802.1X Overview and EAP Types

Documentation

Content TypeProduct Information & Documentation

Article ID000006999

Last Reviewed02/14/2020

|  |  |
| --- | --- |
| **Note** | This data isn't intended for home or small-office users who typically don't use advanced security features such as those discussed within this page. However, these users may find the topics interesting for informational purposes. |

**802.1X overview**

802.1X is a port access protocol for protecting networks via authentication. As a result, this type of authentication method is extremely useful in the Wi-Fi environment due to the nature of the medium. If a Wi-Fi user is authenticated via 802.1X for network access, a virtual port is opened on the access point allowing for communication. If not successfully authorized, a virtual port isn't made available and communications are blocked.

There are three basic pieces to 802.1X authentication:

1. **Supplicant**A software client running on the Wi-Fi workstation.
2. **Authenticator** The Wi-Fi access point.
3. **Authentication Server** An authentication database, usually a radius server such as Cisco ACS\*, Funk Steel-Belted RADIUS\*, or Microsoft IAS\*.

Extensible Authentication Protocol (EAP) is used to pass the authentication information between the supplicant (the Wi-Fi workstation) and the authentication server (Microsoft IAS or other). The EAP type actually handles and defines the authentication. The access point acting as authenticator is only a proxy to allow the supplicant and the authentication server to communicate.

**Which should I use?**

Which EAP type to implement, or whether to implement 802.1X at all, depends on the level of security that the organization needs, the administrative overhead, and features desired. Hopefully the descriptions here and a comparative chart will ease the difficulties in understanding the variety of EAP types available.

**Extensible Authentication Protocol (EAP) authentication types**

Because Wi-Fi Local Area Network (WLAN) security is essential and EAP authentication types provide a potentially better means of securing the WLAN connection, vendors are rapidly developing and adding EAP authentication types to their WLAN access points. Some of the most commonly deployed EAP authentication types include EAP-MD-5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-Fast, and Cisco LEAP.

* EAP-MD-5 (Message Digest) Challenge is an EAP authentication type that provides base-level EAP support. EAP-MD-5 is typically not recommended for Wi-Fi LAN implementations because it may allow the user's password to be derived. It provides for only one-way authentication - there's no mutual authentication of Wi-Fi client and the network. And very importantly it doesn't provide a means to derive dynamic, per session wired equivalent privacy (WEP) keys.
* EAP-TLS (Transport Layer Security) provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point. One drawback of EAP-TLS is that certificates must be managed on both the client and server side. For a large WLAN installation, this could be a very cumbersome task.
* EAP-TTLS (Tunneled Transport Layer Security) was developed by Funk Software\* and Certicom\*, as an extension of EAP-TLS. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel (or tunnel), as well as a means to derive dynamic, per-user, per-session WEP keys. Unlike EAP-TLS, EAP-TTLS requires only server-side certificates.
* EAP-FAST (Flexible Authentication via Secure Tunneling) was developed by Cisco\*. Instead of using a certificate to achieve mutual authentication. EAP-FAST authenticates by means of a PAC (Protected Access Credential) which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution.
* Extensible Authentication Protocol Method for GSM Subscriber Identity (EAP-SIM) is a mechanism for authentication and session key distribution. It uses the Global System for Mobile Communications (GSM) Subscriber Identity Module (SIM). EAP-SIM uses a dynamic session-based WEP key, which is derived from the client adapter and RADIUS server, to encrypt data. EAP-SIM requires you to enter a user verification code, or PIN, for communication with the Subscriber Identity Module (SIM) card. A SIM card is a special smart card that is used by Global System for Mobile Communications (GSM) based digital cellular networks.
* EAP-AKA (Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement) is an EAP mechanism for authentication and session key distribution, using the Universal Mobile Telecommunications System (UMTS) Subscriber Identity Module (USIM). The USIM card is a special smart card used with cellular networks to validate a given user with the network.
* LEAP (Lightweight Extensible Authentication Protocol), is an EAP authentication type used primarily in Cisco Aironet\* WLANs. It encrypts data transmissions using dynamically generated WEP keys, and supports mutual authentication. Heretofore proprietary, Cisco has licensed LEAP to a variety of other manufacturers through their Cisco Compatible Extensions program.
* PEAP (Protected Extensible Authentication Protocol) provides a method to transport securely authentication data, including legacy password-based protocols, via 802.11 Wi-Fi networks. PEAP accomplishes this by using tunneling between PEAP clients and an authentication server. Like the competing standard Tunneled Transport Layer Security (TTLS), PEAP authenticates Wi-Fi LAN clients using only server-side certificates, thus simplifying the implementation and administration of a secure Wi-Fi LAN. Microsoft, Cisco, and RSA Security developed PEAP.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **802.1X EAP Types**  **Feature / Benefit** | **MD5 --- Message Digest 5** | **TLS --- Transport Level Security** | **TTLS --- Tunneled Transport Level Security** | **PEAP --- Protected Transport Level Security** | **FAST** **---** **Flexible Authentication via Secure Tunneling** | **LEAP --- Lightweight Extensible Authentication Protocol** |
| Client-side certificate required | no | yes | no | no | no (PAC) | no |
| Server-side certificate required | no | yes | yes | yes | no (PAC) | no |
| WEP key management | no | yes | yes | yes | yes | yes |
| Rogue AP detection | no | no | no | no | yes | yes |
| Provider | MS | MS | Funk | MS | Cisco | Cisco |
| Authentication Attributes | One way | Mutual | Mutual | Mutual | Mutual | Mutual |
| Deployment Difficulty | Easy | Difficult (because of client certificate deployment) | Moderate | Moderate | Moderate | Moderate |
| Wi-Fi Security | Poor | Very High | High | High | High | High when strong passwords are used. |

**A review of the above discussions and table usually provides the following conclusions:**

* MD5 isn't typically used as it only does a one-way authentication, and perhaps even more importantly doesn't support automatic distribution and rotation of WEP keys so does nothing to relieve the administrative burden of manual WEP key maintenance.
* TLS, while very secure, requires client certificates to be installed on each Wi-Fi workstation. Maintenance of a PKI infrastructure requires additional administrative expertise and time in addition to that of maintaining the WLAN itself.
* TTLS addresses the certificate issue by tunneling TLS, and thus eliminating the need for a certificate on the client side. Making this an often preferred option. Funk Software\* is the primary promoter of TTLS, and there's a charge for supplicant and authentication server software.
* LEAP has the longest history, and while previously Cisco proprietary (works with Cisco Wi-Fi adapters only), Cisco has licensed LEAP to a variety of other manufacturers through their Cisco Compatible Extensions program. A strong password policy should be enforced when LEAP is used for authentication.
* EAP-FAST is now available for enterprises that can't enforce a strong password policy and don't want to deploy certificates for authentication.
* The more recent PEAP works similar to EAP-TTLS in that it doesn't require a certificate on the client side. PEAP is backed by Cisco and Microsoft and is available at no additional cost from Microsoft. If desired to transition from LEAP to PEAP, Cisco's ACS authentication server will run both.

**Another option is VPN**

Instead of relying on Wi-Fi LAN for authentication and privacy (encryption), many enterprises implement a VPN. This is done by placing the access points outside the corporate firewall and having the user tunnel in via a VPN Gateway - just as if they were a remote user. The downsides of implementing a VPN solution are cost, initial installation complexities, and ongoing administration overhead.