@stake consultants David Pollino and Mike Schiffman, CISSP, conducted the testing and analysis. Mr. Pollino is the Director of the Wireless Center of Excellence at @stake. He is a respected information security consultant with an extensive networking background. Mr. Schiffman is the Director of Security Architecture at @stake. He has researched and developed many cutting-edge technologies, including tools such as firewalk and tracerx, and Libnet. He has also spoken in front of several institutions and government agencies such as NSA, CIA, DOD, AFWIC, SAIC, and army intelligence.

AUGUST 2002

Secure Use of VLANs: An @stake Security Assessment

"In the interests of identifying and precisely defining security risks associated with VLANs implemented using the Cisco Catalyst family of products, @stake designed and executed a comprehensive test program. Through techniques devised to penetrate security weaknesses from a staging point within one VLAN, the @stake test suite attempted to send packets to a different VLAN and receive packets from a different VLAN. The results of @stake's test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms."

Executive Summary

VLANs offer a flexible, agile means of securely organizing network segments within an enterprise. Despite the promise of VLAN architecture to simplify network maintenance and improve performance, security questions have raised concerns and caused some network architects to re-examine the associated issues. One area of concern, VLAN hopping, involves a variety of mechanisms by which packets sent from one VLAN can be intercepted or redirected to another VLAN, threatening network security. Under certain circumstances, attackers have been able to exploit these mechanisms, gaining the capability of sniffing data at the switch level, extracting passwords and other sensitive information at will. As part of the security assessment that is summarized in this paper, @stake performed a battery of tests to evaluate the security features of the Cisco Catalyst family of products.

@stake has earned international recognition for expertise in network and application security solutions, and has configured and deployed VLANs for many of the world's largest enterprises. Cisco Systems' decision to hire @stake as an independent third-party consulting firm relied strongly on @stake's reputation in this field.

The results of @stake's test sequences clearly demonstrate that VLANs on Cisco Catalyst switches, when configured according to best-practice guidelines, can be effectively deployed as security mechanisms. Best-practice guidelines appear in summary in this paper and are detailed extensively in the Cisco document, *SAFE: A Security Blueprint for Enterprise Networks.*

Cisco VLAN Security Review

In the interests of identifying and precisely defining security risks associated with VLANs implemented using the Cisco Catalyst family of products, @stake designed and executed a comprehensive test program. The test suite, summarized in this section, targeted both known and theoretical vulnerabilities with the Catalyst family of products.

Through techniques devised to penetrate security weaknesses from a staging point within one VLAN, the @stake test suite attempted to send packets to a different VLAN and receive packets from a different VLAN.

Testing Scenarios

Test suites were constructed using open source tools, and proprietary software and utilities developed by @stake. Four Cisco Catalyst switches used in the VLAN configurations supported several test configurations, including a single-switch VLAN, multiple-switch VLAN, and VLANs with and without trunk ports enabled. Tests were conducted with knowledge of existing vulnerabilities, and were focused on identifying any unknown or potential vulnerabilities outside of well-understood issues, such as VLAN hopping through enabled trunk ports.

Categories of Tests

@stake employed a number of categories of tests during the security analysis, and executed several different individual tests in each category. Certain categories of tests are highlighted in the section below:

- **Frame Tagging**: Through use of different forms of encapsulation (including ISL and 802.1q), these tests attempted to forward frames to a different VLAN, bypassing normal security constraints.
- **Denial of Service or Failure Conditions:** In these tests, @stake attempted to send frames to the switch to cause abnormal or Denial of Service (DoS) behavior. These DoS attacks included:
    - **CAM Table Attacks**. By attempting to overwrite the CAM table entries on a VLAN, these tests attempt to interrupt traffic and force a switch to forward packets to different destinations.
    - **Flooding**. Flooding attacks rely on one or more attacker machines to produce denial of service situations, such as producing MAC flooding to get a switch to exhibit an abnormal failure condition. The response of a switch to the resulting failure condition represents a potential security hole. Multicasting techniques—generating frames to a wide range of addresses over extended periods in an attempt to produce a failover scenario—also fit in this category
- **Address Spoofing**: Forging MAC addresses and attempting to redirect traffic and extract data from packets represents a common technique for defeating

security measures. Tests in this category apply address spoofing in an attempt to redirect VLAN traffic with malicious intent.

@stake Testing & Results

The independent testing performed by @stake, at the request of Cisco Systems Incorporated, evaluated the security issues associated with VLANs in the context of a deployment on the Cisco Catalyst family of products. The test methodology included attempts to circumvent VLAN network security by launching an aggressive series of attacks to exploit both known and theoretical vulnerabilities in the Cisco Catalyst family of products. Following testing, @stake offered recommendations on updating the Cisco best practices framework for maintaining optimum VLAN security.

At the conclusion of this testing, @stake determined that there is minimal risk when deploying VLANs across security zones. The following table summarizes @stake findings for tests on Cisco 2950, 3550, 4006 and 6000 Series Catalyst Switches. The analysis baseline, lab configuration and version information used to conduct the testing are itemized in *Exhibit A: Analysis Baseline*.

@stake Testing

TEST	RESULTS
MAC Flooding Attacks	Normal behavior observed; traffic was repeated on local VLAN only.
802.1q and ISL Tagging Attacks	Normal behavior observed; switches only forwarded traffic on configured trunk ports.
ARP Poisoning Attack	Attack failed; VLAN hopping was not possible.
Layer 2 Proxy Attack	Normal behavior observed; IP forwarding needs to be properly configured.
Multicast Brute-force Failover Analysis	Attack failed; IP forwarding needs to be properly configured.
VLAN Hopping Using Spanning Tree Protocol Exploitation	Attack failed; dynamic protocols need to be properly configured.
Random Frame Stress Attack	Attack failed; VLAN hopping was unsuccessful.

MAC Flooding Attacks

The MAC flooding attacks are targeted denial-of-service attacks designed to get the switch to fail open. This is a well-documented attack that works with a number of vendor's switches.

802.1q and ISL Tagging Attacks

Tagging attacks attempt to get the switch to forward frames from one VLAN to another. Frames are modified with the addition of ISL or 802.1q encapsulation and sent tagged for destination on another VLAN.

ARP Poisoning Attack

ARP poisoning attacks involve using a known MAC and IP address of a host on a remote VLAN to get the switch to forward packets.

Layer 2 Proxy Attack

Hosts configured for standard IP forwarding will forward packets sent from one subnet to the same subnet. This is referred to as layer 2 proxy in this document. Potential Private VLAN attacks rely on a layer 2 proxy to bypass private VLAN access controls. Cisco Systems requested @stake to test common network devices to identify what devices - if any - an attacker could use as a layer 2 proxy.

Multicast Brute-force Failover Analysis

@stake tested the Catalyst switches' resiliency against a storm of multicast frames. This test involved spoofing, in rapid succession, a series of multicast frames.

VLAN Hopping Using Spanning Tree Protocol Exploitation

The 802.1d Spanning Tree Protocol (STP) avoids switching loops that can cripple layer 2 networks. Most mid- to high-range switches, including all of the Catalyst switches tested by @stake, support this protocol. By default, STP is turned on and every port on the switch both speaks and listens for STP. @stake tested to see if the PVST (per VLAN spanning tree) would fail open across multiple VLANs under specific conditions.

Random Frame Stress Attack

This test generates a field of random type and length, as well as a random payload (a completely random packet in which only the source and destination addresses remain constant). After repetitive testing, no packets were found to have hopped VLANs. Additionally, no errors or reboots were indicated on the switch's console log.

VLAN Security Measures

Certain VLAN configurations result in conditions where it is possible for frames to be redirected from one VLAN to another by a malicious party manipulating frame tags or address tables at the switch level. Receiving or sending frames from one VLAN to another—referred to as VLAN hopping—can only occur under specific circumstances. VLAN hopping can be prevented by configuring the Catalyst family of products in a manner that diminishes security vulnerabilities.

Simple measures, such as configuring hosts to be in a VLAN separate from trunk ports and disabling auto trunking in a VLAN configuration can greatly diminish the risk of attackers exploiting VLAN hopping. In addition, @stake noted that the "VLAN 1" designation should only be used for necessary management functions and not for other network traffic. Other security considerations include ensuring the

VLAN management interface is protected, having provisions for denial of service attacks, and maintaining secure handling of failure conditions. [1]

@stake Summary - Best Practices for Secure Use of VLANs

VLANS can be used to increase the security of a network environment if best practices are followed. Based on the results of testing, @stake recommends these best practices for the Cisco Catalyst family of switches:

- Restrict management access to the VLAN so that parties on non-trusted networks cannot exploit management interfaces and protocols, such as SNMP.
- Prevent denial of service attacks and other exploitation by locking down spanning tree and other dynamic protocols.
- Use IOS ACLs on IP forwarding devices to protect against Layer 2 Proxy on private VLANs. [2]
- Eliminate native VLANs from 802.1q trunks.
- Shut down any unused ports in the VLAN.
- Use port security mechanisms to limit the number of allowed MAC addresses and protect against a MAC flooding attack.
- Use the "VLAN 1" designation only for trusted networks and necessary management traffic.
- Avoid the use of cleartext management protocols, such as TELNET and SNMP, on a hostile network.

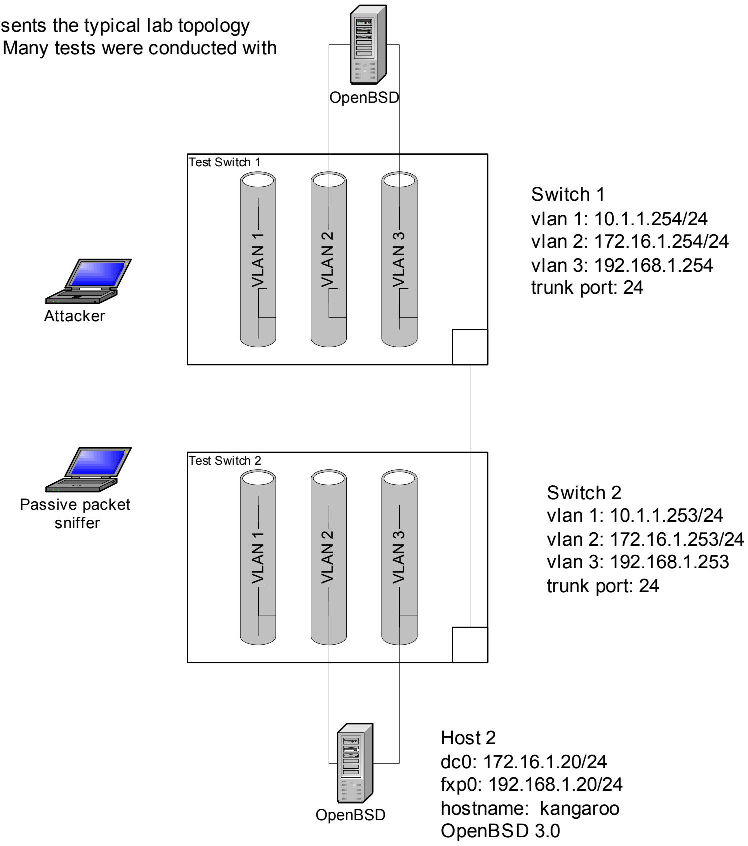
For a more comprehensive set of guidelines for ensuring VLAN security, refer to the Cisco document, *SAFE: A Security Blueprint for Enterprise Networks*, available at http://www.cisco.com/go/safe

Exhibit A: Analysis Baseline

@stake conducted testing of the VLAN security issues in @stake's San Francisco Security Lab and in the Cambridge Headquarters' Lab, using open source tools and @stake proprietary software. These tests, based on research exposing current VLAN security vulnerabilities and theoretical attacks, reflected practices firmly established by @stake's long-standing networking expertise.

Baseline Overview

The @stake lab was set up as shown in the following diagram. Ports on each switch were configured for different VLANs. @stake used a common numbering convention based on addresses specified in RFC 1918 to provide maximum flexibility during the testing with a minimum number of switch reconfigurations. Console port debugging levels were increased to monitor events on the switches.



Note: This drawing represents the typical lab topology used for @stake testing. Many tests were conducted with different configurations.

Equipment and Software Used for Testing

Cisco systems provided @stake with four Catalyst switches for testing in the @stake lab. The following table lists the equipment and software versions used for testing:

Version Information

HARDWARE	SOFTWARE VERSION
2950	IOS (tm) C2950 Software (C2950-I6Q4L2-M), Version 12.1(6)EA2b, RELEASE SOFTWARE (fc1)
3550	IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.1(8)EA1, RELEASE SOFTWARE (fc1)
4006	IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-IS-M), Version 12.1(8a)EW, RELEASE SOFTWARE (fc1)
6009	WS-C6009 Software, Version NmpSW: 7.1(2) IOS (tm) c6sup2_rp Software (c6sup2_rp-JO3SV-M), Version 12.1(11b)E, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1) MSFC2 Software (C6MSFC2-BOOT-M), Version 12.1(8b)E9, EARLY DEPLOYMENT RELEASE SOFTWARE (fc3)

Test Scenarios

The following test scenarios were applied to all of the tests described in the test plan section. Cisco Systems requested each of the following configurations:

- Single switch configuration
- Multiple switch configuration
- With a trunk port configured on the same VLAN as the attacker's
- With a trunk port configured on a different VLAN from the attacker's
- With no trunk ports configured

Tools

MAC Flooding Attacks

The primary tool used for this testing was *macof* written by Dug Song. To maximize impact, the attacks were performed with multiple attacker machines.

802.1q and ISL Tagging Attacks

Libnet, written by Mike Schiffman, was used to write custom programs to test for these vulnerabilities.

@stake Disclaimer

The services performed by @stake were intended to assess and describe the current state of the Cisco Catalyst family of products and related infrastructure. This report makes no representations or warranties of any kind regarding the security of Cisco or its products, or forward-looking statements regarding the effects of future events, and should not be relied upon by third parties when making assessments of the security of the Cisco Catalyst family of products.

About @stake, Inc.

@stake provides corporations with digital security services that secure critical infrastructure and electronic relationships. @stake applies industry expertise and pioneering research to design and build secure business solutions. As the first company to develop an empirical model measuring the Return On Security Investment (ROSI), @stake works where security and business intersect. Headquartered in Cambridge, MA, @stake has offices in Denver, Hamburg, London, New York, Raleigh, San Francisco, and Seattle. For more information, go to www.atstake.com.

Notes and references

[1] The full range of recommended security measures is detailed in the Cisco document, *SAFE: A Security Blueprint for Enterprise Networks*, available at http://www.cisco.com/go/safe

[2] Access controls to Private VLANs can be circumvented by creating a proxy for traffic off the host connected to the promiscuous port. The actual usefulness of this attack is limited—the attacker would need to control both hosts to create a two-communications channel. The proxying behavior relies on the fact that a host configured for standard IP forwarding will forward packets sent from one subnet to the same subnet (referred to as *layer 2 proxy*).