802.1X

802.1X is a network access control mechanism used to authenticate devices wishing to connect to a network. It is an IEEE standard originally defined in 2001 with 802.1X-2010 being the most current revision. Other basic forms of port security are based on MAC address. The most significant limitation with MAC address based methods is that the device is authenticated with no regard given to the user. 802.1X utilizes user identification and authentication managed from a centralized server. This allows the user to be authenticated and not just the device.

802.1X is used to prevent rogue devices from accessing the network. It has the ability to provide personalized network access based on user identification. This functionality varies significantly by switch and server manufacturers, but many provide the flexibility to place devices in a specific VLAN based on identity. For example, a user can connect a laptop anywhere on the network and be granted access to their specific departmental VLAN based on authentication credentials through 802.1X. This allows users to freely move to different areas of the facility while still maintaining access to their needed network resources without any network changes.

Terminology

Many switch manufactures refer to the implementation of this security method simply as 802.1X. Others have specific names to reference this feature set within their specific operating systems.

- Cisco = Dot1x
- Extreme Networks = Netlogin

How does 802.1X work?

802.1X identifies the three primary participants as follows:

**Supplicant**
This is the end-point device wishing to connect to the network. When first connected to the network, it will negotiate with the authenticator to request access to the network. The supplicant communicates with the authenticator using the EAP protocol.

**Authenticator**
This is the network switch and is responsible for authenticating the supplicant before granting access to the network. When a new device is plugged into a secured port, it will request identity and authentication information from the endpoint. Until the endpoint has been authorized, only traffic related to the authentication process is allowed. All other traffic* will be dropped by the switch. The authenticator communicates with the supplicant using the EAP protocol and...
with the authentication server using the RADIUS protocol.

**Authentication Server**
This is a server that contains the user database used to authenticate endpoints that wish to gain access to the network. The authenticator and authentication server communicate using the RADIUS protocol. The authenticator relays messages between the authentication server and the supplicant to exchange authentication credentials. If the supplicant is successfully authenticated, the server informs the authenticator which then allows traffic to flow through the port.

* Some switch manufacturers do allow certain layer 2 network control protocols such as CDP and STP to pass on an unauthenticated port.

**Protocols**

802.1X utilizes two distinct network protocols:

**EAP or EAPol (Extensible Authentication Protocol over lan)**
This is a layer 2 protocol used to communicate between the supplicant and authenticator during the authentication process.

**RADIUS (Remote Authentication Dial In User Service)**
This is a layer 3 protocol used by the authenticator to communicate with the authentication server. EAP messages that must be sent between the supplicant and authentication server are encapsulated in a RADIUS message. Since it is layer 3, the server does not need to be located on the local network segment.

![Authentication Process Diagram](image)

**Authentication process**

Here is a very simplified description of the 802.1X authentication process.
• **Step 1:** The supplicant is connected to a network port with 802.1X enabled. The supplicant can send the optional *Start* message using the EAP protocol to indicate it wishes to authenticate.

• **Step 2:** Once the switch has detected a connected device, it will send an *Identity Request* message to the supplicant using the EAP protocol.

• **Step 3:** The supplicant responds to the authenticator with its user identity and authentication information over EAP.

• **Step 4:** The authenticator encapsulates the EAP identity response into a RADIUS message and sends it to the authentication server.

• **Step 5:** The authentication server and supplicant exchange a sequence of messages used to verify the identity of the supplicant. This exact process depends on the level of security and encryption used to protect the credentials. The same process of encapsulation/de-encapsulation between protocols is maintained.

• **Step 6:** The authentication server responds to the authentication with either a RADIUS *Access-Accept* or *Access-Reject* message.

• **Step 7:** The authenticator responds to the supplicant with either an EAP *Success* or *Failure* message.

If access is accepted, the authenticator will then open up the port to the appropriate network traffic. If rejected, the port remains restricted to EAP traffic and the authentication process is attempted again.

### 802.1X security

The standard allows for protecting the 802.1X traffic using varying degrees of encryption to prevent authentication credentials from passing over the wire as clear text. This reduces the vulnerability of a “man in the middle” attack that intercepts network traffic.

Biamp supports the following security types:

- EAP-MD5
- EAP-PEAP/MSCHAPv2
- EAP-FAST
- EAP-TTLS/EAP-MCHAPv2
- EAP-TLS

### What Biamp products support 802.1X?

*(802.1X is only available with Tesira firmware version 3.7 or higher. 802.1X support on AVB ports is only available with Tesira firmware version 3.8 or higher.)*

802.1X is supported on the **control** and **AVB** ports for the following devices:

- Tesira SERVER**
- Tesira SERVER-IO
- TesiraFORTÉ (all models)
802.1X is supported on the **VoIP interface** ports on the following devices:

- Tesira SVC-2
- TesiraFORTÉ VI & VT

**NOTE:** 802.1X is only available on Tesira devices running Tesira firmware version 3.7 or higher.

**NOTE:** 802.1X will not operate on any Tesira devices that are operating in recovery mode.

**NOTE:** 802.1X on dynamic VLAN (AVB) enabled ports is not supported by Extreme Networks. Control ports are supported. In order to utilize this feature, disable dynamic VLAN (MVRP) in XOS and manually create the AVB VLAN (VLAN 0002). Contact Extreme Networks GTAC for support on this feature.

** 802.1X is not supported when using server redundancy mode.

**Configuring 802.1X**

802.1X is configured through the Device Maintenance window in the Tesira software or from the device management page in SageVue. The configuration options are identical between the two methods.
Tesira 802.1X Configuration Page

![Tesira 802.1X Configuration Page](image1)

SageVue – Device Management page

![SageVue – Device Management page](image2)

Configuration Options

**Interface**
This dropdown list allows you to select the interface to be configured. The list is restricted to only ports that support 802.1X on that device.

**Mode**
This dropdown list allows you to select the 802.1X mode to be used. Supported modes are:

- EAP-MD5
- EAP-PEAP/MSCHAPv2
- EAP-FAST
- EAP-TTLS/EAP-MCHAPv2
- EAP-TLS

**EAP-FAST Provisioning Mode / Fast Method Provisioning Enabled**

This allows you to select authenticated or unauthenticated provisioning for the EAP-FAST mode.

**Anonymous Identity**

This field is used for EAP-TTLS and EAP-FAST modes. When used, the text from this field is included as the identity in the initial EAP negotiation messages while the *Identity (username)* field be transmitted in subsequent encrypted messages. This provides a mechanism to protect the *Identity (username)* from being transmitted in clear text that is viewable using a packet sniffer.

**Identity (user name)**

This is the login identity to be used for authentication. It is required for all modes.

**Password**

This is the password associated with the Identity for authentication. It is required for EAP-MD5, EAP-PEAP, EAP-TTLS, and EAP-FAST modes. It is not required for EAP-TLS as this mode uses certificates for full authentication.

**Root Certificate**

This button is used to upload a root certificate to the device. Root certificates should be provided by the IT security management group for the facility. Root certificates must be either .pem or .der format and are limited to a size of 10K. A root certificate is required for EAP-PEAP, EAP-TTLS, and EAP-TLS modes.

**Client Certificate**

This button is used to upload a client certificate to the device. Client certificates should be provided by the IT security management group for the facility. Root certificates must be either .pem or .der format and are limited to a size of 10K. A client certificate is required for EAP-TLS. It is required for EAP-FAST when authenticated provisioning is enabled.

**Further reading**

- [SageVue](#)
- [Wikipedia 802.1X](#)
- [IEEE 802.1X-2010](#)
- [Wireless Networking (contains good descriptions of the different EAP modes)](#)