

Implementation of Virtual LANs for Virus Containment

December 9, 2004

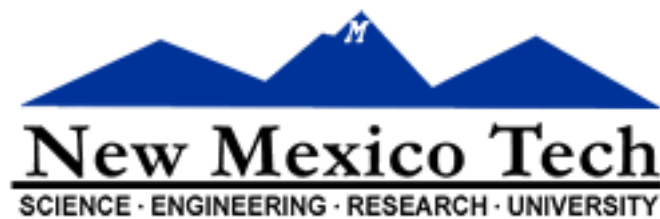
Aaron M. Soto

Prepared for:

Dr. Peter Anselmo

Information Technology Department

New Mexico Tech, Socorro, NM



Abstract

The goal of this project is to create a system to easily and reliably quarantine network traffic. Through the use of Virtual LANs (VLANs), the New Mexico Tech Information Services Department (ISD) would be able to move traffic from the standard network into a quarantine. This quarantine VLAN could funnel into a server, providing minimal services for quarantined users, allowing them to patch and clean their infected PCs (or hosts).

Currently, the project has produced a test quarantine server capable of filtering traffic based upon a list of allowed websites. The quarantine server is also running an informational website along with DNS services. The server has been configured to properly run with a switch, similar to those deployed across the NMT campus, providing both quarantined and standard services on the same hardware.

Focus is now on the refinement and testing of the quarantine server. Additionally, research into the automation of moving hosts in and out of the quarantined VLAN would be of significant value, if time permits. Pending ISD approval, the project may extend into the implementation of the quarantine VLAN across multiple buildings or even throughout campus.

Problem Statement

Large networks of any type are plagued by surges of traffic, which can lead to significantly degraded network performance as well as downtime. These surges of traffic are frequently due to virus outbreaks.

A system to easily and reliably control network traffic from infected machines would be of great value to a number of organizations. In cooperation with the New Mexico Tech Information Services Department (ISD), this project's goal is to design and implement such a system through the use of Virtual LANs. While New Mexico Tech will serve as the main design base for this project, efforts will also be focused on making a scalable and adaptable system for use in other organizations.

Background

For some time, switches, routers and other manageable network equipment have included support for Virtual LANs (VLANs). The original basis for this system was so that large organizations could isolate networks based upon their purpose. For example, several departments (management, accounting, etc.) could run isolated and secured networks while reducing the amount of hardware required. Instead of having separate networking hardware for each department, each department can be separated by VLANs. This technology is aimed at organizations implementing security on a budget.

What few know is how scalable VLANs are across a network. For example, multiple switches can connect so that VLANs can be relayed between switches. This means that even when environments prohibit users on the same network from being physically united, VLANs allow for ports across a number of switches or routers to be merged.

Proposed Solution

Overview

On the New Mexico Tech campus, an emphasis is placed on using reliable and manageable equipment campus-wide. While this is mainly for the purposes of network administration, it also allows software to retrieve data from switches and routers. This infrastructure provides an ideal environment for the implementation of VLANs.

As a solution to quarantine computers that may be infected, New Mexico Tech ISD could implement campus-wide VLANs. Specifically, these VLANs could extend to nearly all switches on campus, allowing network administrators to seamlessly transfer individual ports on a switch into a quarantined VLAN. This means that without any action or confirmation

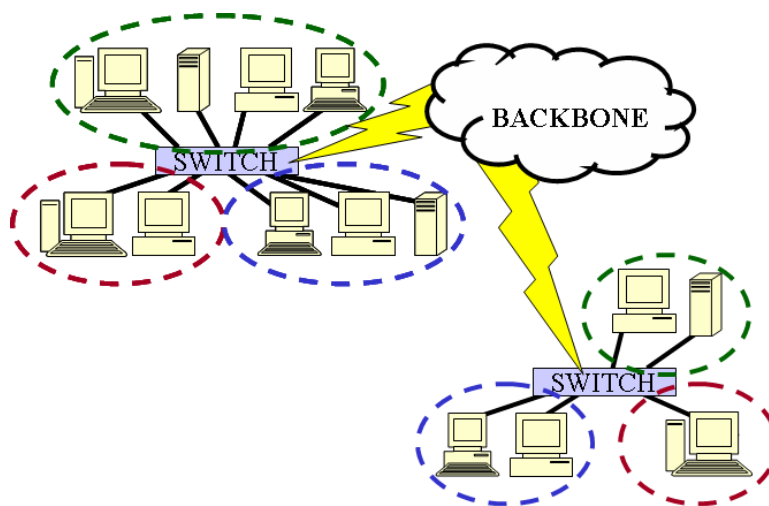


Figure 1: Example use of VLANs across multiple switches to secure independent networks across the same hardware.

by the compromised host, all traffic would be removed from the New Mexico Tech network and diverted to an isolated network. This solution uses the equipment already in place, allowing for a very low-cost VLAN-based quarantine system.

While the advantages for network administrators are clear, this does not immediately appear to provide benefits for the end user. However, upon closer inspection, the implementation of these VLANs could include a heavily-modified gateway which would restrict traffic from leaving the quarantine. This means that users would be able to access websites which have been pre-approved by the network administrator. These websites could include update sites (i.e. Microsoft WindowsUpdate), Anti-Virus update servers (i.e. Norton LiveUpdate, McAfee AutoUpdate) or other websites to assist in the removal of malware from the compromised host.

Implementation

This project will concentrate on three areas. First, closest to the end-users, a manageable switch with VLAN support must be in place to move the port to and from the quarantined VLAN. Second, a firewall or gateway must be configured to separate all traffic from the Internet connection to the quarantine server if it is marked for the quarantine VLAN. Last, a highly-secured quarantine server will be responsible for the filtering of traffic and allowing access to the list of pre-approved websites. The New Mexico Tech campus is comparatively technologically advanced in the sense that great thought and expense are put into the network design. Current, advanced switches have been installed throughout the entire network.

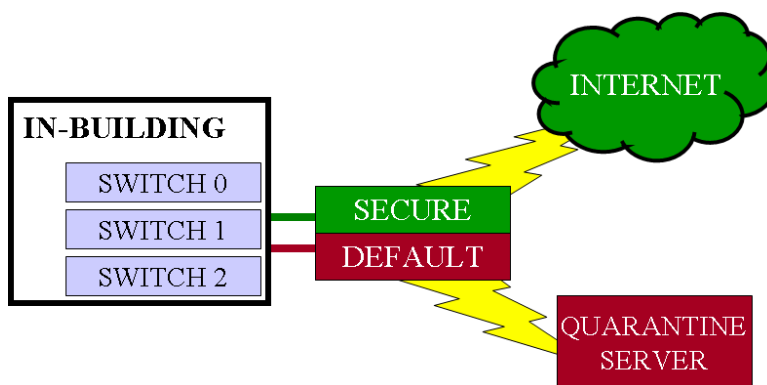


Figure 2: Proposed layout of the link between in-building switches, on-campus routers and the quarantine server.

The vast majority of these are manageable and have VLAN support. The few that do not meet this criteria are in line to be upgraded.

The campus network already has a main router in place for the purposes of connecting the large number of hosts and networks within the university. This router is capable of VLAN support and is able to route packets based upon their VLAN ID. This means that any packets from quarantined hosts will immediately be removed from the main network and transferred into the quarantine zone. This allows the gateway to be replaced by the quarantine server.

The quarantine server, being as secure as possible, can also manage other tasks. For example, the server could offer a number of tools for download to allow users to install the latest patches for their operating systems, run cleaning tools for specific viruses, or download instructions regarding the removal of malware. It can also be used to verify that the formerly compromised host has been cleaned before moving it back into the secure VLAN.

Current Progress

The primary focus has been the quarantine server, as it is the most complex portion of the system and requires significant forethought. Currently, a temporary server located at the ISD offices is running Red Hat Linux (Fedora Core 3), along with the latest version of iptables, Apache HTTP server and Bind DNS services. This server is connected to a switch identical to many of those on-campus containing two VLANs: a secure and a quarantined network. As the server is currently setup, it functions as a gateway for the quarantined network, capturing traffic of all hosts attempting to gain Internet access. It is capable of selectively passing traffic from the quarantine onto the Internet, based upon the destination.

```
mailhost.nmt.edu -p tcp --dport 110 -j ACCEPT -A PREROUTING --dst
externalweb.nmt.edu -p tcp --dport 80 -j ACCEPT -A PREROUTING --dst
webmail.nmt.edu -p tcp --dport 80 -j ACCEPT -A PREROUTING --dst
webmail.nmt.edu -p tcp --dport 443 -j ACCEPT

-i eth1 -j DNAT --to-destination 129.138.XXX.XXX

tcp -s 129.138.XXX.XXX/24 -j MASQUERADE
```

Figure 3: A snippet of ipTables configuration demonstrating the unique selective filtering used by the firewall.

The key to the success of the system is that the quarantine server must become the default gateway when a host is moved from the secure network to the quarantine network. No reconfiguration on the infected host should ever take place. As such, the quarantine server will need to be supplied with a number of IP addresses (including those of each default gateway), over one or more network connections.

Currently, the quarantine server is capable of providing all of these services. Additionally, it has been tested using a variety of hosts. Further testing is in progress.

Future Work

The VLAN configuration at the switch and router levels is such that it is very specific to the manufacturer and model of the device. However, this process is very simple and would be easily accomplished through the use of provided documentation. This portion of the project has been left to the ISD administrative network staff during the final stages of the project.

Further work remains in the areas of setting up DHCP services as well as enhancing the ruleset of the permitted websites and allowed services. Close collaboration with the ISD administrative staff will be required during this phase.

Research on the SNMP patterns of the switches will also need to be done so that verification of VLAN placement can take place. If time permits, automation of VLAN transfers can be researched, leading into a series of scripts useable by ISD.