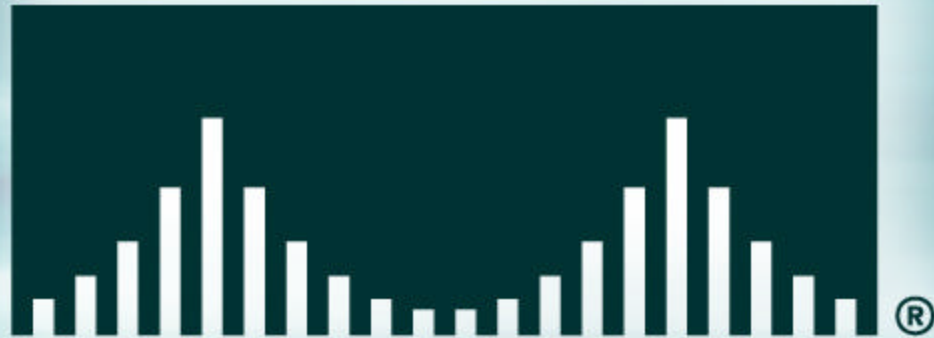


CISCO SYSTEMS



Networking Professionals Online TechTalk

**Securing and Managing
Your 802.11 Wireless Network**

Networking Professionals Online TechTalk

Cisco.com



Bruce Alexander
Technical Marketing Manager



Byron Henderson
Director, Enterprise Product Marketing

Agenda

- **WLAN Security Requirements**
- **WLAN Security Studies**
- **Existing WLAN Security Solutions**
- **Latest WLAN Security Solutions**
 - TKIP, MIC, Broadcast Key Rotation, PSPF**
- **802.11i Progress**
- **WECA Security Direction**

Security Requirements for WLANs

- **First generation security**
 - SSID
 - Static 40 or 128-bit WEP
- **2nd generation security**
 - Centralized user-based authentication (ACS2000 v2.6) integrated with network logon
 - Dynamic 128-bit WEP
 - VPN
 - Access control lists
- **Leading edge security**
 - TKIP
 - MIC
 - AES
 - Rogue AP detection



Security and Management

- **Managing the security side of you networks requires several things**

Protecting the 'network' from intruders

Requires authentication for users

Protecting the Wireless DATA from sniffers

Requires some type of encryption

Protecting you RF networks from being detected

The ability to MANAGE you users credentials

Includes WEP keys, users names, passwords, etc.

Protecting your wireless infrastructure from improper configuration

Required a good user manager interface on APs

WEP—Encryption

- **Encryption options**
 - No encryption
 - 40-bit encryption
 - 128-bit encryption
- **Software-based WEP**
 - As much as 20+% performance hit (@128 bit)
- **Hardware-based WEP**
 - 3% performance hit (@128 bit)
- **Static WEP requires someone to “touch” EVERY client and AP**



Wireless Ethernet Compatibility Alliance (WECA)

Cisco.com



- **WECA certifies interoperability between products**
- **This provides assurance to customers of migration and integration options**
- **Cisco is a founding member of WECA**
- **Certified products can be found at www.wi-fi.com**
- **Today Wi-Fi Certification Supports ONLY 802.11b**
Wi-Fi5 certification for 802.11a will be available in mid-2002
- **Today Wi-Fi only requires 40 Bit WEP for certification**

802.11a and 802.11g

- **The market is seeing the of new products become available at 802.11a 5GHz**
- **There has been a lot of talk about 802.11g for later this year**
- **Both promise higher data rates up to 54Mbps**
- **Security—Same issues that 802.11b has today**

WLAN Security Update

Cisco.com

- **WLAN studies**
- **Cisco LEAP**
- **New security enhancements**

TKIP

MIC

Broadcast Key Rotation

PSPF

Fluhrer Paper/AirSnort Utility

- **Key recovery possible due to statistical analysis of plaintext and “weak” IV**

Leverages “weak” IVs—large class of weak IVs that can be generated by RC4

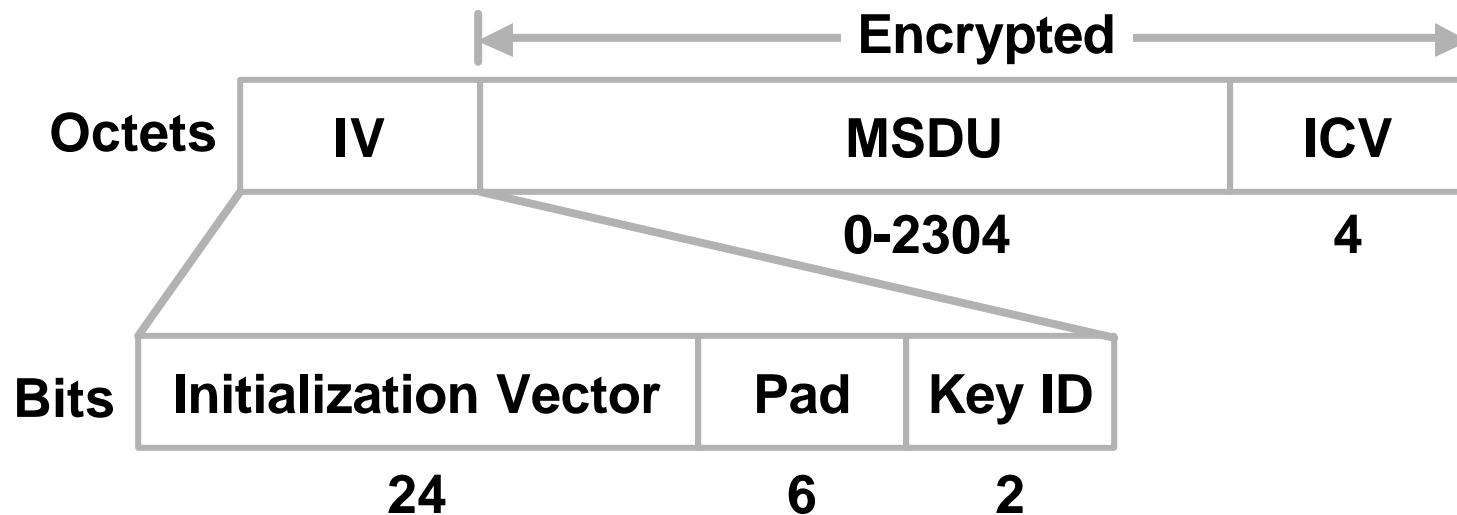
Passive attack, but can be more effective if coupled with active attack

- **Two major implementations**

AirSnort v0.1.0 tests

AT&T/Rice University tests (not released)

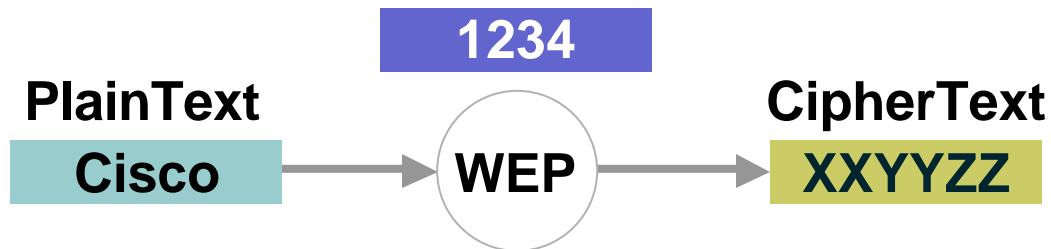
What is an IV?



- IV is short for **Initialization Vector**
- 24 bits long
(24 bits IV + 104 bits WEP key = 128 bits)

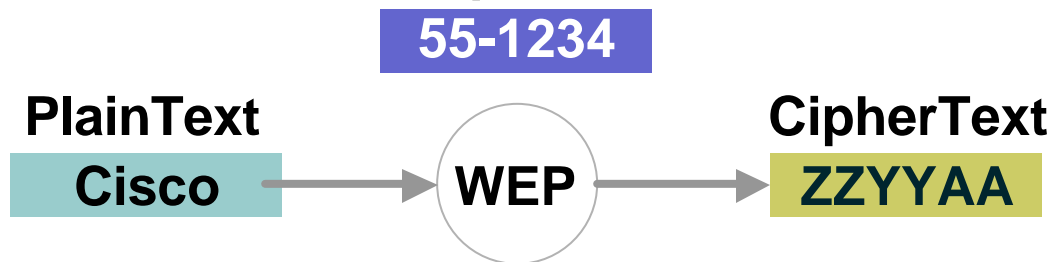
What is an IV?

Stream Cipher—No IV



Without an IV, the PlainText Will Always Produce the Same CipherText; An Eavesdropper Will Be Able to 'See' Patterns and Predict PlainText

Stream Cipher—with IV



With the IV, the CipherText Will Change as the IV Changes, So It Will Be More Difficult for an Eavesdropper to 'See' Patterns and Predict PlainText

- Same plaintext packet should not generate same ciphertext packet
- IV is random, and changes per packet

What is a “Weak” IV?

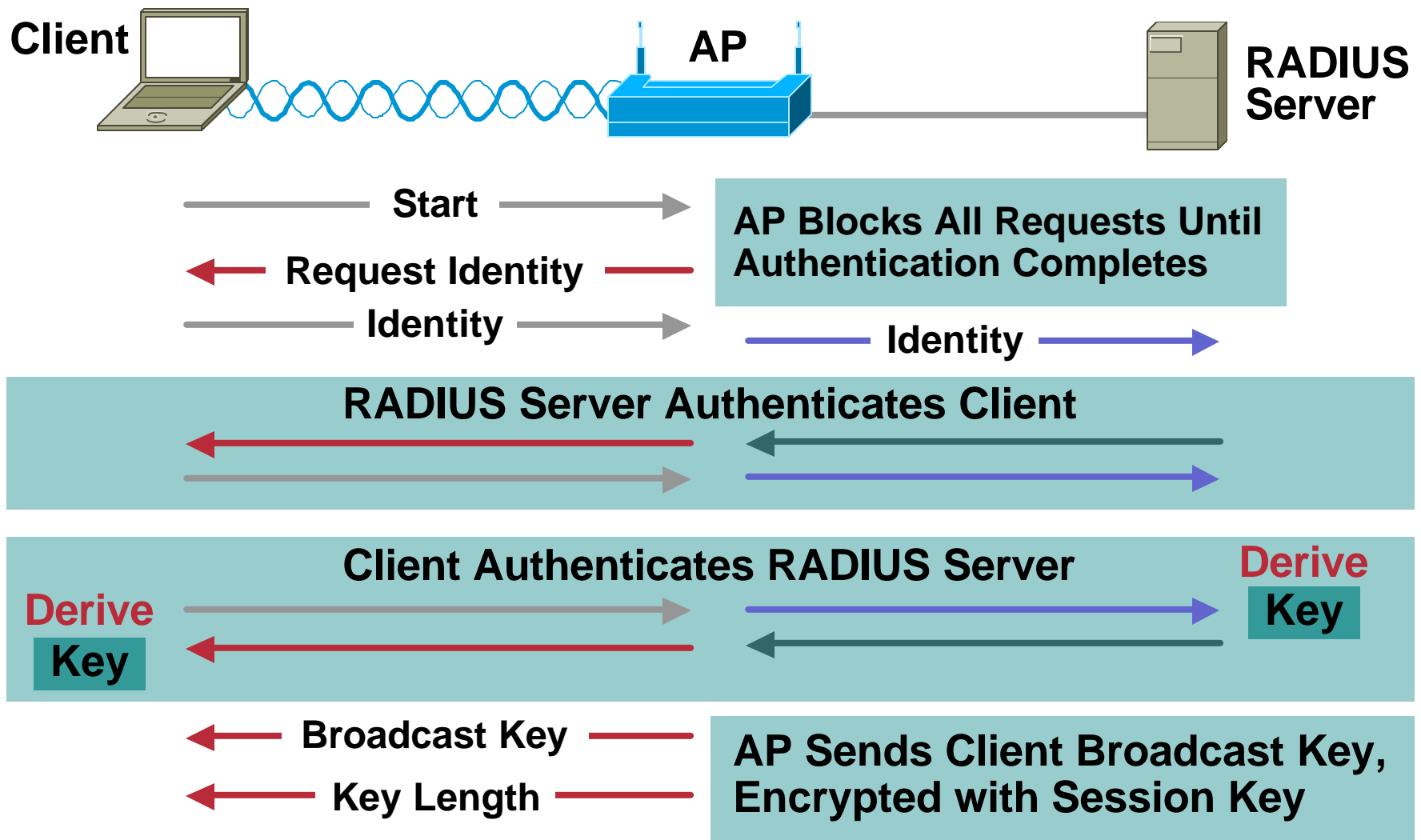
- In the RC4 algorithm the Key Scheduling Algorithm (KSA) creates an IV-based on the base key
- A flaw in the WEP implementation of RC4 allows “weak” IVs to be generated
- Those IVs “give away” info about the key bytes they were derived from
- An attacker will collect enough weak IVs to reveal bytes of the base key

Cisco LEAP Overview

- **Provides centralized, scalable, user-based authentication**
- **Algorithm requires mutual authentication**
 - Network authenticates client, client authenticates network
- **Uses 802.1X for 802.11 authentication messaging**
 - APs will support WinXP's EAP-TLS also
- **Dynamic WEP key support with WEP key session timeouts**

LEAP Authentication Process

Cisco.com



UC Berkeley Study

- **Bit flipping**

Bits are flipped in WEP encrypted frames, and ICV CRC32 is recalculated

- **Replay**

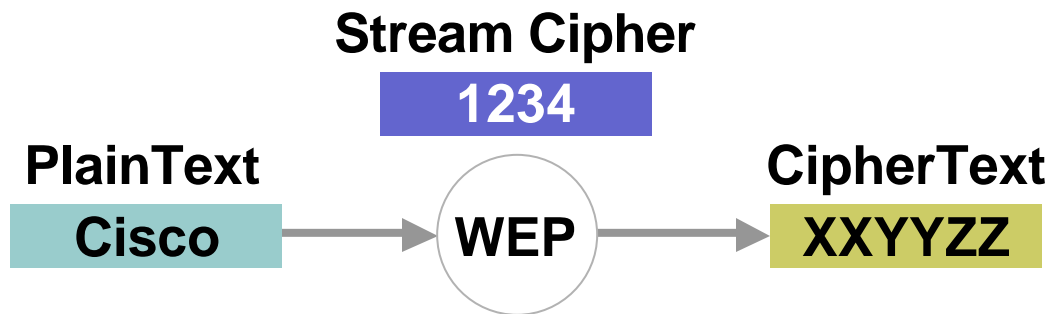
Bit flipped frames with known IVs resent

AP accepts frame since CRC32 is correct

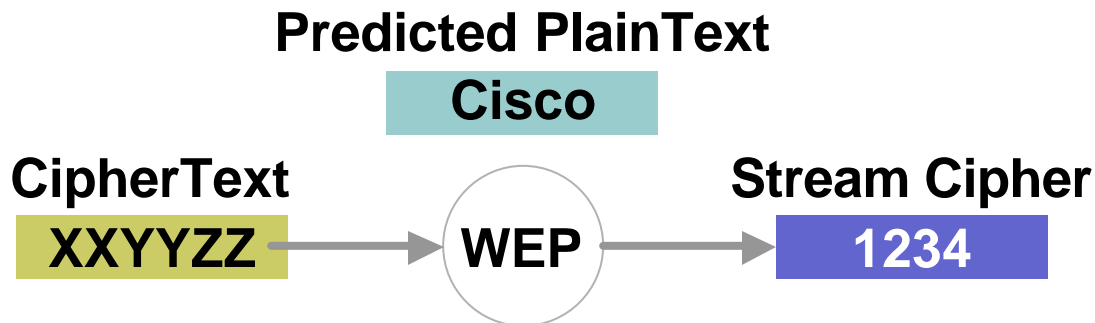
Layer 3 device will reject, and send predictable response

Response database built and used to derive key

UC Berkeley Study

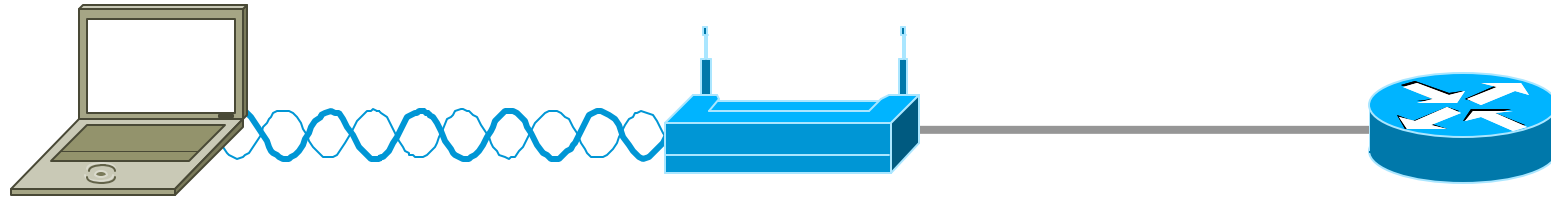


PlainText Data Is XORed with the WEP Stream Cipher to Produce the Encrypted CipherText



If CipherText Is XORed with Guessed PlainText, the Stream Cipher Can Be Derived

UC Berkeley Study



Bit Flipped Frame Sent →

**Frame Passes ICV
Forwarded to Dest MAC** →

← **Upper Layer
Protocol Fails CRC
Sends Predictable
Error Message to
Source MAC**

← **AP WEP Encrypts
Response and
Forwards to Source MAC**

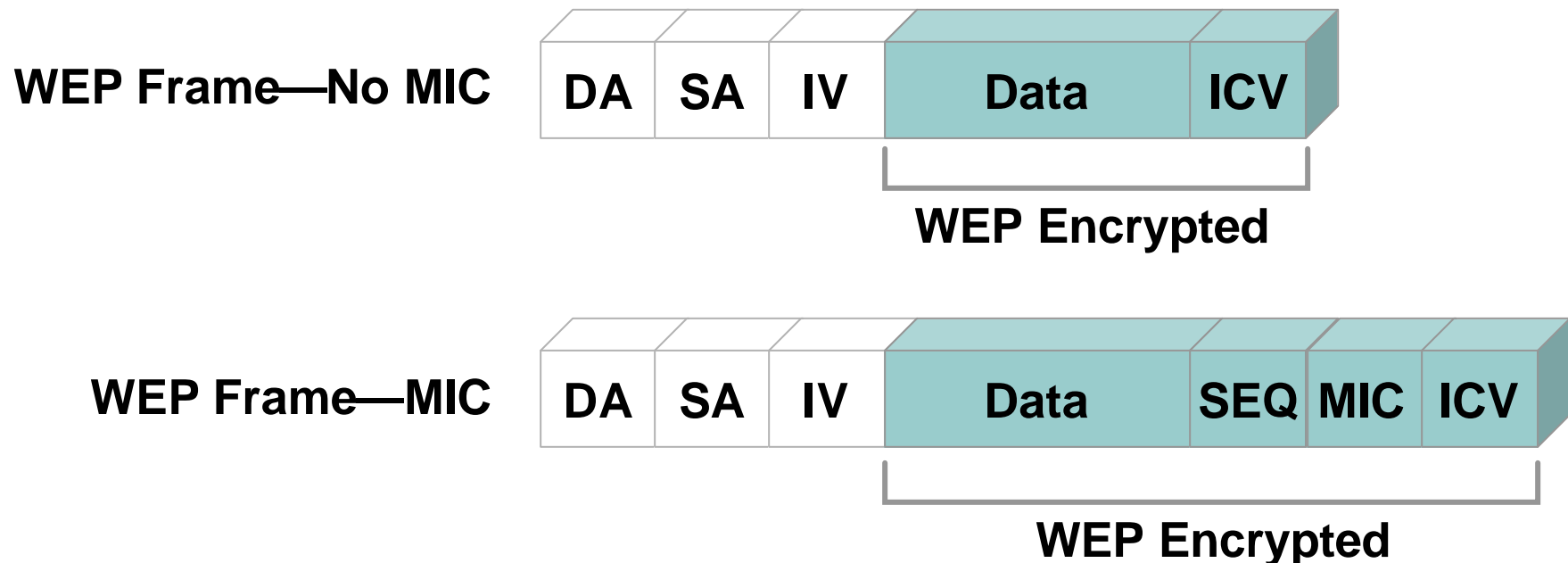
← **Attacker Anticipates
Response from Upper
Layer Device and
Attempts to Derive Key**

Message Integrity Check (MIC)

- **The MIC will protect WEP frames from being tampered with**
- **The MIC is based on seed value, destination MAC, source MAC, and payload**
 - Any change to these will change MIC value**
- **The MIC is included in the WEP encrypted payload**

Message Integrity Check

- MIC uses a hashing algorithm to stamp frame
- The MIC is still pre-standards, awaiting 802.11i ratification



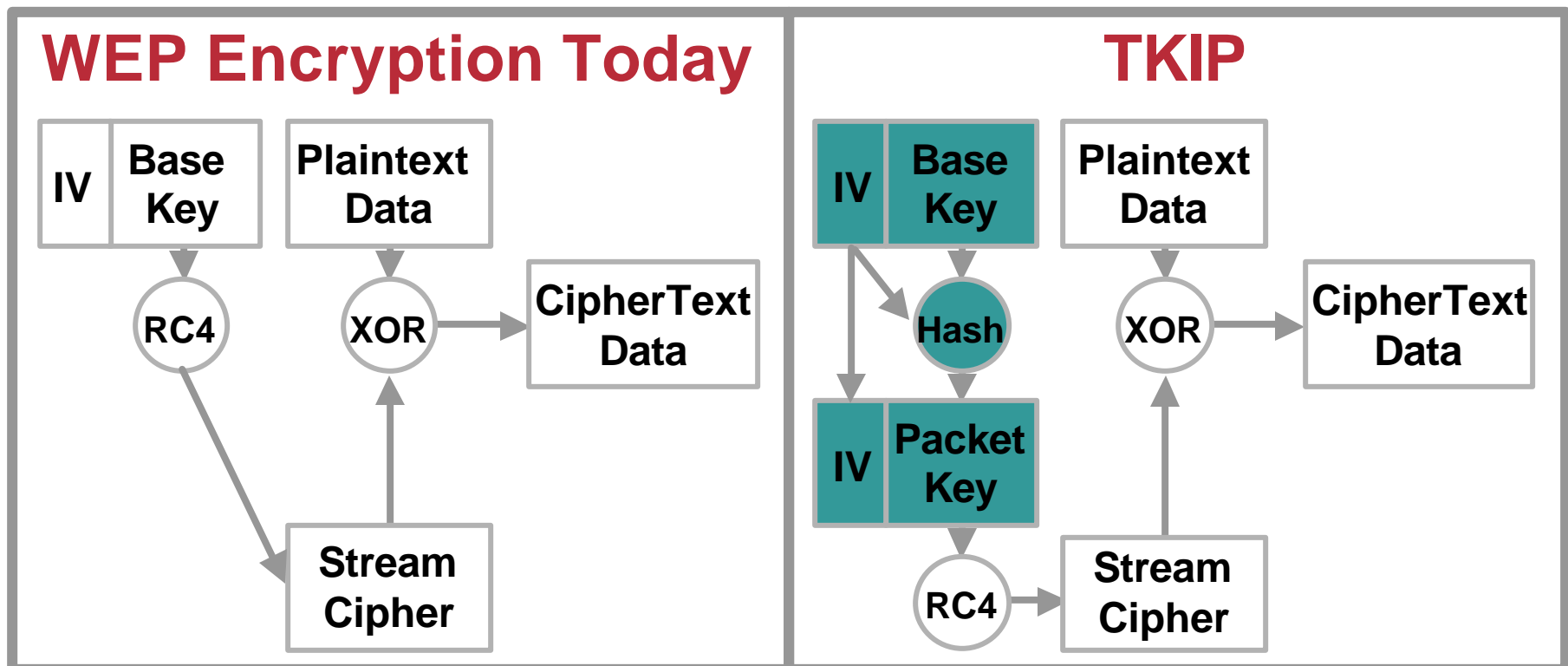
Temporal Key Integrity Protocol (TKIP)

Cisco.com

- **Base key and IV hashed**
Transmit WEP Key changes as IV changes
- **Key hashing is still pre-standards, awaiting 802.11i ratification**

WEP and TKIP Implementations

- WEP today uses an IV and base key; this includes weak IVs which can be compromised
- TKIP uses the IV and **base** key to **hash** a new key—thus a new key every packet; weak keys are mitigated



WECA Security Improvements

- **Will develop a new test plan that will require TKIP as part of certification**
- **This will include 128 bit encryption**
- **Products certified prior to new plan will not need to be re-tested (and do not need to include TKIP)**

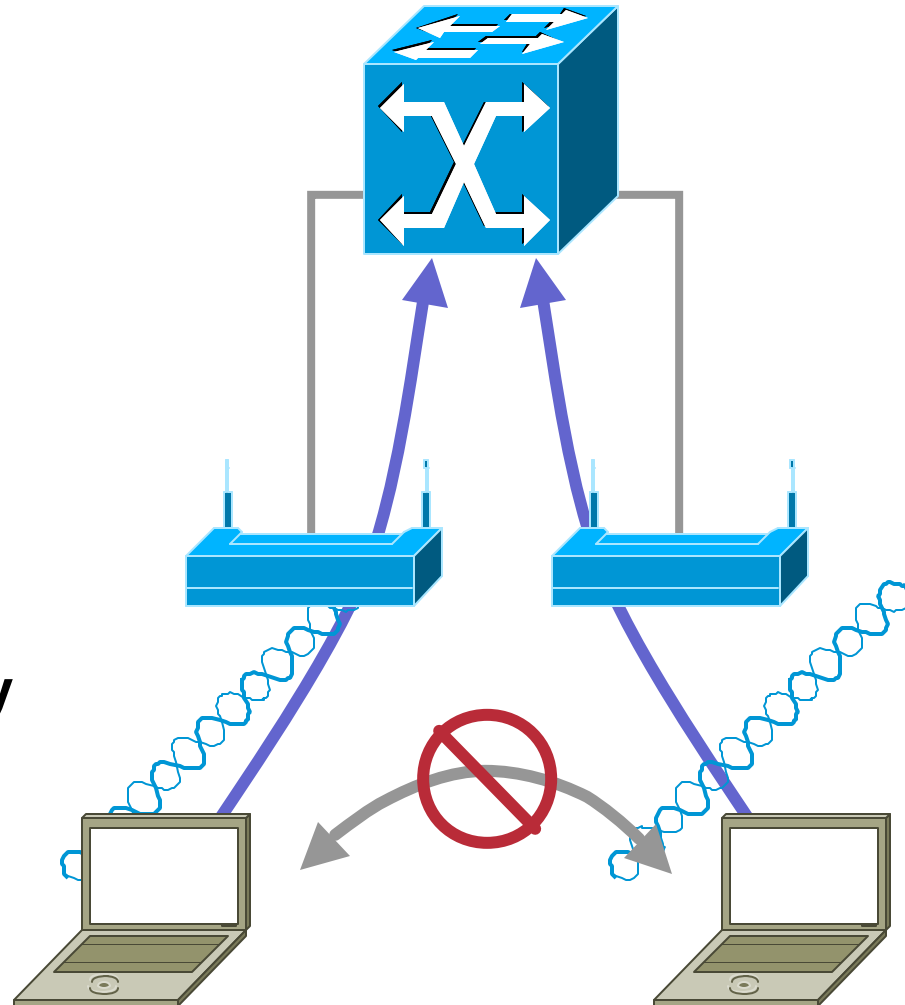
Broadcast Key Rotation

- **Pre-11.10T broadcast key is static**
- **Every user in the APs cell uses the same broadcast key**
- **Static broadcast key is vulnerable to AirSnort attack over time**

Similar to pre-11.10T static WEP keys

PSPF—Blocking Inter-Client Communication

- **PSPF—Publicly Secure Packet Forwarding**
- **Prevents WLAN inter-client communication**
- **Relies on MAC address**
- **Same subnet devices only**



Managing Your Secure 802.11 Network

- **Static WEP keys not only are insecure, but difficult to manage and scale**
- **Cisco EAP (Leap) utilizes RADIUS servers, and a single database to manage users' credentials**
- **Cisco APs support management via SNMP, WEB (with secure User Manager settings), CiscoWorks 2000, and Wavelink**

IEEE 802.11i Security Task Group

Cisco.com

- Presently incorporates TKIP and MIC as **informative text**

Software upgrade capabilities

Provides migration path for existing installations

- **Advanced Encryption Standard (AES)**

Second alternative

AES will require a hardware implementation for performance issues (software can reduce throughput by as much as 75%)

- **Completion date—????? (date to come)**

Now Available

Cisco.com

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

The SAFE Blueprint is a flexible, dynamic blueprint for security and VPN networks

Shows what changes when WLAN is introduced into the SAFE Enterprise and SMB designs

Available as of 12/31/01

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

<http://www.cisco.com/go/safe>

Summary

- **As a WLAN user, you need to understand:**
 - What is available**
 - What works with your system**
 - What systems work with what other systems**
 - Traditional WEP has inherent weaknesses**
 - Other methods of security need to be implemented**
 - Problem for ALL technologies of WLANS—
802.11a, 802.11b and 802.11g**
- **IEEE 802.11i is working on an industry standard**
- **Security solutions for WLANs **available** today are very strong, scalable and manageable**

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION

Networking Professionals Connection

Cisco.com

Visit Our Interactive Web Site for:

- Discussion forums
- Online events
- Biweekly newsletter

The screenshot shows the Cisco Networking Professionals Connection website. At the top, there is a navigation bar with links for Solutions, Products, Ordering, Support, Partners, Training, and Corporate. Below this is a search bar and a navigation menu with links for Home, How to Buy, Login, Register, Feedback, Search, and Help. The main content area is divided into several sections:

- Search:** A search box with a "Go" button and a "Forums" dropdown menu.
- NEWSLETTER:** A section for the Cisco Networking Professionals Newsletter, with a "Sign Up Now!" button.
- NETWORKING PROFESSIONALS CALENDAR:** A section for the networking professionals calendar, with a "Click Here!" button.
- TECH TALKS:** A section for technical presentations, with a "Click Here!" button.
- JOIN THE DISCUSSION:** A section for discussion forums, with a "Click Here!" button.
- Network Infrastructure:** A section for network infrastructure, with links for WAN, Routing and Switching, LAN, Switching and Routing, Network Management, Remote Access, and Enterprise Data Center Networking.
- Content Networking:** A section for content networking, with links for Caching | SSL Acceleration, Live & On-Demand Content Delivery, Local & Global Server Load Balancing, and Enterprise Data Center Networking.
- Voice & Video:** A section for voice and video, with links for IP Telephony, Video Over IP, Open Voice Applications, and Contact Center | General.
- Wireless - Mobility:** A section for wireless mobility, with links for WLAN Radio Standards, Security and Network Management, and Wireless IP Voice & Video General.
- Virtual Private Networks:** A section for virtual private networks, with links for Security, Network Management Services, and General.
- Security:** A section for security, with links for Firewalling, Intrusion Detection, and AAA | General.
- Career Certifications:** A section for career certifications, with links for Certifications and Training.
- IP + Optical:** A section for IP + optical, with links for Core | Metro and Service PoP.
- TECHTALKS:** A section for technical presentations, with a "Click Here!" button.
- NETWORKING NEWS:** A section for networking news, with a "Click Here!" button.
- ASK THE EXPERT:** A section for asking questions, with a "Click Here!" button.

www.cisco.com/discuss/networking

Networking Professionals Online TechTalk

Cisco.com



Byron Henderson
Director, Enterprise Marketing



Bruce Alexander
Technical Marketing Manager

You Are Listening to...

**Securing and Managing
Your 802.11 Wireless Network**

Networking Professionals Online TechTalk

Cisco.com

**The First 25 Listeners Who
Fill Out an Evaluation Will
Receive a Free CD**

***Cisco Aironet Wireless
Networking Solutions***

Click on

Evaluation



Networking Professionals Online TechTalk

Cisco.com

Live Q&A

Submit Your Questions Now!

Networking Professionals Online TechTalk

Cisco.com



- **Cisco's 13th annual user conference**

More than 100 technical training sessions on Cisco products, technologies and solutions—led by Cisco experts

For more information and to register:

www.cisco.com/networkers

Networking Professionals Online TechTalk

Cisco.com

**Want to Know More About
Securing and Managing
Your 802.11 Wireless Network?**

**Contact Your Local
Cisco Account Representative**

This Networking Professionals Online Tech Talk Has Ended

Thank You for Participating