IEEE 802.1X Overview

Port Based Network Access Control

802.1X Motivation and History

- Increased use of 802 LANs in public and semi-public places
- Desire to provide a mechanism to associate end-user identity with the port of access to the LAN
  - establish authorized access
  - enable billing and accounting mechanisms
  - personalize network access environment
- Leverage existing AAA infrastructure currently used by other forms of network access (e.g. dial-up).
- Initially intended for 802.1D, but since expanded to include other access devices (e.g. 802.11, smart repeater).

802.1X Overview

- A method for performing authentication to obtain access to IEEE 802 LANs. Ideally occurs at the first point of attachment (i.e. the edge).
- Specifies a protocol between devices desiring access to the bridged LAN and devices providing access to the bridged LAN.
- Specifies the requirements for a protocol between the Authenticator and an Authentication server (e.g. RADIUS).
- Specifies different levels of access control and the behavior of the port providing access to the bridged LAN.
- Specifies management operations via SNMP.

Definitions

Authenticator

The entity that requires the entity on the other end of the link to be authenticated.

Supplicant

The entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.

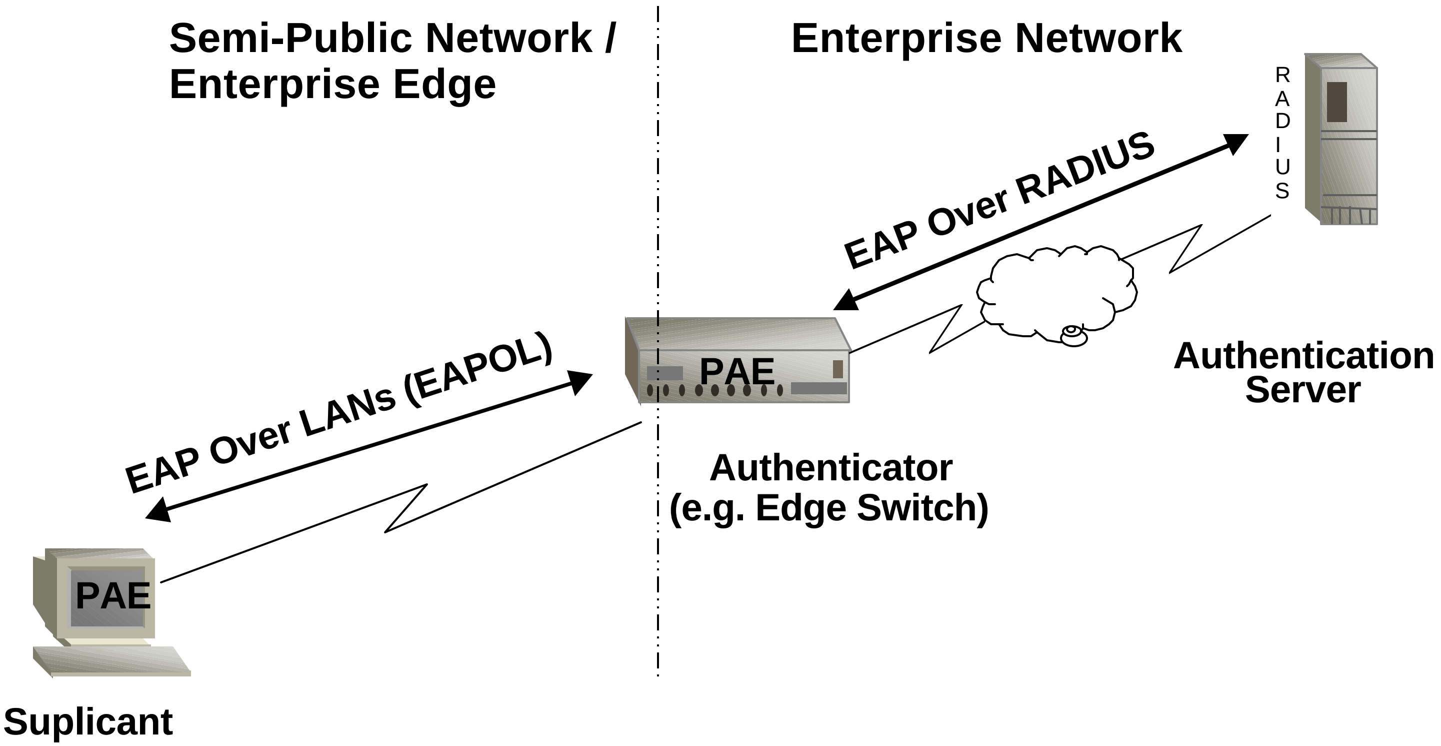
Port Access Entity (PAE)

The protocol entity associated with a port. May support functionality of Authenticator, Supplicant or both.

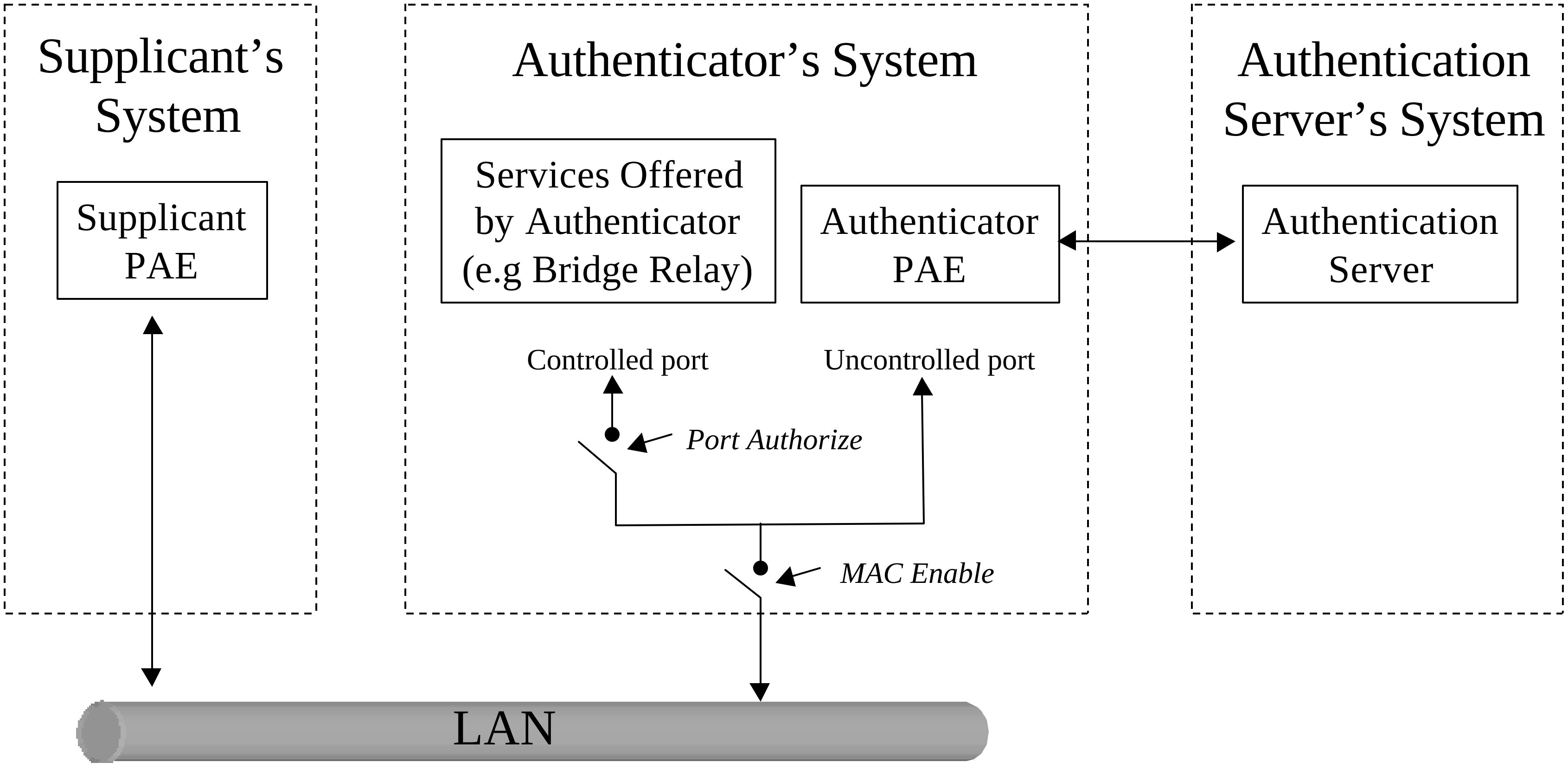
Authentication Server

An entity providing authentication service to the Authenticator. Maybe co-located with Authenticator, but most likely an external server.

General Topology



Principal of Operation



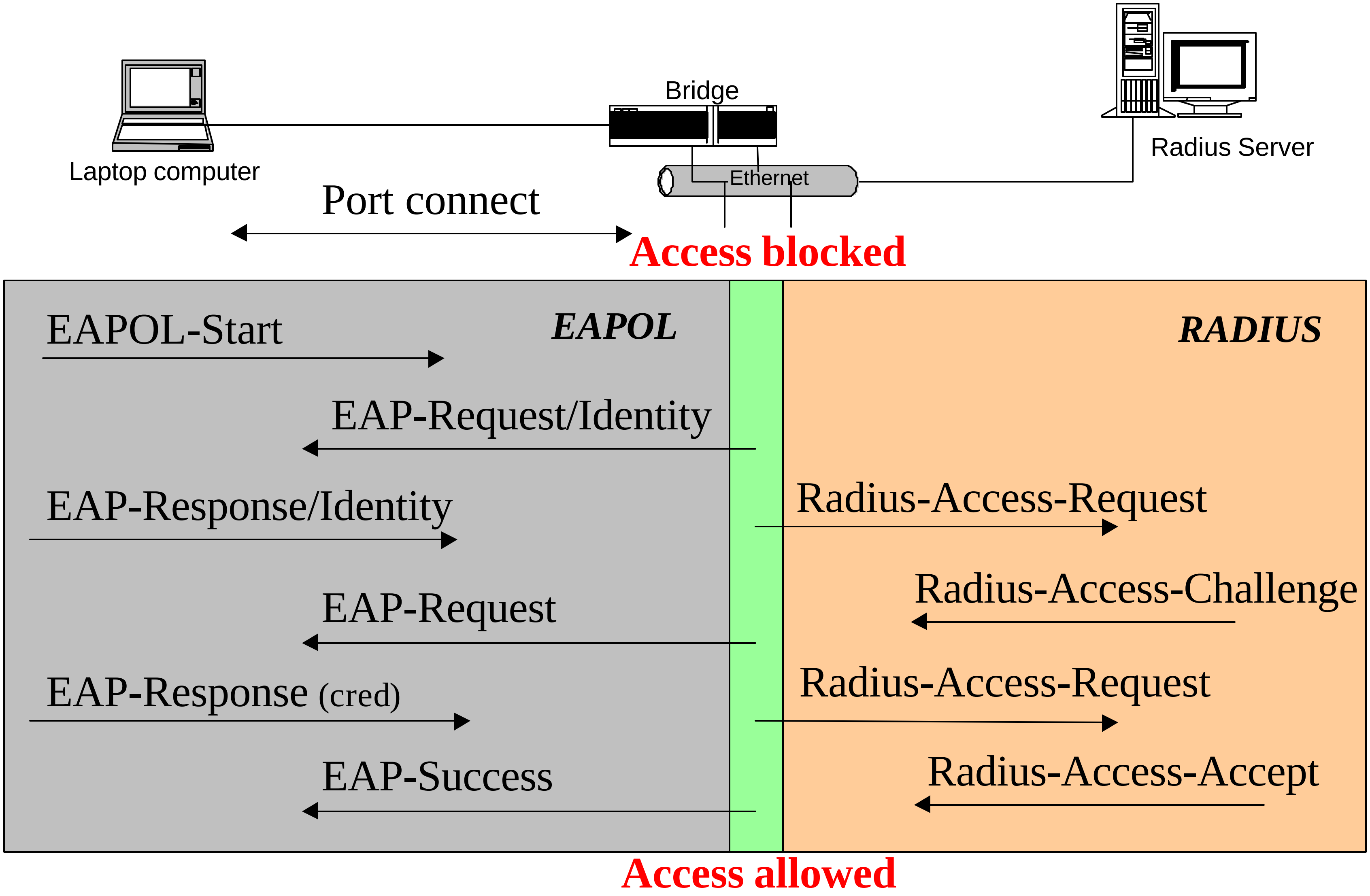
Full Control and Partial Control

- Full Control prohibits transmission and reception through the controlled port unless authorized.
- Partial Control allows transmission through the controlled port to support Wake-on-LAN
- Partial Control may be changed to Full Control by higher layers (e.g. Bridge Detection software to avoid Spanning Tree Loops).

Protocol Overview

- Encapsulate the Extensible Authentication Protocol (RFC 2284) in 802 Frames (EAPOL) with a few extensions to handle unique characteristics of 802 LANs.
- EAP is a general protocol supporting multiple authentication methods (smart cards, Kerberous, public key, one-time password, etc).
- Authenticator passes authentication exchanges between supplicant and authentication server.
- Authenticator PAE enables the controlled port based upon the result of the authentication exchanges.

IEEE 802.1X Conversation



Port connect

Access blocked

EAPOL

RADIUS

EAPOL-Start

EAP-Request/Identity

EAP-Response/Identity

Radius-Access-Request

Radius-Access-Challenge

EAP-Request

EAP-Response (cred)

Radius-Access-Request

Radius-Access-Accept

EAP-Success

Access allowed

Possible Additional Services

- Allow port VLAN membership to be assigned as outcome of authentication
  - enables the un-authenticated VLAN
  - enables end-station manageability after failed authentication
  - enables the association of VLAN assignment to user identity
- Allow mechanism to initiate LAN usage accounting.
- Supports a mechanism to associate incoming traffic priority with user identity
- Exchange of 802.11 session keys

802.1X Summary

- Low impact mechanism for addressing end-user authenticated access to 802 LANs
- Applicable to a variety of access devices (e.g. 802.1D bridges, 802.11 APs, Smart 802.3 repeaters, DSL environments)
- Leverages existing AAA infrastructure
- Extensible protocol to support future authentication methods.