Wireless LAN Security

Chris Johnson – CSE - Cisco Federal

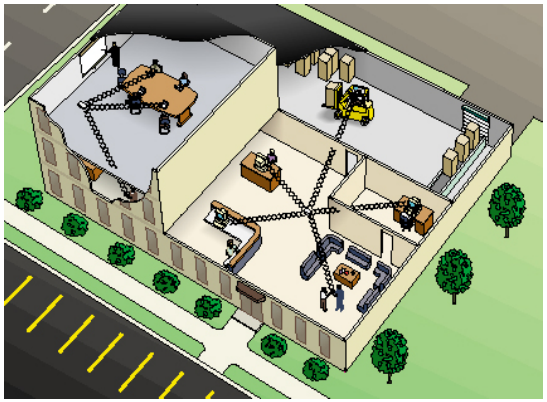
chrisj@cisco.com - 703 484 5661

Agenda

- 802.11 Standards
- WLAN Security Solutions
- WLAN Design Concepts
- Conclusion

WLAN –
Changing how we Work, Live Play and, Learn

In-Building Wireless LANs



Campus Networking

Public Access Hot Spots

Home Networking

Comparing 802.11 Standards

- **802.11b**

2.4Ghz

11Mb (auto stepdown)

Available today

WiFi Interoperability

Security – WEP, WPA 802.11i (Q12004)

- **Cisco Aironet 340/350/1100/1200**

Aironet 340/350

- **802.11a**

5 Ghz

54Mb (auto stepdown)

Available today

WiFi Interoperability

Security – WEP, WPA 802.11i (Q1 2004)

- **Cisco Aironet 1200**

Aironet 1200

- **802.11g**

2.4Ghz

54 Mb (auto stepdown)

Ratified June 2003

Compatible w/802.11b

Security – WEP, WPA 802.11i (Q1 2004)

Cisco Products – Q4CY03

Cisco Aironet 1200, 1100

Aironet 1100

WLAN Security Overview & Directions

- Network Security
- WLAN Security Issues
- WLAN Security Components
- IPSec WLANs

WLAN Security is not an End Point It's a Journey!

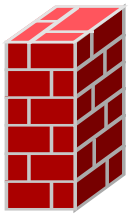
- There are solutions to today's threats
- There will be threats to today's solutions
- Many security issues can be resolved by awareness, good implementation & good design

Key Components of a Secure Network Wired or Wireless

Secure Connectivity

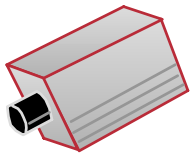
VPN
Tunneling
Encryption

Perimeter Security



ACLs
Firewalls

Security Monitoring



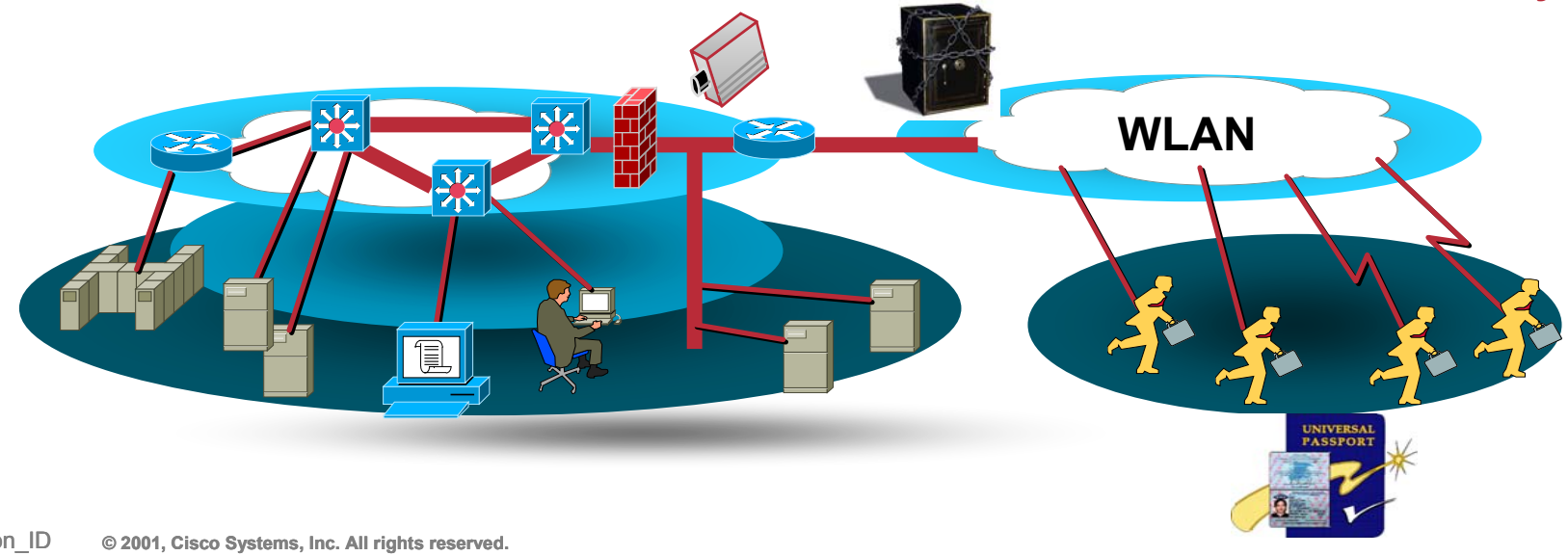
Intrusion Detection
Scanning

Identity

Authentication
Digital Certificates

Security Management

Policy Mgmt
Device Mgmt
Directory Svcs

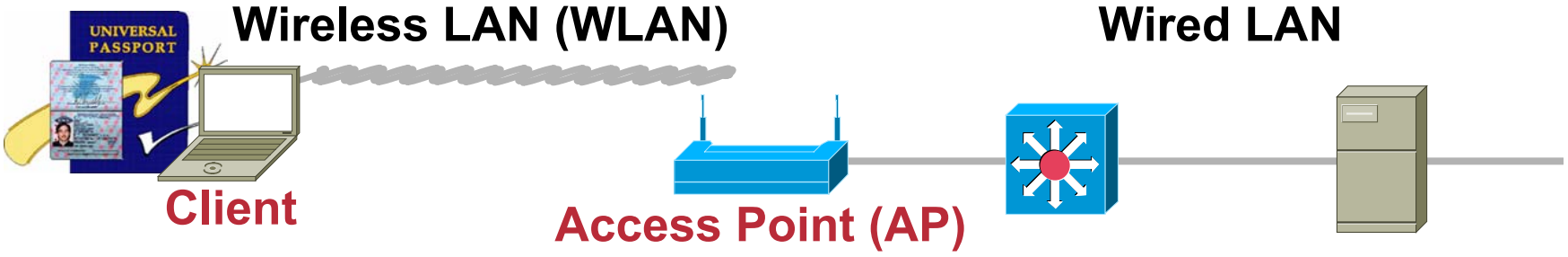


802.11 WLAN Security Issues

- **Authentication**
- **Data Privacy**

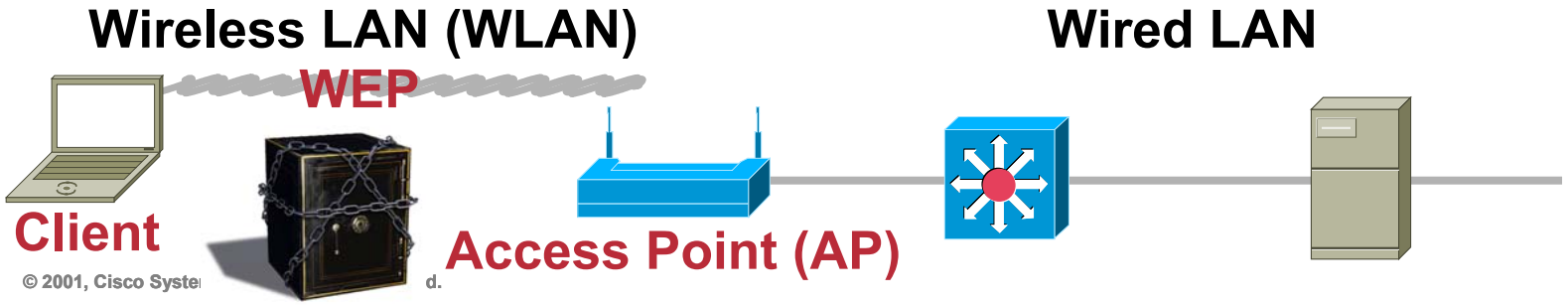
IEEE 802.11 Security – Authentication (Pre WPA)

- **Open** – No Authentication
  - Issue – Anyone can be authenticated
- **Shared** – Use WEP Key to encrypt AP Challenge
  - Issue – Easy to determine WEP Key
- Assumed Authentication Methods - SSID, MAC Address
  - Issue – SSID – Association, never intended for security
  - Issue – MAC – Sent in clear, very easily spoofed
- Published Papers – University of Maryland, April 2001



IEEE 802.11 Security – Data Privacy (Pre WPA)

- **Wired Equivalency Privacy**
  - Based on RC4 Algorithm (good algorithm)
  - Weak Implementation (Weak IV, IV sent in clear, common WEP key
- **Issues (Based on WEP implementation)**
  - Weak IV – FMS Paper, July 2001
  - Key Derivation via monitoring - AirSnort
  - Key Derivation via bit flipping – UC Berkley, Feb. 2001
  - IV & WEP Key Replay Attack - DoS, knowing IV & WEP
  - No Key Management – Lends to invasion
  - WiFi Interoperability Certification – 40 bit only



WLAN Security Components (WPA & 802.11i)

- Authentication Framework (802.1X)
- Authentication Algorithm (EAP)
- Data Encryption Algorithm (TKIP, AES)

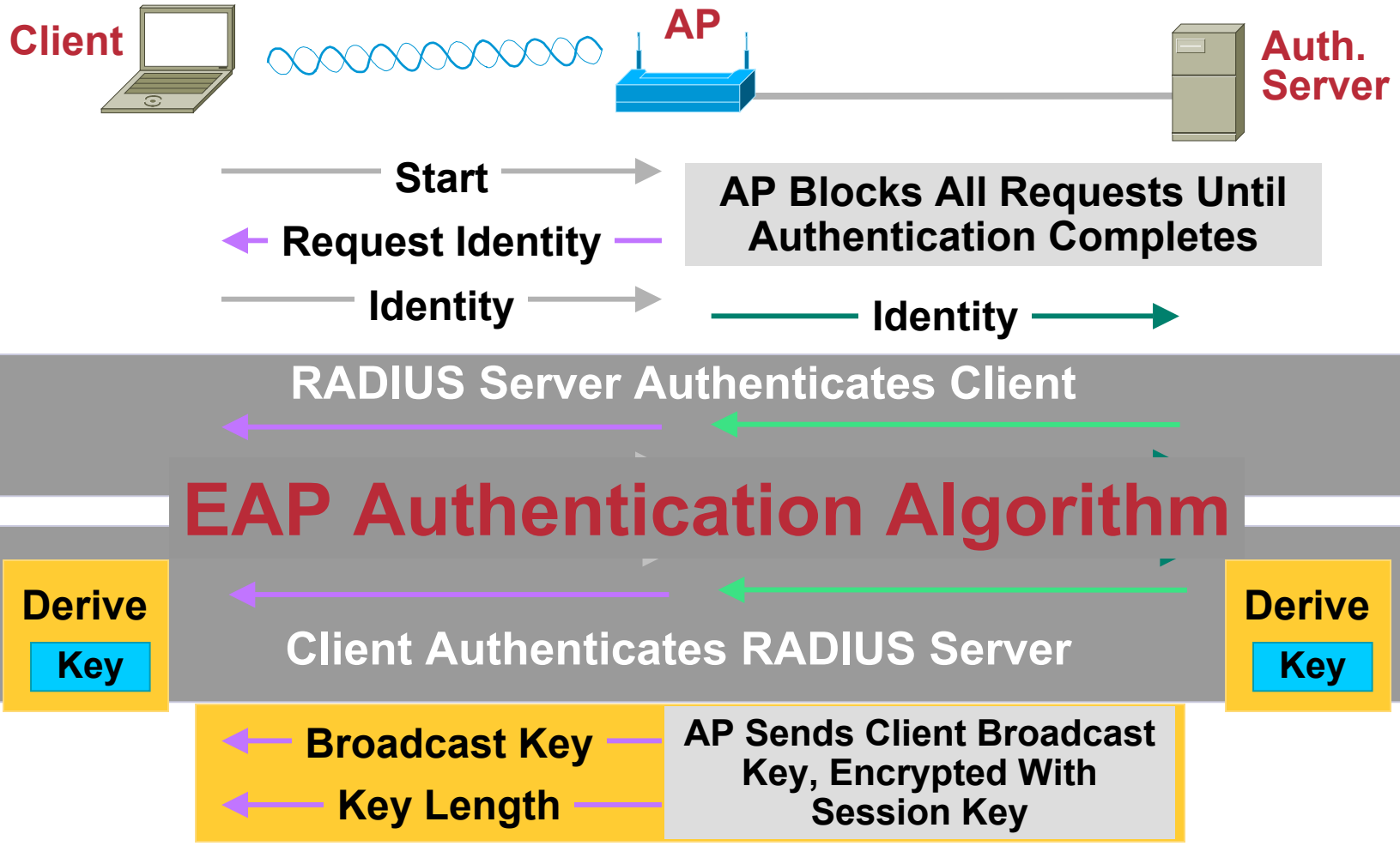
WLAN Security Standards

- IEEE 802.11 TGi - Proposed Standard 802.11i
  - IEEE Task Group focused on WLAN Security Improvement
  - Enhancement Proposed - 802.1X, EAP, TKIP, MIC, AES
  - Expected Ratification – Q4CY03
  - http://www.ieee.org
- WECA – Wireless Ethernet Compatibility Alliance
  - "Compatibility "Seal of Approval"
  - WiFi Interoperability "WiFi" – WLAN Interoperability CY2000
  - WiFi Protected Access (WPA) – 802.1X, EAP, TKIP, MIC
    - Accepted January 2003, Testing started February 2003
  - http://www.weca.net
- FIPS – Federal Information Processing Standard
  - Not specific for WLAN but does have implications for encrypting data sent over WLANs
  - Regulated by NIST
  - http://csrc.nist.gov/publications/fips/index.html
  - http://www-08.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf - Federal WLAN Guide

FIPS Certification & Standards Implementation

- **What FIPS 140-1/2 does:**
  - **Certification of Encryption Algorithm(s) & Modes**
    - **DES, 3DES, AES – only certain modes of these algorithms**
- **What FIPS 140-1/2 does not do:**
  - **Certification of implementation standards (ie IEEE or IETF)**
- **Therefore proprietary FIPS approved solutions exist**
  - **FIPS Certified IPSec and 802.11i (when ratified) solutions offer open standards based, government certified solutions**
  - **WPA probably will never be FIPS certified**

802.1X Authentication Process



WEP Key never sent over the wire, derived by end station & Authentication server

802.11i & WPA Encryption Algorithms

- Static WEP – Not recommended

  (especially for Enterprise Configurations)

- Dynamic WEP - Hardened WEP Session Keys - WPA

  Temporal Key Integrity Protocol (TKIP)

  - Reduce IV attack, strengthen key integrity

  Message Integrity Check (MIC)

  - Prevent Replay attack, authenticity of frame

- Alternative to WEP-RC4 – 802.11i

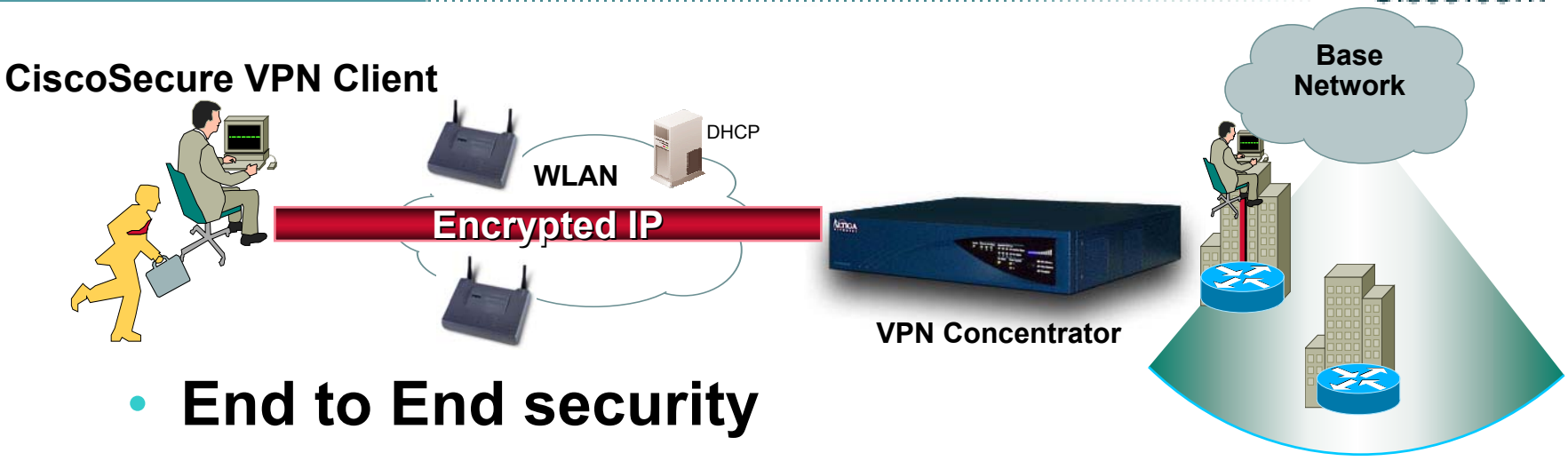
  Advanced Encryption Standard (AES)

  - As strong as 3DES, faster computation, FIPS 140-2 direction (NIST & IEEE)

  - Currently DES nor 3DES supported as a data privacy algorithm in any 802.11 direction

IPSec WLAN

IPSec VPN



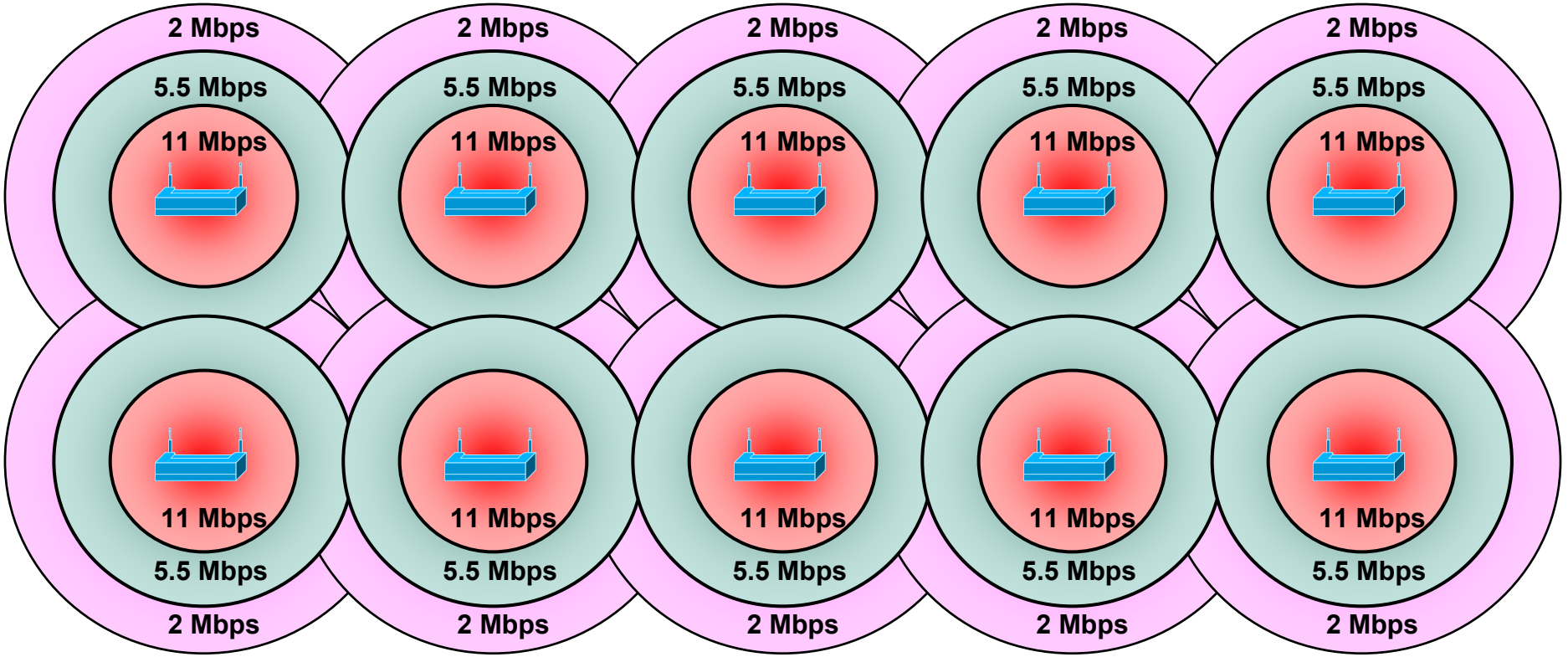
- **End to End security**
  - **IPSec VPN – Layer 3 – Client to Concentrator**
  - **Haul back to Central Point of Data Privacy**
  - **Stronger Data Encryption (3DES, AES) – today**
  - **Standards based – RFC 2401**
  - **Can be implemented on top of Layer 2 WLAN**
    - **Part of a Defense in Depth approach**

Additional benefits of IPSec VPNs

- **Can be used for wired & wireless**
  - **Remote Access (Cable)**
  - **Dial-In (RAS)**
  - **Traffic separation (Communities of Interests)**
- **Same software for wired & wireless**
  - **Usability, Support, Cost benefits**

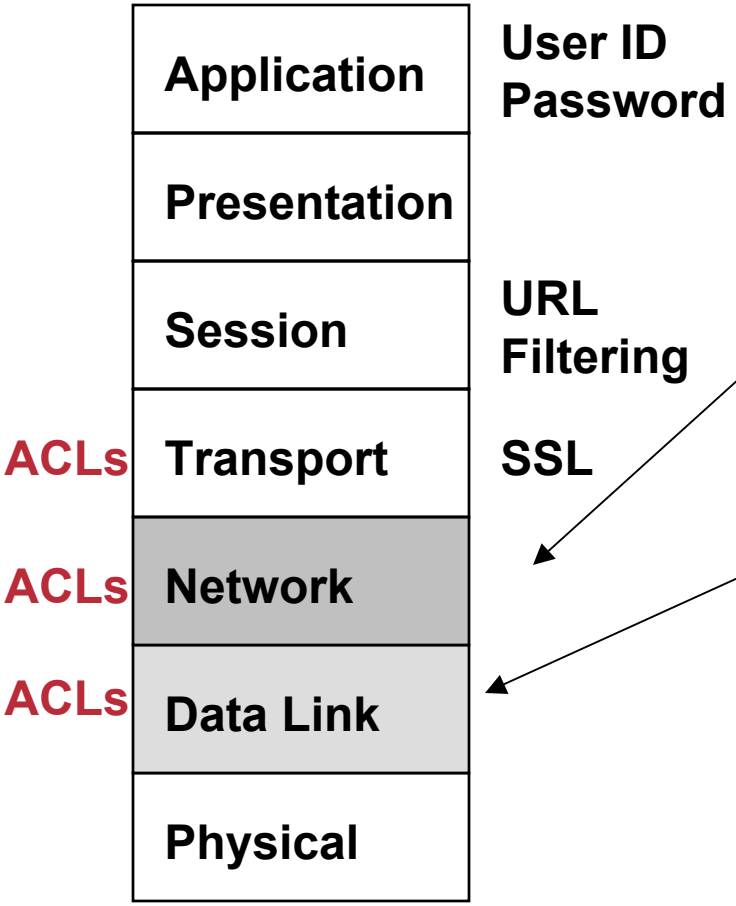
WLAN Design Concepts

Design Security
Reducing Bandwidth Coverage



- 11 Mbps connections only (or on edges of perimeter only)
- Can also reduce the radio power to reduce coverage area

OSI Layer & WLAN Security

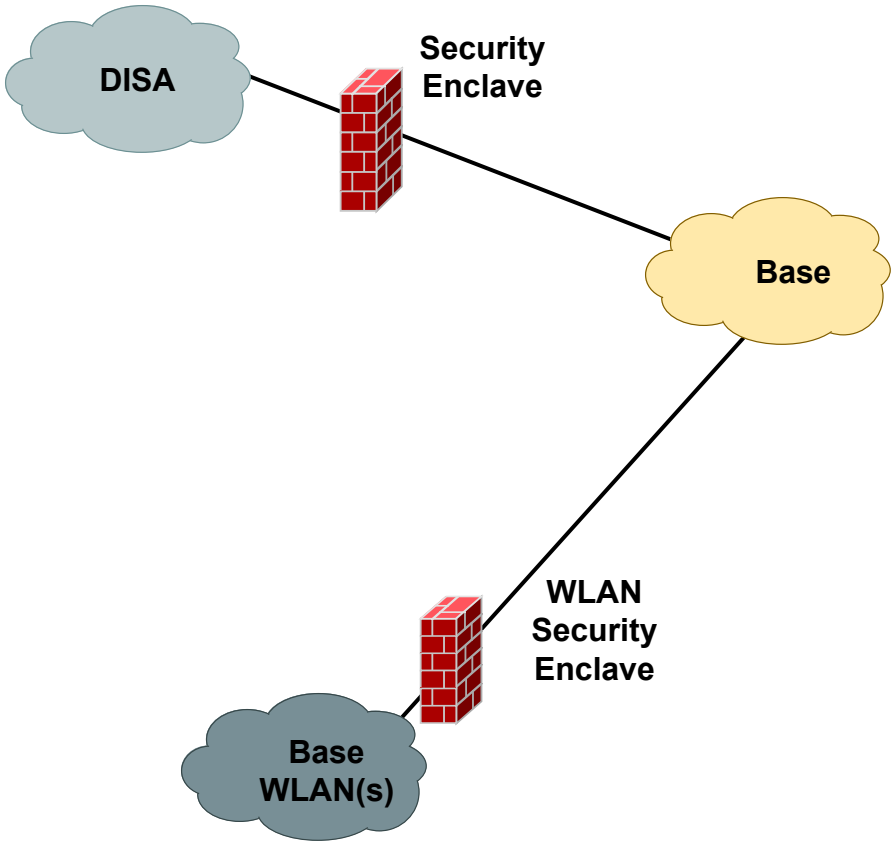


- **IPSec – Network Layer**
  - IETF Standards (RFC 2401)
  - IP
  - DES, 3DES, AES
- **WLAN – Data Link**
  - IEEE Standards (802.11)
  - Ethernet
  - WEP (RC4)
  - WEP “Alternative” (AES)

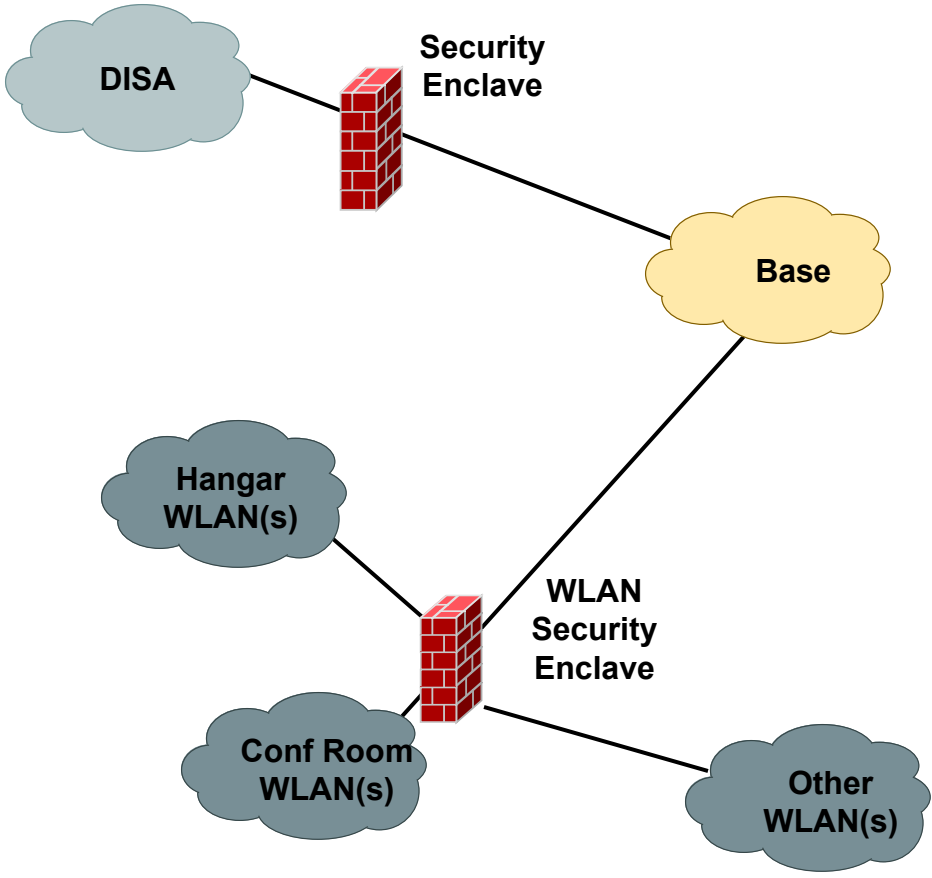
Lends to Defense in Depth Approach

Conceptual View

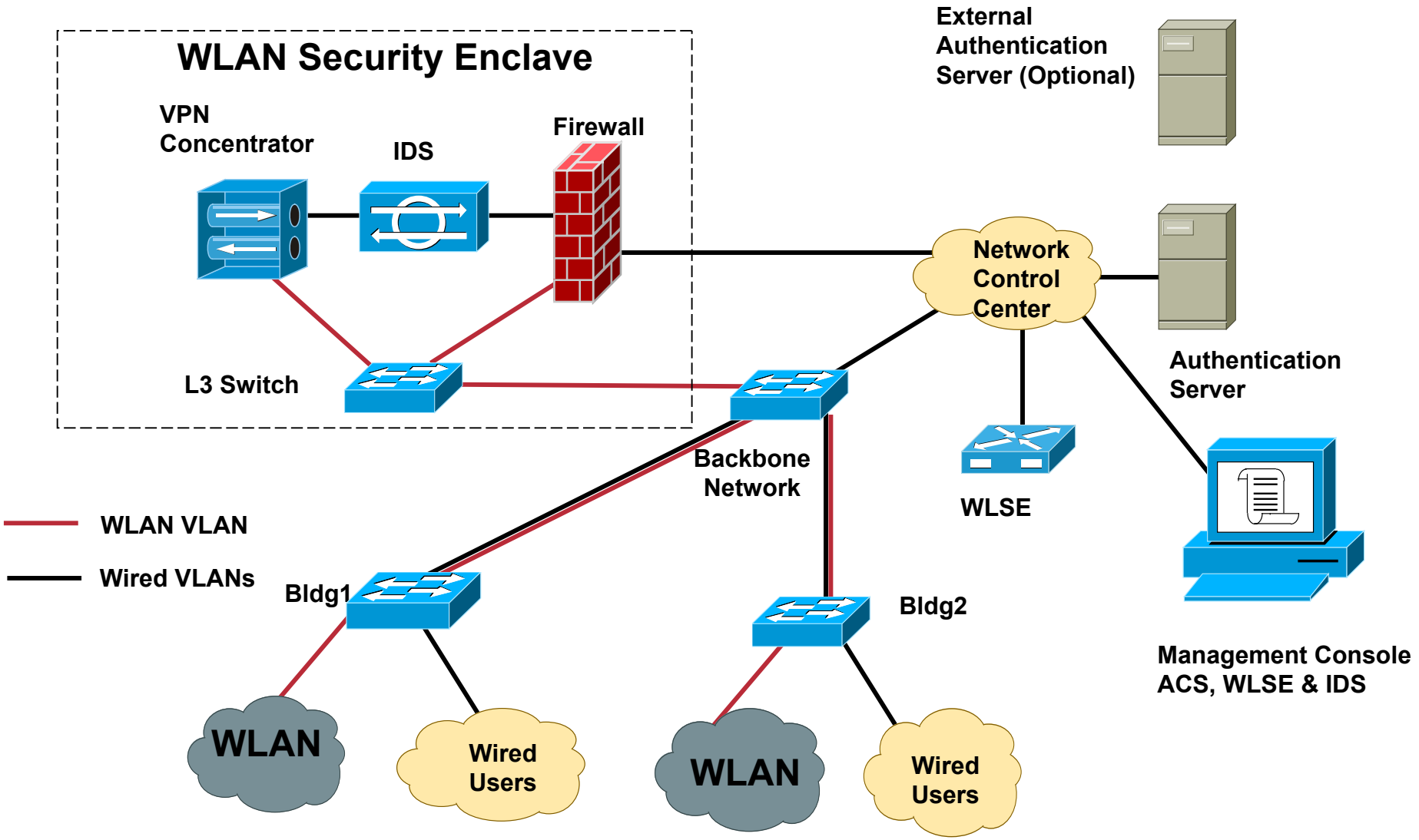
Configuration A



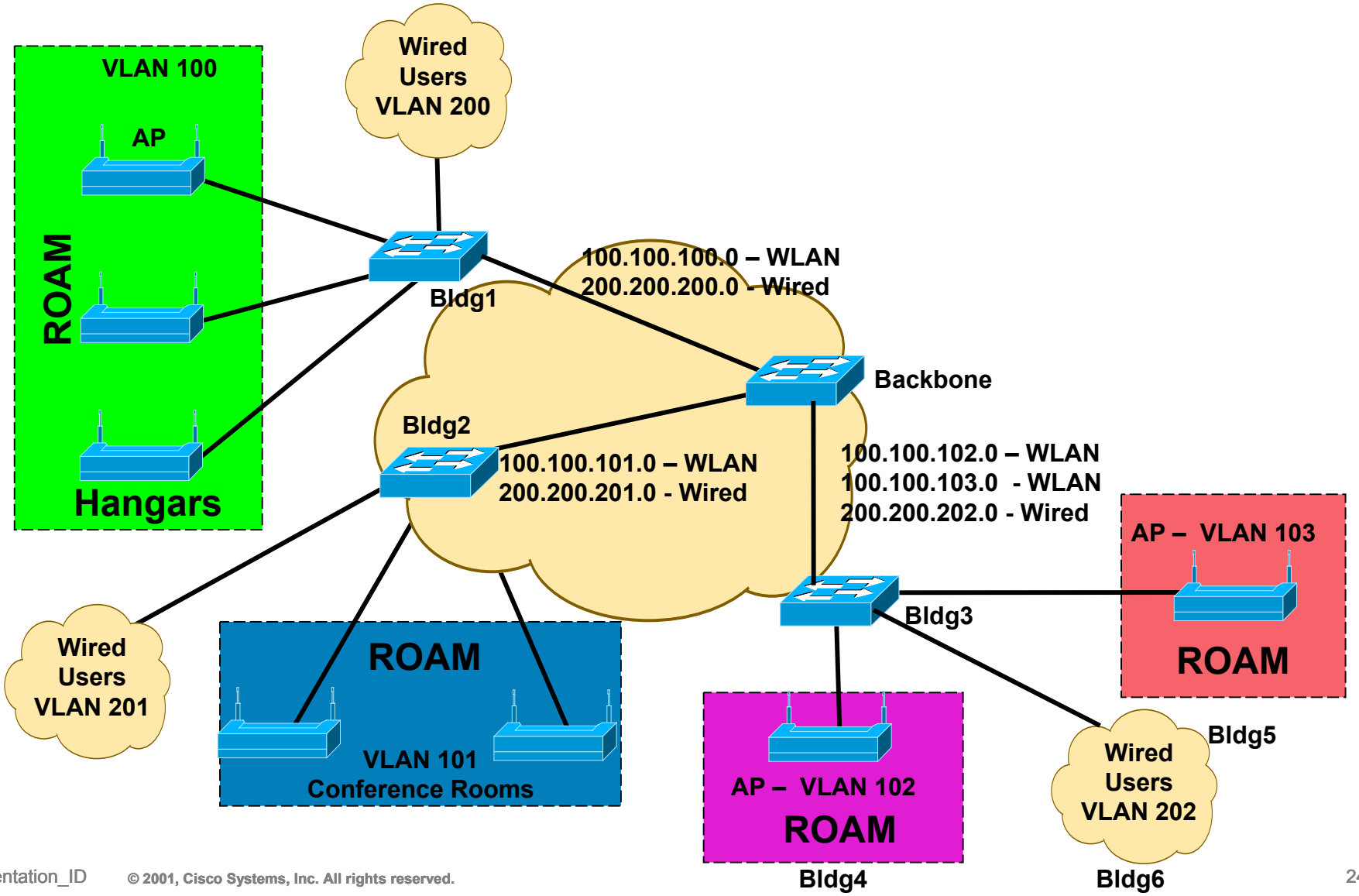
Configuration B



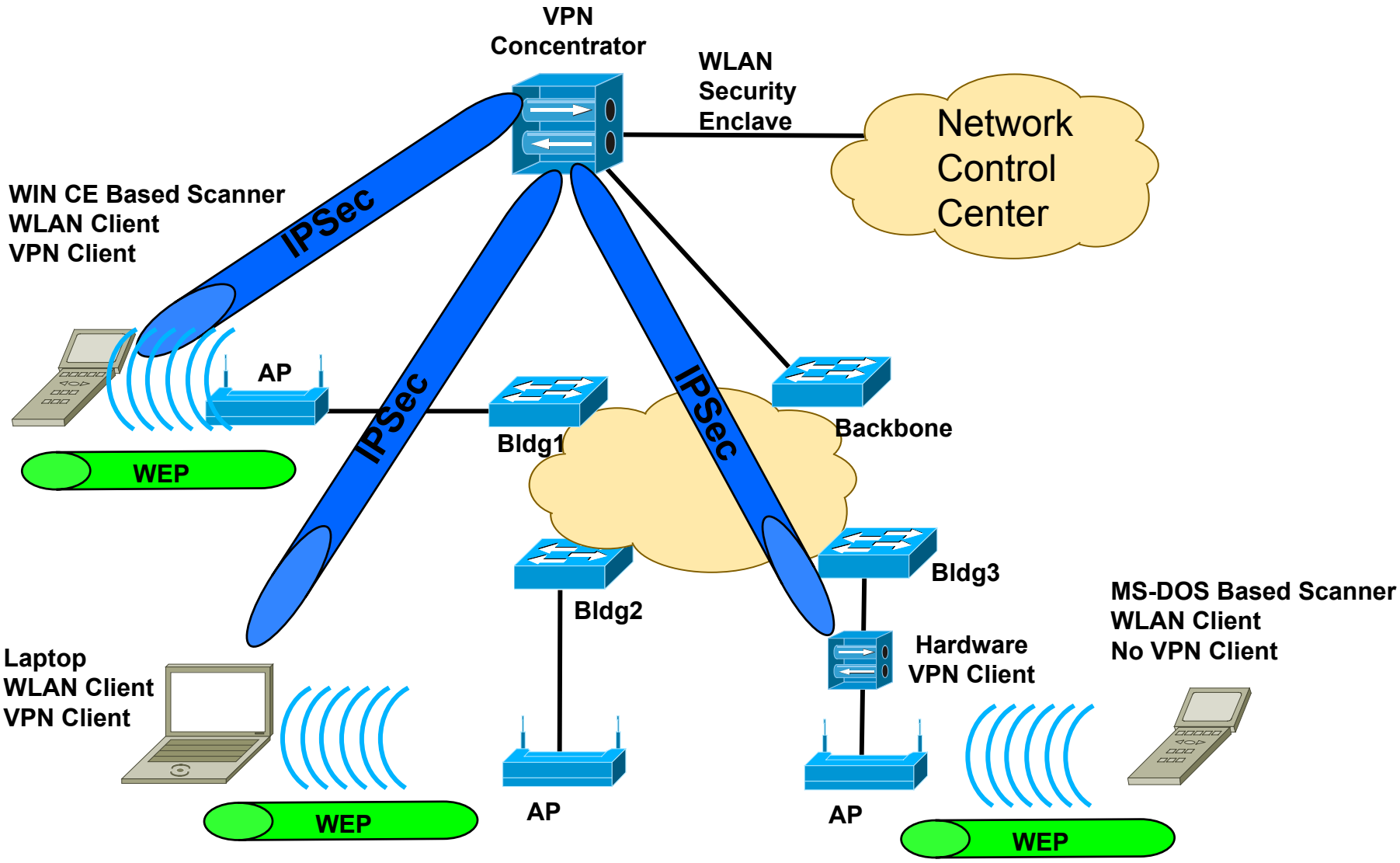
WLAN Security Enclave



802.11 Wireless Mobility



Wireless IPSec

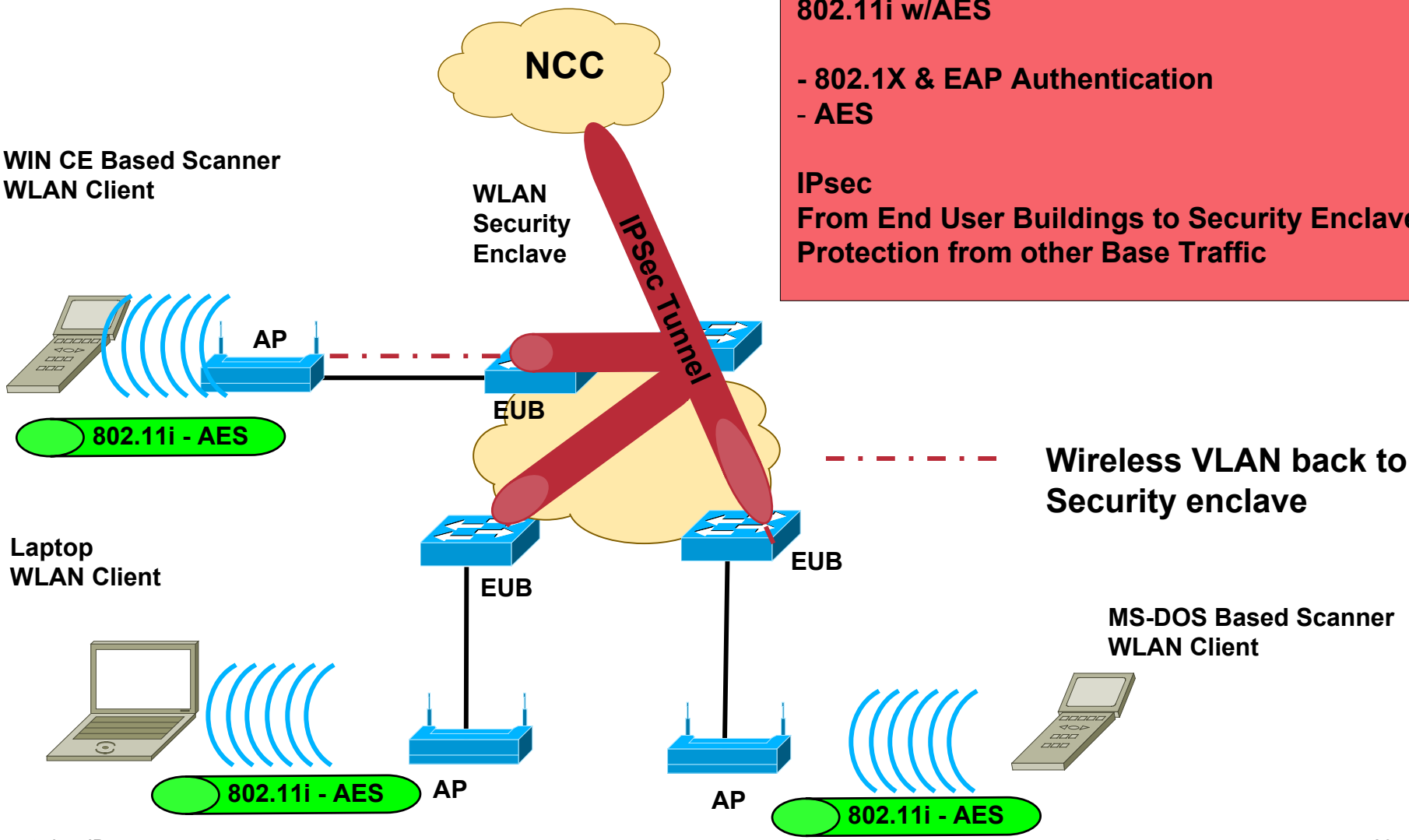


802.11i with AES Design

802.11i w/AES

- 802.1X & EAP Authentication
- AES

IPsec
From End User Buildings to Security Enclave
Protection from other Base Traffic



Different Users, Different Access – Common WLAN

Authentication via EAP for all users

- Group 1 (Internal WLAN Users)

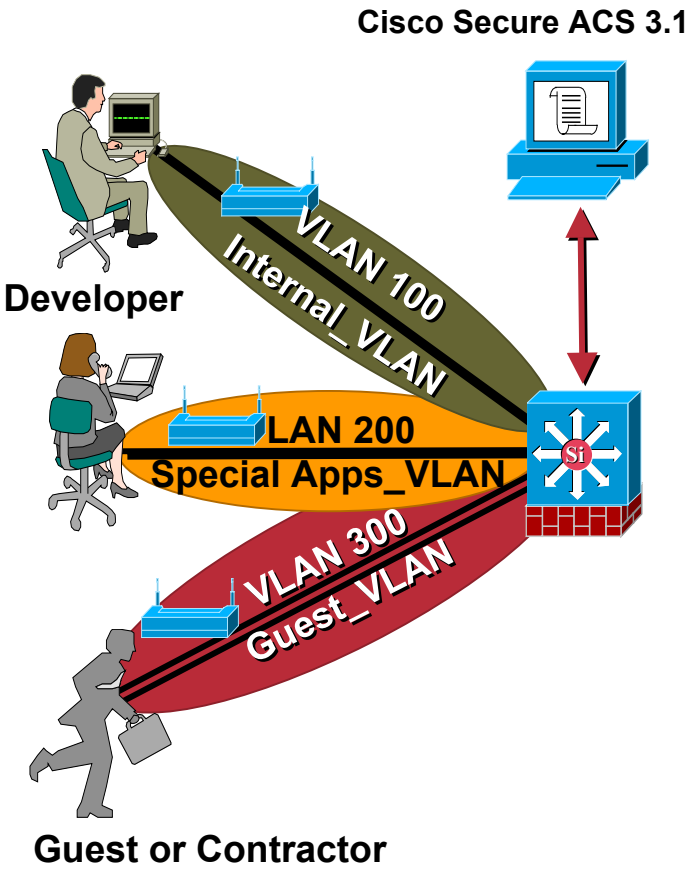
  IPSec VPN, Dynamic WEP, VLAN 100

- Group 2 (Scanner & Special Applications)

  No VPN, Dynamic WEP, VLAN 200

- Group 3 (Visiting Users)

  EAP (guest access or registration), No VPN, Internet Access ONLY, VLAN 300



Conclusion

Recommendations for WLAN Security

- Change product defaults

  Unique SSID, turn off SSID broadcast, WEP Key (128 bit), userid/password on AP

- Tie WLAN into your Organizational Security Policy
- Site Survey – Know your environment, understand your implementation and goals

  Antennas Types, Association Parameters (Data Rate, Power, MAC Address), AP Placement

- Separate network for WLAN

  Firewall and IDS before entering private LAN, separate infrastucture or VLAN & IP Addresses.

- Defense in Depth Approach

  Layer 2 – WPA, 802.11i, Layer 3 – VPNs

  Boundary Protection – IDS, Firewalls

  Interoperability - Standards based, FIPS-140

Conclusion

- **Wireless is here to stay**
  - **Enables new applications, new enterprise**
- **Security not just a WLAN issue – a Network issue**
  - **Treat the network as an untrusted network and secure appropriately**
- **WLAN can be extremely secure**
  - **No quick fixes – planning and design**
  - **Solutions to address security are available today and will continue to evolve**

Cisco WLAN Security Links

- **Cisco WLAN Security website**

  http://www.cisco.com/go/aironet/security

- **Cisco Wireless Security Suite software downloading instructions**

  http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1674_pp.htm

- **SAFE: Wireless LAN Security in Depth**

  http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

- **Cisco Mobile Office: At Work (Click on - Technology Overview)**

  http://www.cisco.com/go/atwork

Chris Johnson – CSE - Cisco Federal

chrisj@cisco.com - 703 484 5661

Other IEEE 802.11 Standard Activities

- 802.11a—5 GHz, ratified in 1999
- 802.11b—11Mb 2.4 GHz, ratified in 1999
- 802.11g—Higher Datarate at 2.4 GHz
- 802.11e—Quality of Service
- 802.11f—Inter-Access Point Protocol (IAPP)
- 802.11h—Dynamic Channel Selection and Transmit Power Control mechanisms
- 802.11i—Authentication and Security

802.1X & EAP

- 802.1X – IEEE Authentication Framework

  Originally designed for wired networks, used (natively) for WLAN

  Supplicant – Client (software on mobile device)

  Authenticator – AP

  Authentication Server – RADIUS
- EAP – Authentication Protocol (RFC2284)

  Works inside the 802.1X Authentication Framework

  802.11i does not stipulate any authentication algorithm

  Cisco EAP, EAP-TLS, EAP-SIM (GSM), PEAP (Hybrid), Others
- EAP –

  Mutual Authentication

  WLAN authenticates the client, client authenticates the WLAN

  Dynamic WEP Key Generation

  Unique WEP Key per authenticated user

WLAN Data Transmission

- **Dynamic Session Key**
  - Used for encryption of data, unique to each authenticated user
  - Derived independently by client and authentication server
  - Session key sent to AP over wired network
    - Session Key never sent over wireless network
  - Timeout & renegotiate session keys – Cisco Value Add
    - Optional but recommended (hourly good idea)

802.11, WPA, 802.11i Comparison

Feature	Authentication	Encryption	Comments
Open Authentication	✓		802.11
Shared Authentication	✓		802.11
802.1X	✓		WPA/802.11i
EAP	✓		WPA/802.11i
WEP 40/128bit		✓	802.11/WiFi
Dynamic Encryption Key		✓	WPA/802.11i
WEP-TKIP (128 Bit)		✓	WPA/802.11i
MIC		✓	WPA/802.11i
AES		✓	802.11i

Additional Cisco Value Add Features

AP Authentication

– Rogue Access Point Detection

Per-packet hashing

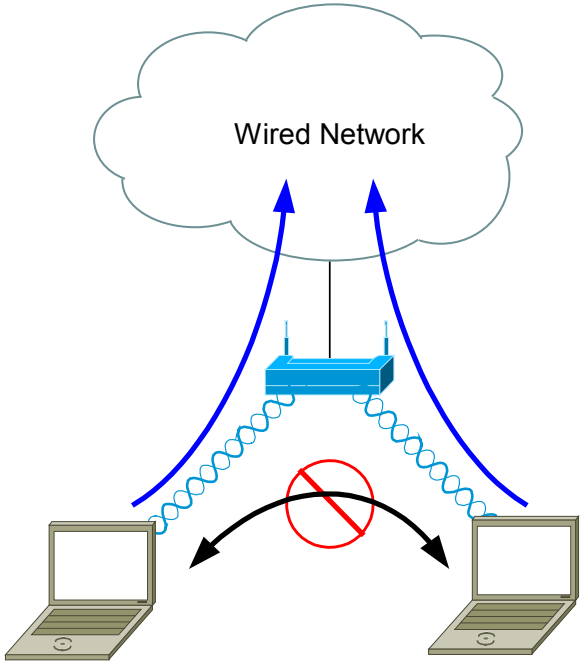
– Change WEP key per packet

Broadcast key rotation

– Change WEP Key for broadcast and multicast

Publicly Secure Packet Forwarding (PSPF)

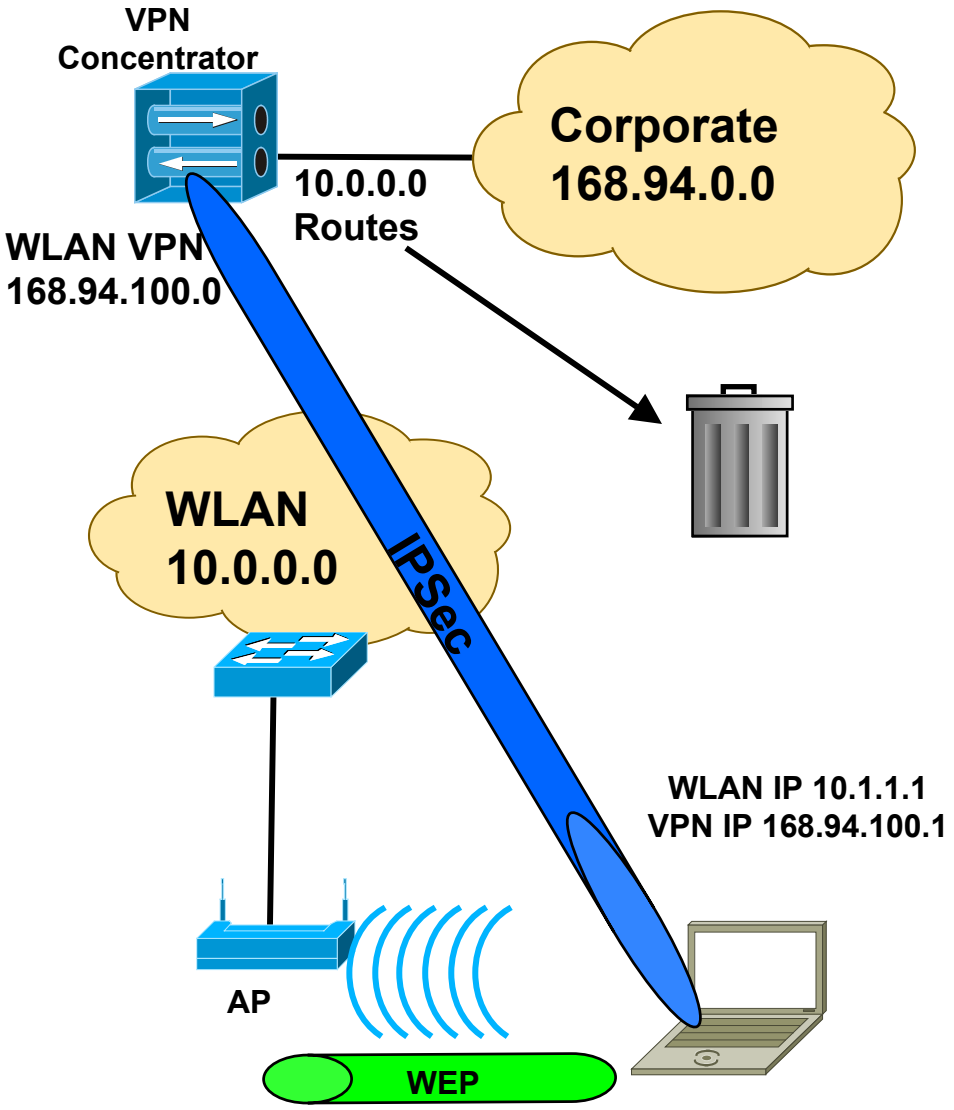
– Prevent client to client communication in a WLAN



PSPF

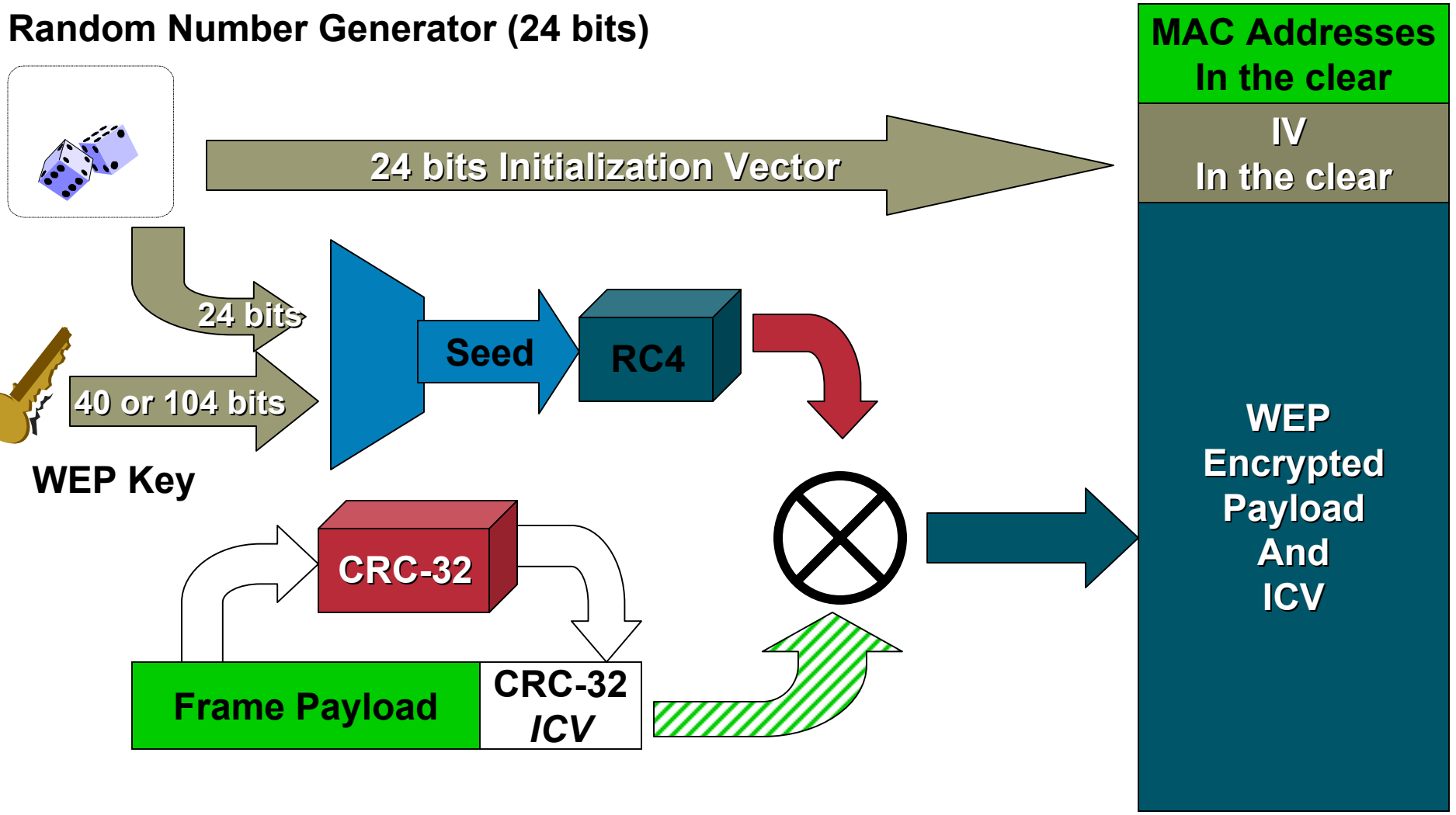
IPSec VPN Design Ideas

- "Dummy" network – WLAN
  - Unique IP address range (ie 10.0.0.0)
  - Not routed outside WLAN perimeter
  - Only devices on network are APs
- After VPN Authentication
  - Client assigned valid IP address (in IPSec tunnel)
  - Special IP range just for WLAN users (ie 168.94.100.0/24)

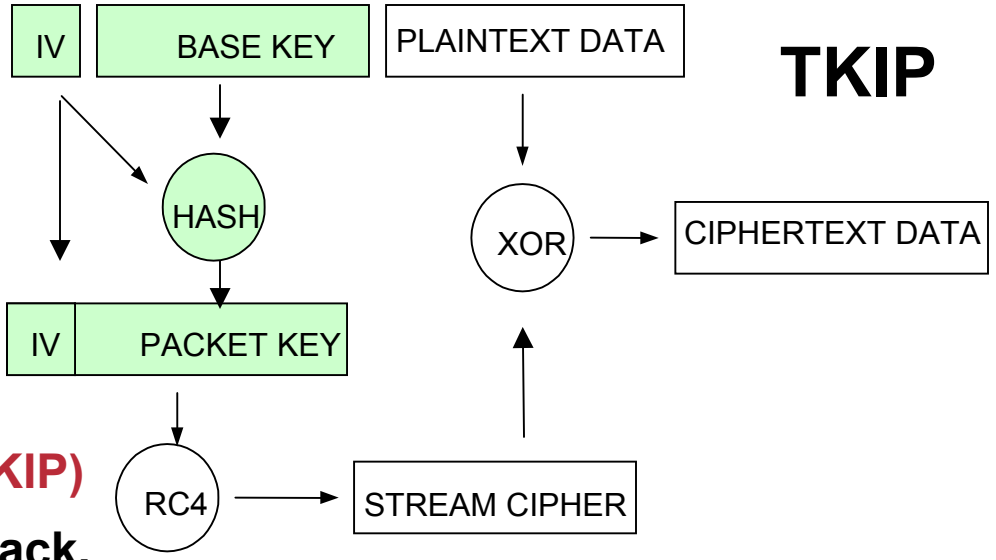


Initial IEEE 802.11 Security – Data Privacy

How 802.11 WEP Encryption Works



802.11i Encryption Algorithms



- **Hardening WEP**

Temporal Key Integrity Protocol (TKIP)

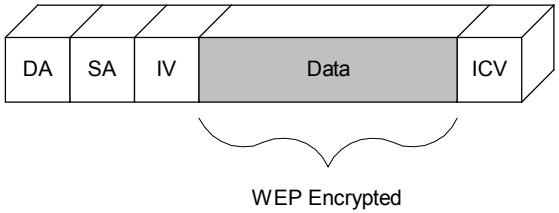
- Stronger keys, reduce IV attack, rotation of keys

Message Integrity Check (MIC)

-Prevent Replay attack, authenticity of frame

MIC

WEP Frame - No MIC



WEP Frame - MIC