Cisco Systems®

Denver Tech Days 2002
WLAN Security

Mike Morrato

System Engineer

Cisco Systems

April 10, 2002

Agenda

- Past security methods in Wireless LANs
- The problem with 802.11 - Wireless Insecurity
- The standards based fix - 802.1x / EAP-TLS / LEAP
- Cisco security enhancements
- Bringing it all together
- Conclusion

Cisco.com

The original 802.11 security

An oxymoron by anyone’s standards

Past Security Methods

- **SSID** (Service Set Identifier)

  Commonly used feature in Wireless LANs which provides a rudimentary level of security.

  Serves to logically segment the users and Access Points that form part of a Wireless subsystem.

  May be advertised or manually pre-configured at the station.

Wired Equivalent Privacy WEP

Cisco.com

- Uses the RC4 stream cipher of RSA Data Security, Inc. (RSADSI) for encryption.
- RC4 Keystream = (24 bits IV , static WEP Key)
- Key must be shared by both the encrypting and decrypting endpoints.
- IEEE 802.11 has chosen to define how 40-bit keys work. Several vendors like Cisco support 128-bit WEP encryption with their WLAN solutions.
- Key distribution or key negotiation is not mentioned in the standard.

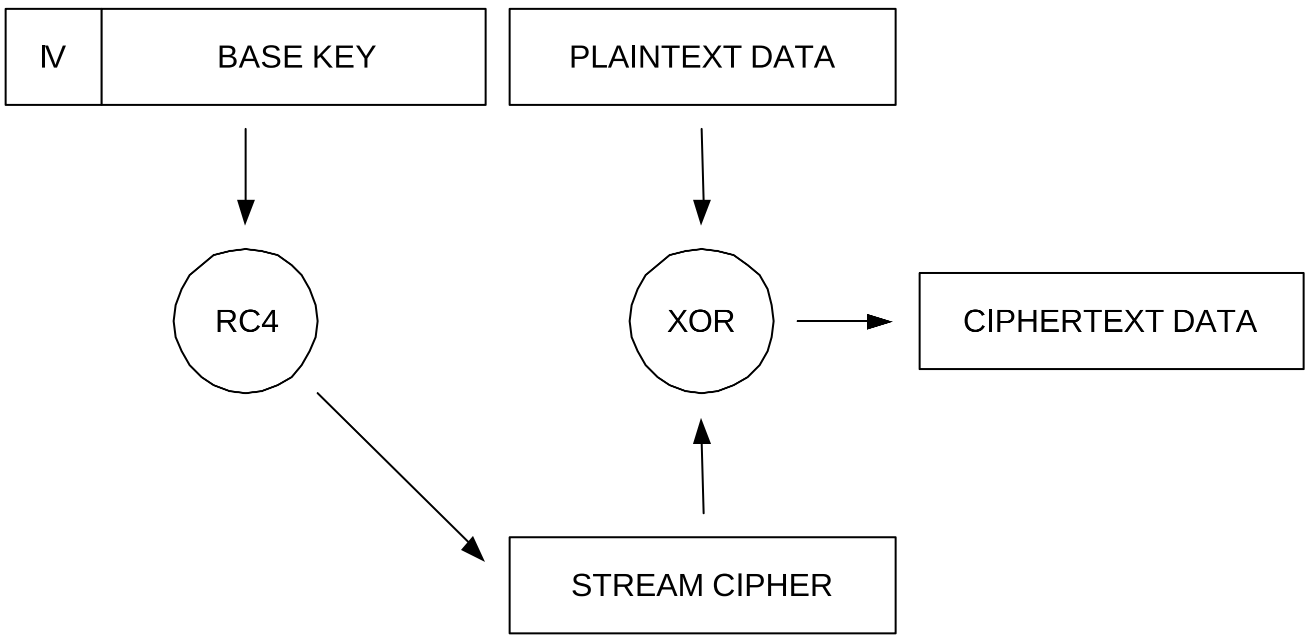
MAC Filtering

- **A list of allowed or disallowed MAC addresses**
- **Same shortcomings as static WEP key management**

IV Key Hashing

Cisco.com

Standard WEP Encryption



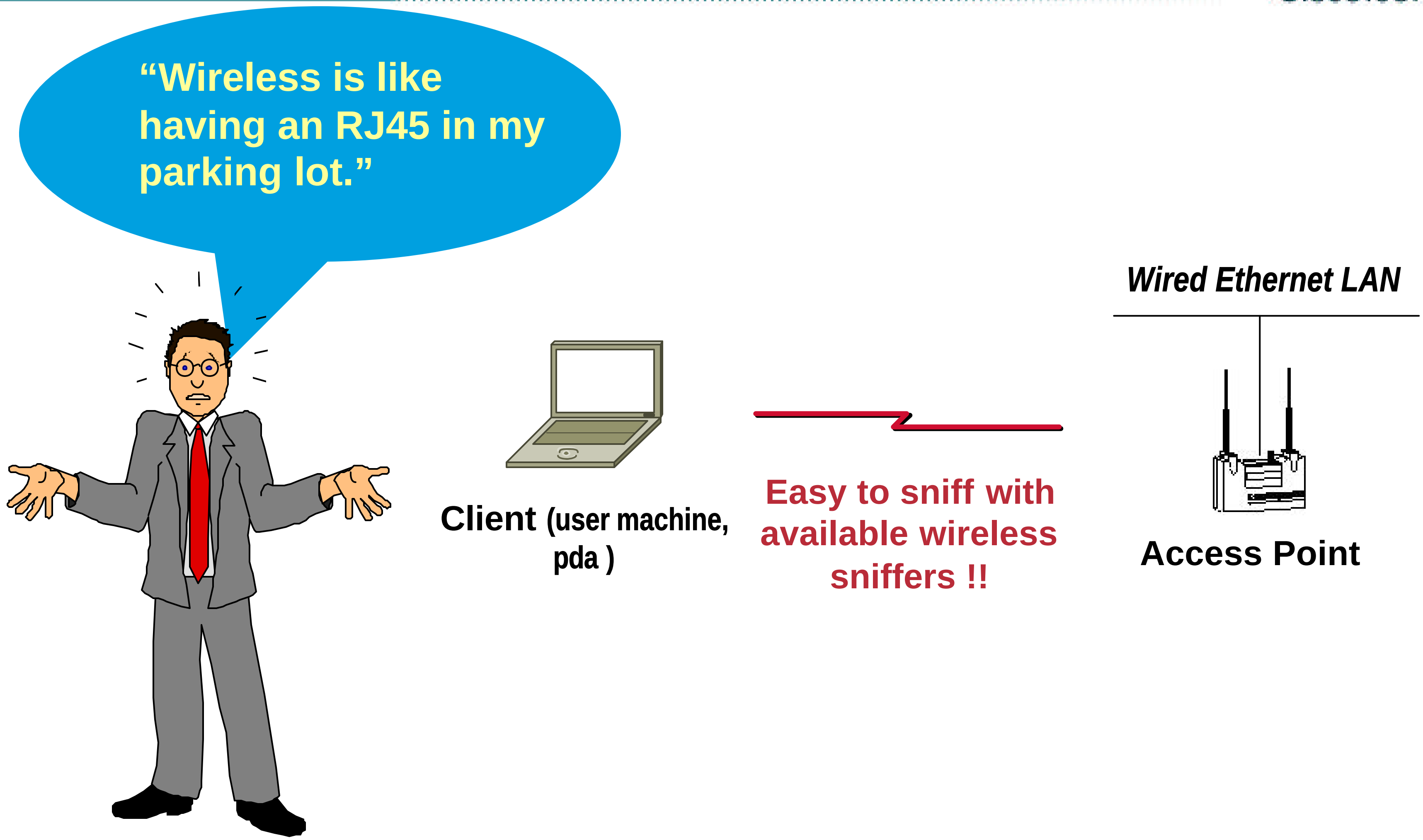
What is an IV?

- **IV is short for INITIALIZATION VECTOR**
- **24 bits long (24 bits IV + 104 bits WEP key = 128 bits)**
- **Same plaintext packet should not generate same ciphertext packet**
- **Random, and changes per packet**

Wireless Insecurity : What went wrong

Hacked in 180 seconds

Wireless LAN



Authentication/ Association

- Association is the process of associating a client with a given access point in the WLAN.
- Authentication is the process of verifying the credentials of a client desiring to join a WLAN.

SSID problem

- **32 ASCII character string**
- **Under 802.11, any client with a ‘NULL’ string will associate to any AP regardless of SSID setting on AP**
- **This is NOT a security feature!**

Issues with WEP/RC4

Cisco.com

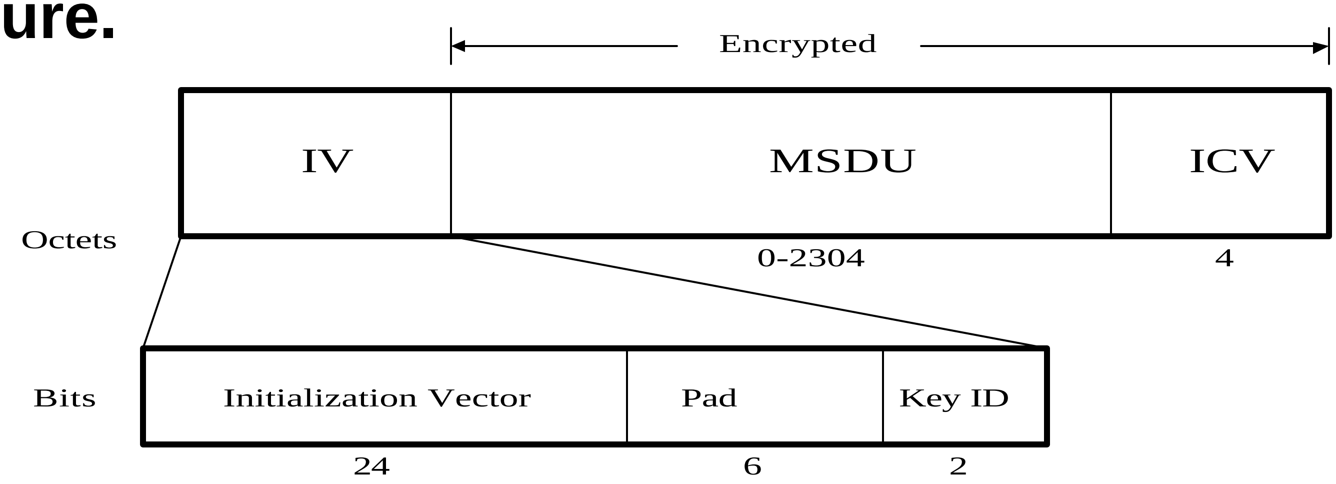
- RC4 stream cipher poorly suited in environment with packet loss

- **Known plaintext attacks are easy against RC4**

(Watch Shared-key authentication !!)

- Bad use of the IV initialisation vector. Part of the key

- ICV : CRC-32 linear, bad choice again ! Cryptographicly insecure.



Classes of Attacks Against WEP v1.0

- **IV (key) reuse**
  - **Made possible by small IV space in WEPv1.0, lack of IV replay protection**
  - **Enables statistical attack against ciphertexts w/reused IVs**
- **Known plaintext attack**
  - **Lots of known plaintext in IP traffic: ICMP, ARP, TCP ACK, etc.**
  - **Can send pings from Internet through AP to snooping attacker**
  - **Enables recovery of key stream of length N for a given IV**
  - **Can forge packets of size N by reusing IV in absence of a keyed MIC**

Classes of Attacks (cont’d)

- **Partial known plaintext**
  - May only know a portion of the plaintext (e.g. IP header)
  - Possible to recover M octets of the keystream, M < N
  - Via repeated probing, can extend keystream from M to N [Arbaugh]
  - Possible to flip bits in realtime, adjust CRC32, divert traffic to attacker
    - Enabled by linearity of CRC32, absence of keyed MIC
- **Authentication forging**
  - WEP v1.0 encrypts challenge using IV chosen by client
  - Recovery of key stream for a given IV enables re-use of that IV for forging WEP v1.0 authentication
  - Does not provide key, so can’t join LAN

Classes of Attacks (cont'd)

- **Denial of service**

  Disassociate, reassociate messages not authenticated

- **Dictionary attack**

  Possible where WEP keys derived from passwords

- **Realtime decryption**

  Repeated IV reuse, probing enables building of a dictionary of IVs, key streams

  Enables decryption of traffic in realtime

  Possible to store dictionary due to small IV space

    Need 1500 octets of key stream for each IV

    2^24 * 1500 octets = 24 GB

Issues of WEP/RC4

- **Issue #1: Stateless Protocol**
  - ✍ **Replay Attack**
- **Issue #2: Linear Checksum**
  - ✍ **Packet Modification (bits flip)**
- **Issue #3: IV Reuse**

IV Reuse Problem

Cisco.com

- RC4 keystream should not be reused
- Two packets P1 and P2 with same IV
- C1 = P1 XOR RC4(k||IV)
- C2 = P2 XOR RC4(k||IV)
- C1 XOR C2 = P1 XOR P2
- Known plaintext P1 gives P2, or use statistical analysis to find P1 and P2
- How to get known plaintext?
  - IP traffic pretty predictable
  - Authentication challenge
  - Send packets from outside

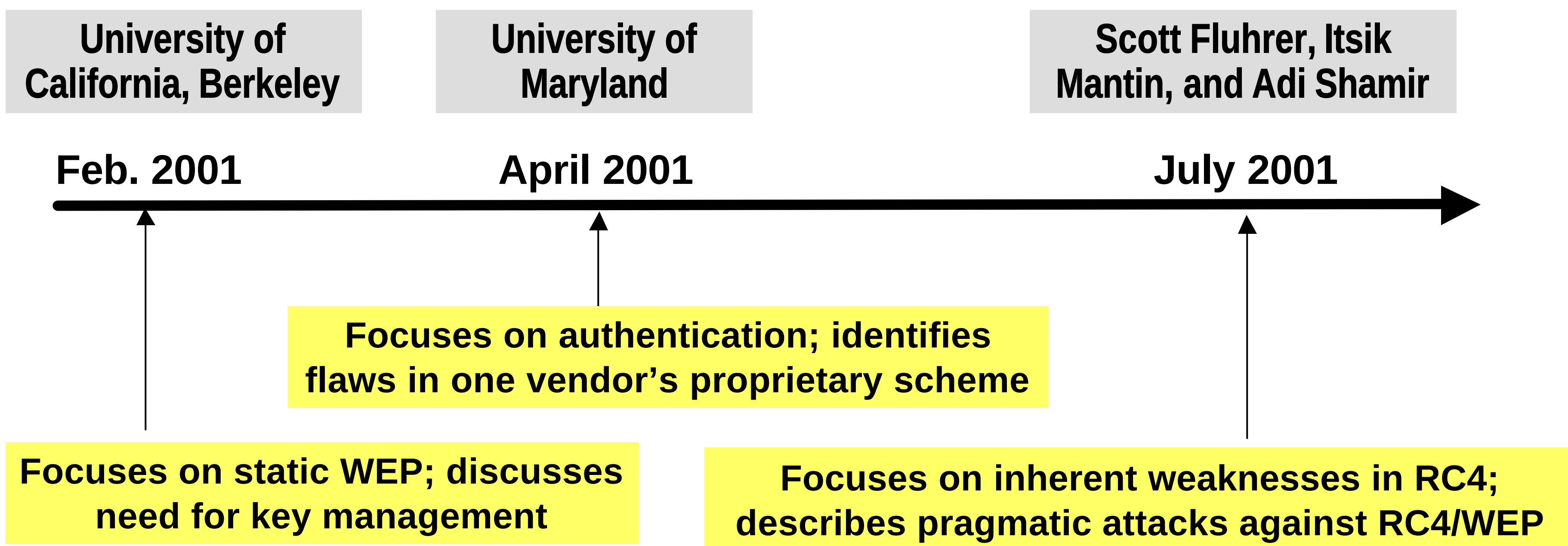
IV Collision: Can it happen?

- IV space – 2^24 possibilities ~ 16.7 Million
- Rough estimate: a busy AP sends 1000pps
- What if random IVs were used?

- Collision after 4000 packets
  - collision every 4s!
- Even with counting IV (best case)
  - rollover every few hours

Papers on WLAN Security

Cisco.com



* "In practice, most installations use a single key that is shared between all mobile stations and access points. More sophisticated key management techniques can be used to help defend from the attacks we describe…"

? University of California, Berkeley report on WEP security, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Recent Attacks

- **Weak IV Attack**

  Key recovery possible due to statistical analysis of plaintext and 'weak' IV

- **Berkeley Attack**

  DoS and key derivation via bit flipping and replay attacks

Weak IV attack

Cisco.com

- July, 25, 2001
- http://www.crypto.com/papers/rc4_ksaproc.ps
- Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir (Weizmann Institute)
  - WEP 40 bits cracked in 15-30 minutes

    With modern tools, can be cracked in 3-5 minutes
  - Scales linearily with key length

Weak IV attack

- August 6th, 2001
- Rice University
- http://www.cs.rice.edu/~astubble/wep/wep_attack.html
- Practical implementation of the attack
  - Passive attack
  - Mitigation by using discard on initial bytes of RC4 keystream
  - Quicker Key rotation + discarding weak IV pairs

- Available "tool" based on the "Fluhrer" paper : Airsnort
- http://airsnort.sourceforge.net/

Fluhrer/AirSnort Attack – Target Compromise

- **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.

- **2 Major Implementations**

  AirSnort v0.1.0

  AT&T/Rice University (not released)

UC Berkeley Attack

- **Bit Flipping**

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

- **Replay**

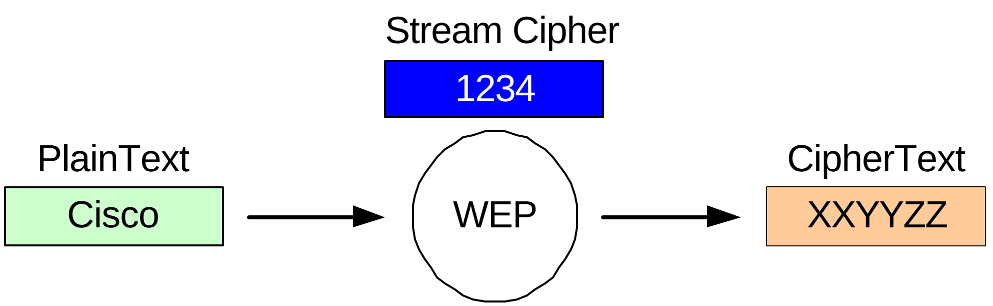
  Bit flipped frames with known IVs resent.

  AP accepts frame since CRC32 is correct

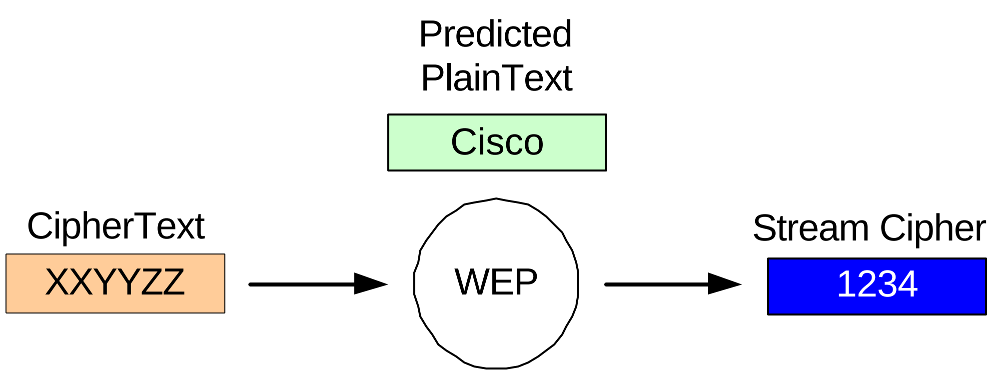
  Layer 3 device will reject, and send predictable response

  Response database built and used to derive key

UC Berkeley Attack

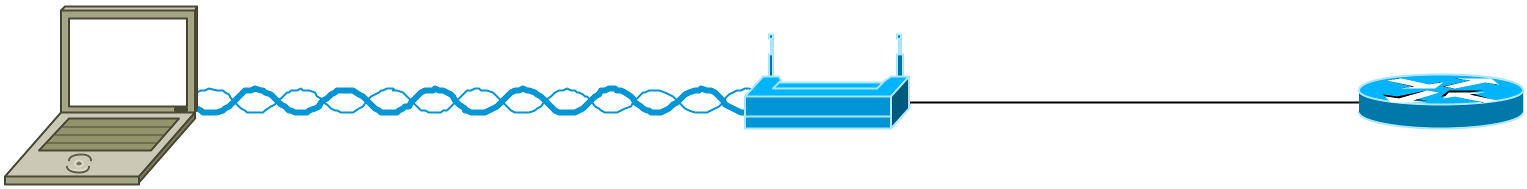


Plaintext data is XORed with the WEP stream cipher to produce the encrypted Ciphertext



If Ciphertext is XORed with guessed Plaintext, the stream cipher can be derived.

UC Berkeley Attack



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

Knight in shining armor: 802.1x

LEAP & EAP-TLS overcome basic security issues

What Is 802.1X ?

- IEEE Standard in progress
- Port Based Network Access Control

Advantages of 802.1x for Wireless LAN Security

- **Improved user authentication: username and password**
- **Dynamic, session-based encryption keys**
- **Centralized user administration**

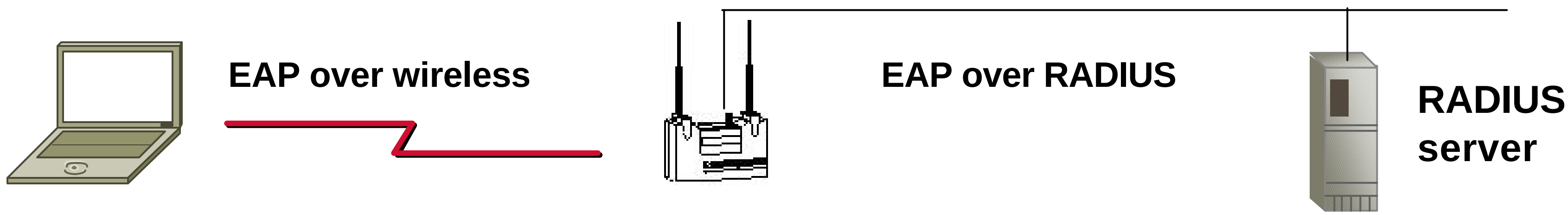
  RADIUS support (RFC 2138, 2139) for centralized authentication, authorization, and accounting

  RADIUS/EAP (draft-ietf-radius-ext-07.txt) for forwarding of EAP packets within RADIUS

General Description of IEEE 802.1x Terminology

Cisco.com

semi-public network | *enterprise edge* | *enterprise network*



Supplicant

Operates on client

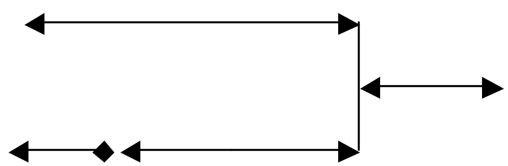
Authenticator

Operates on devices at network edge, like APs and switches

Authentication Server

EAP plug-in goes in RADIUS server

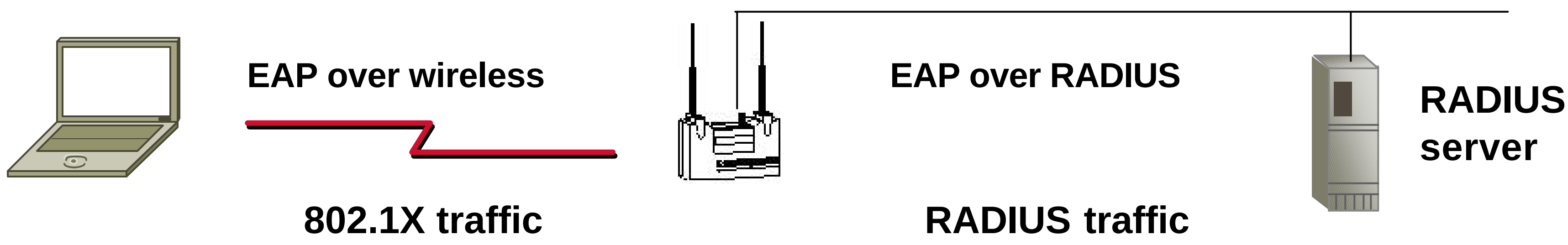
Open port:
Authentication traffic

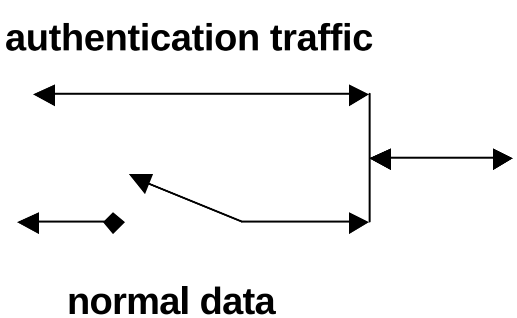


Controlled port:
Data traffic

Before EAP Start

802.11 association complete; data blocked by AP

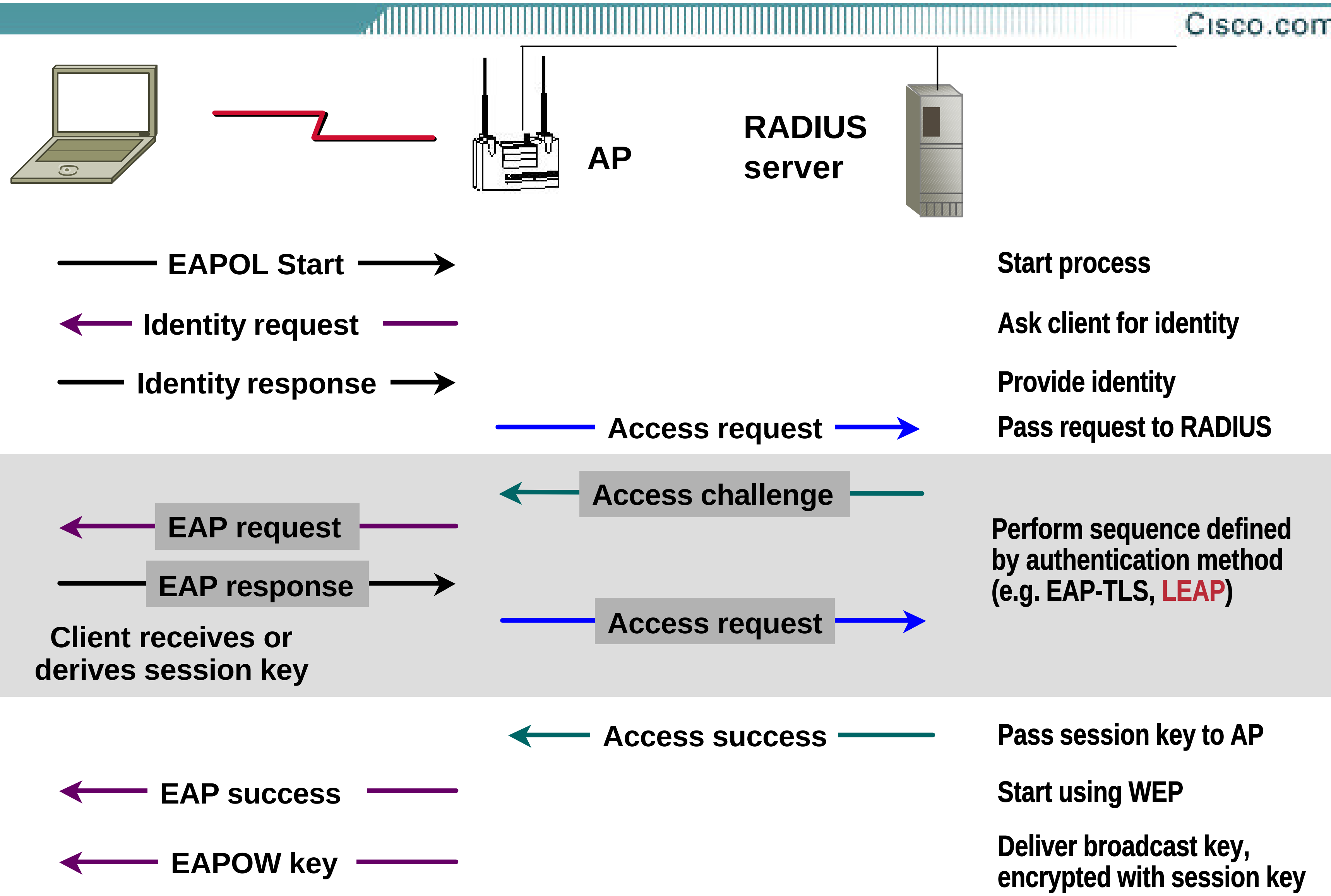




AP "encapsulates" 802.1x traffic into RADIUS traffic, and visa versa

AP blocks everything but 802.1x-to-RADIUS authentication traffic

EAP Steps



Cisco.com
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
Perform sequence defined by authentication method (e.g. EAP-TLS, LEAP)
Access request
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

Why LEAP ?

Cisco.com

- Cisco Lightweight EAP (LEAP) Authentication type
  - No native EAP support currently available on legacy operating systems
  - EAP-MD5 does not do mutual authentication
  - EAP-TLS (certificates/PKI) too intense for security baseline feature-set
  - Quick support on multitude of host systems
  - Lightweight implementation reduces support requirements on host systems
  - Need support in backend for delivery of session key to access points to speak WEP with client

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**

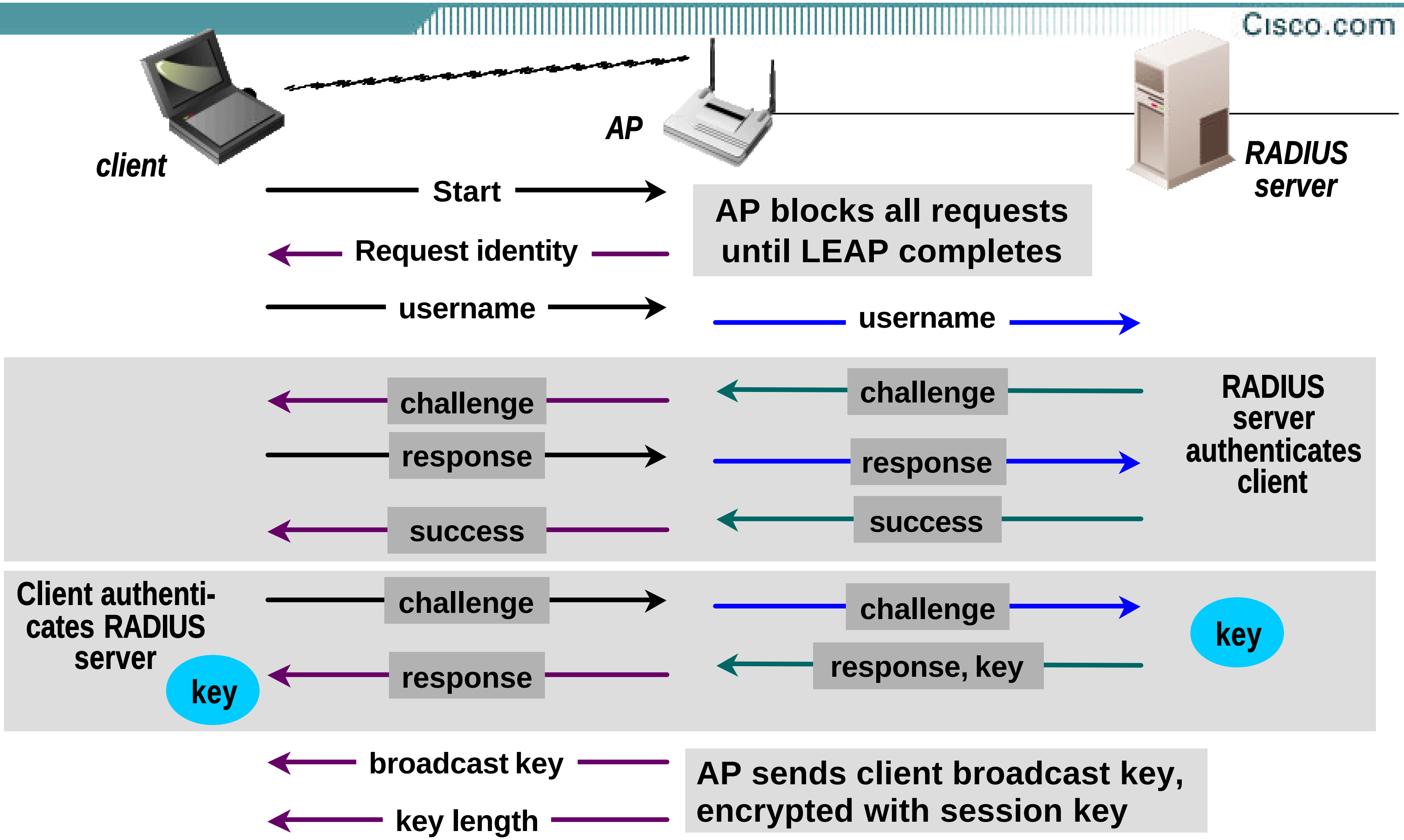
Why Cisco LEAP?

- EAP was intended for PPP, not WLAN
- IEEE 802.1x EAP over LAN (EAPOL) defines EAP encapsulation for Ethernet and Token Ring
- Need for mutual authentication between WLAN client and AAA server
- In 802.1X mutual authentication provided by

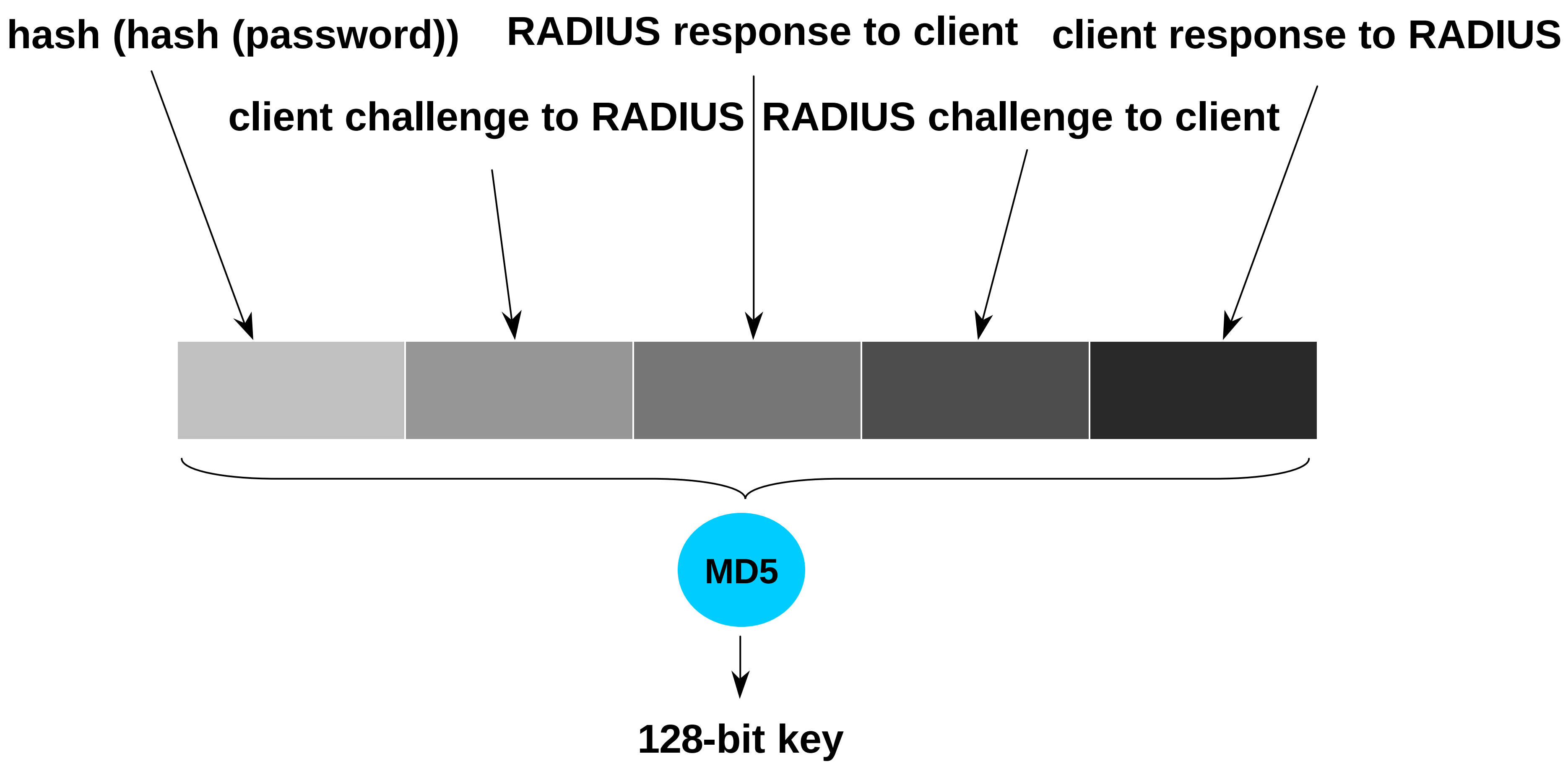
  EAP TLS (Certificates)

  EAP GSS_API (Kerberos)

LEAP Steps


Cisco.com
client
AP
RADIUS server
Start
Request identity
username
AP blocks all requests until LEAP completes
username
challenge
response
success
challenge
response
success
RADIUS server authenticates client
Client authenti-cates RADIUS server
key
challenge
response
challenge
response, key
key
broadcast key
key length
AP sends client broadcast key, encrypted with session key

Deriving the Session Key



How Often Does the Key Change?

Cisco.com

- Every time a client roams to a new AP, it will go through the same authentication and session WEP key exercise
- The radius server will also require a new authentication/key at a timed interval (programmable).
- IETF Radius attribute #27 : "Session timeout"
- This provides different WEP keys often, and totally unique keys to each client
- NOTE: This is a global setting in ACS, and may adversely impact VPN or Dial-In users, if same group is used for LEAP

Calculating WEP Timeout

- **Best known implementation of Fluhrer attack can derive WEP key in 1,000,000 packets (AT&T/Rice University)**
- **To be conservative, assume 500,000 packets**
- **Max observable packet rate for client is 1,000pps @ 64 Byte packets**
- **500,000 packets / 1000 pps = 8 min 20secs**
- **This is a WORST CASE value!**

Cisco.com

Cisco takes it one step further

Message Integrity Check

WEP Key Hashing

Broadcast Key Rotation

Locking down intra-client communication

Message Integrity Check

- **The MIC will protect WEP frames from being tampered with.**
- **The MIC is based on Seed value, Destination MAC, Source MAC, and payload.**

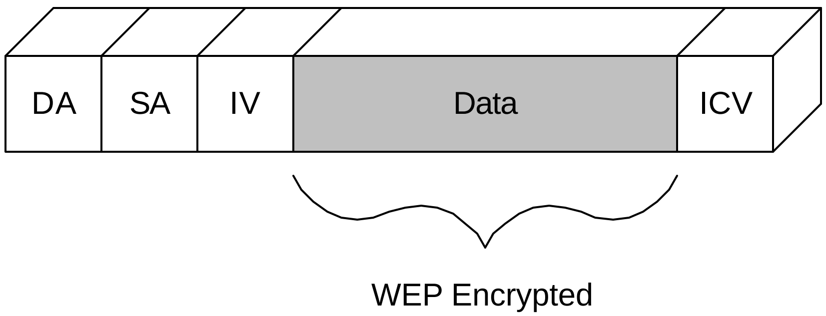
  Any change to these will change MIC value
- **The MIC is included in the WEP encrypted payload**

Message Integrity Check

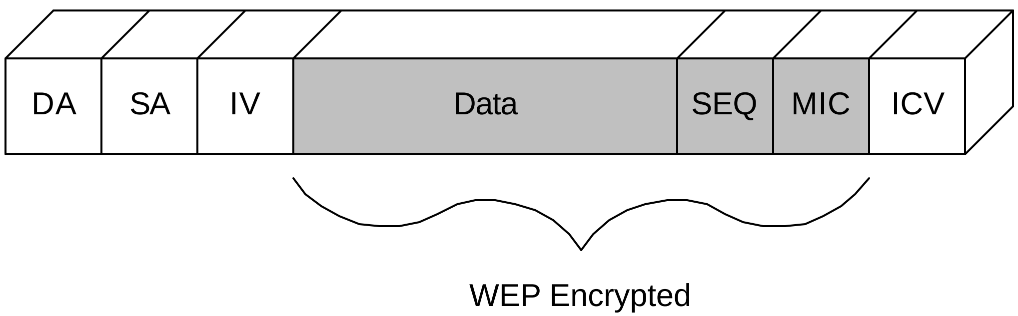
- **Unlike CRC32, MIC uses a hashing algorithm to stamp frame.**
- **The MIC is still pre-standards, so this is currently Cisco Proprietary.**

Message Integrity Check

WEP Frame - No MIC



WEP Frame - MIC



WEP Key Hashing

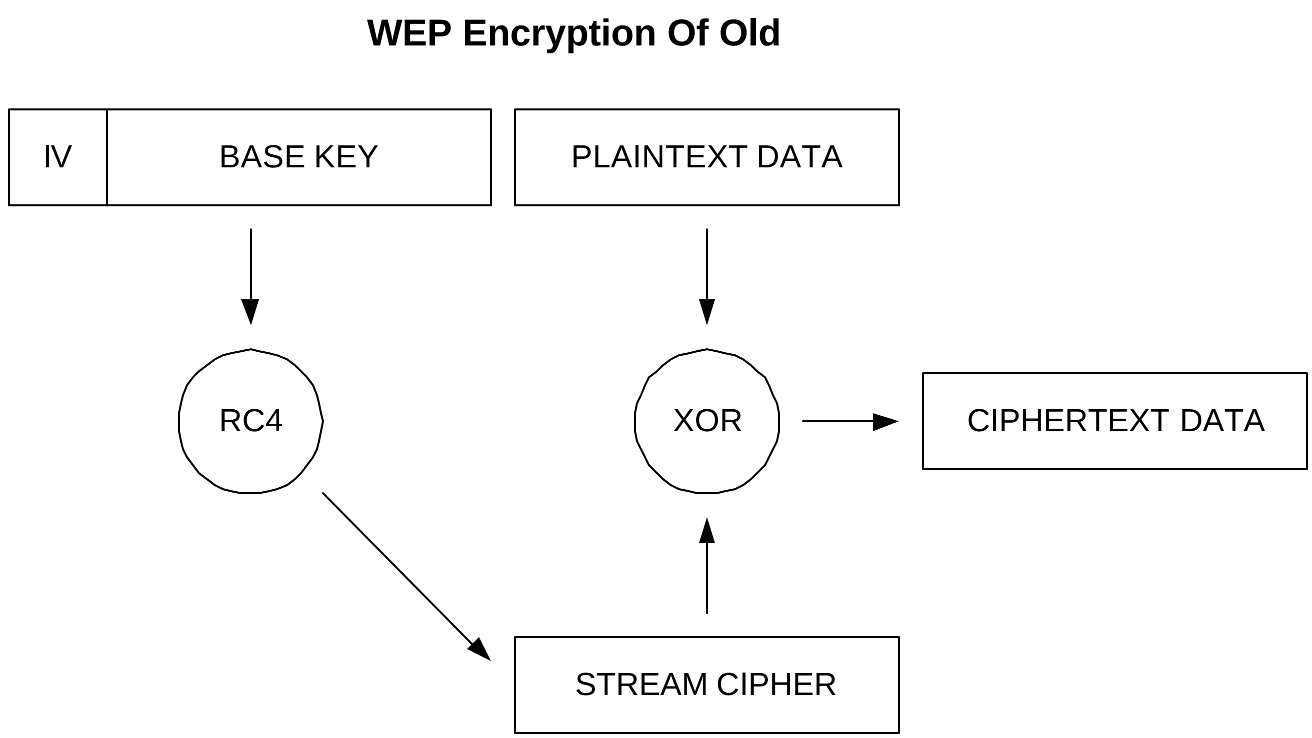
- **Base key and IV hashed**
    - **Transmit WEP Key changes as IV changes**
- **Cisco Proprietary (for now…)**

WEP Key Hashing

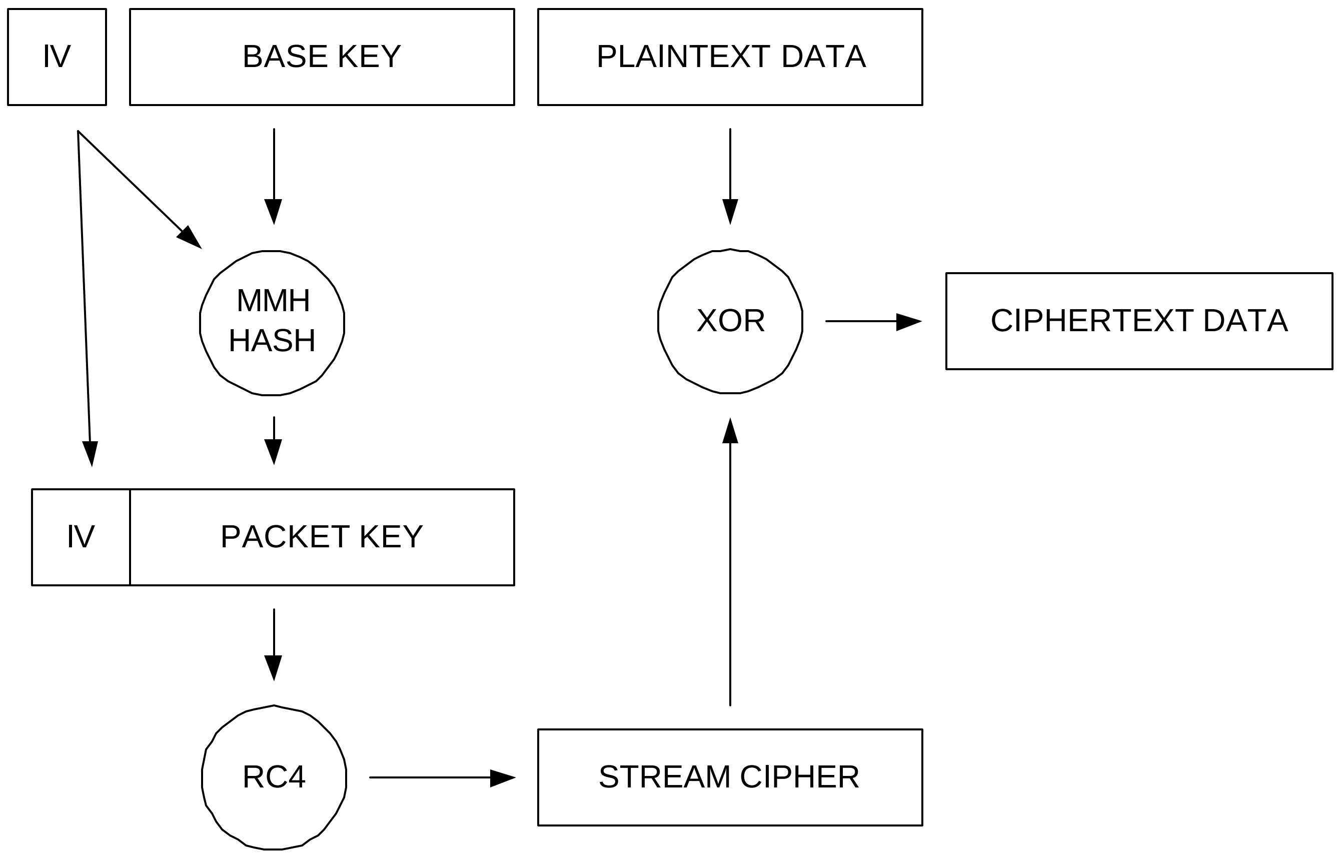
Cisco.com

- **Hash function includes the AID (association ID) in the generation of the hash key.**
- **Ensures that the key generated is different for each connection to avoid IV collisions.**
- **The uplink (packets to AP) will use even IV and downlink (packets from AP) will use odd IV.**
- **IV will increment on transmits. An anti-replay measure will verify that any receive packets with an old IV will be dropped**

WEP Key Hashing



WEP Key Hashing



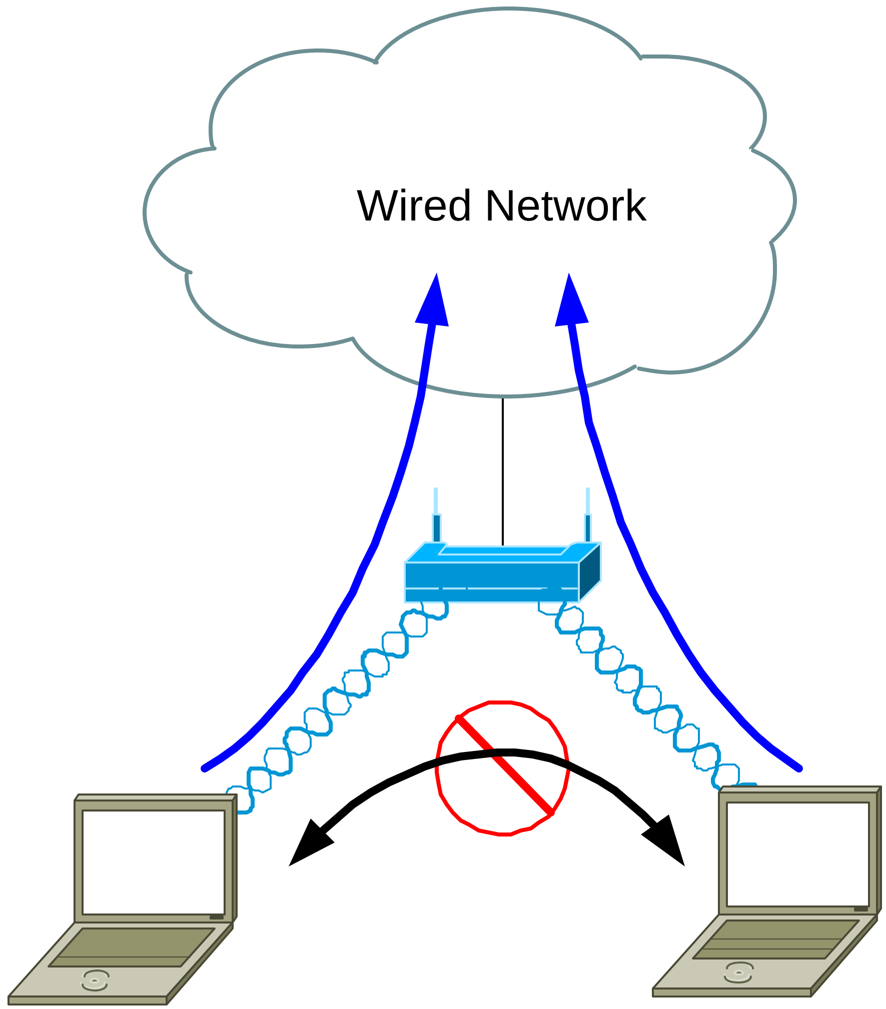
Broadcast Key Rotation

- **Prior to 11.10T, Broadcast Key is static**
- **Static Broadcast Key is vulnerable to the Weak IV attack over time**
  - **Similar to Pre-11.10T WEP Keys**
- **BK = Hash (seed, ap_mac_addr, nboots)**

PSPF - Blocking Inter-client Communication

- **PSPF - Publicly Secure Packet Forwarding**
- **Prevents WLAN inter-client communication**

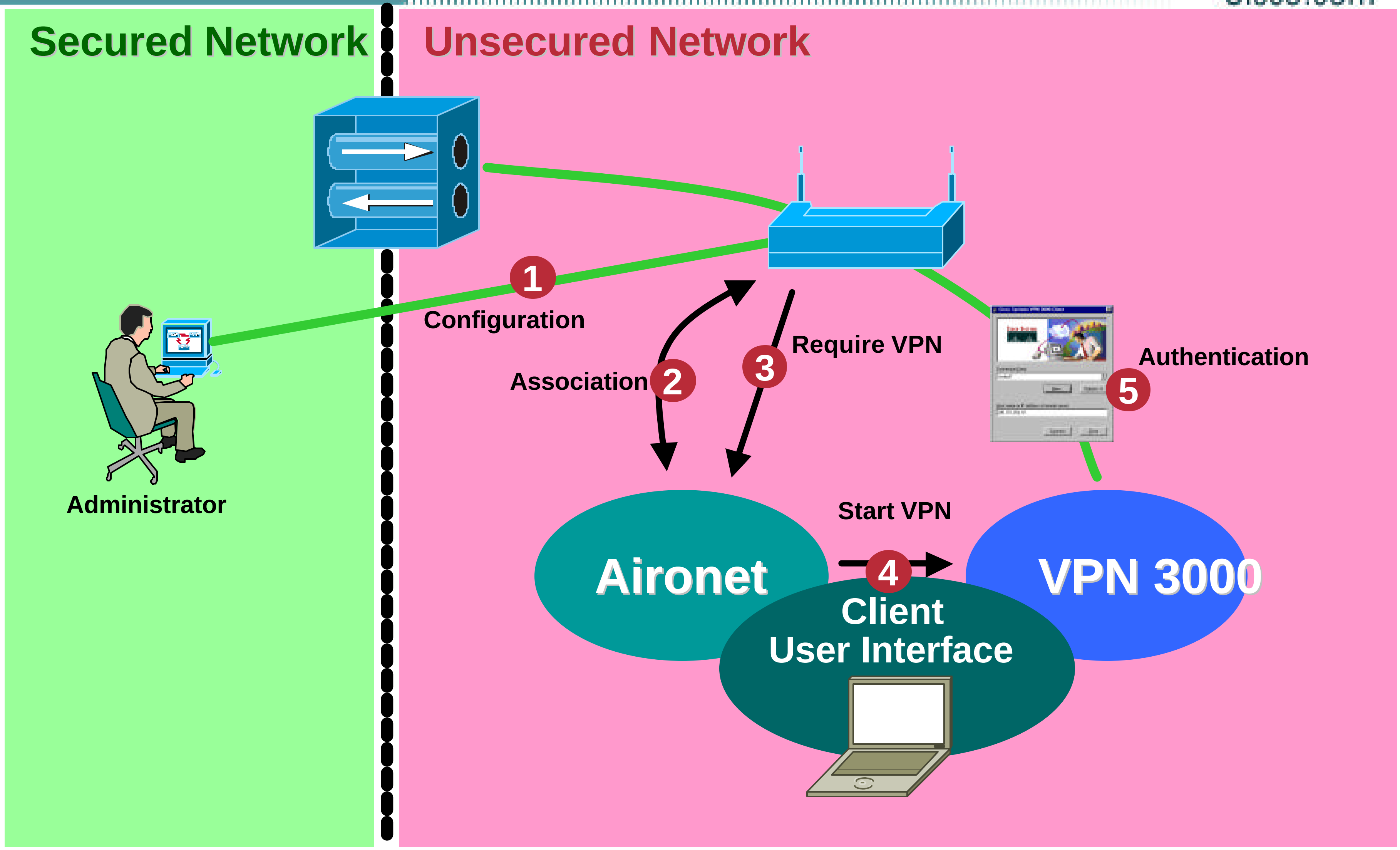
PSPF – Blocking Inter-client communication



Not secure enough?

Add a drop of IPSec, mix and let stand

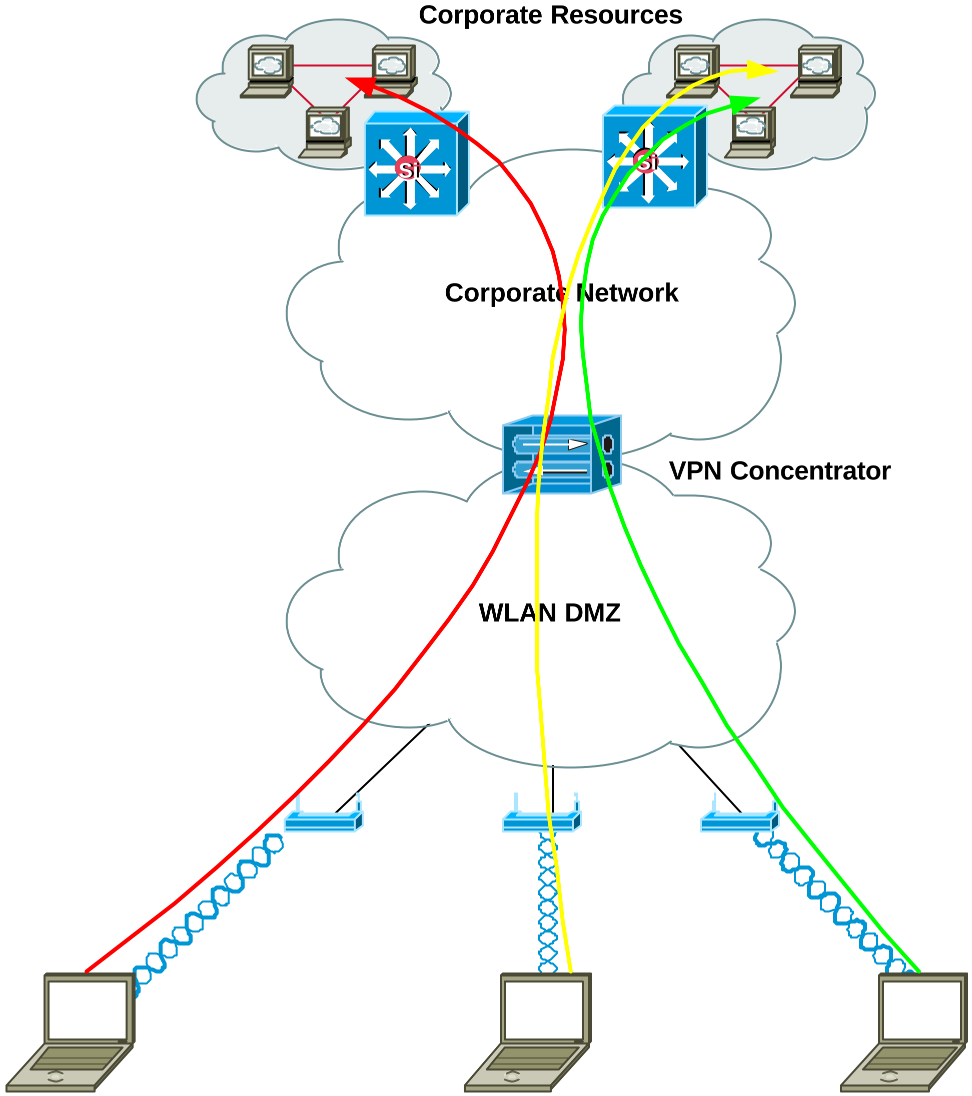
Still not enough ?



When should I use VPN?

- **In mixed client environments**
- **Where security is more important that performance or usability**
- **For home office or remote telecommuters**

VPN over WLAN Infrastructure



Bringing it all together

Recap and integration of all these features

Quick Summary – Vulnerabilities Thwarted

Cisco.com

Attacks	WEPv1.	WEPv1.0 + LEAP	WEP v1.0 LEAP B'cast Rot	WEP v1.0 + LEAP IV Hash	WEPv1.0 LEAP MIC+Replay
Unintentional IV reuse		X	X	X	X
Intentional IV reuse				X	
Fluhrer		x	x	X	
Bit flipping attack					X
Static Broadcast key			X		
Brk B'cst+replay-n-brk'ucast			X		X
Known plaintext					X
Partial known plaintext					X
Authentication forging					X
Denial of Service					
Dictionary attack					

Other features to help secure the WLAN

- **Turn off SSID Broadcast**
- **Use LEAP to authenticate MAC address**
- **Block telnet / web access to the AP**
- **Use VPN over wireless connections**
- **http://www.cisco.com/go/safe**

Cisco.com

Conclusion

Any questions?

Summary

- Standard 802.11 security is insufficient for large WLAN deployment
- 802.1X for 802.11 provides scalable and solid solution
- Only two authentication types, LEAP and EAP-TLS are really deployed in today's implementations (Kerberos ? OTP ?)
- LEAP is available on nearly every client platform and with an increasing number of backend Radius servers

Please Complete Your Evaluation Form:

Wireless LAN Security

Make your plans to attend Cisco Networkers 2002!

- **San Diego, CA - June 24-28**
- **Orlando, FL - July 8-12**

Cisco Systems

Empowering the Internet Generation℠

Cisco Systems

Empowering the Internet Generation