White Paper

Using VLAN’s in Network Design

Kevin Colo
December, 2012
1. Background

To this day, end users still ask if VLANs (Virtual LANs) are a fundamentally secure technique for isolating networks.

The answer: Yes.

VLAN hopping (the ability to gain access to a different VLAN than the one you are supposed to) was a large security concern about 12 years ago. Today, these legacy exploits are well understood and are mitigated using proper network device configuration.

The idea of using a separate physical switch for different security domains is no longer prevalent in modern enterprise campus networks. At the enterprise edge, separate switches have been displaced by VLANs, multi-context firewalls, and consolidated chassis implementations.

Today, when a “one switch per VLAN” design is used, it typically implies:

- The “Outside” switch of an internet connection, and sometimes the “DMZ” switch. Even in this case, it is now common to have multiple DMZs separated using VLANs.
- A desire to do things, “the way we did it last time”.
- A desire to not have equipment be audited (e.g., in-scope for PCI compliance)
- Specific internal network policy that when researched, hasn’t been updated in many years.

VLANS are safe to use for network security isolation, but like anything else, network devices must be configured correctly using standard best practices. There are many documentation references available to assist in the proper configuration of network devices.

From RFC 4554:
Ethernet VLANs are quite commonly used in enterprise networks for the purposes of traffic segregation.

From Wikipedia:
There are two primary methods of VLAN hopping: switch spoofing and double tagging. Both attack vectors can be easily mitigated with proper switchport configuration.

The V stands for Virtual

The use of VLANs ranges from the well-known LAN switches to firewalls, wireless APs, virtual switches in virtualized environments, to the underlying customer isolation techniques used by Internet Service Providers. Modern network designs would not be possible without the use of VLANs for traffic and security segmentation. Service Providers offer VPLS, MPLS, and 802.1QnQ services that leverage VLANs (and in the case of MPLS/VPLS, Virtual Routing/Forwarding VRF) for customer isolation.

Long before virtualization became a buzzword, VLANs were used as fundamental component of network virtualization. 1 switch + 2 networks = virtualization. Virtualization technologies assume the consolidation of physical hardware assets for a large number of well-known reasons (power, efficiency, management, etc.) These reasons carry over to why VLANs are so popular and trusted as a network security isolation technique.
It took a bit of training and experience, but today’s IT departments have embraced the idea of taking one piece of hardware, separating it into multiple logical domains, and leveraging it more efficiently.

Always follow the manufacturer’s configuration recommendations for all network devices. For instance, mitigating VLAN hopping attacks on LAN switches typically comes down to:

1. Always use a dedicated VLAN ID for all trunk ports.
2. Disable unused ports and put them in an unused VLAN.
3. Do not use VLAN 1 for anything.
4. Disable auto-trunking on user facing ports (DTP off).
5. Explicitly configure trunking on infrastructure ports.
6. Use all tagged mode for the native VLAN on trunks.
7. Use PC voice VLAN access on phones that support it.
8. Use 802.1Q tag on all trunk ports.

Note: There are a number of OSI Layer 2 attacks not related to VLAN hopping. Specific mitigation techniques are also available for these attacks.
### VLAN Use Examples

<table>
<thead>
<tr>
<th>1.1 Campus</th>
<th>1.4 Firewalls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to distribution</td>
<td>Multi-context mode firewalls</td>
</tr>
<tr>
<td>Virtualization technologies that</td>
<td>Transparent Mode Firewalls</td>
</tr>
<tr>
<td>assume the consolidation of</td>
<td>Firewall trunk ports</td>
</tr>
<tr>
<td>physical hardware:</td>
<td>Intrusion Protection Systems</td>
</tr>
<tr>
<td>• VSS (Virtual Switching System)</td>
<td></td>
</tr>
<tr>
<td>• vPC (Virtual Port Channel)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.2 Data Center / Services</th>
<th>1.5 Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switching (vPC)</td>
<td>MPLS</td>
</tr>
<tr>
<td>Blade Chassis Switching</td>
<td>VPLS</td>
</tr>
<tr>
<td>Virtual switches</td>
<td>802.1Q-inQ Trunking Service (802.1ad)</td>
</tr>
<tr>
<td>Load Balancers</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>1.3 Wireless LAN</th>
<th>1.6 Network Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote access points</td>
<td>Remediation / Posture Assessment VLAN</td>
</tr>
<tr>
<td>Wireless LAN controller aggregation ports</td>
<td>Guest VLAN</td>
</tr>
<tr>
<td></td>
<td>Corporate user VLAN</td>
</tr>
</tbody>
</table>
References

Cisco

- Understanding and Preventing Layer 2 Attacks in IPv4 Networks
- Virtual LAN Security Best Practices
- Enterprise Campus 3.0 Architecture: Overview and Framework
- Cisco SAFE: A Security Blueprint for Enterprise Networks
- Network Virtualization - Path Isolation Design Guide
- Network Virtualization - Access Control Design Guide
- Network Virtualization - Services Edge Design Guide
- Cisco Wireless LAN Controller Configuration Guide, Release 7.2
- Deploying Cisco 440X Series Wireless LAN Controllers
- Secure Wireless Design Guide 1.0
- Next Generation Enterprise MPLS VPN-Based MAN Design and Implementation Guide

RFC

- RFC 2196 – Site Security Handbook
- RFC 2401 - Security Architecture for the Internet Protocol
- RFC 5517 - Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment
- RFC 4554 - Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks

Other

- VLAN Security Guidelines - WatchGuard Technologies, Inc.
- Secure Use of VLANs: An @stake Security Assessment
- VLAN Hopping - Wikipedia