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/block blocked until authentication succeeds, at which point it transitions to forwarding state.
- Ageing and re-authentication by switch may be supported, but port remains forwarding 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

Semi-Public Network / Enterprise Edge

Enterprise Network

EAP Over 802 Networks

EAP Over RADIUS

Authentication Server

LAN Client/ End System

Edge Switch
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

<table>
<thead>
<tr>
<th>0 1 2 3</th>
<th>4 5 6 7</th>
<th>8 9 0</th>
<th>1 2 3 4</th>
<th>5 6 7 8</th>
<th>9 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Destination Address...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Destination Address.</td>
<td>Source Address...</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Source Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Type</td>
<td>Version</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Identifier</td>
<td>Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>+---------+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 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

LAN Client/End System  Edge Switch  Authentication Server

EAP (Request Identity)  Detect Connection  EAP (Response Identity)

EAP (Request Authentication)

EAP (Response Authentication)

EAP (Success/Failure)

Semi-Public Network/Enterprise Edge  Enterprise
Client Initiation

LAN Client/End System  Edge Switch  Authentication Server

EAP (Request Start)  
EAP (Request Identity)  
EAP (Response Identity)  
EAP (Request Authentication)  
EAP (Response Authentication)  
EAP (Success/Failure)  

Semi-Public Network/Enterprise Edge  Enterprise
Client Statemachine

Acquiring
EAP_Start

Acquired
EAP_Resp_ID

Authenticating
EAP_Resp_Auth

Authenticated
EAP_Resp_ID

Start_timeout &&
Start_count < MAX

Start_timeout &&
Start_count >= MAX

EAP_Req_ID

Auth_Timeout

EAP_Req_ID

Auth_Timeout

Auth_Timeout

EAP_Req_Auth

EAP_Req_Auth

EAP_Req_ID

EAP_Success

EAP_Failure

EAP_Req_ID

EAP_Req_ID
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