

# Comprehensive approach to 802.1x protocol testing

By David Charlu  
Chief Technology Officer  
Net-O<sub>2</sub> Technologies  
E-mail: davidc@net-o2.com

The original intent of IEEE in introducing the 802.1x port-based network access standard based on the IETF extensible authentication protocol was to enable LAN infrastructure as a means of authenticating and authorizing devices attached to them over point-to-point connections (scenario 1 in **Figure 1**).

However, as a result of the vulnerabilities reported in early deployments of 802.11 WLANs, several vendors have released their own solutions (LEAP, PEAP, etc.) based on the 802.1x standard. Since WLANs use shared-media connectivity (scenario 2 in **Figure 1**) as opposed to point-to-point connections used over Ethernet switches, several improvements in using 802.1x for WLANs have been suggested. The IEEE and Wireless Ethernet Compatibility Alliance have also specified the use of IEEE 802.1x for enhanced security in WLANs.

As a result of 802.1x becoming a key piece in the LAN security framework, testing for 802.1x support in Ethernet switches and WLAN access points has become an important activity considering the various

AdminMACstate	System Auth control	Auth controlled port control	EAP authentication	Auth controlled port status
Enabled	Enabled	Force authorized	x	Enabled
		Force unauthorized	x	Disabled
		Auto	Success	Enabled
			Failure	Disabled
Disabled	x	x	x	Enabled
		x	x	Disabled

Table 1: The Ethernet switch should be tested for all the combinations for the resulting value of AuthControlledPortStatus.

combinations that must be supported to ensure compatibility.

802.1x describes the architectural framework within which the authentication and consequent actions take place. Moreover, it supports various authentication methods such as one-time passwords, certificate-based authentication and SIM-based authentication.

The standard defines that the systems on the LAN adopt one of the following distinct roles within an access control interaction:

- Authenticator—The port that wishes to enforce authentication before allowing access to the services accessible via the port.
- Supplicant—The port that wishes to access the services used by the authenticator's system.

A further system role is described as the authentication server. This performs the au-

thentication functions necessary to check the credentials of the supplicant and indicates to the authenticator as to whether the supplicant is authorized to access authenticator's services. Remote authentication dial-in user service (RADIUS) has become the most commonly implemented protocol between the authenticator and the authentication server, although 802.1x does not mandate the use of RADIUS.

Although the three roles are necessary to complete the authentication process, there can be several variations possible. In a simplified system, for example, an authenticator and authentication server may be co-located within the same system without the need for an external server. Also, a port may adopt the supplicant role in some exchanges, and authenticator role in others. The latter scenario is useful when a WLAN access point that has

been newly added to the LAN has to be authenticated by a port of the Ethernet switch before it can authenticate other WLAN hosts that will connect using its services.

## Start with configurations

The operation of 802.1x has the effect of creating two distinct points of access to the authenticator (any frame received on the physical port is made available to both points of access):

- Uncontrolled port—This point of access allows for uncontrolled exchange of PDUs regardless of the authorization state.
- Controlled port—This point of access allows for exchange of PDUs only if the current state of the port is authorized.

The AuthControlledPortStatus indicates the status of the controlled port as being either authorized or unauthorized. In addition, an AuthControlledPortControl parameter allows administrator control to set the port as ForceUnauthorized, Auto or ForceAuthorized.

The values of the AuthControlledPortControl parameter for every port in a system can be overridden by means of the SystemAuthControl parameter. Thus, for example, setting the SystemAuthControl parameter to 'disabled' causes authentication to be disabled on all ports and forces all ports to be authorized. Meanwhile, setting it to 'enabled' causes each port's authentication status to be controlled in accordance with the value of the port's AuthControlledPortControl parameter. Finally, any access to the network is subject to the current adminis-

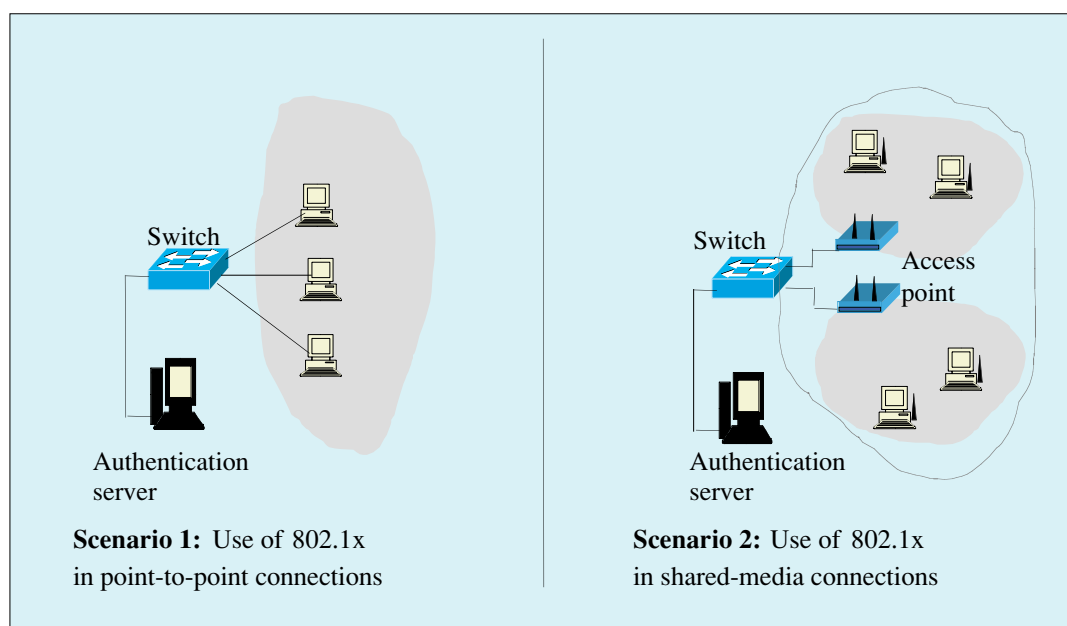


Figure 1: Since wireless LANs use shared-media connectivity as opposed to point-to-point connections in Ethernet switches, several improvements in using 802.1x wireless LANs have been suggested.

Category	Description	Test
802.1x authentication	EAPOL authentication with RADIUS-based authentication server	Supplicant-connection with authenticator, authentication, held state, log off  Authenticator-connection with supplicant, request/response to AS, authentication timeout, reauthentication of supplicant, controlled directions, mutual authentication
EAP authentication types	Supported authentication types such as EAP-TLS, EAP-TTLS and security mechanism such as LEAP, PEAP etc. with RADIUS-based authentication server	Verification of supplicant and authenticator for support of EAP types
Key management	Key generation and distribution	Key generation and distribution

Table 2: 802.1x tests categories.

trative and operational state of the MAC. If the MAC is rendered inoperable, then no protocol exchange of any kind can take place.

In secure configurations, SystemAuthControl will be set to 'enabled' and AuthControlledPortControl will be set to 'auto' or ForceUnauthorized. Meanwhile, the Ethernet switch should be tested for all the combinations for the resulting value of AuthControlledPortStatus (Table 1).

#### Authentication framework

When using 802.1x authentication in a LAN, the station (supplicant) needs to be authenticated by the LAN infrastructure (Ethernet switch). However, this simple scheme causes a potentially dangerous situation similar to the "man-in-the-middle attack", wherein an intruder masquerades itself as the authenticator and gets access to the authentication information

from the station. Mitigation of this type of attack requires a two-step authentication—the workgroup switch is authenticated by the main Ethernet switch, and then the station is authenticated by the workgroup switch. Thus, a workgroup switch should be tested for support of both the supplicant and the authenticator.

In WLAN situations, it is also necessary to test if the mutual authentication between the host station and the authentication server via the access point is performed correctly. This is necessitated to mitigate the rogue-access point scenario, where the access point is introduced by the intruder to gain access to the host station and eventually to other stations in the network.

Interoperability with the authentication server has to be tested to verify that the authentication procedures are properly implemented. The compo-

nent of the 802.1x implementation that interacts with the authentication server is called the back-end authentication state machine. Since 802.1x supports timeout of authorization state information on a periodic basis, this aspect should also be tested.

Tests should be conducted for all the supported authentication types, such as EAP-MD5, EAP-TLS, EAP-TTLS, and supported security mechanisms such as PEAP, LEAP, etc. Some of these methods involve the use of a third-party certification server.

#### Key management

The enhanced privacy, data authentication and replay protection mechanisms require fresh cryptographic keys. Hence, the 802.1x's support for automatic key distribution is used in WLANs. This is another critical component of 802.1x that needs to be tested.

802.1x's widespread application results in many more test scenarios. Two other examples of this are link aggregation and virtual LAN (VLAN). Since 802.1x acts on physical ports, testing it with 802.3ad link aggregation in Ethernet switches require configuration of ports as unaggregated ports. After authentication, the port can join an aggregate link; similarly unauthorized ports should be forced to leave the aggregate.

Testing with 802.1Q VLANs also work with a similar policy of allowing assignment of VLAN based on the outcome of the 802.1x authentication. An Ethernet switch port has to be in the forwarding state during authentication, permitting access to the non-authenticated LAN. Once authentication has succeeded, a new VLAN-ID is assigned to the port while the port remains in the forwarding state.

Security being a critical aspect of today's enterprise networks, the 802.1x standard is being increasingly implemented by Ethernet switch vendors and WLAN vendors alike. As more improvements to the security frameworks are being made, implementors have to ensure conformance to the standards and interoperability with other vendor implementations with the added challenge of maintaining compatibility with legacy protocols. A comprehensive approach to testing will help address the challenge of releasing consistently well-tested standards-based products in the marketplace. □