Layer 3 Switch Security & Network Configuration Guide

1. VLAN Configuration

VLANs (Virtual Local Area Networks) allow logical segmentation of a network within the same physical infrastructure. This helps improve security, performance, and manageability by isolating broadcast domains. Each department or group can be placed in its own VLAN to limit unnecessary traffic.

2. Inter-VLAN Routing

By default, VLANs cannot communicate with each other. Inter-VLAN routing enables traffic to flow between different VLANs by using a Layer 3 switch and configuring Switch Virtual Interfaces (SVIs). This is crucial for communication between departments while maintaining isolation.

3. ACL Configuration

Access Control Lists (ACLs) are used to filter network traffic based on IP addresses, protocols, and ports. Applying ACLs enhances security by only allowing legitimate traffic and blocking unauthorized access to specific VLANs or resources.

4. Port Security

Port security restricts access to a switch port by allowing only known devices based on MAC addresses. This prevents unauthorized devices from connecting to the network and helps detect and log violations, increasing access control at the hardware level.

5. 802.1X Authentication

802.1X is a port-based network access control protocol that requires devices to authenticate before accessing the network. Combined with RADIUS, it ensures that only authorized users or devices can connect, supporting enterprise-level security policies.

6. DHCP Snooping

DHCP snooping prevents rogue DHCP servers from distributing IP addresses. It acts as a filter that allows DHCP messages only from trusted ports. This helps protect the network from attacks like DHCP spoofing and IP address conflicts.

7. Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection protects against ARP spoofing attacks by validating ARP packets against known IP-to-MAC bindings. It ensures devices cannot impersonate others, which is essential in preventing man-in-the-middle (MITM) attacks.

8. Syslog Logging

Syslog enables centralized logging of system events and errors. By directing log messages to a syslog server, administrators can monitor and audit network activity, helping in troubleshooting and identifying security incidents quickly.

9. SNMP Configuration

Simple Network Management Protocol (SNMP) is used for monitoring and managing network devices. By setting SNMP communities and trap receivers, you enable real-time alerts and performance tracking, which is vital for maintaining uptime and security.

Additional Security Best Practices

Firewall & ACLs: A firewall acts as the first line of defense by filtering traffic based on defined rules.
Secure Wireless Networking: Use WPA3 or WPA2-Enterprise and isolate guest traffic.
Network Access Control (NAC): Enforce 802.1X with RADIUS/TACACS+.
IDS/IPS: Deploy tools like Snort for detection and Suricata for prevention.
Endpoint Security & Patch Management: Keep antivirus updated and patch systems regularly.
Secure Remote Access: Use VPNs and enable Multi-Factor Authentication.
Logging & Monitoring: Use SIEM tools and enable alerts for anomalies.
Physical Security: Lock network devices and use RFID or biometrics.
Security Awareness Training: Train staff regularly on threats and best practices.

References

- Cisco - Layer 3 Switch Inter-VLAN Routing Without Router: https://www.cisco.com
- Cisco - Configuring Network Security with ACLs: https://www.cisco.com
- Cisco - Configuring IEEE 802.1X Port-Based Authentication: https://www.cisco.com
- Cisco - Configuring Dynamic ARP Inspection: https://www.cisco.com
- Cisco - Small Business Network Security Checklist: https://www.cisco.com/c/en/us/solutions/small-business.html
- FTC - Cybersecurity for Small Business: https://www.ftc.gov/business-guidance/resources/cybersecurity-small-business
- CISA - Cyber Guidance for Small Businesses: https://www.cisa.gov/resources-tools/resources/cyber-essentials

- Intel - Small Business Cybersecurity Best Practices: https://www.intel.com
- SBA.gov - Strengthen your cybersecurity: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity
- PurpleSec - Security Awareness and Password Policies: https://purplesec.us