Wireless LANs
Designing, Deploying, Managing and Securing an Enterprise Wireless Network

Oisin Mac Alasdair
IT Program Manager
Wireless Strategy and Architecture
Intelligent Network Solutions
Agenda

Overview of Cisco’s Current and Future WLAN

WLAN Benefits

Securing WLANs

Managing WLANs
Enterprise Wireless at Cisco

- 3,100+ APs
  - 75% 350s, 25% 1200s
- 350+ sites in ~95 countries
- Over 50,000 wireless users
- Approximately 55,000 wireless clients
  - Primarily Cisco adaptors, but CCX* clients appearing
  - ~2,000 7920 wireless handsets
  - ~3,000 PDAs (with rapid expansion underway)

* Cisco Client Extensions
Enterprise Wireless at Cisco

- Cisco Access Control Server (ACS) for AAA
  13 “hubs” world-wide
- Cisco Building Broadband Services Manager (BBSM) for guest networking
- Support overhead—approximately 1000 “calls per month”
  .24 calls, per user, per annum

Annualized cost of support = US$14.78 per user.
Current WLAN Architecture Topology

- Cisco Campus Building
- Data Centre/Site Backbone
- Cisco Remote Building
- Campus Network/WAN

EMAN
Console and Production Network—AP Connectivity

Production Network

Standard Access Layer Workgroup Switch

Cable Connected Directly to Ethernet Port on Access Point

Access Point

Console Network

Console Server, for Out of Band (OOB) Management

Cable Connected Directly to Console Port on Access Point
SSID Architecture

SSID: Voice
- EAP-FAST Authentication
- WPA Encryption
- Broadcast = NO

SSID: Guestnet
- Open authentication
- No encryption
- Broadcast = YES

SSID: Internal
- EAP-FAST Authentication
- WPA Encryption
- Broadcast = NO

All 3,100 access Points, Across All Sites, Configured with SSID Settings as Displayed

Cisco Wireless Voice Users

Cisco Wireless Data Users

NON-Cisco, Guest WLAN Users
Guest Wireless Networking

Centralized Pair of BBSMs in DMZ

“http://hotspot.cisco.com”
Guest Wireless Networking

Centralized Pair of BBSMs in DMZ

Corporate

“http://hotspot.cisco.com”

Employee Generates Access Code Via Portal

Guest

Production

Guest

Production
Guest Wireless Networking

Centralized Pair of BBSMs in DMZ

Corporate

Guest Traffic Tunneled in GRE

“http://hotspot.cisco.com”
Guest Wireless Networking

User Code Authenticated by BBSM

Centralized Pair of BBSMs in DMZ

“http://hotspot.cisco.com”
Guest Wireless Networking

Centralized Pair of BBSMs in DMZ

“http://hotspot.cisco.com”
## Snapshot—the Past, Present and Future

<table>
<thead>
<tr>
<th></th>
<th>2001 Where We Were</th>
<th>2005 Where We Are</th>
<th>2006 Where We Are Going</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Infrastructure</strong></td>
<td>Completed Initial WLAN Deployment, 3,000 AP350s, Distributed, VxWorks</td>
<td>25% of APs New Model 11xx/12xx Series; Migrated from VxWorks to IOS</td>
<td>“NexGen WLAN”; 6,000+ APs, CUWN—Cisco Unified Wireless Network; LWAPP and IOS Access Points; Introduction of 802.11n</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>WEP for Encryption, LEAP for Authentication</td>
<td>Migrating to EAP-FAST (Authentication), WPA (Encryption)</td>
<td>802.11i, Wireless Intrusion Detection Systems (WIDS); Management Frame Protection (MFP)</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>No management Tools</td>
<td>Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)</td>
<td>Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)</td>
</tr>
<tr>
<td><strong>Clients</strong></td>
<td>34,000 Cisco Adaptors</td>
<td>~50,000 &amp; ~3,000 PDAs</td>
<td>Heterogeneous CCX Environment; 60,000+ Clients</td>
</tr>
<tr>
<td><strong>Enhanced Services</strong></td>
<td>None</td>
<td>Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)</td>
<td>Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets</td>
</tr>
<tr>
<td><strong>SLA</strong></td>
<td>P4 (48 hr fix)</td>
<td>P4 (48 hr fix), Treated as P2</td>
<td>P2/P1 (Wireless as Primary Access Medium)</td>
</tr>
</tbody>
</table>

**Evolving Capabilities**

- **2001 Where We Were**
  - Completed Initial WLAN Deployment, 3,000 AP350s, Distributed, VxWorks
- **2005 Where We Are**
  - 25% of APs New Model 11xx/12xx Series; Migrated from VxWorks to IOS
  - Migrating to EAP-FAST (Authentication), WPA (Encryption)
- **2006 Where We Are Going**
  - “NexGen WLAN”; 6,000+ APs, CUWN—Cisco Unified Wireless Network; LWAPP and IOS Access Points; Introduction of 802.11n

**Management**

- **2001 Where We Were**
  - No management Tools
- **2005 Where We Are**
  - Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)
- **2006 Where We Are Going**
  - Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)

**Clients**

- **2001 Where We Were**
  - 34,000 Cisco Adaptors
- **2005 Where We Are**
  - ~50,000 & ~3,000 PDAs
- **2006 Where We Are Going**
  - Heterogeneous CCX Environment; 60,000+ Clients

**Enhanced Services**

- **2001 Where We Were**
  - None
- **2005 Where We Are**
  - Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)
- **2006 Where We Are Going**
  - Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets

**SLA**

- **2001 Where We Were**
  - P4 (48 hr fix)
- **2005 Where We Are**
  - P4 (48 hr fix), Treated as P2
- **2006 Where We Are Going**
  - P2/P1 (Wireless as Primary Access Medium)

**Evolving Capabilities**

- **2001 Where We Were**
  - No management Tools
- **2005 Where We Are**
  - Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)
- **2006 Where We Are Going**
  - Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)

**Clients**

- **2001 Where We Were**
  - 34,000 Cisco Adaptors
- **2005 Where We Are**
  - ~50,000 & ~3,000 PDAs
- **2006 Where We Are Going**
  - Heterogeneous CCX Environment; 60,000+ Clients

**Enhanced Services**

- **2001 Where We Were**
  - None
- **2005 Where We Are**
  - Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)
- **2006 Where We Are Going**
  - Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets

**SLA**

- **2001 Where We Were**
  - P4 (48 hr fix)
- **2005 Where We Are**
  - P4 (48 hr fix), Treated as P2
- **2006 Where We Are Going**
  - P2/P1 (Wireless as Primary Access Medium)

**Evolving Capabilities**

- **2001 Where We Were**
  - No management Tools
- **2005 Where We Are**
  - Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)
- **2006 Where We Are Going**
  - Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)

**Clients**

- **2001 Where We Were**
  - 34,000 Cisco Adaptors
- **2005 Where We Are**
  - ~50,000 & ~3,000 PDAs
- **2006 Where We Are Going**
  - Heterogeneous CCX Environment; 60,000+ Clients

**Enhanced Services**

- **2001 Where We Were**
  - None
- **2005 Where We Are**
  - Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)
- **2006 Where We Are Going**
  - Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets

**SLA**

- **2001 Where We Were**
  - P4 (48 hr fix)
- **2005 Where We Are**
  - P4 (48 hr fix), Treated as P2
- **2006 Where We Are Going**
  - P2/P1 (Wireless as Primary Access Medium)

**Evolving Capabilities**

- **2001 Where We Were**
  - No management Tools
- **2005 Where We Are**
  - Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)
- **2006 Where We Are Going**
  - Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)

**Clients**

- **2001 Where We Were**
  - 34,000 Cisco Adaptors
- **2005 Where We Are**
  - ~50,000 & ~3,000 PDAs
- **2006 Where We Are Going**
  - Heterogeneous CCX Environment; 60,000+ Clients

**Enhanced Services**

- **2001 Where We Were**
  - None
- **2005 Where We Are**
  - Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)
- **2006 Where We Are Going**
  - Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets

**SLA**

- **2001 Where We Were**
  - P4 (48 hr fix)
- **2005 Where We Are**
  - P4 (48 hr fix), Treated as P2
- **2006 Where We Are Going**
  - P2/P1 (Wireless as Primary Access Medium)

**Evolving Capabilities**

- **2001 Where We Were**
  - No management Tools
- **2005 Where We Are**
  - Extensive Web-services based Management Tools (EMAN); Wireless LAN Solutions Engine (WLSE)
- **2006 Where We Are Going**
  - Wireless Control System (WCS) and Wireless LAN Solutions Engine (WLSE)

**Clients**

- **2001 Where We Were**
  - 34,000 Cisco Adaptors
- **2005 Where We Are**
  - ~50,000 & ~3,000 PDAs
- **2006 Where We Are Going**
  - Heterogeneous CCX Environment; 60,000+ Clients

**Enhanced Services**

- **2001 Where We Were**
  - None
- **2005 Where We Are**
  - Guest WLAN Networking (Using BBSM); Wireless VoIP (7920)
- **2006 Where We Are Going**
  - Location Based Services (LBS); WLAN to Cellular Voice Roaming; Dual Mode Handsets

**SLA**

- **2001 Where We Were**
  - P4 (48 hr fix)
- **2005 Where We Are**
  - P4 (48 hr fix), Treated as P2
- **2006 Where We Are Going**
  - P2/P1 (Wireless as Primary Access Medium)
The Future—NexGen WLAN

- Cisco Unified Wireless Network
  Centralized WLAN solution (LWAPP* access points)
  Distributed WLAN solution (Cisco IOS® access points)
- Migration to dual-band 802.11a/g
- Enhanced services
  Enhanced Wireless LAN management
  Wireless intrusion detection and prevention systems
  Location-based services
  Outdoor coverage
- Improved WLAN voice support

* Lightweight Access Point Protocol
NexGen WLAN Methodology

• Categorize Cisco sites
  Six different sites based on network architecture and number of APs

• Apply NexGen WLAN architecture appropriate to size/type of site
  Double number of access points
  Deploy WLAN management tools appropriate to architecture
  Integrate with existing enterprise management tools
  Integrate with existing network security tools
Campus Sites

- Centralized WLAN solution
- Variable number of access points
  Usually 100+
- Several buildings arranged into clusters
- Each cluster served by two or more Cat6K WiSM’s (dual chassis)
- Multiple clusters per Mobility Group
- Management via WCS
Campus sites

- Centralized WLAN solution
- Variable number of access points
  Usually 100+
- Several buildings arranged into clusters
- Each cluster served by two or more Cat6K WiSM’s (dual chassis)
- Multiple clusters per Mobility Group
- Management via WCS
Medium to large Field Sales Offices

- Centralized WLAN Solution
- 5 to 98 access points
  - Four categories
- Dual WLAN controller appliance
- Management via WCS

![Diagram of LWAPP Tunnel to Primary and Secondary Controllers]

FSO Site Mobility Group

- LWAPP Tunnel to Primary Controller
- Path for LWAPP Tunnel to Secondary Controller
Small Field Sales Office

- Distributed WLAN Solution
- Two to four access points
- Cisco IOS access points
- No local WLAN controller
- Dedicated access point providing wireless domain services
- Management via WLSE
## Site Categories Summary

<table>
<thead>
<tr>
<th>Site Category</th>
<th>Description</th>
<th>APs Before Upgrade</th>
<th>APs after Upgrade</th>
<th>Architecture Type</th>
<th>Controller Assignment</th>
<th>Number of Bldg</th>
<th>Number of AP</th>
<th>Mgt Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Campus sites</td>
<td>Variable 50+</td>
<td>Variable 100+</td>
<td>Centralized</td>
<td>Multiple WiSM’s</td>
<td>79</td>
<td>3168</td>
<td>WCS EMAN</td>
</tr>
<tr>
<td>Type 2</td>
<td>FSO</td>
<td>27-49</td>
<td>51-98</td>
<td>Centralized</td>
<td>Dual 4404</td>
<td>12</td>
<td>800</td>
<td>WCS EMAN</td>
</tr>
<tr>
<td>Type 3</td>
<td>FSO</td>
<td>13 – 26</td>
<td>25 – 50</td>
<td>Centralized</td>
<td>Dual 4402-50 AP</td>
<td>24</td>
<td>670</td>
<td>WCS EMAN</td>
</tr>
<tr>
<td>Type 4</td>
<td>FSO</td>
<td>7 – 12</td>
<td>13 – 24</td>
<td>Centralized</td>
<td>Dual 4402-25 AP</td>
<td>28</td>
<td>464</td>
<td>WCS EMAN</td>
</tr>
<tr>
<td>Type 5</td>
<td>FSO</td>
<td>3-6</td>
<td>5 – 12</td>
<td>Centralized</td>
<td>Dual 4402-12 AO</td>
<td>76</td>
<td>640</td>
<td>WCS EMAN</td>
</tr>
<tr>
<td>Type 6</td>
<td>FSO</td>
<td>1 - 2</td>
<td>1 – 4</td>
<td>Distributed</td>
<td>None, IOS only, WDS</td>
<td>118</td>
<td>366</td>
<td>WLSE EMAN</td>
</tr>
</tbody>
</table>
NexGen WLAN Architecture

- Campus Buildings with High Density LWAPP APs.
- Dual Cat6K WLAN Controllers in Data Centres Serve Multiple Campus Buildings.
- WLSE Will Provide WLAN Management to Small FSO Sites that Retain IOS Access Points.
- Small Sites Retain IOS Autonomous AP Model.

- Outdoor Mesh WLAN at Campus Sites
- Wireless Control System Provides Enhanced WLAN Management, Security, Visualization Etc
- Location Servers in Data Centres Provide Location Based Services for Campus
- Remote Offices Have Two local WLAN Controllers

- Data Center/Site Backbone
- Cat 6K WLAN Controllers
- WCS
- Location Server
- WLSE

- Remote Sites
- Local WLAN Controllers

- FSO
WLAN Benefits
WLAN Benefits

• Extremely successful
  97%+ use wireless regularly
  27%+ use it as their only network access method

• Users appreciate being untethered from their desk

• Reduced risk of rogue deployments

• Increased productivity by providing on demand access to enterprise network
WLAN Productivity Benefits

• The major recurring question
  “How do I calculate the real benefits of this technology to my enterprise?”

• Differing opinions, differing approaches
  Undertake formal, independent studies
  Calculate savings on prudent estimates of user activity

• Let’s look at both in turn
NOP Study—
Wireless LANs Increase Productivity

Results of Survey of 300+ U.S. Organizations with More than 100 Employees:

- End users stayed connected to corporate network an average of 3 ½ hours more per day
- Average daily time savings: 90 minutes

‘NOP World’ Study (2003)

Highlights

• 3.5 hours additional time online, per day, due to wireless

• 1.5 hours of “time saved” (Productive time) due to wireless

• Based on average reported salary of US$80K, this equates to Productivity Benefit of US$14K, per employee per annum

• For enterprise the size of Cisco (50,000 wireless enabled employees), this would equate to US$700M

  Based on 100% adoption
Cisco IT Approach

- Derived Productivity Benefit of US$700M per annum (as per NOP Study) deemed “best case scenario”
- Cisco IT took more conservative approach in estimating Productivity Benefit for Cisco employees
- Methodology detailed in following slides
WLAN Benefits—Productivity
One Example of Calculating the VALUE of Deploying a WLAN

Primary Assumption:
• Users will save approximately 10 minutes productive time PER DAY

Secondary Assumptions:
• 230 work days per year
• 96,600 work minutes per year (7 hours per day)
• Average cost of $120,000 per employee per year (salary, WPR costs etc)
• Average cost per work minute: $1.24 / minute

Ten minutes saved * $1.24 * 230 work days
= $2,852 per employee

For Cisco, with 50,000 wireless users, maximum productivity improvement = US$142,500,000
Normalization

• Figure of **US$142,500,000** is based upon 100% of users gaining ten minutes per day

• Let’s be more conservative…

• Calculate savings if users gain only ten minutes of time PER WEEK.

• Productivity benefit is still considerable:

  Benefit of **US$28,520,000**

  Ten minutes saved * $1.24 * 46 weeks = $570.40 per employee

  50,000 x 570.40 = 18,538,000
Financial Prudence

- Cisco users gaining ten minutes productive time a week accrue Productivity Benefit of **US $28,520,000**
- For accuracy and prudence, do not assume 100% uptake
- If only **50%** of Cisco staff gain ten minutes productive time a week…
- Productive Benefit is still **US$14,260,000**

Cisco IT Believes the Real Figure Is Somewhere in Between
Or Use Your Own Formula

\[ C \times M \times Y = P \text{ (Productivity Benefit per Employee)} \]

\[ P \times \text{Total Employees} = \text{Benefit to Enterprise} \]

- **C** = Cost of Employee Minute
- **M** = Extra Minutes Productive time
- **Y** = Number of Minutes per year

Try It Yourself!
Ten minutes? What Ten Minutes?

• So where do these ten minutes actually come from?
  Meetings
  Cafeterias
  Mobile workers (support staff etc)
  Hot desking
  Quick setup when visiting offices—walk in and you’re online

• In reality, it’s very easy to gain ten minutes per week, if not per day
Additional Considerations—Soft Benefits

• In a recent survey in Cisco, 25% of respondents said they use WLANs as their primary method of connecting to the network

  Our target is 50%

  20 minutes saved x $1.24 x 230 work days = $5,704 per employee

  For Cisco, if 50% of 50,000 wireless users save 20 mins per day, productivity improvement = US$142,600,000

• Cisco’s WLAN is now being used for wireless VoIP (7920 handset)

• Cisco now provides visitors to our EBCs with “Guest WLAN networking”

• Workplace flexibility and design

  Increased user density per building
Additional Considerations—Costs

- There’s also a cost involved in deploying WLANs
- Cost of clients (wireless NICs or wireless ready laptops)
- Cost of managing the WLAN
- Cost of securing the WLAN
- Lesson is “Don’t take Productive Benefit in isolation—Offset it against the cost of deploying WLANs”
## Alternative Wireless LAN “Pay Back” Calculator

### WLAN Cost

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>$300 (year 1) + $150 (year 2 ...)</td>
</tr>
<tr>
<td>Infrastructure</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td></td>
</tr>
<tr>
<td>WLAN Client Adapter</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

≈ $300 (year 1) + $150 (year 2 ...)

≈ $.50-$1 Per Day Per User

### Employee Cost

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salary</td>
<td>$60K – $120K /year /employee</td>
</tr>
<tr>
<td>Benefits</td>
<td></td>
</tr>
<tr>
<td>Furniture, Equipment</td>
<td></td>
</tr>
<tr>
<td>Allocated Expenses</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
</tbody>
</table>

≈ $60K – $120K /year /employee

$.50-$1 Per Minute Per Employee

### Employee Productivity Savings

Payback = 1-2 Minutes per Day per Employee
Applying the Calculator to Cisco’s Internal Global Deployment

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost (000’s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation</td>
<td>1,100.00</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>1,408.00</td>
</tr>
<tr>
<td>Support</td>
<td>564.00</td>
</tr>
<tr>
<td>Client costs</td>
<td>1,200.00</td>
</tr>
<tr>
<td>Other (vendors)</td>
<td>1,340.00</td>
</tr>
<tr>
<td><strong>Total Year 1</strong></td>
<td><strong>5,613.00</strong></td>
</tr>
<tr>
<td><strong>Per Employee–34k Employees</strong></td>
<td><strong>0.165</strong></td>
</tr>
</tbody>
</table>

WLAN Cost

<table>
<thead>
<tr>
<th>Item</th>
<th>Cost (000’s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salary</td>
<td>—</td>
</tr>
<tr>
<td>Benefits</td>
<td>—</td>
</tr>
<tr>
<td>Assets</td>
<td>—</td>
</tr>
<tr>
<td>Allocated Exps</td>
<td>—</td>
</tr>
<tr>
<td>Other</td>
<td>—</td>
</tr>
<tr>
<td><strong>Annual Per Emp.</strong></td>
<td><strong>120</strong></td>
</tr>
<tr>
<td><strong>Total Cost–Cost 34k Employees</strong></td>
<td><strong>4,080</strong></td>
</tr>
</tbody>
</table>

Cost Per Day, Per User: $0.72

Cost Per Minute: $1.75

Payback Achieved with Less Than One Minute Productive Use Per Day
Wireless LAN Security
Different Security Models

• **WLAN is “trusted”**
  
  Treated as simply another transport medium
  
  Integrated into existing network
  
  Security provided by robust authentication and encryption systems

• **WLAN is “untrusted”**
  
  APs are on DMZ
  
  Access to network via VPN
  
  Security provided by VPN overlay
Trusted WLAN

• Advantages
  
  Ease of use
  
  Wide variety of EAP mechanisms for authentication
  
  Single sign-on
  
  Easy L2 and L3 roaming
  
  Wireless voice
  
  Other multi-cast traffic

• Disadvantages
  
  Successful attack on WLAN provides access to enterprise network
Untrusted WLAN

• Advantages
  Wireless network behind VPN concentrators
  Successful attack on WLAN provides no access to enterprise network
  Security is provided by robust 3DES and OTP

• Disadvantages
  Requires VPN infrastructure
  Requires VPN/SSL support on all client
  Scalability
  Less user friendly
  Reduces productivity value proposition
  Requires PKI
The Dual Aspects of WLAN Security

• WLAN security consists of two fundamental concepts; Authentication and Encryption
• Authentication
  Ensure users are identified and authorized to use the WLAN
• Encryption
  Ensure data integrity is maintained by encrypting it in a strong fashion
• Both are required
  Strong encryption is no good if someone can easily spoof their way onto the network
  Rock solid authentication is no good if someone can simply intercept and decrypt traffic without logging on
EAP Mechanisms (Authentication)

Ease of deployment vs. Security

- EAP-OPEN
- EAP-MD5
- LEAP
- EAP-TTLS
- EAP-TLS
- EAP-FAST
- PEAP
- EAP-OPEN

For Display Purposes Only
Cisco IT Recommends You Undertake Your Own Formal Security Requirements Analysis
EAP Mechanisms

- **EAP-TLS**
  Open standard PKI—tunneled authentication
- **EAP-FAST**
  Successor to LEAP—tunneled authentication
- **LEAP**
  Cisco standard—wide adoption, cross platform support
- **EAP-TTLS**
  Funk standard—variation of EAP-TLS; tunneled authentication
- **PEAP**
  IETF Draft—tunneled authentication; vulnerable to MITM attacks
- **EAP-MD5**
  Outdated and insecure
- **EAP-OPEN**
  Only used for public WLAN—no authentication
Choosing an EAP Mechanism

“The EAP Mechanism You Choose will Depend Upon Your Clients, Policy, and Existing Infrastructure”

• Is there a Certificate Authority (CA)
• What client platforms do you support
• What existing authentication systems exist
## EAP Protocols and Database Compatibility

<table>
<thead>
<tr>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>EAP-TTLS</th>
<th>LEAP</th>
<th>EAP-FAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login scripts (MS DB)</td>
<td>Yes(^1)</td>
<td>Yes(^1)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Password Expiration (MS DB)</td>
<td>N/A</td>
<td>Yes(^1)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Client and OS Availability</td>
<td>XP, 2000, CE and Others(^2)</td>
<td>XP, 2000, CE, CCXv2 clients(^3) and Others(^2)</td>
<td>Funk</td>
<td>Cisco/CCXv1 or Above Clients and Others(^2)</td>
</tr>
<tr>
<td>Allocated Exps</td>
<td>Yes(^1)</td>
<td>Yes(^1)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MS DB Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LDAP DB Support</td>
<td>Yes</td>
<td>Yes(^5)</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>OTP Support</td>
<td>No</td>
<td>Yes(^5)</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

1. Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)
2. Greater Operating System coverage is available from Meetinghouse and Funk supplicants
3. PEAP/GTC is supported on CCXv2 clients and above
4. Cisco 350/CB20A clients support EAP-FAST on MSFT XP, 2000, and CE operating systems. EAP-FAST supported on CB21AG/PI21AG clients with ADU v2.0 and CCXv3 clients
5. Supported by PEAP/GTC only, i.e., not PEAP-MSCHAPv2

---

\(^1\) Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)
\(^2\) Greater Operating System coverage is available from Meetinghouse and Funk supplicants
\(^3\) PEAP/GTC is supported on CCXv2 clients and above
\(^4\) Cisco 350/CB20A clients support EAP-FAST on MSFT XP, 2000, and CE operating systems. EAP-FAST supported on CB21AG/PI21AG clients with ADU v2.0 and CCXv3 clients
\(^5\) Supported by PEAP/GTC only, i.e., not PEAP-MSCHAPv2
# EAP Protocols: Feature Support

<table>
<thead>
<tr>
<th>Feature</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>EAP-TTLS</th>
<th>LEAP</th>
<th>EAP-FAST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off-Line Dictionary Attack Vulnerability</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Local Authentication (Cisco IOS)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Application Specific Device (ASD) Support (Cisco NIC)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Certificates?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Client Certificates</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Deployment Complexity</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>RADIUS Server Scalability Impact</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>Low/Medium</td>
</tr>
</tbody>
</table>
Wireless LAN Security: Recommended Best Practices

- Implement secure management policy for APs/bridges
  - Disable Telnet, disable http access, disable CDP, enable SSH, and enable TACACS for Admin authentication
- Management VLAN for APs and bridges
  - Restrict access to Management VLAN
- Layer-2 Mac address spoofing prevention
  - Lock-down critical MAC addresses: Default Gateway, BBSM, etc.
- PSPF—Enable PSPF on VLANs
- Virus scanning + firewall recommended on WLAN clients
- RF monitoring and rogue AP detection
  - Radio, client and network based scanning
  - Wireless IDS (WLSE and WCS)
- Select appropriate EAP mechanism
Wireless LAN Security: Recommended Best Practices (Cont.)

- Clearly defined and *communicated* wireless security policies
- Clearly defined security posture
  - EAP mechanism
  - Encryption method
  - Approved clients and standards
- Educate your user base
- Mobile devices
  - Adoption position and security policy essential for PDAs, “Smart-phones” etc
  - "Securing access is not sufficient. You must also secure INFORMATION"
  - Encryption and passwords on mobile devices
Q and A