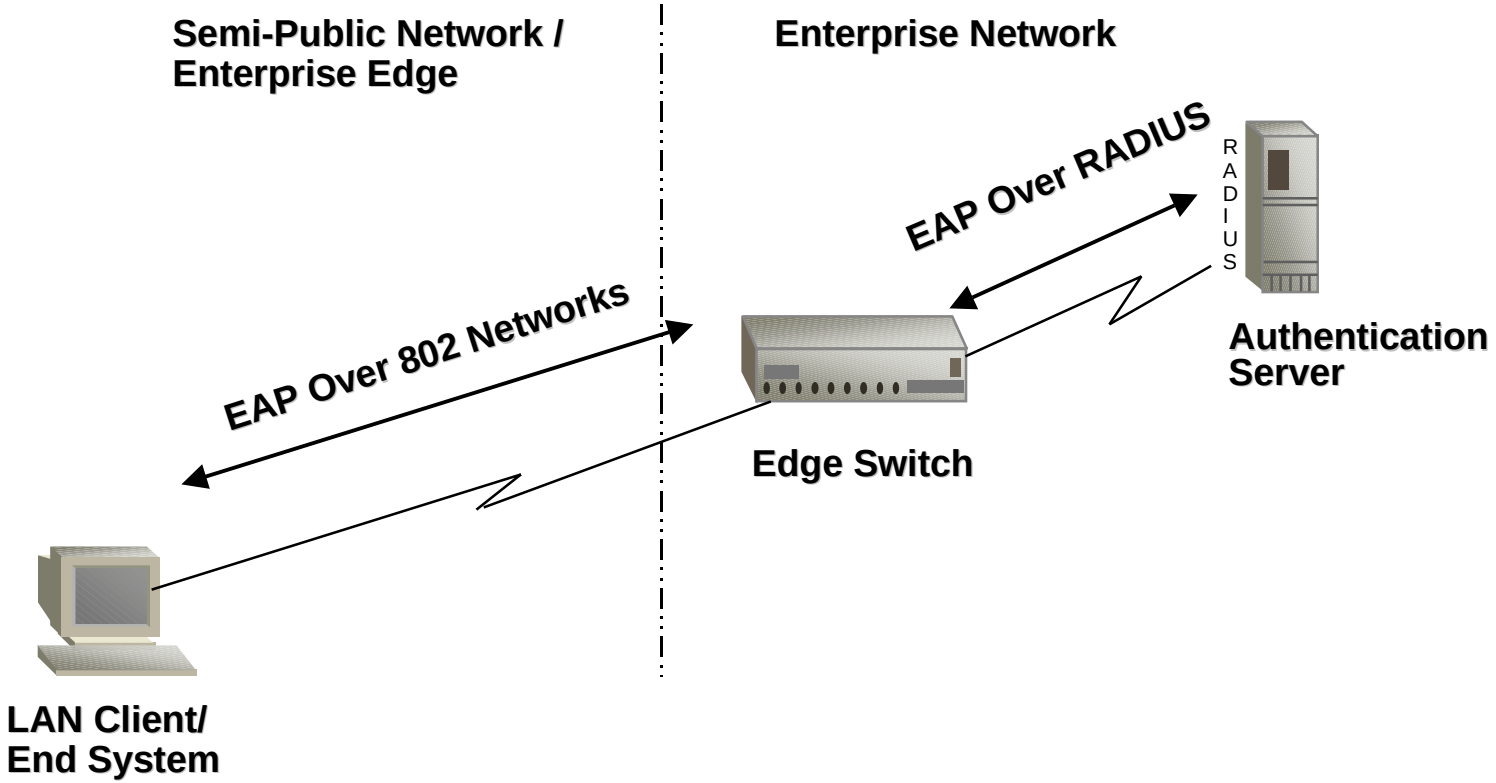
# Port Based Network Login

EAP Over Ethernet
Overview

# Overview

- Method for performing authentication of host to obtain access to switched LAN. Occurs at the first point of attachment (i.e. the edge).
- Occurs early in the start-up process. Ideally before DHCP.
- Switch Port remains disabled/blocked until authentication succeeds, at which point it transitions to fowarding state.
- Ageing and re-authentication by switch may be supported, but port remains fowarding unless re-authentication fails.
- Authentication should be a per-port control. Some ports will not run the authentication protocol (e.g. uplinks).
- Client OS should couple with log on/logoff mechanisms

# General Topology



# Why Edge Authentication

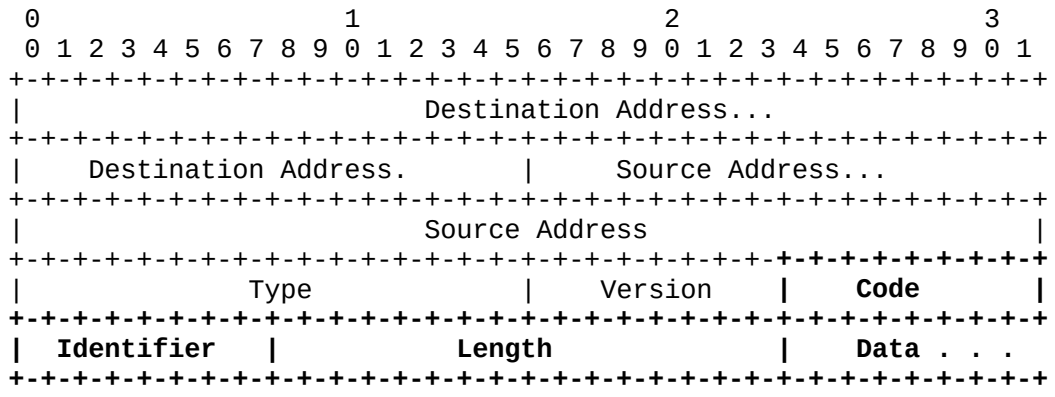
Instead of in the core of the network

- Better security - fewer points of attack
- Simplicity - simple topology considerations.
- Scalability - manage port state not FDB entries.
- Availability - Core switch failover is transparent and edge switch failure only impacts small set of clients.
- No Media Translation - no issues converting PDU formats.
- Minimal Multicast Propagation - no downstream switches

# Protocol Overview

- Encapsulate the Extensible Authentication Protocol (RFC 2284) in Ethernet Frames (EAPOE).
- EAP is a general protocol supporting multiple authentication methods (smart cards, Kerberous, public key, one-time password, etc).
- Switch relays authentication exchanges between client and ‘back-end’ authentication server.
- Switch controls port forwarding state based upon the result of the authentication exchanges.

# EAPOE Frame Format



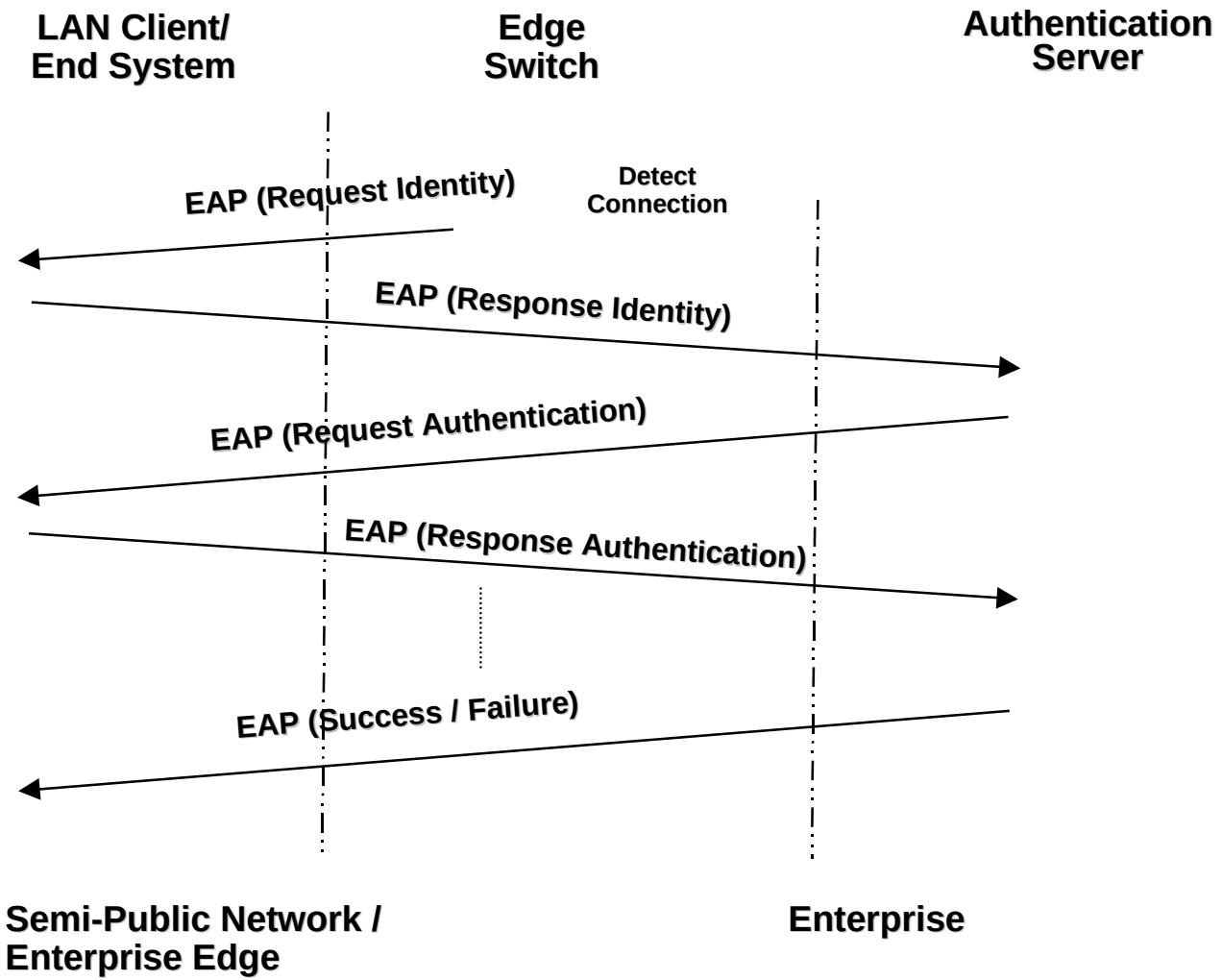

Some Interesting Fields

DA - multicast (perhaps in BPDU range)
Type - new Ethertype
Version - current version number of EAPOE protocol
Code - type of EAP packet (req, resp, success, failure)
Identifier - random value to identify exchange session
Length - size of EAP packet (includes Code, ID, Len, and Data)
Data - zero or more code dependent octets, up to max PDU.

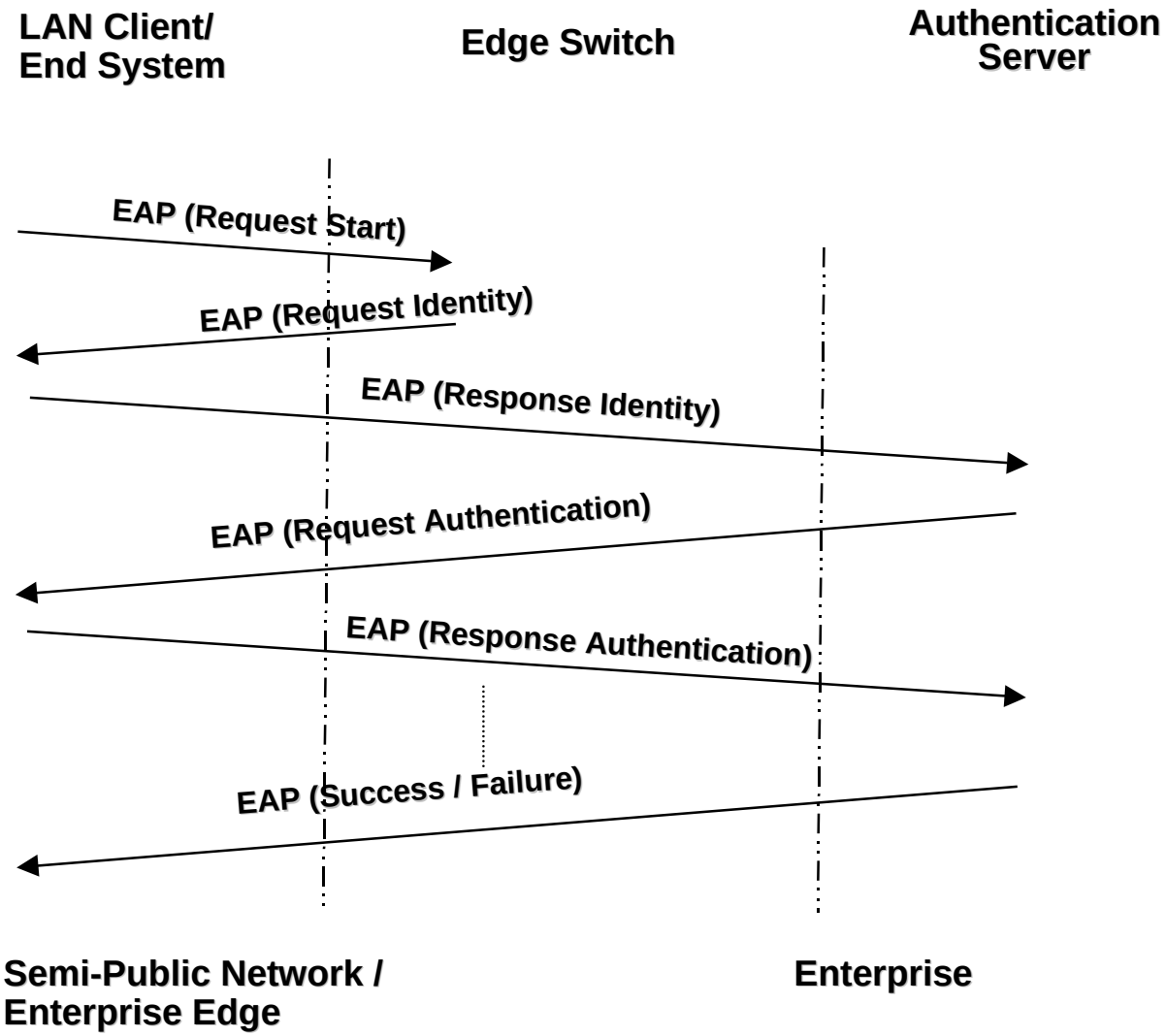
# Protocol Operation

- Initiated by Client or Switch. Switch initiates on ‘port up’ indication. Client initiates at boot-up and/or login.
- Switch always requests identity. Client requests switch initiate identity request.
- Use exponential backoff if responses are not received. Switch responsible for retransmissions.
- If identity is known, may use unicast DA else use multicast DA. (However, issues ever using unicast DA).

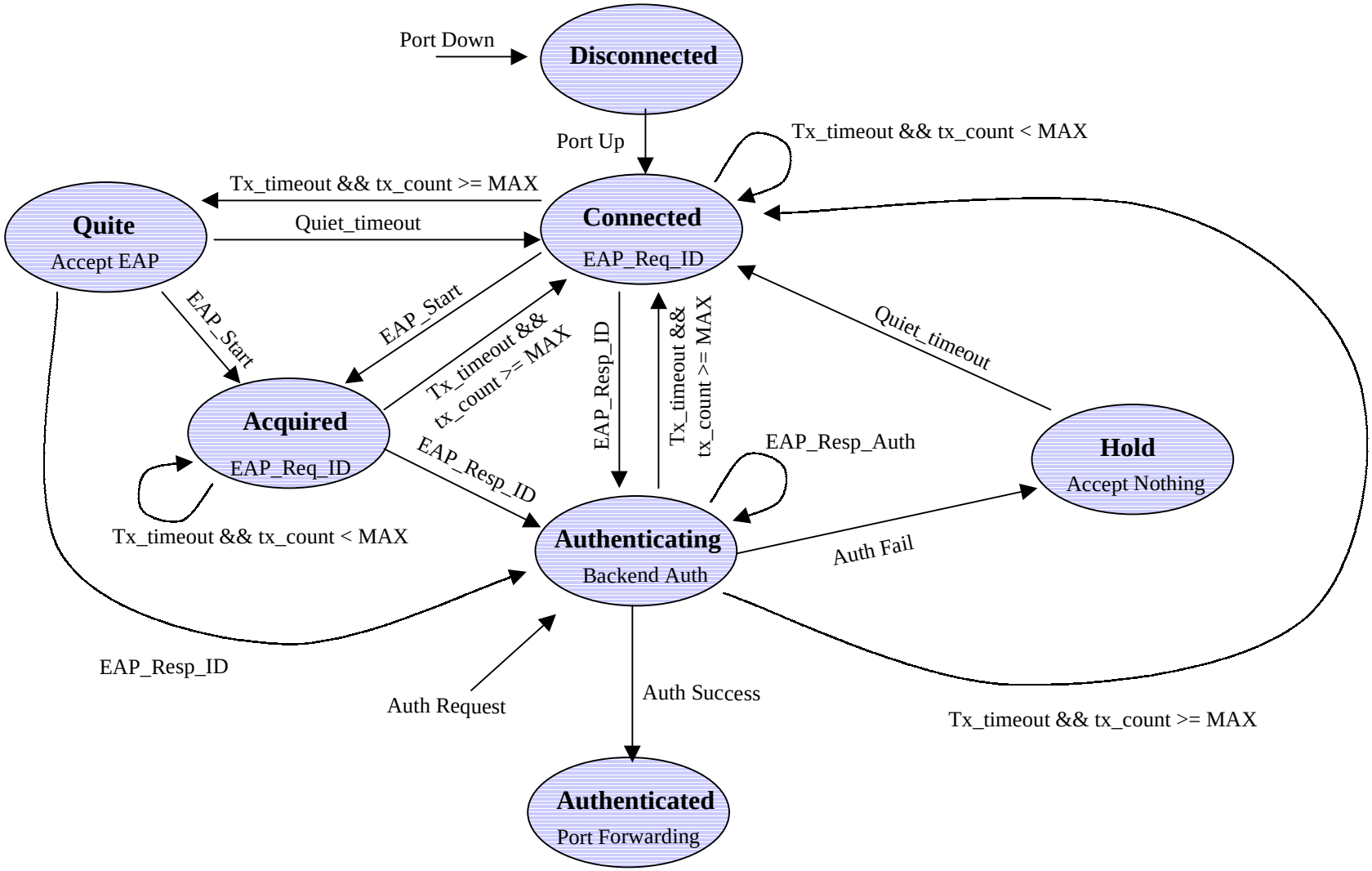
# Switch Initiation



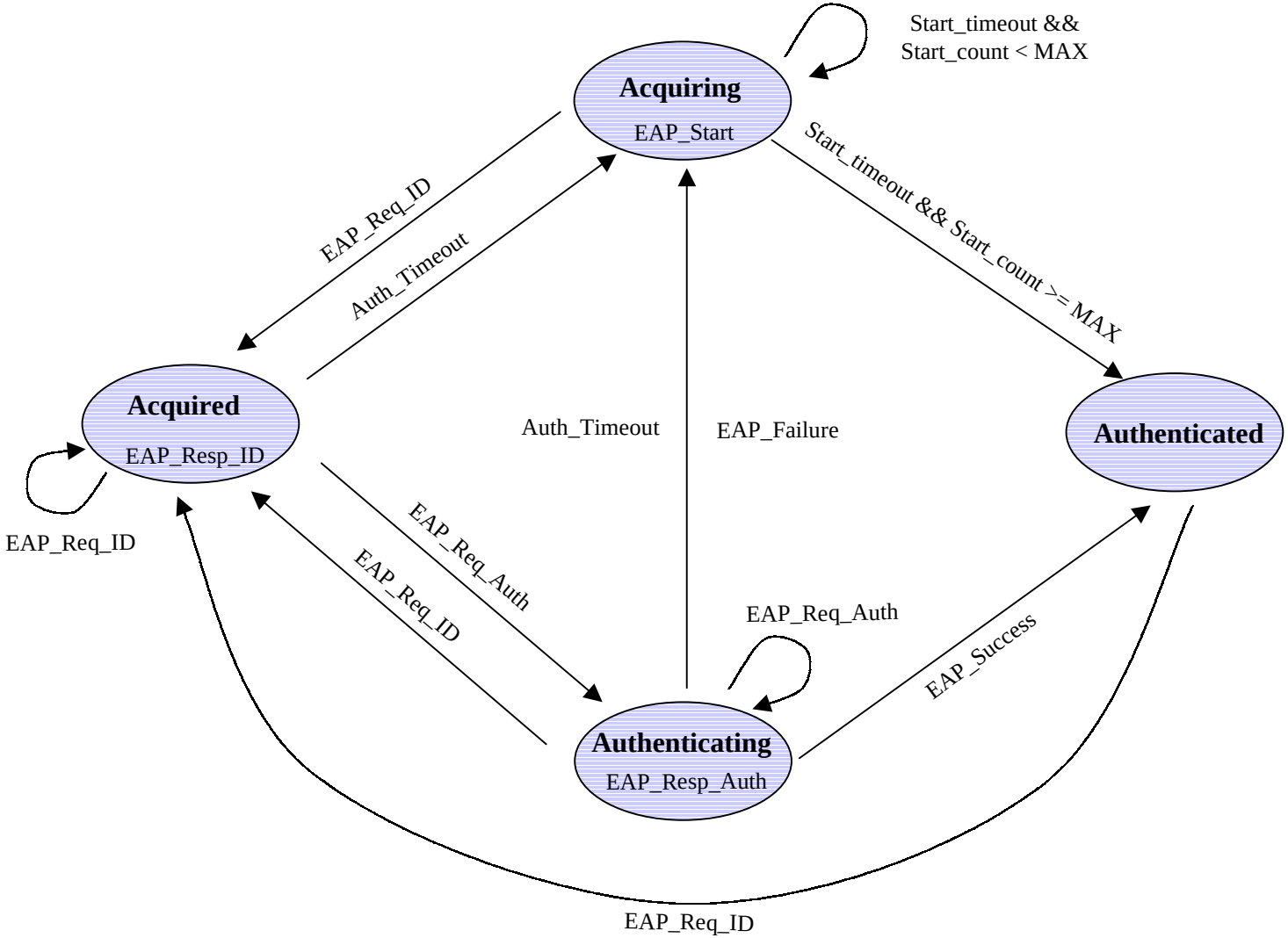
# Client Initiation



# Switch Statemachine



# Client Statemachine



# 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