

# 802.1X

Port-Based Network Authentication

Ronny Haryanto  
[ronny@haryan.to](mailto:ronny@haryan.to)  
October 2004

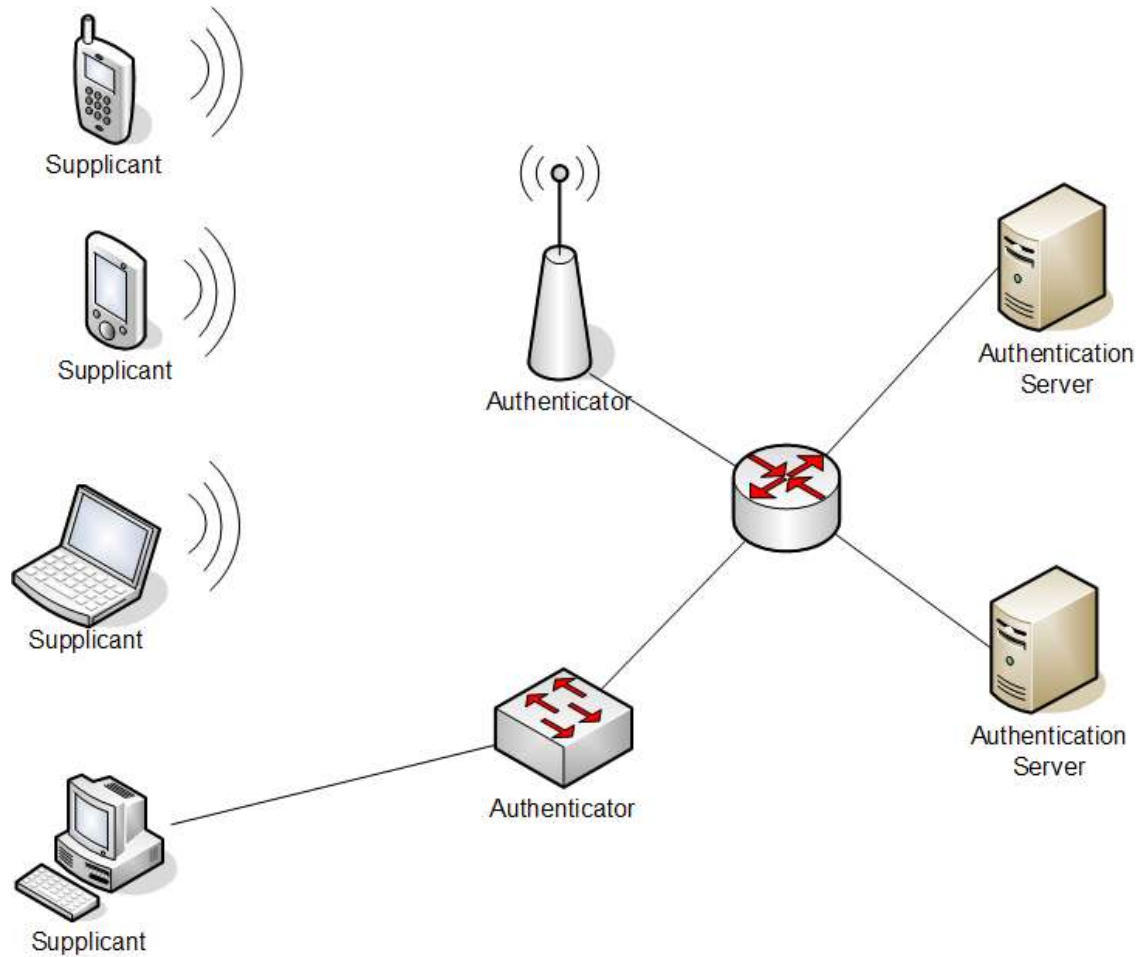
# Port-Based Authentication

- Old ways:
  - MAC address based
  - Shared key (e.g. WEP, password)
  - Higher level (e.g. VPN)
  - Open but monitor
- Problems:
  - Manageability
  - Scalability
  - Security, AAA

# 802.1X

- Layer 2
- Authentication only
  - But some provide keying material
- Originally designed for Wired LANs, before 802.11 wireless
- EAP: modular and extensible
- Scalable: 3-tier design

# 802.1X Components

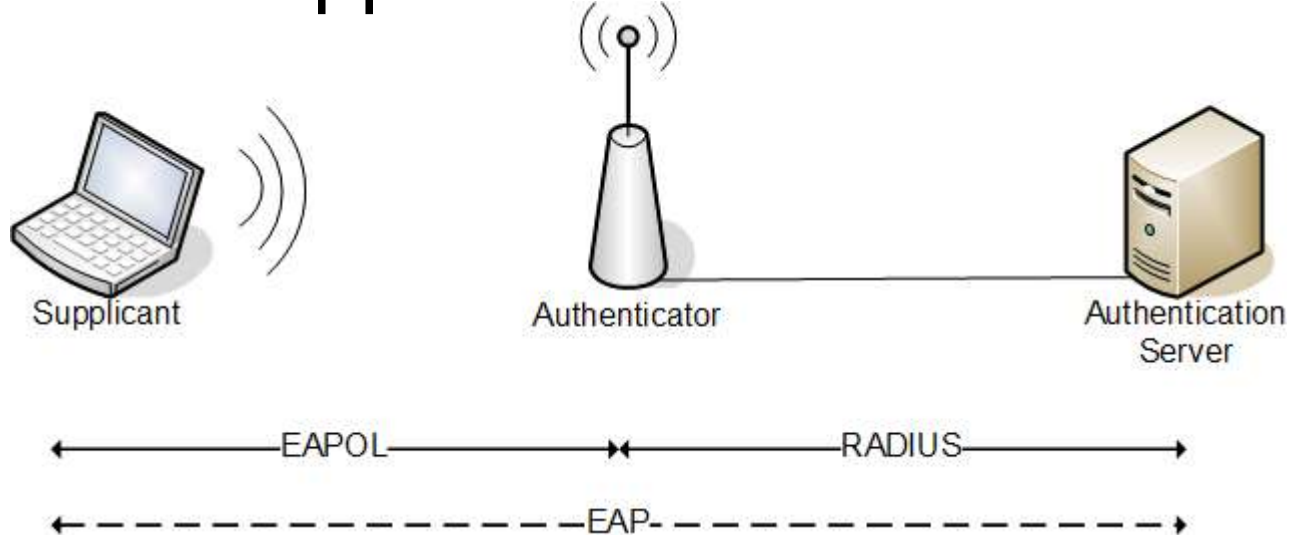


# EAP and EAPOL

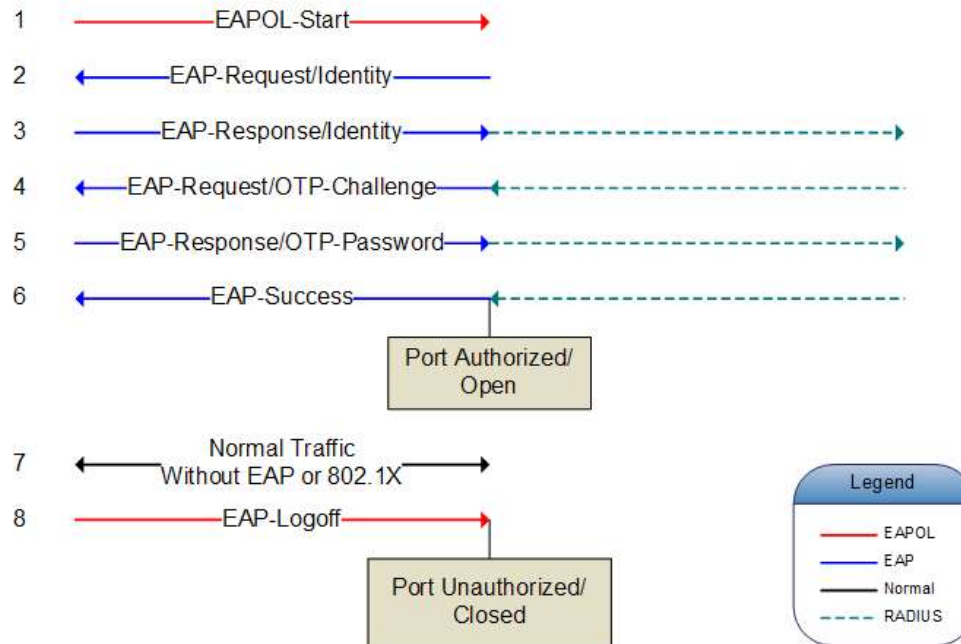
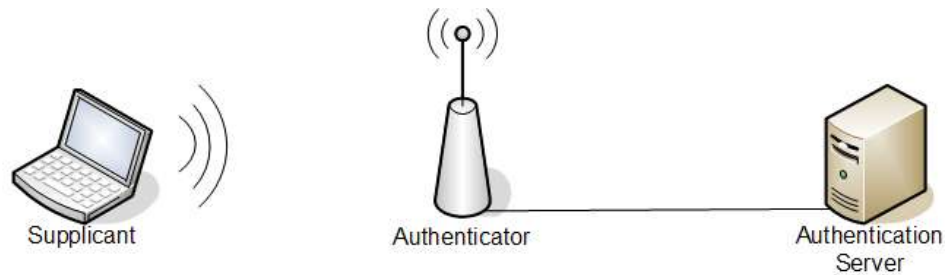
- Extensible Authentication Protocol
  - Originally for PPP (normally dial-ups); RFC 2284.
  - Authentication mechanisms: MD5, passwords (OTP), generic token card,
- EAP over LANs
  - Layer 2 wrapper for EAP
  - No PPP stuff

# EAP and EAPOL (cont'd)

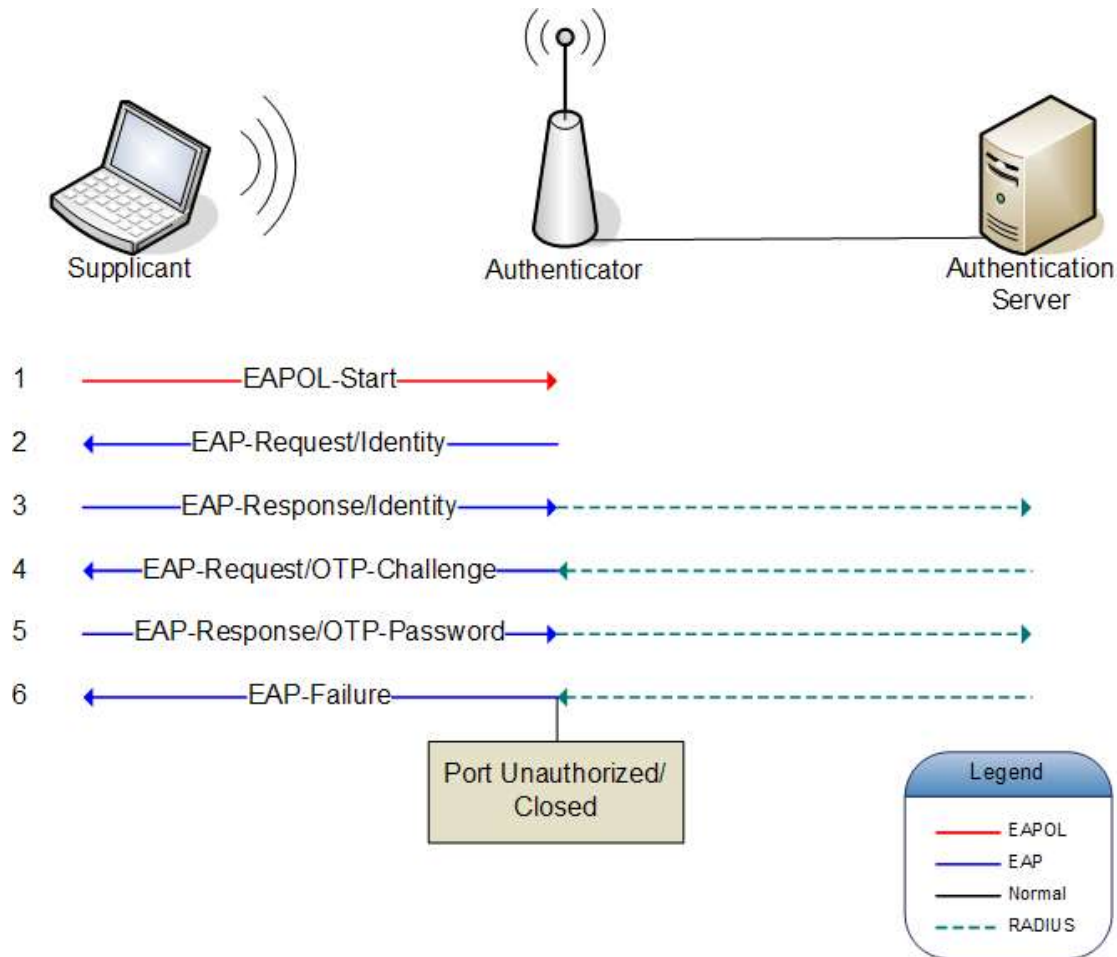
- Authenticator acts as proxy; real auth between supplicant and auth server



# How 802.1X Works



# How 802.1X Works (cont'd)



# EAP Types

- **EAP-MD5**: Challenge-Handshake
- **LEAP**: MD5 based with improvements
- **EAP-TLS**: requires server and client certs
- **EAP-TTLS**: tunneled TLS, can do old auth mechanisms
- **PEAP**: similar to TTLS, but EAP only
- Others: EAP-FAST, SIM, SecureID, AKA

# Flaws and Solutions

- Mishra and Arbaugh paper
- Lack of **Mutual Authentication**
- **Session Hijacking** (for wireless)
- Other minor problems:
  - Roaming
  - Single point of failure: auth server
- Solutions:
  - Mutual Auth (LEAP, EAP-(T)TLS, PEAP)
  - Dynamic Keying, Per-packet Keying
  - Message Integrity Checking
  - 802.11i for wireless-related issues

# Conclusion

- Originally for wired LANs, now more popular for 802.11 wireless
- 802.1X is part of 802.11i
- Available now, supported by many vendors
- Pick the right EAP type

# Q & A

- Paper available from:  
<http://ronny.haryan.to/files/802.1x.pdf>