802.1X

IEEE 802.1X is a standard for authentication in computer networks

The **IEEE 802.1X** standard provides a general method for authentication and authorization in IEEE 802.1X networks. At network access, a physical port on the LAN, a logical IEEE 802.1Q VLAN, or a WLAN, a subscriber is authenticated by the authenticator, which uses an authentication server (**RADIUS server**) to verify the authentication information provided by the subscriber (supplicant) and, if necessary, to allow or deny access to the services (LAN, VLAN, or WLAN) provided by the authenticator.

This possibility of using an authentication server makes network access possible even for locally unknown subscribers. For example, members of many universities can use **WLAN** at other universities via **eduroam** without having to set up guest access or the like open to everyone.

The standard recommends the **Extensible Authentication Protocol (EAP)** or the **PPP-EAP-TLS Authentication Protocol** for authentication, since no separate authentication protocols are defined.

According to IEEE, a capital letter must be used for the notation, since IEEE 802.1X is a stand-alone standard and does not supplement an existing standard.

- **Supplicants**
  are all **IEEE 802.1X-authenticable** devices (see **IEEE 802.1X** Article 5.1 "Requirements") that must authenticate to the network according to the network rule before the network device is allowed access to the network resources.
  In practice, the supplicant is implemented in the form of a software implementation. For example, Windows XP (including SP2) natively supports a supplement implementation. Furthermore you can also use the free supplicant implementations from the projects of Open1x or SecureW2 to build up an IEEE 802.1X infrastructure. However, not all network components (such as network printers) are able to authenticate to the network via IEEE 802.1X. Often old and even newer hardware lacks the IEEE 802.1X supplicant implementation. This is the biggest criticism of IEEE 802.1X when introducing IEEE 802.1X into production systems. Some switches provide the "MAC bypass" function for this problem, for example. This makes it possible to authenticate the network device using the MAC address. This allows authentication of devices that do not have an IEEE 802.1X supplicant implementation.

- **The authenticator**
  exists between the supplicant and the network to be protected. The role of the authenticator is to verify the authenticity of the supplicant, similar to the role of a doorman in an identity card check. If the supplicant can successfully identify himself to the authenticator with valid credentials, the supplicant is granted access to the network by the authenticator. If authentication fails, access is denied. In practice, the authenticator can be an IEEE 802.1X-enabled switch, router or IEEE 802.11 WLAN access point. The credentials are usually requested by the Authenticator from an Authentication Server (AS). The authentication server is found in the IEEE 802.1X model in a trusted network.

- **Port Access Entity: PAE**
  The PAE, which can be presented in practice as a port at the switch, implements a state machine by always mapping the respective authentication state between supplicant and authenticator at the controlled port. The IEEE 802.1X provides three possible access modes for supplicants for the access setting in the PAE:
  - ForceUnauthorized: The controlled port is in "not authorized" mode. This blocks any access by a supplicant. It does not matter whether the supplicant can authenticate successfully or not, access is always blocked.
  - ForceAuthorized: The opposite of ForceUnauthorized. The controlled port is in "authorized" mode. The supplicant is always granted access. It is not important whether the supplicant can authenticate to the authenticator, access is always allowed. This mode is useful for setting up IEEE 802.1X switches. For example, enabling IEEE 802.1X authentication in conjunction with
  - ForceAuthorized mode enables IEEE 802.1X to be activated successively. In ForceAuthorized mode, for example, internal IEEE 802.1X functionality tests can be performed on the switch before activating the productive "auto" mode, which forces all supplicants to authenticate.
  - Auto: Requires successful authentication from the supplicant. If the supplicant has successfully authenticated, access is granted, otherwise it remains blocked.

    The PAE can assume a supplicant or authenticator functionality.

- **Authentication Server (AS)**
  The AS provides an authentication service to the Authenticator. The AS is usually installed in the protected network and does not need to authenticate itself. In practice, the AS can be a RADIUS server service, as provided freely by the FreeRadius project, for example. If the operating systems Windows 2000 or Windows 2003 are used, a RADIUS server can be operated with the "Internet Authentication Service" (IAS). Every major manufacturer of switches and routers also provides its own RADIUS implementation, please refer to the product offerings of the respective manufacturers.
  The credentials to be checked can be located directly on the AS in the form of a simple text file, but the AS can also access a database service using database drivers. The back-end possibilities are theoretically unlimited for an AS. In practice, an LDAP connection is often preferred. The advantage is obvious: Existing domain user IDs already exist in the Active Directory Service (ADS) of Microsoft operating systems. In the case of free LDAP implementations, it can also be the OpenLDAP3 service, which is suitable for LDAP operation. The manifold backend possibilities of the RADIUS server are therefore also advantages for the use of IEEE 802.1X. This example clearly shows that the IEEE 802.1X standard is based on existing interfaces and thus strives to be practical.
  In the context of RADIUS terminology, the term network access server (NAS) is used instead of the term "authenticator". Dialing computers regard the NAS as a server. From the RADIUS server's point of view, the NAS is a client.
  The range of services and the user ID (assignment of the VLAN)

RADIUS access accept messages from the Authentication Server to the Authenticator are a major advantage when using IEEE 802.1X. RFC 2869 "RADIUS Extensions" describes a large number of attributes that are sent from the AS to the authenticator. Three interesting attributes are called "Tunnel-Type", "Tunnel-Medium-Type" and "Tunnel-Private-Group-Id". At the end of RADIUS authentication, the RADIUS server sends an access accept message to the network access server. If these three attributes are appended to the Access Accept message, the NAS will request that the supplicant be assigned to the relevant VLAN. The VLAN ID is located exactly in the attribute "Tunnel-Private-Group-Id" of the reply packet. The NAS switches the port from the guest VLAN to the VLAN intended for the supplicant. In practice, this means that the user information that the authenticator sends to the AS can be used to provide an adapted range of services for the supplicant. On Linux, BSD or Windows servers it is relatively easy today to implement several VLANs and thus provide a selection of services for each VLAN.

Source: https://en.wikipedia.org/wiki/IEEE_802.1X

Related Links:

- 802.1Q
- 802.1X
- Basics of networks
- Broadcasting
- Bus topology
- CIDR - Classless Inter-Domain Routing
- CIDR-Notation
- CSTA - Computer-supported telecommunications applications
- Determining local hosts and remote hosts
- DHCP - Dynamic Host Configuration-Protokoll
- DNS - Domain Name Service
- EHS - Electronic Hook Switch
- How can I set up Snom phones for TCP support
- How to setup SNMP
- HowTo - Networking - IPv6