IEEE 802.1X

**802.1X Header**

<table>
<thead>
<tr>
<th>Version</th>
<th>Type</th>
<th>Length</th>
<th>EAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**EAP Header**

<table>
<thead>
<tr>
<th>Code</th>
<th>Identifier</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**EAP Flow Chart**

Supplicant → Authenticator → Authentication Server

- Identity Request
- Identity Response
- Challenge Request
- Challenge Response
- Success
- Access Request → Access Challenge → Access Accept

**Configuration**

### Global Configuration
- Define a RADIUS server
- radius-server host 10.0.0.100
- radius-server key MyRadiusKey
- Configure 802.1X to authenticate via AAA
- aaa new-model
- aaa authentication dot1x default group radius
- Enable 802.1X authentication globally
- dot1x system-auth-control

### Interface Configuration
- Static access mode
- switchport mode access
- Enable 802.1X authentication per port
- dot1x port-control auto
- Configure host mode (single or multi)
- dot1x host-mode single-host
- Configure maximum authentication attempts
- dot1x max-reauthREQ
- Enable periodic reauthentication
- dot1x reauthentication
- Configure a guest VLAN
- dot1x guest-vlan 123
- Configure a restricted VLAN
- dot1x auth-fail vlan 456
- dot1x auth-fail max-attempts 3

**Terminology**

**Extensible Authentication Protocol (EAP)**
A flexible authentication framework defined in RFC 3748

**EAP Over LANs (EAPOL)**
EAP encapsulated by 802.1X for transport across LANs

**Supplicant**
The device (client) attached to an access link that requests authentication by the authenticator

**Authenticator**
The device that controls the status of a link; typically a wired switch or wireless access point

**Authentication Server**
A backend server which authenticates the credentials provided by supplicants (for example, a RADIUS server)

**Guest VLAN**
Fallback VLAN for clients not 802.1X-capable

**Restricted VLAN**
Fallback VLAN for clients which fail authentication

**802.1X Packet Types**

<table>
<thead>
<tr>
<th>Code</th>
<th>Type</th>
<th>Length</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>EAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>EAPOL-Start</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>EAPOL-Logoff</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>EAPOL-Key</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EAPOL-Encap-ASF-Alert</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EAP Codes**

| 1    | Request |
| 2    | Response |
| 3    | Success |
| 4    | Failure |

**EAP Req/Resp Types**

| 1 | Identity |
| 2 | Notification |
| 3 | Nak |
| 4 | MD5 Challenge |
| 5 | One Time Password |
| 6 | Generic Token Card |
| 254 | Expanded Types |
| 255 | Experimental |

**Interface Defaults**

- Max Auth Requests: 2
- Reauthentication: Off
- Quiet Period: 60s
- Reauth Period: 1hr
- Server Timeout: 30s
- Supplicant Timeout: 30s
- Tx Period: 30s

**Port-Control Options**

- **force-authorized**
  Port will always remain in authorized state (default)
- **force-unauthorized**
  Always unauthorized; authentication attempts are ignored
- **auto**
  Supplicants must authenticate to gain access

**Troubleshooting**

- show dot1x [statistics] [interface <interface>]
- dot1x test eapol-capable [interface <interface>]
- dot1x re-authenticate interface <interface>