Supplemental Reading on IEEE 802.1X

IEEE 802.1X

When clients are trying to communicate on a local network, the devices must have a standard method of communication and authentication. The Institute of Electrical and Electronics Engineers (IEEE) created a standard called IEEE 802.1X. This standard specifies a common architecture, functional elements, and protocols that support authentication between the clients of ports attached to the same Local Area Network (LAN). This reading will cover what 802.1X is, basic components of authentication and how it works, and different kinds of authentication available for use under the standard.

IEEE 802.1X Protocol

IEEE 802 networks are deployed in locations that provide access to critical data, support mission critical applications, or charge for service. Port-based network access control regulates access to the network, guarding against attacks by unauthorized parties, network disruption, and data loss.

Authentication

The three main components in the authentication process are:

- **Supplicant** is the client making the request to access the LAN or wireless access point.
- **Authenticator** takes the packet from the supplicator and sends it to the authentication server until the session is authenticated. Any other information sent before authentication occurs is dropped.
- **Authentication server** provides a database of information required for authentication, and informs the authenticator to deny or permit access to the supplicant.

Authentication occurs when a client first connects to a network. The client sends a packet of information and the authenticator sends the packet to the authentication server. In some instances, the authenticator and authentication server may be integrated into a single point. The authentication server then verifies the identity or key against the information in its database. If the credentials are valid, the authentication succeeds. Then the server begins processing the connection request. If the credentials are not valid, the authentication fails. The authentication server sends an Access Reject message and the connection request is denied.

Authentication methods

When the request is sent to the authentication server there are a couple of methods for authentication. IEEE defines two different link-level authentication methods:

- **Shared key system** is a shared key or passphrase that is manually set on both the mobile device and the AP/router.
- **Open system** is when the authentication server has a list of authorized clients to check against when a client requests access. This list is usually in the form of MAC addresses but it varies by network.

Shared Key authentication methods

There are several shared key authentication methods that are commonly used:

- **Wired Equivalent Privacy (WEP)** is not recommended for a secure WLAN. The main security risk is hackers capturing the encrypted form of an authentication response frame, using widely available software applications, and using the information to crack WEP encryption.
- **Wi-Fi Protected Access (WPA)** complies with the wireless security standard and strongly increases the level of data protection and access control (authentication) for a wireless network. WPA enforces IEEE 802.1X authentication and key-exchange and only works with dynamic encryption keys.
- **Wi-Fi Protected Access 2 (WPA2)** is a security enhancement to WPA. Users must ensure the mobile device and AP/router are configured using the same WPA version and pre-shared key (PSK).
- **Association** allows the access point or router to record each mobile device so that data is properly delivered. This occurs after authentication is complete.

These authentication methods are standardized under the IEEE 802.1X protocol.

Key takeaways

IEEE 802.1x is a protocol developed to let clients connect to port based networks using modern authentication methods.

- There are three nodes in the authentication process: supplicant, authenticator, and authentication server.
- The authentication server uses either a shared key system or open access system to control who is able to connect to the network.
- Based on the criteria of the authentication server the supplicator will grant the authentication request and begin the connection process or it will be sent an Access Reject message and terminate the connection.

Mark as completed

Like **Dislike** **Report an issue**

?