Multi-AS Small Campus Network Design

Designing and implementing a robust, scalable, and secure campus network using Huawei eNSP.

Project Overview: Building a Connected Campus

This project focuses on creating a multi-Autonomous System (AS) campus network, supporting departmental segmentation and dynamic routing. Our goal is to simulate a real-world network environment, emphasizing scalability and security.

Four Autonomous Systems

AS100, AS200, AS300, AS400 configured for departmental segmentation.

Backbone area

Integrated BGP/MPLS IP VPNs to establish secure, scalable, and isolated network segments, simulating a service provider environment.

Scalable Infrastructure

Designed for future expansion and increased user demand.

Dynamic Routing

OSPF for internal routing and iBGP for inter-AS communication.

Core Network Design Steps

A systematic approach was followed to ensure a robust and functional network.

01

Layered Topology Design

Defined Access, Aggregation, and Core layers; connected PCs to Access switches; configured trunk links.

02

VLAN Planning & Assignment

Created two VLANs per AS for departmental segmentation across all 6 switches.

03

Switch Port Configuration

Assigned user PCs to VLAN access ports; configured switch-to-switch as trunks.

04

Routing Protocol Setup

OSPF enabled within each AS; iBGP configured in AS500 for inter-AS routing.

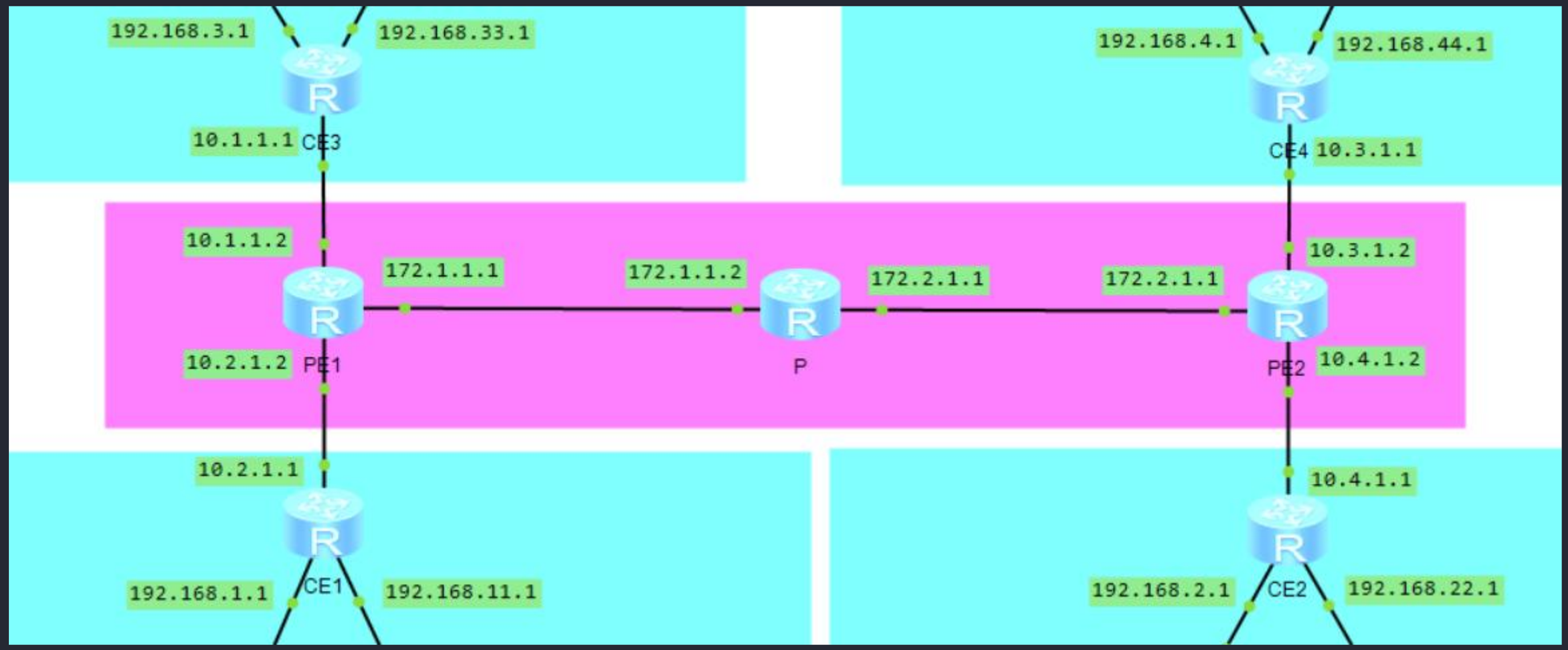
05

End-to-End Connectivity Verification

Extensive ping tests performed across VLANs and ASes to confirm full network functionality.

Network backbone

Integrated BGP/MPLS IP VPNs to establish secure, scalable, and isolated network segments, simulating a service provider environment.

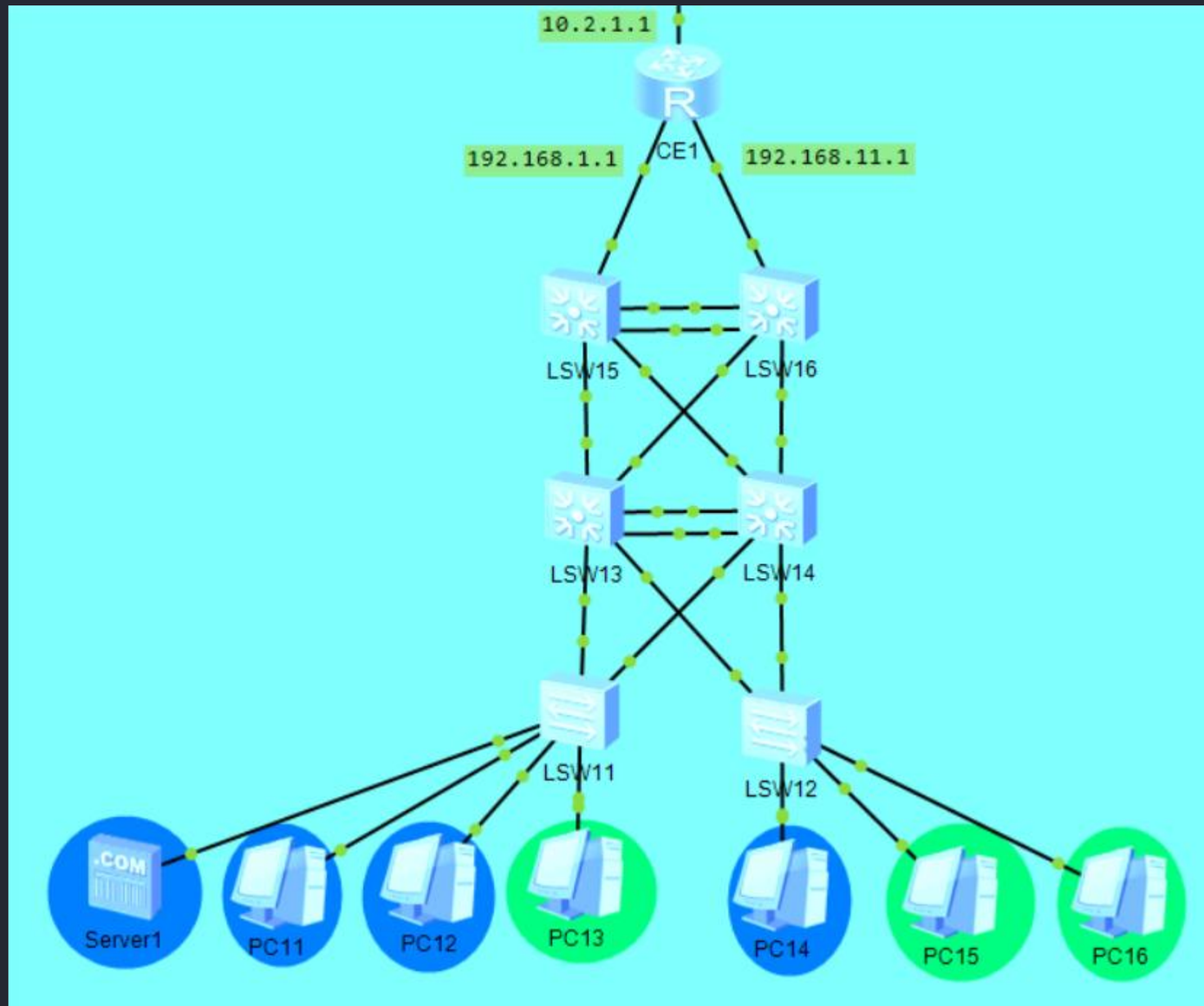


Autonomous System Architecture

Each AS is a self-contained network, mirroring a department's infrastructure, connected to a central core.

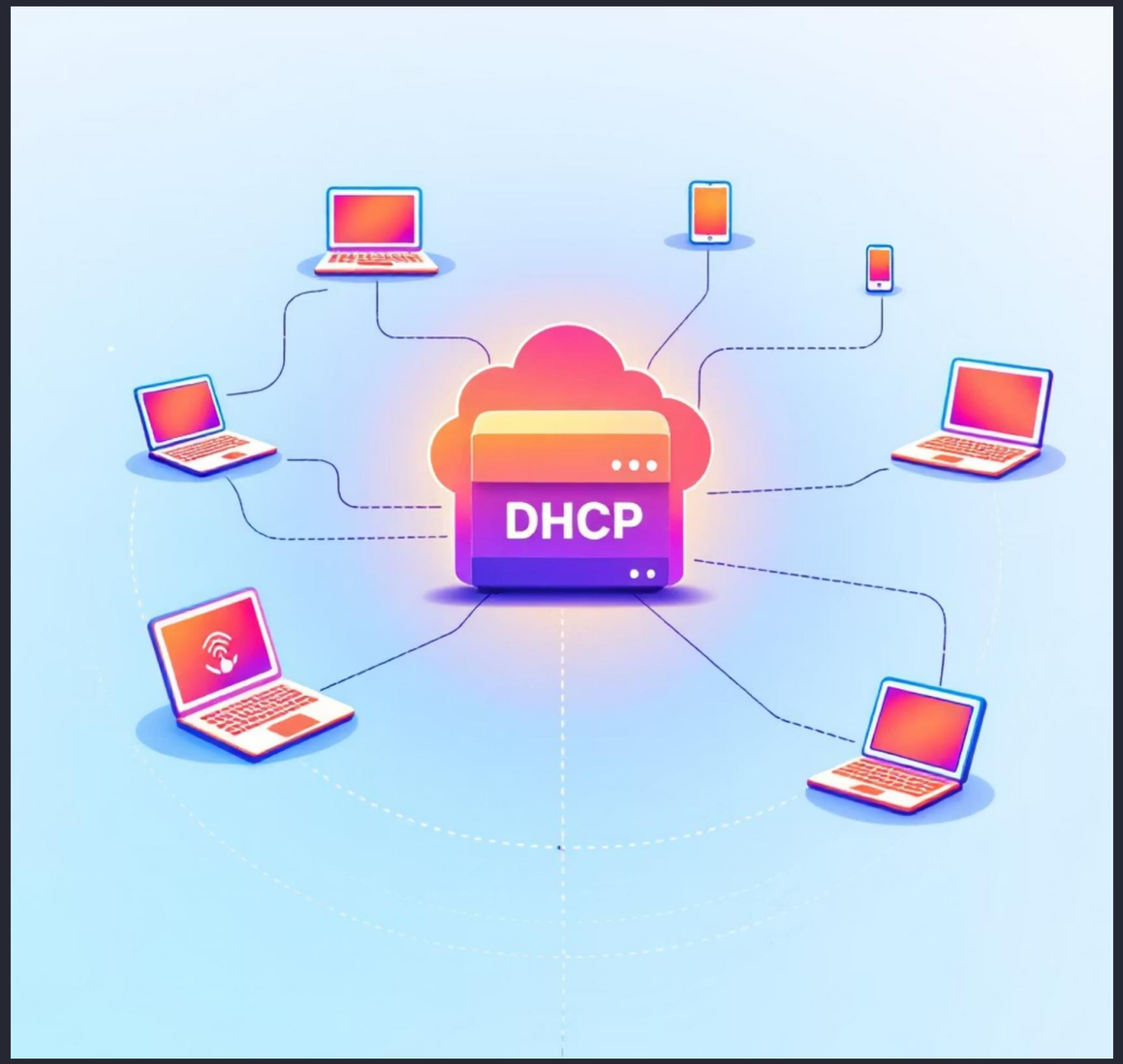
Components per AS:

- ***6 PCs:*** *End-user devices.*
- ***6 Switches:*** *2 Access, 2 Aggregation, 2 Core layers.*
- ***1 Router:*** *Running OSPF for internal routing.*
- ***1 Server:*** *Hosting essential services.*



Streamlining IP Management with DHCP

DHCP was crucial for efficient IP address assignment, reducing administrative overhead and ensuring consistent network configurations.



Key Benefits:

- ***Automated Assignment:*** *IPs, subnet masks, gateways, and DNS servers automatically distributed.*
- ***Reduced Manual Errors:*** *Minimizes misconfigurations common with static IP assignments.*
- ***Simplified Management:*** *Centralized control over IP address pools for each VLAN.*
- ***Enhanced Scalability:*** *Easily accommodates new devices without individual configuration.*

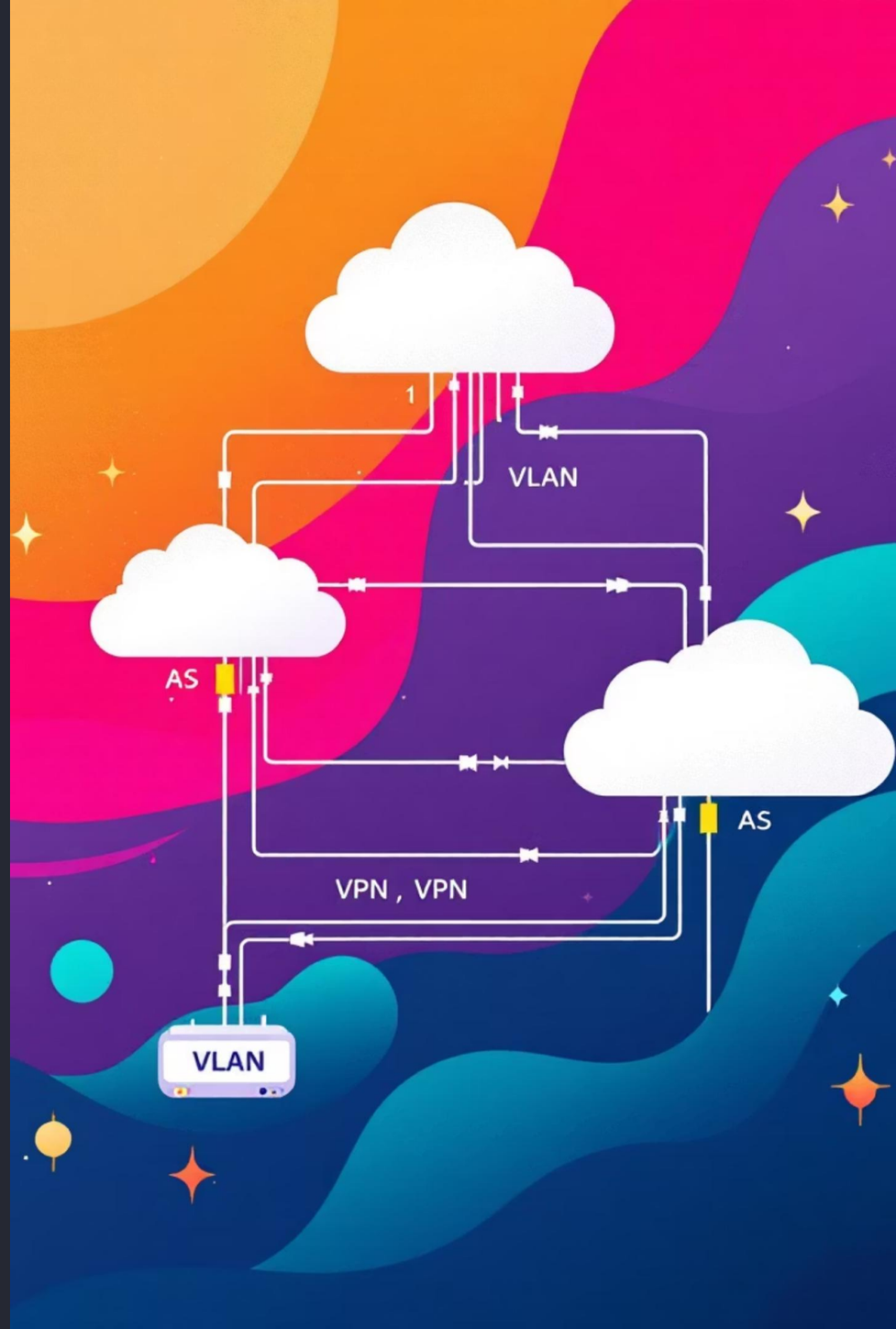
Network Design Summary

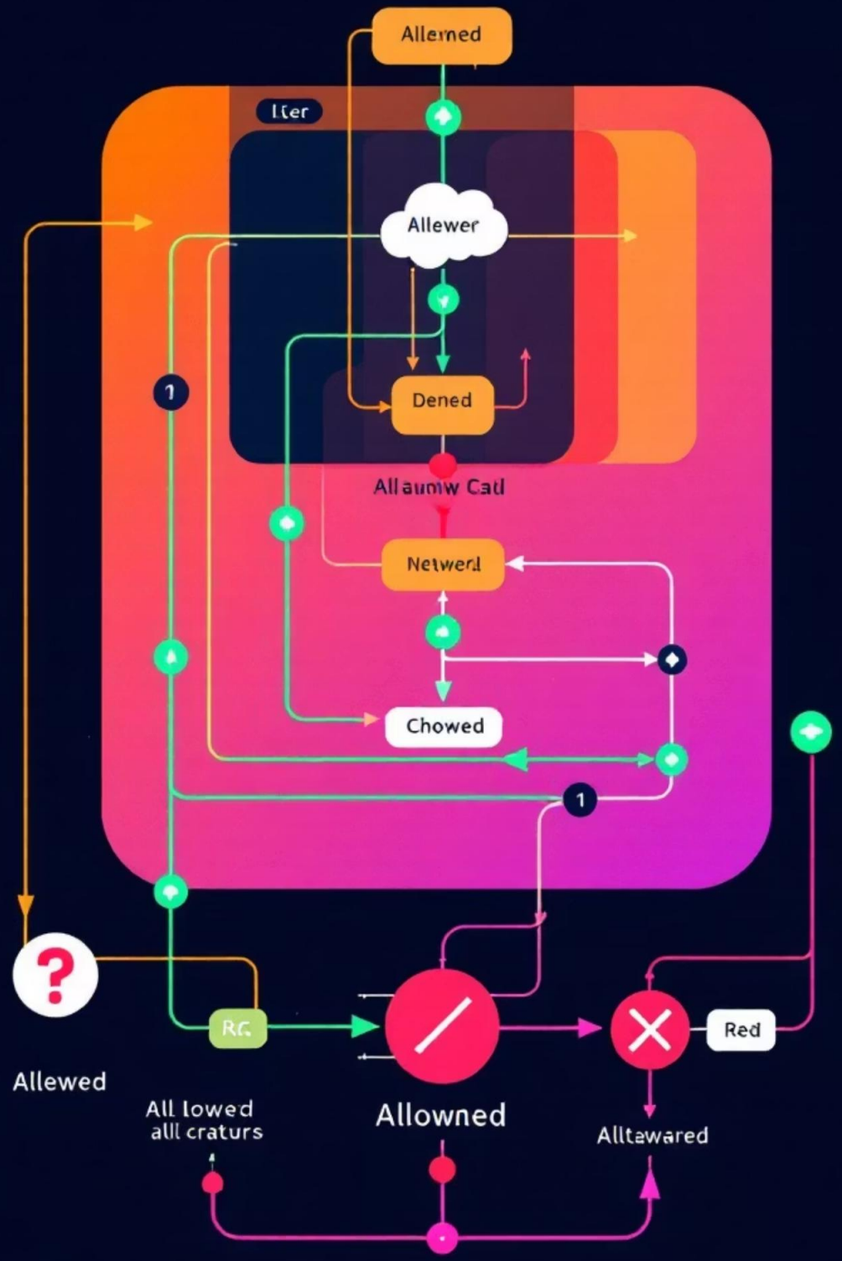
Autonomous Systems & VLANs

Each AS contains a High-Priority VLAN (HP-VLAN) for PCs and a server, and a Low-Priority VLAN (LP-VLAN) for PCs only.

AS Grouping via VPN

Four ASs are paired into two VPNs: VPN-A (AS1 ↔ AS2) and VPN-B (AS3 ↔ AS4). ASs within the same VPN can communicate, but ASs in different VPNs cannot.





Inter-VLAN & Inter-AS Communication Policy

Within the Same AS

- *HP-VLAN PCs ⇆ HP-VLAN server: Allowed*
- *LP-VLAN PCs → HP-VLAN server: Denied*

Between ASs in Same VPN

- *HP-VLAN PCs (AS1) ⇆ HP-VLAN PCs (AS2): Allowed*
- *LP-VLAN PCs (AS1) → HP-VLAN PCs (AS2): Denied*

Between VPNs

- *AS1/AS2 ↛ AS3/AS4: Fully Blocked*
- *Enforced through VPN separation + ACLs.*

VPN Implementation

Two separate VPNs ensure secure AS-to-AS tunneling, controlling traffic flow between specific VLANs.

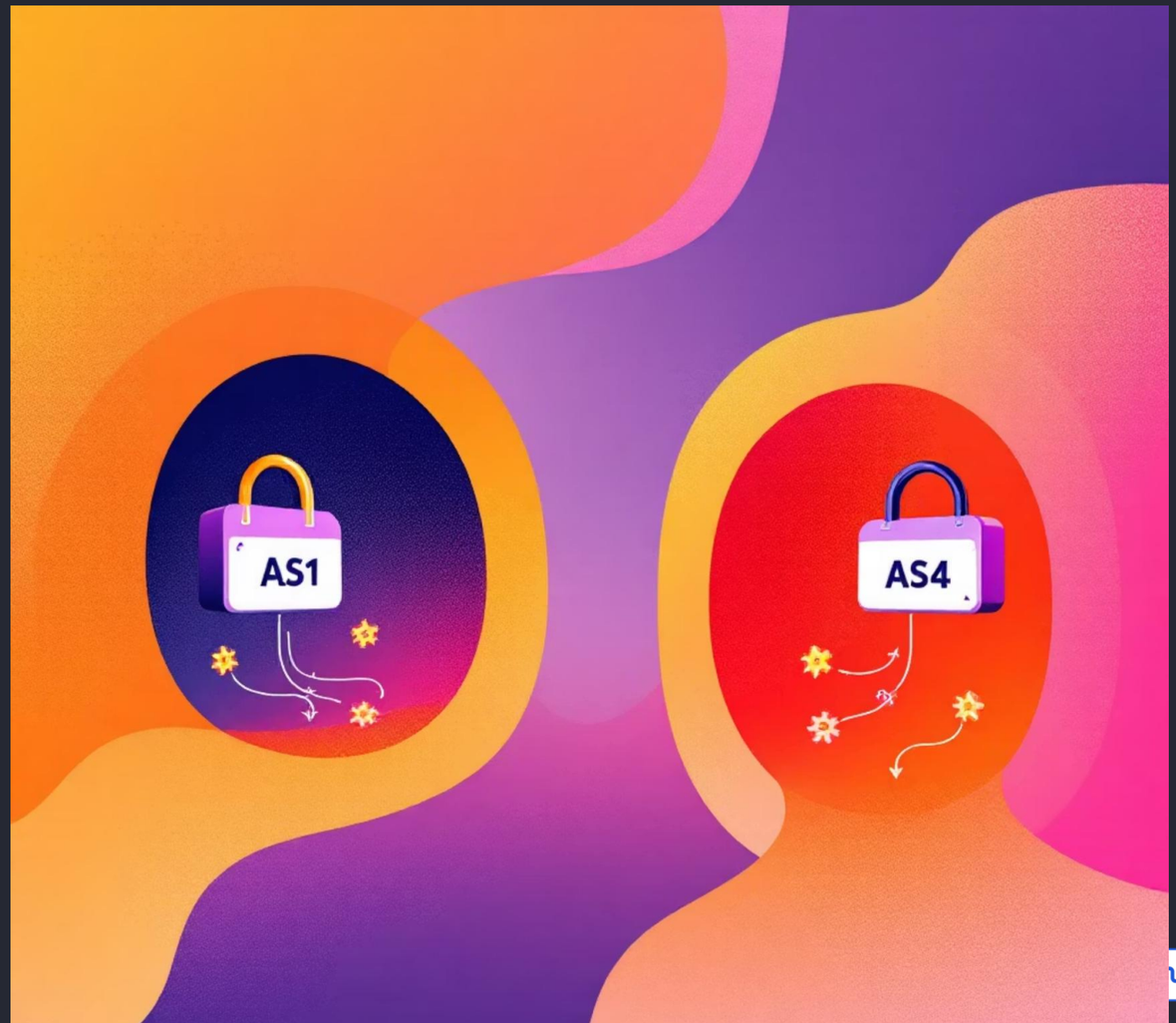
VPN-A

Connects AS1 and AS2, allowing traffic only between:

- *HP-VLAN 10 (AS1) ↔ HP-VLAN 30 (AS2)*
- *LP-VLAN 20 (AS1) ↔ LP-VLAN 40 (AS2)*

VPN-B

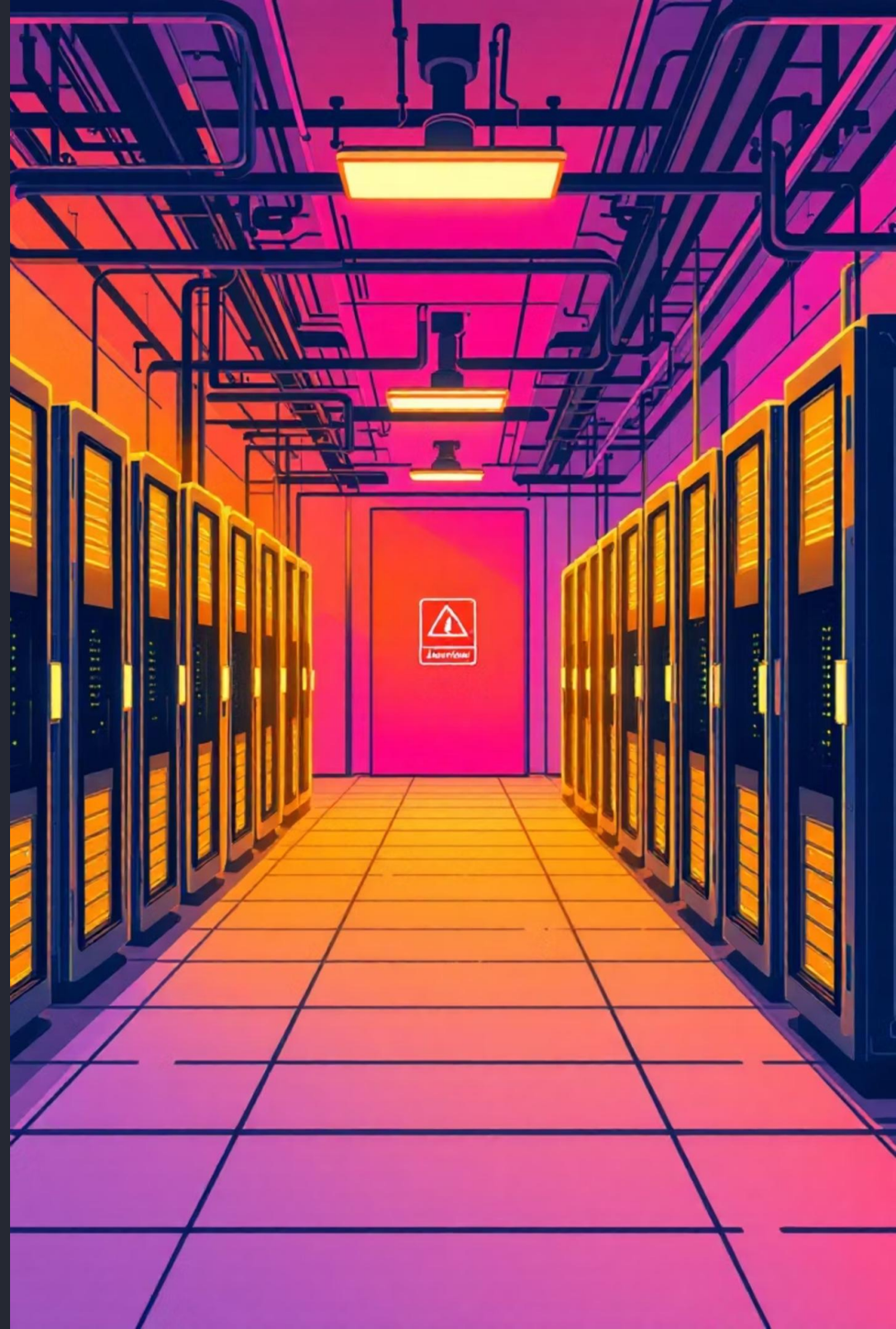
Connects AS3 and AS4 with identical communication rules, ensuring parallel secure connectivity.



Access Control List (ACL) Rules

A. Server Access Restriction

Each AS has a local server in its HP-VLAN. Only PCs within the same HP-VLAN can access their local server. All other traffic to the server is denied.



ACL Rules: Isolation

B. HP-VLAN vs LP-VLAN Isolation

ACL ensures LP-VLAN cannot access HP-VLAN (any AS) and HP-VLAN cannot access LP-VLAN (any AS). This enforces strict segmentation and prevents privilege escalation.

ACL Rules: Inter-AS Traffic Filtering

Same VPN Traffic

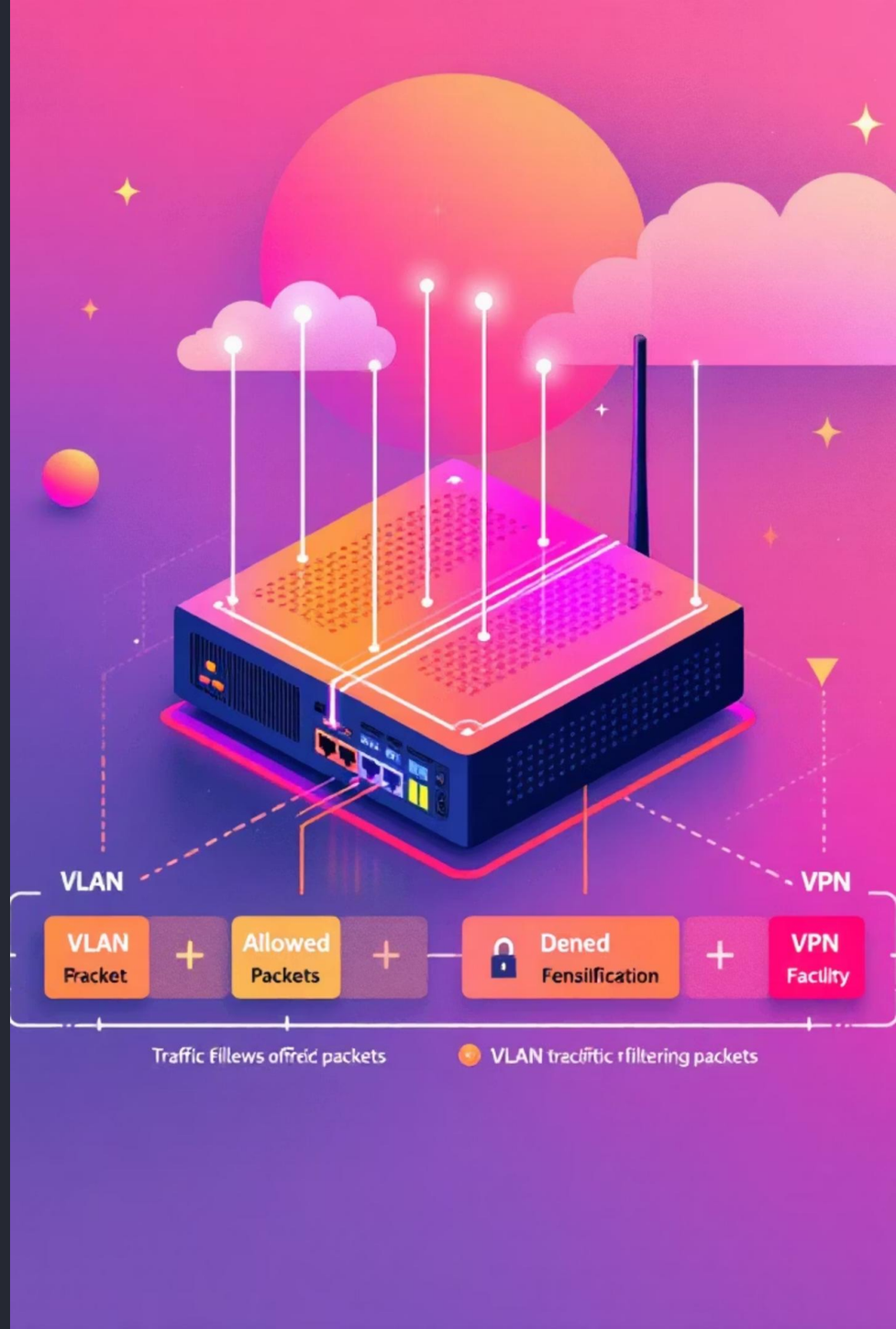
Allow HP-VLAN to HP-VLAN traffic and LP-VLAN to LP-VLAN traffic only between ASs within the same VPN.

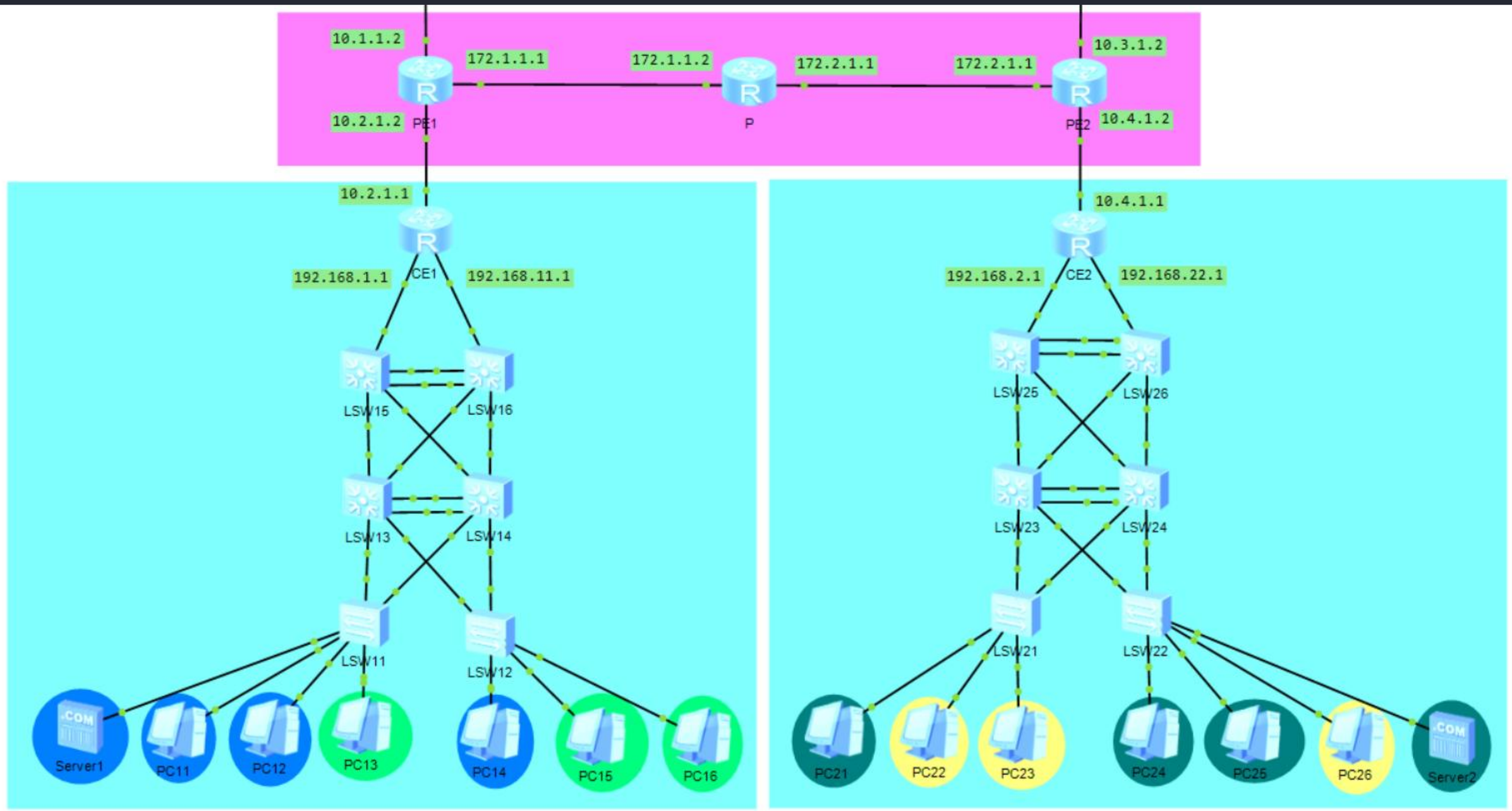
Cross-Type Communication

Deny any HP → LP or LP → HP communication.

Inter-VPN Traffic

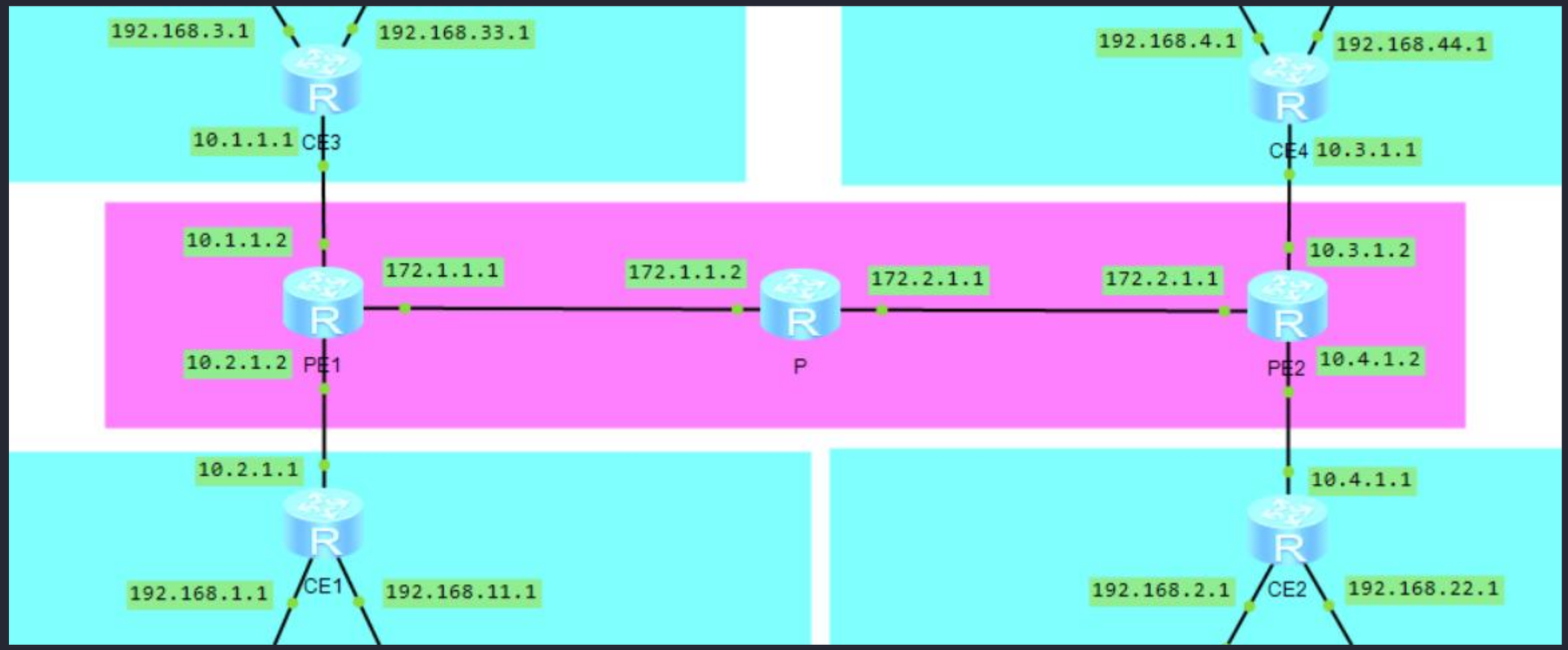
Deny all traffic toward ASs in the other VPN.





Network backbone

Integrated BGP/MPLS IP VPNs to establish secure, scalable, and isolated network segments, simulating a service provider environment.



MPLS: Multiprotocol Label Switching

MPLS is a high-performance forwarding technology that speeds up traffic flow and provides efficient network utilization by forwarding packets based on short labels instead of IP routing.

Label Switching

Packets forwarded using labels, not full IP lookups.

Label Switched Path (LSP)

Predetermined path through the MPLS cloud.

Advantages

Low latency, traffic engineering, QoS, scalable VPN support.

VPN: Virtual Private Network

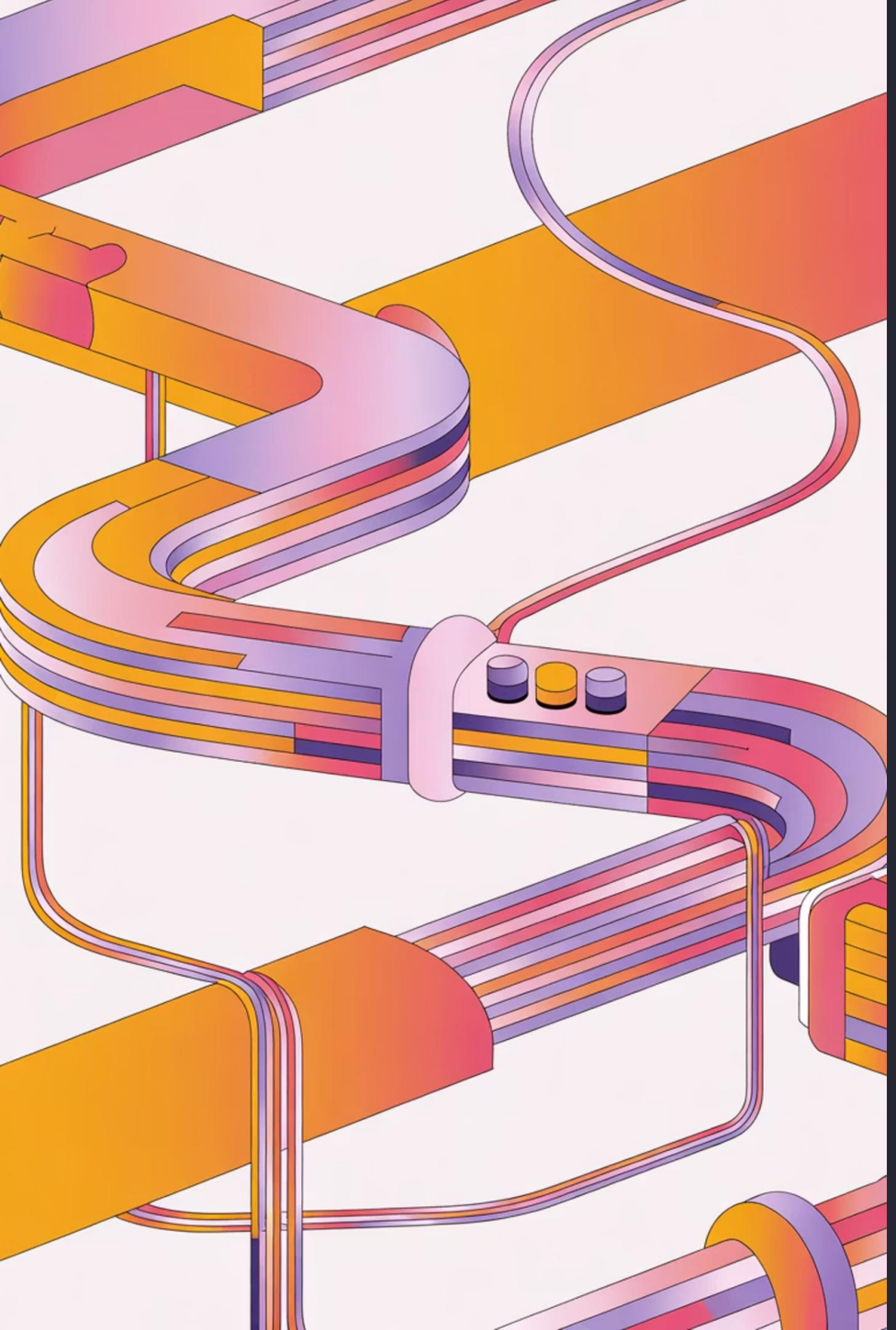
A VPN offers secure and isolated communication over a shared provider network. MPLS VPNs rely on label-based isolation rather than encryption.

Key Concepts

- ***VRF:*** *Dedicated routing table for each customer.*
- ***RD:*** *Makes customer prefixes globally unique.*
- ***RT:*** *Controls route import/export between VRFs.*

Advantages

- *Strong isolation*
- *High scalability*
- *Flexible topologies*
- *No customer-side encryption required*



BGP: Border Gateway Protocol

BGP is responsible for exchanging customer VPN routes between PE routers in MPLS networks, ensuring multi-tenant separation and scalability.

1

Why BGP?

Handles large routing tables and supports extended attributes like RDs and RTs for complete isolation.

2

Key Concepts

MP-BGP: *Transports VPNv4/VPNv6 routes.* ***VPNv4 Route:*** *Customer prefix + RD.* ***Route Target:*** *Determines VRF route reception.*

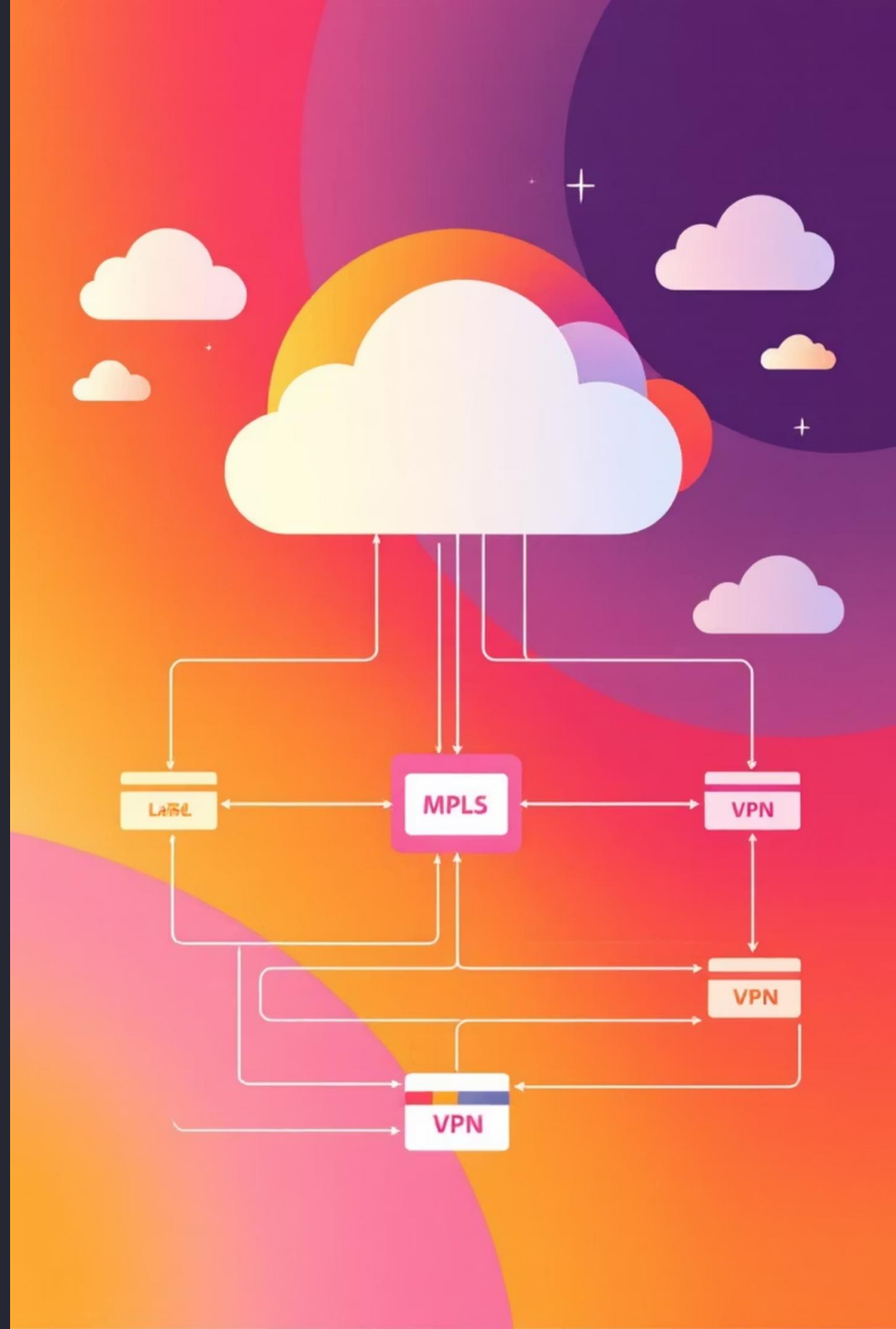
3

Role in MPLS VPNs

Exchanges VPN routes, maintains multi-tenant separation, and supports scalable, multi-customer environments.

Advanced Interconnection: BGP/MPLS IP VPN

We integrated BGP/MPLS IP VPNs to establish secure, scalable, and isolated network segments, simulating a service provider environment.



Purpose: Why BGP/MPLS IP VPN?

Virtual Private Networks

Creation of isolated virtual networks over a shared infrastructure.

Routing Domain Isolation

Ensuring complete separation and security between different routing domains.

Scalable Inter-site Communication

Enabling efficient and scalable communication across multiple sites or departments.

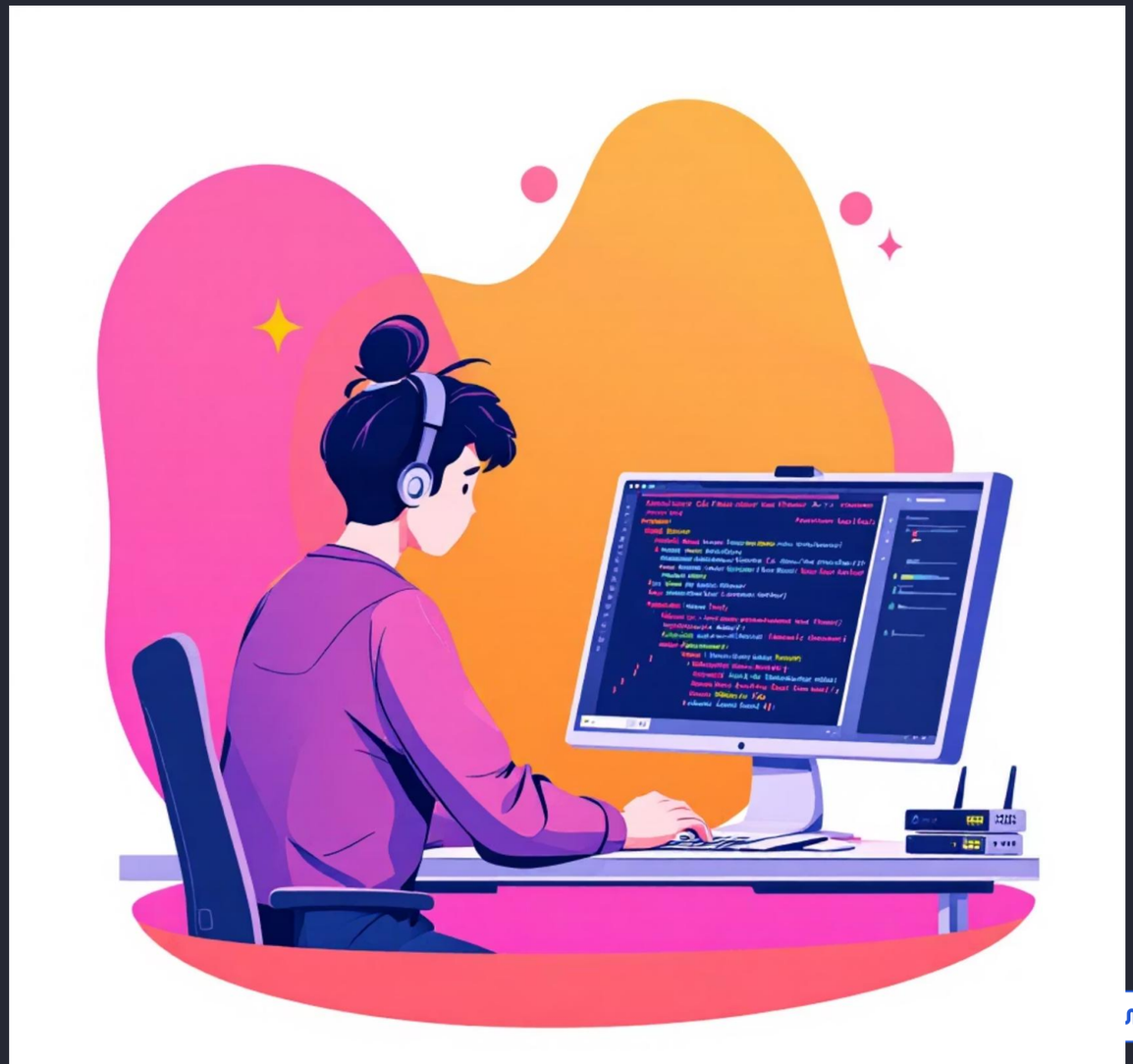
ISP Simulation

Realistic simulation of service provider operations for educational purposes.

Implementation: Bringing MPLS VPN to Life

The implementation involved configuring several key components to create the VPN functionality.

- ***MPLS Activation:*** *Enabled on backbone routers for label switching.*
- ***VRF Creation:*** *Virtual Routing and Forwarding instances to segregate customer routing tables.*
- ***MP-BGP Configuration:*** *Multiprotocol BGP between Provider Edge (PE) routers to exchange VPN routes securely.*
- ***LSP Establishment:*** *Label Switched Paths across the provider core for high-speed packet forwarding.*



Achieved Benefits: Advanced Network Functionality

The BGP/MPLS IP VPN implementation provided significant advantages for the campus network.

1

Secure Routing

Guaranteed separation of routing tables for different network segments.

2

Optimized Routing

Efficient data forwarding through MPLS label switching.

3

Scalable Design

Easily accommodates growth for multiple branches or customer networks.

4

Realistic Simulation

Hands-on experience with ISP-level VPN service provisioning.

Concluding Thoughts: A Foundation for Future Networks

This project successfully incorporated advanced service provider technologies, demonstrating end-to-end connectivity within a modern MPLS VPN architecture. The design serves as a robust foundation for more complex network scenarios.

The comprehensive design and implementation process provided valuable insights into building scalable, secure, and manageable enterprise-level networks.