Wireless LAN Security

Raj Jain

Washington University in Saint Louis

Saint Louis, MO 63130

Jain@cse.wustl.edu

These slides are available on-line at:

http://www.cse.wustl.edu/~jain/cse574-06/

Overview

- Wired Equivalent Privacy (WEP)
- WEP Problems and IEEE 802.11i Enhancement
- Extensible Authentication Protocol (EAP)
- RADIUS
- Transport Layer Security (TLS)
- Kerberos
- Temporal Key Integrity Protocol (TKIP)
- AES-CCMP
- VPN Protocols: GRE, L2TP, IPSec
- Attack Tools

Security Solutions

1. Open Access

2. MAC address filtering

3. Encryption: WEP

4. Wireless Protected Access (WPA)

5. Wireless Protected Access 2 (WPA2)

6. 802.1x/EAP-x/RADIUS

7. Virtual Private Network (VPN) with PPTP, L2TP

MAC Address Filtering

❑ Access Point contains MAC addresses of NICs

❑ Problem:

  ❑ Easy to find good MAC addresses by sniffing and then address spoofing

Wired Equivalent Privacy (WEP)

- WEP $\Rightarrow$ Privacy similar to a wired network
  $\Rightarrow$ Intellectual property not exposed to casual browser
  $\Rightarrow$ Not protect from hacker
- First encryption standard for wireless. Defined in 802.11b
- Provides authentication and encryption
- Shared Key Authentication
  $\Rightarrow$ Single key is shared by all users and access points
- Two modes of authentication: Open system and Shared Key
- Shared Key: Challenge-response verifies client has the key
- Manual key distribution
- If an adapter or AP is lost, all devices must be re-keyed
- Broken by Berkeley researchers, February 2001
- Ref: www.isaac.cs.berkeley.edu/isaac/wep-faq.html

WEP Details

❑ Each device has 4 static WEP keys

❑ KeyID sent w Initialization Vector (IV) in clear in each packet

❑ Per-Packet encryption key =24-bit IV + one of pre-shared key

❑ Encryption Algorithm: RC4

❑ Standard: 24 + 40 = 64-bit RC4 Key

❑ Enhanced: 24 + 104 = 128 bit RC4 key

❑ WEP allows IV to be reused

❑ CRC-32 = Integrity Check Value (ICV)

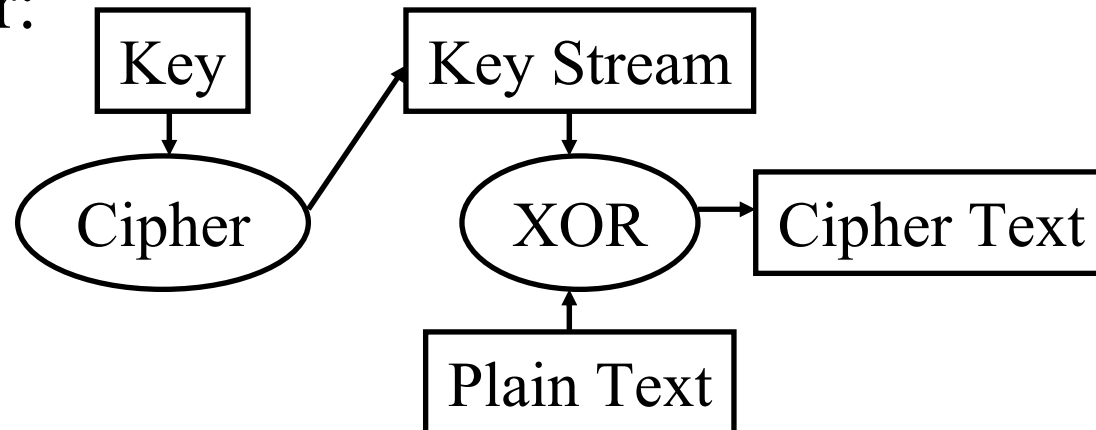❑ Data and ICV are encrypted under per-packet encryption key

802.11 Header	Data	CRC

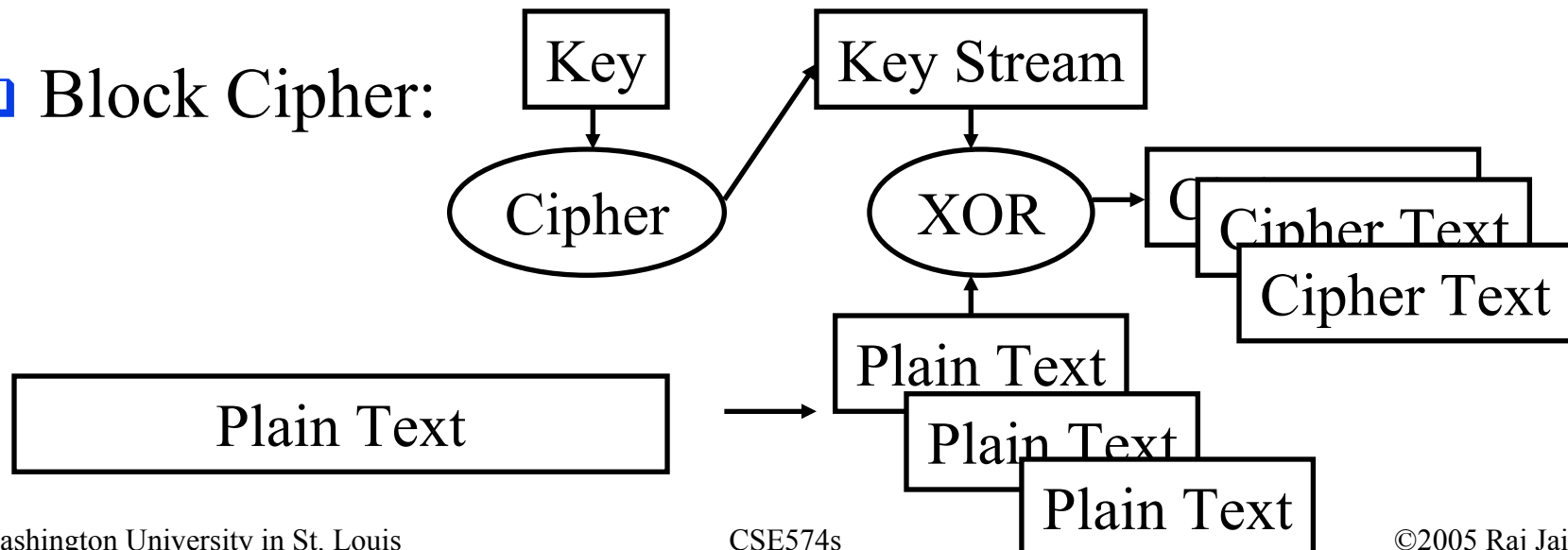| 802.11 Header	IV	Data	ICV
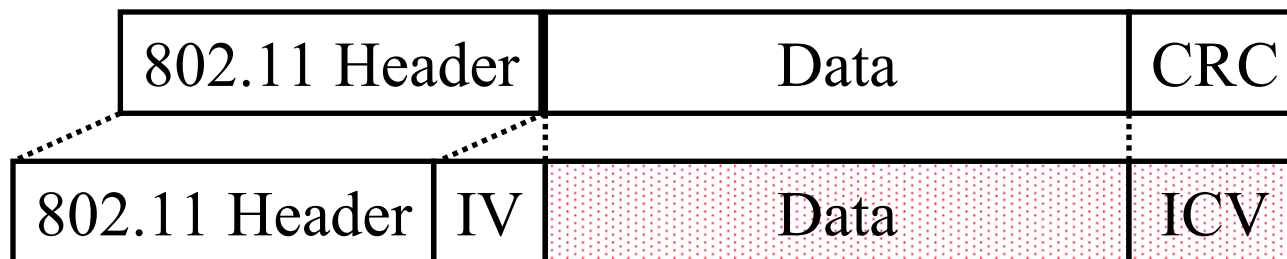
WEP Keys

❑ **Default Key**: Also known as shared key, group key, multicast key, broadcast key. 40-bit or 104 bit. Static.

❑ **Key mapping key**: Also known as individual key, per-station key, unique key. Access points need to keep a table of keys. Not generally implemented.

❑ To allow smooth change over, two default keys are required (old and new).

❑ WEP allows 4 default keys. Keys are numbered 0..3.
$\Rightarrow$ Can use different keys in two directions.

❑ The base key is combined with a 24-bit initialization vector (IV) $\Rightarrow$ Different key for each packet

❑ WEP does not specify how to select IV. Many vendors generate random IV.

Stream Cipher vs Block Cipher

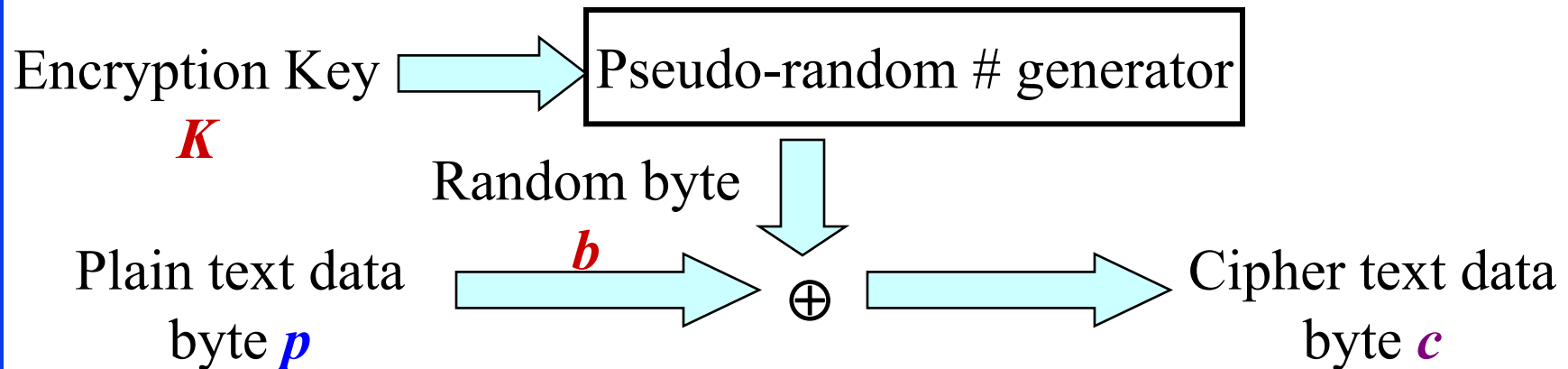❑ Stream Cipher:

Key	Key Stream

Cipher → Key Stream

XOR → Cipher Text

Plain Text

❑ Block Cipher:

Key	Key Stream

Cipher → Key Stream

XOR → Cipher Text

Cipher Text

Cipher Text

Plain Text

Plain Text

Plain Text

Plain Text

RC4

Encryption Key **K** ⟹ | Pseudo-random # generator |

Random byte **b**

Plain text data byte **p** ⟹ ⊕ ⟹ Cipher text data byte **c**

- ❑ Developed by Ron Rivest in 1987. Trade secret. Leaked 1994.
- ❑ $c1 = p1 \oplus b$; $c2 = p2 \oplus b \Rightarrow c1 \oplus c2 = p1 \oplus p2$
- ❑ Two packets w same IV ⟹ Difference in plain text
- ❑ 50% chance of using the same IV in 4823 packets.
- ❑ Pattern recognition can be used to find the plain text
- ❑ Recovered ICV ⟹ Plain text is correct
- ❑ Possible to recover all 2^{24} key streams in a few hours
- ❑ Send email to a victim and observe the response on the wireless and compare with the plain text received.

RC4 Computation

- Encryption key used to generate a pseudo-random bit stream
- S-Box is a 256-byte array filled with 0-256
- K-box is a 256-byte array filled with the key, repeated as many times as necessary

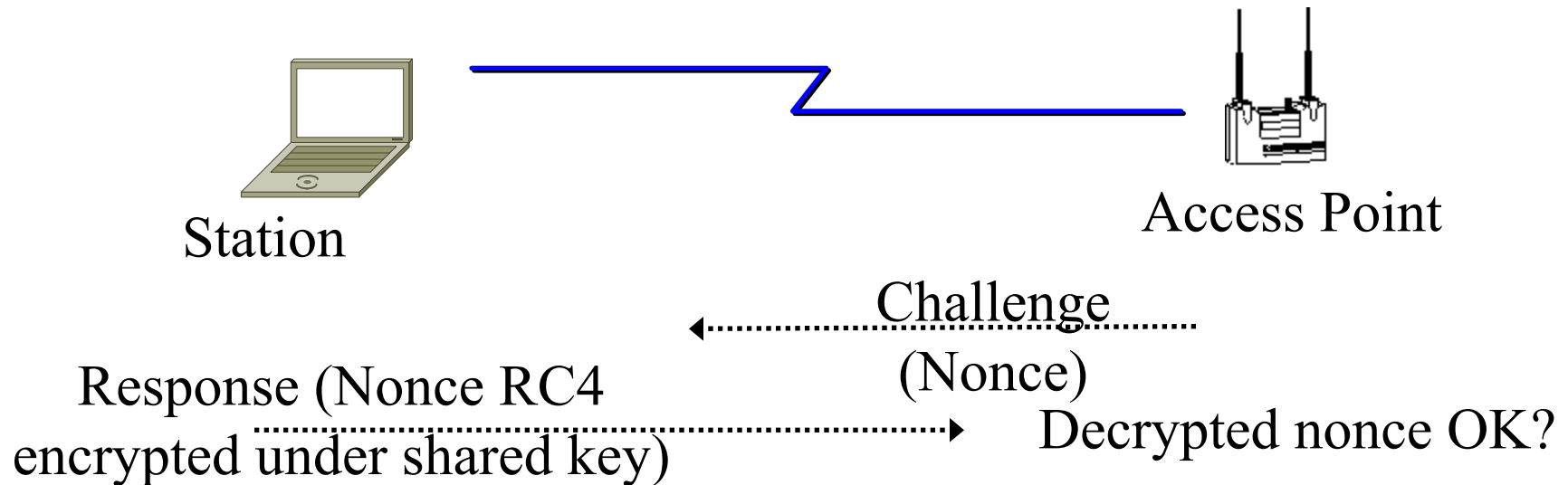| S_0	S_1	S_2	S_3	S_4	…	S_{254}	S_{255}

K_0	K_1	K_2	K_3	K_4	…	K_{254}	K_{255}
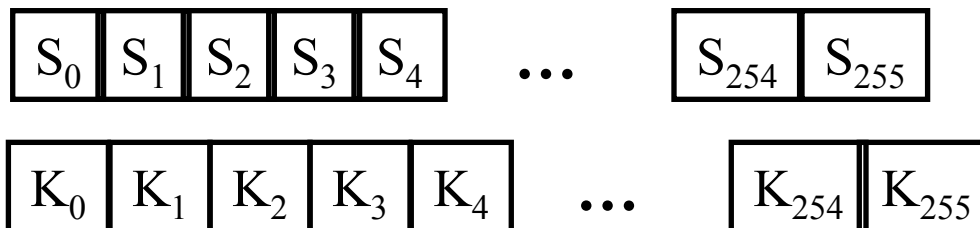
S-Box Initialization:
$i = j = 0$
For $i = 0$ to 255 do
$j = (j + S_i + K_i) \bmod 256$
Swap S_i and S_j
End

Random Stream Generation:
$i = (i + 1) \bmod 256$
$j = (j + S_i) \bmod 256$
Swap S_i and S_j
$k = (S_i + S_j) \bmod 256$
$R = S_k$

WEP Authentication w/o Key

- ❑ Authentication is a via Challenge response using RC4 with the shared secret key.
- ❑ Record one challenge/response
- ❑ XOR the two to get the key stream
- ❑ Use that key stream to encrypt any subsequent challenge

Station

Access Point

Challenge
(Nonce)

Response (Nonce RC4 encrypted under shared key)

Decrypted nonce OK?

WEP Traffic Modification

❑ Let plain text

$$p = p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 x^0$$

Plain text with ICV

$$px^{32} + \text{ICV}(p) = p_n x^{n+32} + p_{n-1} x^{n+31} + \ldots + p_0 x^{32} + \text{ICV}(p)$$

Let $b = n+32$ bit RC4 stream used for encryption

Then sent message

$$px^{32} + \text{ICV}(p) + b$$

❑ ICV is linear: $\text{ICV}(p+q) = \text{ICV}(p) + \text{ICV}(q)$

$$(p+q)x^{32} + \text{ICV}(p+q) + b = px^{32} + qx^{32} + \text{ICV}(p) + \text{ICV}(q) + b$$

❑ Conclusion: XOR any CRC-32 valid plain text to encrypted packet. The modified packet will pass the ICV after decryption.

❑ Encryption $\nRightarrow$ Integrity

WEP Problems

❑ No centralized key management
  Manual key distribution $\Rightarrow$ Difficult to change keys

❑ Single set of Keys shared by all $\Rightarrow$ Frequent changes necessary

❑ Weak Encryption: RC4 is very weak
  $\Rightarrow$ Challenge-Response can be used to obtain the shared key

❑ No mutual authentication

❑ No user management (no use of RADIUS)

❑ IV value is too short. Not protected from reuse.

❑ Weak integrity check.

❑ Directly uses master key

❑ No protection against replay

IEEE 802.11i Security Enhancement

❑ Packet sequence number to prevent replay

❑ AES-128 encryption

❑ 802.1X Authentication

❑ Extensible Authentication Protocol (EAP)

❑ Many authentication methods. Default=IAKERB

❑ Mutual Authentication (Station-Key Distribution Center, Station-Access Point)

❑ AP send security options in probe response if requested

802.11 Security Protocol Stack

Station   Access Point   Authentication Server

TLS	TLS
EAP	EAP
802.1X	RADIUS
802.11	TCP/IP
	802.3
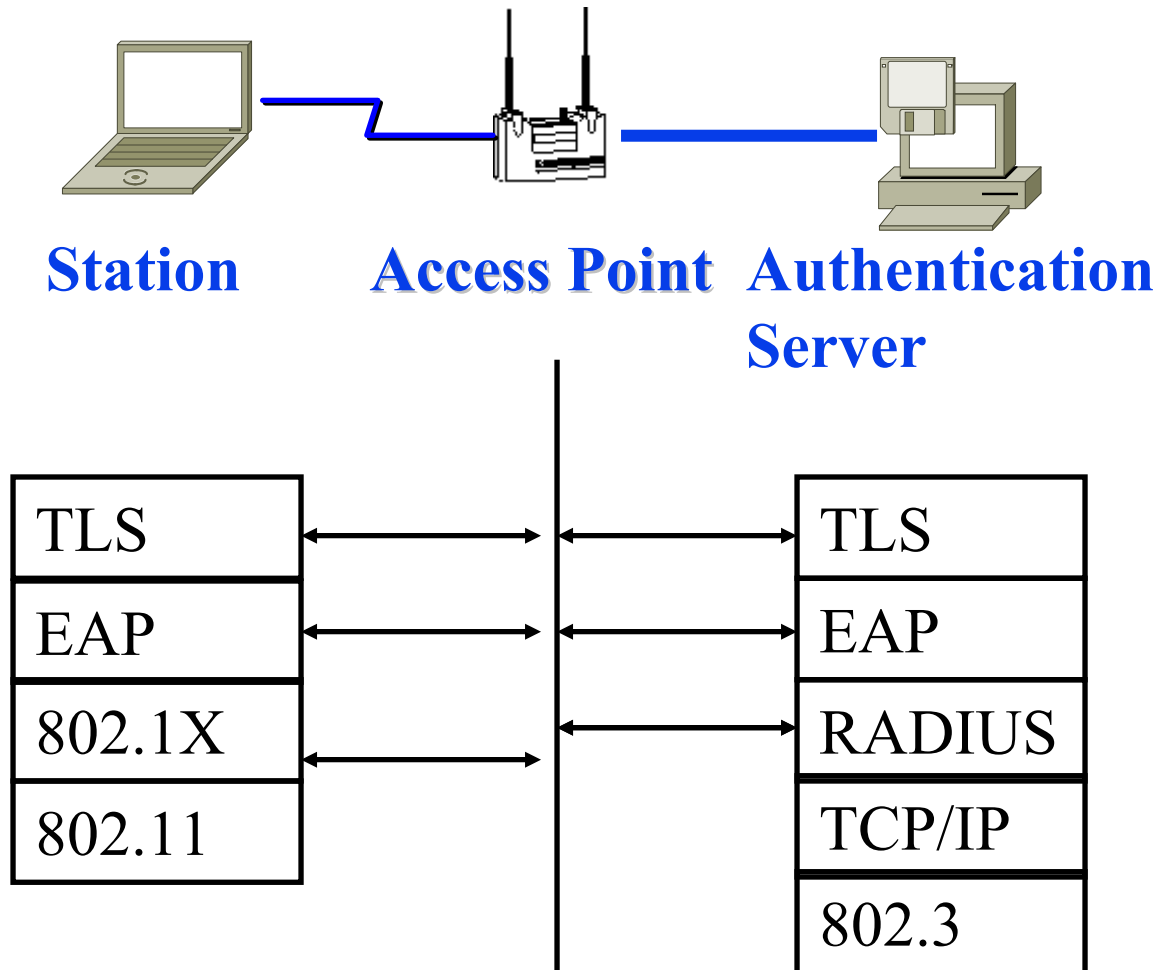
PAP and CHAP
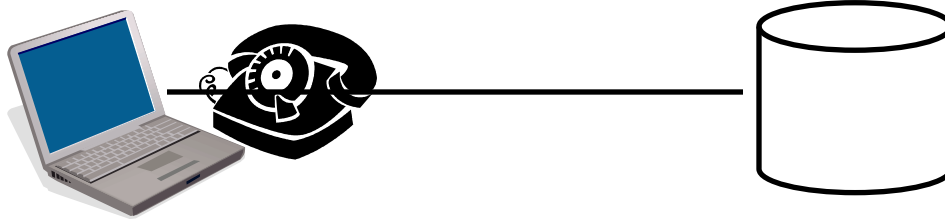
- Authentication on Point-to-point protocol (PPP)

  - Password authentication protocol (PAP)

  - Challenge Handshake Authentication Protocol (CHAP) – RFC1994

  - Each authentication protocols required a new protocol type number $\Rightarrow$ Extensible Authentication Protocol
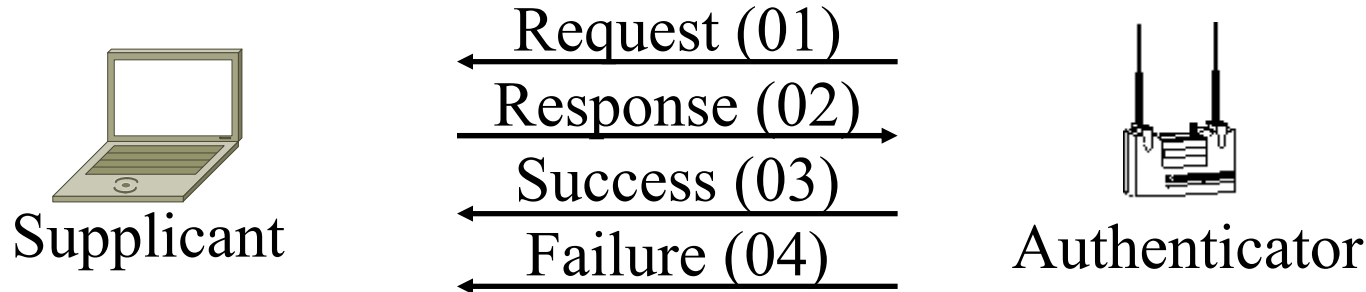
Extensible Authentication Protocol (EAP)

❑ Flexible link layer security framework. Does not require IP.

❑ Initially developed for point-to-point protocol (PPP)

❑ Allows using many different authentication methods

    ❑ Certificate based: EAP-TLS (Transport Level Security)

    ❑ Password based: EAP-OTP (One-time Password), EAP-MD5 (Message Digest 5)

    ❑ Smart card based: EAP-SIM (Subscriber Identity Module)

    ❑ Hybrid: EAP-TTLS (Tunneled TLS)

    ❑ Proprietary: Cisco's LEAP (Lightweight EAP)

❑ Can run on any link layer (PPP, 802, ...). Does not require IP.

❑ No window flow control. No fragmentation.
Ack/Nack $\Rightarrow$ Can run over lossy link

❑ Ref: RFC3748

EAP Exchange

❑ EAP Message Format:

Code	Identifier	Length	Data
8b	8b	16b	
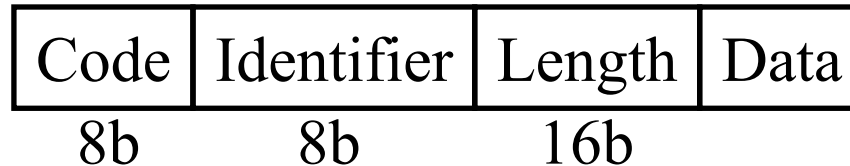
❑ Only four types of messages:

Supplicant

Request (01) ←
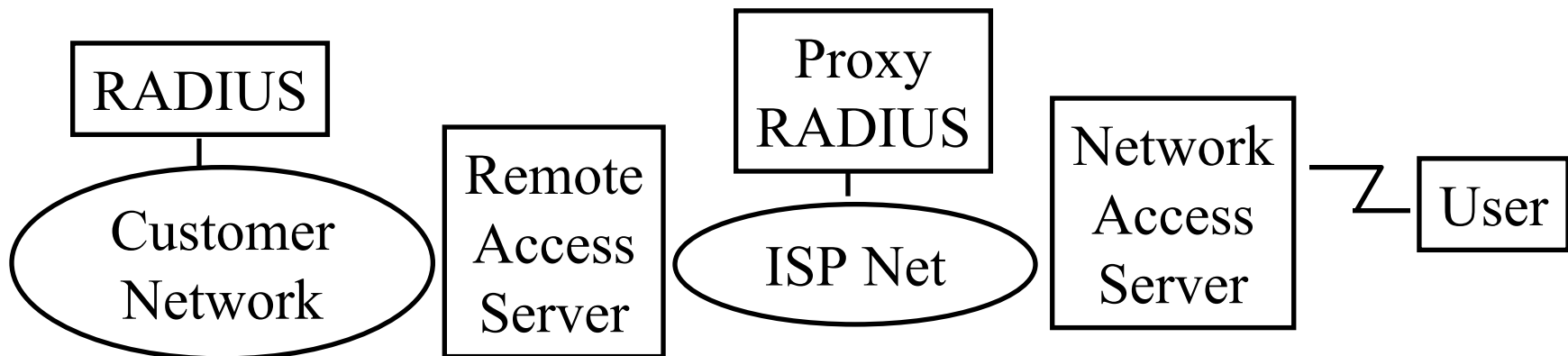Response (02) →
Success (03) ←
Failure (04) ←

Authenticator

❑ 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.
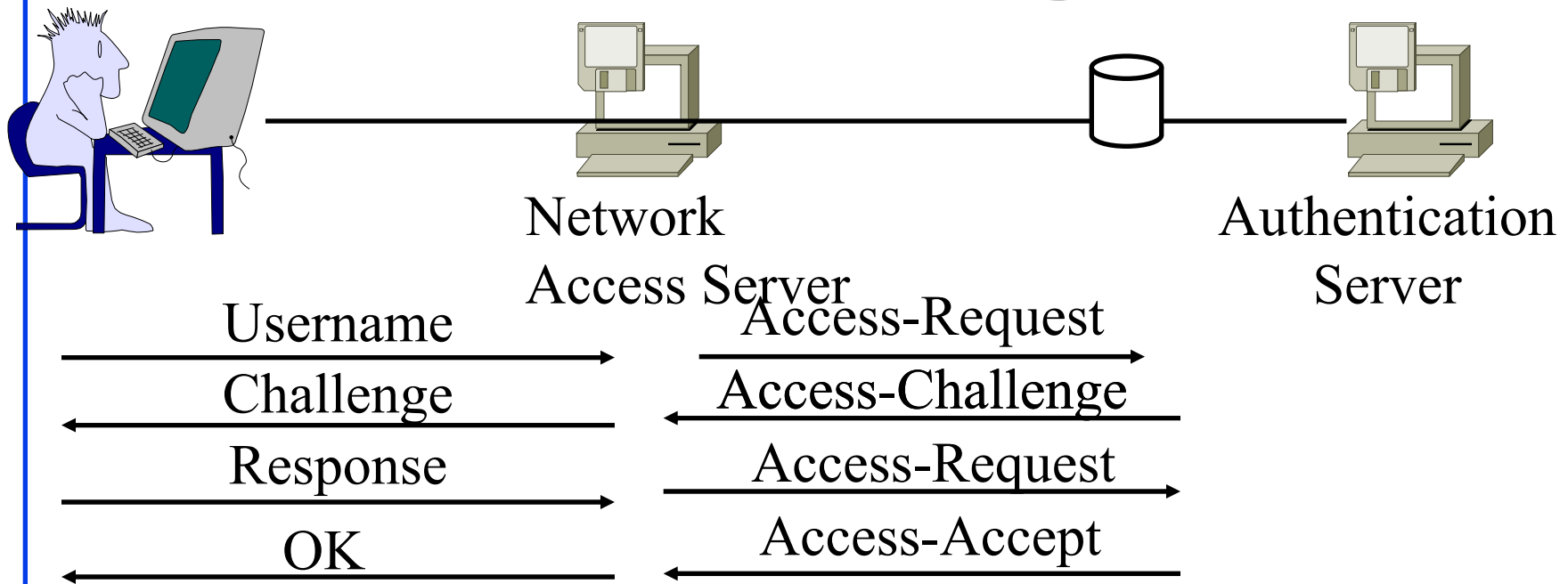Assigned by Internet Assigned Number Authority (IANA)

Code	Identifier	Length	**Type**	Data

RADIUS

❑ Remote Authentication Dial-In User Service

❑ Central point for Authorization, Accounting, and Auditing data
$\Rightarrow$ AAA server

❑ Network Access servers get authentication info from RADIUS
servers

❑ Allows RADIUS Proxy Servers $\Rightarrow$ ISP roaming alliances

❑ Normally runs on UDP $\Rightarrow$ Can loose accounting packets

❑ FreeRADIUS and OpenRADIUS implementations available

RADIUS — Customer Network — Remote Access Server — Proxy RADIUS — ISP Net — Network Access Server — User

RADIUS Messages

|	
Username →	Access-Request →
← Challenge	← Access-Challenge
Response →	Access-Request →
← OK	← Access-Accept

- ❑ 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

802.1X

❑ Authentication *framework* for IEEE802 networks

❑ Supplicant (Client), Authenticator (Access point),
   Authentication server

❑ No per packet overhead $\Rightarrow$ 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

Authenticator	Authenticator

External
Device

Connected
Device
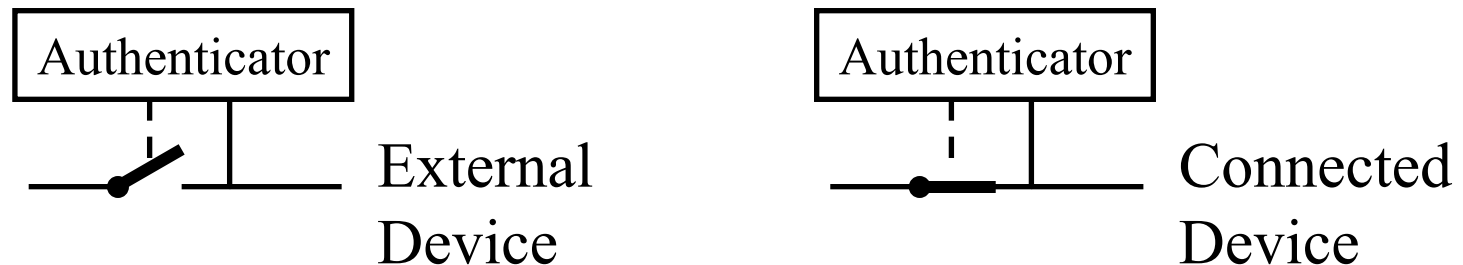
EAP over LAN (EAPOL)

❑ EAP was designed for Point-to-point line
❑ IEEE 802.1X extends it for LAN ⇒ 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
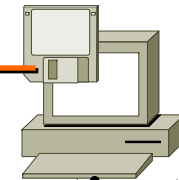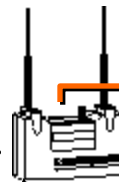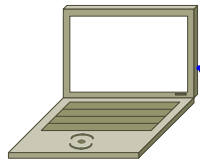
Station	Access Point	Authentication Server
Can I connect please?	·········Associate·········▶	
What's your user name?	◀·····EAP Identity Request·····	
My user name is john	EAP Identity Response ·············▶	EAP Identity Response ·············▶
What's your password?	◀·····EAP Auth Request·····	◀·····EAP 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

802.1X Protocol Stack

Method Layer

```
Backend AAA Infrastructure
Radius, Kerberos, …
```

EAP Layer

| VPN | TLS | GSS API | GSM SIM | LEAP |

EAP API

EAP

NDIS API

Media Layer

| PPP | 802.3 | 802.11 |
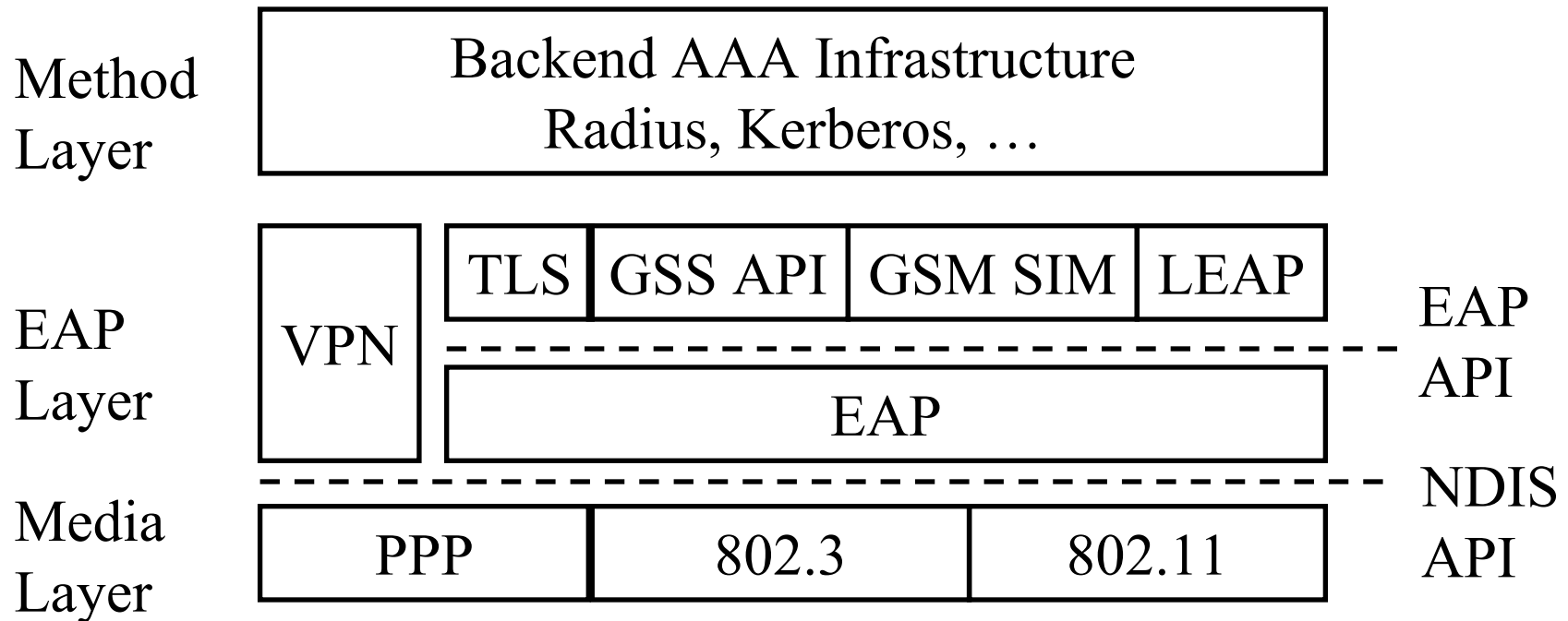
Transport Layer Security (TLS)

- ❑ Based on Secure Socket Layer (SSL) v3 developed by Netscape for secure commerce in 1994
- ❑ Standardized by IETF in 1999 in RFC2246
- ❑ Both Microsoft and Netscape support TLS
- ❑ Uses public key certificates for authentication and key exchange
- ❑ Customer does not need a certificate (provides a credit card #)

Client Hello: Hi BigCo! I speak RSA, DES2, SHA-1.

Server Hello: Hi! Here is our certificate and public key. Let us use RSA, DES, SHA-1. Random #

Here is a *pre-master secret* encrypted with your public key

Both use the pre-master secret to generate 6 secret session keys.
The keys is used for encryption, MAC, cipher initialization (IV), in each direction

Kerberos

- Cerberus = three headed dog guarding the underworld
- Developed by Needham and Schroeder in 1987. Uses tickets.
- Provides confidentiality, authentication, integrity, access control, availability, and key management
- Quick re-authentication $\Rightarrow$ Quick handoffs
- Implemented in Windows NT and in Open Source Foundation's Distributed Computing Environment.
Sources available from MIT
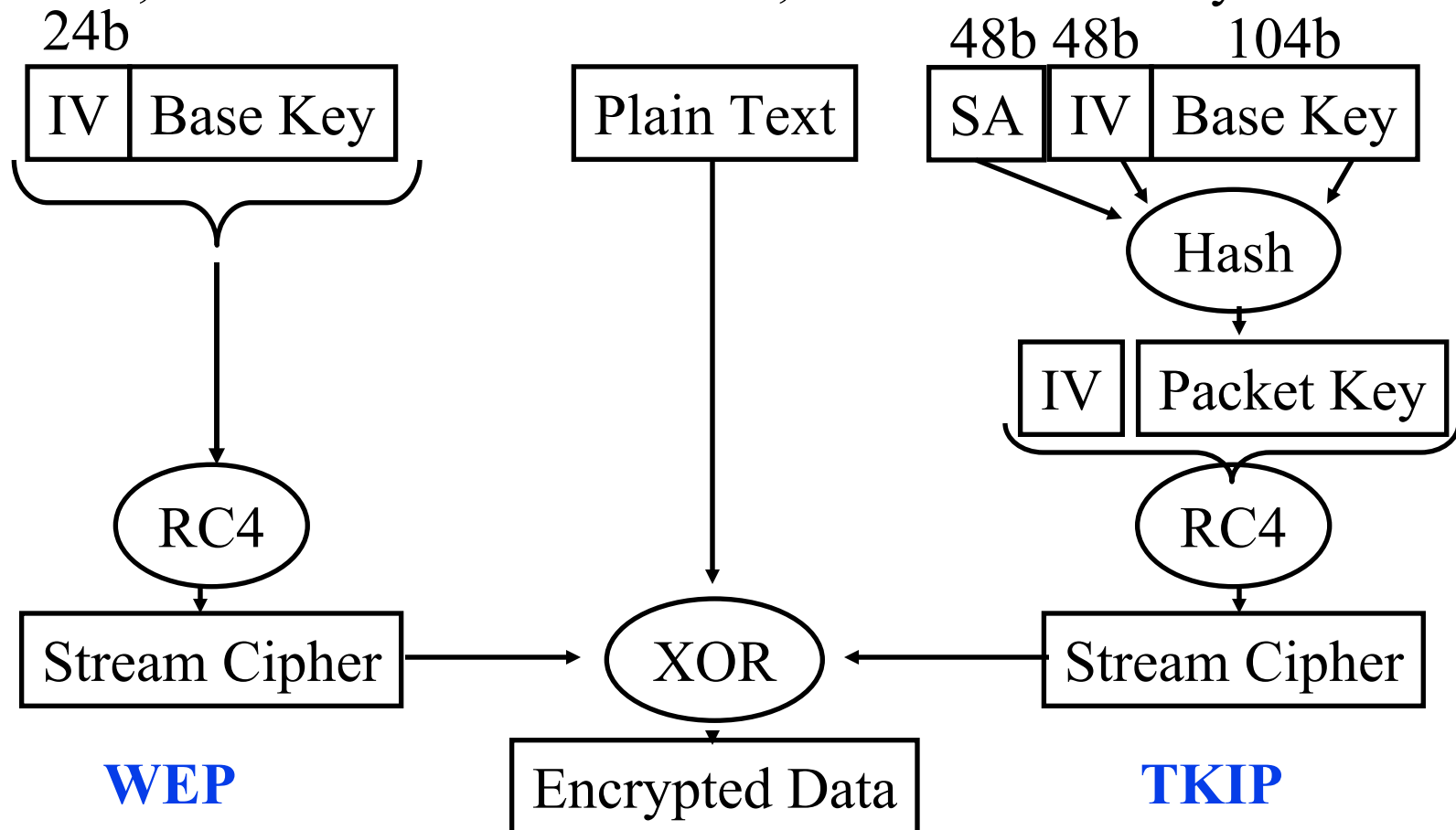- Mandatory for 802.11e (QoS enhancement)

Kerberos (Cont)

❑ Four Processes:

   ❑ Authentication Exchange: Authentication Server generates a session key for user-TGS communication and sends it to the user encrypted with user's secret key, also sends a ticket containing the session key, user info, and encrypted with TGS's key

   ❑ Ticket Granting Service (TGS) Exchange: User sends the ticket to TGS and gets tickets for other servers (AP, DHCP, ..).

   ❑ User/Server Exchange: User sends the tickets to AP and gets connected

   ❑ Secure Communication: Uses AP session key to communicate with AP.

❑ Ref: RFC4120

Wi-Fi Protected Access (WPA)
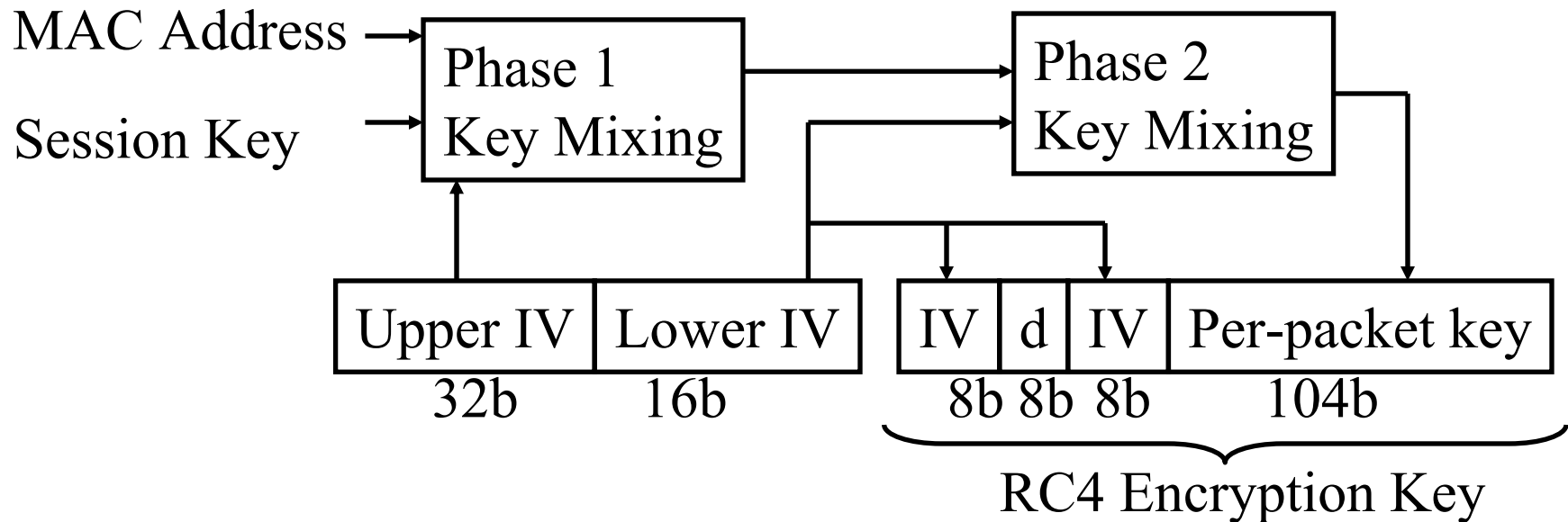
- Temporal Key Integrity Protocol (TKIP)
  - KeyMix: Key hashing
  - Michael: Nonlinear message integrity check
  - Rapid re-keying
- Pre-Shared key mode
- Managed mode: 802.1x and EAP
- Software/firmware upgrade for current devices 802.11i needs new hardware $\Rightarrow$ WPA2
- All access points and subscribers need to use WPA
- WPA+WEP $\Rightarrow$ WEP

Temporal Key Integrity Protocol (TKIP)

❑ WEP: Same base key is used in all packets

❑ TKIP: New packet key is derived for each packet from source address, 48-bit initialization vector, and 104b base key

24b

| IV | Base Key |

48b 48b 104b

| SA | IV | Base Key |

Plain Text

Hash

| IV | Packet Key |

RC4

Stream Cipher

RC4

Stream Cipher

XOR

Encrypted Data

WEP

TKIP

RC4 Encryption Key

MAC Address →

Session Key →

| Phase 1 Key Mixing | | Phase 2 Key Mixing |

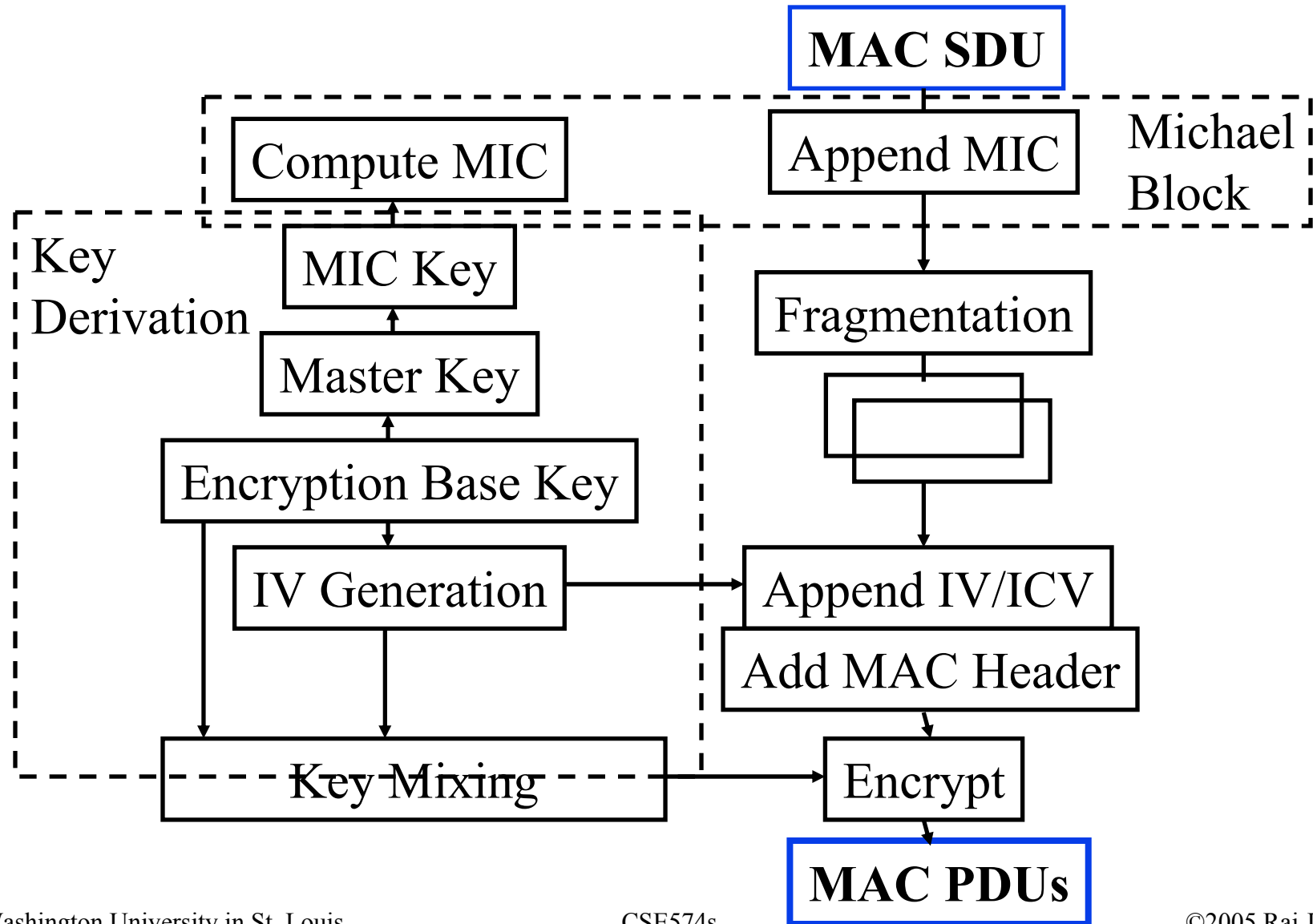| Upper IV | Lower IV | IV | d | IV | Per-packet key |
| 32b | 16b | 8b | 8b | 8b | 104b |

RC4 Encryption Key

- ❑ Phase 1: Transmitters MAC address, session key, and upper 32b of the IV are hashed together

- ❑ Phase 2: Lower 16 bits of IV is hashed to produce per-packet key

- ❑ d is a dummy byte designed to avoid weak keys.

TKIP Message Integrity Check (MIC)

❑ Michael – A non-linear integrity check invented by Neil Furguson. Designed for WPA.

❑ A separate MIC key is derived from the master session key

❑ 8-byte check value is added to "MAC SDU"

❑ MIC is computed using a virtual header containing MAC destination and source address

DA	SA	MAC User Data

TKIP Transmission

MAC SDU

Michael Block
- Compute MIC
- Append MIC

Key Derivation
- MIC Key
- Master Key
- Encryption Base Key
- IV Generation
- Key Mixing

- Fragmentation
- Append IV/ICV
- Add MAC Header
- Encrypt

MAC PDUs

WEP vs. WPA

WEP	WPA
No centralized key management Manual key distribution => Difficult to change keys	EAP/TLS allows per session keys
Single set of Keys shared by all => Frequent changes necessary	RADIUS allows each user to be authenticated individually
Weak Encryption: RC4 is very weak => Challenge-Response can be used to obtain the shared key	RC4 is kept. Authentication key is different from encryption key
No mutual authentication	Mutual Authentication
No user management (no use of RADIUS)	RADIUS
IV value is too short. Not protected from reuse.	48-bit IV
Weak linear integrity check.	Michael – non-linear integrity check
Directly uses master key	Uses derived keys
No protection against replay	Protection against replay

WPA2 (802.11i)

- Advanced Encryption Standard (AES)
  $\Rightarrow$ Need hardware support
- Secure fast handoff preauthentication
- Secure de-association and de-authentication
- Security for peer-to-peer communication (Ad-hoc mode)

AES-128 Encryption

- ❑ Provides both privacy and integrity
- ❑ NIST standard. Highly parallelizable
- ❑ Iterated Block cipher: encrypts 128-bit blocks
- ❑ Uses 128-, 192-, or 256-bit keys
- ❑ Offset codebook (OCB) mode
- ❑ Session sequence number added to avoid replay
- ❑ Base key is mapped to get session key using OCB mode tag

802.11 Header	Data

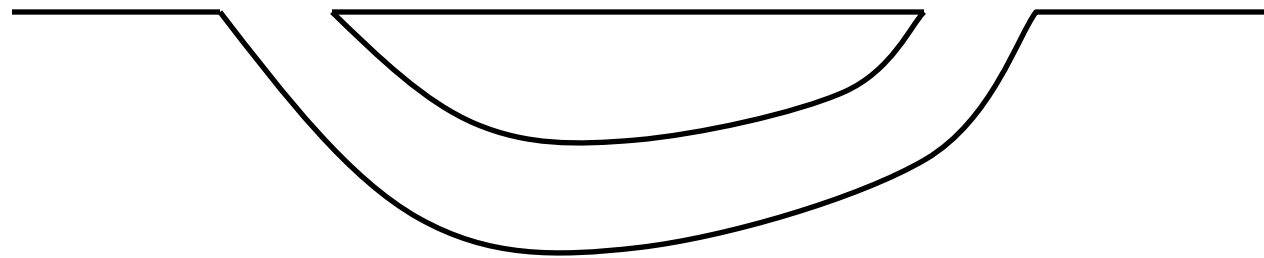| 802.11 Header	IV	Data	Seq #	MIC

128b   128b
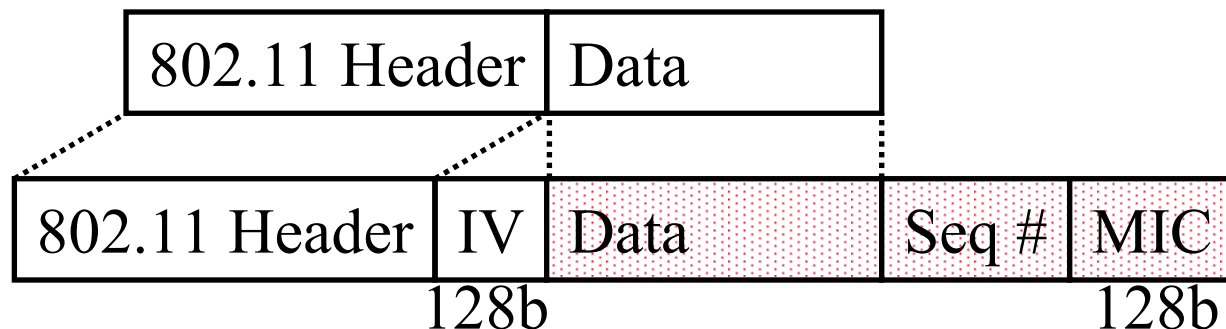
AES-CCMP

❑ Stronger than TKIP. Used in WPA2 = 802.11i

❑ Requires new hardware.

❑ AES is a block cipher. It has many modes.
802.11i uses Counter-Mode Cipher block chaining MAC Protocol

❑ Counter is incremented for each successive block processed.

❑ Counter is encrypted and then xor'ed with data.

•Counter can be started at a arbitrary value.

•Repeating blocks give different cipher text

					Message
1	2	3	4	5	Counter
E	E	E	E	E	AES Encryption
					XOR
					Cipher text
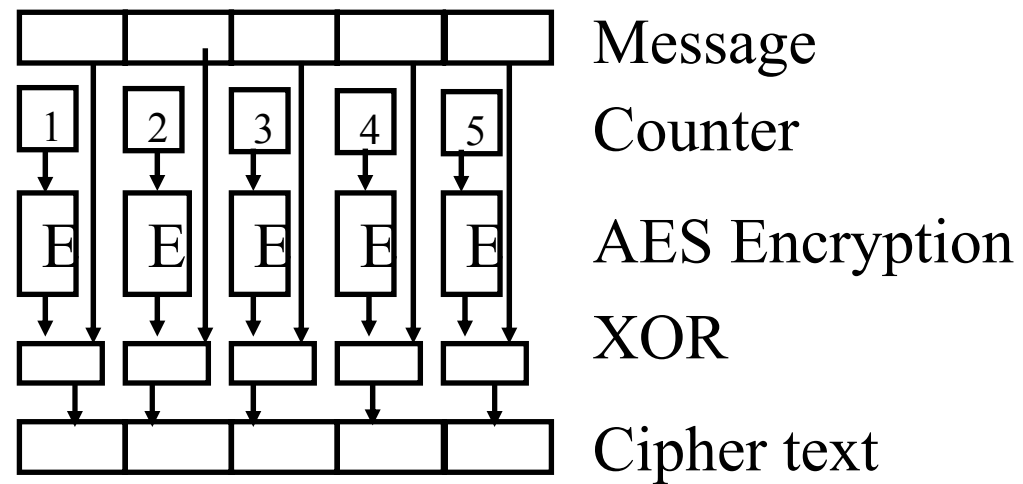
Tunnel

IP Land   IP Not Spoken Here   IP Land

Non-IP Header	IP Header	Payload

- ❑ Tunnel = Encaptulation
- ❑ Used whenever some feature is not supported in some part of the network, e.g., multicasting, mobile IP

GRE

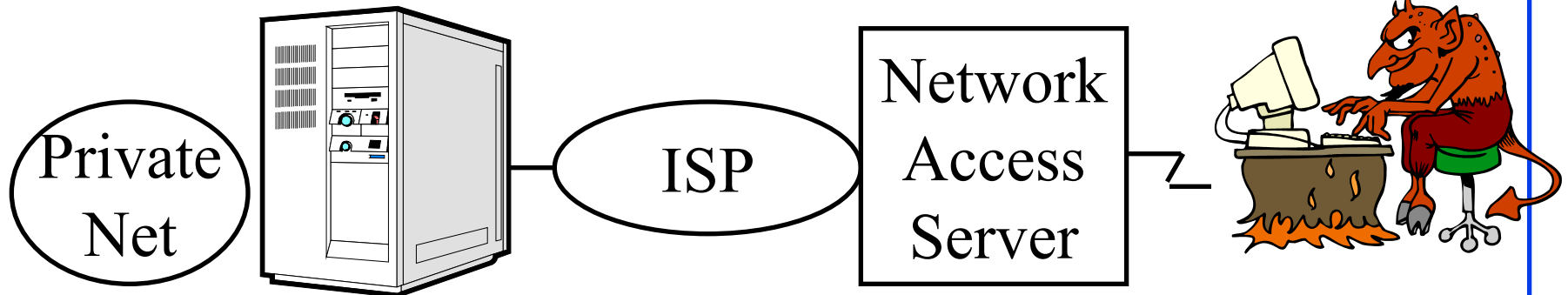| Delivery Header	GRE Header	Payload

- ❏ Generic Routing Encaptulation (RFC 1701/1702/2784/4023)
- ❏ Generic $\Rightarrow$ X over Y for any X or Y
- ❏ GRE header contains only version # and protocol type. Optional Checksum, Loose/strict Source Routing, Key, etc.
- ❏ Over IPv4, GRE packets use a protocol type of 47 in the delivery header
- ❏ Following protocol types in GRE header are used for payload: 0x8000=IPv4, 0x8847=MPLS Unicast, 0x8848=MPLS Multicast
- ❏ Restricted to a single provider network $\Rightarrow$ end-to-end

L2TP

L2TP Server ISP Network Access Server **Client**

L2TP Tunnel
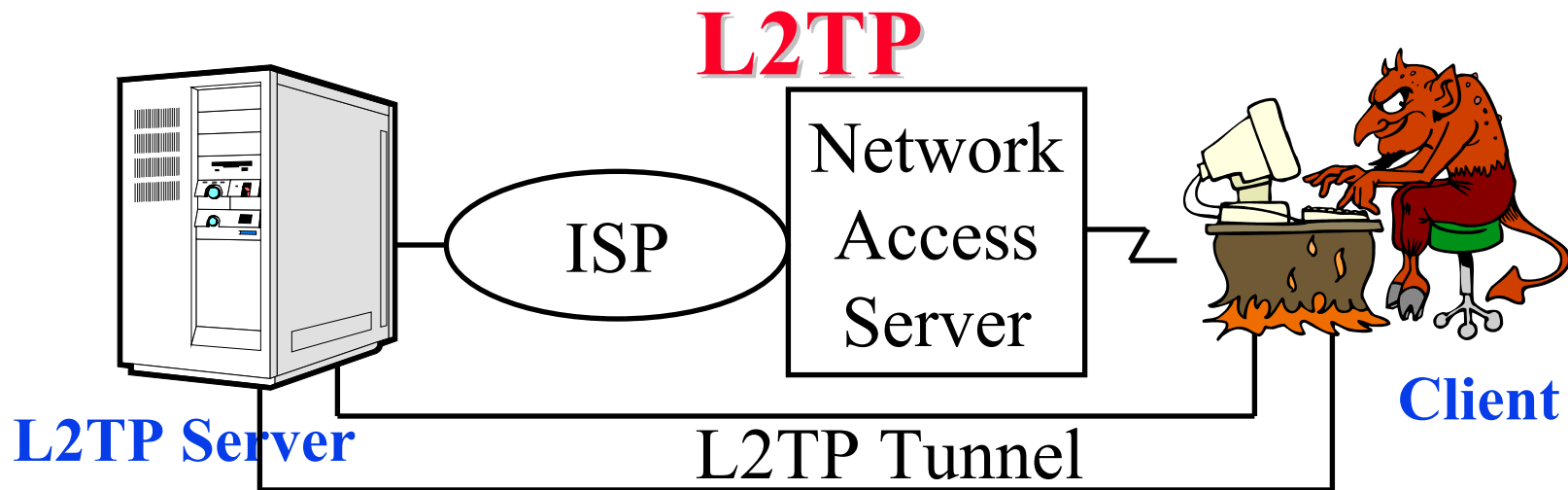
- ❑ L2TP = Layer Two Tunneling Protocol
  = Layer 2 Forwarding (L2F) from Cisco +
  Point-to-Point Tunneling Protocol (PPTP) from Microsoft
- ❑ Allows PPP frames to be sent over non-IP (Frame relay, ATM) networks also (PPTP works on IP only)
- ❑ Allows multiple (different QoS) tunnels between the same end-points. Better header compression. Supports flow control
- ❑ Implemented in Windows 2000 onwards
- ❑ REF: RFC3931 (L2TPv3)

L2TP Packets

Client

Private Net

PPTP Server

ISP

Network Access Server

L2 Header
IP
IPSec
UDP
L2TP
PPP
IP/IPX/NetBEUI
Data

L2 Header
IP
IPSec
UDP
L2TP
PPP
IP/IPX/NetBEUI
Data

Public IP Addressing

IP/IPX/NetBEUI
Data

Internal IP Addressing

☐ Encrypted

IPSec

❑ Secure IP: A series of proposals from IETF. RFC4301.

❑ Separate Authentication and privacy

❑ Authentication Header (AH) ensures data *integrity* and *data origin authentication and anti-replay service*

❑ Encapsulating Security Protocol (ESP) ensures *confidentiality, data origin authentication, connectionless integrity, and anti-replay service*

IP Header	AH	ESP	Original IP Header*	Original Data	Trailer

← Encrypted →

← Authenticated →

* Optional

IPSec (Cont)

- ❑ ESP is required. AH is optional because ESP provides a superset of AH services.

- ❑ Two Modes: Tunnel mode, Transport mode

- ❑ Tunnel Mode $\Rightarrow$ Original IP header encrypted

- ❑ Transport mode $\Rightarrow$ Original IP header removed. Only transport data encrypted.

- ❑ Supports a variety of encryption algorithms

- ❑ Better suited for WAN VPNs (vs Access VPNs)

Attack Tools

❑ Net Stumbler: Gives a quick view of all WLANs available. www.netstumbler.com

❑ Kismet: Passive war driving. Does not transmit probe requests. You can see text strings being transmitted. www.kismetwireless.net

❑ Bsd-airtools: AP detection, WEP cracking, traffic monitoring and analysis www.dachb0den.com/projects/bsd-airtools.html

❑ Airsnort: WEP cracking in the background http://airsnort.shmoo.com

❑ Airjack: DoS attack, Man-in-the-middle attack, …

❑ More tools at http://www.wi-foo.com/index-3.html

Summary
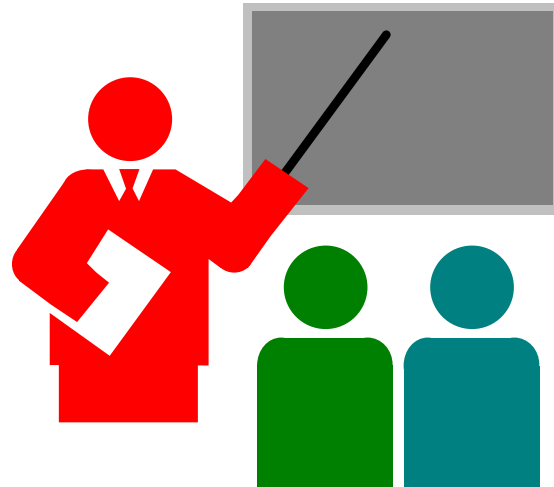
- WEP is insecure, not scalable, no user management
- Current hardware can be upgraded to WPA, which provides better encryption, mutual authentication
- Next generation WPS2 will implement 802.11i
- IEEE 802.1X with EAP, TLS, RADIUS provides user management
- VPNs using L2TP/IPSec can also be used over wireless

References

- J. Edney and W.A. Arbaugh, "Real 802.11 Security: Wi-Fi Protected Access and 802.11i," Addison-Wesley, 2004, 481 pp., ISBN:0321156209

- H.X. Mel and D. Baker, "Cryptography Decrypted," Addison-Wesley, 2000, 352 pp., ISBN:0201616475

RFC's

- ❏ RADIUS: RFC 2865
- ❏ EAP: RFC3748
- ❏ Kerberos V5: RFC4120
- ❏ TLS: RFC2246, RFC3546
- ❏ EAP-TLS: RFC2716
- ❏ GSM-SIM over EAP: RFC4186
- ❏ GRE: RFC2784
- ❏ L2TP: RFC3931
- ❏ IPSec: RFC4301
- ❏ AH: RFC4302
- ❏ ESP: RFC 4303