INTERLINK NETWORKS

White Paper

Introduction to 802.1X for Wireless LANs

Abstract

Wireless networking (Wi-Fi) has presented a significant security challenge over the past few years. This paper looks at the fundamentals on how the IEEE 802.1X network access control standard applies and provide an inherently secure solution to wireless networks. It provides an overview of 802.1X, the history behind the technology, and an overview of the 802.1X architecture. It concludes with an explanation of the advantages of using 802.1X in wireless networks.

Introduction

Most 802.11 wireless LAN access points and switches deploy IEEE 802.1X for enhanced security. Trade articles about 802.1X call it a "security protocol," a "security feature," a "security standard," an "authentication method," or a "user authentication protocol" and promise "enhanced security" and a "more secure environment." These claims do not always provide an accurate picture of how 802.1X fits into wireless LAN security. 802.1X, when utilized properly, indeed provides a high level of network security for wireless LANs.

802.1X Overview

The IEEE 802.1X standard, *Port-based Network Access Control*, defines a mechanism for port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructure. It provides a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics. It also prevents access to that port in cases in which the authentication and authorization fails.

The 802.1X specification includes a number of features aimed specifically at supporting the use of Port Access Control in IEEE 802.11 LANs (WLAN). These include the ability for a WLAN access point to distribute or obtain global key information to/from attached stations, by means of the EAPOL-Key message, following successful authentication. .

www.interlinknetworks.com
2500 Packard Road, Ste 202, Ann Arbor, MI 48104 USA
Phone: +1 (734) 821-1200 Fax: +1 (734) 821-1235

Motivation and History

Several emerging trends and needs motivated the development of 802.1X access control into IEEE 802 based networks:

The Increased Use of LANs in Public and Semi-Public Places

802.1X was originally designed to control access to wired networks. Prior to 802.1X, if a user could plug into a live network port, the user gained full access to the network. 802.1X was originally developed to control access to the network by fording the user to authenticate and be authorized before getting on the network.

This issue is magnified with the rapid growth of WLANs. Any user within physical range of a WLAN access point can attempt to utilize network resources. As wireless network deployed the physical boundaries of the network, and many times extend the networks into public spaces, they must control which users have access, and encrypt the user data over the network.

The Need for Per-Port Network Control

Since the port is a user's network attachment point, it is the logical place to control the user's access. It is also a logical point to apply packet and protocol filtering. Thus, by controlling the users network attachment point, the user's network environment can be personalized to meet the user's needs and access permissions.

The Need for Authentication, Authorization and Accounting (AAA)

Many organizations have invested in authentication, authorization, and accounting (AAA) technology to control their users' network access, typically dial-in remote access or access via a firewall. 802.1X can leverage currently installed AAA servers, typically RADIUS servers, to provide these functions to new 802.1X clients.

The Need to Distribute Dynamic Encryption Keys

The original goal of WEP (Wired Equivalent Privacy) was to provide a level of security roughly equivalent to that of a wired network. Unfortunately, WEP broke down when researchers published algorithms that could quickly decipher and break the WEP encryption keys by listening to network traffic.

WEP has been updated with TKIP and AES, more secure encryption technologies as part of the 802.11i standard. 802.1X is also called out in the 802.11i standard and provides a method for distributing encryption keys to access points and stations. This distribution of keys can be used with dynamic WEP, TKIP, and AES.

Terminology

In order to understand the various components in an 802.11 network utilizing 802.1X, consider Figure 1.

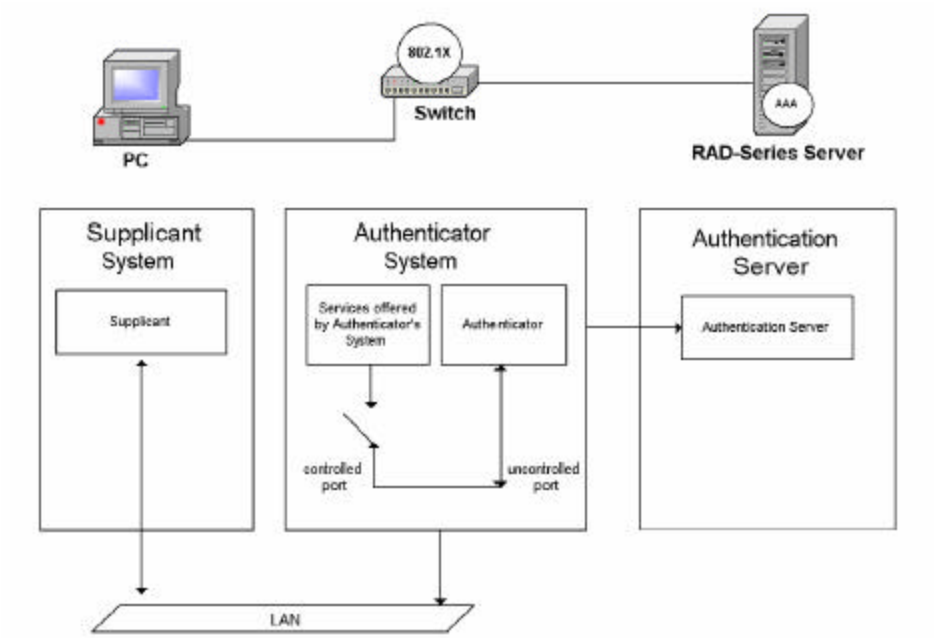

Figure 1. This diagram shows the supplicant, authenticator, and authentication server in an 802.1X wired network. The controlled port shown above is not authorized and therefore is not allowing traffic.

Port

A port in this context is a single point of attachment to the LAN infrastructure. Note that in the 802.11 LAN case, an access point manages "logical" ports. Each of these logical ports communicates one-to-one with a station's port.

Authenticator

The authenticator enforces authentication before allowing access to services that are accessible via that port. The authenticator is responsible for communication with the supplicant and for submitting the information received from the supplicant to a suit-able authentication server. This allows the verification of user credentials to deter-mine the consequent port authorization state.

It is important to note that the authenticator's functionality is independent of the actual authentication method. It effectively acts as a pass-through for the authentication exchange.

Supplicant

The supplicant accesses the services accessible via the authenticator. The supplicant is responsible for responding to requests from an authenticator for information that establishes its credentials.

EAP

The Extensible Authentication Protocol (EAP) is a method of conducting an authentication conversation between a user and an authentication server. Intermediate de-vices such as access points and proxy servers do not take part in the conversation. Their role is to relay EAP messages between the parties performing the authentication. 802.1X employs the Extensible Authentication Protocol (EAP) as an authentication framework.

Extensible Authentication Protocol Over LAN (EAPOL):

802.1X defines a standard for encapsulating the Extensible Authentication Protocol (EAP) messages so that they can be handled directly by a LAN MAC service. This encapsulated form of EAP frame is known as EAPOL. In addition to carrying EAP packets, EAPOL also provides control functions such as start, logoff, and key distribution.

RADIUS

RADIUS is the Remote Access Dial In User Service. It is the standard way of providing Authentication, Authorization, and Accounting services to a network. Although RADIUS protocol support is optional within IEEE 802.1X, it is expected that many IEEE 802.1X authenticators will function as RADIUS clients. In fact, Annex D of the 802.1X standard describes guidelines for 802.1X RADIUS usage and most access points that support 802.1X support it using RADIUS.

802.1X Architecture

802.1X Port-based access control has the effect of creating two distinct points of access to the authenticator's attachment to the LAN. One point of access allows the exchange of frames between the system and other systems on the LAN. Often, this uncontrolled port allows only authentication messages (EAP messages) to be ex-changed. The other (controlled) point of access allows the exchange of frames only if the port is authorized.

When a host connects to the LAN port on an 802.1X switch the authenticity of the host is determined by the switch port according to the protocol specified by 802.1X *before* the services offered by the switch are made available on that port. Until the authentication is complete, only EAPOL frames are allowed exchanged. Once the host authentication is successful, the port switches traffic as a regular port.

Recall that 802.1X was developed to address point-to-point networks. In other words, there must be a one-to-one relationship between a supplicant and an authenticator. In a wired LAN, a supplicant is directly connected to an authenticator. As shown in Figure 1 above, a workstation is directly connected to a LAN switch port. Each port on the LAN switch has an associated authenticator. The workstation gains access to the network when its supplicant authenticates to the LAN port authenticator.

802.1X in 802.11 Wireless LANs

The 802.1X specification includes two main features aimed specifically at supporting the use of Port Access Control in IEEE 802.11 LANs:

1. **Logical Ports.** The ability to make use of the MAC address of the station and access point as the destination address in EAPOL protocol exchanges.
2. **Key Management.** The ability for an access point to distribute or obtain global key information to/from attached stations, by means of the EAPOL-Key message, following successful authentication.

Logical Ports and MAC Address Association

In an 802.11 LAN environment, stations are not physically connected to the network. In addition, multiple connecting stations share the network access media (the RF airspace). A special case of shared media access exists in IEEE 802.11 Wireless LANS in which a station must form an association with an access point in order to make use of the LAN.

The protocol that establishes the association allows the station and access point to learn each other's MAC addresses. This effectively creates a "logical port" that the station can use to communicate with the access point. Access points are configured to use Open Authentication. This allows the supplicant to associate with the Access point before dynamically derived encryption keys are available. Once the association has been established, that attached station may authenticate using the Extensible Authentication Protocol (EAP).

Encryption Key Management

The 802.1X neither excludes nor requires any encryption algorithm. However, it does provide a mechanism for distributing encryption key information from an access point to a client using the EAPOL-Key message. This encryption key information is distributed on a per-session basis to establish dynamic WEP, TKIP and AES keys and to thwart key discovery.

Association and EAP Authentication Procedure

As previously mentioned, a station must first associate with a given access point. Once the station is associated with an access point, it can exchange EAP messages with the authentication server to authorize the port. Before the logical port has been authorized, it only exchanges EAP messages. Figure 2 details a typical EAP ex-change between a station and an authentication server.

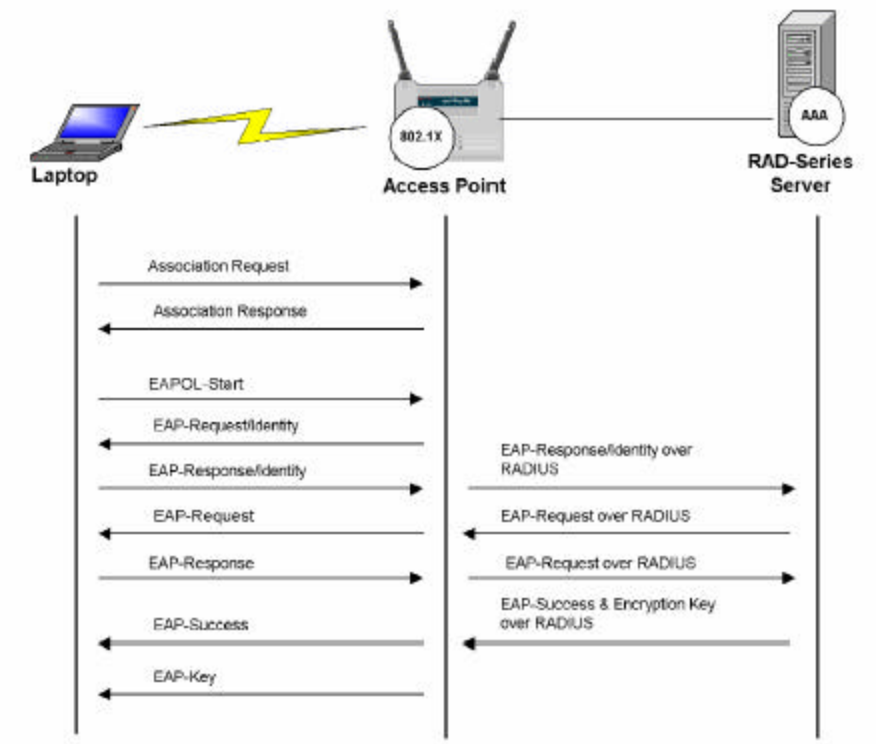

Figure 2. This diagram shows the steps that occur for association, authentication, and key distribution.

Note that the EAP dialog is carried by EAPOL between the station and access point. The dialog is carried by EAP over RADIUS between the access point and the authentication server. This effectively creates an EAP conversation between the station and authentication server that allows the user to authenticate. Once the user is authenticated, the EAP-Key message is sent to relay keying information between to the station.

Advantages of Using 802.1X in Wireless Networks

There are many advantages to using 802.1X in 802.11 LANS.

Control at the Network Edge

802.1X allows a network to restrict access at the edge, where it is most easily managed. Controlled ports, wired or wireless, stop unauthenticated intruders from ever gaining access to your network.

Dynamic Session Key Management

802.1X has a framework that allows a system to use dynamic session encryption keys; to periodically re-key a session; and to periodically re-authenticate a user. This enhances security by eliminating static encryption keys and by foiling attacks on the encryption key that require the collection of large amounts of data encrypted with a single key.

Low Overhead

802.1X does not involve encapsulation, so it adds no per-packet overhead (other than that imposed by enabling encryption such as TKIP or AES) and can be implemented on existing switches and access points with little performance impact. This means that it is scalable, and can be enabled on most existing switch hardware with a firmware upgrade. Since 802.1X can be implemented in the NIC driver, updated drivers from the NIC vendor can usually provide this functionality without the need to install a new operating system.

Utilizes Standards

802.1X integrates well with standards for authentication, authorization and accounting (including RADIUS) allowing it to be implemented on the existing infrastructure for managing dialup networks and VPNs. RADIUS servers that support EAP can be used to authenticate 802.1X-based network access requests.

Interlink Networks Support for 802.1X

Interlink Networks supports 802.1X in its RAD-Series RADIUS Servers with a wide variety of industry standard EAP protocols..

To see how the RAD-Series server is configured to use 802.1X see the application note, *Using 802.1X for Wireless Local Area Networks with Interlink Networks RAD-Series RADIUS Server*.

Interlink Networks delivers the most powerful, robust, and scalable RADIUS server solutions on the market. Since 1991, our RAD-Series Servers have provided access management solutions to some of the largest Carrier and Service Providers around the world.

Interlink Networks, LLC.
2500 Packard Rd, Suite 202
Ann Arbor, MI 48104

Main - (734) 821-1200
Sales - (734) 821-1228
Fax - (734) 821-1235