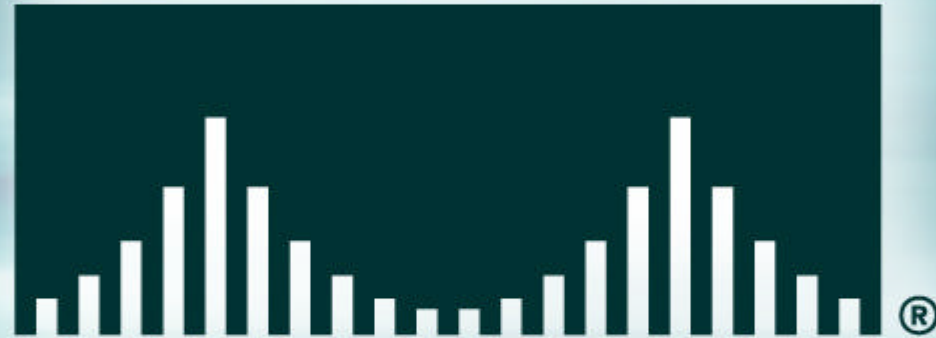


# CISCO SYSTEMS



**Beat Augsburger**  
**Systems Engineer**  
**Cisco Systems**  
**[baugsbur@cisco.com](mailto:baugsbur@cisco.com)**  
**Phone: +41 79 606 57 57**

# Agenda

Cisco.com

- **Wireless LANs Secure Ethernet Access Anywhere, Anytime**
- **Wireless LAN Standards**
- **Security**
- **W-LAN Cisco Products**

# Agenda

- **Wireless LANs Secure Ethernet Access Anywhere, Anytime**
- **Wireless LAN Standards**
- **Security**
- **W-LAN Cisco Products**

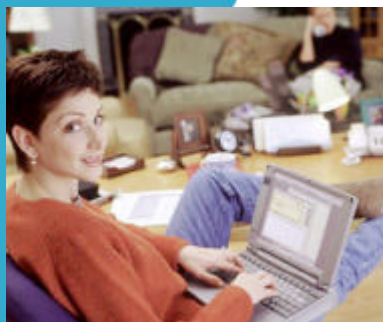
# Cisco Mobile Office

Cisco.com

**On the Road**



**At Home**



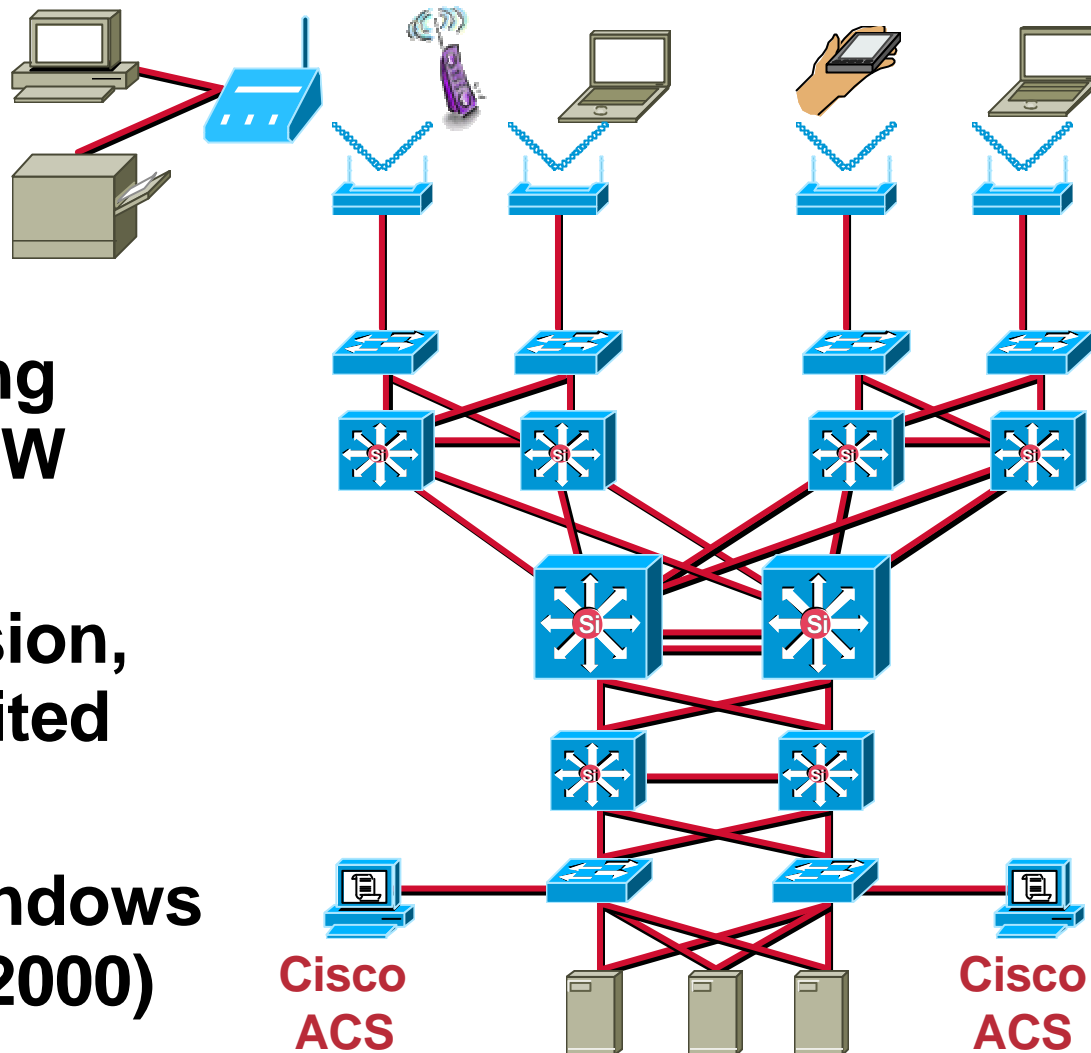
**At Work**



**Pervasive  
Connectivity**

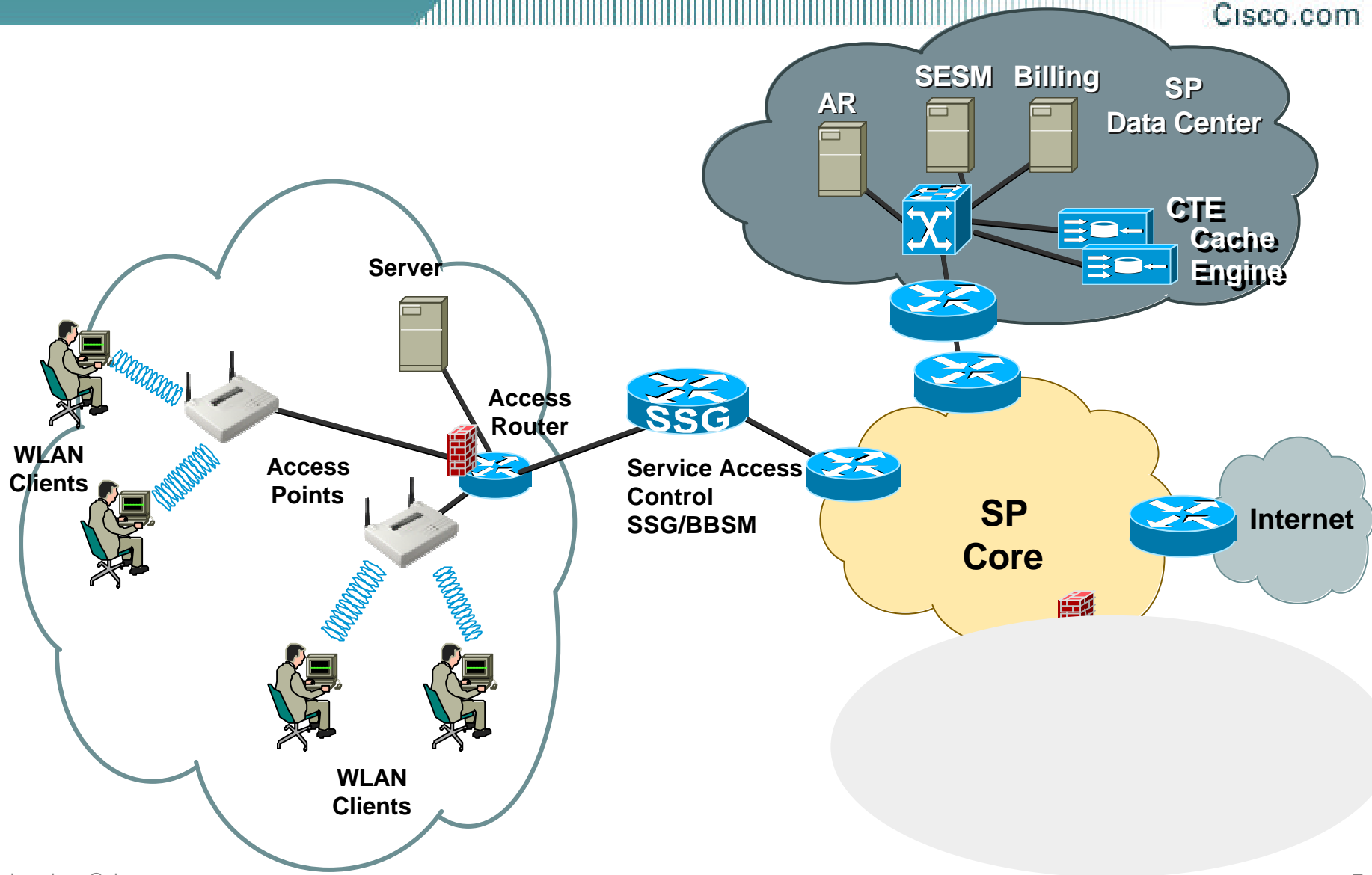
# Campus WLAN EAP

Cisco.com

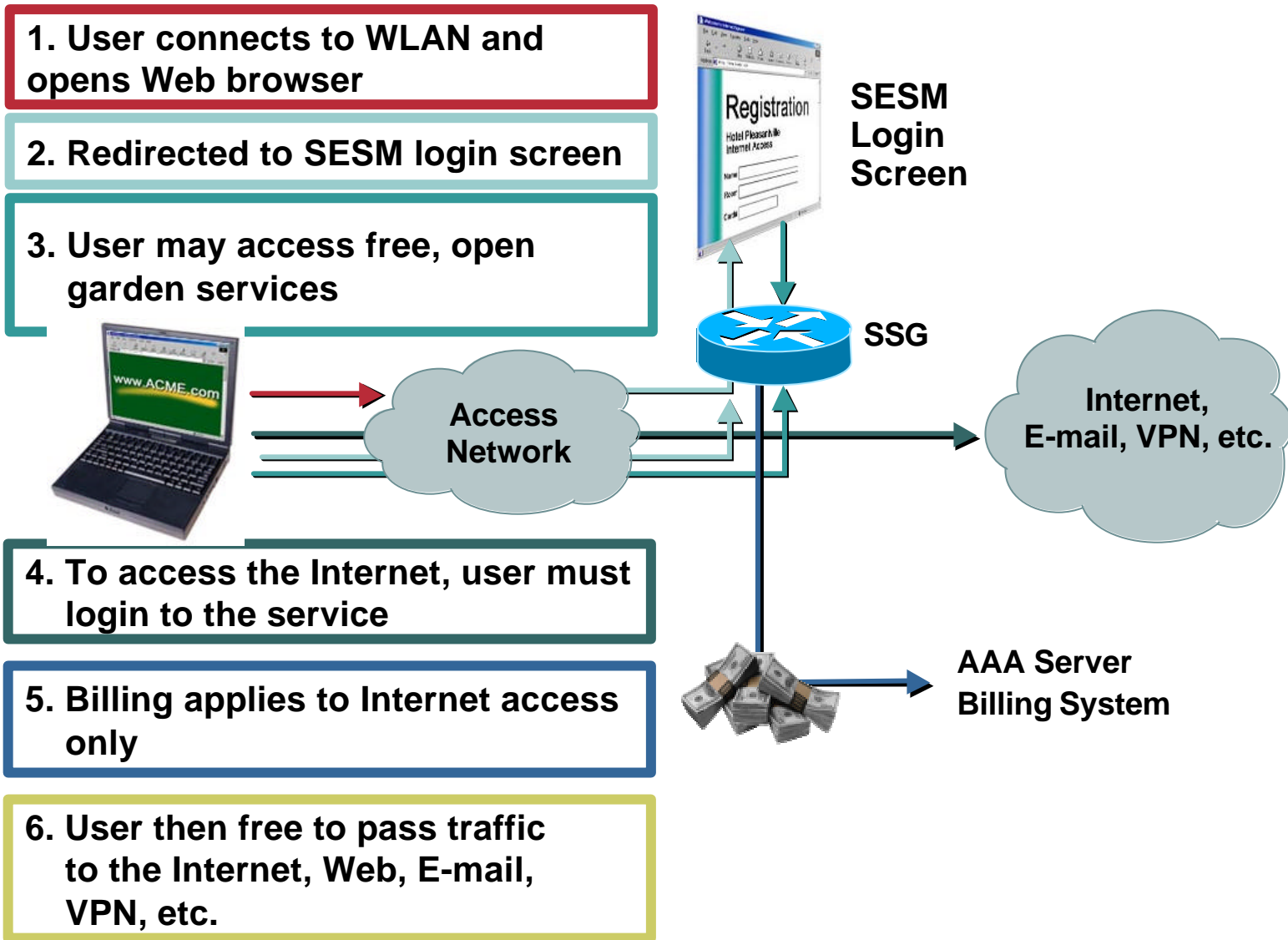


- **LEAP uses existing windows userid/PW database**
- **Dynamic per session, per user, time limited keys**
- **Cisco NICS or Windows XP (possibly Win2000)**

# PW-LAN Architecture



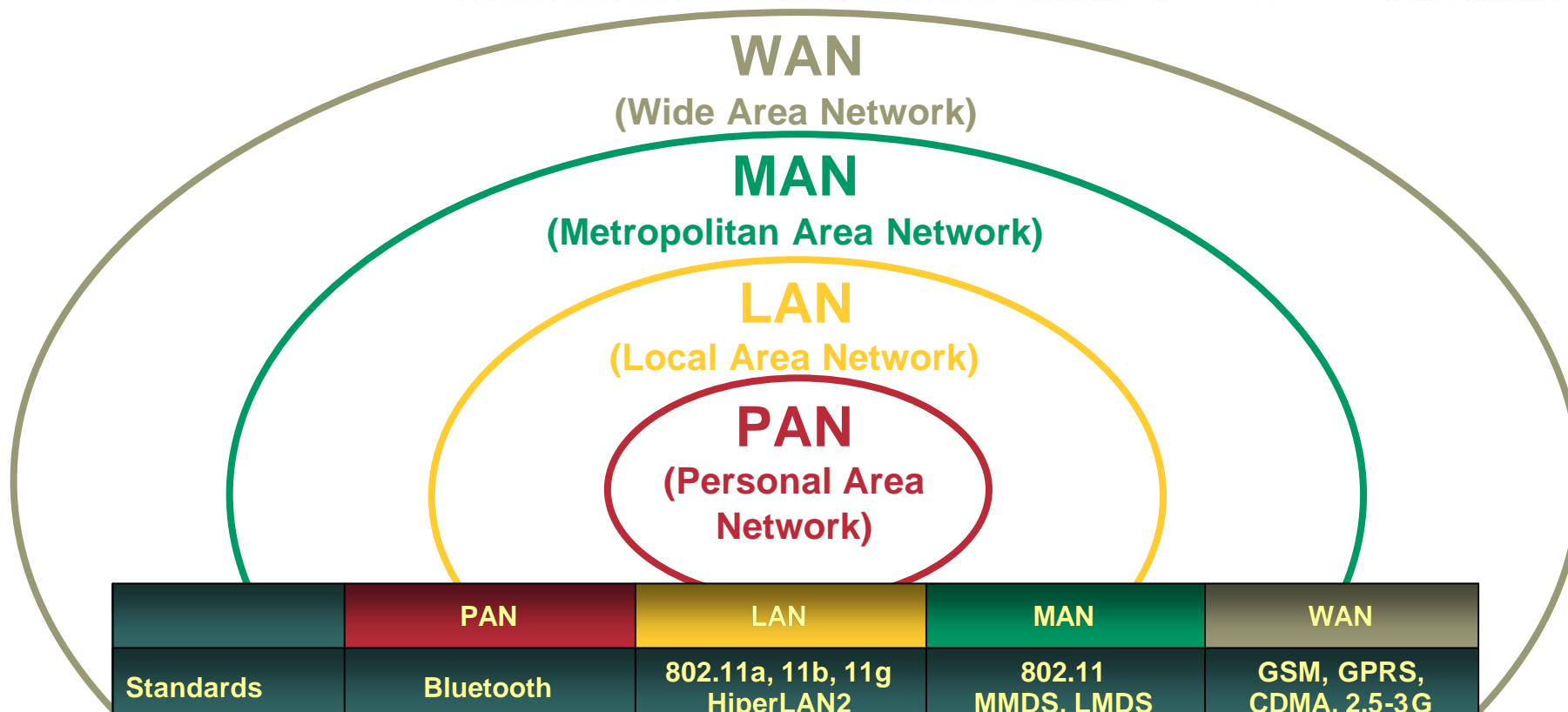
# User Experience



# Agenda

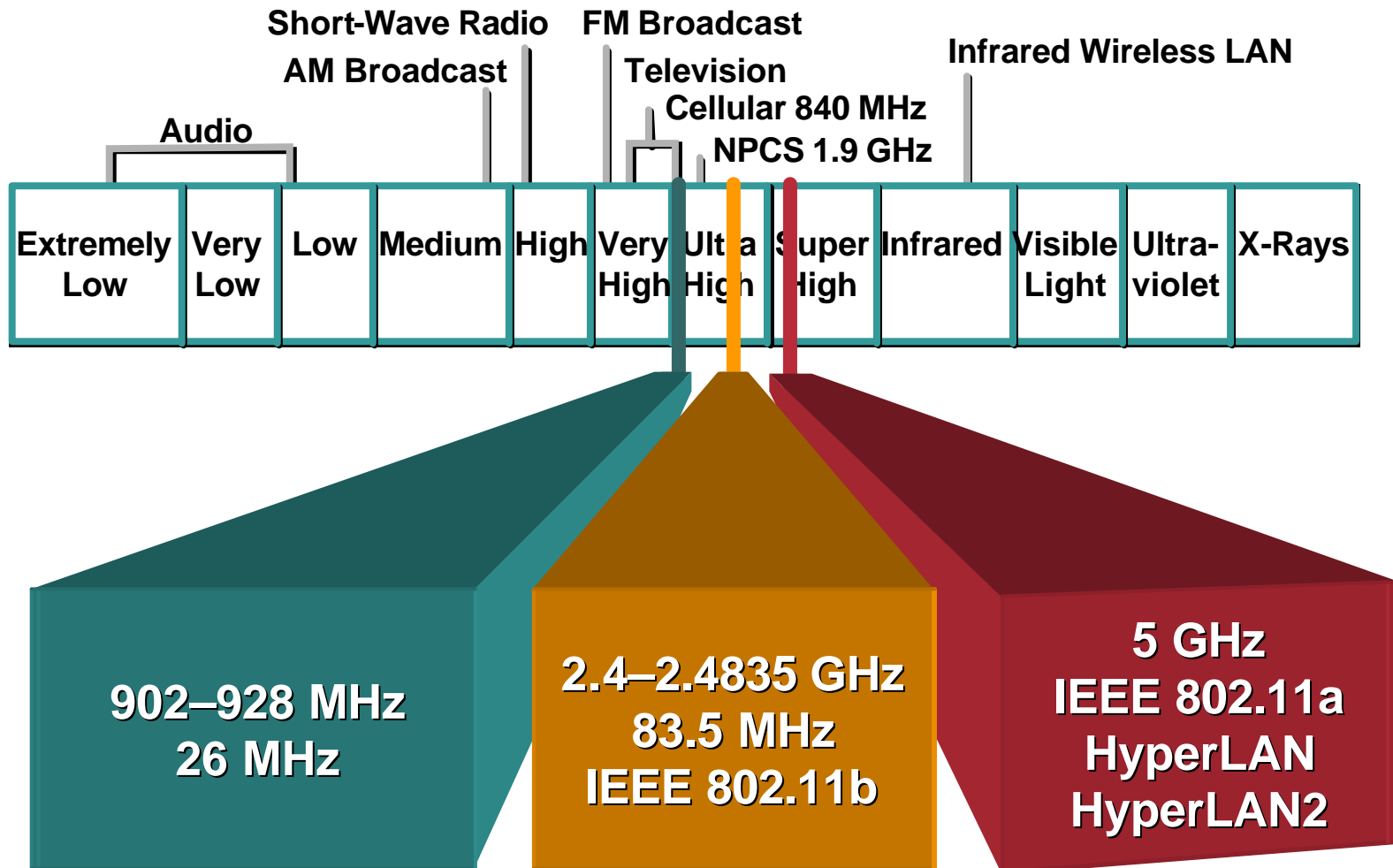
- **Wireless LANs Secure Ethernet Access Anywhere, Anytime**
- **Wireless LAN Standards**
- **Security**
- **W-LAN Cisco Products**

# Wireless Technologies



	PAN	LAN	MAN	WAN
Standards	Bluetooth	802.11a, 11b, 11g HiperLAN2	802.11 MMDS, LMDS	GSM, GPRS, CDMA, 2.5-3G
Speed	< 1 Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384 Kbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer Device-to-Device	Enterprise networks	Fixed, last mile access	PDA's, Mobile Phones, cellular access

# ISM Unlicensed Frequency Bands



# IEEE 802.11 Standard Activities

Cisco.com

- **802.11a** - 5GHz- ratified in 1999
- **802.11b** - 11Mbps 2.4 GHz- ratified in 1999
- **802.11d** - Additional regulatory domains
- **802.11e** - Quality of Service
- **802.11f** - Inter-Access Point Protocol (IAPP)
- **802.11g** - Higher Data rate (>20 Mbps) 2.4 GHz
- **802.11h** - Dynamic Frequency Selection and Transmit Power Control mechanisms
- **802.11i** - Authentication and security

# 802.11 Positioning

Cisco.com

## 5GHz - 802.11a

- **Maximum Wireless LAN performance: 54Mbps**
- **Higher expected throughput than 802.11g**
- **8 channels**
- **Works only in U.S., Japan, and other FCC countries**
- **5 GHz band has less interference**

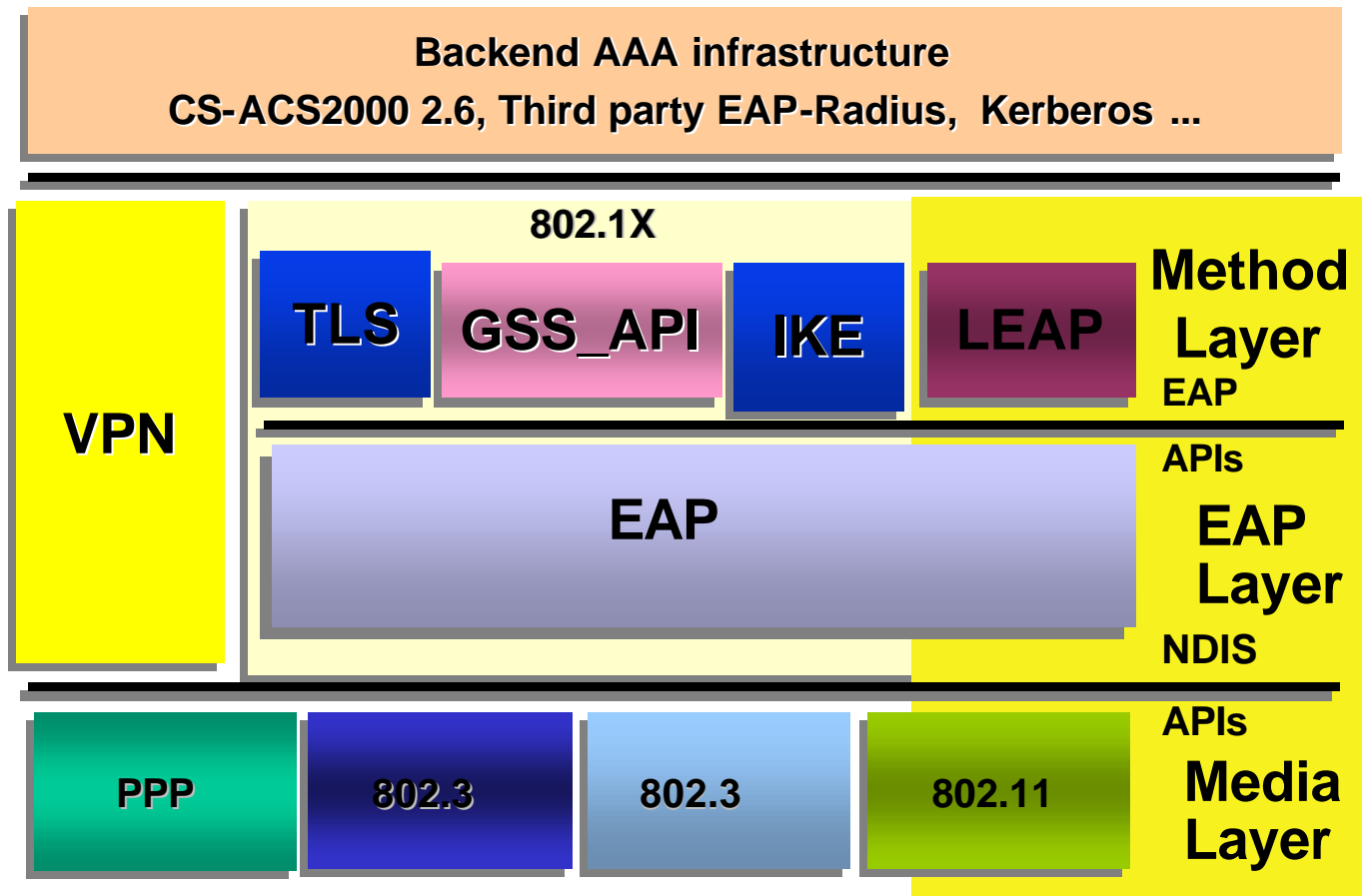
## 2.4GHz - 802.11b & g

- **11Mbps → 36Mbps → 54Mbps**
- **3 channels**
- **Worldwide compatibility**
- **Compatibility with installed base of 802.11b products**
- **Easy upgrade path to high-speed 802.11g**
- **Wide selection of client devices**
- **Lower cost products**
- **Lower power products (important for handhelds)**

# Agenda

- **Wireless LANs Secure Ethernet Access Anywhere, Anytime**
- **Wireless LAN Standards**
- **Security**
- **W-LAN Cisco Products**

# Cisco Security Framework



# 802.1X Authentication Types

- **EAP**

Extensible Authentication Protocol (EAP) is a flexible authentication protocol (specified in RFC 2284) that typically rides on the top of another protocol such as 802.1X, RADIUS, or TACACS+. It is an extension of the Point-to-Point Protocol (PPP) that enables the support of advanced authentication methods without the need to update the AAA client.

- **EAP-TLS (Transport Layer Security)**

802.1X EAP authentication algorithm based on the TLS protocol (RFC2246). TLS utilizes mutual authentication based on X.509 certificates. EAP-MD5

Username/password method that incorporates MD5 hashing for more secure authentication.

## 802.1X Authentication Types (cont.)

Cisco.com

- **LEAP**  
802.1X EAP authentication type developed by Cisco to provide dynamic per-user, per-session WEP encryption keys
- **PEAP (Protected EAP)**  
802.1X EAP authentication type designed to leverage server-side EAP-Transport Layer Security (EAP-TLS) and support a variety of different authentication methods, including log-on passwords and one-time passwords (OTPs)  
<http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-05.txt>

# 802.1X Authentication Types (cont.)

- **EAP-GTC (Generic Token Card)**  
Allows One Time Password (OTP) authentication.
- **EAP-TTLS**  
is an 802.1X EAP authentication type from Funk Software that provides similar functionality to PEAP. It uses server-side TLS and supports a variety of authentication methods, including passwords and OTPs.
- **EAP-SIM**  
EAP mechanism for authentication and session key distribution using the GSM Subscriber Identity Module  
<http://www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-05.txt>

# 802.1X Authentication Types (cont.)

- **LEAP (EAP Cisco Wireless)**
  - User authentication via user ID and password
  - Supports Windows, CE, Linux, Mac OS, and DOS
  - Licensed to Apple Computer and other vendors
- **EAP-TLS (EAP-Transport Layer Security)**
  - User authentication via client certificates and server certificates
  - Supported in XP and soon other Windows versions
- **PEAP (Protected EAP)**
  - User authentication via user ID and password or OTP
  - Supported by Cisco Aironet client adapters and by Microsoft in various Windows versions
  - Uses server-side TLS, which requires only server certificates
- **EAP-TTLS**
  - User authentication via user ID and password or OTP
  - Supported by Funk Software's Odyssey
  - Uses server-side TLS

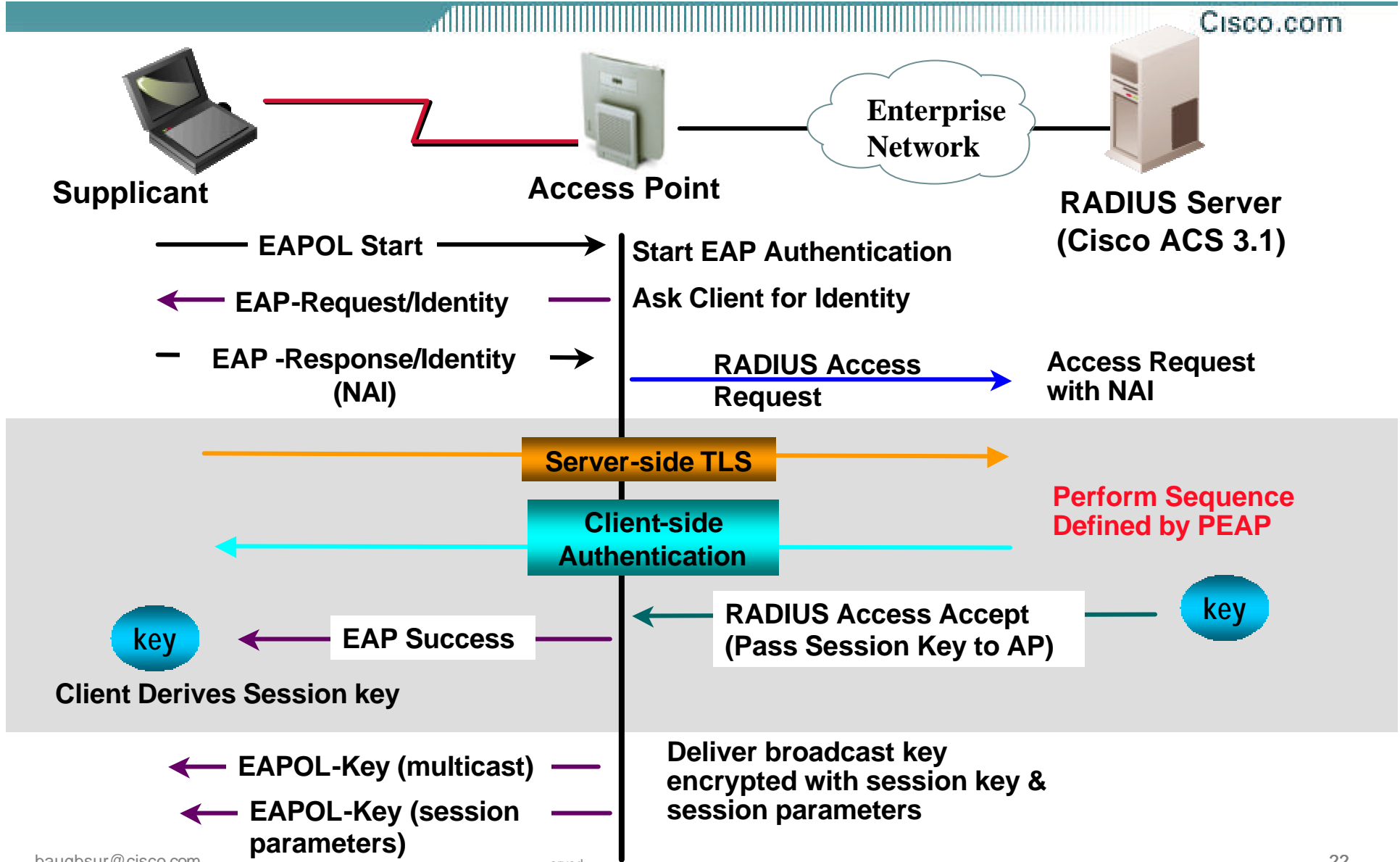
# What is PEAP?

- **802.1X- based authentication protocol**
- **Based on EAP**
- **Leverages server-side EAP-TLS using digital certificates**
- **Supports a variety of different client authentication methods, including log-on passwords and one-time passwords (OTPs)**
- **Based on a RFC Draft jointly submitted by Cisco Systems, Microsoft and RSA Security to the IETF**
- **Initial support on Windows XP**

# PEAP Authentication Process

- **Two Phase Authentication:**
  - **Phase 1: Server side TLS authentication is performed to create an encrypted tunnel (similar to SSL)**
  - **Phase 2: Methods such as Generic Token Card (GTC) are used to authenticate the Client to the Server**
- **PEAP requires Server side certificate only (whereas EAP-TLS requires both Server and Client side certificates)**

# PEAP – Two Phase Authentication



# Agenda

- **Wireless LANs Secure Ethernet Access Anywhere, Anytime**
- **Wireless LAN Standards**
- **Security**
- **W-LAN Cisco Products**

# Wireless LAN Infrastructure for the Enterprise

Cisco.com

- **The Cisco Aironet 1200 Series Access Point delivers on enterprise requirements**



# Cisco Aironet 1200 Series



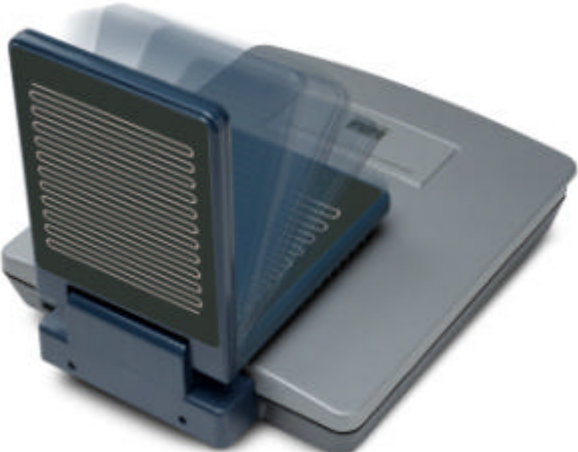
802.11b



802.11a



802.11b+a  
(802.11g+a)



# Performance

- **Initial 802.11b release**

**Builds on Cisco Aironet historic leadership in throughput and range**

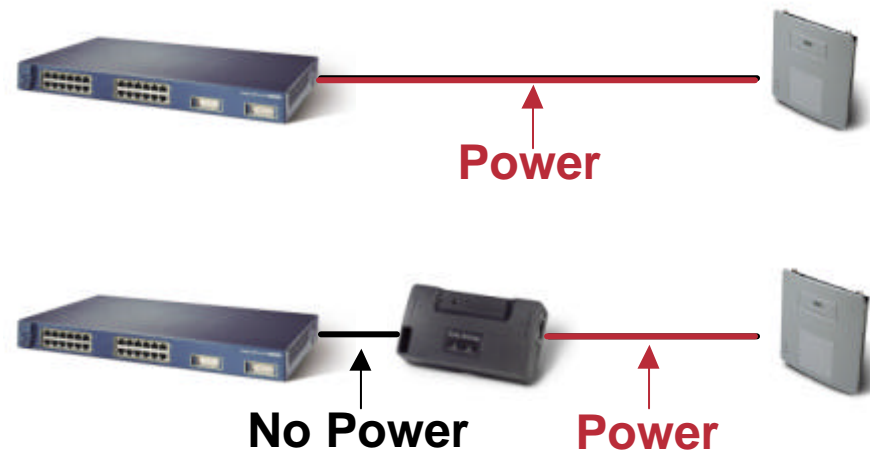
- **Follow on Dual Radio 802.11a/802.11b release**

**Delivers 54 Mbps, the next generation of performance**

# Aironet 1200 Ethernet In-Line Power

Cisco.com

- Aironet 350 uses Ethernet in-line power ONLY
- Eliminates need for local power and AC infrastructure cost
- Draws in-line power from edge devices (-48 Volts)
- Catalyst power switches support device discovery mode



## Ethernet In-line Power Source:

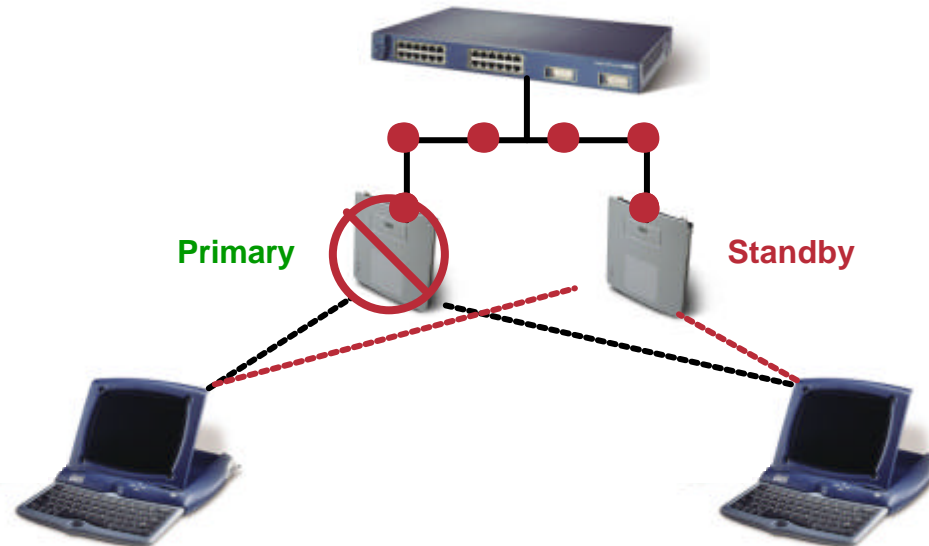
- Aironet Power Injector

## Ethernet In-line Power Source:

- Catalyst 3524-PWR XL Switch
- Catalyst 4006 and 6500 Series Switches
- 48 Port Power Patch Panel

# Redundancy-Hot Standby

Cisco.com



- Both APs have same configuration, including RF channel
- Standby AP continually monitors primary AP
- When primary AP goes down, standby AP automatically becomes active and takes over for failed primary

# Cisco Aironet 350 Series WLAN Client Adapters

Cisco.com

- PCMCIA card for Laptops and PDAs
- PCI adapter for Desktops
- Mini-PCI for embedded applications
- Driver Support
  - Windows 95, 98, Me, NT 4.0, 2000, XP
  - Windows CE 2.11, 3.0 (Pocket PC)
  - Linux
  - Mac OS 9, X
- Utilities include user configuration and site survey tool for simple installation and upgrade
- Workgroup Bridge



# 350 Series Wireless Bridge

Cisco.com

- **Building-to-building links of up to 25 miles (40.2 km)**
- **Flexibility: point-to-point and point-to-multipoint**
- **Metal case for durability and plenum rating; UL 2043 certified**
- **Inline power; simplified installation tools; industry-leading receive sensitivity**
- **Management capabilities:**
  - SNMP, Telnet, FTP, HTML
  - 802.1d spanning tree



# Cisco Aironet Antennas

## Directional

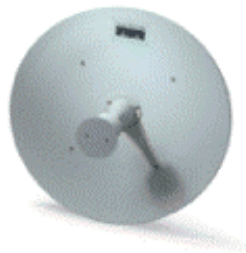
- Patch



- Yagi



- Dish



## Omni Directional

- Dipole



- Mast mount



- Ceiling mount



- Ground plane



# Pointers

- [http://www.cisco.com/warp/public/779/smbiz/wireless/wlan\\_security.shtml](http://www.cisco.com/warp/public/779/smbiz/wireless/wlan_security.shtml)
- **IEEE 802.1X**  
<http://grouper.ieee.org/groups/802/1/pages/802.1x.html>
- **RADIUS**  
<http://www.ietf.org/rfc/rfc2138.txt>  
<http://www.ietf.org/rfc/rfc2139.txt>  
<http://www.ietf.org/rfc/rfc2548.txt>  
<http://www.ietf.org/internet-drafts/draft-ietf-radius-radius-v2-06.txt>  
<http://www.ietf.org/internet-drafts/draft-ietf-radius-accounting-v2-05.txt>  
<http://www.ietf.org/internet-drafts/draft-ietf-radius-ext-07.txt>  
<http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-auth-09.txt>  
<http://www.ietf.org/internet-drafts/draft-ietf-radius-tunnel-acct-05.txt>
- **EAP**  
<http://www.ietf.org/rfc/rfc2284.txt>  
<http://www.ietf.org/rfc/rfc2716.txt>

# Wireless LAN Roadmap

# Cisco Aironet Software Roadmap: Major Themes

Cisco.com

- Enhance industry-leading WLAN security solution to extend leadership
- Provide QoS and VLAN services to support new applications
- Create partnerships to provide customer solutions for network management, wireless IP telephony, site surveys, and interoperable security
- Lead IEEE standards activities and incorporate latest standards in our products

# Twin Peaks: AP Feature Release

Cisco.com

- **VLANs**
  - Support for 16 VLANs
  - Per-VLAN security
  - Permit/Deny policies per user
- **QoS**
  - Respect for .1q tags on Ethernet side of AP
  - Voice prioritization for Symbol and Cisco 802.11b phones
- **Proxy Mobile IP (Phase 1)**
- **Admin authentication through RADIUS and TACACS+**
- **Rogue AP detection**
- **Primary RADIUS server fallback**
- **Additional accounting attributes (SIM, OTPs, VLANs, others)**
- **Handling of lost Ethernet**
- **SSH**

***Target FCS: CQ3 2002***

# Bear: Client Support for More Authentication Types on Windows

- **One-time passwords**

**PEAP: New 802.1X type**

**Leverages EAP-TLS to create secure tunnel**

**Supports authentication via OTPs (tokens), passwords, etc. through tunnel**

**Initial support will be for OTPs and PAP (clear-text passwords)**

**Requires ACS V3.1**

- **GSM-SIM**

**Some GSM phones authenticate via SIM cards**

**GSM operators want to authenticate “hot spot” users via SIM cards**

**SIM authentication can be done over EAP-TLS**

***Target FCS: CQ3 2002***

# CISCO SYSTEMS



EMPOWERING THE  
INTERNET GENERATION