Authentication, Authorization, Accounting (AAA)

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

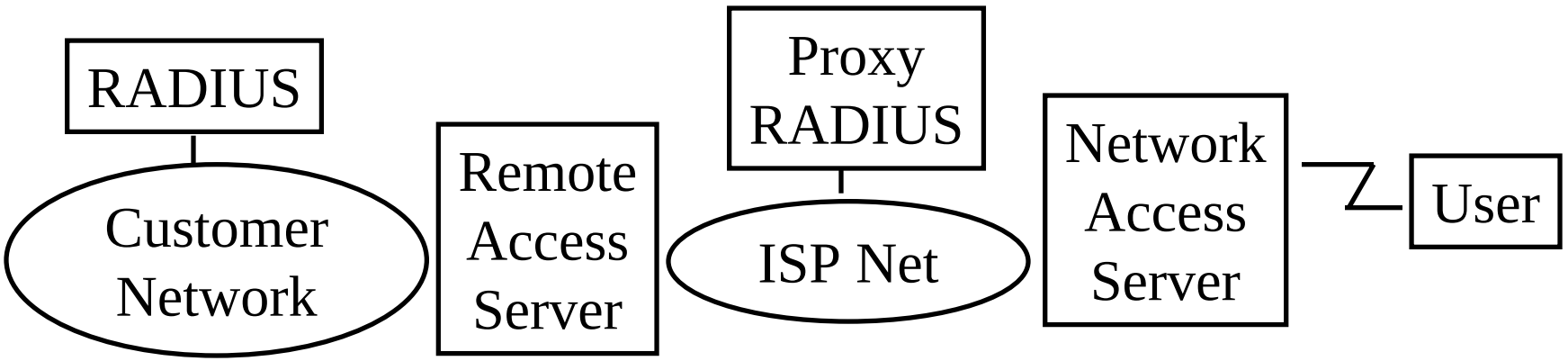
Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-09/

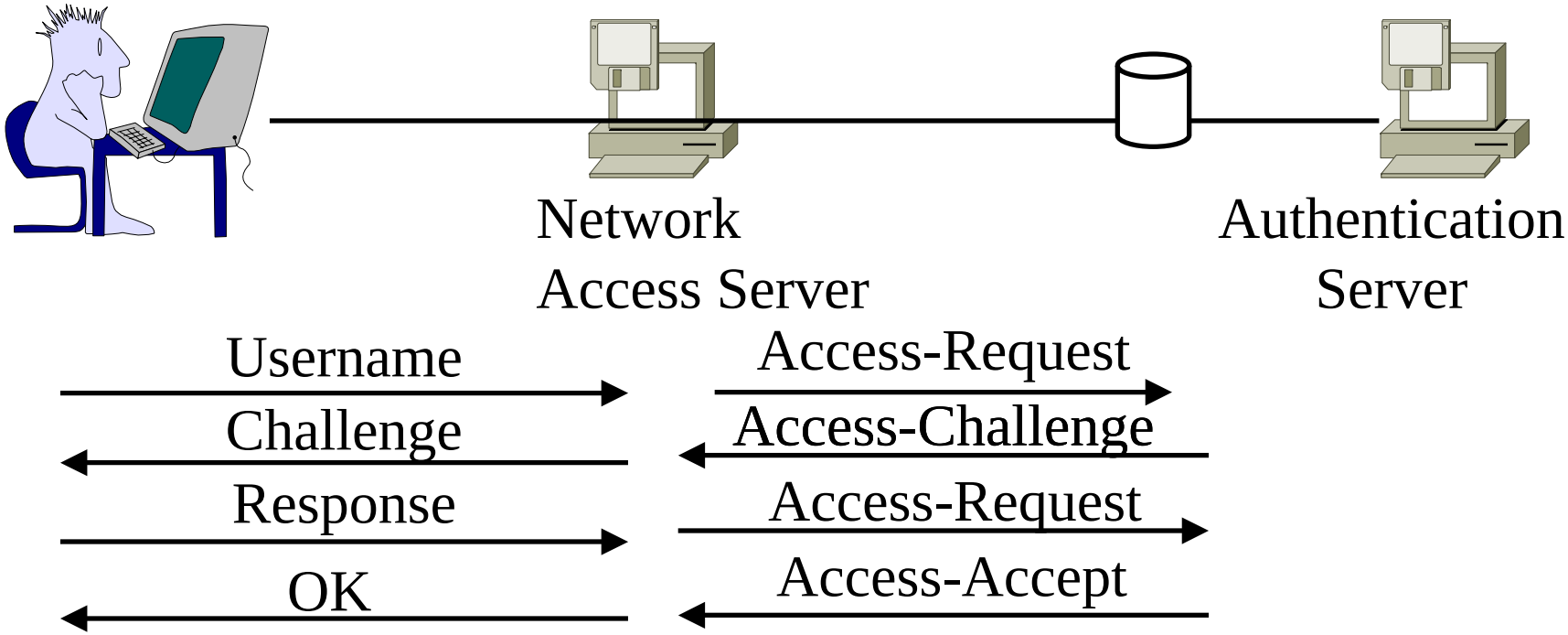
- RADIUS
- Authentication Protocols: PAP, CHAP, MS-CHAP
- Extensible Authentication Protocol (EAP)
- EAP Upper Layer Protocols
- 802.1X

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ AAA server
- Network Access servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application level retransmission required
  - TCP takes to long to indicate failure



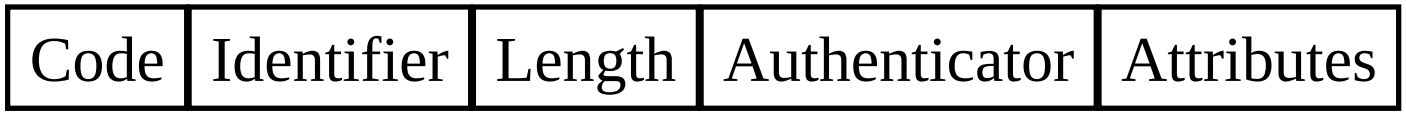
RADIUS Messages



- Four Core Messages: Request, Challenge, Accept, Reject.
- Message Format: Code is the message type.
  Identifier is used to match request/response.

Code	Identifier	Length	Authenticator	Attributes

RADIUS Packet Format



Codes:

1 = Access Request

2 = Access Accept

3 = Access Reject

4 = Accounting request

5 = Accounting Response

11 = Access Challenge

12 = Server Status (experimental)

13 = Client Status (Experimental)

255 = Reserved

RADIUS Accounting

- RFC 2866, June 2000
- Client sends to the server:
  - Accounting Start Packet at service beginning
  - Accounting Stop Packet at end
- All packets are acked by the server
- Packet format same as in authentication

RADIUS Server Implementations

Public domain software implementations:

- FreeRADIUS
- GNU RADIUS
- JRadius
- OpenRADIUS
- Cistron RADIUS
- BSDRadius
- TekRADIUS

Problems with RADIUS

- Does not define standard failover mechanism
  $\Rightarrow$ varying implementations
- Original RADIUS defines integrity only for response packets
- RADIUS extensions define integrity for EAP sessions
- Does not support per-packet confidentiality
- Billing replay protection is assumed in server.
  Not provided by protocol.
- IPsec is optional
- Runs on UDP $\Rightarrow$ Reliability varies between implementation.
  Billing packet loss may result in revenue loss.
- RADIUS does not define expected behavior for proxies, redirects, and relays $\Rightarrow$ No standard for proxy chaining

Problems with RADIUS (Cont)

- Does not allow server initiated messages
  ⇒ No On-demand authentication and unsolicited disconnect
- Does not define data object security mechanism
  ⇒ Untrusted proxies can modify attributes
- Does not support error messages
- Does not support capability negotiation
- No mandatory/non-mandatory flag for attributes
- Servers name/address should be manually configured in clients ⇒ Administrative burden
  ⇒ Temptation to reuse shared secrets

Diameter Base Protocol

- Enhanced RADIUS. Light weight.
- Can use UDP, TCP, SCTP (Stream Control Transmission Protocol)
- PDU format incompatible with RADIUS
- Can co-exist with RADIUS in the same network
- Defines standard failover algorithm
- Supports:
  - Delivery of attribute-value pairs (AVPs)
  - Capability negotiation
  - Error notification
  - Ability to add new commands and AVPs
  - Discovery of servers via DNS
  - Dynamic session key derivation via TLS

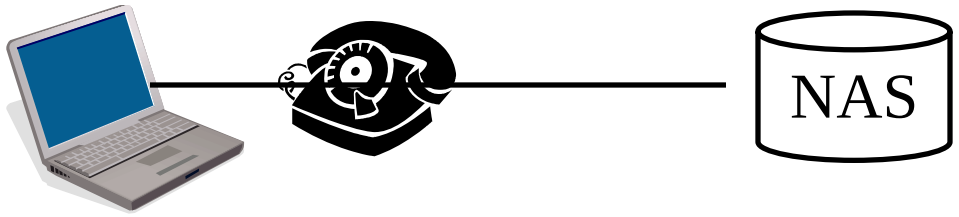
Diameter Base Protocol (Cont)

- All data is delivered in the form of AVPs
- AVPs have mandatory/non-mandatory bit
- Support for vendor specific Attribute-Value-Pairs (AVPs) and commands
- Authentication and privacy for policy messages
- Peer-to-peer protocol ⇒ any node can initiate request.
- Servers can send unsolicited messages to Clients
  ⇒ Increases the set of applications
- Documents: Base, transport profile, applications
- Applications: NAS, Mobile IP, Credit control (pre-paid, post-paid, credit-debit), 3G, EAP, SIP

PAP and CHAP

- Point-to-point protocol (PPP) allows two authentication methods:
  - Password authentication protocol (PAP)
  - Challenge Handshake Authentication Protocol (CHAP) – RFC1994

Password Authentication Protocol (PAP)



- RFC 1334, Oct 1992
- Authenticator sends a authentication request
- Peer responds with a username and password in plain text
- Authenticator sends a success or failure
- Code: 1=Auth Request, 2=Auth Ack, 3=Auth Nak

Code	ID	Len	Name Len	Name Val	Pswd Len	Pswd Val
1B	1B	2B	1B	Var	1B	Var

Code	ID	Len	Success/Failure Message
1B	1B	2B	1B

CHAP

- Challenge Handshake Authentication Protocol
- RFC 1994, August 1996
- Uses a shared secret (password)
- Authenticator sends a challenge
- Peer responds with a MD5 checksum hash of the challenge
- Authenticator also calculates the hash and sends success or failure
- Requires both ends to know the password in plain text
- Replay attack prevention $\Rightarrow$ Use a different challenge every time

MS-CHAP

- Microsoft version of CHAP
- MS-CHAP in RFC 2433, Oct 1998
- Does not require password in plain text
- Uses hash of the password
- 8B challenge ⇒ 24B LM compatible response, 24B NTLM compatible response and 1B use NTLM flag
- LM passwords are limited to 14 case-insensitive OEM characters
- NT passwords are 0 to 256 case-sensitive Unicode characters
- Flag ⇒ NT response is meaningful and should be used
- Also allows users to change password

MS-CHAPv2

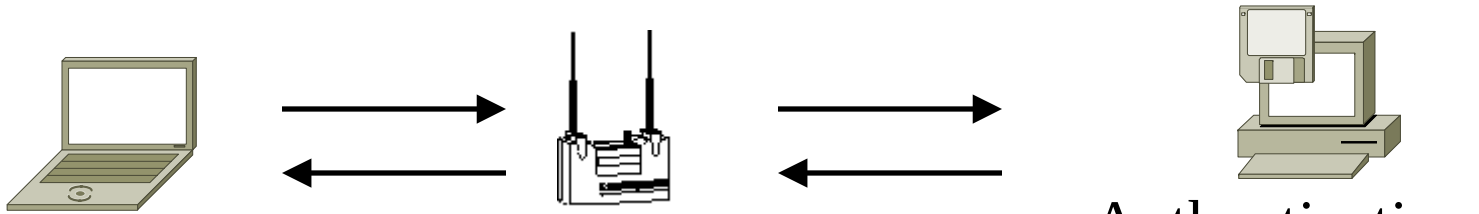
- MS-CHAPv2 in RFC 2759, Jan 2000
- MS-CHAPv2 in Windows 2000 onwards.
- Vista does not support MS-CHAPv1
- LCP option 3 =0x81 $\Rightarrow$ MS-CHAPv2
- V2 provides mutual authentication between peers by piggybacking a peer challenge on the response packet and an authenticator response on the success packet.
- Does not support change password

Extensible Authentication Protocol (EAP)

- Each authentication protocols required a new protocol
  ⇒ Extensible Authentication Protocol
- Initially developed for point-to-point protocol (PPP)
- Allows using many different authentication methods
- Single-Step Protocol ⇒ Only one packet in flight
  ⇒ Duplicate Elimination and retransmission
  Ack/Nak ⇒ Can run over lossy link
- No fragmentation. Individual authentication methods can deal with fragmentation. One frag/round trip ⇒ Many round trips
- Allows using a backend authentication server ⇒ Authenticator does not have to know all the authentication methods
- Can run on any link layer (PPP, 802, ...). Does not require IP.
- Ref: RFC 3748, "EAP," June 2004.

EAP Terminology

- Peer: Entity to be authenticated = Supplicant
- Authenticator: Authenticating entity at network boundary
- Authentication Server: Has authentication database
- EAP server = Authenticator if there is no backend Authentication Server otherwise authentication server
- Master Session Key (MSK)= Keying material agreed by the peer and the EAP server. At least 64B. Generally given by the server to authenticator.

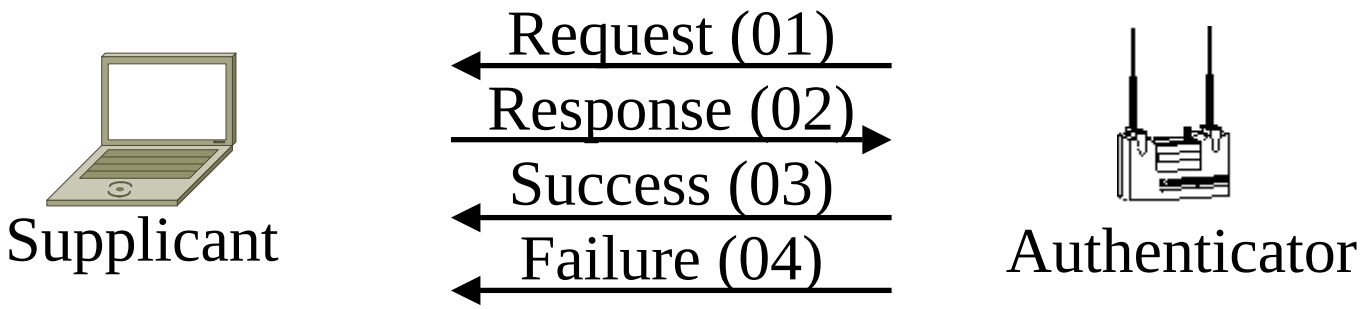


EAP Exchange

- EAP Message Format:

Code	Identifier	Length	Data
8b	8b	16b	

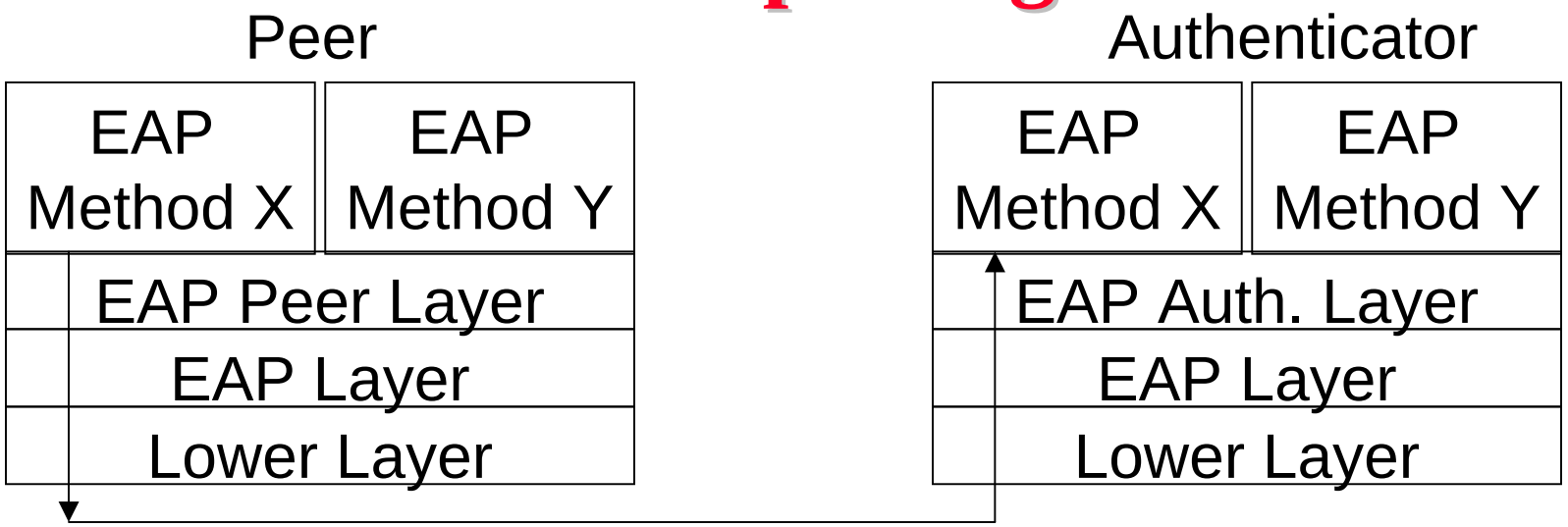
- Only four types of messages:



- Identifier is incremented for each message.
  Identifier in response is set equal to that in request.
- Type field in the request/response indicates the authentication.
  Assigned by Internet Assigned Number Authority (IANA)

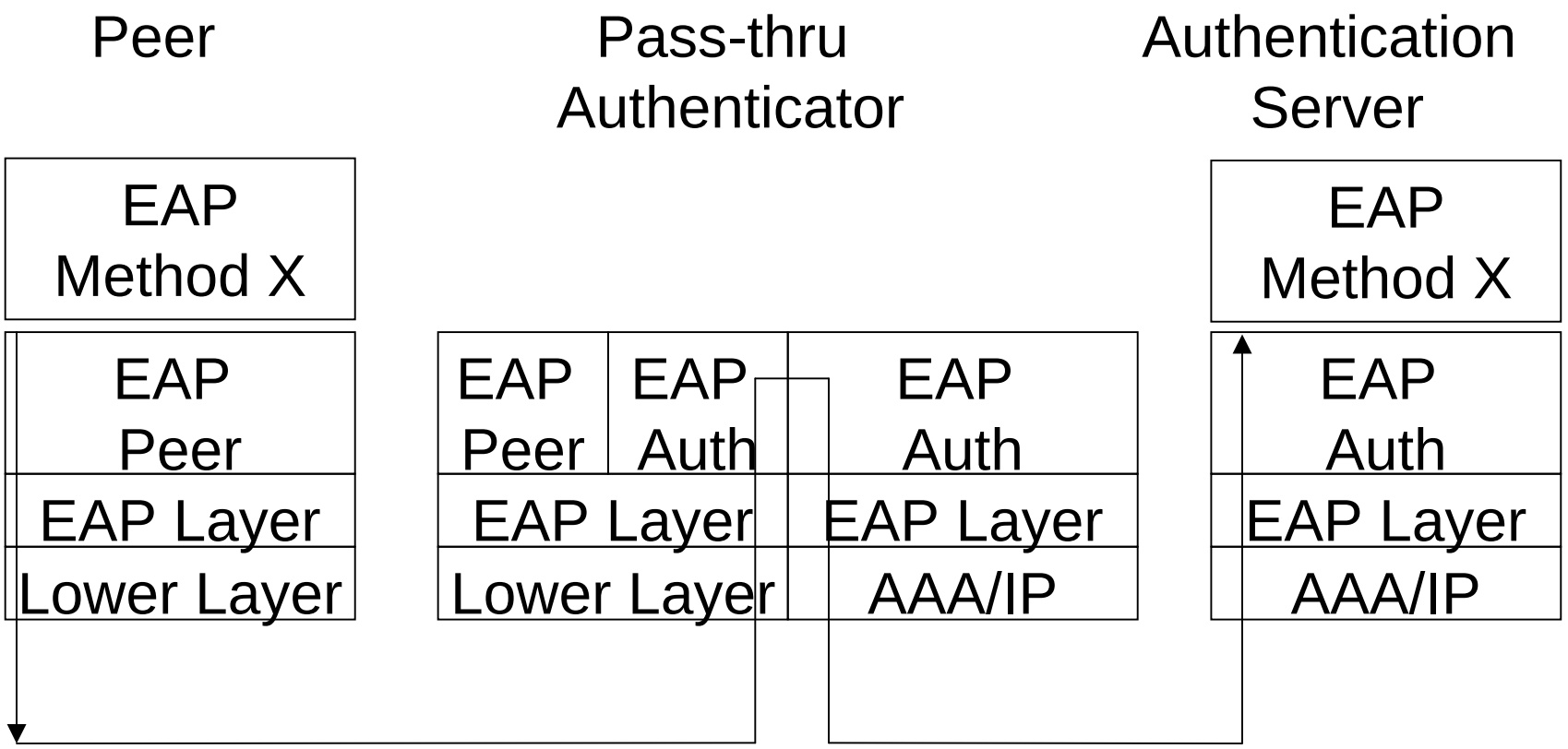
Code	Identifier	Length	**Type**	Data

EAP Multiplexing Model



- Code 1 (request), 3 (success), and 4 (failure) are delivered to the peer layer
- Code 2 (response) is delivered to the EAP authenticator layer.
- Both ends may need to implement peer layer and authenticator layer for mutual authentication
- Lower layer may be unreliable but it must provide error detection (CRC)
- Lower layer should provide MTU of 1020B or greater

EAP Pass through Authenticator



EAP Upper Layer Protocols

- Lightweight EAP (LEAP): Uses MS-CHAP. Not secure.
- EAP-TLS: Transport Level Security. Both sides need certificates
- EAP-TTLS: Tunneled TLS. Only server certificates. Secure tunnel for peer.
- EAP-FAST: Flexible Authentication via Secure Tunneling. Certificates optional. Protected tunnels.
- Protected EAP (PEAP): Server Certificates. Client password.
- PEAPv1 or EAP-GTC: Generic Token Cards. Client uses secure tokens.
- EAP-SIM: Used in GSM. 64b keys.
- EAP-AKA: Authentication and Key Agreement. Used in 3G. 128b keys.
- EAP-PSK: Pre-shared key+AES-128 to generate keys
- EAP-IKEv2: Internet Key Exchange. Mutual authentication. Certificate, Password, or Shared secret

Security Token

- Security Token = Small hardware device carried by users. May store cryptographic keys, biometric data (finger print), PIN entry pad.
- Based on USB, Bluetooth, Cell phones (SMS or Java)
- Use smart cards
- Two-factor authentication = What you have and what you know

[Wikipedia]

One-Time Password

- Three Types:
  1. Use a math algorithm to generate a new password based on previous
  2. Uses time to generate password
     $\Rightarrow$ Synchronized time between server and client
  3. Use a math algorithm to generate a new password based on a challenge from the server and a counter.
- Time synchronized approach allows users to generate password and not use it. The server may compare with the next n passwords to allow for time miss-synchronization.
- Non-time synchronized OTP do not need to be powered all the time $\Rightarrow$ battery lasts long. Have been attacked by phishing. Time-based OTP need to be used right-away.

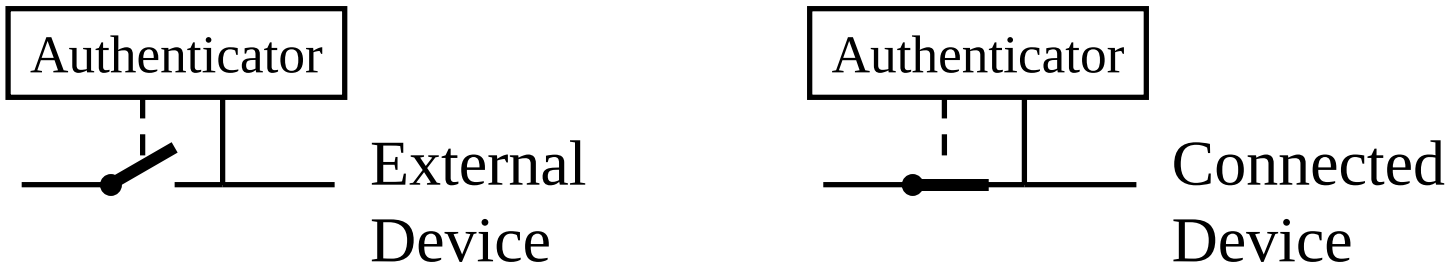
EAP over LAN (EAPOL)

- EAP was designed for Point-to-point line
- IEEE extended it for LANs ⇒ Defines EAPOL
- Added a few more messages and fields
- Five types of EAPOL messages:
  - EAPOL Start: Sent to a multicast address
  - EAPOL Key: Contains encryption and other keys sent by the authenticator to supplicant
  - EAPOL packet: Contains EAP message
  - EAPOL Logoff: Disconnect
  - EAPOL Encapsulated-ASF-Alert: Management alert
- Message Format: Version=1, Type=start,key,…,

Ethernet Header	Version	Type	Packet Body Len	Packet Body

802.1X

- Authentication *framework* for IEEE802 networks
- Supplicant (Client), Authenticator (Access point), Authentication server
- No per packet overhead ⇒ Can run at any speed
- Need to upgrade only driver on NIC and firmware on switches
- User is not allowed to send any data until authenticated



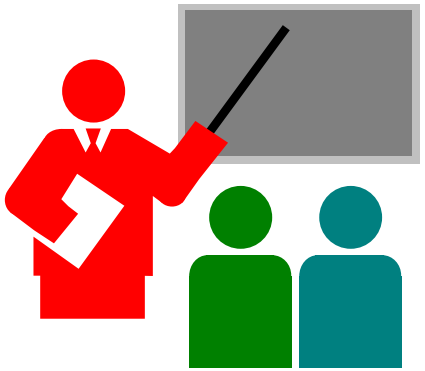
802.1X Authentication

Station | **Access Point** | **Authentication Server**

Can I connect please?	Associate ⟶	
What's your user name?	EAP Identity Request ⟵	
My user name is john	EAP Identity Response ⟶	EAP Identity Response ⟶
What's your password?	EAP Auth Request ⟵	EAP Auth Request ⟵
My password is mary?	EAP Auth Response ⟶	EAP Auth Response ⟶
You can connect!	EAP-Success ⟵	EAP-Success ⟵

- Authentication method can be changed without upgrading switches and access points
- Only the client and authentication server need to implement the authentication method

Summary



- RADIUS allows centralized authentication server and allows roaming
- EAP allows many different authentication methods to use a common framework => Authenticators do not need to know about authentication methods
- Many variations of EAP authentication methods depending upon certificates, shared secrets, passwords
- 802.1X adds authentication to LAN and uses EAPOL

Homework 18

- How would you implement Kerberos v4 over EAP in a LAN environment. Show the sequence of EAP messages that will be sent for authentication and key generation. Show also EAPOL headers on the messages.
- Hint: Use the 6 messages used in Kerberos and put EAPOL headers on them.

Acronyms

- AAA Authorization, Accounting, and Auditing
- AES Advanced Encryption System
- AK Authentication Key
- AKA Authentication and Key Agreement
- ARPAnet Advanced Research Project Agency Network
- AVP Attribute-Value Pair
- BBN Bolt Beranek and Newman
- CHAP Challange Handshake Protocol
- COPS Common Open Policy Service
- CRC Cyclic Redundancy Check
- DIAMETER Extension of RADIUS protocol
- EAP Extensible Authentical Protocol

Acronyms (Cont)

- EAP-AKA EAP with Authentication and Key Agrement
- EAP-FAST EAP with Flexible Authentication via Securre Tunneling
- EAP-GTC EAP using Generic Token Cards
- EAP-IKEv2 EAP using Internet Key Exchange version 2
- EAP-PSK EAP using preshared key
- EAP-SIM EAP using Subscriber Identity Module
- EAP-TLS EAP using Transport Level Security
- EAPOL EAP over LAN
- EMSK Extended Master Session Key
- GNU GNU is Not Unix
- GSM Global System for Mobile Communications

Acronyms (Cont)

- GSM-SIM SIM cards used in GSM phones
- ID Identification
- IEEE Institution of Electrical and Electronics Engineers
- IKE Internet Key Exchange
- IPX Novell Netware
- IPsec IP Security
- ISBN International Standard Book Number
- KDK Key Derivation Key
- LAT Local Area Terminal protocol
- LCP Logical Control Protocol
- LM LAN Manager
- MAC Media Access Control

Acronyms (Cont)

- MD5 Message Digest 5
- MS-CHAP Microsoft Challenge Handshake Protocol
- MTU Maximum Transmission Unite
- NAS Network Access Server
- NAS Network Attached Storage
- NIC Network Interface Card
- OTP One-Time Password
- PAC Protected Access
- PAP Password authentication protocol
- PEAP Protected EAP
- PIN Personal Identification Number
- PPP Point-to-Point Protocol

Acronyms (Cont)

- RADIUS Remote Authentication Dial-In User Service
- RAND Random challenge
- RFC Request for Comment
- SIM Subscriber identity module
- TACACS Terminal Access Controller Access-Control System
- TLS Transport Level Security

References

- J. Edney and W.A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i," Addison-Wesley, 2004, 451 pp., ISBN:0321136209
- http://en.wikipedia.org/wiki/RADIUS
- http://en.wikipedia.org/wiki/DIAMETER
- http://en.wikipedia.org/wiki/Password_Authentication_Protocol
- http://en.wikipedia.org/wiki/Challenge-handshake_authentication_protocol
- http://en.wikipedia.org/wiki/MS-CHAP
- http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol#_note-0
- http://en.wikipedia.org/wiki/EAP-FAST

References (Cont)

- http://en.wikipedia.org/wiki/Eapol
- http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol
- http://en.wikipedia.org/wiki/Security_token
- http://en.wikipedia.org/wiki/One-time_password
- http://en.wikipedia.org/wiki/EAP-SIM
- http://en.wikipedia.org/wiki/EAP-AKA
- http://en.wikipedia.org/wiki/EAP-TTLS#EAP-FAST

EAP RFCs

- RFC 2716 "PPP EAP TLS Authentication Protocol," October 1999.
- RFC 3579 "RADIUS Support For EAP," September 2003.
- **RFC 3748 "EAP," June 2004.**
- RFC 4017 "EAP Method Requirements for Wireless LANs," March 2005.
- RFC 4072 "Diameter EAP Application," August 2005.
- RFC 4137 "State Machines for EAP Peer and Authenticator," August 2005.
- RFC 4186 "EAP Method for GSM SIMs (EAP-SIM)," January 2006.
- RFC 4187 "EAP Method for 3G Authentication and Key Agreement (EAP-AKA)," January 2006.

EAP RFCs (Cont)

- RFC 4284 "Identity Selection Hints for the EEAP," January 2006.
- RFC 4746 "EAP Password Authenticated Exchange," November 2006.
- RFC 4763 "EAP Method for Shared-secret Authentication and Key Establishment (EAP-SAKE)," November 2006.
- RFC 4764 "The EAP-PSK Protocol: A Pre-Shared Key EAP Method," January 2007.
- RFC 4851 "The Flexible Authentication via Secure Tunneling EAP Method (EAP-FAST)," May 2007.

AAA RFCs

- RFC2903, "Generic AAA Architecture," Aug 2000.
- RFC2904, "AAA Authorization Framework," Aug 2000.
- RFC2905, "AAA Authorization application examples," Aug 2000.
- RFC2906, "AAA Authorization requirements," Aug 2000.
- RFC2989, "Criteria for Evaluating AAA Protocols for Network Access," Nov 2000.
- RFC3141, "CDMA2000 Wireless Data Requirements for AAA," Jun 2001.
- RFC3539, "AAA Transport Profile," Jun 2003.
- RFC3957, "AAA Registration keys for Mobile IPv4," Mar 2005.
- RFC4962, "Guidance for AAA Key Management," Jul 2007

RADIUS RFCs

- RFC2548 Microsoft Vendor-specific RADIUS Attributes, March 1999.
- RFC2809 Implementation of L2TP Compulsory Tunneling via RADIUS. April 2000.
- **RFC2865 RADIUS. June 2000.**
- RFC2866 RADIUS Accounting. June 2000.
- RFC2867 RADIUS Accounting Modifications for Tunnel Protocol Support. June 2000.
- RFC2868 RADIUS Attributes for Tunnel Protocol Support. June 2000.
- RFC2869 RADIUS Extensions. June 2000.
- RFC2882 Network Access Servers Requirements: Extended RADIUS Practices. July 2000.

RADIUS RFCs (Cont)

- RFC3162 RADIUS and IPv6. August 2001.
- RFC3575 IANA Considerations for RADIUS. July 2003.
- RFC3576 Dynamic Authorization Extensions to RADIUS. July 2003.
- RFC3579 RADIUS Support For Extensible Authentication Protocol (EAP). September 2003.
- RFC3580 IEEE 802.1X RADIUS Usage Guidelines. September 2003.
- RFC4014 RADIUS Attributes Suboption for the DHCP Relay Agent Information Option. February 2005.
- RFC4590 RADIUS Extension for Digest Authentication. July 2006.
- RFC4668 RADIUS Authentication Client MIB for IPv6. August 2006.

RADIUS RFCs (Cont)

- RFC4669 RADIUS Authentication Server MIB for IPv6. August 2006.
- RFC4670 RADIUS Accounting Client MIB for IPv6. August 2006.
- RFC4671 RADIUS Accounting Server MIB for IPv6. August 2006.
- RFC4672 RADIUS Dynamic Authorization Client MIB. September 2006.
- RFC4673 RADIUS Dynamic Authorization Server MIB. September 2006.
- RFC4675 RADIUS Attributes for Virtual LAN and Priority Support. September 2006.
- RFC4679 DSL Forum Vendor-Specific RADIUS Attributes. September 2006.

RADIUS RFCs (Cont)

- RFC4818 RADIUS Delegated-IPv6-Prefix Attribute. April 2007.
- RFC4849 RADIUS Filter Rule Attribute. April 2007.
- RFC5030 Mobile IPv4 RADIUS Requirements. October 2007.
- RFC 5080 "Common Remote Authentication Dial In User Service (RADIUS) Implementation Issues and Suggested Fixes," December 2007.
- RFC 5090 "RADIUS Extension for Digest Authentication," February 2008.
- RFC 5176 "Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)," January 2008.

Diameter RFCs

- **RFC3588 Diameter Base Protocol. September 2003**.
- RFC3589 Diameter Command Codes for 3GPP Release 5. September 2003.
- RFC4004 Diameter Mobile IPv4 Application. August 2005.
- RFC4005 Diameter Network Access Server Application. August 2005.
- RFC4006 Diameter Credit-Control Application. August 2005.
- RFC4072 Diameter EAP Application. August 2005.
- RFC4740 Diameter SIP Application. November 2006.
- RFC 5224 Diameter Policy Processing Application, March 2008.
- RFC 5431 Diameter ITU-T Rw Policy Enforcement Interface Application, March 2009.
- RFC 5447 Diameter Mobile IPv6: Support for Network Access Server to Diameter Server Interaction, February 2009.