NTS® QA MONTHLY

802.1x Standard Interoperability Testing

The IEEE-802.1x standard with Extensible Authentication Protocol (EAP) is becoming the security implementation of choice for wireless 802.11b networks. The 802.1x standard provides a mechanism for 802.11b Wireless Access Points to provide a port-based network access control, allowing connection requests from wireless clients to be authenticated through an MD5 challenge or TLS, which provides mutual authentication of client and server. This is a vast improvement over the highly criticized WEP protocol which provides security only at the physical level and does nothing to authenticate the user.

What is 802.1x?

The IEEE 802.1x standard is a security development for 802 compliant LAN devices. Defined, it is a mechanism for port-based network access control that makes use of the physical characteristics of 802 LAN devices, but for the purpose of this article, we are only concerned with how it provides this service for 802.11b networks and when used in conjunction with EAP, can provide a secure method of access for wireless networks. The Extensible Authentication Protocol is an extension of PPP, an authentication scheme used primarily for point-to-point links, like dial-up internet access or PPP over Ethernet used in most DSL implementations. For authentication to occur during a PPP connection attempt, both sides of the point-to-point link must agree on the authentication protocol configuration during the Link Control Phase before any data can pass. EAP in contrast, does not select a specific authentication prior to the Link Control Phase and has the ability to postpone this until actual authentication has occurred by the authenticator or Access Point. Once the Link Establishment phase is completed, the authenticator will send request(s) to the client for authentication and will permit or deny access depending on the correct or incorrect response. There are three main components for an EAP implementation; the following are the devices and how they are referenced in relation to EAP:

- Authenticator | Access Point
- Authentication Server | RADIUS / AAA Server
- Supplicant | Wireless Client

EAP-TLS in action

There are two flavors of EAP that can be used with the 802.1x standard. One flavor provides a mechanism for an MD5 challenge and the other is EAP-TLS. EAP-TLS (Transport Level Security) enables mutual authentication system that allows the client to authenticate to the server and the server to the client through the use of a Certificate Authority. Certificates on both the Certificate Authority and the client must be valid in order for a connection to be established. Here is a quick explanation on the EAP-TLS conversation that takes place when a wireless client wants to access an 802.1x network via EAP-TLS:

1. Wireless Client gets associated with the Access Point

2. Access Point does not permit the client to send any data at this point and sends an authentication request.

3. Client's screen displays a logon screen. The supplicant will then respond with an EAP-Response Identity with userId back to the Authentication Server.

4. RADIUS server responds back to the client with an EAP-TLS Start Packet. The EAP-TLS conversation starts at this point.

5. The peer sends an EAP-Response back to the authentication server which contains a client_hello handshake message, a cipher that is set for NULL that will remain this value until change_cipher_spec are negotiated, and TLS version number

6. The server will present it's certificate to the client as well as request a valid one from the client. The authentication server responds with an EAP-Request packet that contains the following:

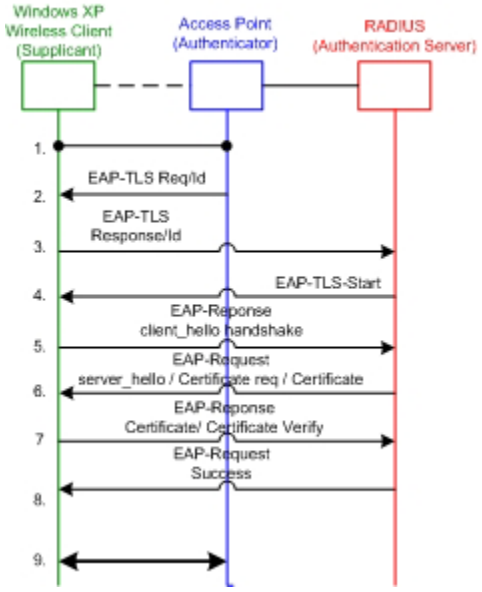
   - TLS server_hello
   - handshake message
   - certificate
   - server_key_exchange
   - certificate request
   - server_hello_done.

7. Client responds with a EAP-Response message that contains the following:

   - Certificate – Server can validate to verify that it is trusted.
   - client_key_exchange
   - certificate_verify – Verifies the server is trusted
   - change_cipher_spec
   - TLS finished

8. After the client authenticates successfully, the EAP server will respond with an EAP-Request which contains the change_cipher_spec and finished handshake message. The finished handshake message contains the authentication response from the server. Upon receiving this the client will verify the hash in order to authenticate the EAP server. A new encryption key is dynamically derived from the master secret during the TLS handshake.

9. At this point the EAP-TLS enabled wireless client can access the wireless network.



In conclusion, the 802.1x standard along with EAP-TLS, provide a secure method to authenticate access to your wireless network. NTS labs can provide the test environment to verify that your 802.11b compliant network device can interoperate using the 802.1x standard with other vendor offerings. Our labs are composed of the latest wireless gear from vendors like Cisco, 3Com, Linksys, Netgear, Intel, and Orinico to name a few. We can also deploy environments using a mixture of different vendor implementations of Authentication Software and Operating Systems. Can your product access an 802.1x enabled wireless network? Find out now!

Contact one of our NTS Account Managers today for more information.