

EAP Methods

William H. Wolfe II (4.5 mins)

I've mentioned the EAP - Extensible Authentication Protocol methods a number of times and what I want to do here is talk about how one would choose one of the EAP methods, because there are multiple EAP methods that we'll be reviewing.

The key reason to specifically choose one EAP method over the other is –

- does my authentication server support this?
- Security versus complexity, and management and configuration and
- does the client support it? That tends to be one of the most important of the three reasons for choosing because each client's wireless LAN client driver or what we call the supplicant supports certain EAP methods and does not support other EAP methods.

If you have a Windows client, a Mac and an Apple iOS device such as a iPhone or an iPad, you're going see that different EAP methods are supported.

We'll talk about the EAP methods in detail in just a moment.

What are the methods that tie back to the WPA2 enterprise environment? Well, we have what we call protective tunnel methods which are PEAP and EAP-FAST. EAP-Fast is a development specifically by Cisco. We also have authentication credential methods, and that's the EAP-MSCHAP from Microsoft, and the EAP-GTC authentication method.

Now, the last one is specifically considered a certificate based authentication and that's EAP-TLS (Transport Layer Security). So, that is a certificate based solution that requires both a client-side and server-side certificate.


In all cases, AES strong encryption is used with a 128-bits key.

Some EAP method comparisons here between TLS, PEAP and EAP-FAST, which are the three most common ones used. Secure roaming and local authentication using a wireless LAN controller are supported in all of them.

One-Time Password support is not necessary for EAP-TLS because of these certificates.

In the case of server and client certificates, one unique characteristic is that EAP-TLS needs both server and client certificates.

PEAP is a server certificate based solution only and EAT-FAST does not use



certificates at all. It actually uses something known as a PAC (Protected Access Credential) which is actually delivered and configured dynamically at the time of the first connection in which you authenticate using a user ID and password solution.

Complexity for deployment is extremely high for EAP-TLS because of the need for signed certificates and certificates servers,

EAP-FAST is actually considered low deployment complexity but yet, it has the characteristics after the authentication is done, to actually use components of EAP-TLS and of course the high encryption AES 128 bits.