Global Information Assurance Certification Paper

Network Lock Down

By

Jason Chung-Tung

GSEC Practical Assignment v.1.4b, Option 1

Oct 12, 2004

Table of contents

1 Abstract

The IT Security community has come to a consensus that the devastating effects of the insurgence of works, outbreaks of viruses and proliferation of Trojan horses are largely preventable if the desktop, laptops, servers and network appliances are kept up-to-date with the latest operating system patches, virus protection definitions, adware patterns and spyware signatures. Many organizations have been successful in implementing desktop security compliance policies for the corporate desktops by implementing technologies such as OS patch management tools, centralized Anti-virus protection and desktop software installation restrictions. Unfortunately, these policies are only enforced on corporate desktops and servers, and do not address potentially infected workstations introduced by visitors, consultants and temporary staff.

This paper proposes a Network Lock Down solution based on various technologies that address restricting network access to authorized users and hosts in an effective manner. An analysis of the technologies, which include portbased 802.1X authentication and mac-based authentication, will be discussed and, the implementation of the associated technologies on Cisco Catalyst switches and Microsoft workstation operating systems will be outlined.

Next, a network solution design will be proposed to address the Network Lock Down requirements based on the technologies discussed. The configuration of the Network Lock Down specifications on the Cisco Catalyst switches will be provided for switches running both Cat OS and Native IOS. As well, the requirements and procedures to configure the Network Lock Down specifications will be detailed for Microsoft Windows XP and Windows 2000 operating system.

Lastly, other considerations relating to technologies that could be supplementary to the Network Lock Down solution will be discussed. These include products currently available, as well as, future developments.

2 Introduction

In the last 12 months, Chief Information Officers and IT executives have been marred with operational nightmares stemming from the insurgence of worms, the outbreaks of viruses and the proliferation of Trojan horses.

A July 2004 report from the Aberdeen Group [1], a leading computer and telecom market research firm serving major corporate technology end-users around the world, stated that the average revenue losses associated with the devastating effects of a security-related incident, such as malware, spyware and adware, is estimated to be $ 2 million per incident, based on a study performed on a cross section of all industries globally.

For years, a nalysts from various information security vendors (such as Symantec, Network Associates), as well as, research institutes (such as SANS and CERT) have analyzed the behavior of various malware. Sadly, o ne common theme in their findings is that the great majority of threats paused by the viruses, Trojan horses or worms can be mitigated and virtually eliminated if the proper OS patches are applied to the servers and workstations, the most updated malware signatures are downloaded and installed on the virus protection, adware filtering, and spyware sanitization software.

In light of these findings, the IT departments of many large enterprise organizations have made a conscious effort to ensure that all corporate desktop workstations, laptops and servers are updated with the latest OS patches and protected with the most up-to-date virus signature files. This all seems fine, but there is one major issue that needs to be addressed. Visitors, consultants and temporary staff often connect laptops that do not comply with the corporate OS patch and virus protection management policy, to the corporate network. Since these devices are usually not subject to the same security policy scrutiny which regulates corporate workstations, they are more prone to being infected with various malware. The ultimate question is: How does one effectively prevent unauthorized laptops that have potentially been infected, from accessing the enterprise network.

This document discusses a solution based on various technologies that address restricting network access to authorized users and hosts in an effective manner: Network Lock Down.

3 The Problem: Unrestricted Network Access

In most enterprise networks, network access is prevalent in corporate office buildings. RJ 45 jacks are under the desk in each cubicle, in meeting rooms and sometimes even the kitchen/lunch area. Often, the jack provides an instant

connection to the enterprise switch and a DHCP server, which is all that is required to get access to the enterprise resources from a laptop.

In the past, some network administrators have considered limiting access to the network by making use of the port security feature available on most Cisco Catalyst workgroup and enterprise switches. Port security relies essentially on allowing access to the network, based on verification of authorized and registered MAC address of the user's NIC. This scheme can prove to be very labor intensive taking into consideration all *Moves Adds and Changes* of users in the corporation, as it involves compiling and maintaining a database of all registered MAC addresses on each switch, as well as the specific port where they are allowed to connect. Also, i n most large organizations, users are mobile and often work from corporate offices other than their native office. Tracking the MAC address of such mobile users quickly becomes extremely resource intensive .

In response to this challenge, Cisco developed the Secure User Registration Tool (URT) [3] in combination with the VLAN Membership Policy Server (VMPS) [4] which promised to provide central management of port security and administration of MAC addresses. However, the technology has several limitations. First, Its implementation can be quite complex, as it requires the implementation of Virtual Trunking Protocol (VTP) on all switches in the enterprise. In many organizations, security policies specify that VTP should be disabled or configured in transparent mode in order to shun the possible security vulnerability associated with it. Second, the access control relies largely on a database (containing MAC-to-VLAN membership records) which is transferred from the VMPS server to the switches using a weak and unprotected file transfer protocol (e.g. TFTP). Third, the database is downloaded to the switch at boot time, and can only be updated manually. This functionality provides scalability limitations. Forth, the entire database of all MAC address records on the enterprise must be loaded on each switch, which exhausts memory resources, thereby affecting the operational performance of the switch and limiting the number of workstations, laptops and servers that can be policed. Fifth, cloning of MAC addresses are relatively easy to configure, and circumvents the access control mechanism. For these reasons, Port Security, URT and VMPS are rarely implemented to control workstation/laptop access to the network in large enterprises.

In cases where IT budgets are not available to fund the resources and tools necessary to prevent network security incidents, the need to provide network access to users, from anywhere and everywhere in the corporate office, largely outweighs the need to protect it against potential malware infection through unauthorized network access. As a result, many IT organizations choose to provide unrestricted network access with the pretext of ensuring employee productivity. But in fact, this network access prevalence also provides network access to unauthorized users, such as visitors, consultants and temporary staff

who may unintentionally be carriers of viruses, worms and Trojans horses. The simple request to print a document on the LAN-attached printer or access the Internet by a visitor or consultant may seem benign, but provides ample opportunity to contaminate the environment.

There are several other threats that can exploit the weakness of unrestricted network access. These threats include network intelligence reconnaissance through the use of sniffers and man-in-the middle attacks through the use of rogue DHCP serve rs, to name a few. However, the focus of this document is not to emphasize on the threats associated with unrestricted network access, rather it is to explore the various countermeasures that could be used to overcome the vulnerability.

4 The Solution: Network Lock Down

4.1 Overview

In order to control which devices are allowed to access the corporate enterprise network, some form of authentication is required. In the same way that employees of an organization are granted access to the corporate office facilities by presenting or scanning some form of identification (badge, token or electronic pass card), network access should be granted by means of username and password authentication. User identification provides the ability to restrict unauthorized users, such as visitors, consultants and temporary staff, from accessing the network. The port-based access control mechanism based on the 802.1X standard can be implemented to enforce user authentication on the access/workgroup switches connecting end user workstations and laptops to the enterprise network.

It should be noted that user authentication does not guarantee that the workstation being connected to the network complies with the operating system patching and virus protection internal policies. However, it does provide a means for tracing the offending user. This paper does not focus on the e nforcement of such policies, however, some suggestions are discussed in Section 5 Other Considerations.

Unfortunately, user authentication does not provide the same effectiveness with devices other than the end user workstations and laptop, because 802.1 X support is not practical for servers and not available for printers and miscellaneous network appliances such as IP-enabled KVM switches. For these 802.1X non-compliant devices, a different access control mechanism must be implemented. Since these devices are stationary and relatively permanent by nature, configuration of Port Security provides an effective solution.

The following sections wi ll discuss the 802.1X port-based authentication mechanism, as well as, the MAC-based authentication Port Security technology.

Because of the prevalence of Cisco devices in the enterprise market place, this paper will discuss specific features supported on the Cisco Catalyst family of switches. Undoubtedly, these features may also be supported by other vendors such as Foundry Networks.

4.2 Technology Specifications

4.2.1 Port-Based Authentication

Access to the network can be controlled using Port-based Authentication which is based on the IEEE 802.1X-2001 standard. The IEEE standard for Port-Based Network Access Control 802.1 X in Local and Metropolitan Area Networks [2] was sponsored by the LAN/WAN Standards Committee of the IEEE Computer Society, was approved by the IEEE-SA Standard Board on June 14, 2001, and further approved by the American National Standards Institute (ANSI) on October 25, 2001. The standard describes the mechanism for authenticating network clients on a user ID or device basis before granting access to the network.

The 802.1X standard applies to end devices and users trying to connect to ports of other devices such as a switch or a wireless access point. Authentication and authorization can be implemented with back-end connection to an authentication server such as a RADIUS server. With the support for the RADIUS protocol, authentication can be performed through the AAA server as a proxy to various directory services such as an LDAP directory server, a Windows NT Domain Controller or a Windows Active Directory. The standard provides automated user identification, centralized authentication, key management, and provisioning of LAN connectivity. It ties the Extensible Authentication Protocol to both the wired and wireless LAN media and supports multiple authentication methods, such as RSA SecurID token cards or key fobs, Kerberos, one-time passwords, certificates, and public key authentication.

Once 802.1X authentication is enabled (both in the client and authenticator), a successful authentication must be completed before virtually ANY traffic is allowed to transit the network from the client, including critical traffic, such as DHCP requests, regardless of whether the link is established between the client and authenticator (switch port). The only traffic that is allowed on the port, prior to a successful authentication includes the following protocols: 802.1X, Spanning Tree Protocol (STP) and CDP (Cisco Discovery Protocol) if enabled.

The use of 802.1X is well on its way to becoming an industry standard. Windows XP implements 802.1X natively. Microsoft 802.1X Authentication Client is

available for Windows 2000, Windows 98 and Windows NT 4.0. Please refer to section 4.3.2 Desktop Operating System Support for more details.

As well, Cisco also supports the IEEE 802.1X standard on newer Catalyst switches. Further information on specific 802.1X Authentication features supported on the various switch models and IOS image versions is detailed in the section 4.3.1 Cisco Hardware and Software Support.

The 802.1X Port-based authentication standard grants a workstation access to the network based on a user's username and authentication key. The standard does not validate that the appropriate operating system patches, application fixes and virus definition updates have been applied. However, this mechanism does allow the administrator to control network access and identify active users.

4.2.2 802.1 X Protocol

The IEEE 802.1X Port-based Authentication protocol uses the Extensible Authentication Protocol (EAP) to exchange messages between a workstation (referred to as the *supplicant)* and the workgroup switch (referred to as the *authenticator)* by means of a centralized user database (referred to as the *authentication server).* The 802.1X standard specifies the encapsulation method over various media types such as EAP over LAN (EAPOL) and EAP over Wireless (EAPOW).

To initiate the authentication process, both the workstation and the switch must be enabled with the 802.1X feature. Upon connection, either the supplicant or the authenticator can initiate the authentication process. If configured to automatically initiate the process, the authenticator will request a n EAP identity from the supplicant. However, if the supplicant is not configured to request the EAP identity automatically, the supplicant may send an EAPOL Start message to the supplicant. In return the authenticator will transmit an EAP identity request message.

Upon receipt of the request, the supplicant will begin to exchange authentication packets with the authentication server through the intermediary of the authenticator.

The following diagram [6] illustrates the 802.1X Authentication process between the supplicant, the authenticator and the authentication server.

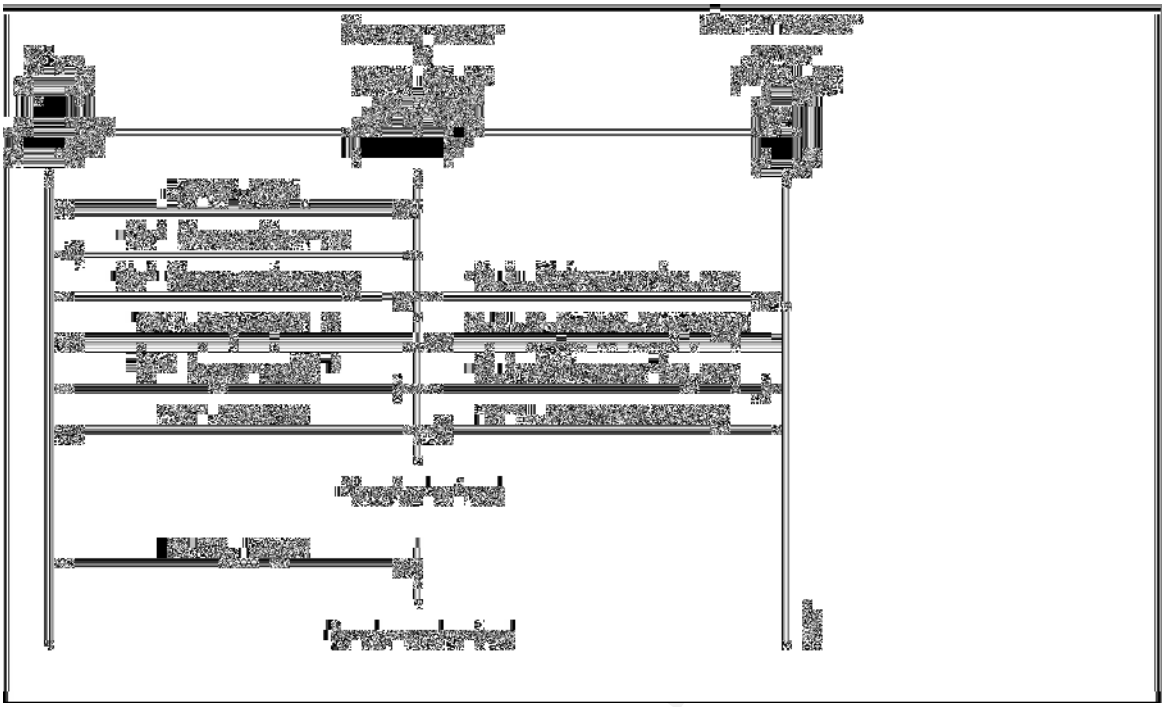

Figure 1. 802.1X Authentication Process. Source: www.cisco.com [6]

Once the authentication process is complete, the switch port will be in one of two states: authorized and unauthorized. Upon successful completion of the 802.1X authentication process, the switch will change the state of the port from unauthorized to authorize, thereby allowing all traffic to flow through. In the unauthorized state, however, the switch will block and drop all packets except for the 802.1 X, CDP and STP traffic, as is the case prior to the authentication process.

4.2.3 MAC-Based Authentication

With MAC-based authentication, access to the switch ports is controlled by comparing the MAC address of the device connected with a list of predefined MAC addresses allowed to communicate on the port.

As discussed earlier, MAC-based authentication can be implemented using Port Security feature available on Cisco Catalyst Switches which allows the network administrator to specify which MAC addresses are allowed to communicate on the specific port of a specific switch.

MAC-based authentication can be implemented using a more dynamic approach, which would allow MAC addresses to roam across the enterprise from switch to switch. This approach involves the implementation of the Cisco URT tool and the VMPS server.

Although the effectiveness of port security based on MAC address authentication for mobile users is limited, it can still be very effective in controlling LAN access for devices that do not require mobility relative to the switch (such as servers) , or those devices that do not support authentication mechanism (such as printers, HP printers server appliances, KVM console management appliances.

In addition to MAC address authentication, the Port Security feature also provides the ability to limit the number of devices (e.g. MAC addresses) allowed on each given switch port.

For the purpose of this paper, we will primarily discuss Port Security without The URT Tool and the VMPS server, as our application of the MAC-based authentication focuses on securing ports for servers, printers and network appliances that are relatively permanent and do not require mobility.

4.2.4 Port Security

The Cisco Catalyst Port Security feature provides the ability to control port access to a switch based on MAC address. As well, Port Security extends the access control to VLAN membership. In addition, Port Security provides the ability to control how many devices are allowed to communicate on a given port.

While implementing Port Security with MAC address configuration, the MAC address can be manually configured or dynamically learnt from the switch-attached device.

As well, Port Security provides the ability to control the action taken by the switch in the case of a security violation. The switch may be configured to shutdown the port, or simply drop all packets while remaining enabled.

4.3 Hardware and Software Support

4.3.1 Cisco Hardware and Software Support

The 802.1 X Authentication feature is supported on the following Cisco platforms: Catalyst 6500, Catalyst 6000, Catalyst 4900 series, Catalyst 4003, 4006, Catalyst 3750, Catalyst 3550, Catalyst 2970, Catalyst 2955, Catalyst 2950 and Catalyst 2940 switches. In addition to the hardware specification, the operating system (Cat OS or Native IOS) must support RADIUS and 802.1X Authentication.

In order to support 802.1X Authentication, Cisco Catalyst switches must run Cisco IOS 12.1(13)E or later releases, or, Cisco Cat OS Release 6.2 or later releases.

4.3.2 Desktop Operating System Support

Microsoft supports the 802.1X authentication client natively in the Windows XP operating system.

For workstations running the Windows 2000 operating systems workstations with Service Pack 3, a software package is available free of charge from Microsoft that provides the necessary tool to support 802.1X client authentication. For users that have updated their windows 2000 workstations with Service Pack 4, no additional software packages are required, as the 802.1X client authentication features are included.

Microsoft has also developed the 802.1X Authentication Client packages for Windows 98 and Windows NT 4.0 Workstation. These packages are available through Microsoft Premier and Alliance Support organizations.

The following table summarizes the support for 802.1X Client Authentication on the Microsoft suite of operating systems [5]:

Operating System	Service Pack Required	802.1x Authentication Support Comments
Windows XP	All	Supported natively
Windows 2000	SP3	Requires download of 802.1X authentication client package
Windows 2000	SP4	Supported natively
Windows 98	All	Requires download of 802.1X authentication client package
Windows NT 4.0 workstation	All	Requires download of 802.1X authentication client package

Table 1. 802.1X Authentication Support For Various Desktop Operating Systems

4.4 Solution Design

4.4.1 Network Design

For the Network Lock Down solution, all switch ports connecting to end user desktop and laptop workstations will enforce the security policy compliance to port-based authentication by using the 802.1X authentication protocol. In effect, all users connecting to the network using corporate workstations will be prompted to provide a valid username-password pair of attributes before being granted access to the network enterprise.

One limitation of the current 802.1X authentication implementation in the Cisco Native IOS running on Catalyst switches, lies in the fact that only one client

needs to be authenticated per port, for all hosts to be granted network access. Cisco recommends having Port Security configured on 802.1X switch ports. With Port Security enabled, only one MAC address is allowed on the port, and only one client will authenticate with the RADIUS server. As a result, this mechanism will not effective ly support environments where workstations are connected to hubs before aggregating on a Catalyst switch. For example, only the first user that connects to the hub authenticates with the switch to provide access, but also disconnects all users on the hub when it disconnects from the network. This is a significant limitation, which draws to the conclusion that hubs should not be implemented where 802.1 X authentication is required.

It is important to note, that the 802.1X authentication implementation in the Cisco Cat OS does provide the ability to authenticate multiple hosts independently.

In the event that the user fails to authenticate successfully, a VLAN (e.g. guest-vlan) will be implemented to provide minimal and restrictive access. The 802.1X authentication implementation on Cisco Catalyst switches provides the ability to block all traffic or allow the user to join a specific VLAN. By implementing strict access control list (ACL) to the VLAN, the guest-vlan can be an effective solution to provide users the ability to access limited resources such as the latest OS patches, virus definitions, or simply the Internet.

All switch ports providing connectivity to servers, printers and non-802.1X-compliant devices, will be authenticated using the MAC address of the network interface cards. The MAC address of each of these devices will be configured on the port of the switch to which it connects using the Port Security feature of Cisco Catalyst switches. In the event that the MAC address authentication was to fail, the port will be configured to shutdown.

4.4.2 Topology

The topology of the network assumes a layered network architecture consisting of Core routers, Distribution switches and Access/Workgroup switches. Enforcement of the network security appliance is performed at the Access layer for the desktop and laptop workstations, and at the Access or Distribution layer for the servers, printers and shared network appliances.

The following diagram illustrates a typical network topology on which the Network Lock Down solution can be applied.

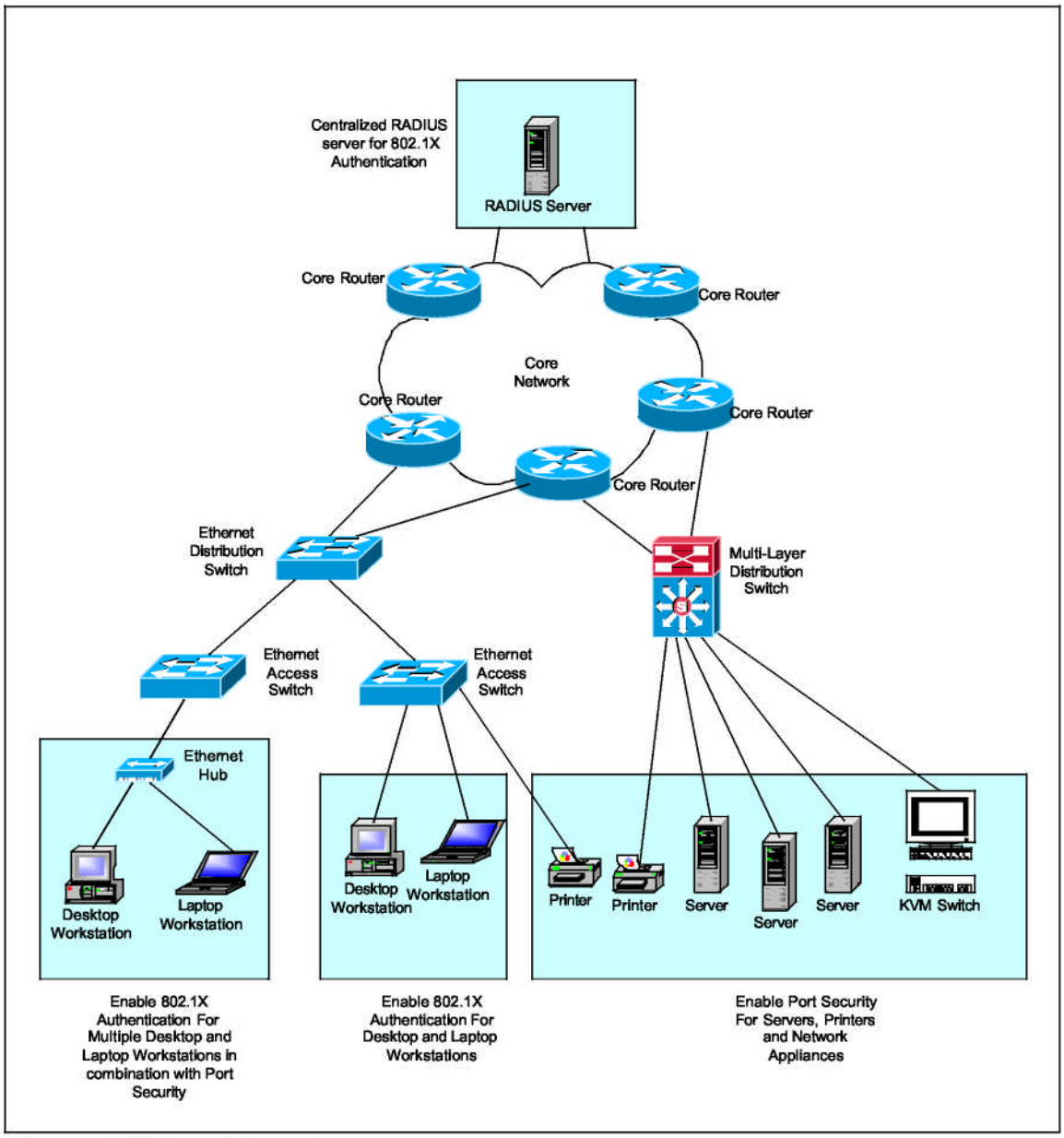

Figure 2. Network Topology

4.5 Device Configuration

4.5.1 802.1X Switch Configuration

4.5.1.1 Cat OS switches

A pre-requisite to running 802.1X authentication on the Catalyst switch is the configuration of a least one RADIUS server. The following commands enable switch authentication using a RADIUS server:

```
Set radius server <ip-address> auth-port <port>
Set radius key <key>
Set authentication enable radius enable
```

For more details on configuring Authentication using RADIUS protocol on Cisco Catalyst Switches running Cat OS, please refer to [11].

In order to enable 802.1X authentication support on the Catalyst switch, the service must be enabled. The following global command enables the 802.1X authentication service globally:
To enable 802.1X authentication on a specific switch port, the port must be configured as illustrated in the following commands:

```
Set dot1x system-auth-control enable
```

To allow unauthorized devices (device having failed 802.1x authentication) to join a

```
Set port dot1x <module>/<port> port-control auto
```

guest-vlan, the port must be configured as illustrated in the following commands:
To enable multiple hosts to perform 802.1X authentication on a single port, the

```
Set port dot1x <module>/<port> guest-vlan <vlan-number>
```

port must be configured as illustrated in the following command:

When configured with multiple-host authentication, an 802.1X authentication will

```
Set port dot1x <module>/<port> multiple-authentication
enable
```

only join the VLAN assigned to the port, as opposed to that configured in the RADIUS server.

For more details on configuring 802.1X Authentication on Cisco Catalyst Switches running Cat OS, please refer to [11].

4.5.1.2 Native IOS switches

As discussed in the Cat OS switch configuration, the Native IOS switches must be configured to authenticate using at least one RADIUS server, in order to enable 802.1 X authentication. The

The following configuration commands enable switch authentication using a RADIUS server:

```
radius-server host <ip-address> auth-port <port> key <key>
aaa new-model
aaa authentication dot1x default group radius enable
```

In order to enable 802.1X authentication support on the Catalyst switch, the service must be enabled. The following global configuration command enables the 802.1X authentication service globally:
To enable 802.1X authentication on a specific switch port, the port must be configured as illustrated in the following configuration commands:

```
dot1x system-auth-control
```

To allow unauthorized devices (device having failed 802.1x authentication) to join a guest-vlan, the port must be configured as illustrated in the following configuration

```
      interface <module>/<port> dot1x port-control auto
```

commands:

```
interface <module>/<port>
 dot1x guest-vlan <vlan-number>
```

Enabling multiple hosts to gain access into an 802.1X port, does not provide an effective restriction. In native IOS, only the first host is required to authenticate. Once authenticated, all other hosts are allowed to access the network without authentication. Furthermore, once the first hosts disconnects, all other hosts are disconnected simultaneously. As discussed earlier, the behavior in Cat OS is somewhat different.

For more details on configuring 802.1X Authentication on Cisco Catalyst Switches running native IOS, please refer to [6].

4.5.2 802.1X Workstation Configuration

4.5.2.1 Windows 2000

Workstations that are running Windows 2000 with Service Pack 3 require the manual download and installation of the Microsoft 802.1X Authentication Client.

However, Windows 2000 with Service Pack 4 includes the Microsoft 802.1X Authentication Client.

To configure the Microsoft 802.1X Authentication Client, it is necessary to start the Wireless Configuration service on the workstation. The workstation can be

configured to start the service manually or automatically, however, it is recommended that the service be started automatically every time the workstation is booted.

Once started, the next step is to configure 802.1X on the network interface card. This can be done by displaying the properties of the Network Connection, and selecting the Authentication Tab of the specified LAN connection. The following figure illustrates the configuration window.

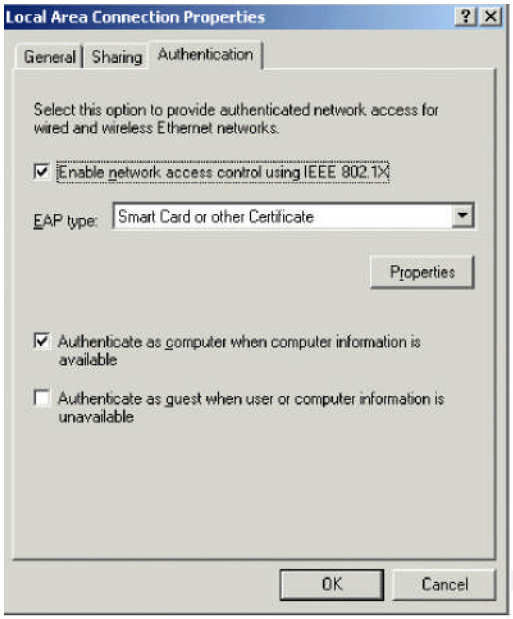

Figure 3. LAN Connection Properties: 802.1 X Configuration for Windows 2000.

There are several ways to EAP authentication types. For the simplest form of authentication, simply select the followi ng EAP type: Protect EAP (PEAP), which will use your Windows username and password to authenticate.

For more details on configuring 802.1X Authentication on Windows 2000, please refer to [9].

4.5.2.2 Windows XP

To configure the Microsoft 802.1X Authentication Client, it is necessary to start the Wireless Zero Configuration service on the workstation. The workstation can be configured to start the service manually or automatically, however, it is recommended that the service be started automatically every time the workstation is booted.

To configure 802.1 X authentication on the network interface of a Windows XP workstation, display the properties on the specific Network Connection. Select the Authentication Tab, to configure the 802.1X properties.

As indicated in the Windows 2000 configuration of 802.1X Authentication, select the Protect EAP (PEAP) option as the EAP Type, in order to use the Windows username and password for authentication. The following diagram illustrates the configuration window:

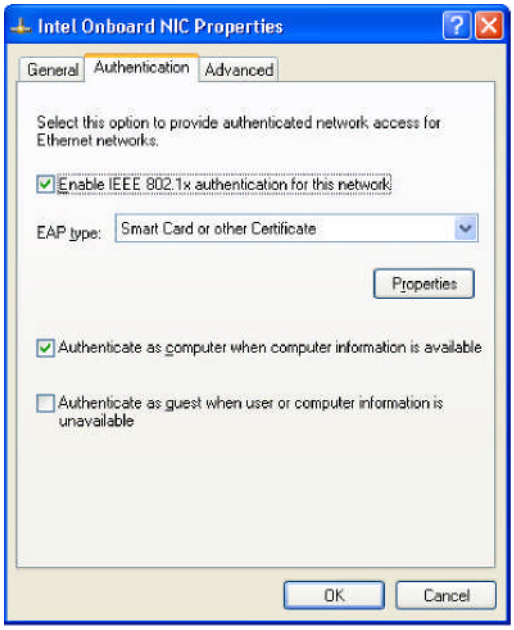

Figure 4. LAN Connection Properties: 802.1 X Authentication for Windows XP.

For more details on configuring 802.1X Authentication on Windows XP, please refer to [10].

4.5.3 Port Security Switch Configuration

Switch ports that are connected to servers, printers and other network appliances such as KVM switches, must be configured with Port Security, in order block all other devices from being able to gain access to the network. To enable this feature, the switch port must be configured with the MAC address of the device that is allowed to connect to the network.

4.5.3.1 Cat OS switches

The following Cat OS command [7] illustrates the configuration of one or multiple MAC addresses to secure on the switch port, as well as, the VLAN membership specification:

```
Set port security <module>/<port> enable <mac-address>
<vlan>
```

The following Cat OS command illustrates the configuration of the maximum number of MAC address to secure on the switch port:

```
Set port security <module>/<port> maximum <number-of-mac>
```

The following Cat OS command illustrates the configuration of the action to

```
Set port security <module>/<port> violation shutdown
```

execute upon port security violation.

4.5.3.2 Native IOS switches

The following native IOS command [8] illustrates the configuration of one or multiple MAC addresses to secure on the switch port. Note, VLAN membership specification can not be configured on the native IOS switches.

```
      interface <module>/<port> switchport mode access
 switchport port-security <mac-address>
```

The following native IOS command illustrates the configuration of the maximum number of MAC address to secure on the switch port:

```
interface <module>/<port>
 switchport port-security maximum <number-of-mac>
```

The following native IOS command illustrates the configuration of the action to execute upon port security violation.

```
interface <module>/<port>
 switchport port-security violation shutdown
```

5 Other Considerations

The solution described in this paper can be supplemented by the use of endpoint enforcement tools. These tools provide the ability to enforce desktop security compliance by validating authorized standard Operating Systems, installation of the latest OS patches, virus definitions files and authorized software before granting access to the network. The scheme used by most tools is based on a lightweight agent that resides on the client workstation. The agent provides the access control server with the system attributes that are verified for desktop security policy compliance.

A recent article published in the Information Security magazine [13] provides a brief analysis of several products currently available on the market. The products that seem to provide the most potential are the CyberGatekeeper LAN from InfoExpress and the Sygate Secure Enterprise by Sygate. Both tools make use of a persistent agent mechanism that runs on the client workstation to enforce security compliance for the desktop.

In June 2004, Cisco announced the availability of the first generation of Network Admission Control solutions [14]. The solution is currently supported one a series of Cisco Access and Mid-range routers. Endpoint security policy enforcement is performed by the Cisco Trust Agent software which is installed on the desktop/laptop workstation. The agent communicates with a centralized server which verifies the desktop attributes for compliance through the intermediary of the Cisco router. An article in Network World Fusion [15] pointed out that the development of NAC-support on Catalyst switches was targeted for the first quarter of 2005, but its future was uncertain.

6 Acronyms

ANSI	American National Standard Institute
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAPOW	EAP over Wireless
IEEE	The Institute of Electrical and Electronic Engineers
KVM	Keyboard Video and Mouse Local Area Network
LAN	Media Access Control
MAC NIC	Network Interface Card
RADIUS	Remote Access Dial In User Service
STP TFTP	Spanning Tree Protocol Trivial File
URT	Transfer Protocol Cisco's User
VLAN	Registration Tool Virtual Local
VMPS	Area Network VLAN Membership
VTP	Policy Server Virtual Trunking Protocol

7 References

[1] Hurley, Jim "Return on Risk: Managing Security Spend to Avoid and Prevent Financial Loss from Internet Security Problems", Aberdeen Group, July 27, 2004. URL: http://www.aberdeen.com/summary/report/perspective/07040001.asp

[2] IEEE Standard 802.1X, 2001 Edition, "IEEE Standards for Local and Metropolitan Area Networks: Port-Based Network Access Control", June 14, 2001. URL: http://standards.ieee.org/getieee802/download/802.1 X-2001.pdf

[3] Cisco Systems Inc., "White Paper: Assigning Host-Based VLANs in Cisco Switch Products Using Cisco Secure User Registration Tool". URL: http://www.cisco.com/warp/public/cc/pd/wr2k/urto/prodlit/urt_wp.pdf

[4] Cisco Systems Inc., "Configuring Dynamic Port VLAN Membership with VMPS", Catalyst 6000 Family Software Configuration Guide, Release 6.3 and 6.4, Chapter 18. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/confg_gd/vmps.pdf

[5] Microsoft Corporation, "Microsoft 802.1X Authentication Client", Market Bulletin, January 10, 2003. URL: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021 xclient.asp

[6] Cisco Systems Inc., "Configuring IEEE 802.1 Port-Based Authentication", Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2SX, Chapter 33. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/dot1x.pdf

[7] Cisco Systems Inc., "Configuring Port Security", Catalyst 6500 Series Switch Software Configuration Guide, Release 8.3, Chapter 36. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/secport.pdf

[8] Cisco Systems Inc., "Configuring Port Security", Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, Release 12.1E, Chapter 26. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/port_sec.pdf

[9] Microsoft Corporation, "Using 802.1x Authentication on Computers Running Windows 2000", Article Q313664, Revision 13.0, January 16, 2004. URL: http://support.microsoft. com/default.aspx?scid=kb;en-us; 313664

[10] Microsoft Corporation, "To Set up 802.1X Authentication", Windows XP Professional Product Documentation. URL: http://www.microsoft. com/resources/documentation/windows/xp/all/proddocs/en-us/8021x_client_configure.mspx

[11] Cisco Systems Inc., "Configuring 802.1X Authentication", Catalyst 6500 Series Switch Software Configuration Guide, Release 8.3, Chapter 37. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/8021x.pdf

[12] Cisco Systems Inc., "Configuring the Switch Access using AAA", Catalyst 6500 Series Switch Software Configuratio n Guide, Release 8.3, Chapter 21. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_3/confg_gd/authent.pdf

[13] Curtis E. Dalton, "End of the Line: New Solutions Help you Secure Endpoints", Information Security, June 2004. URL: http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss407_art812,00.html

[14] Cisco Systems Inc., "Cisco Announces Availability of Network Admission Control Solutions", News Release, June 21, 2004. URL: http://newsroom.cisco.com/dlls/2004/prod_062104b.html

[15] Phil Hochmuth, "Cisco Set to Unleash Security Plan", Network World Fusion, June 18, 2004. URL: http://www.nwfusion.com/news/2004/0618cisconac.html