Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wired 802.1x Security

Any typical TCP/IP network that uses DHCP is defenseless against individuals who can find an unsecured network drop . The DHCP server dutifully grants the unauthorized computer an IP address, and the attacker is able to launch a variety of attacks, such as breaking into specific servers, eavesdropping on network packets, and unleashing a worm or Denial of Service (DoS) attack. An Internet attacker breaching your firewall would have the same level of access. 802.1x provides a solution for such problems. It is mostly use...

Copyright SANS Institute
Author Retains Full Rights

AD

WIRED 802.1X SECURITY

By Mohammed Younus

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

802.1x and other LAN Technology 5
802.1x Authentication Process 5
802.1X Guidelines and Restrictions 8
Configuring 802.1x Authentication 9
Displaying 802.1X Statistics and Status 10
Optional Configuration Parameters 11
Periodic Re-Authentication 11
Manually Re-Authenticating a Client Connected to a Port 11
Quiet Period 11
Switch-to-Client Retransmission Time 11
Switch-to-Client Frame-Retransmission Number 12
Multiple Hosts 12
Benefits of Cisco's implementation of 802.1x 13
Setting up Windows XP Professional for 802.1x Client Authentication 13
Configuring the 802.1x client (Windows XP Professional) 15

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

Any typical TCP/IP network that uses DHCP is defenseless against individuals who can find an unsecured network drop . The DHCP server dutifully grants the unauthorized computer an IP address, and the attacker is able to launch a variety of attacks—such as breaking into specific servers, eavesdropping on network packets, and unleashing a worm or Denial of Service (DoS) attack. An Internet attacker breaching your firewall would have the same level of access.

802.1x provides a solution for such problems. It is mostly used to secure Wi-Fi networks, but 802.1x can provide protection even for the wired network. This paper shows how to implement this IEEE standard on a wired network to guard against unauthorized individuals exploiting physical access to the network.

This paper defines the fundamentals of 802.1x authentication, explains how the authentication process works in 802.1x, and provides the detailed steps to implement 802.1x in a switched LAN environment using Cisco's Implementation of 802.1x. This paper will also show you how to setup the Microsoft Client for 802.1x authentication in the wired LAN environment. In conclusion, we provide packet captures of 802.1x traffic.

Background

Historically, we have relied on physical security to limit access to network drops and used fully switched networks to derive a degree of protection against eavesdropping. However, malicious users can use Address Resolution Protocol (ARP) redirects to fool switches into facilitating eavesdropping attacks. Unauthorized individuals can plug into a company's network and attack resources. All it takes is one branch office, connected to the corporate network [intranet: internal web server] that fails to control access to network drops at its location. Securing DHCP servers from leasing IP addresses to unauthorized computers simply isn't practical or effective. An attacker can find unused IP addresses easily (Tulloch, 2004). Implementing 802.1x on the network solves the problem mentioned above whereby all the clients will need to authenticate before accessing the network.

Introduction

IEEE 802.1x is a standardized framework defined by Institute of Electrical and Electronics Engineers (IEEE), designed to provide port-based network access. 802.1x authenticates network clients using information unique to the client and with credentials known to the client ("Overview of 802.1x", n.d. , Page 1). By authenticating user access at the network edge, network administrators can be assured that no unauthorized access will take place, and all user authentication can take place on a centralized authentication server.

© SANS Institute 2000 - 2005 Author retains full rights.

Fundamentals of 802.1x

To understand 802.1x, let us define some fundamental terminology.

Supplicant (Client) – In IEEE terminology, the supplicant refers to the client software that supports the 802.1x and EAP Protocols. The supplicant software may be integrated into the client operating system, included in the client device firmware, or implemented as add-in software. The term supplicant also refers to the actual client requesting access to the network, ("Overview of 802.1x", n.d, Page 2).

Authenticator – The device to which the supplicant directly connects and through which the supplicant obtains network access is known as authenticator. The authenticator could be LAN switch ports and Wireless Access Points (WAP). In case of LAN the switch must support 802.1x in order to work as authenticator.

Authentication Server – As the name suggests, this is the actual source of authentication services provided to end points. Based on the username/password or the user credentials supplied to the server, it decides whether to allow or deny users access to the network. The 802.1x standard specifies that Remote Authentication Dial-In User Service (RADIUS) is the required Authentication Server that supports the following RFC's:

- RFC 2284 PPP Extensible Authentication Protocol ("PPP EAP", 1998)
- RFC 2865 -Remote Authentication Dial In User Service ("RADIUS", 2000))
- RFC 2869 - RADIUS Extensions ("RADIUS Extension", 2000)

Port Access Entry (PAE) – The PAE refers to the processes executing the authentication protocols and algorithms associated with a port. PAE is the 802.1x "logical" component of the client and authenticator that exchange EAP messages.

EAP – The Extensible Authentication Protocol RFC 2284 was originally written as an optional authentication mechanism for the Point-to-Point Protocol RFC 1661 ("ppp", 1994). EAP is used between the client and the authenticator. EAP Messages are carried over different media depending upon the encapsulation method used by 802.1x. Some of the encapsulation methods are:

- EAP over LAN (EAPOL)
  This encapsulation method defines how the EAP packets are encapsulated when transmitted over LAN media protocol like Ethernet, Token Ring or FDDI.

- EAP over Wireless (EAPOW)
  Describes how EAP packets are encapsulated when transmitted over wireless media.

© SANS Institute 2000 - 2005 Author retains full rights.

802.1x and other LAN Technology

In a typical Microsoft network, in order to access the File/Print Server the clients needs to provide the domain user name and password. This kind of client / server authentication is also used for other network services including email, intranet and other specialized applications. This method does not provide total network security. Some network equipment vendors include VLAN's, ACL and MAC filtering as the effective mechanism for securing network access. Each control mentioned above provides a unique advantage, but are often unique to each vendor. IEEE 802.1x is a standardized method for securing network access at the network device. By combining 802.1x with the existing network security methods the administrators can be confident that their network perimeter (edge access) is secure.

802.1x Authentication Process

The client and the switch must support 802.1x and needs to be enabled before any authentication takes place. A successful authentication is required before allowing ANY traffic to transit the network from the client side including the DHCP traffic.

Before Authentication

The only messages that will be accepted from the client are the EAP messages, which will be forwarded to the authentication Server. The authenticator's PAE is set to uncontrolled state. As you can see in *figure 1 - Before Authentication* ("Using IEEE 802.1x to enhance network security", n.d, page 4), in this state all other network services are disabled

Authentication Process

After 802.1x client is powered on it will transmit the EAP message to the switch. The switch will forward the client's request to the authentication (RADIUS) server without changing its contents. The RADIUS server will verify the user credential and transmit back its response to the switch, which will determine whether the port remains in an uncontrolled state (access denied), or changes to a controlled state (access granted), as you can see in *figure 2 - After Successful Authentication*, ("Using IEEE 802.1x to enhance network security", n.d, page 5). If the RADIUS response is "Access granted" then client port state will change to "controlled " and it will then allow other network services to flow. If the authentication fails, the switch port will remain in an uncontrolled state, and in some cases the port will be disabled (depends on vendor implementation).

© SANS Institute 2000 - 2005 Author retains full rights.

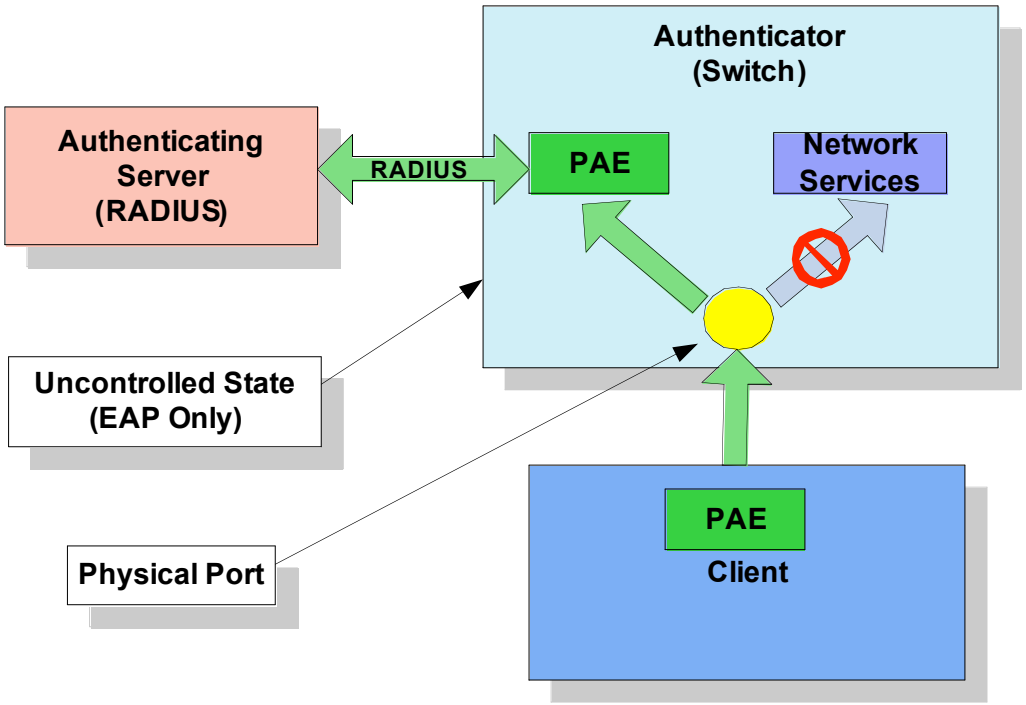


Figure 1 - Before Authentication

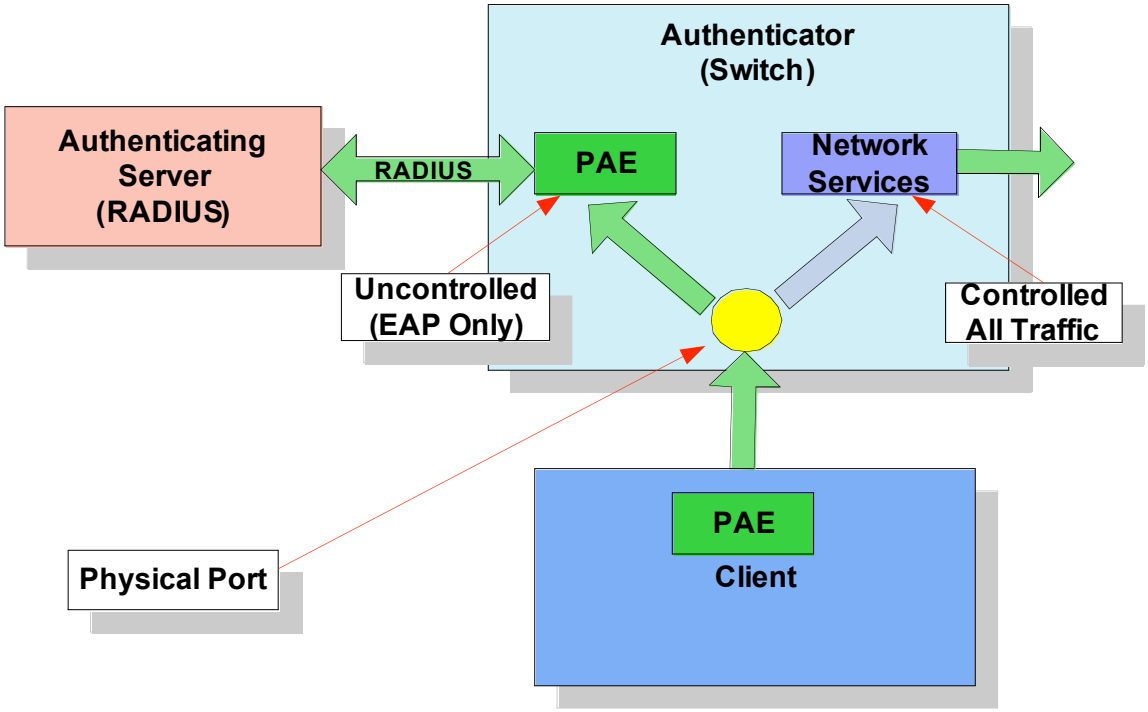


Figure 2 – After Successfull Authentication

© SANS Institute 2000 - 2005 Author retains full rights.

Cisco's Implementation of 802.1X:

After understanding the basic principles of 802.1x we will take a scenario and explain how 802.1x authentication works, how it should be implemented and configured. The scenario uses Cisco 3550 switches and RADIUS Server with clients as indicated in *figure 3 - 802.1x Device Roles.*

Note: Cisco implementation refers to the uncontrolled and controlled states as unauthorized state and authorized state.

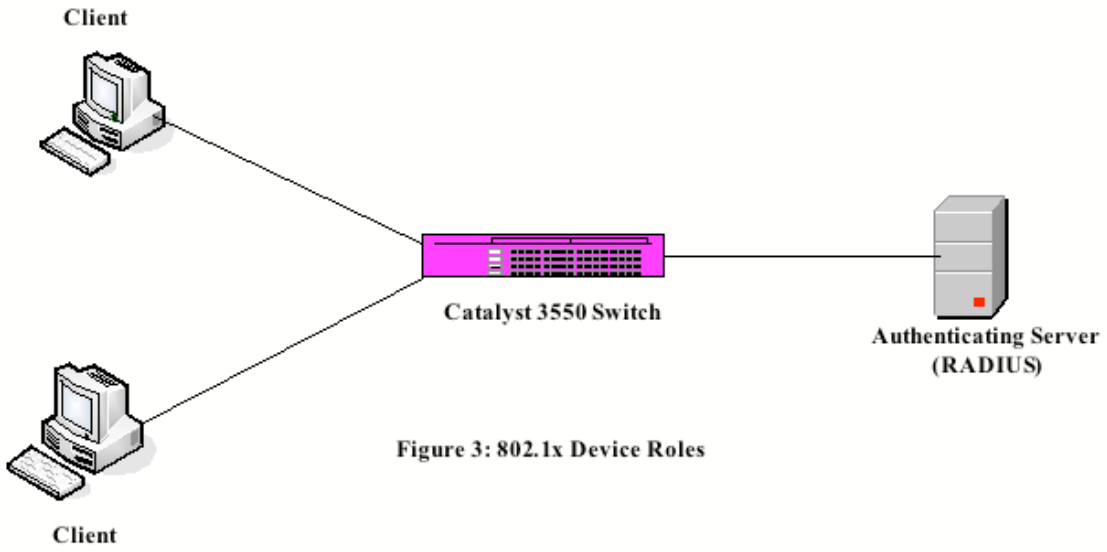


Figure 3: 802.1x Device Roles

In Cisco's implementation either switch or client can initiate authentication. Exchange of EAP frames depends on the authentication method being used. *figure 4 - Message Exchange* shows message initiated by the client using the One-Time-Password (OTP) authentication method with a RADIUS server. The client starts authentication by sending an EAPOL-start frame to the access switch which then replies with an EAP-request/identity frame to the client to request its identity and after receiving this frame the client responds with an EAP-response/identity frame. When the client supplies its identity, the switch starts working as the role of intermediary, passing EAP frames between the client and the authentication server until authentication succeeds or fails. If the authentication succeeds, the switch port becomes authorized. When a client logs off, it sends an EAPOL-logoff message, causing the switch port to transition to the unauthorized state.

© SANS Institute 2000 - 2005 Author retains full rights.

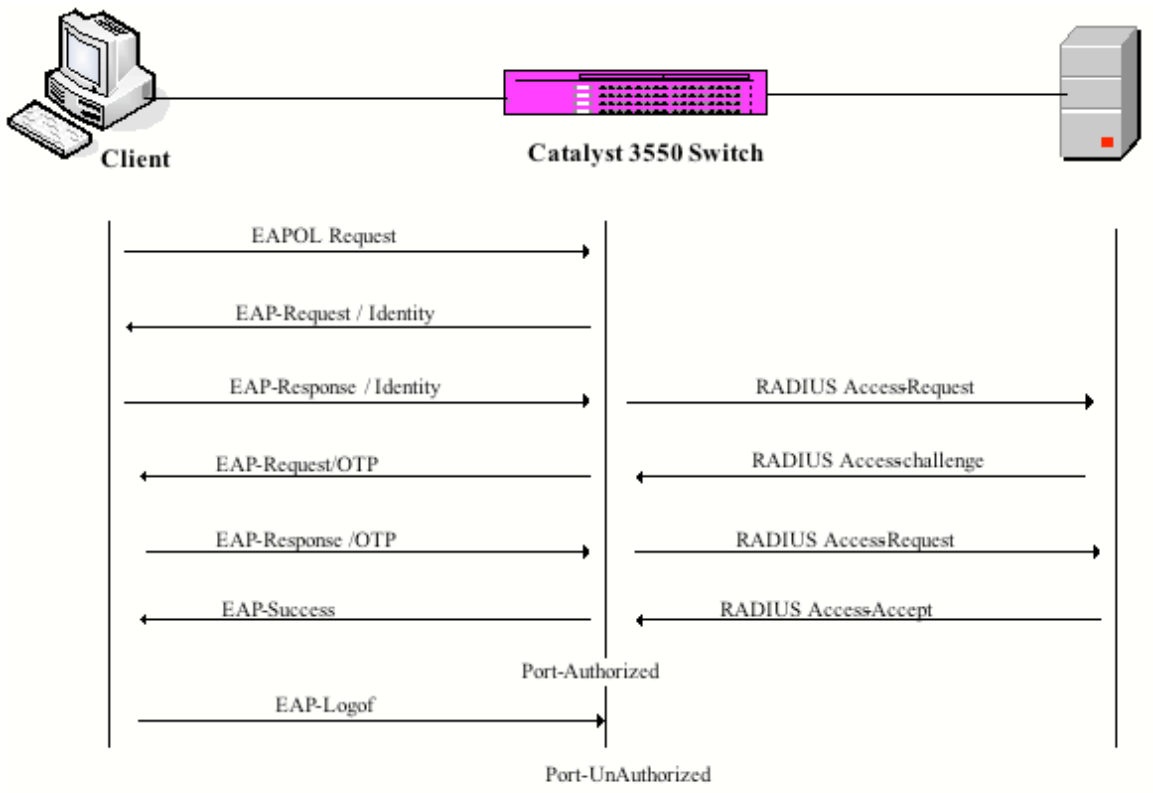


Figure 4 : Message Exchange
("Configuring 802.1x Port-Based Authentication" ,n.d,page3)

802.1X Guidelines and Restrictions

When configuring Cisco switches for 802.1X authentication keep in mind the following configuration guidelines:

- When 802.1X is enabled, ports are authenticated before any other Layer 2 or Layer 3 features are enabled.
- The 802.1X protocol is not supported on these port types:
  –Trunk port
  –Dynamic ports
  –Dynamic-access ports
  –EtherChannel port
  – Secure port
  –Switch Port Analyzer (SPAN) destination port

© SANS Institute 2000 - 2005 Author retains full rights.

Configuring 802.1x Authentication

The first step in configuring 802.1x authentication on the switch is to enable 802.1x authentication on the switch and all ports.

Enabling 802.1X Authentication

Beginning in privileged EXEC mode, follow these steps to configure 802.1X port-based authentication ("Configuring 802.1x Port-Based Authentication", n.d, page 8)

This example shows how to enable AAA and 802.1X on Fast Ethernet port 0/1:

Switch# *configure terminal* ……#1
Switch(config)# *aaa new-model* ----------#2
Switch(config)# *aaa authentication dot1x default group radius* ----------#3
Switch(config)# *interface fastethernet0/1* ----------#4
Switch(config-if)# *dot1x port-control auto*----------#5
Switch(config-if)# *end* ----------#6
Switch # *show dot1x*----------#7
Switch# *Copy running-config startup-config*--------#8

Explanation :

#1 Enter Global configuration Mode
#2 Enable AAA
#3 Create an 802.1x Authentication method list. Use default keyword followed
By the method that are to be used like
Group Radius: Use list of RADIUS Server for authentication.
None: Use no authentication
#4 Specify interface to be enabled for 802.1x Authentication
#5 Enable authentication method on the interface
Options available here are:
Auto: enable 802.1x authentication and causes the port to begin in the unauthorized mode:
Force-Authorized: disables 802.1X authentication and causes the port to transition to the authorized state without any authentication exchange required.
Force-unauthorized—causes the port to remain in the unauthorized state.
#6 Return to privileged EXEC Mode
#7 Verify your entries
#8 Save your entries in the configuration file

© SANS Institute 2000 - 2005, Author retains full rights.

Configuring the Switch-to-RADIUS-Server Communication

In this step the switch should be configured with the RADIUS Server Name or IP Address, the RADIUS server's UDP port used, Encryption Key (optional). This is required so that switch can forward the authentication messages from the client to the RADIUS Server.

Beginning in privileged EXEC mode, follow these steps to configure the RADIUS server parameters on the switch ("Configuring 802.1x Port-Based Authentication", n.d, page 9).

This example shows how to specify the server with IP address 172.20.39.46 as the RADIUS server, to use port 1612 as the authorization port, and to set the encryption key to rad123, matching the key on the RADIUS
Switch# *configure termina*l ……#1
Switch(config)# *radius-server host 172.l20.39.46 auth-port 1612 key rad123* ---#2
Switch(config-if)# *end* ----------#3
Switch # *show running-config*----------#4
Switch# *Copy running-config startup-config*--------#5

Explanation:
#1 Enter Global configuration Mode
#2 Configure RADIUS Server parameters which includes
Hostname or IP Address of the Remote RADIUS Server
Auth-port: Specify UDP port for authentication request: Default is 1812
Key String: specify the authentication and encryption key used between Switch and RADIUS Server
#3 Return to privileged EXEC Mode
#4 Verify your entries
#5 Save your entries in the configuration file

Displaying 802.1X Statistics and Status

To display 802.1X statistics for all interfaces, use the:
show dot1x statistics privileged EXEC command.

To display 802.1X statistics for a specific interface, use the:
show dot1x statistics interface interface-id privileged EXEC command.

To display the 802.1X administrative and operational status for the switch, use the:
show dot1x privileged EXEC command.

To display the 802.1X administrative and operational status for a specific interface, use the:
show dot1x interface interface-id privileged EXEC command.

© SANS Institute 2000 - 2005 Author retains full rights.

Optional Configuration Parameters

There are number of optional configuration parameters that can be configured to enhance security. Some of them include the following:

Periodic Re-Authentication

It is possible to enable periodic re-authentication of the 802.1x client and also specify how often it occurs. This is a global setting on the switch and individual ports cannot be configured with different settings.

Example: How to enable periodic re-authentication and set 4000 as the number of seconds between re-authentication attempts

Switch (config-if) # *dot1x re-authentication*
Switch (config-if) # *dot1x timeout re-authperiod 4000*

[note why this is a good idea. ...]

Manually Re-Authenticating a Client Connected to a Port

It is possible to manually re-authenticate the client connected to a specific port.

Example: Manually re-authenticate the client connected to Fast Ethernet port 0/1:
Switch# *dot1x re-authenticate interface fastethernet0/1*
starting re-authentication on FastEthernet0/1

[why would a user chose this configuration option?]

Quiet Period

The switch remains idle for a set period of time and then tries again when the switch cannot authenticate the client. This idle time is called the quiet-period.

Example : Set 30 seconds as the quiet time on the switch
Switch (config-if) #*dot1x timeout quiet-period 30*

Switch-to-Client Retransmission Time

When the clients boots up, the switch sends EAP-Request/identity frame and the client must respond with the EAP-response/identify frame within a period of time. If the switch does not get a response from the client, it waits for a set period of time (retransmission time) and then retransmits the frame.

Example: Set 60 as the Switch-client-Retransmission time.

© SANS Institute 2000 - 2005 Author retains full rights.

Switch(config)#*dot1x timeout tx-period 60*

Switch-to-Client Frame-Retransmission Number

This is the number of times that the switch sends an EAP-request/identity frame (assuming no response is received) to the client before restarting the authentication process.

Example: Set 5 as the Switch-to-Client Frame –Retransmission Number.

Switch(config-if)# dot1x max-req 5

Multiple Hosts

If you want multiple hosts to be connected to Single 802.1x-enabled port , you need to enable multiple-hosts on each port of the switch wherever it requires.

Example: How to enable multiple hosts on Fast Ethernet interface 0/1

Switch (config) # interface fastethernet0/1
Switch (config-if) # dot1x port-control auto
Switch (config-if) # dot1x multiple-hosts

© SANS Institute 2000 - 2005, Author retains full rights.

Benefits of Cisco's implementation of 802.1x

Implementing Cisco's 802.1x offers many benefits in combination with the Cisco supported technology. Some of them are:

- 802.1x with VLAN Assignment.
  When 802.1x is implemented with VLAN this feature allows the authenticated users to be placed automatically in their preconfigured VLAN. This feature lets you maintain a username-to-VLAN association with a RADIUS server. Thus, 802.1x authenticated ports are assigned to a VLAN based on the identity of the user .

- 802.1x with Port Security
  This feature lets you configure port security on an 802.1x port. If port security is enabled for only one Media Access Control (MAC) address on the port, all other MAC users are denied access, which eliminates the security risk of additional users attaching to a switch to bypass authentication. [but what about if you have additional users with the same MAC/IP? Would they still be able to transmit during quiet times of the authenticated host?]

- 802.1x with Voice VLAN ID
  This feature helps organizations combine the benefits of Cisco Architecture for Voice, Video and Integrated Data (AVVID), voice over IP (VoIP), and dynamic port security mechanisms like 802.1x. [how does it do so?]

- 802.1x guest VLAN
  With this feature enabled, users trying to connect to the network that do not have an 802.1x compatible device are placed in the guest VLAN.

- 802.1x with ACL Assignment
  Access control lists (ACL's) allow you to dynamically assign an access control policy to an interface based on 802.1x user authentication. You can use this feature to restrict users to certain segments of the network, limit access to sensitive servers, or even restrict the protocols and applications used.

Setting up Windows XP Professional for 802.1x Client Authentication

After configuring the switch for 802.1x there is some configuration that needs to be done on the client. The client could be any PC or laptop that supports 802.1x. In order to explain the client setup I considered Windows XP professional. One of the excellent features of Windows XP is the availability of IEEE 802.1X authentication for all LAN adapters. Microsoft 802.1X Authentication Client uses IEEE 802.1X to authenticate network connections (including wireless).

© SANS Institute 2000 - 2005 Author retains full rights.

Microsoft Windows XP supports the following Authentication method for 802.1x:

- MD5 Challenge: is the most basic EAP-Type for authentication as defined in RFC 2284 . It is analogous to the PPP CHAP protocol. A challenge string is sent from the Authentication Server to the Supplicant in the MD5-Challenge Request. The challenge string with the user password is hashed using MD5 and the hash is returned in the MD5-Challenge Response. The Authentication Server performs the same hash and compares the result with that returned by the Supplicant to determine whether the authentication is a Success or Failure. It does not require a key/certificate infrastructure.

The other two methods work on the concept of certificates. A certificate is an encrypted set of authentication credentials. A certificate includes a digital signature from the certification authority that issued the certificate.

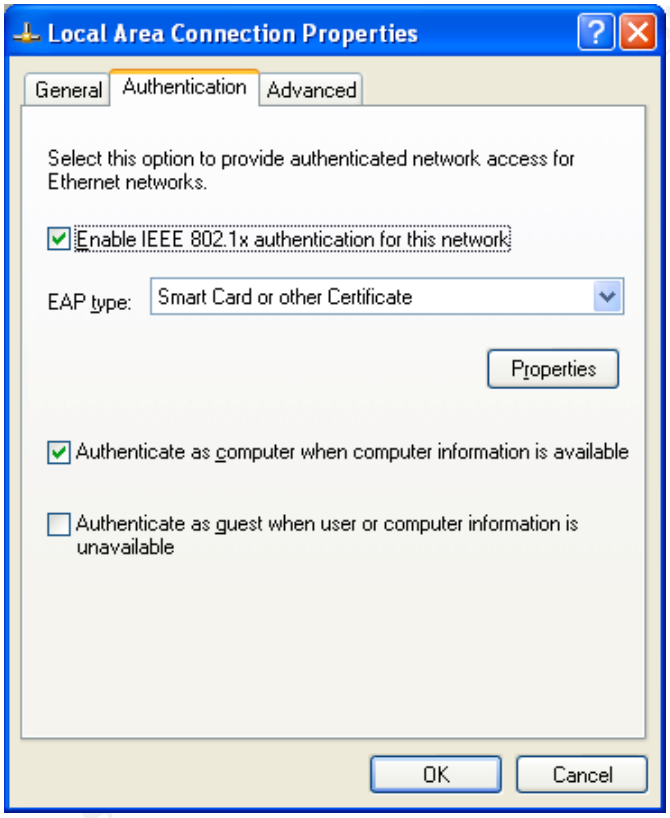
- Protected EAP (PEAP) is an authentication method that uses TLS to enhance the security of other EAP authentication methods. PEAP for Microsoft 802.1X Authentication Client provides support for TLS (”The TLS Protocol”,1999) which uses certificates for both server authentication and client authentication; and Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2), which uses certificates for server authentication and password-based credentials for client authentication.

- Smart Card or other certificate: In this type of EAP the smart card is used for authentication. A smart card is credit card-sized device used to securely store public and private keys, passwords, and other types of personal information. In this method the certificate is either installed on the computer or stored on the smart card and is used for authentication.

© SANS Institute 2000 - 2005 Author retains full rights.

Configuring the 802.1x client (Windows XP Professional)

1. From the start program, Select control panel.
2. Select network and Internet connections, and then select "Network connection".
3. Right-click on "Local Area connection "and then click Properties.
4. Select authentication Tab
   In order to access this tab you need to have Local administrative right.



5. In authentication Tab select "Enable IEEE 802.1x authentication for this network"
6. In EAP-type you need to select the authentication method .As explained above three options available here for the selection

- MD-5 challenge: Select MD-5 challenge if you want to use this method for authentication. No additional configuration is required for this setting
- Smart Card or other Certificate in EAP type: If you select this method for authentication then additional properties needs to be configured. Click properties and use the following option:
  - If certificate resides on your smart card for authentication, click Use my smart card.
  - If certificate is stored on your computer for authentication, click Use a certificate on this computer.

© SANS Institute 2000 - 2005 Author retains full rights.

- To verify server certificate is still valid, select the Validate server certificate check box, specify whether to connect only if the server resides within a particular domain, and then specify the trusted root certification authority
- To use a different user name when the user name in the smart card or certificate is not the same as the user name in the domain to which you are logging on, select the Use a different user name for the connection check box.

- Protected EAP (PEAP): If you select this method for authentication then additional properties needs to be configured. Click properties and use the following option.
  - To verify that the server certificate presented to your computer is still valid, select the Validate server certificate check box, specify the server or servers to which your computer will automatically connect, and then specify the trusted root certification authorities.
  - In Select Authentication Method, click the authentication method that you want to use within PEAP, and then click Configure. If you select Secured password (EAP-MSCHAP v2), then, in EAP MSCHAP v2 Properties, specify whether to use the user name and password (and domain, if applicable) that you type in the Windows logon screen for authentication, click OK, and then click OK again.

There is some additional configuration options available if you need to configure it. Other than the windows XP built in 802.1 x authentication client there are some other client software available that supports 802.1x. Some of them are Secure W2 free for non-commercial ("SecureW2",n.d) and WIRE1X ("WIRE1X",n.d). Funk Software ("Funk", n.d.) also has a commercial client available. These are not tested software.

LINUX Client setup: In order to setup the Linux for 802.1x please refer to Setting up Supplicant from ("802.1x port-based authentication How to ", 2004).

Sniffing 802.1X on the Wire

To enhance the comprehension of the processes undertaken during authentication in 802.1x, packet dumps of the applicable processes were taken. The packets were captured using the Tethereal application ("Tethereal", n.d). The client is Windows XP Professional using MD-5 challenge response method of authentication.

The first part of the packet dump shows the EAP exchange messages from the client to the switch and second part shows the RADIUS protocol being used between the Switch and the RADIUS Server.

© SANS Institute 2000 - 2005 Author retains full rights.

Part 1 –Client to Switch

EAP Exchange between the client and the switch ……

```
46  15.765350 NortelNe_51:12:a2 -> 10.0.2.187   EAP Request, Identity [RFC3748]

0000  00 11 43 a5 52 dd 00 0e c0 51 12 a2 88 8e 01 00   ..C.R....Q......
0010  00 48 01 01 00 48 01 54 68 69 73 20 69 73 20 61   .H...H.This is a
0020  20 64 69 73 70 6c 61 79 20 73 74 72 69 6e 67 00    display string.
0030  6e 65 74 77 6f 72 6b 69 64 3d 42 61 73 65 2d 4e   networkid=Base-N
0040  57 2c 6e 61 73 69 64 3d 00 0e c0 51 12 a2 2c 70   W,nasid=...Q..,p
0050  6f 72 74 69 64 3d 00 00 02 a2                      ortid=....

65  22.195633   10.0.2.187 -> Spanning-tree-(for-bridges)_03 EAP Response, Identity [RFC3748]

0000  01 80 c2 00 00 03 00 11 43 a5 52 dd 88 8e 01 00   ........C.R.....
0010  00 09 02 01 00 09 01 74 65 73 74                  .......test

66  22.279928 NortelNe_51:12:a2 -> 10.0.2.187   EAP Request, MD5-Challenge [RFC3748]

0000  00 11 43 a5 52 dd 00 0e c0 51 12 a2 88 8e 01 00   ..C.R....Q......
0010  00 1c 01 14 00 1c 04 10 14 e1 7d 2a be 15 6a d9   ..........}*..j.
0020  9d c4 47 24 b2 74 99 85 48 51 2d 52 41 44 00 00   ..G$.t..HQ-RAD..
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............

 67  22.293561   10.0.2.187 -> Spanning-tree-(for-bridges)_03 EAP Response, MD5-Challenge [RFC3748]

0000  01 80 c2 00 00 03 00 11 43 a5 52 dd 88 8e 01 00   ........C.R.....
0010  00 1a 02 14 00 1a 04 10 0e ee 32 4a bd 3f 89 22   ..........2J.?."
0020  d4 8b 2a 83 4e 3d 5c 4c 74 65 73 74               ..*.N=\Ltest

 68  22.380746 NortelNe_51:12:a2 -> 10.0.2.187   EAP Success

0000  00 11 43 a5 52 dd 00 0e c0 51 12 a2 88 8e 01 00   ..C.R....Q......
0010  00 05 03 14 00 05 00 00 00 00 00 00 00 00 00 00   ................
0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0030  00 00 00 00 00 00 00 00 00 00 00 00               ............
```

© SANS Institute 2000 - 2005 Author retains full rights.

Part 2- Switch to RADIUS Server

RADIUS Protocol exchanges between the switch and the RADIUS Server
[this is much better! Can you highlight a couple features in the packet? E.g. For the RADIUS request things like the ID, and the code for the request?]

```
948  97.778853     10.0.2.4 -> 10.0.4.1     RADIUS Access Request(1) (id=0, l=98)

0000  00 0b cd 4f ad 15 00 0e 62 d5 42 02 08 00 45 00   ...O....b.B...E.
0010  00 7e 31 29 00 00 3f 11 30 42 0a 00 02 04 0a 00   .~1)..?.0B......
0020  04 01 04 0a 06 6d 00 6a 00 00 01 00 00 62 00 00   .....m.j.....b..
0030  78 16 00 00 7b 4d 00 00 3c 92 00 00 34 c7 04 06   x...{M..<...4...
0040  0a 00 02 04 50 12 90 8f 4e 82 45 eb 0e ec de 5a   ....P...N.E....Z
0050  c1 d4 07 b4 b3 66 05 06 00 00 02 af 0c 06 00 00   .....f..........
0060  05 d2 01 06 74 65 73 74 1f 13 30 30 2d 42 30 2d   ....test..00-B0-
0070  44 30 2d 44 36 2d 45 35 2d 42 32 4f 0b 02 04 00   D0-D6-E5-B2O....
0080  09 01 74 65 73 74 06 06 00 00 00 02               ..test......

949  97.780478     10.0.4.1 -> 10.0.2.4     RADIUS Access challenge(11) (id=0, l=103)

0000  00 00 5e 00 01 04 00 0b cd 4f ad 15 08 00 45 00   ..^......O....E.
0010  00 83 38 98 00 00 80 11 00 00 0a 00 04 01 0a 00   ..8.............
0020  02 04 06 6d 04 0a 00 6f 95 3d 0b 00 00 67 5f 41   ...m...o.=...g_A
0030  cd 64 91 d5 f8 52 9c f8 c2 7d 0f bd bc 8d 4f 1e   .d...R...}....O.
0040  01 b2 00 1c 04 10 b2 a2 4e f4 7d ca 53 b7 65 18   ........N.}.S.e.
0050  a7 36 ea 9d 8f e4 48 51 2d 52 41 44 18 23 43 49   .6....HQ-RAD.#CI
0060  53 43 4f 2d 45 41 50 2d 43 48 41 4c 4c 45 4e 47   SCO-EAP-CHALLENG
0070  45 3d 30 2e 31 66 65 2e 32 61 32 34 33 2e 31 50   E=0.1fe.2a243.1P
0080  12 68 a0 5d 09 e1 5f e0 4e 3e e7 af cf bf 8f db   .h.]..._.N>......
0090  b8                                                .

950  97.862650     10.0.2.4 -> 10.0.4.1     RADIUS Access Request(1) (id=0, l=150)

0000  00 0b cd 4f ad 15 00 0e 62 d5 42 02 08 00 45 00   ...O....b.B...E.
0010  00 b2 31 32 00 00 3f 11 30 05 0a 00 02 04 0a 00   ..12..?.0.......
0020  04 01 04 0a 06 6d 00 9e 00 00 01 00 00 96 00 00   .....m..........
0030  6b e4 00 00 11 00 00 00 25 30 00 00 54 eb 04 06   k.......%0..T...
0040  0a 00 02 04 50 12 34 77 91 e9 ad fa f8 91 e5 06   ....P.4w........
0050  46 25 29 ef 6e 1e 05 06 00 00 02 af 0c 06 00 00   F%).n...........
0060  05 d2 01 06 74 65 73 74 1f 13 30 30 2d 42 30 2d   ....test..00-B0-
0070  44 30 2d 44 36 2d 45 35 2d 42 32 18 23 43 49 53   D0-D6-E5-B2.#CIS
0080  43 4f 2d 45 41 50 2d 43 48 41 4c 4c 45 4e 47 45   CO-EAP-CHALLENGE
0090  3d 30 2e 31 66 65 2e 32 61 32 34 33 2e 31 4f 1c   =0.1fe.2a243.1O.
00a0  02 b2 00 1a 04 10 5d ec fe 4a 6e e4 06 6d 18 ed   ......]..Jn..m..
00b0  e7 e9 79 fe ce 02 74 65 73 74 06 06 00 00 00 02   ..y...test......

953  97.901303     10.0.4.1 -> 10.0.2.4     RADIUS Access Accept(2) (id=0, l=103)

0000  00 00 5e 00 01 04 00 0b cd 4f ad 15 08 00 45 00   ..^......O....E.
0010  00 83 38 e9 00 00 80 11 00 00 0a 00 04 01 0a 00   ..8.............
0020  02 04 06 6d 04 0a 00 6f 84 36 02 00 00 67 9b 22   ...m...o.6...g."
0030  15 b3 12 31 4d 66 c0 01 26 0f ff 88 0d 06 42 04   ...1Mf..&.....B.
0040  02 32 42 04 03 32 06 06 00 00 00 06 40 06 02 00   .2B..2......@...
```

© SANS Institute 2000 - 2005 Author retains full rights.

```
0050  00 0d 40 06 03 00 00 0d 40 06 04 00 00 0d 41 06   ..@.....@.....A.
0060  02 00 00 06 41 06 03 00 00 06 51 04 02 33 51 04   ....A.....Q..3Q.
0070  03 33 0e 06 00 00 00 00 4f 07 03 b2 00 05 00 50   .3......O......P
0080  12 a8 ed 99 f5 25 cb 18 3e 56 bf 7e d2 63 fb e1   .....%..>V.~.c..
0090  dc                                                .

956  97.989586     10.0.2.4 -> 10.0.4.1     RADIUS Accounting Request(4) (id=1, l=54)

0000  00 0b cd 4f ad 15 00 0e 62 d5 42 02 08 00 45 00   ...O....b.B...E.
0010  00 52 31 37 00 00 3f 11 30 60 0a 00 02 04 0a 00   .R17..?.0`......
0020  04 01 04 0a 06 6e 00 3e 00 00 04 01 00 36 50 6b   .....n.>.....6Pk
0030  9f af cd c3 bf 38 fc 80 3a f6 53 49 69 0d 04 06   .....8..:.SIi...
0040  0a 00 02 04 2c 0a 30 39 30 30 30 30 33 64 05 06   ....,.0900003d..
0050  00 00 02 af 01 06 74 65 73 74 28 06 00 00 00 01   ......test(.....

960  98.095940     10.0.4.1 -> 10.0.2.4     RADIUS Accounting Response(5) (id=1, l=20)

0000  00 00 5e 00 01 04 00 0b cd 4f ad 15 08 00 45 00   ..^......O....E.
0010  00 30 39 07 00 00 80 11 00 00 0a 00 04 01 0a 00   .09............
0020  02 04 06 6e 04 0a 00 1c b7 7b 05 01 00 14 78 20   ...n.....{....x
0030  4e 90 59 33 f4 eb 2f 69 45 d8 e7 c4 ac d2         N.Y3../iE.....
```

© SANS Institute 2000 - 2005, Author retains full rights.

Conclusion

We have discovered in this paper an understanding of the terminology, features and capabilities of the 802.1x with its ability to deny unauthorized network access, but also identified important limitations, such that 802.1x cannot control network traffic from "authorized" users.

It is essential to note when deploying this technology that the administrator needs to plan and consider the specific requirements in the context of their own network and applicable policies.

It is also vital to emphasize that 802.1x technology is complimentary with existing security technologies, but not a replacement. It is essentially a perimeter security measure, providing an important component to an overall security strategy.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Reference

Tulloch Mitch (2004). DHCP Server security. Retrieved January 5, 2006 from http://www.windowsecurity.com/articles/DHCP-Security-Part1.html

Overview of 802.1x and Cisco IBNS Technology. What is 802.1x? Retrieved Dec 20,2005 from www.cisco.com/application/pdf/en/us/guest/ netsol/ns75/ ccmigration_09186a0080258e2f.pdf

Overview of 802.1x and Cisco IBNS Technology. What is 802.1x supplicant. Retrieved from Dec 20,2005 www.cisco.com/application/pdf/en/us/guest/ netsol/ns75/ ccmigration_09186a0080258e2f.pdf

PPP Extensible Authentication Protocol. Retrieved Dec 25,2005 from http://www.ietf.org/rfc/rfc2284.txt?number=2284

Remote Authentication Dial in User Service, Retrieved Dec 25,2005 from http://www.ietf.org/rfc/rfc2865.txt?number=2865

RADIUS Extension. Retrieved Dec 25, 2005, from http://www.ietf.org/rfc/rfc2869.txt?number=2869

Point to Point Protocol. Retrieved Dec 27,2005 , from http://www.ietf.org/rfc/rfc1661.txt?number=1661

Using IEEE 802.1x to enhance network security. 802.1x Authentication process. Retrieved Dec 29,2005 from www.foundrynet.com/solutions/appNotes/PDFs/802.1xWhite_Paper.pdf

Configuring 802.1x port-based Authentication. Enabling 802.1x Authentication. Retrieved January 2, 2006 from http://www.cisco.com/en/US/products/hw/ switches/ps646/products_configuration_guide_chapter09186a008014f342.html

Configuring 802.1x port-based Authentication. Configuring switch-to-RADIUS-Server Communication. Retrieved January 2, 2006 from http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide _chapter09186a008014f342.html

The TLS Protocol . Retrieved January 3,2006 from http://www.ietf.org/rfc/rfc2246.txt?number=2246

SecureW2. The Powerful open source EAP-TTLS Client for Windows . Retrieved January 3, 2006 from http://www.securew2.com/uk/index.htm

WIRE1X .Retrieved January 3, 2006 from http://wire.cs.nthu.edu/tw/wire1x/

© SANS Institute 2000 - 2005 Author retains full rights.

Funk Software, Odyssey® Client. Retrieved January 3, 2006 from http://www.funk.com

802.1X Port-Based Authentication HOWTO. Setting up XSupplicant. Retrieved January 4, 2006 from http://www.linux.org/docs/ldp/howto/8021X-HOWTO/index.html

Tethereal-Dump and Analyze network traffic. Retrieved January 5,2006 from http://www.ethereal.com/docs/man-pages/tethereal.1.html

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced