Global Information Assurance Certification Paper

VLAN Security in the LAN and MAN Environment

Chris Hoffmann
27 April 2003

Abstract

VLANs are no-longer confined to LAN environments and are becoming more widespread in their use. Unfortunately VLAN security is not always considered in their implementation.

This paper discusses security issues, and their risks, caused by both mis-configuration and hardware flaws for VLANs in both the LAN and MAN environment.

Introduction

Since the creation of VLANs (Virtual Local Area Networks) their use has become far more widespread than the simple concept of separating traffic into smaller, logical broadcast domains.

Today VLANs are not only used as an integral part of the LAN environment, they are now also being used as a means of providing WAN (Wide Area Network) / MAN (Metropolitan Area Network) services.

This paper discusses security issues, and their risks, caused by both mis-configuration and hardware flaws for VLANs in both the LAN and MAN environment.

Unless otherwise stated the paper is based upon configuration and hardware implemented in a Cisco environment.

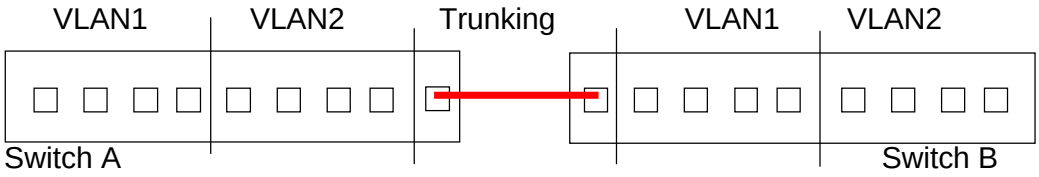
VLAN Background

Modern switches have added the capability to have Virtual LANs (VLANs). This came about so that you would be able to group ports according to functionality, location or business purpose.

The reason you want to be able to do this from a technical perspective is due to broadcast flooding. A switch has to flood broadcasts out all ports, so all NICs (network interface cards) need to process the broadcast before they can decide that it is not of use to the host. Therefore the more hosts you have on a network the more unnecessary traffic that is being processed by all machines. There are differing opinions as to how many hosts are too many for the one broadcast domain, as it depends on what protocols and applications are being used. 500 is commonly mentioned, but the best way it to use network analysis tools to determine what your actual network load is.

By creating VLANs in a network you create extra broadcast domains (1 per VLAN). Simply put, when you create VLAN's on a switch you are dividing your smart switch into a number of smaller dumb switches. Then you are able to utilize "Trunking" which is a method of joining switches together with only

one media connection yet still being able to carry data for multiple VLANS. (see the diagram below)



Traffic broadcast on Switch A port 1 will appear on Switch A ports 2, 3, 4 and Switch B ports 1, 2, 3, 4 but not ports 5, 6, 7, 8 on either switch.

How does traffic get from VLAN1 to VLAN2?

In most circumstances very little traffic will traverse VLANs in situations where it does you then use a router to route traffic between your VLANs also giving you a point to control/firewall the traffic that is able to flow between networks.

Example Network

Throughout the paper, I will be using an example network with the following properties to demonstrate examples of poor configuration.

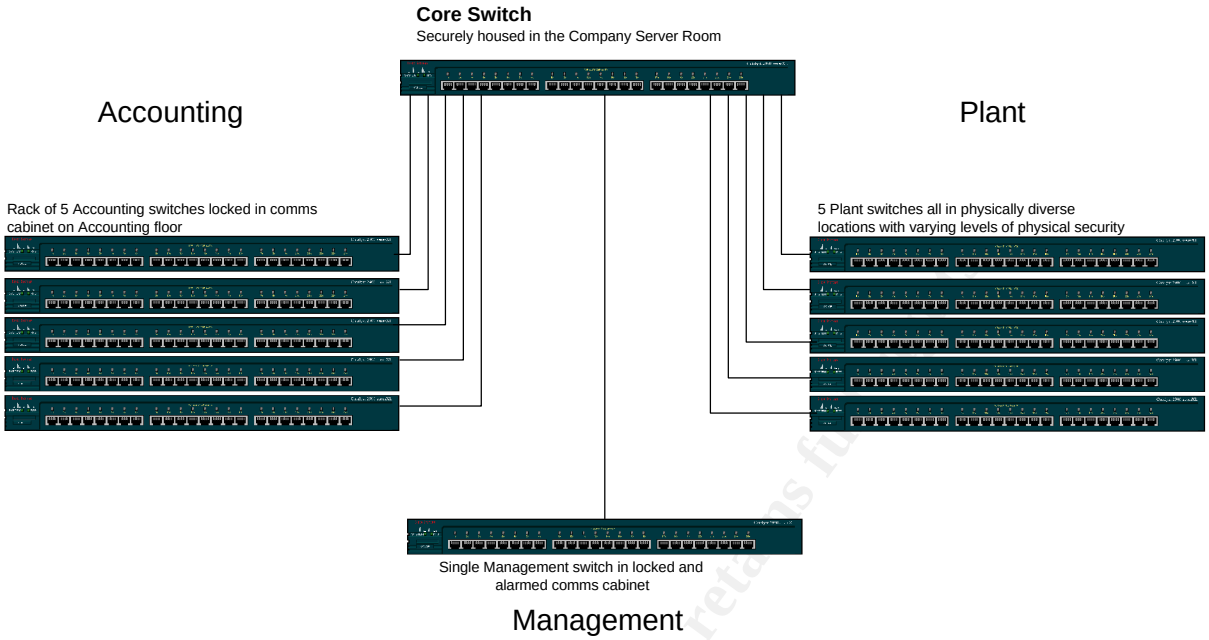
The network consists of the following VLANs:

- Plant
- Management
- Accounting
- Administration

VLAN ID's:

VLAN Name	VLAN ID	Description
Administration	VLAN 100	Used only for device Admin
Accounting	VLAN 11	Accounting Staff
Management	VLAN 12	Management Staff
Plant	VLAN 13	Plant Staff and Plant Equipment

Example Network Diagram:



The links between the switches in the diagram above indicate trunking.

So what's the problem?

The primary downfall with VLAN security is incorrect configuration. Due to the nature of VLAN's there are vast configuration options each with the ability to increase the networks susceptibility to data theft or network subversion. Simple measures, such as configuring hosts to be in a VLAN separate to the native VLAN circumvent the vulnerability to major attacks.

There are a number of malicious attacks that can be performed on an incorrectly configured device. Listed below are two that are particularly nasty as they are open with default configuration:

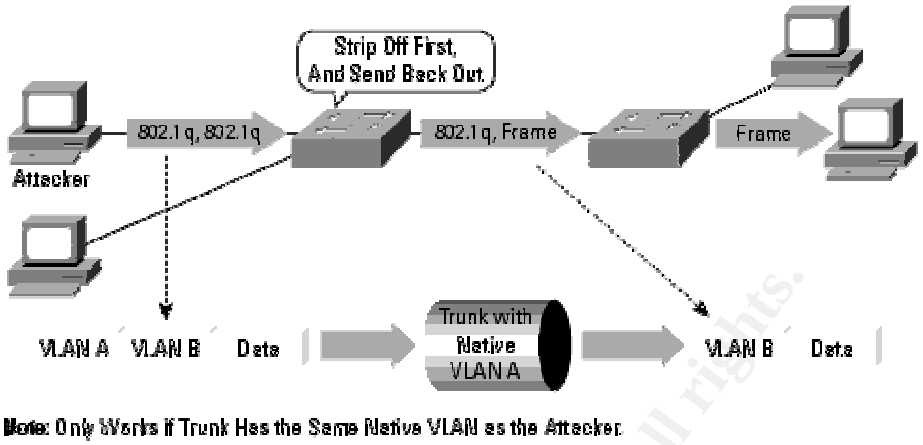
- Double-Encapsulated 802.1Q Attack
- 802.1Q Tagging Attack

Other attacks which Cisco switching equipment has been proven to withstand

- Random Frame Stress Attack
- Multicast Brute Force Attack

The following section lists best practices, common errors in configurations and touches on the repercussions that may be incurred by such configurations. Included also are configuration examples of how to avoid attack via mis-configuration.

Double-Encapsulated 802.1Q Attack



Source [4]

In the diagram shown above, the attacker is connected to a port on the switch which happens to be configured with the same VLAN (VLAN A) as the Native VLAN for the trunk. When a port (configured as per the diagram) receives traffic it tags it with a 802.1Q tag, but when the traffic reaches the trunk, it strips off the tag as non tagged packets are taken to be the native VLAN.

An Attacker can use this by "Double-Encapsulating" packets with the outer tag being the correct tag for his VLAN and the inner tag having the VLAN ID of the Target VLAN. When the packet gets to the trunking port, the switch strips off the outer tag, therefore the inner tag becomes the permanent tag for that packet until it is routed out the port on the switch containing the mac-address of the target.

This method of "VLAN Hopping" can be easily defended against by never having the native trunk VLAN, configured on a port.

802.1Q Tagging Attack

Tagging attacks are one of the most dangerous attacks on your switching security infrastructure. It is also one of the most easy to miss when configuring a switch.

Leaving a port with default configuration and not shut down opens up all VLANs that are trunked to/through the switch to unauthorized access.

An attacker is able to send DTP (Dynamic Trunking Protocol) traffic to the switch to trick the port into thinking that it is talking to another switch or dot1q device. The attacker can then craft their packets to whichever VLAN they want. In effect it is giving them complete access to any VLAN.

Simply put, without any reconfiguration of the switch that port can be used to access VLANs other that the default.

```
!
interface FastEthernet0/21
```

```
 description Static Access Port
 switchport access vlan 100
!
```

With the config shown above, the switch will only talk on port 21 with VLAN 100

VTP Domain Configuration

VTP is used to keep VLAN information consistent across the entire switching architecture. If you add a VLAN to one switch VTP will make sure that the VLAN details are correctly propagated to all switches in the VTP Domain. The following commands are used to configure VTP (IOS)

```
(config)# vtp domain [VTP DOMAIN]
(config)# vtp mode [CLIENT/SERVER]
(config)# vtp password [PASSWORD]
(config)# vtp pruning
```

VTP domain – this is a friendly name that has to be consistent across your LAN when using VTP

VTP Mode – One switch on your network needs to be defined as the VTP server. All other switches on the network then need to be configured as clients. Please note that by default a switch acts as a VTP server.
VTP password – it is recommended that you set a password for your VTP domain, because without a password, there is no way for the switch to verify the VTP updates.

VTP pruning – By enabling VTP pruning the VTP server calculates which switches need which VPN traffic, then only trunks those VPNs to them. For example, in the example network, as long as there are no ports on the management VLAN (12) in the plant or on the accounting floor, it will not be trunked from the core switch to plant/accounting switches. Therefore VTP pruning is a good security feature.

VLAN 1

The default configuration of Cisco switching devices is set up with all ports on the Default VLAN, VLAN1. The switch has a virtual interface VLAN1 which is used for management of the switch:

```
!
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
!
```

After an ip address has been configured, and a password set, you can telnet to the switch via the VLAN interface to perform remote Administration.

This can be moved from the Default VLAN. Most switches can only support 1 Virtual interface so they can only be managed from only 1 VLAN. It is recommended that you shift your administration VLAN to something other than the default or alternatively configure all ports (except those used for administration) to use another VLAN and have a dedicated VLAN only for the administration of switching devices. This prevents direct attacks from hostile hosts on the LAN.

```
!
interface VLAN1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 shutdown
!
interface VLAN100
 ip address 10.0.0.200 255.255.255.0
 no ip directed-broadcast
 no ip route-cache
!
line vty 0 4
 password cisco
 login
!
```

(Cisco config excerpt for 2900 series showing a shifted Administration VLAN and telnet password set)

Physical Security

As with all devices, Physical security is key to information security. A switch may be configured to provide access on all ports to the 'Plant' (example LAN with no sensitive data) LAN yet the switch may have the 'Accounting' and 'Management' (example LANs with sensitive data) LANs being trunked to it. With physical access to the console port of the switch an unauthorized party could easily perform a password override/restore, reconfigure the switch and gain access to sensitive data.

Monitoring

A correctly monitored network can give warning of a number of network security violations including a physical security breach.

Monitoring should be dealt with in a double barreled approach utilizing both alerts from the device and details polled from the management console.

The SNMP (Simple Network Management Protocol) traps notify the management console of any configuration updates, whilst continual polling and verification of the VLAN databases ensure that no hosts end up on the wrong network.

Also polling the MAC-address table, on a per VLAN/switch can be used as a final check that all hosts are on the correct network.

Restrict VLANS that are trunked

One method of minimizing the risk or incorrect VLAN association is to restrict the VLAN id's that are trunked to edge devices. Used the example Network detailed above, if there are no host devices for the plant network (VLAN13) on the switch that is going to be situated in the accounting area, the switch does not need to have the Plant Network Trunked to it.

```
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 11
 switchport mode trunk
!
```

Metropolitan Area Network considerations

Companies using a service provider providing a point-to-point Ethernet connection need to pay special attention to VLAN security. Some service providers will simply provide you with a connection to their MAN switch, in this situation, there are many things to be aware off.

1. Your data is unlikely to be encrypted by the service provider unless otherwise stated.
2. Any mistake in configuration by the service provider could lead to having your network bridged with that of another client
3. Any street cabinets that contain switching equipment is a prime target and an easy way into your network
4. You do not have administrative control of their network so you are unable to make sure correct measures are put in-place to prohibit other customers on the shared network from 'hopping VLAN' using crafted 802.1Q packets

Recommendations for the MAN Environment

The easiest way to overcome most of the issues listed above with MAN/WAN service providers is to encrypt all data between your physical sites with a VPN. By doing this you still get the benefits of a cheap way of linking your sites, utilizing a MAN yet still remaining confidence that your data is not being subverted.

How to secure the example network

For this example refer to the example network diagram. In this example there will only be reference to 1 plant switch, 1 Management switch and 1 accounting switch.

Core Switch:

Port 1 – cross over cable to the accounting switch
Port 2 – cross over cable to the management switch
Port 3 – cross over cable to the plant switch

Port Config Example:

```
!
interface FastEthernet0/1
 description Accounting Uplink
 switchport trunk native vlan 101
 switchport trunk allowed vlan 11
 switchport mode trunk
!
interface FastEthernet0/2
 description Management Uplink
 switchport trunk native vlan 102
 switchport trunk allowed vlan 12
 switchport mode trunk
!
interface FastEthernet0/3
 description Plant Uplink
 switchport trunk native vlan 103
 switchport trunk allowed vlan 13
 switchport mode trunk
!
```

Ports 4 – 23

```
interface FastEthernet[0/4 - 0/23]
 description Unused port
 switchport access vlan 999
 shutdown
!
```

Accounting Switch:

Port 1 – 23 - hosts
Port 24 - cross over cable to the core switch

Port Config Example:

Ports 1 – 23

```
interface FastEthernet[0/1 - 0/23]
 description Accounting Port
 switchport access vlan 11
!
interface FastEthernet0/24
 description Core Uplink
 switchport trunk native vlan 101
 switchport trunk allowed vlan 11
 switchport mode trunk
!
```

Management Switch:

Port 1 – 10 - hosts
Port 11 – 23 - unused
Port 24 - cross over cable to the core switch

Port Config Example:

Ports 1 – 10

```
interface FastEthernet[0/1 - 0/10]
 description Management Port
 switchport access vlan 12
!
```

Ports – 11-23

```
!
interface FastEthernet[0/11 - 0/23]
 description Unused port
 switchport access vlan 999
 shutdown
!
interface FastEthernet0/24
 description Core Uplink
 switchport trunk native vlan 102
 switchport trunk allowed vlan 12
 switchport mode trunk
!
```

Plant Switch:

Port 1 – 23 - hosts
Port 24 - cross over cable to the core switch

Ports 1 – 23

```
interface FastEthernet[0/1 - 0/23]
 description Accounting Port
 switchport access vlan 13
!
interface FastEthernet0/24
 description Core Uplink
 switchport trunk native vlan 103
 switchport trunk allowed vlan 13
 switchport mode trunk
!
```

All Switches

All switches in the example should be configured using the following commands. This is the process required to remove the switch from the default VLAN.

(config)# interface VLAN 100
(config-if)# ip address [switch ip]
(config)# interface VLAN 1

```
(config-if)# shutdown
(config)# interface VLAN 100
(config-if)# no shut
```

Conclusion

In conclusion, the primary security issue with VLANs is poor configuration.

There are many configuration issues that need to be addressed during the configuration process in a switching architecture. Major security gains can be obtained with simple configuration changes like always disabling VTP and not using the default VLAN for anything.

If all issues are correctly covered with appropriate configuration, a secure switching architecture can still be obtained when utilizing a Cisco platform.

References:

Online

[1] Peter J. Welcher, Switching: VLAN's
http://www.netcraftsmen.net/welcher/papers/switchvlan.html

[2] Peter J. Welcher, Switching: Trunks and Dynamic Trunking Protocol (DTP)
http://www.netcraftsmen.net/welcher/papers/switchvtp.html

[3] Dave Taylor and Steve Schupp, Bugtraq Submission
http://www.securityfocus.com/archive/1/26008

[4] Virtual LAN Security Best Practices
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm

[5] Secure Use of VLANs: An @stake Security Assessment
http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/tech/stake_wp.pdf

[6] David Taylor ,VLAN Security Test Report
http://www.sans.org/resources/idfaq/vlan.php

[7] Sean Convery, Hacking Layer 2: Fun with Ethernet Switches

http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

Offline

[8]
IEEE Std 802.1Q-1998

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event