

Types of EAP

William H. Wolfe II (5 mins)

There is an ability to actually do something called the local EAP, and the easiest way to think of this is that, this is local ratings. Instead of having an external RADIUS server in your environment, you can actually perform the EAP functionality, i.e., the RADIUS functionality inside a Cisco Wireless LAN controller.

In that particular situation, you actually have four different EAP methods that are supported. One of them is one that we haven't mentioned previously called LEAP, that's the Lightweight Extensible Authentication Protocol.


That was developed actually by Cisco, and was then subsequently in the course of events, replaced by EAP-FAST because LEAP was determined to have vulnerabilities. As you may recall from a very early session in this series, we talked about a tool called 'ASLEAP' that was a hacking tool to crack the LEAP protocol. LEAP was a Cisco solution. It authenticated via user ID and password. It did support single sign-on using Microsoft's Active Directory and it simplified deployment and administration and was supported on multiple operating systems, but, it had to have a specific client or supplicant and again this has similarity been deprecated from the industry.

EAP-FAST, as was mentioned previously, was the replacement for LEAP. EAP-FAST uses a process called Protected Access Credentials and it actually dynamically provisions that. It creates a unique shared credentials and certificate that's used by both the client and the server. It creates a secure tunnel and allows everything to be authenticated via that secure tunnel approach. This also for reference, uses WPA2 and AES for encryption in the enterprise model.

EAP-TLS, which is generally considered the most secure of all authentication methods due to the fact that it requires a client and server-side certificate. It is supported generally by most clients and client supplicants, and it does require a RADIUS server as well.

PEAP is a Microsoft solution. It's a hybrid because it only requires a server-side certificate. It does not require client-side certificates because it uses the MSCHAP or GTC methods. Again, RADIUS is involved, it does require a server certificate and uses One-Time Password, and is supported by LDAP, UNIX, Microsoft's Active Directory as well as Kerberos given the fact that it is a Microsoft developed technology.

One of the things that we have to consider when we're looking at the EAP mechanisms that are supportable by our clients is that every client driver and wireless



LAN NIC card configuration software, also known as the supplicant needs to adhere to something that Cisco actually help defined for the industry, call the Cisco Compatibility Extension versions. As you can see from this slide, we have now migrated ourselves into CCX version 5, and version 5 is that particular client supplicant compatibility version that supports the management frame protection that we spoke about in our 'Vulnerabilities and Mitigation' section.

If we want to have WPA2 and EAP-FAST and AES encryption, our client supplicant needs to be at CCX version 3.

Some EAP protocol feature support are listed here just for reference perspectives.