

802.1x Overview

William H. Wolfe II (4 mins)

Centralizing Wireless LAN Authentication. This is a continuation of our discussion in the previous session tied to specifics regarding the 802.1x process.

So as I previously mentioned, the 802.1x process uses a RADIUS server as the authentication server. It uses a supplicant or the client driver or client configuration utility for your wireless NIC in your computer whether that be a desktop, or laptop, a smartphone, a tablet and the authenticator as it's called is actually the device that actually performs the authentication activity, but passes that request along to the authentication server, in this case, a RADIUS server to validate that the username and password credentials are accepted.


In the wireless world, the authenticator is usually either the access point if it's a standalone access point environment, or the controller in a controller-based environment such as a wireless LAN controller or it could be the cloud controller in a cloud wireless environment.

802.1 x architecture has multiple components, most of which we've had some detailed discussion on previously:

- There's always a credentials portion of 802.1x. We're either going to be doing EAP-TLS, EAP-Fast or PEAP as we have previously discussed that is going to be the authentication component.
- Then, there's going to be a session key component, and again; WPA, WPA2 or the recommended approaches with WPA2 being the preferred standard.
- And then of course, we have the encryption of which AES is once again tied to WPA2 for the best practice approach.

Different types of 802.1x identity can be used because of different mobility use cases:

- So we have a username and password combination, which generally is being used by EAP-Fast, and the PEAP mechanisms utilizing a RADIUS server, which can also be an LDAP server or your Microsoft Active Directory environment.
- Then we have a two-factor authentication process which would use something such as the RSA SecurID or other token base process. That is also supported by EAP-Fast and the PEAP mechanisms.
- The last one is the Digital Certificates, and we spoke about the fact that the certificates are necessary for EAP-TLS. This requires you to have a certificate



service running, a certificate signed by a certificate authority such as Entrust or Verisign, and generally it is EAP-TLS that uses this. EAP-Fast will take advantage of this by performing EAP-TLS after the protective access credential is generated, which then acts as the certificate for the continuing processes.