Global Information Assurance Certification Paper

Improving Network Security Port by Port

GIAC Security Essentials Certification (GSEC)

Option 2

Practical Assignment Version 1.4b

Bruce Hays

23 December, 2003

Table of Contents

Abstract

Network security can be improved by using newer technologies that have begun to mature over the last few years. One of these technologies is IEEE 802.1x. Cisco's Identity-Based Networking Services is based on the IEEE 802.1x standard and is used as the basis of securing a state-wide enterprise network.

A network of many small to large sites was configured to use 802.1x for machine authentication where possible. In locations where this was not feasible, other forms of port security were implemented. At the center of the implementation is a Cisco Access Control Server (ACS) appliance. By isolating visiting and/or public machines from domain resources, network security has been enhanced and possible sensitive information is protected.

Before Snapshot

Problem

To ease the management burden and to facilitate mobility of users, all data ports on switches and hubs within the enterprise are enabled, and DHCP is used is issue IP addresses. No port security has been implemented. This configuration allows any computer to connect to the network and obtain an IP addresses regardless if it is an authorized network device or not. This situation leads to the possibility of hackers gaining access to network resources, eavesdropping, or inflicting some type of denial-of-service or other attack on the network from the "inside" [1]

In designing a security solution, there were several mandates put on the administrators of this network.

1. Only those computers authorized on the domain will be allowed to see and access resources of the domain.
2. Those computers that are not members of the domain, but are authorized to access bandwidth and internet resources, must be allowed to do so without accessing the domain resources.
3. Those unauthorized computers must not be allowed to access any resources or bandwidth.
4. Network administration must be accomplished with a minimal staff.

During Snapshot

The first step in implementing a solution was to gather information about the network. The logical topology information was gathered used Fluke's LAN MapShot (http://www.flukenetworks.com/us/LAN/Monitoring+Analysis+Diagramming/LAN+MapShot/Overview.htm).This program allows an administrator map the network from his desktop and displays the map in a Visio file. The process is fast and accurately identifies all devices except hubs. The drawback is the fact that it is a LAN tool and does not cross WAN links.

Network Topology

The enterprise consists of a Headquarters Local Area Network (LAN) five medium sites, and 12 small sites. The medium sites are connected by a Point to Point T1 to the HQ LAN and the small sites are connected by Frame Relay circuits with a CIR of 256k. See figure 1.

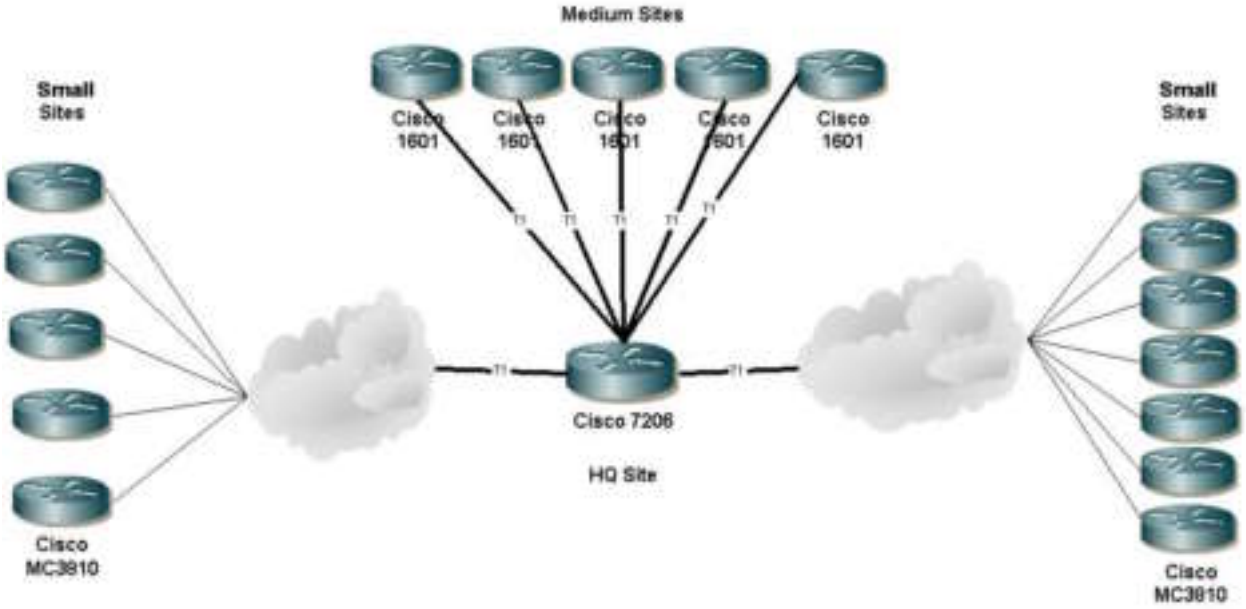

Figure 1: Network Topology

Small Sites

The small sites usually number less than six personnel and are located throughout the state. These sites are typically remote and do not receive much on-site support from technicians. Each site is connected by a Frame T1 with a committed information rate (CIR) of 256k. Each site is issued a sub-netted class A address space, essentially a class C address. Addresses are either issued by DHCP from a small site server located on the premises, or are assigned static address. In addition to the server, the sites also have a Cisco MC3810 router, a Baystack 10BaseT hub, networked printers and workstations (Figure 2). All servers are currently Microsoft Windows NT 4.0 and the workstations are a mix of NT 4.0, Windows 2000 Professional, and XP professional. All workstations are currently being migrated to XP.

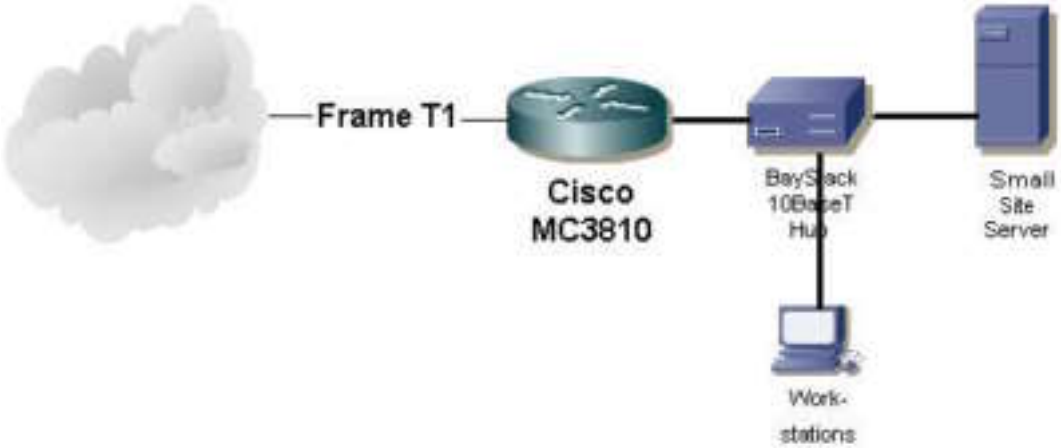

Figure 2: Small Site Topology

Medium Sites

The medium sites are more centralized within the state. These sites have more than six personnel and have either a technical person on staff or have a person who is trained as a "superuser". The medium sites are each connected by a Point to Point T1. Either A Cisco 1601 or a Cisco MC3810 router is located at each site. At each medium site, there is a Windows NT Server that is a domain controller that also acts as a DHCP and WINS server. There is a mixture of hubs and switches at the medium sites. These are 3500xl series Cisco switches, and Baystack 10BaseT hubs.

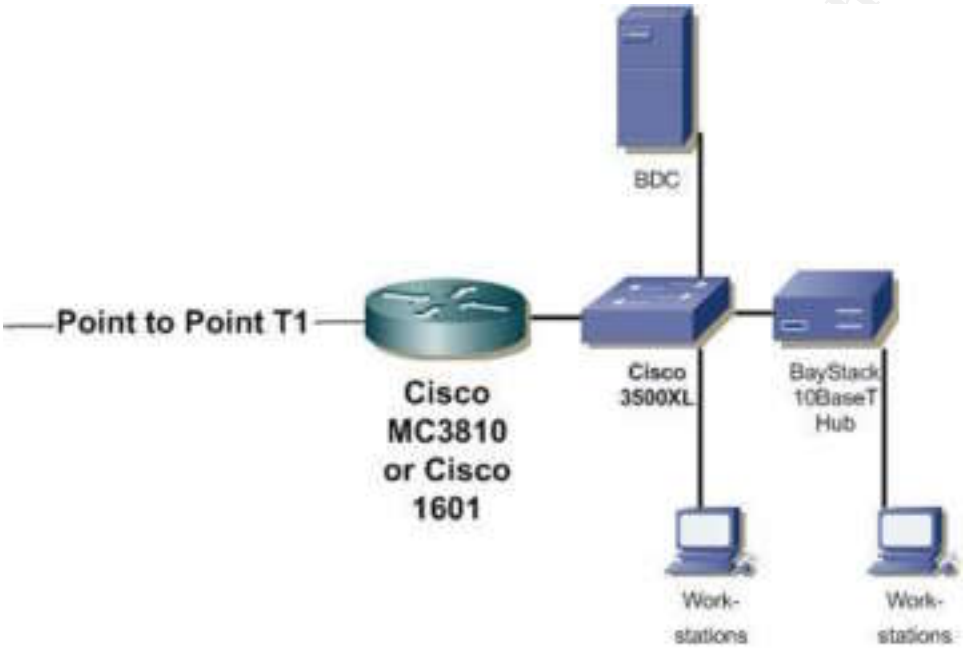

Figure 3: Medium Site Topology

Headquarters Site

The headquarters site is a large LAN. Entry into the LAN is through a Cisco 7206 and a Cisco 5509 switch. Most of the layer two devices are Cisco 3500xl series switches with several layer one 10BaseT and 100BaseT hubs. The servers are located in two separate physical locations and all servers are attached to Cisco 4006 switches. Most of the switches are connected by Gigabit Ethernet and the servers and all workstations off the switches are 100BaseT. The HQ LAN houses the Primary domain controllers, the primary DHCP server, and the exchange servers (Figure 4).

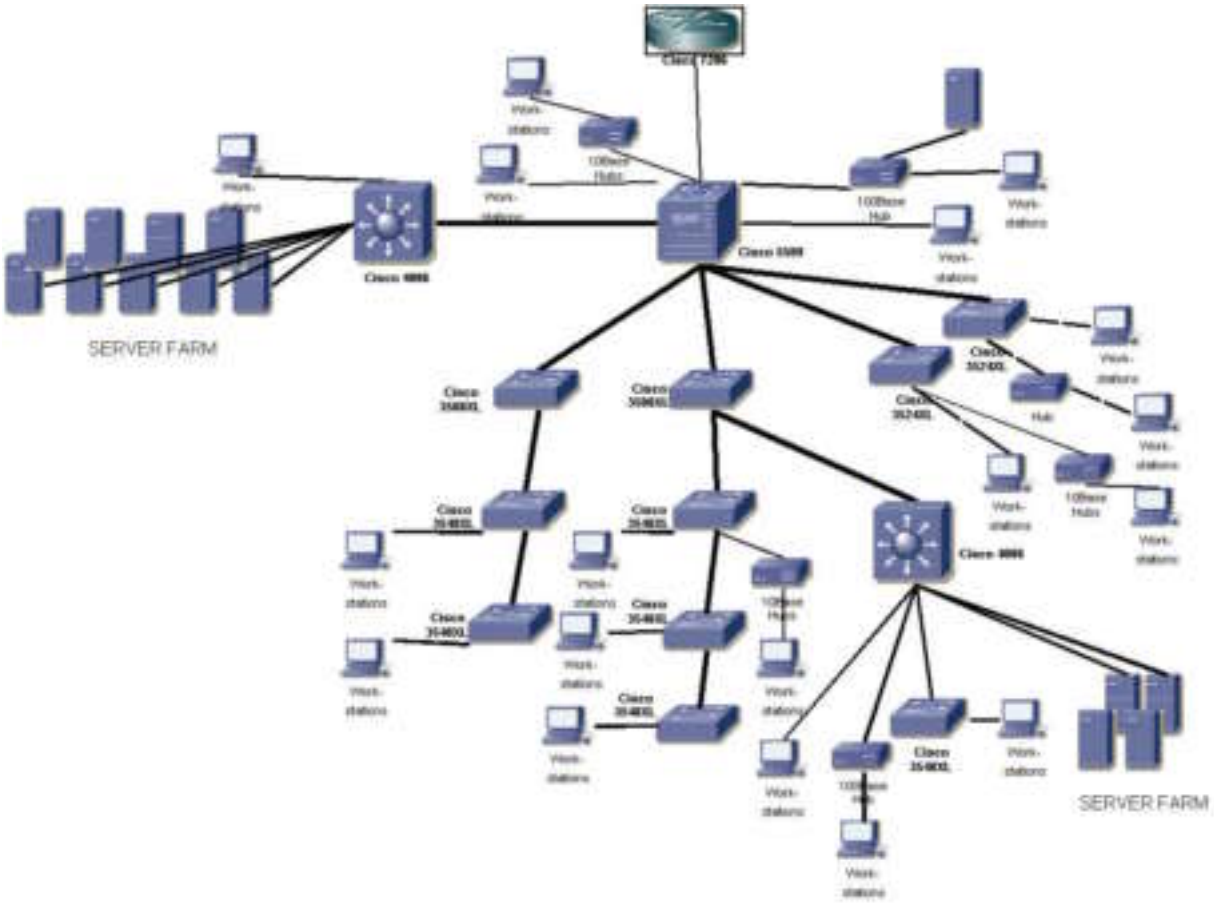

Figure 4: Headquarters LAN Topology

Possible Solutions

The next step involved investigating the possible solutions. Several solutions were proposed and evaluated.

1. Only the ports being actively used would be physically enabled.
2. Use the port security features built into the existing Cisco catalyst switches.
3. Employ IEEE Standard 802.1x, Port-Based Network Access Control

Enabling Active Ports

This solution is most cost effective of the three in terms of new hardware costs. It entails only an administrator having to physically make port active by plugging a patch cable from the patch panel to the switch or hub. Only those network jacks that are physically plugged in by the administrator would be usable.

This method, however, also has a high cost in terms of manpower. Each network jack and corresponding punch-down on the patch panel must be identified and labeled. In a perfect world or newly wired (or rewired) facility, this would be done. In our case, it is not. Any changes in topology; office moves, additions, deletions, etc, would require an administrator to physically touch the local switch. This method also does not provide much in the way of security. By unplugging one computer and plugging in a rouge

machine, or by simply inserting a hub, a user could easily add more computers and circumvent the whole security method.

While this method does offer some, though limited security, it does not meet the mandate that authorized computers not part of the domain be allowed access to bandwidth but not domain resources. It also requires more network administrator man-hours that will be readily available.

Use the Security Features in the Cisco Switches

The layer two devices currently deployed consist of Cisco Catalyst Switches. There are, in addition to the switches, unmanaged hubs located at every facility. The Cisco devices allow the use of MAC addresses to secure the switch and subsequently the network.

The basic switch configuration for security is accomplished by using commands that affect the MAC address table of the switch. The basic commands [2] are
mac-address-table permanent
port secure max-mac-count and
address-violation.

By using the **mac-address-table permanent** command, a MAC address is associated with a port on the switch and will not time out. Thus, the MAC address table is built with known addresses. The **port secure max-mac-count** command will limit the number of address that the port will learn. For maximum security this can be set to one. For greater flexibility and less security, this number can be increased to allow the use of hubs.

The last command, **address-violation** will specify the action taken by the switch for port address violation. For instance, if the max-mac-count has been set to 4, and a fifth MAC address source connects to that port, the switch can either suspend the port, disable the port, or ignore the violation.

An example of configuring a switch is [3]

Switch(config)#**mac-address-table permanent 0001.1111.1111 ethernet 0/2**
Switch(config)#**interface ethernet 0/2**
Switch(config-if)# **port secure max-mac-count**
Switch(config-if)#**exit**
Switch(config)#**address-violation disable**

This method requires that MAC addresses for any computer that is to be configured into the switch be known. This may not always be the case. A tool that will discover MAC addresses is available from SolarWinds. The MAC Address Discovery tool comes as part of a comprehensive set of tools included in the SolarWinds Engineers Edition Toolset (http://www.solarwinds.net/Tools/Engineer/index.htm).

While this method will work fairly well for a limited number of network devices that will be plugged into the network, it quickly becomes a management burden as the number of devices grows. By restricting the device that can connect to a port, movement is limited by personnel around the enterprise. This can be overcome by

allowing a port to "sticky learn" the permanent MAC address. This however allows any computer to be learned, not just enterprise owned.

Users can facilitate movement by notifying an administrator of his move, but once again this becomes a management issue.

Using switch port security as the security solution also does not address the hubs, and how to secure them.

Employ IEEE Standard 802.1x, Port-Based Network Access Control

This method is newest technology of the three. This standard uses the infrastructure in place as far as the physical layer is concerned, minus the hubs. As stated in the IEEE standards document

Port-based network access control makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails. [4]

While this is a paper on implementing network security and not 802.1x theory, a few terms and processes should be explained.

Supplicant – The device requesting access to the network. This is the client or PC.

Authenticator – The network access point. This may be either a switch or WLAN access point.

Authentication Server – The device that actually performs the authentication. This either allows the device to join the network based on username or MAC address.

Extensible Authentication Protocol (EAP) – The protocol used between the supplicant and authenticator.[5]

Before the client can communicate on the network, to include DHCP, the port must be authorized. Figure 5 shows this process between the supplicant, authenticator, and authentication server. [6]

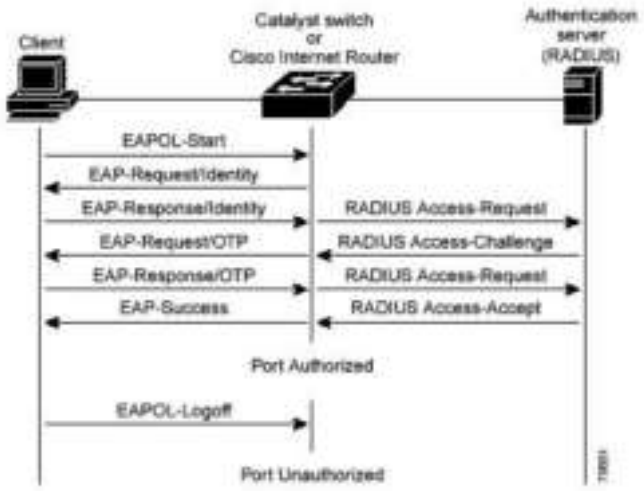

Figure 5: 802.1x Message Exchange

Cisco has implemented an IEEE 802.1x technology called Cisco Identity-Based Networking Services. This technology can be used to identify users or equipment that accesses the LAN. Due to this technology only being recently standardized, not all devices support it. [1]

Cisco Identity-Based Networking Services can be used to authenticate users when accessing the LAN either by way of traditional point-to-point media into a switch, or when accessing via a wireless network. The implementation also allows for machine based authentication via certificates. Only those machines that are authorized to the domain whether PC or IP phone will be authenticated and allowed access. This standard fulfills many of the requirements for our network.

This technology is not without drawbacks. First not all clients in our enterprise support 802.1x. NT 4.0 Workstation is not compliant and will have to be upgraded. Also not all of the layer one and two devices are compatible. The Cisco 3500XL catalyst switches are at End-of-Sale and will not be upgraded to support it. The hubs will not support 802.1x either and will have to be replaced. Upgrading all network switching devices require a large investment of time and money which is in short supply of many organizations.

Machine Authentication

Machine authentication allows a machine to authenticate onto the network based on the devices identity. This is done before the DHCP process and before the user interacts. Network access is blocked before the machine authenticates, so no network access is given unless the machine can authenticate. [7] The Cisco ACS allows different methods of handling unknown machines and users which will allow us to dictate policies. This implementation allows for machine only authentication, user only or both. The diagram shown in figure 6 shows the steps in machine authentication. [7]

Figure 6. Machine Authentication (Courtesy of Cisco Systems)

Implementation

When implementing a solution, it was decided to use a mixture of solutions. The end goal is to have a 802.1x fully compliant network once work is completed. Due to budget constraints, this will have to be implemented in phases.

Access Control Server

The first phase was installing and configuring a Cisco Secure Access Control Server (ACS) appliance. This is a device that is hardened, secure, single function appliance in a 1U rack mounted device. By using this appliance, a separate server did not have to be purchased, loaded with windows and secured. The ACS was installed in the Headquarters Site as to be centralized within the network. While a robust and complicated device, its web interface made the task less time consuming. Still, learning the new technology and implementation of the ACS was the most time consuming step.

As the ACS was being configured, the additional capability of TACACS+ was investigated. While not part of the original configuration plan, this capability was quickly emplaced. After attending the GSEC Security Essentials, I learned the importance of Authentication, Authorization, and Accounting (AAA). The ACS allows us to do all three. The routers and switches were configured to take advantage TACACS+ and were generally hardened as outlined in SANS' "Securing Cisco Routers: Step-by-Step"

The ACS was initially configured for TACACS+ and for basic machine authentication. While many other features are available, these will have to be implemented as time constraints allow.

Switch Configuration

The switch configuration turned out to be a fairly straightforward process. Only three basic steps were needed.

1. Enable RADIUS support on the switch.
2. Enable 802.1x support on the switch globally
3. Configure 802.1x on a port by port basis

Optional commands that are available for the port configuration include the ability to enable or disable port authentication, enable or disable periodic re-authentication, and allow for multiple hosts. This last ability will allow the use of hubs if needed. [8]

Small Sites

After the ACS was installed, it was decided to address the small sites first. As mentioned, these sites can be a far distance from the headquarters site and any support or technicians. By providing a dynamic and hands off type of security solution at each small site, the largest area of the network (geographically), and hence the hardest to physically control would be secured. In addition, installing a solution at these far reaching sites would reduce travel time and support man-hours for network and security managers.

Each of the small sites had in place a 10BaseT BayStack Hub. These hubs which were not compatible, had to be replaced. The Cisco 2950 switch was chosen as a replacement. This switch is compatible with 802.1x, addresses the needs for the amount of personnel in the location and fit in well with future growth plans. The additional consideration of budget also had to be considered. The 2950 is at the low end of the price spectrum from Cisco but still provided everything we needed in a small site switch. Identical switches were ordered for all 12 sites. By using a cookie-cutter approach, we could ensure that installation, configuration, and administration were all standardized. This way no security holes were left unplugged.

Once the switches were installed, they had to be configured to utilize Cisco's Identity-Based Networking Services.

Medium Sites

Unfortunately, the medium sites did not receive all new switches due to budget constraints. However, these sites usually benefit from a better physical layer infrastructure, and better physical security. They also receive more visitors that may need access to the internet.

First those areas that would see high visitor traffic were identified. These "visitor areas" had Cisco 2950 switches installed in place of the hubs. As in the small sites, these switches were configured to utilize Cisco's implementation of 802.1x.

Areas that would not see visitor access did not receive new switches. They did have the older, non-802.1x compliant, 3500XL switches installed. The 3500XL switches were identified and will be replaced by newer 3550 switches as funds become available. These switches utilized MAC address port security as described earlier.

Headquarters Site

This site has the greatest number of users. It also has the most tightly controlled network in terms of physical security. With the IT staff located in the immediate are, response time to changes and security concerns is minimal. This location also has a limited number of visitors. While not nonexistent, the visitors will be confined to certain areas. This area had a new switch installed to take advantage of 802.1x. The areas served by the larger 4006 switches were in good shape. By simply upgrading the supervisor engine, these switches were made compliant.

As in the medium sites, all hubs were removed, and the older switches installed. All switches that were not 802.1x ready, then used MAC address filtering for security.

In certain areas were limited rewires took had recently taken place, added security measures were put in place. This consisted of physically enabling those ports on the switch actually in use.

Client Configuration

As previously mentioned, not all clients are compatible. Working in close consultation with the PC support group, all workstation that were not XP were upgraded as 802.1x was employed. This was not an immediate concern for those areas in the medium sites and headquarters site that would use other means for security.

Accommodations had to be made for the servers. Many of the servers can not be upgraded at this time. Also the servers needed to be on at all times and we did not want them to have to re-authenticate. Since the servers are usually located in a secure area with the switch, it was deemed secure enough not to have the servers authenticate. The server ports were forced not to use 802.1x.

There are other clients that had to be considered. These include such devices that will not support 802.1x including printers, VOIP phones, scanners and other devices that require network access. For these devices, the port on the switch must not use 802.1x or the device will be available for use as it can not authenticate.

Other devices include there own support such as wireless access points. Therefore the port the access point is attached to does not need authentication turned on. [5]

A certificate was generated using our own certificate authority and installed on both the ACS and client. Enabling machine authentication in Windows XP is done from the properties tab in the network connection and following these steps (Figure 7).

1. Select “Enable network access using IEEE802.1x”
2. Select “Authenticate as computer when computer information is available”
3. Select “Smart Card or other Certificate.
4. In the properties section, select “Use a certificate on this computer” and select “Validate server certificate”

Figure 7. Properties for Network Connection

Guest VLANS

Cisco 802.1x compliant switches have a feature called 802.1x Guest VLAN. This feature allows machines that do not authenticate to gain limited internet access. This feature can be enabled only on select switches. By enabling and using this feature, we meet one of the main mandates for designing a more secure network. This allows visiting personnel to use bandwidth and not see any enterprise resources.

By assigning a guest user to a separate VLAN and then access control lists to isolate this subnet, we achieve the goal of allowing internet access while denying access to the enterprise.

After Snapshot

The implementation of our port security solution turned into a very large project. While the Cisco Identity-Based Networking Services promises to be very robust, scalable, and secure solution, implementation can be costly in terms of both man-hours and equipment. This is especially true for an existing infrastructure with legacy switches that do not support 802.1x.

The overall state of security has improved with the elimination of hubs. The presence of hubs allowed any one with physical access to a hub to gain network access. This one act, besides improving security, has also improved network performance.

By installing the Access Control Server first and getting it configured, the central component was put in place and allowed us to work in manageable chunks. With our enterprise separated into distinct remote locations, we were able to tackle the project

one small site at a time. This limited the amount of interruption to the user and allowed us to slowly gain the expertise we needed. As we moved from small sites to medium sites, and finally the headquarters, we knew what the ACS was capable of and what will need to be addressed.

Some of what we found is not going to necessarily apply to all networks. One item of concern is DHCP timeouts, which will have to be looked at closer. 802.1x authenticates the user or machine before DHCP assigned an address. If the authentication takes too long, DHCP will time out.

Switches are a cost that will have to be dealt with. We were not able to implement this solution in all locations. This was due primarily to switch upgrades and cost. The designer of the network in which old switches are in place will have to identify and plan for those areas in which older technologies will have to be used for security.

As much as the security has improved, we also know that 802.1x is not a panacea. By employing this technology, the network edge has been made more secure.[5] A defense-in-depth mentality i.e. ACLs, VLANs, intrusion detection, firewalls, and good user policies will have to be used to ensure a good network security. 802.1x is just a small part of the overall strategy.

References

1. Cisco Systems "Security: Identification, Please." Packet. Vol. 15 No. 3 (2003): 27-29.

2. Wendell Odem. Cisco CCNA Exam #640-607 Certification Guide. Indianapolis: Cisco Press, 2002

3. Cisco Systems. "Configuring the Switch Ports" Catalyst 2900 XL and Catalyst 3500 XL Software Configuration Guide URL: http://www.cisco.com/en/US/products/hw/switches/ps637/products_configuration_guide_chapter09186a008007e838.html (5 Nov. 2003).

4. Institute of Electrical and Electronics Engineers, Inc. (IEEE). "IEEE Standard for Local and metropolitan area networks — Port-Based Network Access Control." 13 July 2001. URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf (5 Nov. 2003).

5. Foundry Networks. "Using IEEE 802.1x to Enhance Network Security" 28 Oct. 2002. URL: http://www.foundrynet.com/solutions/appNotes/PDFs/802.1xWhite_Paper.pdf (4 Dec. 2003).

6. Cisco Systems. "Configuring IEEE 802.1X Port-Based Authentication" Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide URL: http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a00800da6ff.html(17 Sep. 2003).

7. Cisco Systems. "Deploying 802.1x for LAN Security" Cisco Networkers 2003 Presentation Session SEC-2005. 2003.

8. Cisco Systems. "Network Infrastructure Identity-Based Network Access Control and Policy Enforcement" 16 June 2003. URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns178/c649/ccmigration_09186a0080160229.pdf (5 Dec 2003).

9. Cisco Systems. "User Guide for Cisco Secure ACS Appliance" 20 June 2003 URL: http://www.cisco.com/application/pdf/en/us/guest/products/ps5338/c1629/ccmigration_09186a00801a6d06.pdf (18 Sept. 2003)

Last Updated: July 20th, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS