InteropNet Labs

2 in a series

What is 802.1X?

Understanding what IEEE 802.1X is and why you should care about it means understanding three separate concepts: PPP, EAP (Extensible Authentication Protocol), and IEEE 802.1X itself. PPP and EAP are Internet standards, defined through the RFC process. IEEE 802.1X is an IEEE standard that is built on the Internet standard EAP.

What is PPP and what does it have to do with wireless security?

Most people are familiar with PPP, the point-to-point protocol. It's most commonly used for dial-up Internet access. PPP is also used by some ISPs for DSL and cable modem authentication, in the form of PPPoE (PPP over Ethernet). PPP is part of L2TP, a core part of Microsoft's secure remote access solution for Windows 2000.

By any measure, PPP is a very successful protocol. In practice, PPP has gone far beyond its original use as a dial-up access method as it's now used all over the Internet. Although PPP has many parts that make it useful in different networking environments, the part that we care about in this demonstration is the authentication piece. Before anything at Layer 3 (like IP) is established, PPP goes through an authentication phase at Layer 2. With dial-up Internet access, that's the username and password. PPP authentication is used to identify the user at the other end of the PPP line before giving them access. By authenticating at layer 2, you are independent of upper-layer protocol (such as IP, IPX, or Appletalk) and you can make decisions on how to handle layer 3 protocols, such as IP, based on the authentication information. For example, depending on what authentication information you provide, you might get a particular IP address.

How did EAP get into the picture?

As PPP use grew, people quickly found its limitations, both in flexibility and in level of security, in the initial simple built-in authentication methods, such as PAP and CHAP.

Most corporate networks want to do more than simple usernames and passwords for secure access, so a new authentication protocol, called the Extensible Authentication Protocol (EAP) was designed. EAP sits inside PPP's authentication protocol and provides a generalized framework for all sorts of authentication methods. Rather than keep changing PPP, the idea was to simply have a tunnel through the remote access server for a more powerful protocol between the user and the real authentication server. By pulling EAP out into a separate protocol, it then has the option of re-use in other environments---like 802.1X. EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and PKI certificates work smoothly.

With a standardized EAP, interoperability and compatibility across authentication methods becomes simpler. For example, when you dial a remote access server (RAS) and use EAP as part of your PPP connection, the RAS doesn't need to know any of the details about your authentication system. Only you and the authentication server have to be coordinated. By supporting EAP authentication, a RAS server gets out of the business of actively participating in the authentication dialog and just re-packages EAP packets to hand off to a RADIUS server to make the actual authentication decision.

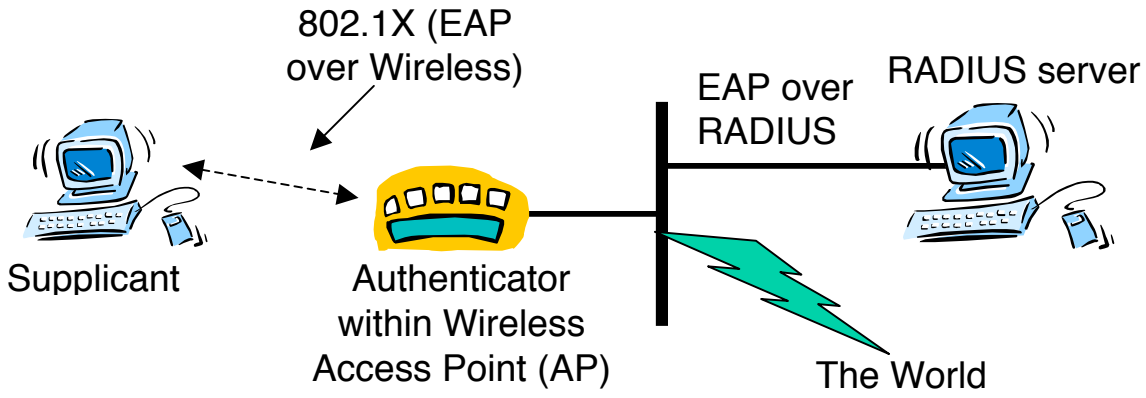
I know what EAP and PPP are. What is IEEE802.1X?

IEEE 802.1X is simply a standard for passing EAP over a wired or wireless LAN. With 802.1X, you package EAP messages in Ethernet frames. It's authentication, and nothing more.

In the wireless environment, 802.1X also describes a way for the access point and the wireless user to share and change encryption keys, and adds some messages which help smooth operations over wireless. The key change messages help solve the major security vulnerability in 802.11, the management of WEP keys. With 802.1X, WEP is brought up to an acceptable level of security for most companies.

IEEE 802.1X uses three terms that you must know. Because a wired or wireless LAN authentication has three parties involved, 802.1X created three labels for them. The user or client that wants to be authenticated is a **supplicant**. The actual server doing the authentication, typically a RADIUS server, is called **the authentication server**. And the device in between these two elements, such as a wireless access point, is called the **authenticator**. One of the key points of 802.1X is that the authenticator can be simple and dumb---all of the

brains have to be in the supplicant and the authentication server. This makes 802.1X ideal for wireless access points, which typically have little memory and processing power.



The protocol in 802.1X is called EAPOL (EAP encapsulation over LANs). It is currently defined for Ethernet-like LANs including 802.11 wireless, as well as token ring LANs like FDDI. EAPOL is not particularly sophisticated. There are a number of modes of operation, but the most common case would look something like this:

1) The Authenticator sends an "EAP-Request/Identity" packet to the Supplicant as soon as it detects that the link is active (*e.g.,* the supplicant system has associated with the access point).
2) The Supplicant sends an "EAP-Response/Identity" packet with their identity in it to the Authenticator, which is then passed on to the Authentication (RADIUS) Server encapsulated in RADIUS protocol.
3) The Authentication Server sends back a challenge to the Authenticator, such as with a token password system. The Authenticator unpacks this from RADIUS and re-packs it into EAPOL and sends it to the Supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports both client-only authentication and strong mutual authentication. Only mutual authentication is considered appropriate for the wireless case.
4) The Supplicant responds to the challenge via the Authenticator, which passes the response onto the Authentication Server.
5) If the supplicant provides proper credentials, the Authentication Server responds with a success message, which is then passed on to the Supplicant. The Authenticator now allows access to the LAN---possibly restricted based on attributes that came back from the Authentication Server. For example, the Authenticator might switch the Supplicant to a particular VLAN or install a set of firewall rules.

EAPOL (EAP over LAN) has other message types as well. For example, when the Supplicant is finished, it can send an explicit "LOGFF" notification to the Authenticator. 802.1X also defines a re-authentication timer, which can be used to periodically require the Supplicant to re-authenticate.

Moving Beyond Authentication to Encryption

One important piece of 802.1X is the ability to set the WEP (Wired Equivalent Privacy) key for a wireless user. Some EAP authentication methods (such as TLS and TTLS) create a "shared secret" as a side-effect of the authentication. With the shared secret, it is possible for the Authenticator and Supplicant to select identical keys for use in WEP. (Read our white paper "EAP Authentication Methods" for more information).

802.1X authentication helps mitigate many of the risks involved in using WEP. For example, one of the biggest problems with WEP is the long life of keys and the fact that they are shared among many users and are well known. With 802.1X, each station could have a unique WEP key for every session. The Authenticator (Wireless Access Point) could also choose to change the WEP key very frequently, such as once every 10 minutes or every 1000 frames.

802.1X does not guarantee improved security. For example, an Authenticator might never change the key it hands out to each Supplicant. Or, the network manager might select an authentication method that does not allow for distribution of WEP keys. 802.1X does, however, give the informed network manager the potential to design and implement a more secure wireless LAN.