
802.1x

ACSAC 2002 – Las Vegas
Jeff.Hayes@alcatel.com

802.1 Projects

The IEEE 802.1 Working Group is chartered to concern itself with and develop standards and recommended practices in the following areas: 802 LAN/MAN architecture, internetworking among 802 LANs, MANs and other wide area networks, 802 overall network management, and protocol layers above the MAC & LLC layers.

ID	Key Projects (status)
802	Overview and Architecture (published)
802.1D	MAC Bridges (published:1998)
802.1G	Remote MAC Bridging (published)
802.1p	Traffic Class Expediting & Dynamic Multicast Filtering (pub)
802.1Q	Virtual LANs (published)
802.1s	Multiple Spanning Trees (draft)
802.1v	VLAN Classification by Protocol and Port (published)
802.1w	Rapid Reconfiguration (Published)
802.1x	Port-Based Network Access Control (published)

802.1x Overview

> IEEE standard

- Initial goal: control access to LAN through an authentication process
 - Implemented at the LAN switch port
 - Port Closed → Authentication → Port Open
 - Driven by LAN switch vendors and Microsoft
- Extended to work with wireless LAN access
 - Implemented on 802.11 access points
- Evolved to be the preferred method to securely access LANs
 - Key to WLAN security
- Layer 2 / MAC protocol
 - Not for WAN access or remote access control solution
- Supports security-in depth
 - Edge-base/Layer 2 security; supplements layer 3-4 and appl security

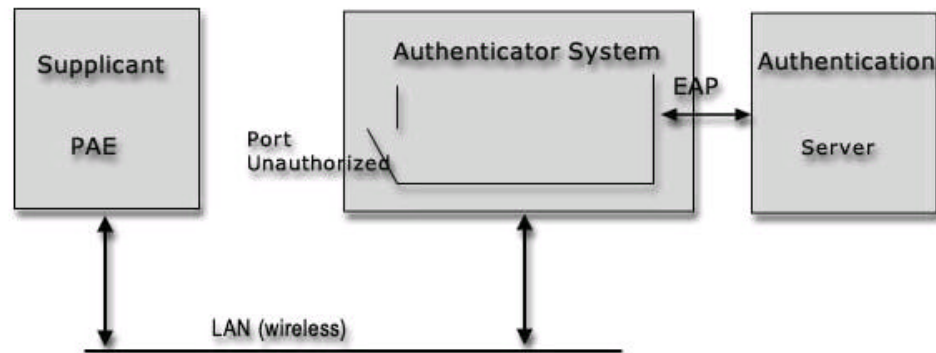
802.1x Overview

> Leverages key technologies

- EAP over Ethernet and wireless
- Works over standard LAN protocols
 - LAN switches (standard IEEE 802 media, including Ethernet)
 - Access Points (802.11 wireless LANs)
- Does not specify an authentication systems but will work with most
 - RADIUS
 - TACACS+
 - Hardware tokens
 - X.509 certificates
 - Kerberos

> Key components

- Supplicant
- Authenticator
- Authentication server

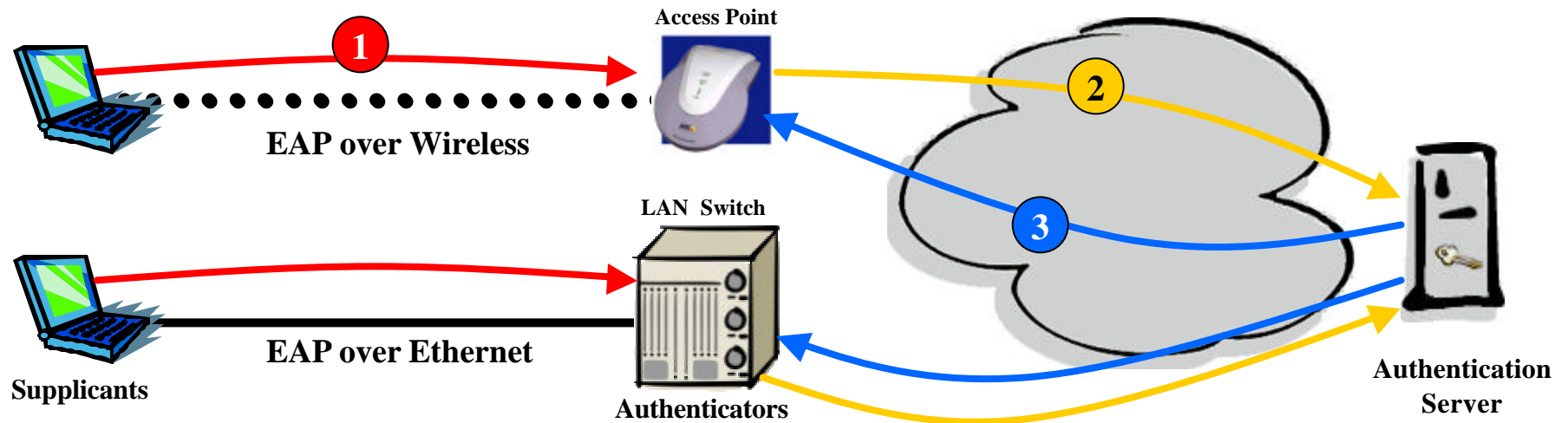


Extensible Authentication Protocol

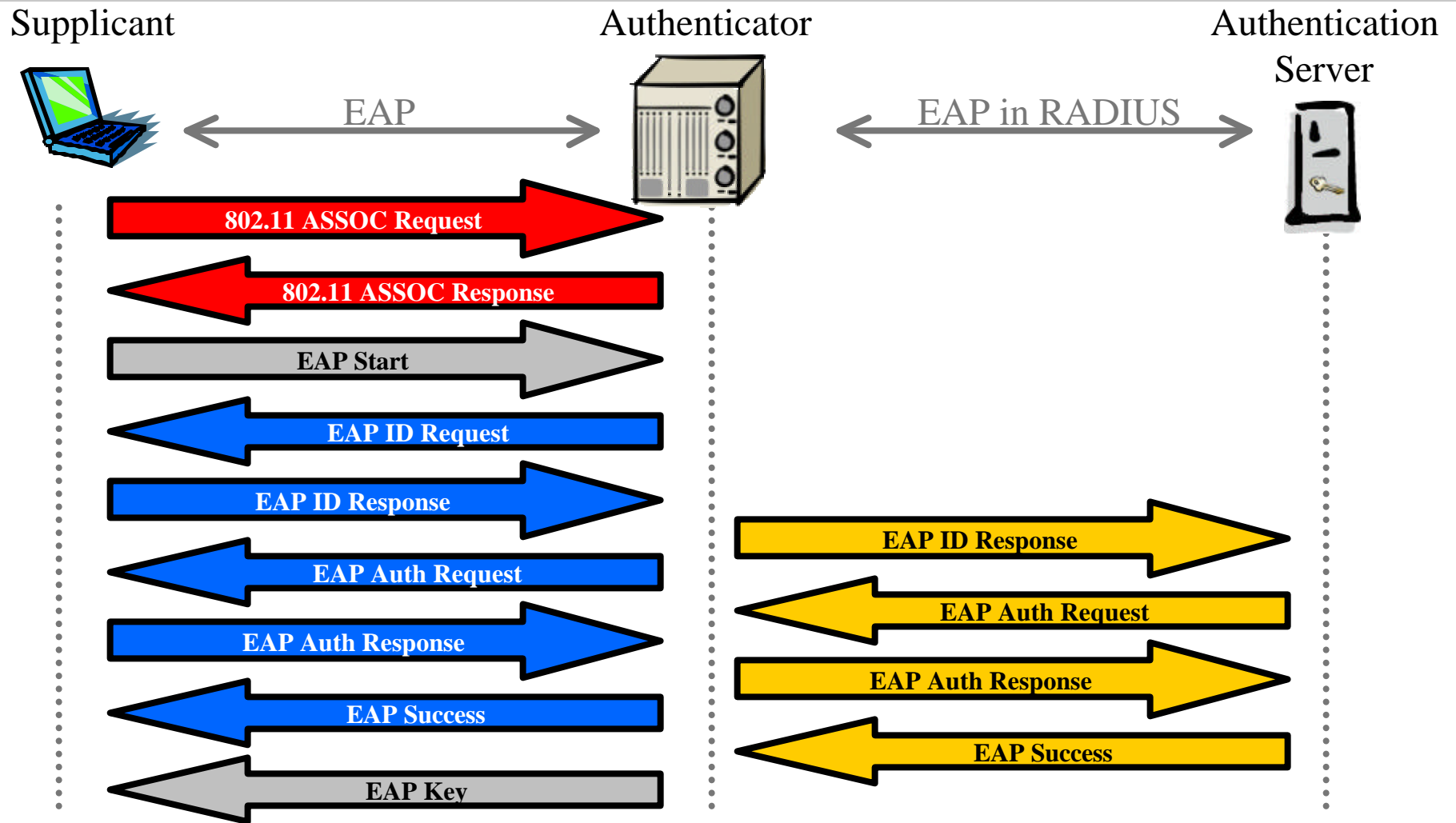
- > EAP is an extension to PPP (RFC 2284; update underway)
- > EAP methods
 - MD5 - basic
 - Transparent LAN Service (TLS) - Windows XP
 - Requires and digital certificate on each supplicant (see RFC 2716)
 - Tunneled TLS Authentication Protocol (TTLS) - Funk Software
 - TTLS does not require digital cert (see Internet Draft)
 - LEAP - Cisco
 - Lightweight EAP (proprietary); Cisco moving to PEAP
 - PEAP – Microsoft & Cisco
 - Protected EAP (proprietary); compromised standard; more secure than LEAP
- > Same EAP on the client device and authentication server
 - Clients = Microsoft XP, Funk Odyssey, and Meetinghouse's AEGIS
 - Servers = RADIUS

Basic Operation

- 1** User makes an authentication/logon request
 - Must have client software on Supplicant (aka - Port Access Entity)
 - AP or switch port starts in un-authenticated mode
- 2** Authentication request between Supplicant and Authentication Server facilitated by Authenticator
- 3** Authentication Server grants or denies access (authorization)



802.1x Message Exchanges



802.1x Issues – WLAN Security

- > Underlying privacy is based on WEP
 - Known security issues; addressed by RADIUS vendors, IEEE and Wi-Fi Alliance
- > RADIUS server authenticates 802.1x supplicant
 - RADIUS server supplies a unique key for that users session
 - One key per session as opposed to WEPs shared key
- > Wi-Fi Alliance extended RC4 with rapid re-keying
 - New agreement called Wi-Fi Protect Access (WPA)
 - APs starting to ship
- > IEEE 802.11i
 - Requires new chips
 - Deployments beginning in late 2003 and into 2004

Wireless Security Issues and Evolution

- > Wired Equivalent Privacy (WEP)
 - Encryption between client and AP
 - “Good-enough” security for most
 - WEP is breakable but some simple procedures minimize vulnerabilities

	WEP (RC4)	TKIP (RC4)	AES-based
Key Size	40 or 104 bits	128 bits	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV (CCMP)
Packet Key	Concat.	TKIP KDF	Not Needed
Integrity			
Data	CRC-32	Michael	Part of Mode*
Header	None	Michael	Part of Mode**
Replay	None	Use IV	Use IV
Key Mgmt	None	EAP-based	EAP-based

* AES-OCB, or AES-CBC-MAC for CCMP

- > Wi-Fi Protected Access (WPA)
 - Wi-Fi Alliance and IEEE effort to bring enhanced and interoperable Wi-Fi security to market
 - Derived from and forward-compatible with 802.11i
 - Designed to run on existing hardware as a software upgrade
 - Key security enhancements
 - Enhanced encryption through Temporal Key Integrity Protocol (TKIP)
 - User authentication via 802.1x and EAP
 - Key hierarchy & mgmt, BSS, cipher/authentication negotiation
- > 802.11i
 - IEEE standard; AES support; requires new hardware due to AES chips

802.1x Issues

- > New standard – critical deployment mass not achieved
 - Client support not ubiquitous
 - Being part of Operating System is ideal – only XP today
 - Not yet supported on Linux, Sun, other Unix, PDAs, MAC operating systems
 - 3rd party applications available – Funk and Meetinghouse – but must purchase
 - What about visitors, contractors, temps?
 - LAN switches and AP beginning to deploy
- > Requires end user involvement via a log-on process
 - Unmanned devices—scanners, printers, servers—not able to participate
- > Proprietary EAP implementations
 - EAP/TLS, LEAP, PEAP TTLS...
 - Requires end-to-end support (Supplicant → Authenticator → Authentication Server)
 - Multi-vendor interoperability is not a given

802.1x Issues – LAN Switch

- > Access is all or nothing ('port on' or 'port off')
 - No provisions for prioritization, bandwidth control or VLAN regulation
 - Spec does not prohibit vendors from addressing this
 - Does not break protocol
 - May impact multi-vendor switch deployments
- > Standard does not address shared media
 - Hub/L2 switch without 802.1x connected to switch with 802.1x is not a supported configuration
 - Cannot support authenticated devices (end users) and non-authenticated devices (printers, servers) on the same port
 - Spec does not prohibit vendors from addressing this by allowing multiple MACs per port
- > Requires additional sign-on/authentication
 - PC log-in, Layer 2 log-in, Domain/NDS log-in, firewall/ACL authentication, application authentication

802.1x Issues – WLAN

- > Underlying privacy is based on RC4 with rapid re-keying
 - WPA / TKIP requires extensions to APs
 - Better have a maintenance contract or be prepared to pay
- > Not all AP capable of supporting security beyond WEP
 - WPA is a firmware upgrade for most
 - Installed base of APs may require forklift upgrades
 - 802.11i is a hardware upgrade
 - Installed base of APs will require forklift upgrades

Resources

- > IEEE 802 LAN/MAN Standards Committee
 - <http://grouper.ieee.org/groups/802/>
- > 802.1 working group home page
 - <http://grouper.ieee.org/groups/802/1/index.html>
- > 802.1x documents / drafts
 - <http://grouper.ieee.org/groups/802/1/index.html>
- > IETF Documents
 - IEEE 802.1X RADIUS Usage Guidelines
 - <http://www.ietf.org/internet-drafts/draft-congdon-radius-8021x-03.txt>
 - EAP-TLS - RFC 2716
 - <ftp://ftp.rfc-editor.org/in-notes/rfc2716.txt>
 - EAP-TTLS
 - <http://www.ietf.cnri.reston.va.us/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt>
- > Open Source Implementation of IEEE 802.1x
 - <http://www.open1x.org/>