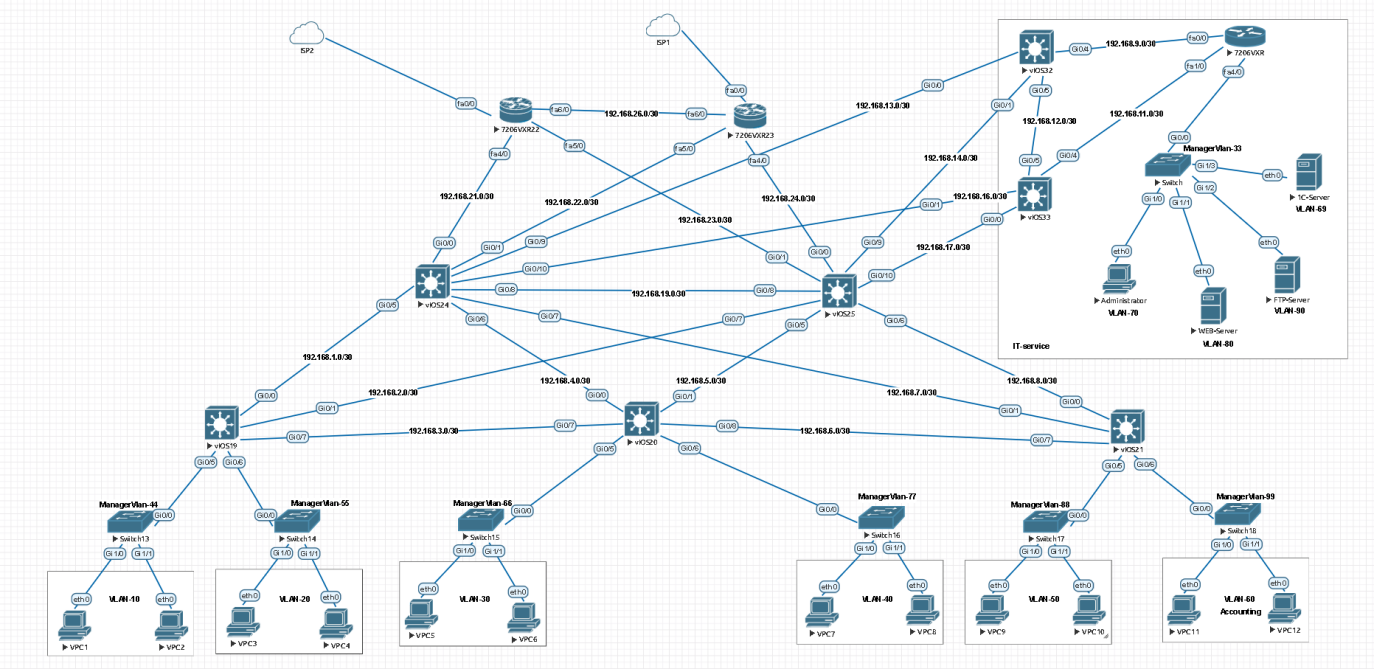
AuroraShield Enterprise Campus: Dual-ISP Resilient Network with Secure Multi-VLAN Services



Batumi-2025

Table of Contents

1. Executive Summary

This document presents the design, implementation and validation of the **AuroraShield Enterprise Campus Network** – a fully functional multilayer Cisco architecture built to demonstrate secure, resilient and scalable connectivity for a modern medium-to-large organization.

The network has been implemented and tested in a virtual lab using Cisco IOS routers, multilayer switches and Layer-2 access switches. It features:

- **Dual-ISP WAN edge** with dynamic failover and intelligent path selection using OSPF and IP SLA.
- **Multilayer campus core** built on vIOS L3 switches, interconnecting multiple buildings and user zones over routed /30 point-to-point links.
- **Segmented access layer** with dedicated VLANs for each user group (VLANs 10, 20, 30, 40, 50, 60) and separate management VLANs (44, 55, 66, 77, 88, 99).
- **Isolated IT-services zone**, hosting Web, FTP and business-critical application servers, together with a dedicated Administrator workstation in VLAN 70.
- **Comprehensive Layer-2 hardening** using DHCP snooping, port-security with sticky MAC, BPDU Guard and err-disable recovery to protect against common campus attacks and misconfigurations.
- **Centralized, yet Windows Server–free control plane**: all core services (routing, DHCP, security, redundancy) are implemented directly on Cisco devices, while a single Administrator PC running Windows 10 Pro in VLAN 70 is used as the logical control center through SSH/HTTPS management tools.

The goal of this project is to show that a carefully engineered Cisco-centric design can deliver carrier-grade resilience and security without relying on heavyweight server infrastructure, while still remaining clear, maintainable and ready for future expansion.

2. Author Profile

Author: *Imeda Sheriphadze*
Date of birth: 1968, Georgia

I am an **Information Technology and Software Engineering specialist** with more than **30 years of professional experience** designing, deploying and operating complex IT infrastructures.

Over the last decade I have additionally focused on **Neural Network Architecture and Applied AI**, designing AI-driven solutions that integrate with real-world systems – from computer networks and cybersecurity to 3D modeling, interior design and image generation.

This project combines both of my core strengths:

1. **Enterprise-grade Cisco networking**, and
2. **System-level thinking inspired by neural-network design** – modular, resilient and highly automated.

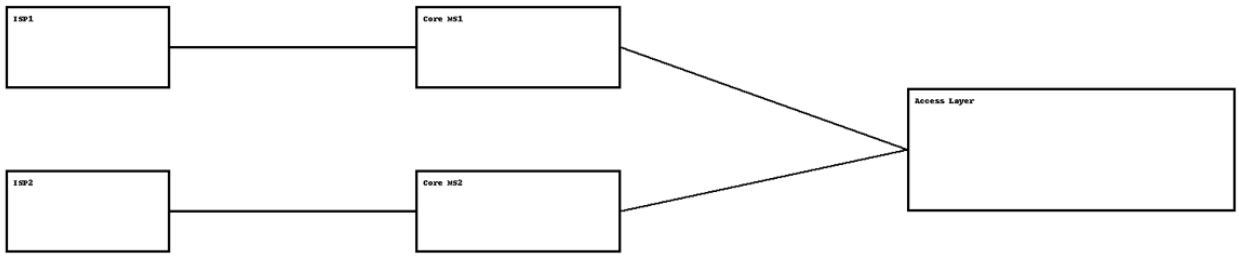
The AuroraShield Enterprise Campus Network is not only a technical lab, but also a demonstration of my engineering philosophy: **simple in operation, rich in capabilities, and ready for intelligent automation.**

3. Project Objectives

The main objectives that guided this design were:

1. **High Availability and Redundancy**
    - Provide continuous connectivity to the Internet through **two independent ISPs**.
    - Ensure fast convergence and deterministic failover using OSPF, IP SLA and default-route injection.
2. **Scalable Campus Segmentation**
    - Build a **multilayer campus topology** with clear separation between core, distribution and access layers.
    - Use **dedicated VLANs** for each user group and each management domain.
3. **Strong Security at Both Layer-2 and Layer-3**
    - Protect the access layer with port-security (sticky MAC), DHCP snooping, BPDU Guard and err-disable recovery.
    - Secure routing with OSPF message-digest authentication and strict NAT boundaries between internal and external zones.
4. **Operational Simplicity Without Windows Server**
    - Implement **all infrastructure services (routing, DHCP, NAT, security)** on Cisco routers and switches.
    - Use a single **Administrator PC in VLAN 70** as the operational control center, running management software on Windows 10 Pro.
5. **Clarity, Documentation and Reusability**
    - Produce a **clean, standards-aligned configuration** for every device.
    - Provide documentation that can be used as a template for real customer deployments or as a reference for Cisco certification scenarios.

4. High-Level Network Architecture



4.1 Logical Topology

The topology represents a single enterprise campus with:

- **Two upstream ISPs**, each connected to a **7206VXR edge router** (PERIMETER-FW1 and PERIMETER-FW2).
- **Core layer** formed by two central multilayer switches (MS1 and MS2) and additional L3 switches (MS3, MS4, MS5) interlinked via /30 routed point-to-point connections.
- **Access layer** consisting of six Layer-2 switches (SWITCH1–SWITCH6) serving user VLANs in different departments (Sales, HR, Management, Accounting, etc.).
- **IT-service block** on the right side, with its own L3 devices (IT-core and Admin switch), hosting Web, FTP and business application servers as well as the Administrator workstation.

All inter-device links in the core and distribution layers use small **/30 or /31 networks**, while user VLANs use larger /24 networks reserved per department.

4.2 VLAN and Addressing Plan (Summary)

- **User VLANs**
  - VLAN 10 – User Segment 1
  - VLAN 20 – User Segment 2
  - VLAN 30 – User Segment 3
  - VLAN 40 – User Segment 4

  - VLAN 50 – User Segment 5
  - VLAN 60 – Accounting and finance segment
- **Management VLANs**
  - VLAN 44, 55, 66, 77, 88, 99 – separate Mgmt networks for each access switch group.
- **IT-Services VLANs**
  - VLAN 33 – Manager/IT core
  - VLAN 69 – Business application server (1C / ERP)
  - VLAN 80 – Web server
  - VLAN 90 – FTP server
  - VLAN 70 – Administrator workstation (Windows 10 Pro control center)

Each user VLAN has its default gateway on the corresponding multilayer switch (SVI), and these gateways participate in OSPF area 0. The ISP routers advertise a default route into the campus, while internal networks are summarized and advertised from the core as needed.

5. WAN Edge and Dual-ISP Design

The Internet edge is built on two Cisco 7206VXR routers:

- **PERIMETER-FW1** – preferred Internet gateway (ISP1)
- **PERIMETER-FW2** – backup Internet gateway (ISP2)

Key features:

1. **OSPF with MD5 Authentication**
    - Both routers participate in **OSPF process 50** with area 0 authentication message-digest and individual ip ospf message-digest-key statements on each LAN interface.
    - Only the LAN-facing interfaces are enabled as non-passive, while all others remain passive for safety.
2. **Default-Route Injection**
    - Each 7206VXR advertises the default route into OSPF using default-information originate, allowing the campus core to dynamically learn gateway availability.
3. **NAT and Security Boundary**
    - An extended standard ACL **FOR-NAT** defines all internal prefixes allowed to exit to the Internet.
    - NAT is performed with ip nat inside source list FOR-NAT interface FastEthernet0/0 overload, turning the WAN interface into a secure demarcation point between public and private address spaces.
4. **IP SLA–based Path Monitoring**
    - On PERIMETER-FW1, **IP SLA 18** performs ICMP echo probes towards **8.8.8.8** sourced from the WAN interface, tracking upstream reachability and delay.
    - On PERIMETER-FW2, a similar IP SLA monitors the reachability of FW1's internal address, ensuring that backup activation reflects real path health.

This combination of OSPF, IP SLA and policy-controlled NAT gives the campus **carrier-grade redundancy** and a clear security boundary.

6. Campus Core and Distribution Design

The core/distribution layer uses several vIOS L3 switches, each with a clear role:

- **MS1 and MS2 (top center)** – primary distribution/core switches, aggregating links from the edge routers and from MS3/MS4/MS5.
- **MS3, MS4, MS5 (middle layer)** – regional L3 nodes that terminate user VLANs and connect to the lower access switches.

Design characteristics:

1. **Routed Point-to-Point Links**
    - All inter-switch uplinks use /30 networks with OSPF enabled and a cost that reflects the desired primary/backup paths.
2. **Gateway SVIs for User VLANs**
    - Each user VLAN default gateway is implemented on the appropriate L3 switch using interface VlanXX with /24 addressing.
    - OSPF advertises these VLAN networks across the campus, providing full IP reachability.
3. **Single OSPF Area for Simplicity**
    - For this lab, a single **area 0** has been chosen to keep the control plane simple and transparent, while still using MD5 authentication to emulate real-world security practices.

The result is a **highly modular core**, where each L3 node can be documented and managed independently, while OSPF ensures automatic route distribution and convergence.

7. Access Layer and User Segmentation

The six access switches (SWITCH1–SWITCH6) are almost identical in structure, following a strict security and configuration template:

1. **Trunk to Distribution Switch**
    - Each access switch uses **GigabitEthernet0/0** as an 802.1Q trunk towards its L3 parent, allowing selected VLANs and a dedicated management VLAN.
2. **Secure Access Ports**
    - User-facing ports are configured as **access ports** with:
        - switchport port-security violation restrict
        - switchport port-security mac-address sticky
        - switchport port-security aging time 5 with aging type inactivity
    - This prevents MAC-flooding and unauthorized device replacement, while still allowing minimal operational flexibility.
3. **DHCP Snooping and Trusted Uplinks**
    - DHCP snooping is globally enabled, with only the uplink trunk towards the L3 switch marked as **trusted**; all access ports remain untrusted and may enforce rate limits.
4. **Spanning-Tree Protection**
    - **PVST** is used with spanning-tree portfast edge default on access ports and **BPDU Guard** enabled to shut down misconfigured or malicious switches.

This template turns the access layer into a **strong first line of defense**, keeping the core safe from user-side incidents.

8. IT-Services Zone and Administrator Control Center

The IT-services block on the right side of the topology is intentionally designed as a **separate security and management domain**.

- A dedicated L3 switch (IT-core) connects to the campus via routed /30 links and trunks that carry VLANs 33, 69, 70, 80, 90 and 100.
- A subordinate switch (AdminSwitch) provides access ports for:
  - **Web server** (VLAN 80)
  - **FTP server** (VLAN 90)
  - **Business application / 1C server** (VLAN 69)
  - **Administrator PC** (VLAN 70)

Each of these ports inherits the same Layer-2 protections as user switches (port-security, BPDU Guard, DHCP snooping), but additionally they serve as **critical infrastructure endpoints**.

8.1 Windows 10 Pro Administrator Workstation (VLAN 70)

In this design there is **no Windows Server domain controller or DHCP server**. Instead:

- All IP address management and gateway functions are served by Cisco devices.
- The **Administrator PC in VLAN 70** runs Windows 10 Pro and hosts:
  - SSH and HTTPS clients for switch/router management,
  - Potential monitoring and automation tools (for example, Python scripts, NMS software, syslog viewers).

This approach demonstrates that a **lean, network-centric architecture** can still deliver excellent manageability without the overhead of server infrastructure, while also being ready for future AI-based management tools.

9. Security Architecture Overview

Security is woven into every layer of the design:

1. **Control-Plane Security**
    - OSPF authentication with MD5 prevents unauthorized routing updates.
    - Edge routers and switches use local AAA with privilege-15 accounts and enable secret for administrative access.
2. **Data-Plane Security**
    - NAT ACL FOR-NAT is the only list of prefixes allowed to reach the Internet, preventing address spoofing and leakage of unknown subnets.
    - Future extensions may include CBAC/Zone-Based Firewall, IPS or external security appliances without altering the current addressing plan.
3. **Layer-2 Security**
    - DHCP Snooping, Port Security, BPDU Guard and err-disable recovery are consistently applied across access and server switches, creating a hardened campus edge.

Overall, the design follows Cisco best practices for campus security while remaining clear and auditable.

10. Testing and Validation

The following tests have been performed in the EVE-NG environment to validate the design:

1. **End-to-End Connectivity**
    - Clients in all user VLANs (10–60) successfully obtain addresses from DHCP and reach both internal servers and the Internet.
    - Traceroute confirms correct routing through the nearest L3 switch and then through the active ISP router.
2. **Dual-ISP Failover**
    - When the primary ISP path is disrupted, the IP SLA on PERIMETER-FW1 marks the probe as failed; OSPF withdraws the default route, and traffic automatically shifts to PERIMETER-FW2, with minimal packet loss.
3. **Security Controls**
    - Plugging an unauthorized switch into a user port triggers BPDU Guard, placing the port into err-disable state.
    - Attempting DHCP spoofing from a user port is blocked by DHCP snooping on untrusted interfaces.
    - Moving a user's cable to a different port without authorization is blocked by port-security sticky MAC address binding.
4. **Management Path**
    - From the Administrator PC in VLAN 70 it is possible to securely reach every core, distribution, access and edge device using SSH or HTTPS, while users in regular VLANs have no direct access to the management plane.

These tests confirm that the design is **operationally sound, resilient and secure**.

11. Future Enhancements

The architecture is intentionally built with room for further growth and integration. Possible future steps include:

- Introducing **HSRP/VRRP** on user gateway SVIs for first-hop redundancy.
- Adding a dedicated **syslog and NetFlow collector**, potentially implemented as a lightweight Linux VM in the IT-services zone.
- Integrating **AI-driven monitoring and anomaly detection**, leveraging my experience in neural networks to analyze NetFlow, syslog and SNMP data for early detection of threats or performance issues.
- Implementing **role-based access control** via TACACS+/RADIUS servers once a small server farm is introduced.

12. Conclusion

The **AuroraShield Enterprise Campus Network** demonstrates how a carefully planned Cisco-based design can deliver:

- **High availability** through dual-ISP connectivity and dynamic failover,
- **Strong security** at Layers 2 and 3,
- **Clear segmentation** for users, management and IT-services, and
- **Operational simplicity**, even without traditional Windows Server infrastructure.

This project reflects my engineering approach as **Imeda Sherifadze** – combining decades of practical networking experience with an AI-driven mindset to build infrastructures that are robust today and ready for tomorrow.

Project author:

Imeda Sheriphadze

Information technology and software specialist and specialist in neural network design and its application in modern life

e-mail: isheriphadze@gmail.com

Mobile / WhatsApp: +995(555)45-92-70