NETWORKERS

Cisco Systems

Cisco.com

Securing 802.11 Wireless Networks

Session ACC-232

Session Information

- **Basic understanding of components of 802.11 networks**
- **Please save questions until the end**

Agenda

- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

Agenda

- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

Key Markets for Wireless

- Enterprise/Mid Market
- Education
- Manufacturing/Warehousing
- Retail
- Healthcare

Enterprise/Mid Market

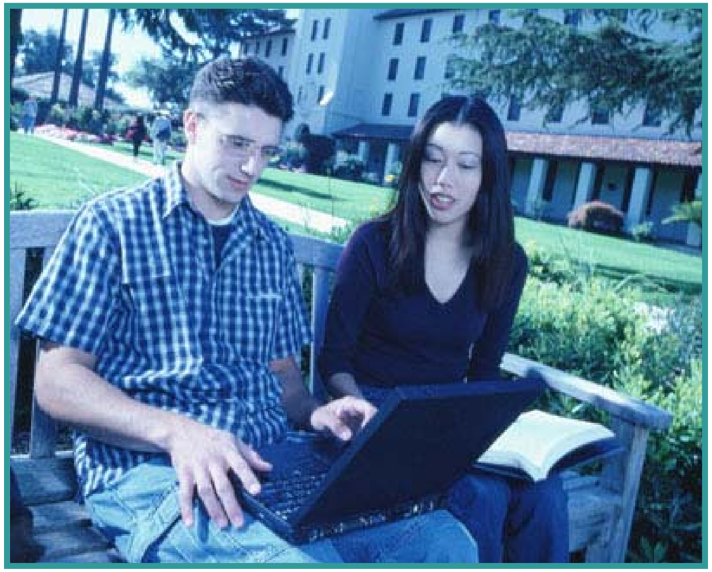
- Employees want wireless
- ROI—Up to 70 minutes more productivity per day
- If IT doesn’t roll out wireless, employees will
  - Low end APs at the local computer reseller shop

Enterprise/Mid Market

- Rogue deployments expose corporate network
- IT should provide WLANs and secure them

Education

- Collaborative learning applications aid students and teachers
- An unsecured WLAN leaves the following vulnerable
  - Student records
  - Administrative DBs
  - Proprietary learning materials



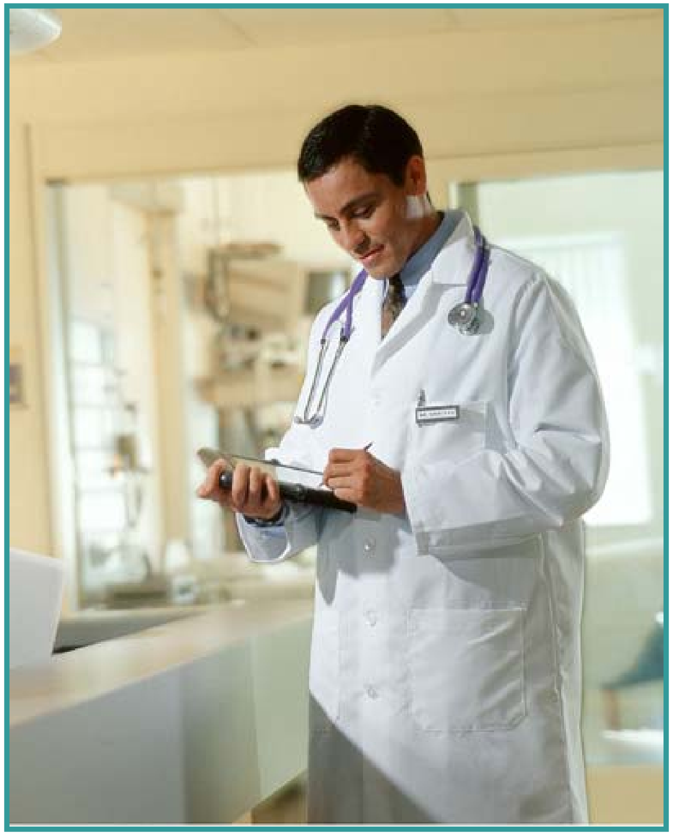
Manufacturing/Warehousing/Retail

- Barcode readers and POS terminals very common
- Many wireless appliances only support static WEP, or don't use any security!
- If connected to corporate network, network is vulnerable

Healthcare

- Wireless enabled patient management applications and devices becoming pervasive
- Insecure deployments leave patient data vulnerable

  Secure wireless LANS
  are an enabler
  for HIPAA compliance



HIPAA : Health Insurance Portability and Accountability Act / US Protection of medical privacy

Agenda

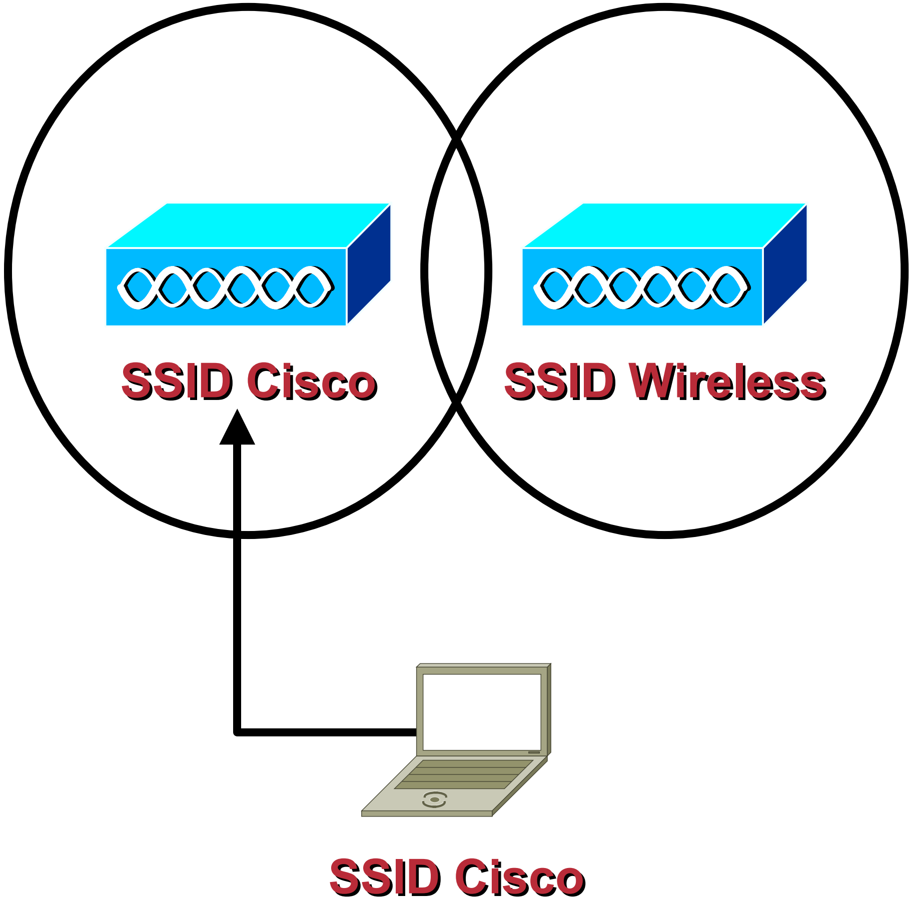
- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

802.11 Wireless Security

- Service Set Identifier (SSID)
- Wired Equivalent Privacy (WEP)
- Open Authentication
- Shared Key Authentication
- MAC Address Authentication

The Service Set Identifier (SSID)

- **Used to logically separate wireless LANs**

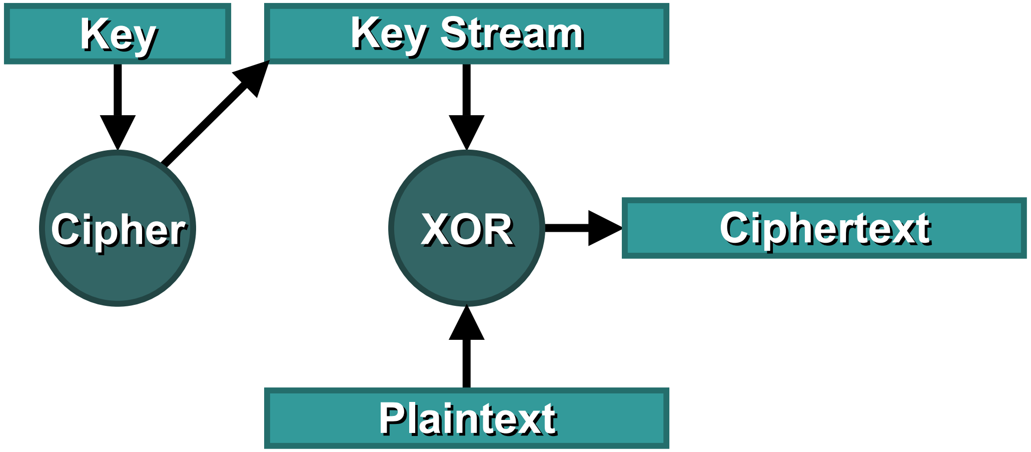


WEP Encryption

- Wired Equivalent Privacy
- Based on the RC4 symmetric stream cipher
- Static, pre-shared, 40 bit or 104 bit keys on client and access point

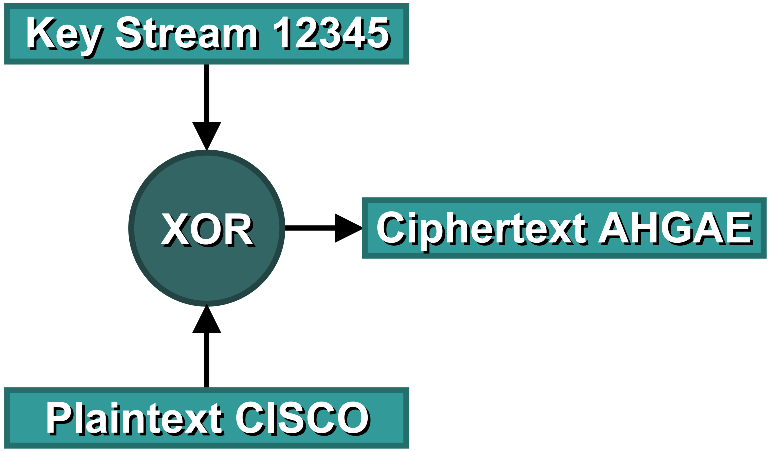
What Is a Stream Cipher?

- Generates a key stream of a desired length from the key
- The key stream is mixed with the plaintext data
- The result is ciphertext data



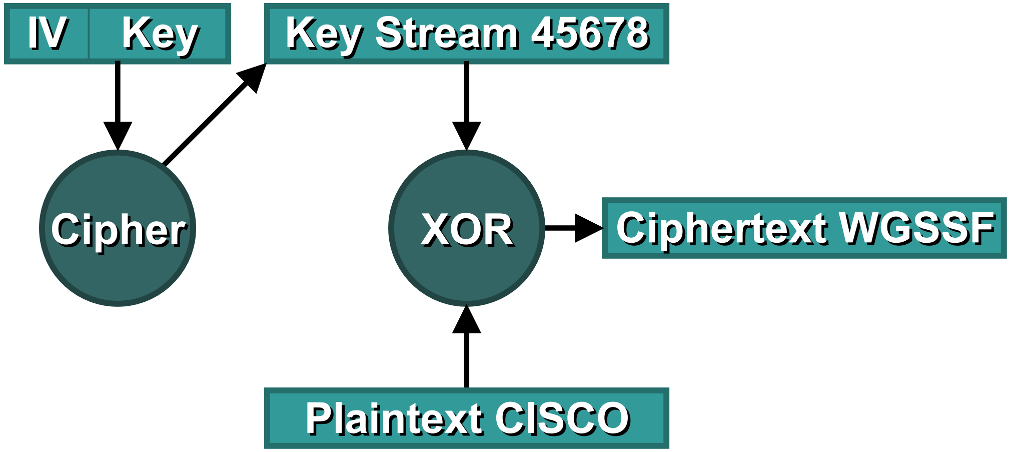
What Is a Stream Cipher?

- Ciphers, like math equations, always produce the same output, given the same input
- This allows eavesdroppers to make educated guesses, and notices changes in the plaintext



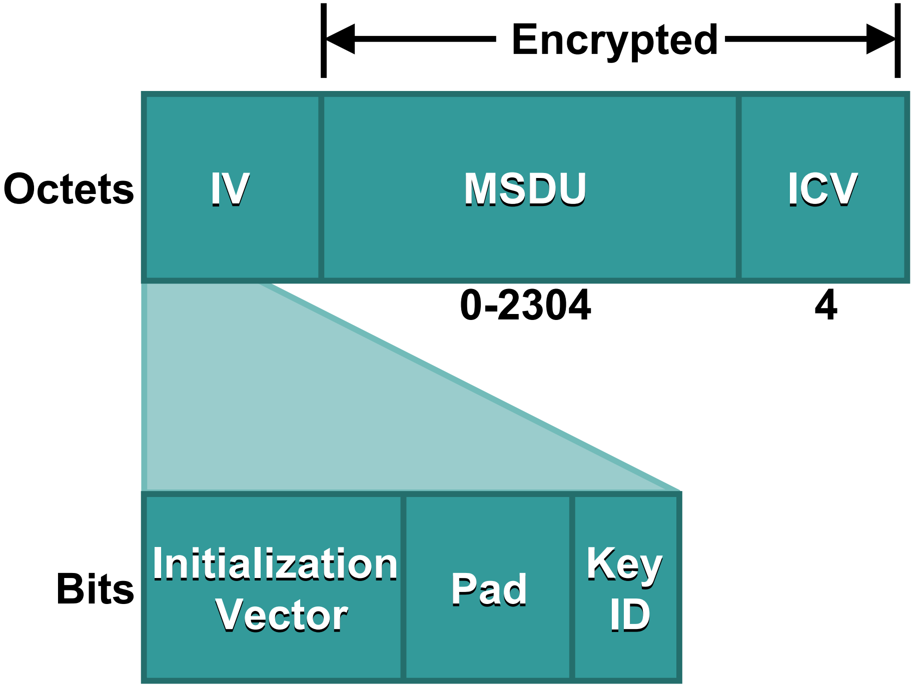
What Is an Initialization Vector?

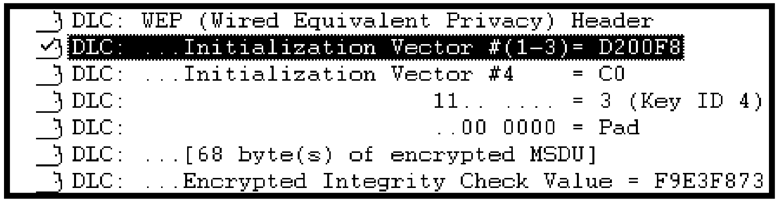
- An initialization vector (IV) is value that alters the key stream
- It augments the key to generate a new key stream
- As the IV changes, so does the key stream



IVs in 802.11 Wireless Security

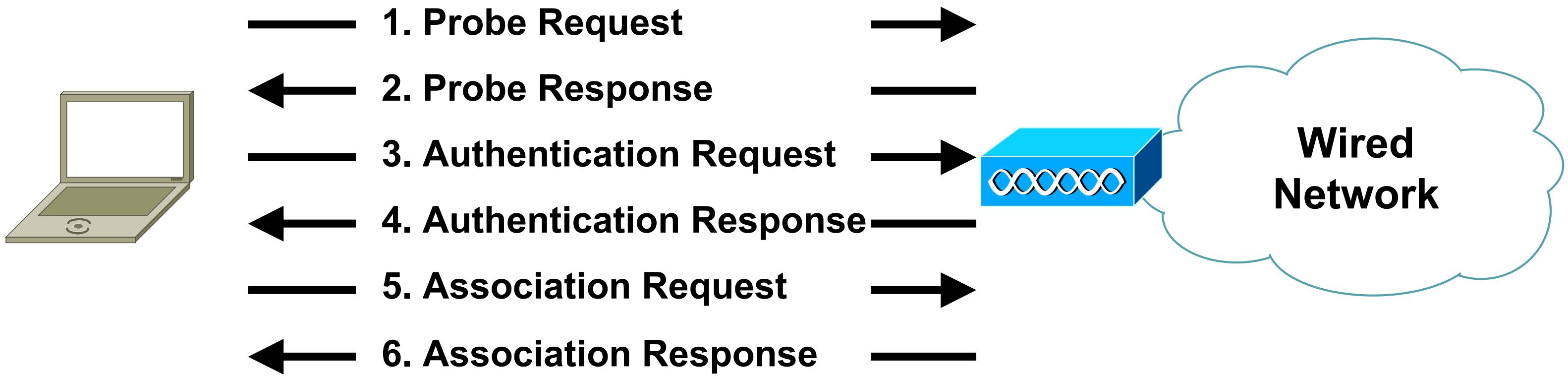
- 802.11 IVs are 24 bit integer values
- Augment 40 bit keys to 64 bits
- Augment 104 bit keys to 128 bits
- Sent in the clear





```
DLC: WEP (Wired Equivalent Privacy) Header
DLC:   ...Initialization Vector #(1-3)= D200F8
DLC:   ...Initialization Vector #4     = C0
DLC:                    11.. ....  = 3 (Key ID 4)
DLC:                    ..00 0000  = Pad
DLC:   ...[68 byte(s) of encrypted MSDU]
DLC:   ...Encrypted Integrity Check Value = F9E3F873
```

802.11 Authentication

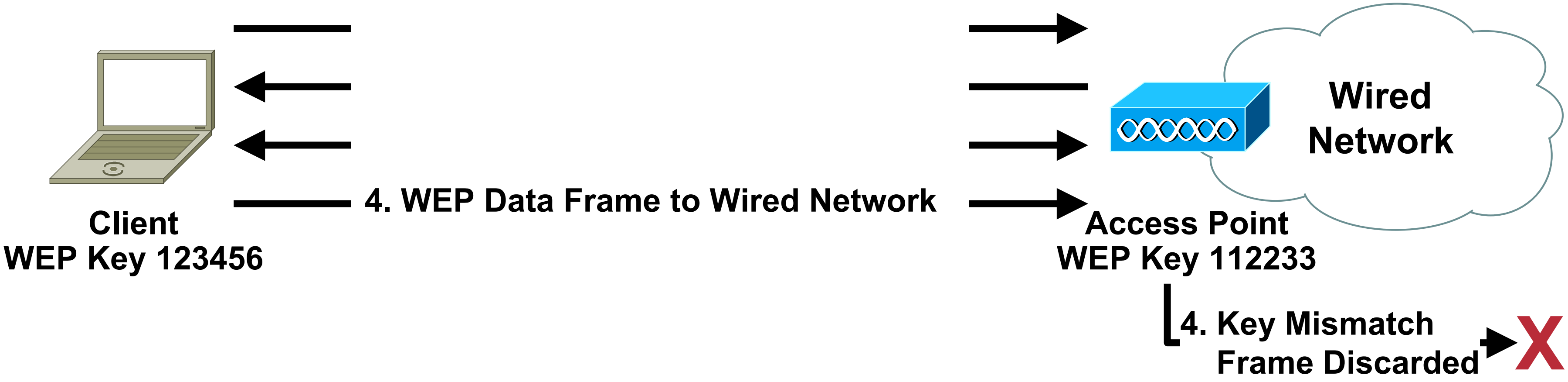


- Client probes for an AP
- Client requests authentication
- Client requests association
- Client can begin data exchange

802.11 Open Authentication

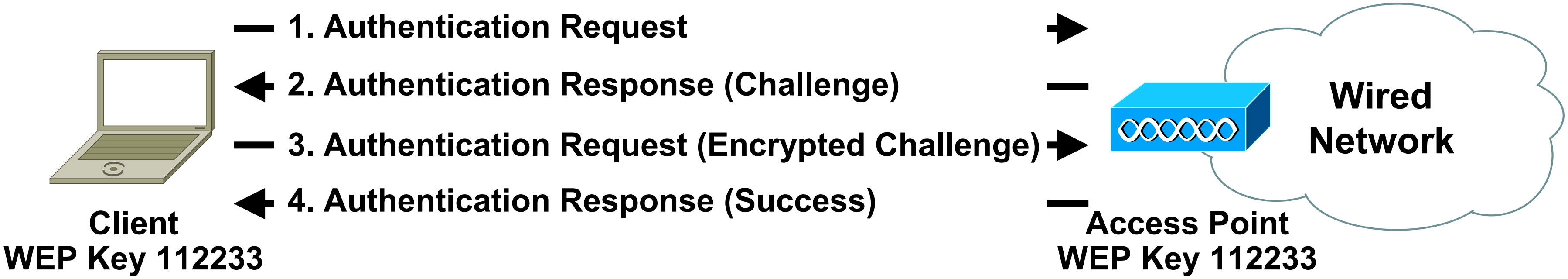
- Device oriented authentication
- Uses null authentication—All requests are granted
- With no WEP, network is wide open to any user
- If WEP encryption is enabled, WEP key becomes indirect authenticator

802.11 Open Authentication



- Client send authentication request
- AP sends Success response
- WEP keys must match for data to traverse AP

802.11 Shared Key Authentication



1. Authentication Request
2. Authentication Response (Challenge)
3. Authentication Request (Encrypted Challenge)
4. Authentication Response (Success)

Client
WEP Key 112233

Access Point
WEP Key 112233

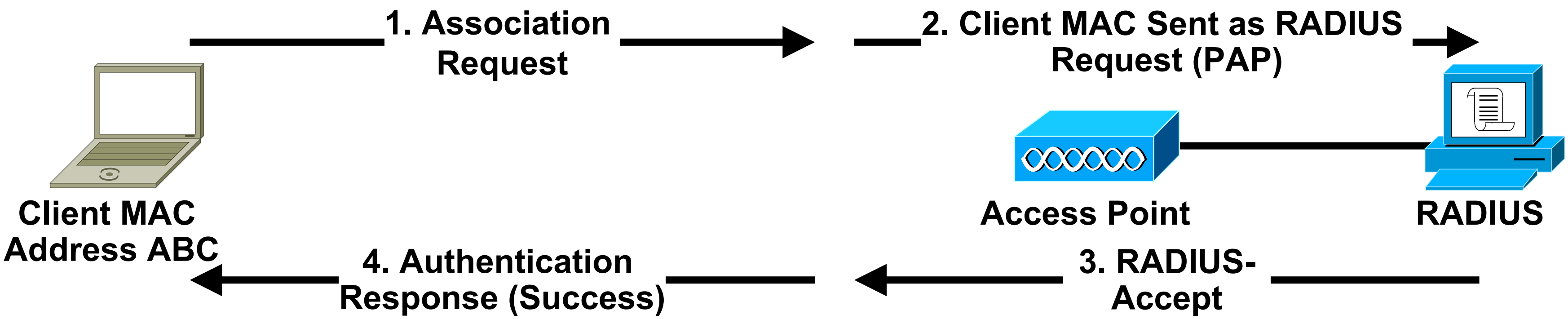
Wired Network

- Client and AP must use WEP with pre-shared keys
- Client requests shared key authentication
- AP sends plaintext challenge
- Client encrypts challenge with WEP key and responds
- If the AP can decrypt the response, client is valid

802.11 MAC Address Authentication

- **Not part of 802.11 specification**
- **Vendor specific implementation**
- **Used to augment Open or Shared Key Authentication**

802.11 MAC Address Authentication


1. Association Request
2. Client MAC Sent as RADIUS Request (PAP)
Client MAC Address ABC
Access Point
RADIUS
4. Authentication Response (Success)
3. RADIUS-Accept

- Client requests authentication
- Client requests association
- AP check MAC against:

  1) Local allowed list

  2) Forward to AAA server
- Accept Association

Wireless Security in 802.11 Summary

- Authentication is device oriented
- Static, pre-shared WEP for encryption
- No key management specified

Agenda

- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

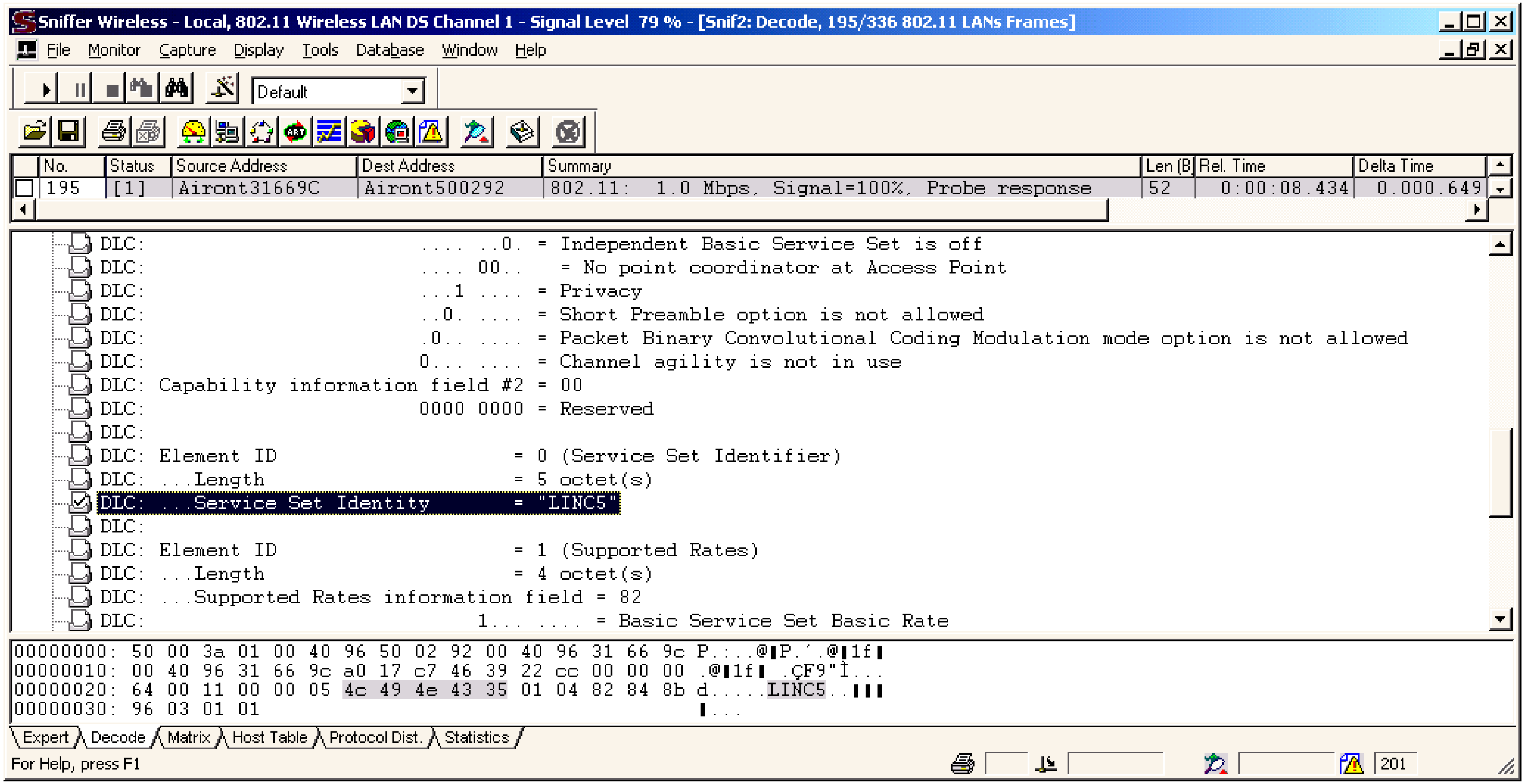
Vulnerabilities in 802.11 Wireless Security

- Authentication Vulnerabilities
- Statistical WEP Key Derivation
- Inductive WEP Key Derivation

Authentication Vulnerabilities

- SSID is not a security mechanism!
- Disabling SSID broadcast in the beacons does not prevent an attacker from seeing them
- Disabling SSID broadcasts may impact WiFi compliance

SSID for Authentication



Sniffer Wireless - Local, 802.11 Wireless LAN DS Channel 1 - Signal Level 79 % - [Snif2: Decode, 195/336 802.11 LANs Frames]

```
No.  Status Source Address  Dest Address   Summary                                             Len (B Rel. Time     Delta Time
195  [1]    Airont31669C    Airont500292   802.11:  1.0 Mbps, Signal=100%, Probe response      52       0:00:08.434  0.000.649
```

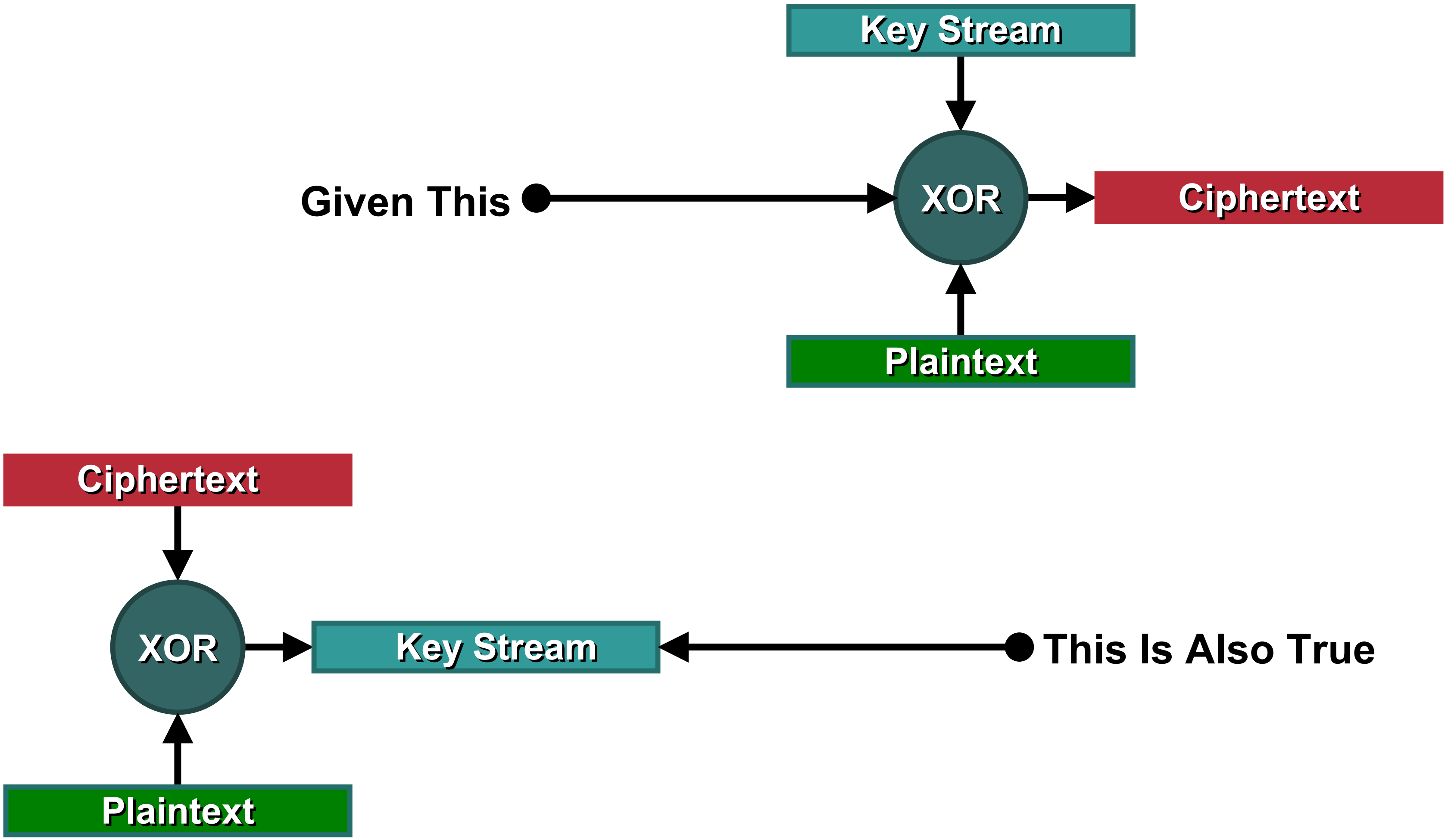
```
DLC:                        .... ..0. = Independent Basic Service Set is off
DLC:                        .... 00..  = No point coordinator at Access Point
DLC:                        ...1 .... = Privacy
DLC:                        ..0. .... = Short Preamble option is not allowed
DLC:                        .0.. .... = Packet Binary Convolutional Coding Modulation mode option is not allowed
DLC:                        0... .... = Channel agility is not in use
DLC: Capability information field #2 = 00
DLC:                        0000 0000 = Reserved
DLC:
DLC: Element ID                       = 0 (Service Set Identifier)
DLC: ...Length                        = 5 octet(s)
DLC: ...Service Set Identity          = "LINC5"
DLC:
DLC: Element ID                       = 1 (Supported Rates)
DLC: ...Length                        = 4 octet(s)
DLC: ...Supported Rates information field = 82
DLC:                           1... .... = Basic Service Set Basic Rate
```

```
00000000: 50 00 3a 01 00 40 96 50 02 92 00 40 96 31 66 9c P.:..@▌P.´.@▌1f▌
00000010: 00 40 96 31 66 9c a0 17 c7 46 39 22 cc 00 00 00 .@▌1f▌ .ÇF9"Ì...
00000020: 64 00 11 00 00 05 4c 49 4e 43 35 01 04 82 84 8b d.....LINC5..▌▌▌
00000030: 96 03 01 01                                     ▌...
```

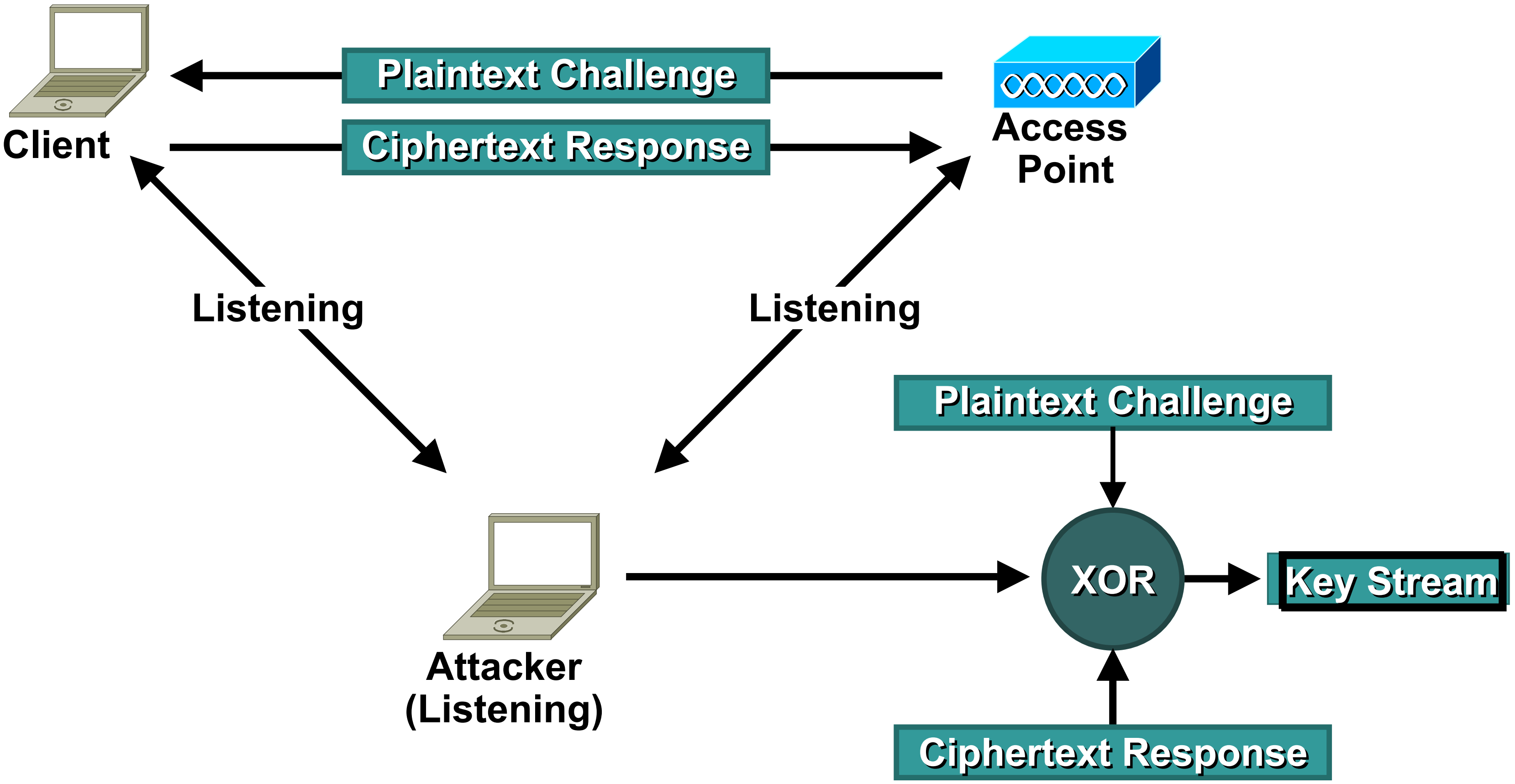
Authentication Vulnerabilities

- Wireless NIC is authenticated, not the user
- Unauthorized users can use authorized devices
  - Lost or stolen laptop
  - Disgruntled Employees

Authentication Vulnerabilities



Authentication Vulnerabilities



- **Shared Key is vulnerable to Man in the Middle Attack**

Authentication Vulnerabilities

- MAC Authentication is weak
- MAC addresses are sent in the clear
- MAC addresses can be sniffed and spoofed

Statistical Key Derivation

- 802.11 WEP is flawed
- A WEP key can be derived in 1M to 4M frames using statistical analysis
- Attacker is passive, and ‘listens’ to wireless LAN
- Implemented in the AirSnort application

Inductive Key Derivation

- An attacker can derive the key by soliciting info from a wireless LAN
- Common Methods

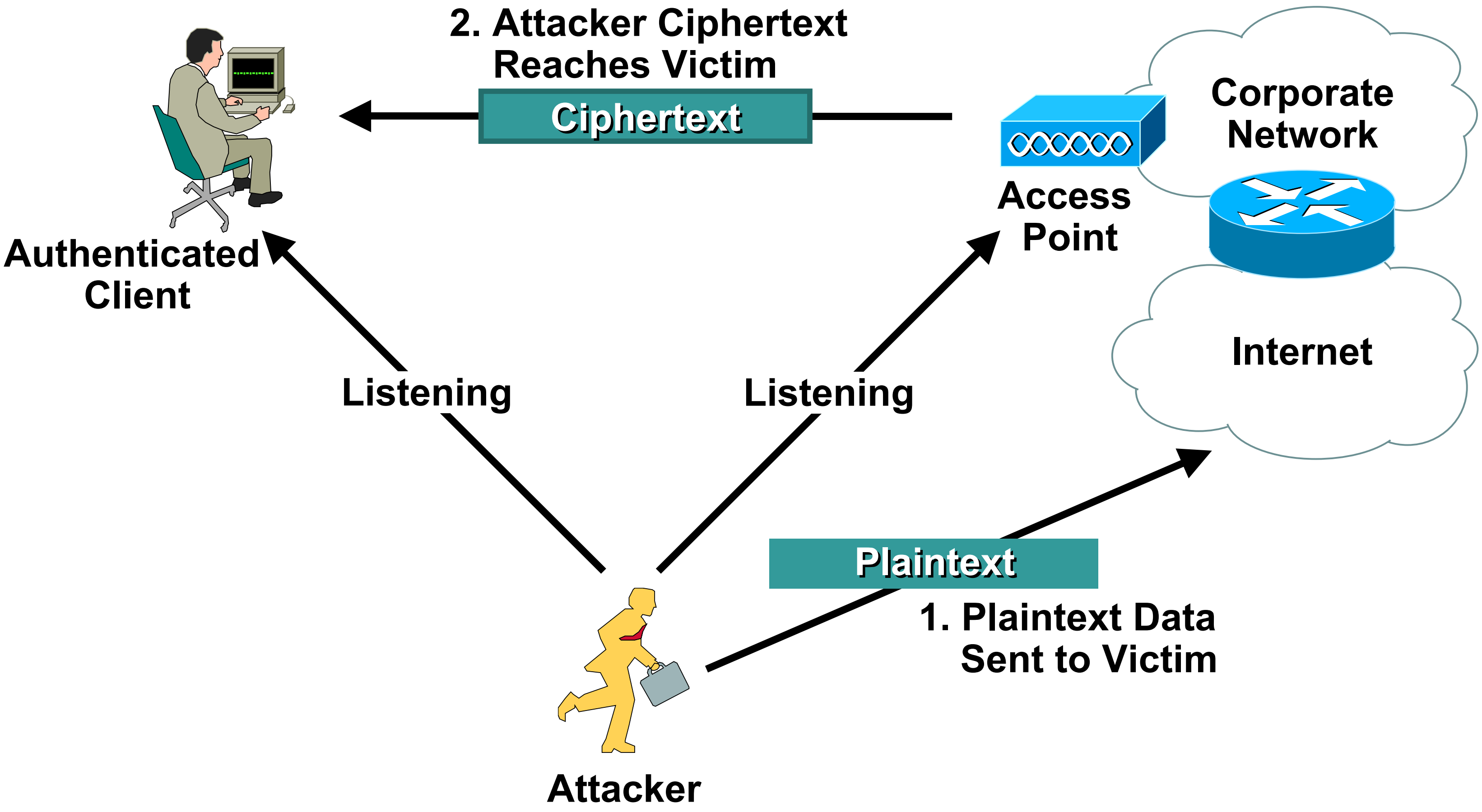
  IV/WEP Key Replay

  Frame Bit Flipping

IV/WEP Key Reuse Vulnerability

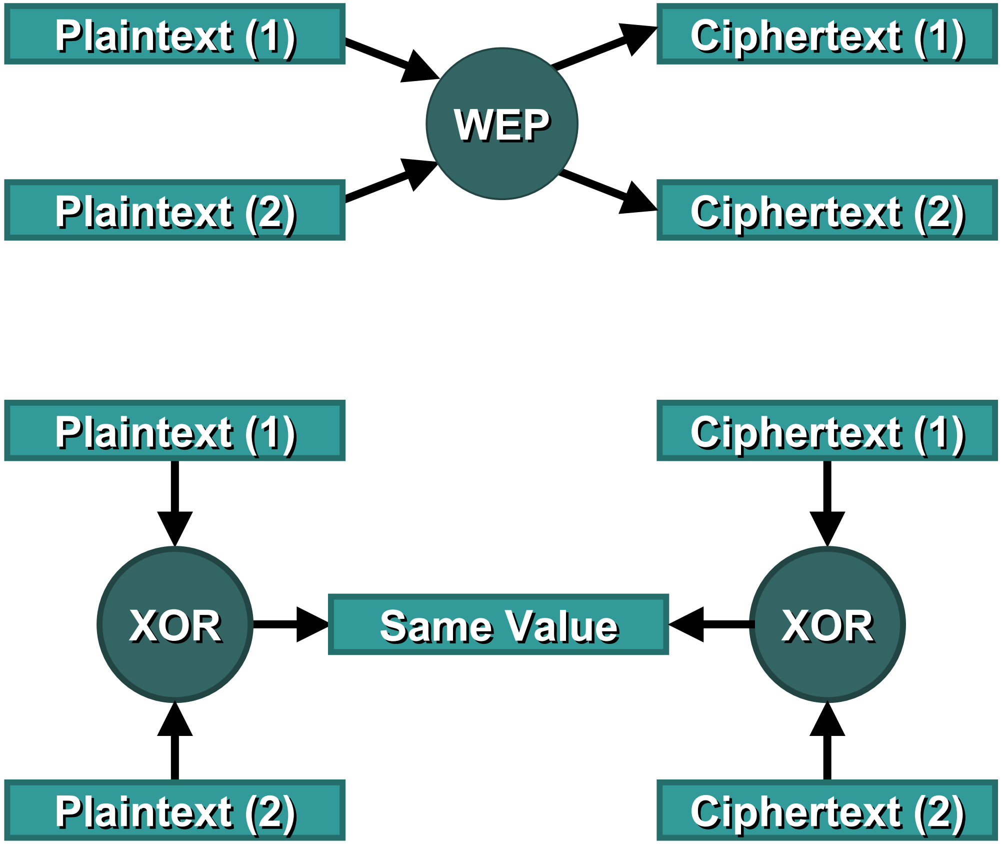
- Attacker can send a known plaintext to an observable wireless client (i.e. via email)
- Attacker will ‘listen’ to wireless LAN, waiting to see predicted ciphertext
- Once attacker ‘sees’ the ciphertext, key stream is derived
- Key stream is valid only for the specific IV

IV/WEP Key Reuse Vulnerability



IV/WEP Key Reuse Vulnerability

- Two plaintexts XORed have the same output as their ciphertexts XORed
- This enhances a snoopers chances of predicting the plaintext



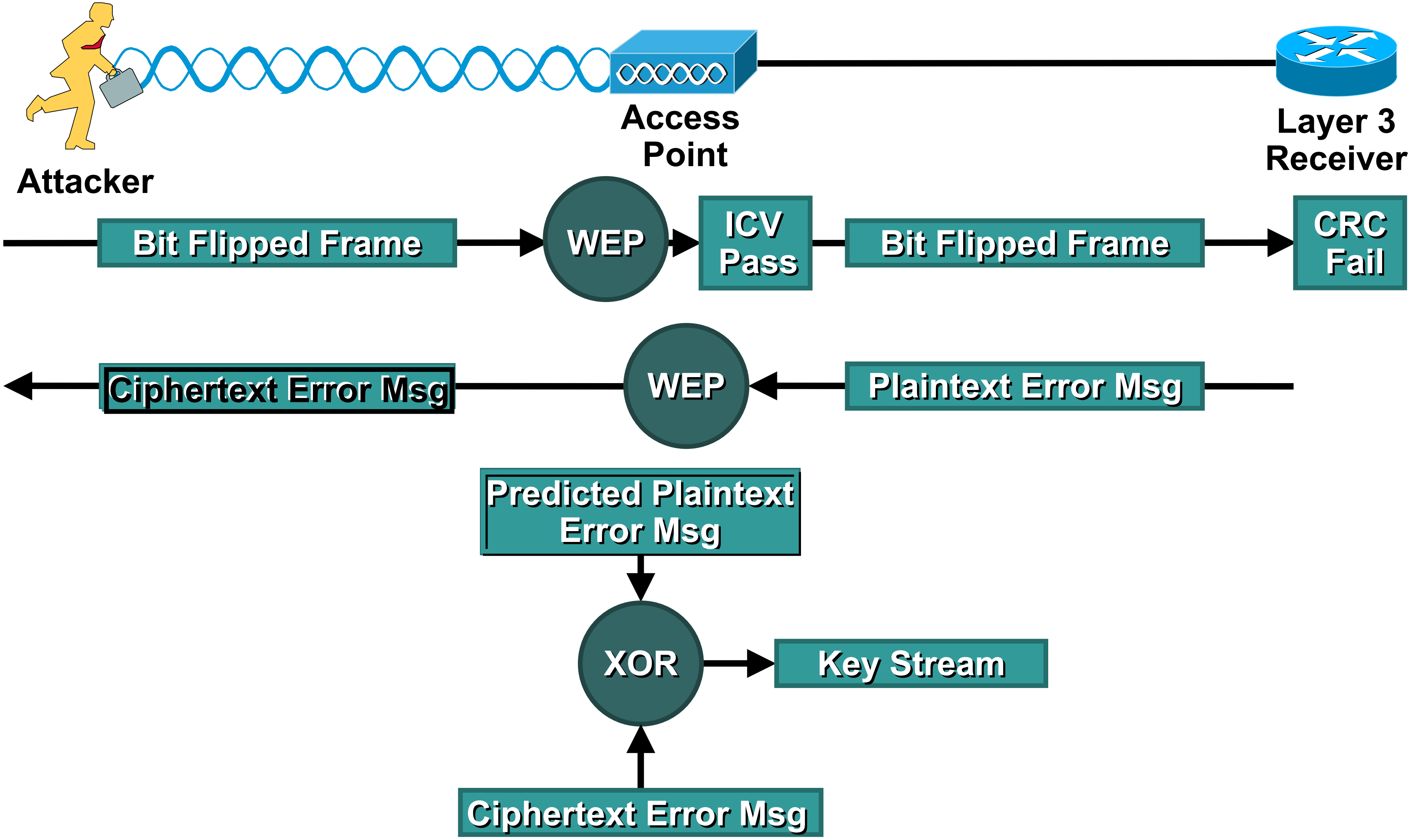
Bit Flipping Vulnerability

- Attacker captures a frame from a wireless LAN
- The frame is modified by flipping bits
- Attacker predicts a high layer error
- Attacker waits for predicted error ciphertext
- The key stream is derived upon ‘seeing’ predicted ciphertext

Bit Flipping Vulnerability

- Integrity Check Value (ICV) based on CRC-32 polynomial
- Known mathematical flaw with ICV allows changes to the encrypted frame and ICV
- AP and or client will accept the frame as valid due to this flaw

Bit Flipping Vulnerability



Attacker

Access Point

Layer 3 Receiver

Bit Flipped Frame

WEP

ICV Pass

Bit Flipped Frame

CRC Fail

Ciphertext Error Msg

WEP

Plaintext Error Msg

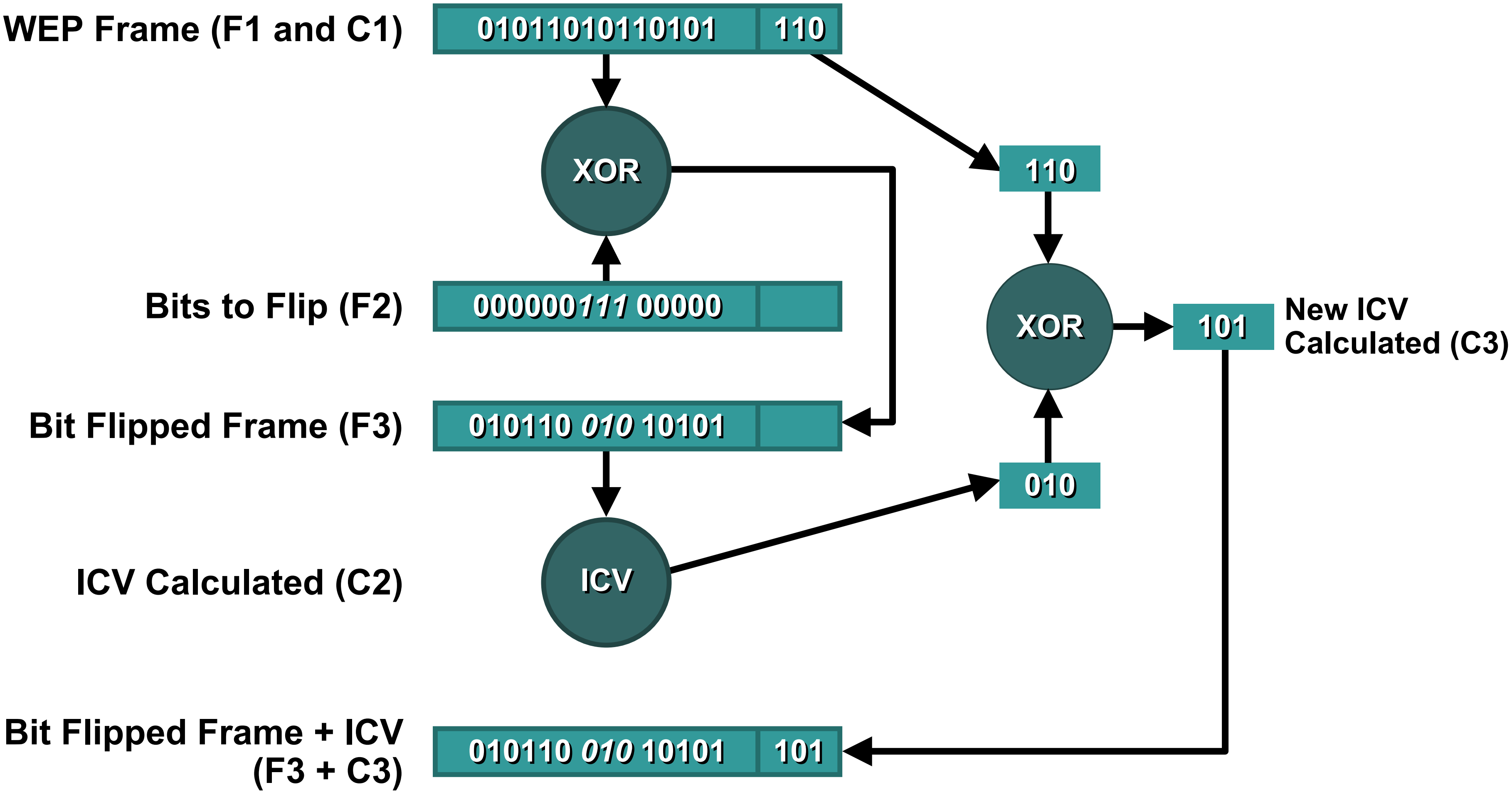
Predicted Plaintext Error Msg

XOR

Key Stream

Ciphertext Error Msg

Bit Flipping Process



802.11 Security Summary

- The security mechanisms in the 1997 802.11 specification are flawed

    Open authentication

    Shared Key authentication

    WEP

- These will NOT secure your wireless LAN!!

802.11 Security Summary

- Requirements for wireless authentication

    User-based, centralized, strong authentication

    Mutual authentication of client and network

- Requirements for wireless privacy

    Strong, effective encryption

    Effective message integrity check

    Centralized, dynamic WEP key management

Agenda

- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

Secure Wireless LANs
User Considerations

- Single sign on
- Extensible authentication support
- Minimal security overhead

Secure Wireless LANs Infrastructure Considerations

- Cost
  - Additional Server Hardware
  - Additional Network Infrastructure
- Rapid Deployment
- Maintenance and Support
  - Impact to client and infrastructure
- Future 802.11 Enhancements
  - Interoperability with enhancements

Technologies for Secure Wireless LANs

- VPN
- 802.1X with TKIP encryption

Secure Authentication Requirements

- Centralized authentication via AAA server
- Mutual authentication of client and network
- Support for dynamic, user-based encryption keys
    - Optional capability to change keys

VPN over 802.11

- Two phase authentication
  - Device authentication via pre-shared key or PKI
  - User authentication via AAA server
- Mutual authentication
- Extensible user authentication types

802.1x Standard

Port-Based Network Access Control

- Falls under 802.1 not 802.11
- This is a network standard, not a wireless standard
- Is part of the 802.11i draft
- Provides network authentication, not encryption
- Incorporated as part of LEAP

802.1x Overview

- Standard set by the IEEE 802.1 working group
- Describes a standard link layer protocol used for transporting higher-level authentication protocols
- Works between the supplicant (client) and the authenticator (network device)
- Maintains backend communication to an authentication (RADIUS) server

EAP Overview

- EAP—The Extensible Authentication Protocol
- A flexible protocol used to carry arbitrary authentication information
- Typically rides on top of another protocol such as 802.1x or RADIUS (could be TACACS+, etc.)
- Specified in RFC 2284
- Support multiple "authentication" types:
  - Plain password hash (MD5) (not mutual)
  - OTP Tokens (not mutual)
  - TLS (based on X.509 certificates)
  - And EAP-Cisco Wireless!!

802.1x and EAP

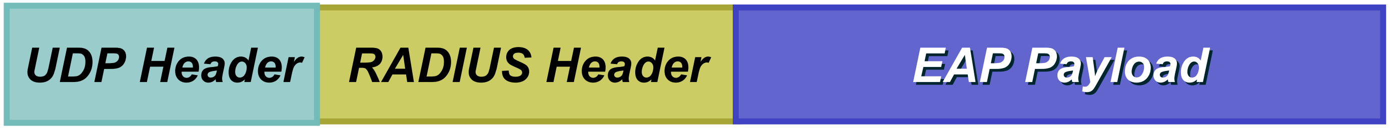
- 802.1x Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- The authenticator (AP or switch) becomes the middleman for relaying EAP received in 802.1x packets to an authentication server by using RADIUS to carry the EAP information
- Three forms of EAP are specified in the 802.1x standard
  - EAP-MD5—MD5 Hashed Username/Password
  - EAP-OTP—One-Time Passwords
  - EAP-TLS—Strong PKI Authenticated Transport Layer Security (TLS)

802.1x Header

EAP Payload

802.1x, EAP and RADIUS

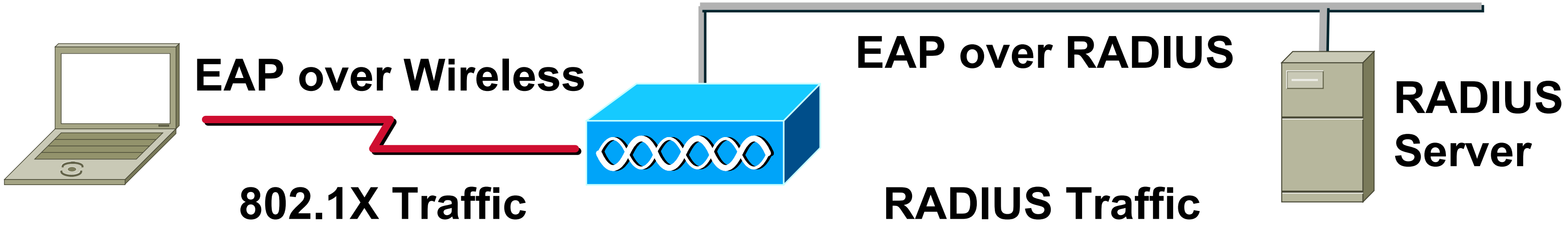
- RADIUS—The Remote Authentication Dial In User Service
- A protocol used to communicate between a network device and an authentication server or database
- Allows the communication of login and authentication information; i.e., username/password, OTP, etc.
- Allows the communication of arbitrary value pairs using “Vendor Specific Attributes” (VSAs)
- Can also act as a transport for EAP messages

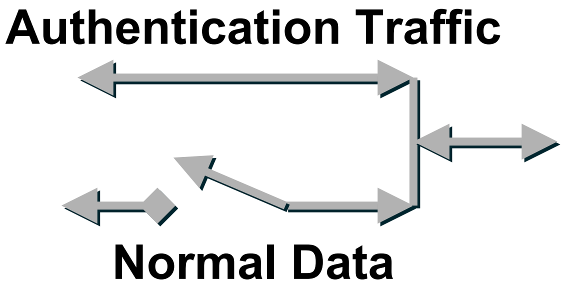


UDP Header | *RADIUS Header* | *EAP Payload*

802.1x / EAP Authentication

802.11 Association Complete; Data Blocked by AP

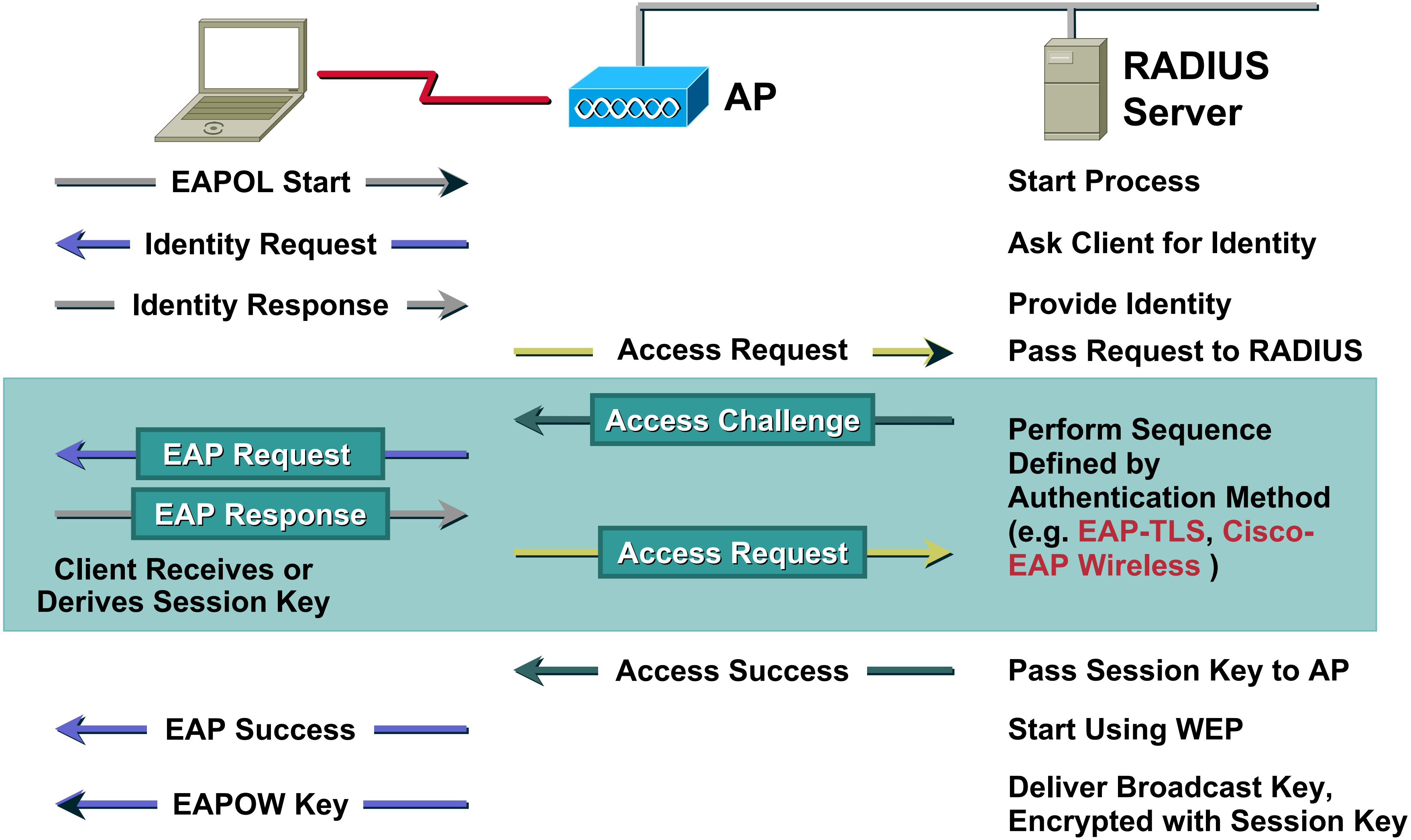




AP "Encapsulates" 802.1x Traffic into RADIUS Traffic, and Visa Versa

AP Blocks Everything but 802.1x-to-RADIUS Authentication Traffic

802.1x / EAP Authentication Steps



AP

RADIUS Server

EAPOL Start — Start Process

Identity Request — Ask Client for Identity

Identity Response — Provide Identity

Access Request — Pass Request to RADIUS

Access Challenge

EAP Request

EAP Response

Access Request

Perform Sequence Defined by Authentication Method (e.g. EAP-TLS, Cisco-EAP Wireless)

Client Receives or Derives Session Key

Access Success — Pass Session Key to AP

EAP Success — Start Using WEP

EAPOW Key — Deliver Broadcast Key, Encrypted with Session Key

802.1x for Wireless LANs

- Cisco has led the way with EAP-Cisco Wireless (LEAP)
- Multiple wireless vendors have adopted 802.1x for WLANs
- 802.1X authentication protocols include EAP-Cisco Wireless, EAP-TLS, EAP-MD5, TTLS, and PEAP
- Microsoft has integrated support for EAP-TLS and EAP-MD5 into Windows XP operating system

  Also has announced support for EAP on native platforms (Windows 2000, Windows NT 4, Windows 98 and Windows ME)

EAP Authentication Types for Wireless LANs

- EAP-Cisco (aka LEAP)

  Password-based

- EAP-TLS (Transport Layer Security)

  Certificates-based

- EAP-PEAP (Protected EAP)

  Hybrid—Certificate/Password

- EAP-TTLS (Tunneled TLS)

  Hybrid—Certificate/Password

- EAP-SIM (SIM Card)

  Authentication by SIM Cards

EAP-Cisco Authentication

- Client Support

  Windows 95-XP

  Windows CE

  Macintosh OS 9.X and 10.X

  Linux

- Device Support

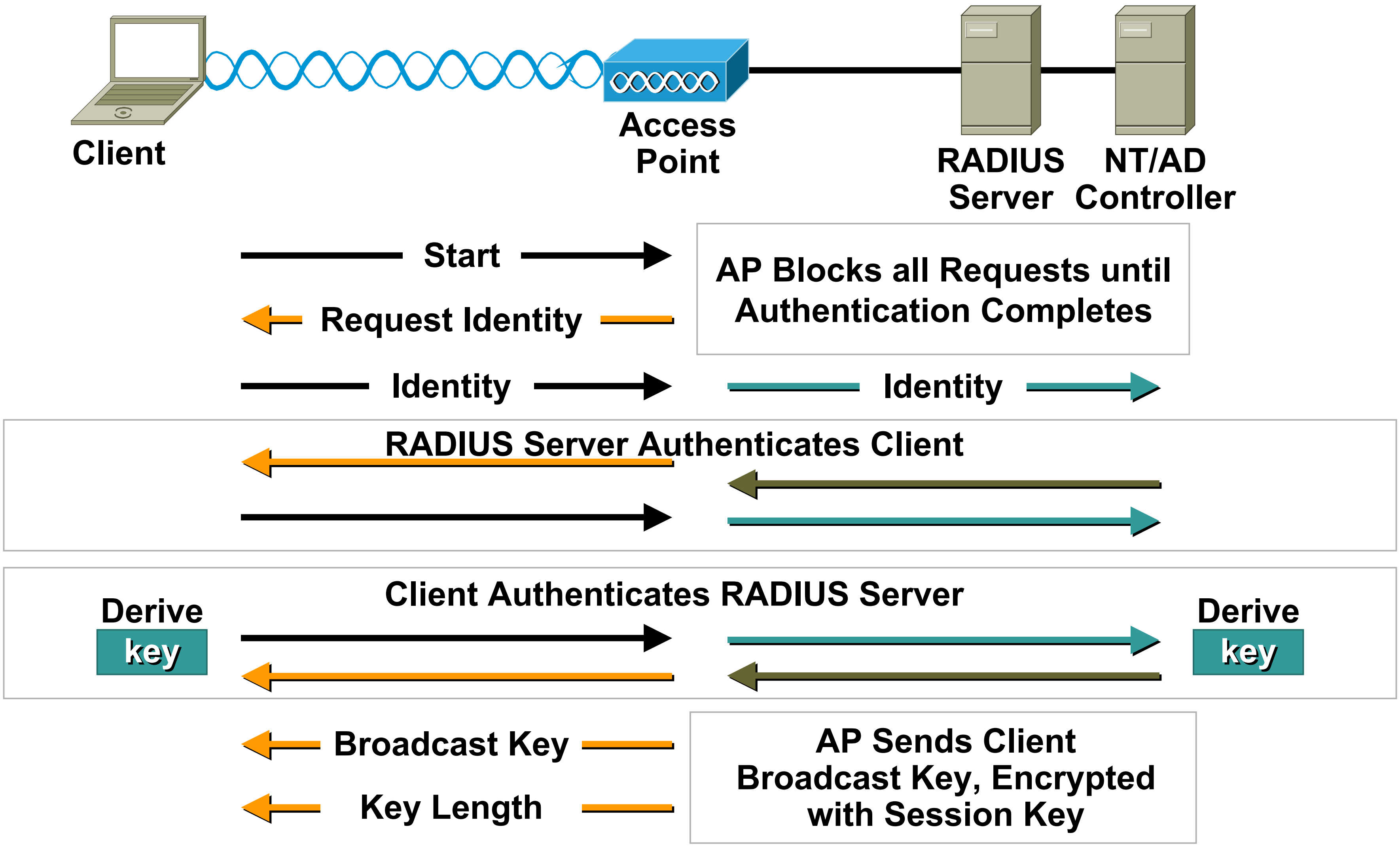
  Workgroup Bridges (WGB 340 and 350)

  Point to Point Bridges (BR350 series)

EAP-Cisco Authentication

- RADIUS Server
  - Cisco ACS
  - Cisco AR
  - Funk Steel Belted RADIUS
  - Interlink Merit
- Microsoft Domain or Active Directory (optional) for back end authentication

EAP-Cisco Authentication



AP Blocks all Requests until Authentication Completes

RADIUS Server Authenticates Client

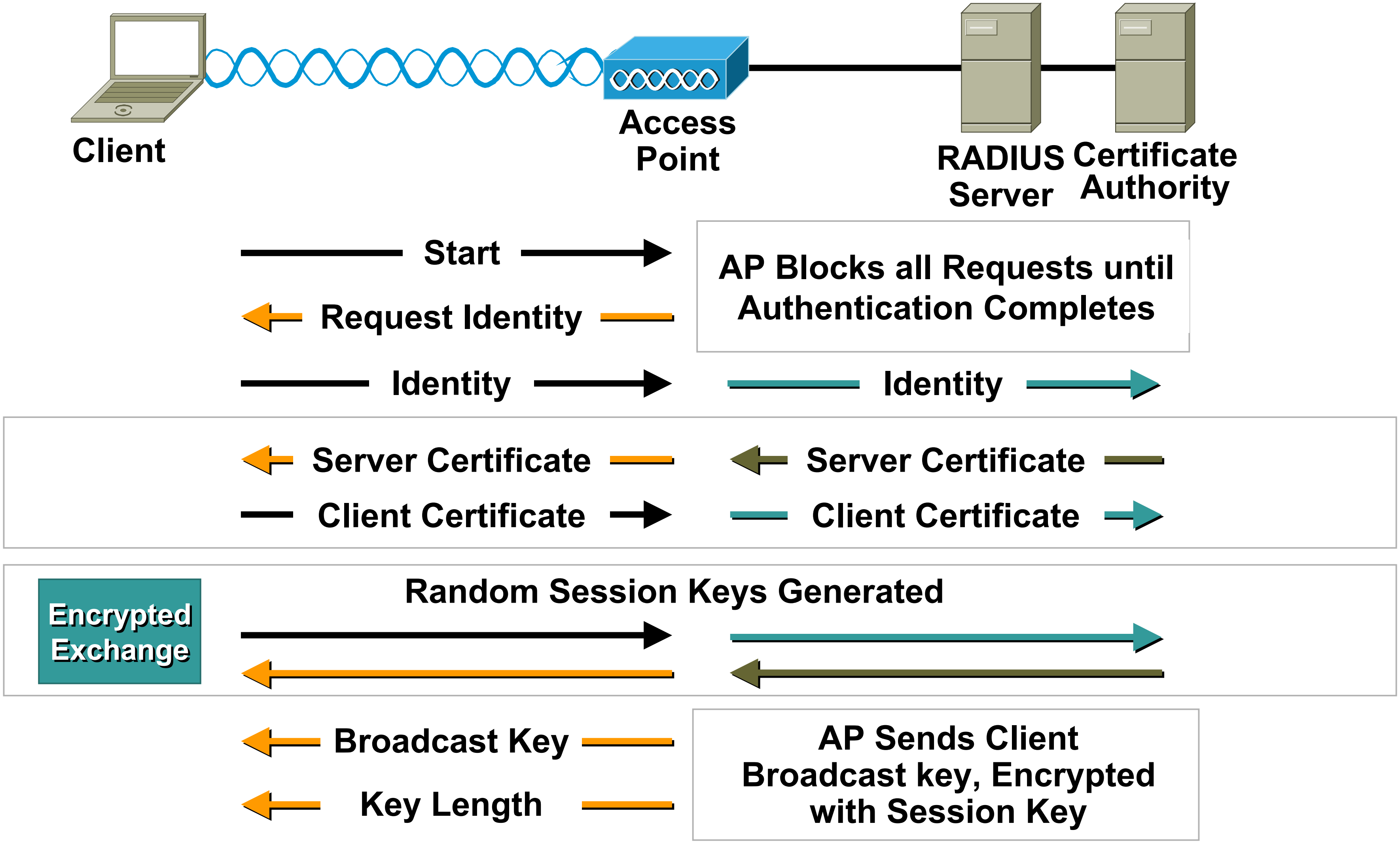
Client Authenticates RADIUS Server

AP Sends Client Broadcast Key, Encrypted with Session Key

EAP-TLS Authentication

- Client Support
  - Windows 2000, XP
  - Clients require a local user or machine certificate
- Infrastructure Requirements
  - EAP-TLS supported RADIUS server
    - Cisco ACS, Cisco AR, MS IAS
    - RADIUS server requires a server certificate
  - Certificate Authority Server
    - Windows 2000 Server

EAP-TLS Authentication



Client

Access Point

RADIUS Server

Certificate Authority

Start

Request Identity

AP Blocks all Requests until Authentication Completes

Identity

Identity

Server Certificate

Server Certificate

Client Certificate

Client Certificate

Encrypted Exchange

Random Session Keys Generated

Broadcast Key

Key Length

AP Sends Client Broadcast key, Encrypted with Session Key

Hybrid Authentication

- EAP-TTLS

  Server side authentication with TLS

  Client side authentication with legacy authentication types (CHAP, PAP, etc)

- EAP-PEAP

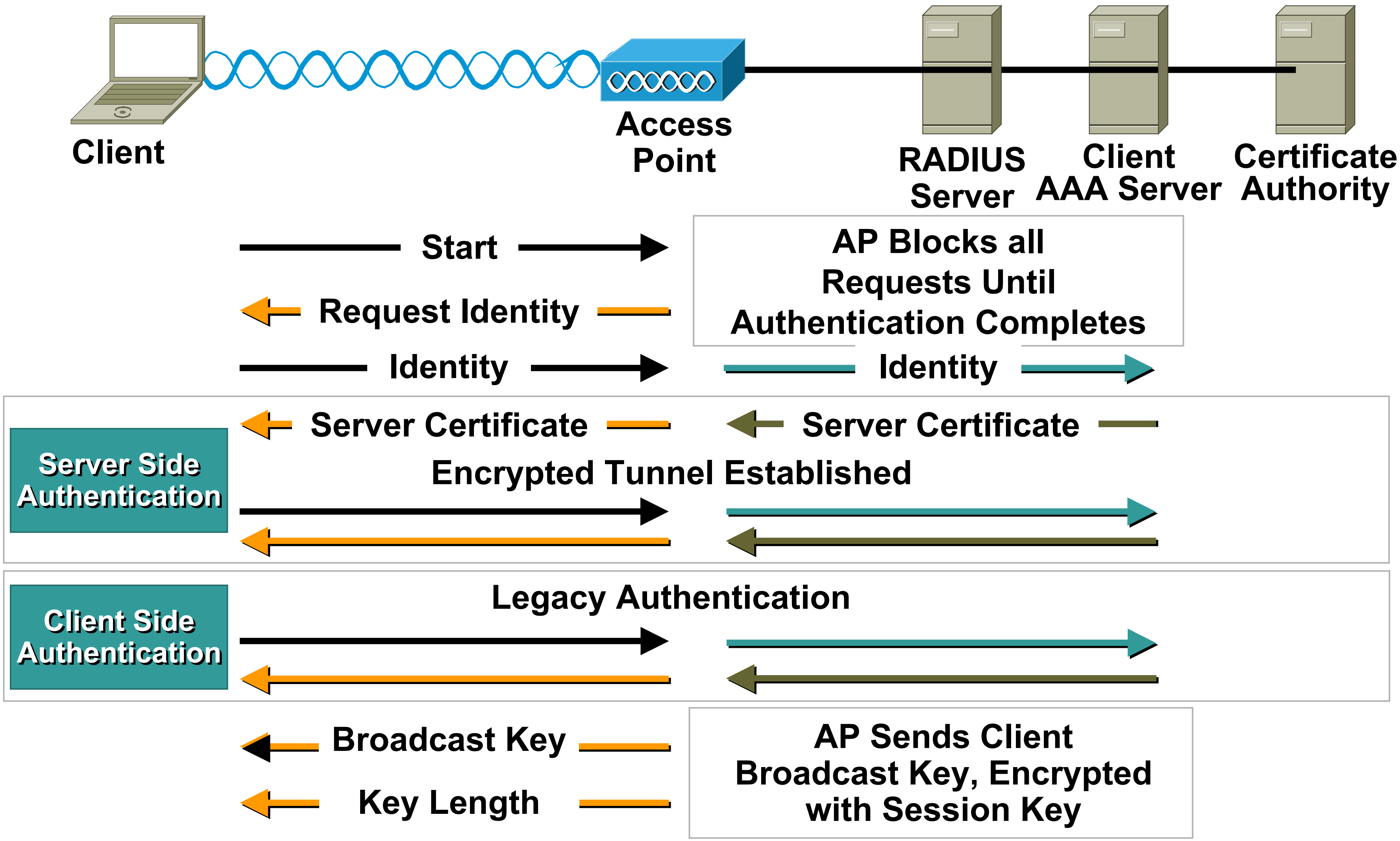
  Server side authentication with TLS

  Client side authentication with EAP authentication types (EAP-GTC, EAP-MD5, etc)

Hybrid Authentication

- Both require CA, as with EAP-TLS
- Clients do not require certificates
  - Simplifies end user/device management
- Allows for one way authentication types to be used
  - One Time Passwords
  - Proxy to LDAP, Unix, NT/AD, Kerberos, etc

EAP-TTLS Authentication



Client

Access Point

RADIUS Server

Client AAA Server

Certificate Authority

Start

Request Identity

AP Blocks all Requests Until Authentication Completes

Identity

Identity

Server Side Authentication

Server Certificate

Server Certificate

Encrypted Tunnel Established

Client Side Authentication

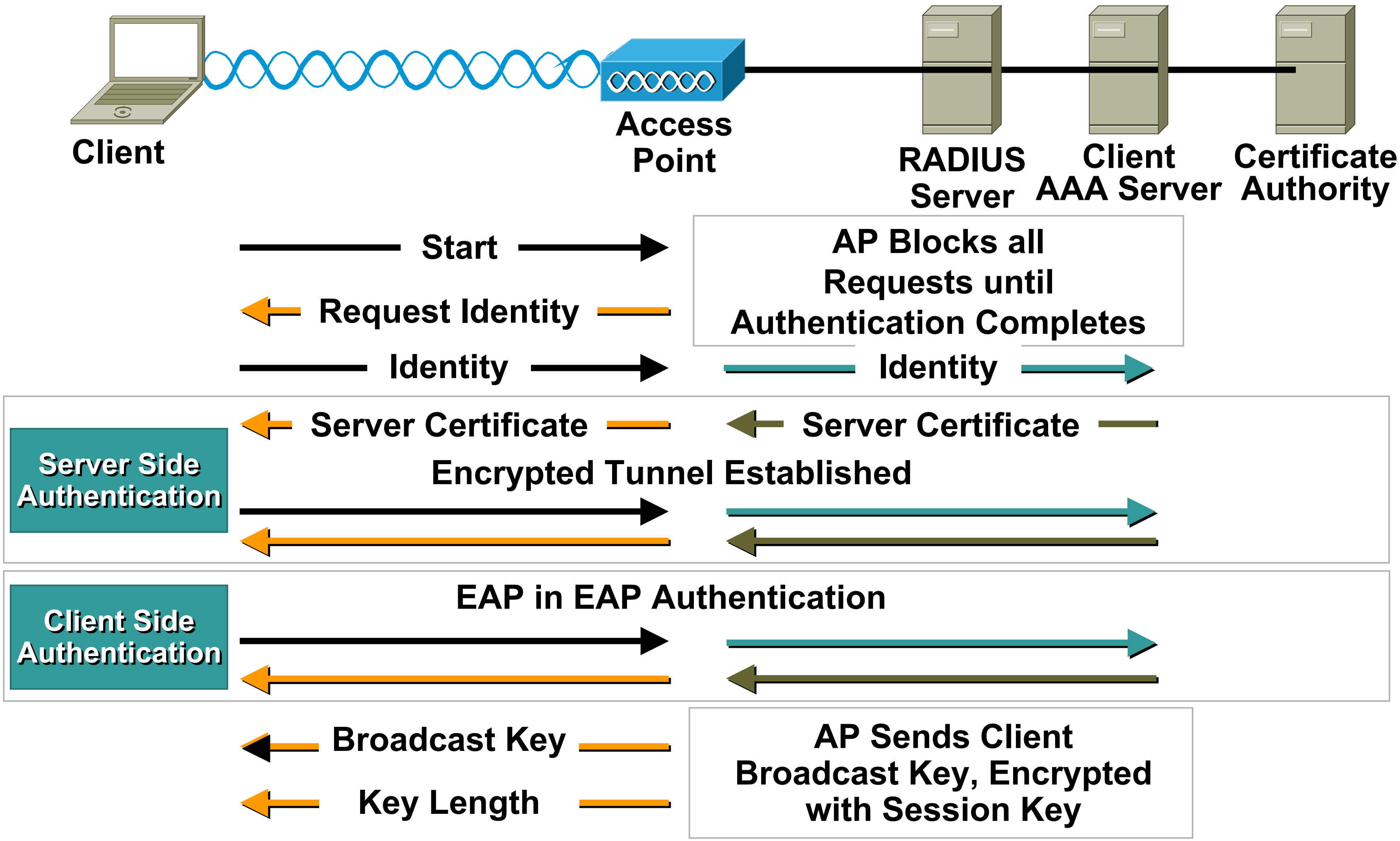
Legacy Authentication

Broadcast Key

Key Length

AP Sends Client Broadcast Key, Encrypted with Session Key

EAP-PEAP Authentication



Client

Access Point

RADIUS Server

Client AAA Server

Certificate Authority

Start

Request Identity

AP Blocks all Requests until Authentication Completes

Identity

Identity

Server Side Authentication

Server Certificate

Server Certificate

Encrypted Tunnel Established

Client Side Authentication

EAP in EAP Authentication

Broadcast Key

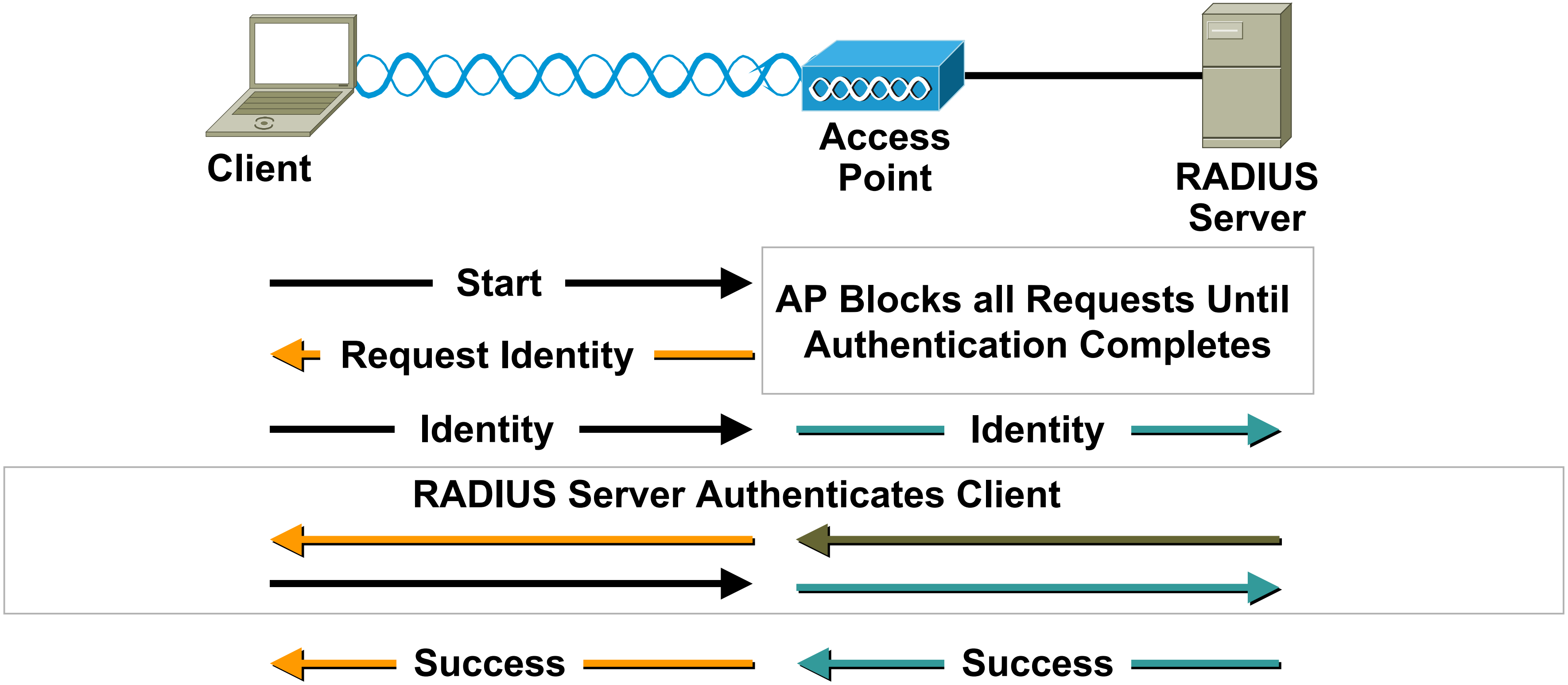
Key Length

AP Sends Client Broadcast Key, Encrypted with Session Key

EAP-MD5 Authentication

- An example of what **NOT** to use in a WLAN
- One way authentication
    - Network authenticates client
- No support for dynamic keys

EAP-MD5 Authentication



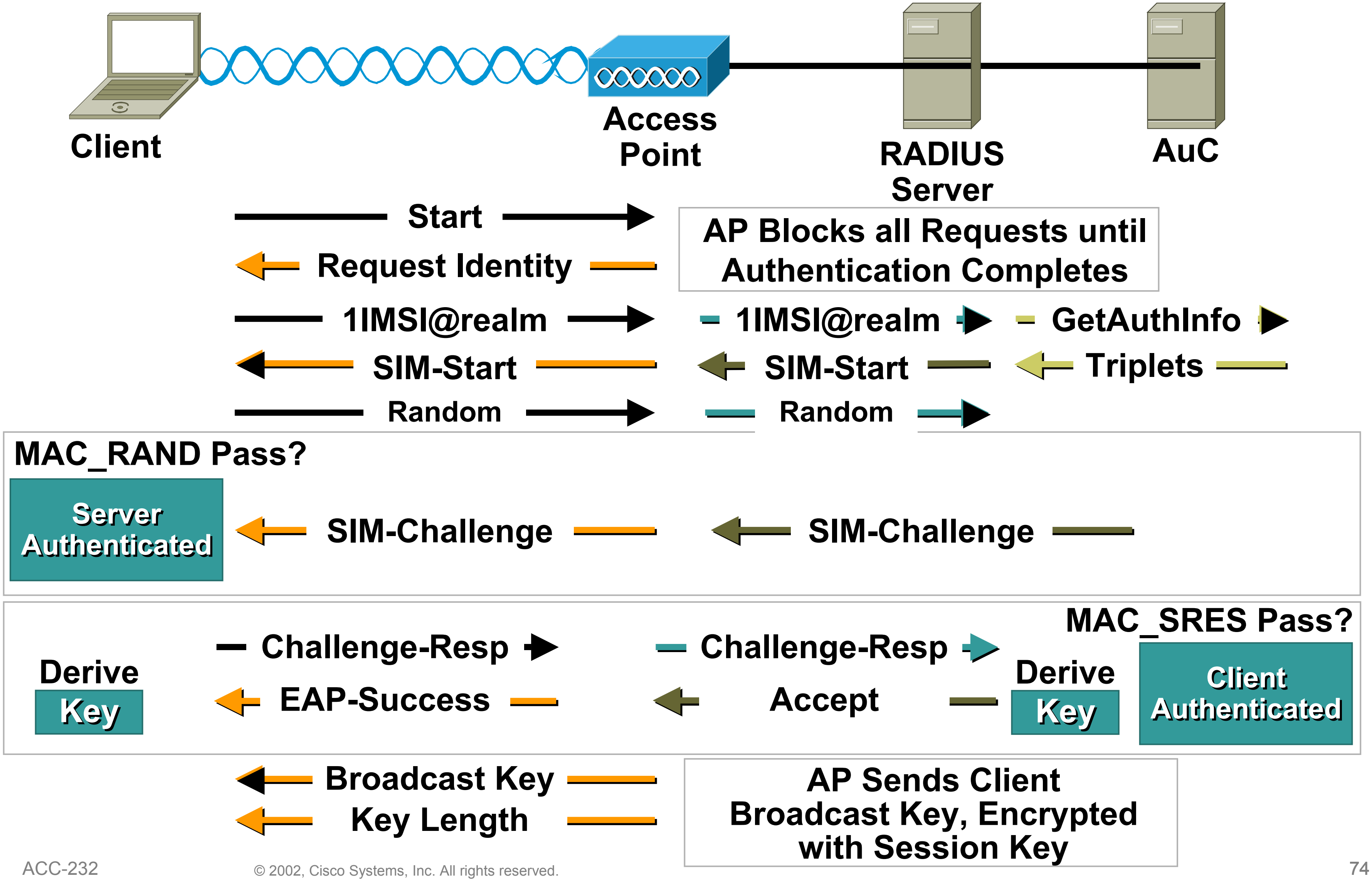
AP Blocks all Requests Until Authentication Completes

RADIUS Server Authenticates Client

EAP-SIM Authentication Overview

- User authentication performed based on an IMSI in the SIM card which is used to authenticate GSM phones today
- Strong Authentication Using 802.1x
  - Mutual authentication (not currently implemented)
  - One time password algorithm
  - Dynamic WEP keys
- Back-end Integration
  - Uses existing GSM operator provisioning chain
  - Leverage existing roaming agreements
  - Leverage existing authentication and billing infrastructure

EAP-SIM Authentication



Client

Access Point

RADIUS Server

AuC

Start

Request Identity

AP Blocks all Requests until Authentication Completes

1IMSI@realm

1IMSI@realm

GetAuthInfo

SIM-Start

SIM-Start

Triplets

Random

Random

MAC_RAND Pass?

Server Authenticated

SIM-Challenge

SIM-Challenge

MAC_SRES Pass?

Challenge-Resp

Challenge-Resp

Derive Key

EAP-Success

Accept

Derive Key

Client Authenticated

Broadcast Key

Key Length

AP Sends Client Broadcast Key, Encrypted with Session Key

Authentication Attack Mitigation

	EAP-MD5	EAP-Cisco	EAP-TLS	EAP-TTLS/PEAP	VPN
Rogue APs		X			
Session Hijacking		X			
Man in the Middle		X			
Dictionary Attack	X*	X*			

X: Mitigates Vulnerability

***Requires the Use of Strong Passwords**

Strong Encryption Requirements

- Cryptographically sound encryption algorithm
- Effective message integrity

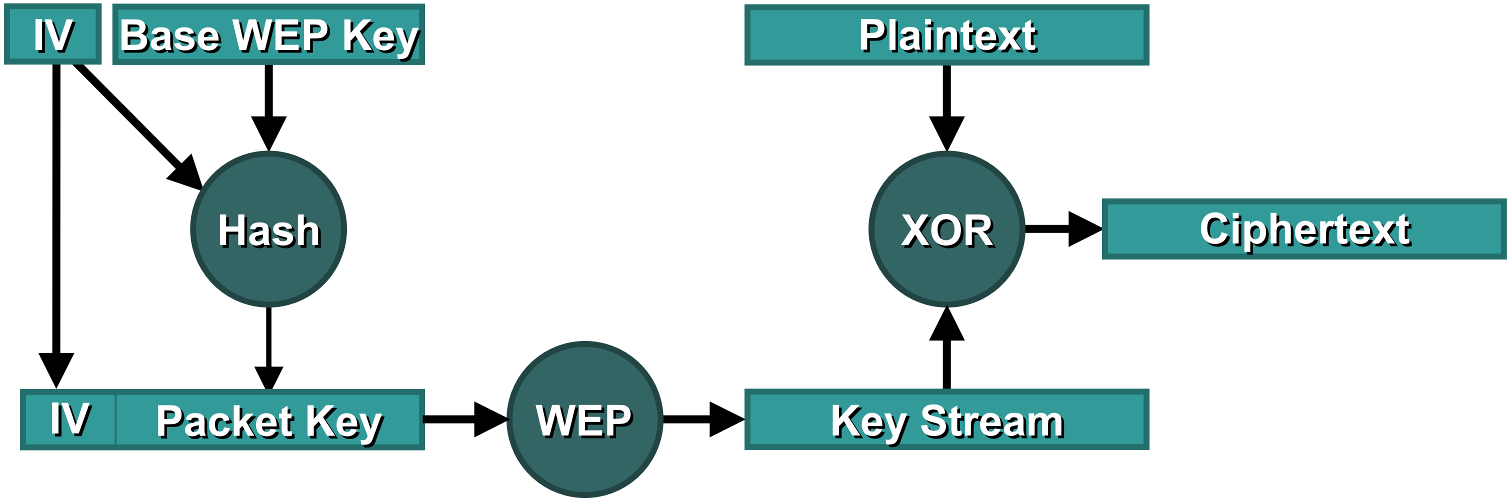
Strong Encryption

- Temporal Key Integrity Protocol (TKIP)
  - Enhances WEP encryption
  - Per Packet Keying
  - Message Integrity Check
- VPN over Wireless
  - 3DES encryption—Tried and true
  - HMAC-SHA1 or HMAC-MD5 message authentication

TKIP Encryption

- Cisco offers a pre-standards implementation
- Per Packet Keying
- Message Integrity Check
- Broadcast Key Rotation

Per Packet Keying Operation



- IV Sequencing—IVs increment by one
- Per Packet IV is hashed with base WEP key
- Result is a new ‘Packet’ WEP key
- The Packet WEP key changes per IV

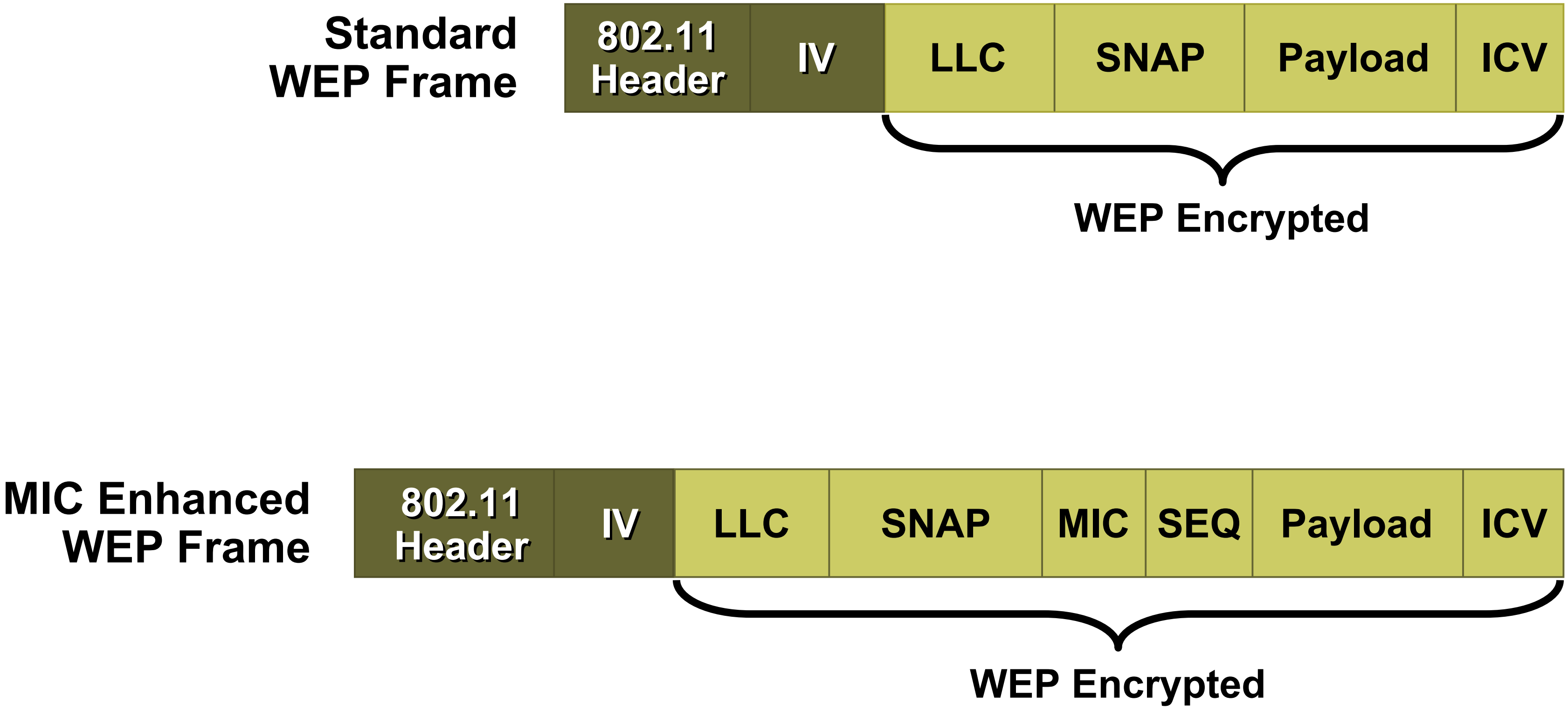
Per Packet Keying Caveats

- Packet key remains unique as long as IV is unique
- 802.11 IV has 2^24 possible integers (roughly 0 to 16.7M)
- Base WEP key must be changed via 802.1X in order to avoid IV/Packet key stream derivation

Message Integrity Check (MIC)

- Prevents IV/WEP key reuse
- Prevents frame tampering

Message Integrity Check (MIC)



Standard WEP Frame

802.11 Header	IV	LLC	SNAP	Payload	ICV

WEP Encrypted

MIC Enhanced WEP Frame

802.11 Header	IV	LLC	SNAP	MIC	SEQ	Payload	ICV

WEP Encrypted

Message Integrity Check (MIC)

- MIC is calculated from

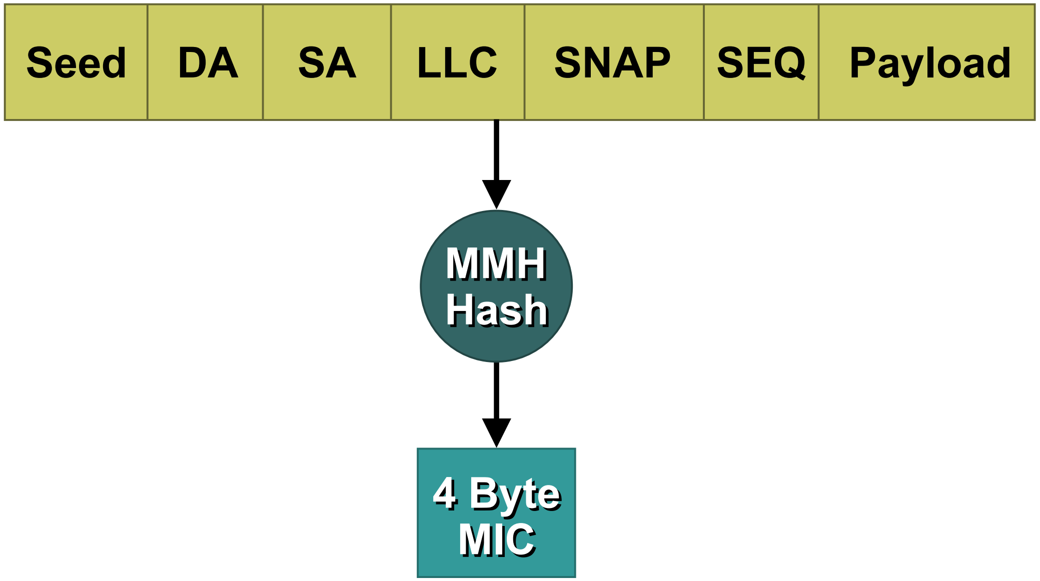
  Random Seed Value

  MAC Header

  Sequence Number

  Data Payload

- Components are hashed to derive a 32 bit MIC
- SEQ number must be in order, or frame is dropped



Broadcast Key Rotation

- Broadcast key is required in 802.1X environments
- Broadcast key is vulnerable to same attacks as static WEP key
- Broadcast key needs to rotate, as with unicast key

Encryption Attack Mitigation

	WEP	TKIP	VPN
Bit Flipping			X
IV Reuse			X
AirSnort			X

Agenda

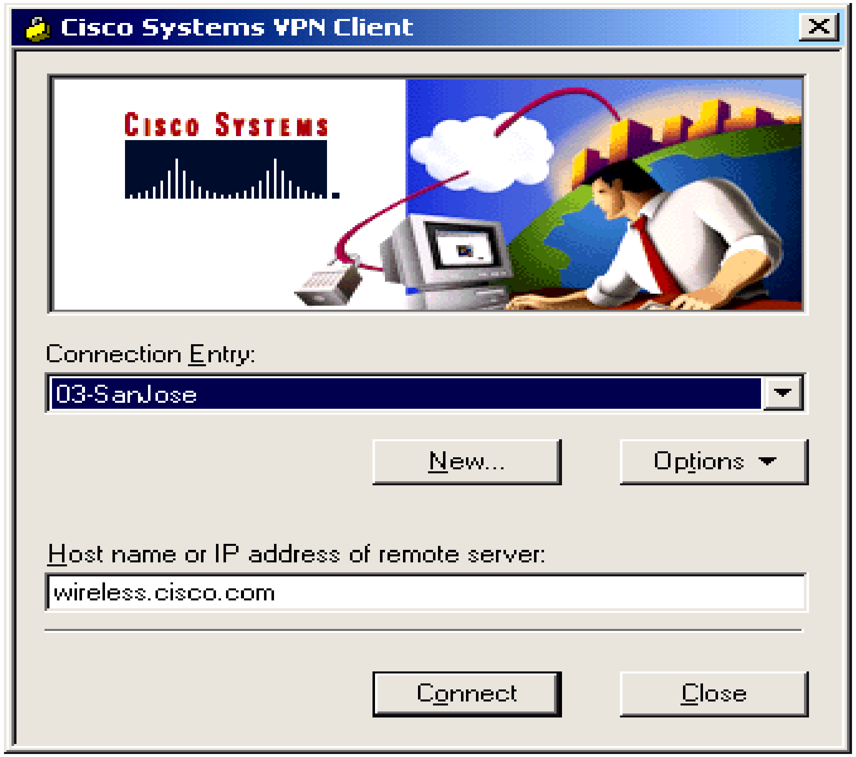
- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

Deploying Secure Wireless LANs

- VPN over 802.11
- 802.1X w/TKIP Encryption

VPN over 802.11—Client

- **Requires a separate logon for VPN**

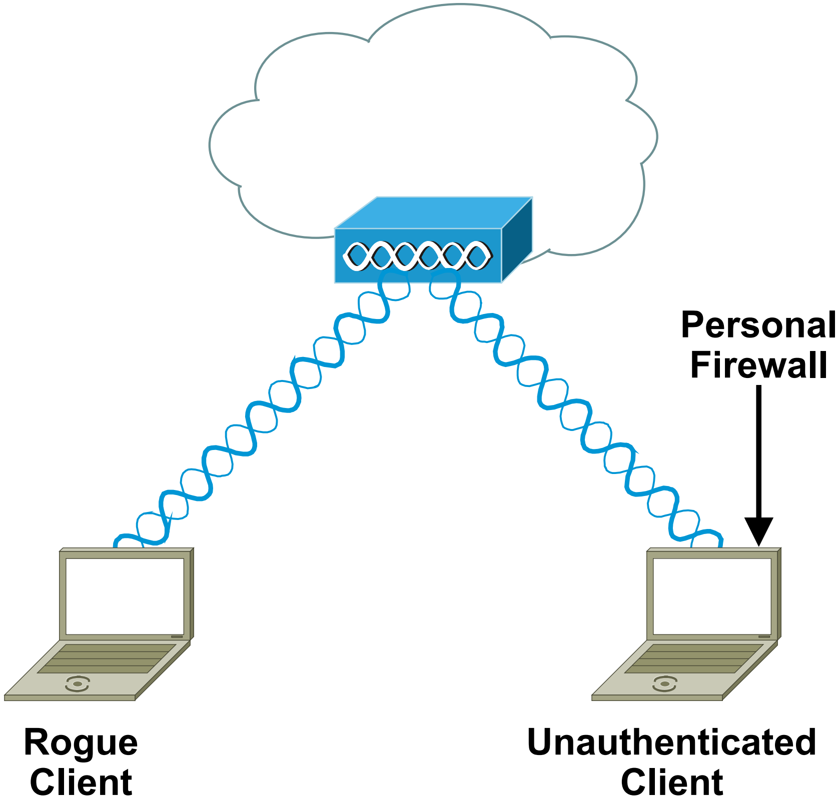


Connection Entry: 03-SanJose

Host name or IP address of remote server: wireless.cisco.com

VPN over 802.11—Client

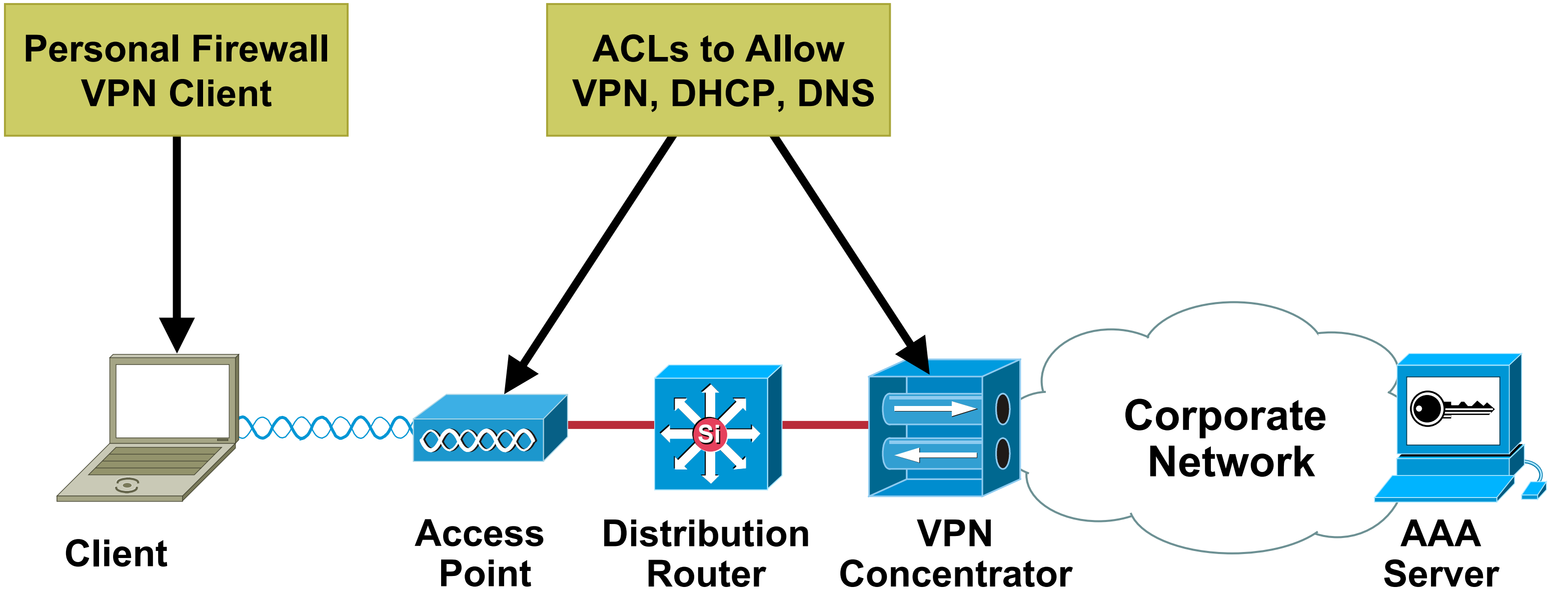
- Before VPN authentication client is on unprotected WLAN
- Personal Firewall can mitigate attacks on these clients



VPN over 802.11— Filters & Access Lists

- Protect as much as we can the open WLAN :
- Filters on the Access Points
- Access Lists on the L3 switches/routers

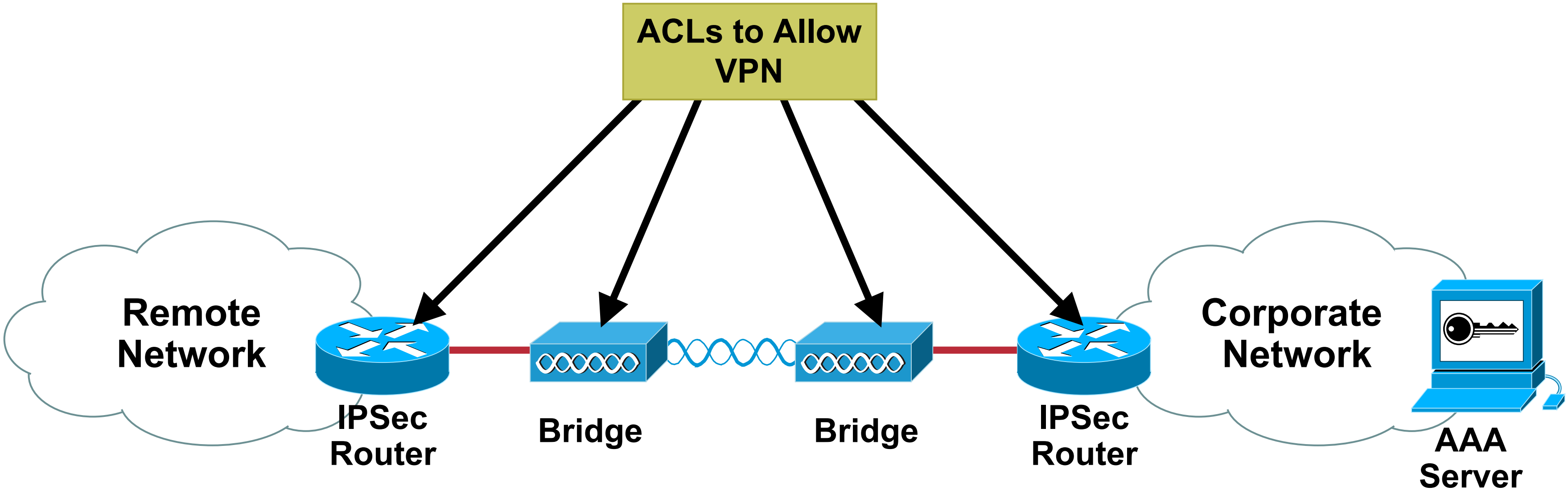
VPN Logical Topology



Personal Firewall VPN Client

ACLs to Allow VPN, DHCP, DNS

VPN over 802.11 Bridging Scenarios



VPN over 802.11—Performance

- All message authenticity and encryption done in software
- Average of 30% to 40% performance impact

VPN over 802.11—Issues

- Client throughput may require multiple concentrators
- Support for IP unicast exclusively

  No support for IPX, AppleTalk

  No support for multicast
- 802.11e QoS enhancements useless for VPN WLAN clients

  All traffic is IP/ESP encapsulated

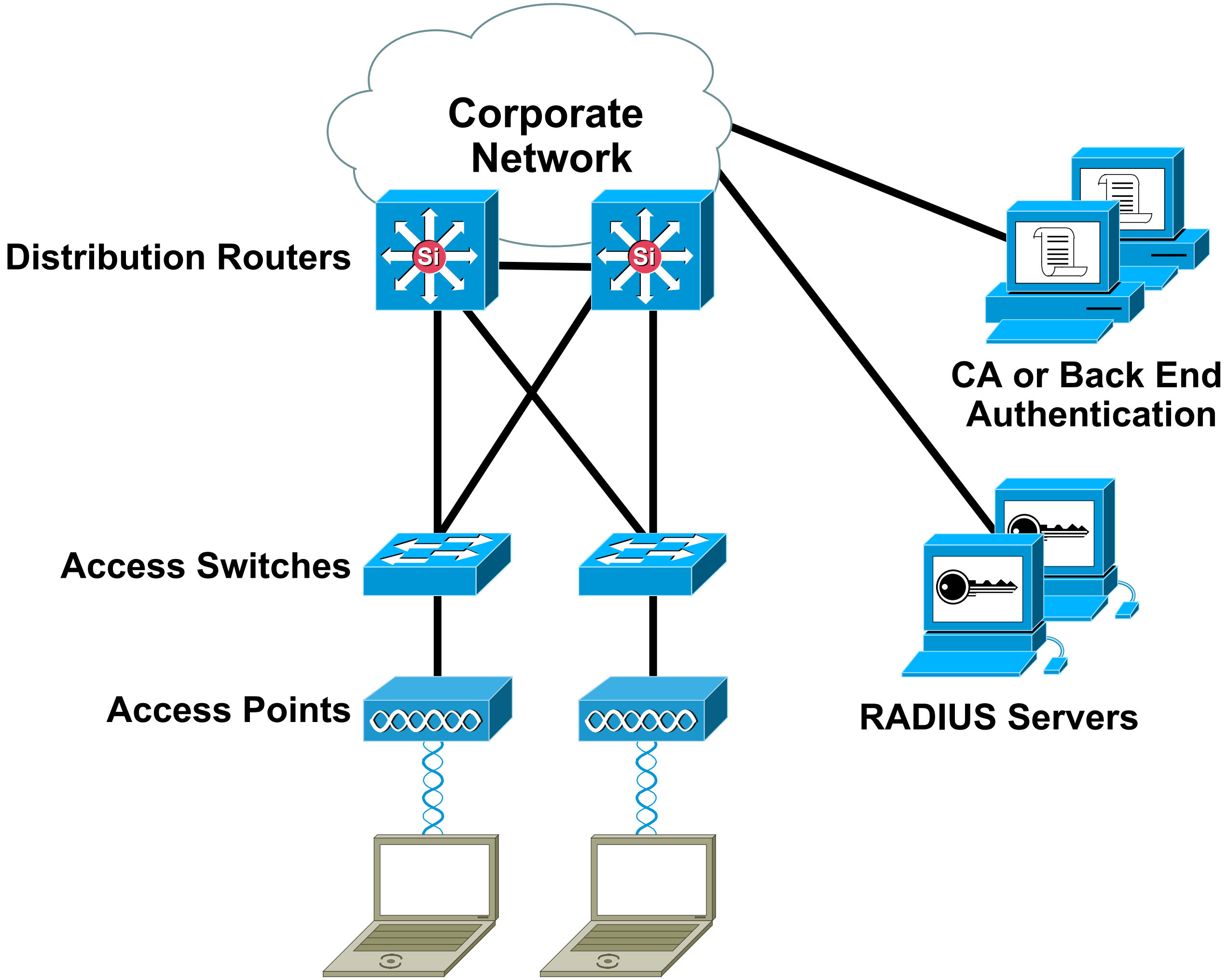
VPN over 802.11—Issues

- No support for WLAN appliances
  - Barcode readers, 802.11 phones
- Roaming Issues
  - Layer 2—ESP session timeout
  - Layer 3—Interoperability with Mobile IP

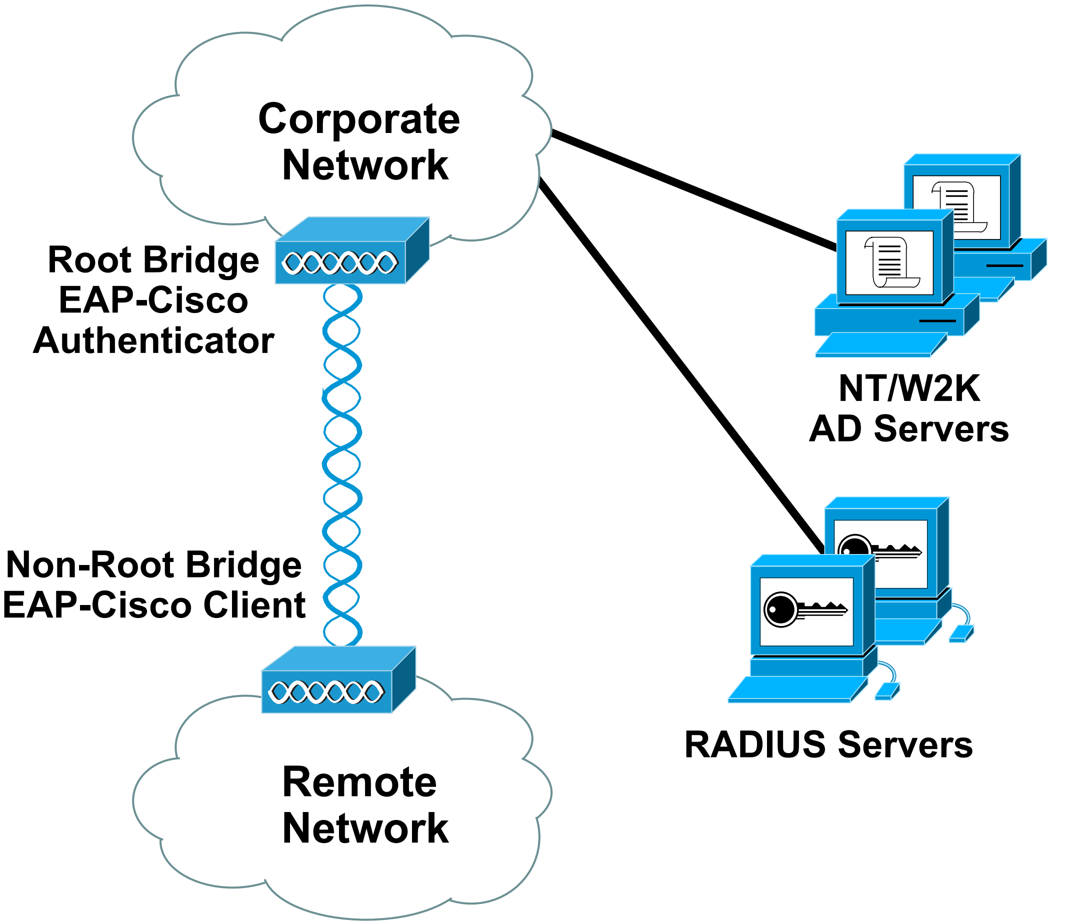
802.1X w/TKIP—Configurations

- EAP-Cisco
- EAP-TLS
- Both require Cisco clients and APs

802.1X w/TKIP—Topology

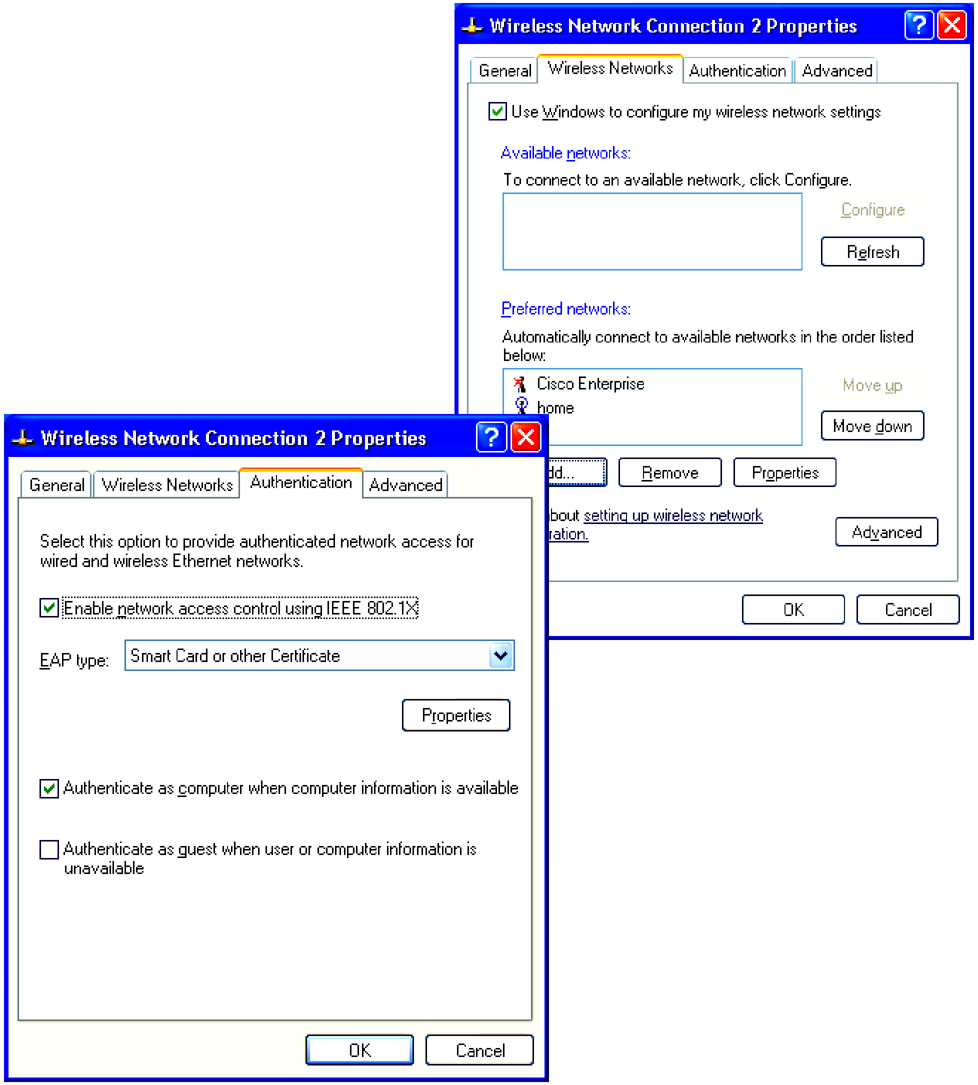


EAP-Cisco w/TKIP—Bridging Scenario


Corporate Network
Root Bridge EAP-Cisco Authenticator
NT/W2K AD Servers
Non-Root Bridge EAP-Cisco Client
RADIUS Servers
Remote Network

EAP-TLS w/TKIP—Client

- Included in WinXP OS release
- Configure multiple network profiles
- Client displays all known networks with broadcast SSID enabled



Wireless Network Connection 2 Properties

☑ Use Windows to configure my wireless network settings

Available networks:

To connect to an available network, click Configure.

Preferred networks:

Automatically connect to available networks in the order listed below:

Cisco Enterprise

home

bout setting up wireless network
ration.

Wireless Network Connection 2 Properties

Select this option to provide authenticated network access for wired and wireless Ethernet networks.

☑ Enable network access control using IEEE 802.1X

EAP type: Smart Card or other Certificate

☑ Authenticate as computer when computer information is available

□ Authenticate as guest when user or computer information is unavailable

802.1X w/TKIP—General Issues

- New cryptographic techniques

  Proven in IEEE, but only time will tell…

- 802.11 standard is evolving

  Changes should be expected

  802.11 task groups E, F, H, and I

802.1X w/TKIP—Performance

- WEP encryption done in hardware
- MIC and per packet keying done in software
- Depending on traffic type, throughput hit of 5% to 15% with enhancements enabled

802.1X w/TKIP—General Issues

- Authentication types not pervasive (yet…)

  No one scheme satisfies every scenario or requirement

- Roaming

  RADIUS request adds ~ 300–600 ms to roam time

  A pre-authentication mechanism is needed to expedite roaming process

Other Security Features

- RADIUS Accounting
- Publicly Secure Packet Forwarding (PSPF)

RADIUS Accounting

- AP will log client associations and disassociations using RFC2866 RADIUS accounting
- No client upgrade required; AP only enhancement
- Vendor Neutral

RADIUS Accounting Overview

- AP will send a start message to the accounting server after client association
- AP will send update messages at configurable intervals
- AP will send a stop message when client disassociates

RADIUS Accounting Overview

- Accounting can be configured for EAP clients, Non-EAP clients, or both
- Non-EAP refers to standard Open/Shared Key authentication and/or MAC authentication

RADIUS Accounting Overview

- What info does RADIUS accounting provide?

  Input/Output bytes

  Input/Output packets

  Session duration

  Association ID

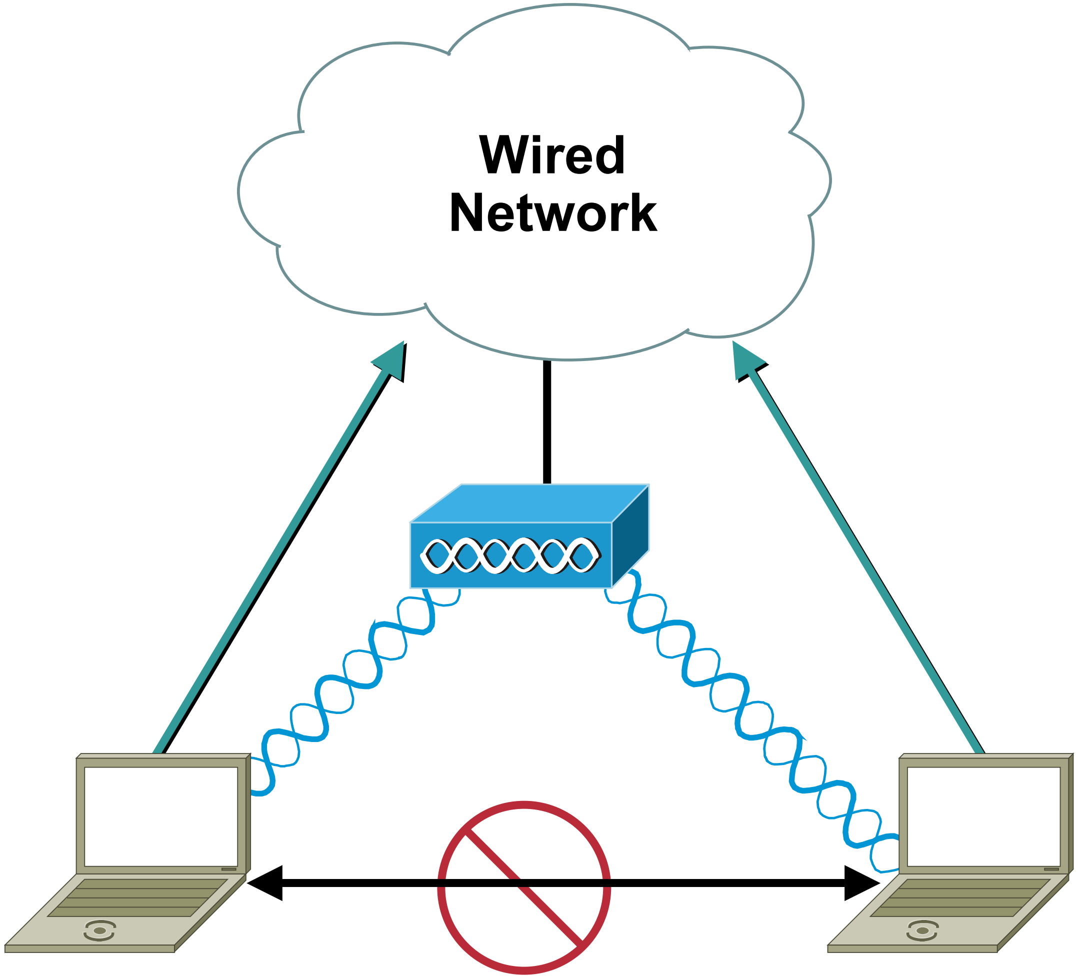
  NAS (Access Point) IP Address

- These values are on a per client basis

Publicly Secure Packet Forwarding

- Prevents WLAN inter-client communication
- Client can communicate out through the AP
- Clients cannot communicate to other stations in the BSS

PSPF—Blocking Inter-client Communication



Agenda

- Drivers for Wireless Security
- Wireless Security in 802.11
- Vulnerabilities in 802.11 Wireless Security
- Technologies for Secure Wireless LANs
- Deploying Secure Wireless LANs
- What Lies Ahead

What Lies Ahead

- Ratification of IEEE 802.11i
- Adoption of TKIP encryption
  - Certifiable vender interoperability (WiFi)
- AES encryption
  - 3DES successor

Securing 802.11 Wireless Networks

Session ACC-232

Please Complete Your Evaluation Form

Session ACC-232

CISCO SYSTEMS ®

EMPOWERING THE
INTERNET GENERATION