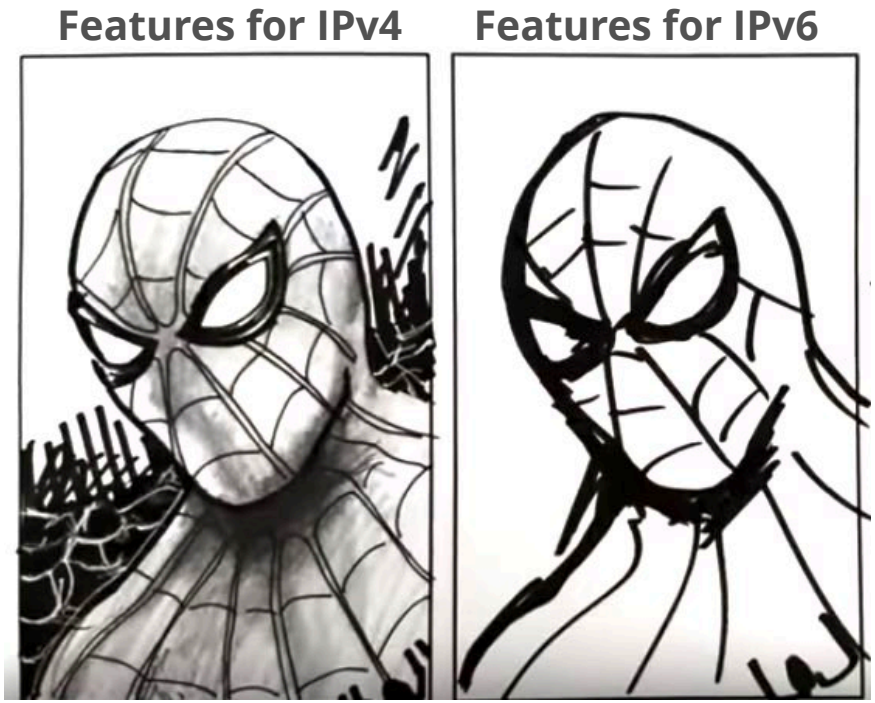
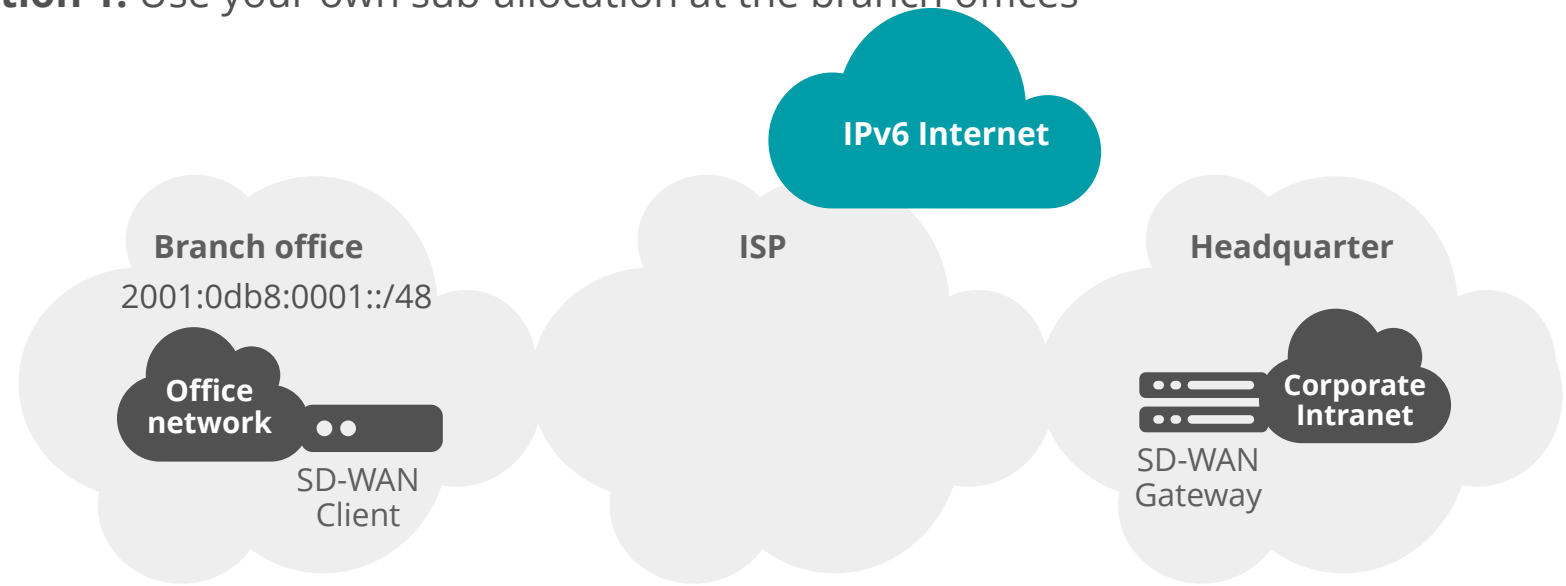


Image Credits: https://www.youtube.com/watch?v=x9wn633vl_c

SD-WAN Challenges for IPv6 Deployment - II

Option 1: Use your own sub-allocation at the branch offices



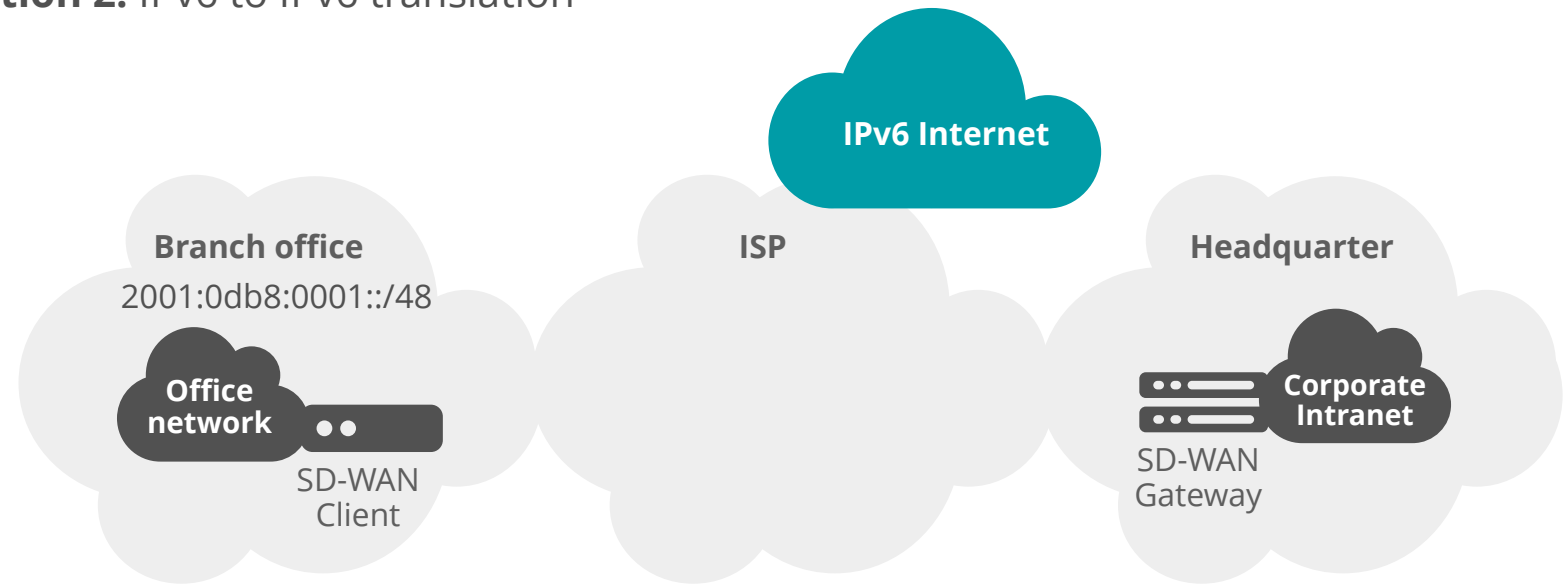
Branch office uses its own sub-allocation (2001:0db8:0001::/48) to reach both IPv6 internet and corporate intranet via overlay IPSec tunnels *(if there is no direct connection to the headquarter via MPLS)*

ISP announces 2001:0db8:0001::/48 to IPv6 Internet

RIR Allocation to the Enterprise 2001:0db8::/32

SD-WAN Challenges for IPv6 Deployment - II

Option 2: IPv6 to IPv6 translation



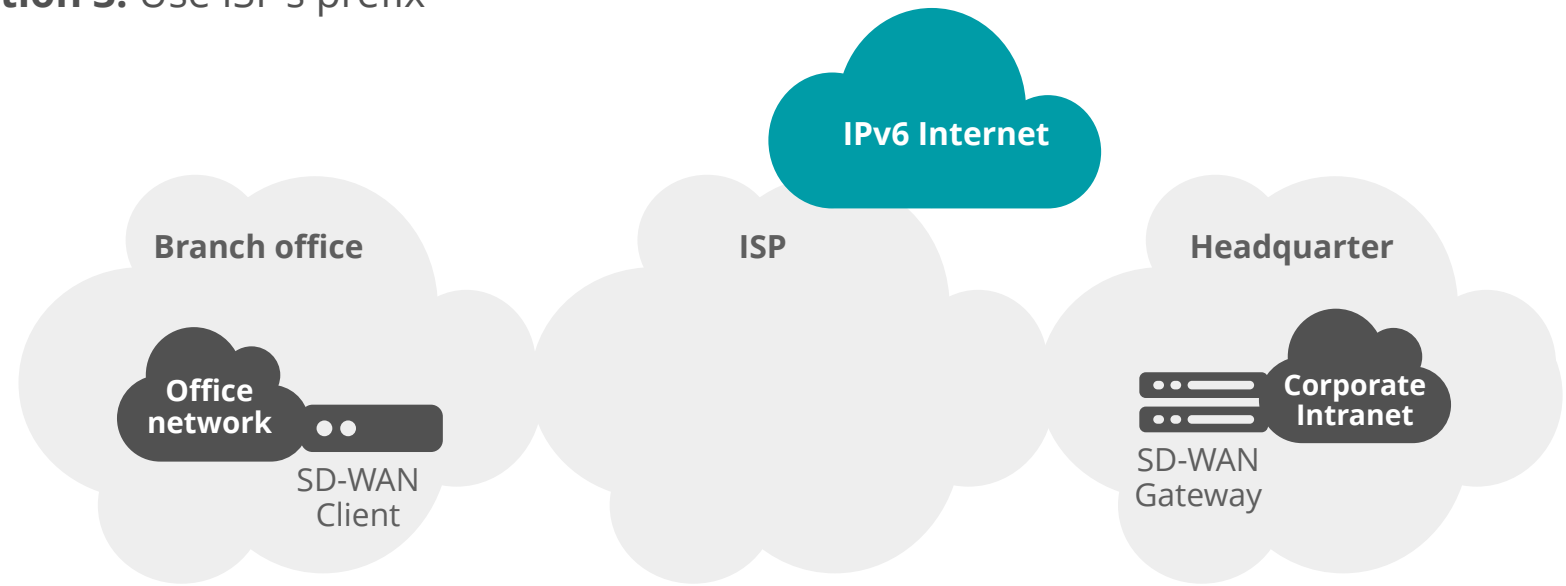
Branch office translates its prefix to ISP's PA prefix with NPTv6 to reach IPv6 Internet. Branch office reaches corporate intranet via overlay IPSec tunnels over ISP backbone *(if there is no direct connection to the headquarter via MPLS)*

ISP Announces its own prefixes to IPv6 Internet

RIR Allocation to the Enterprise 2001:0db8::/32

SD-WAN Challenges for IPv6 Deployment - II

Option 3: Use ISP's prefix



Branch office uses ISP's PA prefix and reaches IPv6 Internet with this prefix. Readdressing inside the branch office is needed in case of a service provider change. If there is a direct connection to the headquarter via MPLS then the policies should be arranged accordingly.

ISP Announces its own prefixes to IPv6 Internet

RIR Allocation to the Enterprise 2001:0db8::/32

Applications

Types of Applications to Check

In-House Developed ISP/DC Substitute Applications

- Instant messaging apps
- Video on demand apps
- Parental control apps
- Cloud Storage apps

And;

- Potentially any apps can be affected

Applications - Questions for IPv6 Support

Are there any **users** of the solution in v6?

Is the **programming language** used compatible with IPv6?

Is the **socket opening code agnostic** of the IP protocol version?

Does an application make calls via **literal address** rather than via DNS lookup?

Is there any **IP address processing** within your application? (Identifying clients by IP?)

Is RFC 8305 "**Happy Eyeballs v2**" correctly implemented to allow fast switching between the 2 protocols?

Source: ARCEP document: “Enterprises: how to deploy IPv6?”
https://www.arcep.fr/fileadmin/cru-1648459125/reprise/observatoire/ipv6/guide-entreprises-how-to-deploy-IPv6-march-2022.pdf

Important Considerations for IPv6 in Applications - I

- It is not recommended to have different applications for IPv4 and IPv6
- IPv6 address sometimes comes in addition to IPv4 - **dual-stack**
- It is **longer** than IPv4 (40 bytes vs. 20 bytes)
- An interface can carry **several IPv6 addresses** (local link, temporary routable, stable routable, etc.

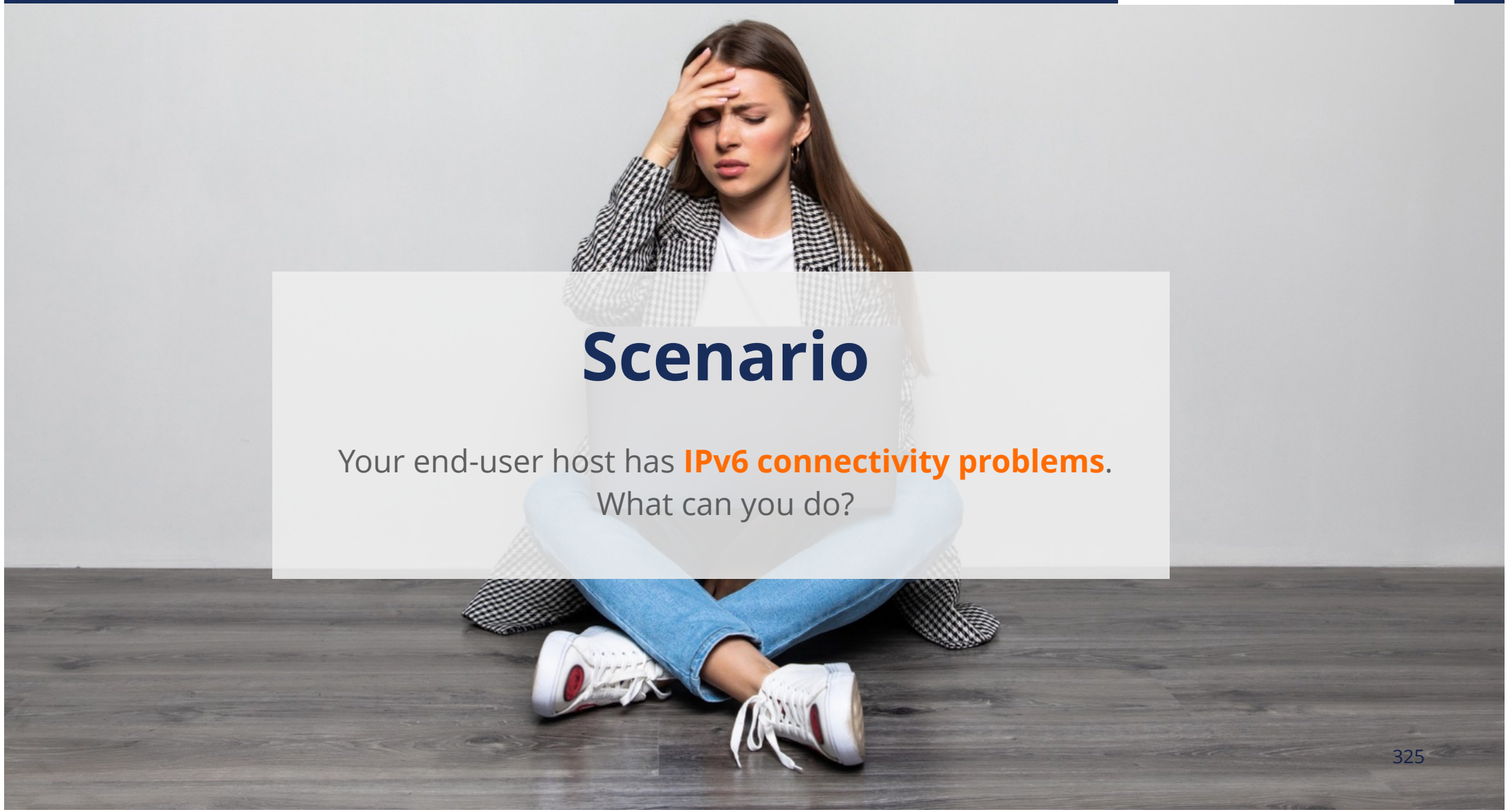
Source: ARCEP document; “Enterprises: how to deploy IPv6?”
https://www.arcep.fr/fileadmin/cru-1648459125/reprise/observatoire/ipv6/guide-entreprises-how-to-deploy-IPv6-march-2022.pdf

Important Considerations for IPv6 in Applications - II

- **Domain names and hostnames** should be used instead of IP literals inside the apps
- IP addresses shouldn't be used as the **session identifiers** - happy eyeballs cookie problem
- A **fall-back mechanism** (from one IP protocol to another) might be useful
- Be careful with the **IPv6 text representation** - there might be several variances - use the library tailored
- In case of **IP GeoLocation service** usage, make sure that your provider supports IPv6

Source: ARCEP document; "Enterprises: how to deploy IPv6?"
https://www.arcep.fr/fileadmin/cru-1648459125/reprise/observatoire/ipv6/guide-entreprises-how-to-deploy-IPv6-march-2022.pdf

Basic Troubleshooting Steps



Scenario

Your end-user host has **IPv6 connectivity problems**.
What can you do?

Steps for Troubleshooting IPv6 Connectivity

Are any of these IPv6 online test tools reachable over IPv6?

- ipv6-test.com
- test-ipv6.com
- v6.de
- bgp.tools
- doesnotwork.eu
- ip6only.me

Answer:	Actions to take:
NO	• Go to the next question in the list
YES	• This means that you can reach some of the IPv6 destinations. If you still have problem with certain IPv6 destinations, check DNS settings, routing configuration and routing tables on the default gateway and in the ISP backbone network.

Steps for Troubleshooting IPv6 Connectivity

Is the interface UP and protocol enabled? Is there any IPv6 address?

Check with ip configuration commands on the local host. For example;

- "ipconfig /all" on Windows
- "ifconfig | grep "inet6"" on MacOS
- "ip -brief -6 address" on Linux operating systems

Answer:	Actions to take:
YES	• Go to the next question in the list
NO	• Check interface configuration in the operating system level • Enable IPv6 on the interface • Restart the interface

Steps for Troubleshooting IPv6 Connectivity

What is the type of IPv6 address? (Link-local/GUA/other*?)

- If you see addresses starting with "**fe80:**", those are link-local addresses and used for on-link communication.
- If you see addresses from the range of 2000::/3, those are global unicast addresses (GUAs) and used for the communication over the Internet globally.
- For the other IPv6 address types check: https://www.ripe.net/participate/member-support/lir-basics/ipv6_reference_card.pdf

Answer:	Actions to take:
Link-Local & GUA Addresses	• Next question in the list
Only Link-Local Addresses ****In rare cases, you can see ULAs which are translated into GUA and/ or IPv4 public addresses and reaching the Internet. This is **not recommended** and not covered here.*	• Check if the configuration is set to manual on the host. If so, configure GUA addresses properly • Check if you have a router on the same link • Check if IPv6 is enabled properly on the router's LAN interface • Check if you receive a RA message from the router - packet capture • Check the option flags and the prefix(es) in the RA message - packet capture • Check if a DHCPv6 server is reachable (if M flag is on) - ping(6)

Steps for troubleshooting IPv6 connectivity

Is there any default route in the routing table?

- Check IPv6 routing table of the host to see if there is any default route. To be able to communicate over the Internet typically you should see a route* for "::/0" or "default".
- Check with ip configuration commands on the local host. For example:
  - "netsh interface ipv6 show route" on Windows
  - "netstat -nr -f inet6" on MacOS
  - "ip -6 route show" on Linux operating systems

Answer:	Actions to take:
YES	• Go to the next question in the list
NO	• Check if the configuration is set to manual on the host. If so, configure default route properly • Check if you still receive the RA messages from the router - packet capture • Check if IPv6 is still enabled on the router's LAN interface • Check if you still have a router on the same link

*It is also possible to communicate over the Internet with a route to 2000::/3, but, we cover the most generic scenario

Steps for troubleshooting IPv6 connectivity

Is the default gateway reachable?

Try to ping the default gateway's ipv6 address.
Ping with the related commands on the local host. For example;

- "ping <ipv6-address>" on Windows
- "ping6 <ipv6-address>" on MacOS
- "ping <ipv6-address>" on Linux operating systems

Answer:	Actions to take:
YES	• Next question in the list
NO	• Check if the configuration is set to manual on the host. If so, configure default route properly • Check if you still have a router on the same link • Check if IPv6 is still enabled on the router's LAN interface • Check the configuration on the router or on the firewall in between - possible ACL?

Steps for troubleshooting IPv6 connectivity

Is the prefix on the host still routed to the host's gateway from the Internet?

Check the delegated prefix on default gateway to see if it is still the same with the prefix used by the host.

Answer:	Actions to take:
YES	• Go to the next question
NO	• Restart or disable/enable the host interface to renew the IPv6 addresses used • If not, it might be related to the non-persistent ipv6 prefix delegation case. Please refer to the document; https://www.ripe.net/publications/docs/ripe-690#5-2--why-non-persistent-assignments-are-considered-harmful

Steps for troubleshooting IPv6 connectivity

Is any server, such as Google DNS server (2001:4860:4860::8844), reachable by using IPv6 literals?

Try to ping Google DNS ipv6 address.
Ping with the related commands on the local host. For example;

- “ping 2001:4860:4860::8844” on Windows
- “ping6 2001:4860:4860::8844” on MacOS
- “ping 2001:4860:4860::8844” on Linux operating systems

Answer:	Actions to take:
YES	• Go to the next question in the list
NO	• Check default gateways WAN connection if IPv6 is enabled and configured properly.

Steps for troubleshooting IPv6 connectivity

Is there any DNS configuration?

Check with the related commands on the local host. For example;

- “ipconfig /displaydns” on Windows
- “scutil --dns | grep nameserver” on MacOS
- “grep "nameserver" /etc/resolv.conf” on Linux operating systems

Answer:	Actions to take:
YES	• Next question in the list
NO	• Check if DNS is received in RA messages (RDNSS option) • Check if DHCPv6 servers send the DNS information • If it is configured manually, check and configure properly.

Steps for troubleshooting IPv6 connectivity

Is the DNS server reachable?

Ping the DNS server with the related commands on the local host. For example;

- “ping <ipv6-address>” on Windows
- “ping6 <ipv6-address>” on MacOS
- “ping <ipv6-address>” on Linux operating systems

Answer:	Actions to take:
YES	• To go the next question
NO	• Try to change the DNS server manually to any of the public DNS servers.

Steps for troubleshooting IPv6 connectivity

Does DNS reply with the correct AAAA information?

Check the replies from DNS server and compare them with replies from another server.
Use the related commands on the local host. For example:

- “nslookup -q=AAAA www.ripe.net” & “nslookup -q=AAAA www.ripe.net <new_server_IP>” on Windows
- “dig AAAA www.ripe.net” & “dig @<new_server_IP> AAAA www.ripe.net” on MacOS
- “dig AAAA www.ripe.net” & “dig @<new_server_IP> AAAA www.ripe.net” on Linux operating systems

Answer:	Actions to take:
YES	• Next question in the list
NO	• Try to change the DNS server manually to any of the public DNS servers.

IPv6 troubleshooting guide for help-desks

- **A BCOP Document** for providing a basic foundation for any user centric helpdesk that deals with IPv6 residential ISP customer connectivity
- **Helpdesks can get confused**! - No experience with IPv6 issues
- A generic **troubleshooting guide** can help!
  - Based on the open source testipv6.com tool
  - Customisable

Link to BCOP Document RIPE-631:
https://www.ripe.net/publications/docs/ripe-631