GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Herny Elisa Erwin
GSEC Practical
Version 1.4b
October, 2002

The IEEE 802.1x Port-Based Network Access Control and Its Implementation

Abstract

Over the past decade, the telecommunication industry has witnessed rapid changes in communication technology due to explosive growth of the Internet Protocol (IP) network infrastructure. Network that used to be a closed network become an open network. This characteristic challenges people on how to provide a better network security.

When we talk about network security, most people will think about firewall. Well, firewall does protect the network from outside attack, but how about protecting the network from the internal side? One of the standard solutions is 802.1x, which is defined by IEEE to provide security for network access from the point of attachment to the Local Area Network (LAN) by authentication. While this standard was originally intended for switched Ethernet networks, it has been adapted during the standardization process for use on IEEE 802.11 wireless shared media Ethernet LAN. This paper is intended to provide information and understanding of the IEEE 802.1x standard and its implementation such as products that support 802.1x, and how to enable 802.1x in wireless network using Cisco's wireless product.

Overview of 802.1x

The 802.1x standard defines a mechanism of Port-based network access control that make use of the physical access characteristics of IEEE 802 Local Area Network (LAN) infrastructures in order to provide a means of authenticating and authorizing devices attached to that port in cases in which the authentication and authorization process fails. A port in this context is a single point of attachment to the LAN infrastructure. [1]

The ports of the LAN infrastructure can be a port of an Ethernet switch, or an IEEE 802.11 Wireless LAN access point.

There are three principal roles in 802.1x operation to make the mechanism work:

- Authenticator:

  An Authenticator is responsible for enforcing the authentication of a device that attaches to its controlled port before allowing access to LAN services

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

that are accessible via that port. An Authenticator is also responsible for controlling the authorization state of its ports accordingly, which will be described later.

An Authenticator is typically the physical or logical ports of a LAN switch that support 802.1x. In Wireless LAN, an authenticator can be an Access Point or a Wireless Bridge set as Root. The Authenticator enforces authentication by forwarding access decision to the Authentication Server.

- Supplicant:

  A Supplicant is responsible for communicating its credentials to the Authenticator in response to request from the Authenticator. The Supplicant may initiate authentication exchanges beside the Authenticator itself, depend on the setting.

  A network adapter of a workstation, or refer as client, may play the role of the Supplicant. The network adapter can be a typical Ethernet card adapter running 802.1x-compliant client software, or a wireless LAN client that support 802.1x.

  A port of network element can also be a supplicant. The examples are, a switch's port that connect to another switch's port, and a Non-root Wireless Bridge that connect to a Root Wireless Bridge.

- Authentication Server:

  The Authentication Server performs the authentication function to check the credentials of the Supplicant on behalf of the Authenticator and indicated whether the Supplicant is authorized to access the LAN services. The Authentication Server is typically a RADIUS (Remote Authentication Dial-In User Service) server with Extensible Authentication Protocol (EAP) support.

All three roles are necessary to complete an authentication exchange.

How 802.1x Works

An Authenticator's port state determines whether or not a Supplicant is granted access to the LAN services. The port starts as uncontrolled port, or unauthorized state. While in this state, the port disallows all ingress and egress traffic except for 802.1x protocol packets. Uncontrolled port only allows 802.1x authentication traffic passing through it.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

When the Supplicant is successfully authenticated, the port transitions to authorized state, or as controlled port, allowing all traffic for the Supplicant to flow normally.

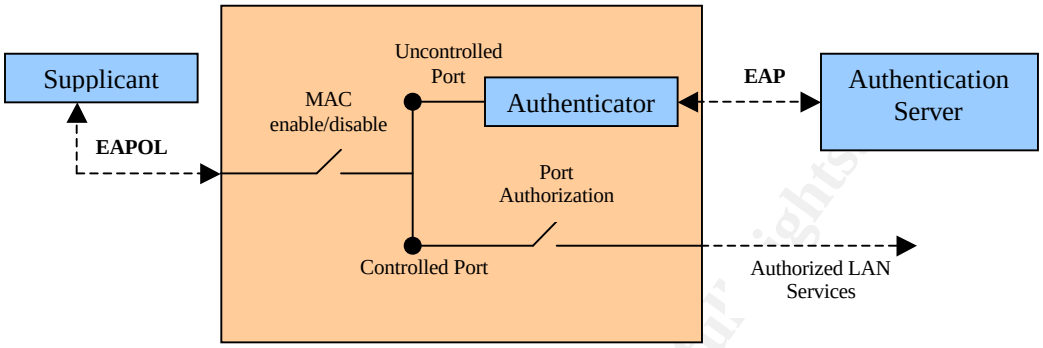

Figure 1. Uncontrolled and Controlled Port

Any access to the LAN is also subject to the current administrative and operational state of the Media Access Control (MAC) associated with the port, as shown in Figure 1. If the port is disabled administratively, then there is no traffic that is allowed through the port.

Communication between the Supplicant and the Authenticator, and between the Authenticator and the Authentication Server (when the Authentication Server is not collocated with the Authenticator), is achieved by means of protocols and procedures defined in following section.

EAP

The IEEE 802.1x uses Extensible Authentication Protocol (EAP), specified in IETF RFC 2284, as the protocol for authentication exchange. EAP is an extension of CHAP/PAP within Point-to-Point Protocol (PPP) that supports communication of authentication information for multiple authentication mechanism. [2]

Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others.

EAP is used as the protocol for communication between a Supplicant and an Authenticator before the Supplicant is granted access. This means that EAP messages need to be encapsulated directly over a LAN medium. EAP over LAN (EAPOL) was defined for this purpose.

The Authenticator then is responsible for forwarding those EAP messages encapsulated in RADIUS packets to the RADIUS Server. In order to provide

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

support for EAP within RADIUS, two new attributes, EAP-Message and Signature, were introduced as RADIUS extensions. [3]

The EAP-Message attribute allows the Authenticator to authenticate the Supplicant via EAP without having to understand the protocol. Authenticator places EAP messages received from the Supplicant into one or more EAP-Message attributes and forwards them to the RADIUS Server within an Access-Request packet.

The Signature attribute is used to protect those EAP messages exchange. All EAP/RADIUS packets must be authenticated using the Signature attribute. This Signature is calculated using an algorithm and inserted in the RADIUS packet. A RADIUS Server supporting EAP-Message must calculate the correct value of the Signature and silently discard the packet if it does not match the value sent, or if it does not contain a Signature attribute.

The use of Signature attribute enables the RADIUS server to verify the integrity of the packets from Authenticator, and vice versa. This provides an integrity protection for the communication of authentication messages.

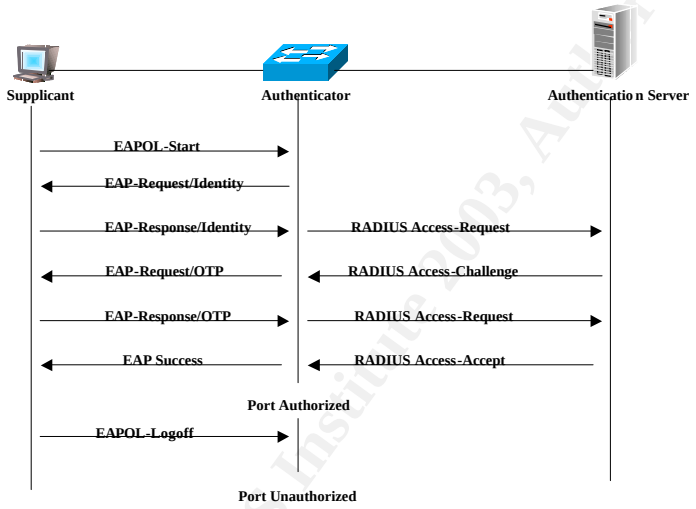

Figure 2. Message exchange

The operation of 802.1x authentication is described as follows:

1. During boot-up, a Supplicant or Client can initiate authentication by sending an EAPOL-start frame, which prompts its attached Authenticator, or in this example is an Ethernet switch, to request the client's identity.
2. The Authenticator or the switch can also initiate authentication. If authentication on a port is enabled on the switch, the switch must initiate authentication when it detects that the link state is active or transitions from down to up. It then sends an EAP-request/identity frame to the Supplicant to request its identity.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. The Client responds with its identity in an “EAP-Response/Identity” packet to the Authenticator.
4. The Authenticator will copy the content of the EAP-Response/Identity into the User-Name attribute of RADIUS, and then forward it in RADIUS Access-Request packet to a RADIUS server as the Authentication Server. The RADIUS server will typically use this packet to determine which EAP type is to be applied to the user. If the RADIUS server supports EAP, it will respond with a RADIUS Access-Challenge packet. If the RADIUS server does not support EAP, it will respond with an Access-Reject.
5. The RADIUS server will use the client’s identity to check with its user database. Then it will create a challenge that will be sent to Authenticator. This challenge and the client’s password is used in EAP algorithm computation to produce a response that will be compared later with response from the client.

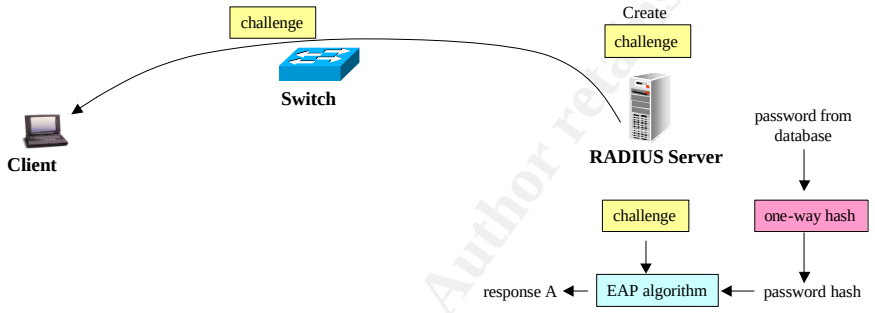

Figure 3. RADIUS Server sends a challenge to client

6. The RADIUS Server forwards the challenge to the Client.
7. The Client will do the same computation as RADIUS, using the challenge and user-supplied password to generate a response for the RADIUS server.

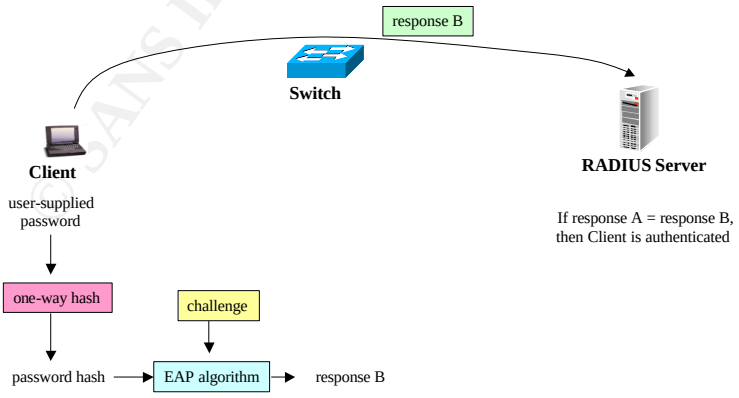

Figure 4. Client sends its response to RADIUS Server

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

8. If the response from Client is the same as response computed by the RADIUS server before, then the Client's credential is correct, and the RADIUS Server responds with a success message, which is then passed onto the Client. The Authenticator's port now is authorized, and Client is allowed access to the LAN.

Authentication Types used with 802.1x

IEEE 802.1x defines an encapsulation technique that allows for the transmission of EAP packets between the Supplicant and Authenticator in the LAN environment. The EAP provides a standard mechanism for support of additional authentication methods within PPP. Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Public Key, One Time Passwords, and others.

There are several EAP authentication types:

- EAP-MD5:

  EAP-Message Digest 5 (EAP-MD5) is an EAP type that uses an MD5 hash of a username and password to create challenges and responses from the client to the RADIUS server.

  In a Wireless LAN environment using EAP-MD5 authentication, the Wired Equivalency Protocol (WEP) key used is a static key. This static WEP key is a weakness in wireless LAN security because someone who sniffs your wireless traffic can easily decode all data that he had captured once the key is decrypted.

  EAP-MD5 also does not provide mutual authentication. It only allows for the server to validate the client. That's why EAP-MD5 is considered to be the least secure EAP authentication types among others.

  A typical use for EAP-MD5 CHAP is to authenticate the credentials of a client by using user name and password security systems.

- EAP-TLS:

  EAP-Transport Layer Security (EAP-TLS) is an EAP type defined in RFC 2716 that is used in certificate-based security environments. The EAP-TLS exchange of messages provides mutual authentication with both the client and server mutually validating each other via certificates.

  In wireless network, EAP-TLS provides dynamic WEP key generation, thus strengthen wireless LAN security. But the strength of EAP-TLS security comes at a high cost because EAP-TLS implementation requires

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

full PKI infrastructure support. It requires server-side and user-side certificates, so EAP-TLS needs more effort for its administration. User's certificates must be managed and might cause a burden in administration.

- EAP-TTLS

  EAP Tunneled Transport Layer Security (EAP-TTLS) is an extension of EAP-TLS, which requires only server-side certificates, eliminating the need to configure certificates for each client. Compared to EAP-TLS, EAP-TTLS simplifies its administration. EAP-TTLS still maintain mutual authentication as EAP-TLS because users are authenticated to the network using ordinary password-based credentials.

- EAP-Cisco Wireless, or also called Lightweight EAP (LEAP)

  This EAP authentication type is developed by Cisco and used primarily in Cisco Wireless LAN devices. It is a proprietary authentication type from Cisco. In the Wireless LAN, it encrypts data transmission using dynamically generated WEP keys, and support mutual authentication. [4]

  LEAP is developed to overcome EAP-MD5 in Wireless LAN where the WEP keys are static, and offers no mutual authentication. LEAP provides mutual authentication because client will authenticate RADIUS server after it is authenticated.

- Protected EAP (PEAP)

  PEAP authentication is designed to support One-Time Password (OTP), Windows NT or 2000 domain, and LDAP user databases over a wireless LAN. It is based on EAP-TLS authentication but uses a password or PIN instead of a client certificate for authentication. In Wireless LAN, PEAP uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. [4]

IEEE 802.1x Implementation [5,6,7,8,9]

While 802.1x was originally developed for wired LAN, it has been adapted for use in wireless LAN because it overcomes some vulnerability in wireless network. Beside authentication, it offers dynamic WEP encryption key. Most of the wireless LAN vendors have included 802.1x support in their product. Cisco for example, has support 802.1x in it's Aironet Client Utility, an utility for its wireless client. For wired network, Cisco Catalyst Ethernet switch also supports 802.1x.

Below is some product that support 802.1x from several networking vendors:

- Universal 802.1x client:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

- Microsoft Windows XP built-in 802.1x client
- AEGIS Client from Meetinghouse Data Communications
- Funk's Odyssey Client

- RADIUS Server:
  - Microsoft Internet Authentication Server (IAS)
  - Cisco Secure Access Control Software (ACS)
  - Odyssey and Steel Belted RADIUS server from Funk Software
  - AEGIS Server from Meetinghouse Data Communications
  - FreeRadius, an open source project that runs on the Linux platform.

- Wireless LAN devices: Cisco Aironet, Orinoco, BreezeNet from Alvarion, etc. Ethernet switches: Cisco Catalyst switches (2950, 3550, 4000, and 6500 Series), Alcatel (OmniSwitch 7000 and 8800), Foundry Networks (FastIron JetCore), and Nortel Networks (BayStack 470).

Below is the summary of those products based on product literature in each website.

Product	O/S						EAP Authentication				
	NT	XP	2000	98	ME	Linux	MD5	TLS	TTLS	LEAP	PEAP
Windows XP		✓					✓	✓			✓
Microsoft IAS			✓				✓	✓			
Aegis Client	✓	✓	✓	✓	✓	✓	✓	✓	✓		
Aegis Server						✓	✓	✓	✓		
Odyssey Client		✓	✓	✓	✓		✓	✓	✓		
Odyssey Server		✓	✓					✓	✓	✓	
Cisco Secure ACS	✓		✓				✓	✓		✓	✓

Table 1. Summary of 802.1x Product Support

To provide a better understanding of 802.1x implementation, this paper will also take an example of how to enable 802.1x authentication on Wireless LAN using the following component:

- Cisco Secure ACS 3.0 as the Authentication
- Cisco Aironet 350 Access Point as the Authenticator
- Server Cisco ACU (Aironet Client Utility) as the Supplicant

Enabling EAP on Cisco Secure ACS 3.0 Configuration [10]

Cisco Secure ACS adds supports for EAP from ACS version 2.6. The example below is taken from Cisco Secure ACS version 3.0. To enable EAP authentication on the Cisco ACS Server, the following setting is required:

1. Add the Access Point in the Network Configuration page. The parameters need to be set are:
   a. IP address of the Access Point.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

b. RADIUS shared secret. Cisco Secure ACS uses the shared secret to encrypt data. This shared secret must be an identical key configured on the Access Point.
c. Authentication method. To enable 802.1x, use *RADIUS (Cisco Aironet)* to enable you to make use of the Cisco Aironet vendor-specific attributes, or *RADIUS (IETF)* to use standard IETF RADIUS attributes.

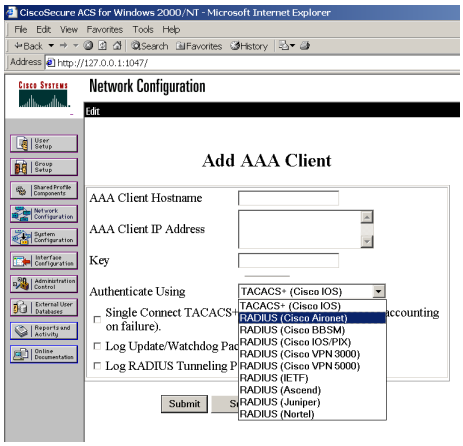

Figure 5. Network Configuration Page

2. Configure the WEP key session timeout to enable dynamic WEP key generation. This re-authentication is specified in 802.1x. Cisco LEAP algorithm uses this option to expire the current WEP session key for the user and issue a new WEP session key. RADIUS attribute used is [027]Session-Timeout. To set RADIUS attribute, on Group Setup page, select the group and click the Edit Settings button. Select [027]Session-Timeout and configure the WEP key timeout value.

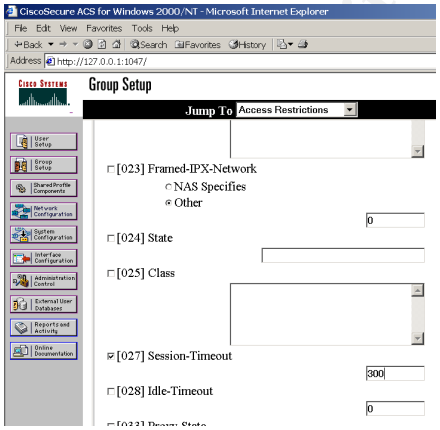

Figure 6. Group Setup Page

3. Add user. User databases that are supported by Cisco Secure ACS is Cisco Secure ACS internal database, Windows NT/2000 Active Directory, generic LDAP, Novell NDS, and token card servers (One Time Password).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

To create user in Cisco ACS internal database, click the User Setup button. Enter user's real name and description. Select *Cisco Secure Database* as the password authentication, and then type in the password.

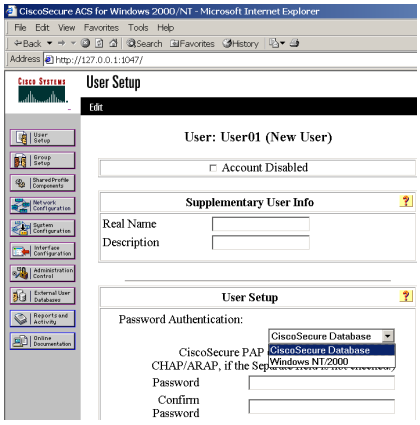

Figure 7. User Setup Page

Enabling 802.1x authentication on Cisco Aironet Access Point

IEEE 802.1x using LEAP authentication on Cisco Aironet 350 Access Point required firmware with version of minimum 11.05a. To enable 802.1x authentication on a Cisco Aironet Access Point, the following setup is required:

1. Add the Authentication Server. The parameters' required are:
    a. 802.1x Protocol Version. The Cisco LEAP version is draft 8 or draft 10.
    b. IP address of the RADIUS server.
    c. Server Type, which is *RADIUS.*
    d. Port number that the RADIUS server uses for authentication. The default setting, *1812,* is the port setting for many RADIUS servers, while *1645* is the port setting for Cisco Secure ACS.
    e. Shared Secret used by the RADIUS Server. The shared secret on the Access Point, which is identical to the key that is configured on the RADIUS Server.
    f. If there are multiple RADIUS servers, the timeout parameter can be used to round robin the authentication to the next configured RADIUS server if the authentication for the first RADIUS server has been timed out.
    g. Enable *EAP Authentication*.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

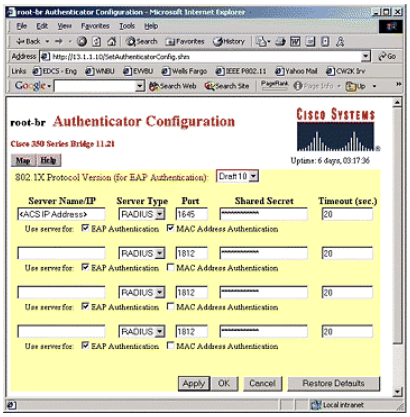

Figure 8. Authenticator Configuration Page

2. Configure data encryption (WEP). On the Security Setup screen, click on Radio Data Encryption (WEP), and set the following parameters:
    a. WEP Key, which is a broadcast WEP key in a 40- or 128-bit key value.
    b. Enable *Network-EAP*.

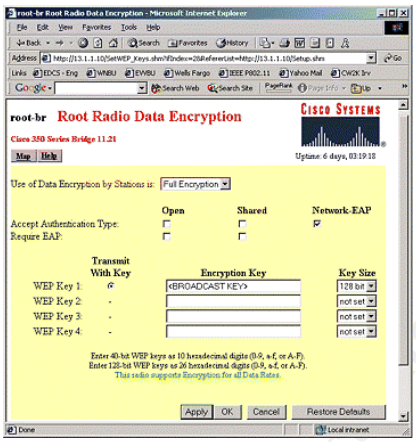

Figure 9. Root Radio Data Encryption Page

Enabling EAP on Cisco ACU 5.01

The client will require minimum of firmware version 4.25.10 for Cisco LEAP. Recommended version of Cisco ACU is version 5.01. When using 802.1x authentication, the client will pass the username and password, captured from the network logon application, to the RADIUS server, and receive the dynamic WEP keys from the RADIUS server and the AP. The client sets and removes the dynamic WEP keys.

To enable LEAP on Cisco ACS, on the properties window, select the Network Security tab and configure the following parameters:

1. Network Security Type, which is *LEAP*.
2. Configure the password settings as needed.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

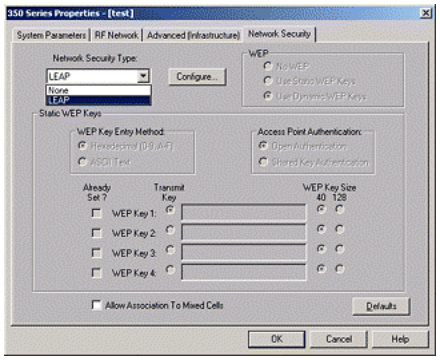

Figure 10. Network Security Tab

Conclusion

IEEE 802.1x port-based network access control provides a significantly improved solution for authentication for switched LAN and wireless LAN. It is a means to authenticate every network user accessing the LAN services. Authentication must be performed prior to any flow of traffic from the host being allowed to be forwarded by the switch, thus provide security from network side.

The benefits offered by 802.1x and EAP authentication are:

- Provide interoperability among vendors for network access authentication – 802.1x is an IEEE standard that is supported by interoperable implementations among vendors.
- Provide extensible authentication support – EAP allows additional authentication methods to be deployed such as password authentication, One-Time Password, smart card authentication, and digital certificates.
- Improved security in Wireless LAN – Using 802.1x and EAP authentication, encryption and authentication in Wireless LAN is enhanced by support of dynamic WEP encryption key generation and mutual authentication.

References

1. "*IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control.*" The Institute of Electrical and Electronics Engineers (IEEE). URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf (July 13, 2001).
2. L. Blunk, J. Vollbrecht. IETF Request for Comment (RFC) 2284. "*PPP Extensible Authentication Protocol (EAP).*" URL: http://www.ietf.org/rfc/rfc2284.txt (March, 1998).
3. Calhoun, Rubens & Aboba. "*Extensible Authentication Protocol Support in RADIUS*". URL: http://www.freeradius.org/rfc/draft-ietf-radius-eap-05.txt (May, 1998).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

4. "*Configuring the Client Adapter through Windows XP*". Cisco System. URL: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/windows/incfg/win_appe.htm
5. "*Wireless Network Security with IEEE 802.1x*". Microsoft Windows XP. URL: http://www.microsoft.com/windowsxp/pro/evaluation/overviews/8021x.asp (November 27, 2001)
6. "*EAP and Internet Authentication Service*". MSDN Library. URL: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/eap/eap/eap_and_internet_authentication_service.asp
7. "*AEGIS: A Wireless Security Solution*". Meetinghouse Data Communications. http://www.mtghouse.com/mdc_datasheet.pdf
8. "*Wireless LAN Security Software*". Funk Software. URL: http://www.funk.com/radius/wlan/ody_ds.asp
9. "Cisco Secure Access Control Server Version 3.1 for Windows". Cisco System. URL: http://www.cisco.com/warp/public/cc/pd/sqsw/sq/prodlit/sacsd_ds.htm
10. "*Cisco Aironet 350 Series Configuring the Cisco Wireless Security Suite*." Cisco System. URL: http://www.cisco.com/en/US/products/hw/wireless/ps458/products_white_paper09186a00800b3d27.shtml

© SANS Institute 2003, Author retains full rights.

Last Updated: April 30th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS