

Cisco.com

WLAN Integration in Mobile Networks

Gaétan Feige
gfeige@cisco.com

© 2002, Cisco Systems, Inc. All rights reserved. 2

WLAN Integration in Mobile Networks

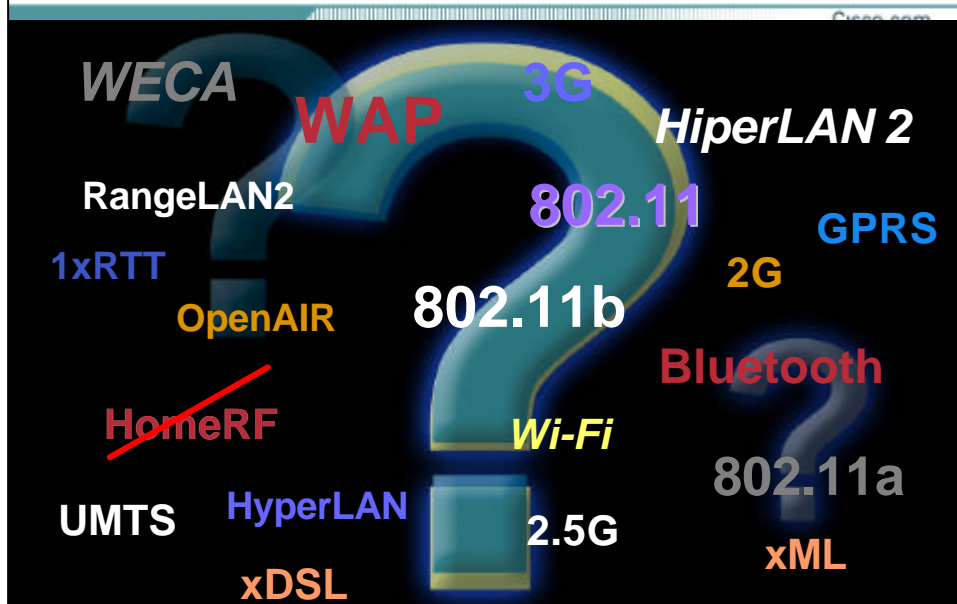
The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security
- Network Architecture
- Summary

© 2002, Cisco Systems, Inc. All rights reserved. 3

Confusion in the Market About Wireless



Wireless Technologies

Cisco.com

PAN "Personal Area Network"	LAN "Local Area Network"	MAN "Metropolitan Area Network"	WAN "Wide Area Network"
Bluetooth 802.15	802.11b 802.11g 802.11a HiperLAN2	802.11 MMDS LMDS	GSM GPRS CDMA 2.5-3 G
Low Data Rates	Higher Data Rates	Higher Data Rates	Lower Data Rates
Short Distances	Medium Distances	Med-longer Distances	Longer Distances
Notebook/PC to Devices/ Printer/Keyboard/Phone	Computer-Computer and to Internet	Fixed, last mile access	PDA Devices and Handhelds to Internet
< 1 Mbps	2 to 54+ Mbps	22+ Mbps	10 to 384 Kbps

© 2002, Cisco Systems, Inc. All rights reserved. 5

IEEE 802.11 Task Group Outline

Cisco.com

- **802.11a** — 5GHz (PHY for UNII), ratified in 1999
- **802.11b** — 11Mb 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 Datarate (>20 Mbps) 2.4 GHz
- **802.11h** — Dynamic Frequency Selection and Transmit Power Control mechanisms
- **802.11i** — Authentication and Security

http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

© 2002, Cisco Systems, Inc. All rights reserved. 6

Wireless LAN Technologies

Cisco.com

	802.11b	802.11g	802.11a	HiperLAN2
Freq. Band	2.4 GHz Public	2.4 GHz Public	5 GHz / Public / Private	5 GHz
Coverage	Worldwide	Worldwide	US/AP	Europe
Data Rate	1-11 Mbps	1-54 Mbps	20-54 Mbps (1-2 yrs) 100+ Mbps (future)	20-54 Mbps (1-2 yrs)
Cisco	Today RF + Features	Standard in final Could be quick	RF + Features	No Standard finalized Will never come to market

The Laws of Radio Dynamics:

Higher data rates = shorter transmission range
 Higher power output = increased range, but lower battery life
 Higher frequency radios = higher data rates, shorter ranges

© 2002, Cisco Systems, Inc. All rights reserved. 7

WLAN and GPRS/CDMA do not compete They Complete each other

Cisco.com

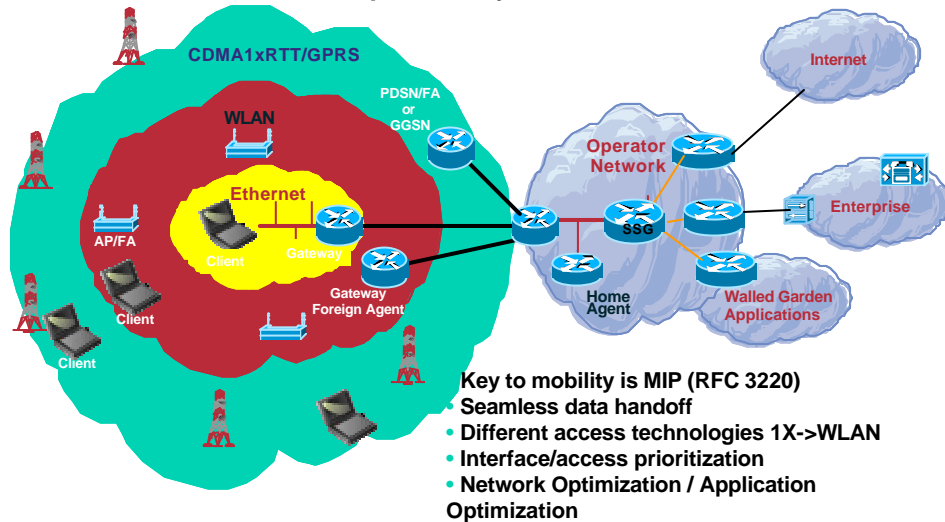
- GPRS/CDMA is sufficient for well thought applications, but requires optimisation and less scalability in throughput:
 - Push
 - Synchronization
 - Consumer Messaging Applications
 - Vertical Markets
- UMTS/CDMA2000 will increase user satisfaction. Applications must be developed today
- WLAN is limited to Hot Spots deployments, delivers high speed and can be deployed instantly
- WLAN does not replace 3G always on capability but enhances this mobile access to high speed in well chosen places.
- Handover between these technologies will become mature very soon, many initial deployments happening

© 2002, Cisco Systems, Inc. All rights reserved. 8

Mobile Architecture Seamless Mobility Solution

Cisco.com

WLAN Is Complementary To CDMA 1xRTT/GPRS



© 2002, Cisco Systems, Inc. All rights reserved. 9

WLAN Integration in Mobile Networks

The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security
- Network Architecture
- Summary

© 2002, Cisco Systems, Inc. All rights reserved. 10

WLAN Key Points

Cisco.com

- “.. public WLANs require **subscription control**, **roaming agreements**, and centralized network management. Roaming is crucial to maximizing coverage.”

Public Wireless LANs: Challenges, Opportunities and Strategies
Datacomm Research Company

- “... the most notable issue to be resolved is the ability of public WLAN operators to provide a wide coverage for potential users. These operators need to pursue **roaming agreements** with each other to minimize the cost of deploying access gateways in every possible hot-spot location.”

Analysis

© 2002, Cisco Systems, Inc. All rights reserved. 11

The Roaming and Authentication Concern

Cisco.com

Global
Equity
Research



April 25, 2002

Global Technology

Global

Tech Compass: Wireless Roaming



Summary

- The lack of roaming capabilities is one of the critical shortcomings of public Wireless LAN adoption to date. We address some of the issues and solutions in the market today with a look towards future needs. Hardware vendors should be watched in the short term, and software vendors should be watched in the long-term.

Action

- Look to the release of roaming software and the adoption and launch of WLAN services from mobile and fixed line operators to spur the continued growth of the WLAN market.
- When the roaming bottlenecks are resolved, hardware vendors of multi-modal access points and integrated multi-modal WLAN cards will be short-term winners.

© 2002, Cisco Systems, Inc. All rights reserved. 12

Levels of inter-working identified by 3GPP

Cisco.com

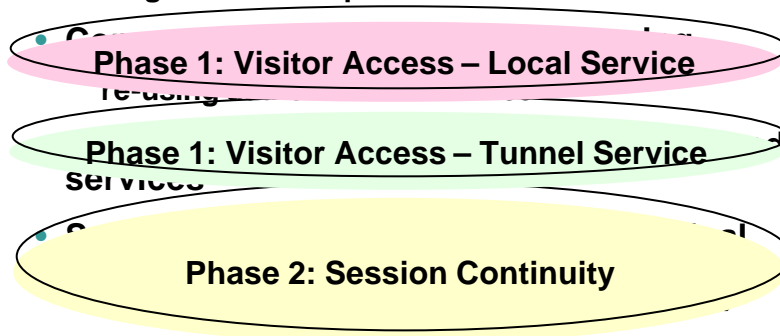
- **Common billing customer care**
single relationship with user
- **Common access control and charging**
re-using authentication service
- **Access to Home operator's UMTS PS based services**
- **Seamless L3 Mobility with single terminal**
- **Seamless L2 Mobility (e.g., integrated Iu)**

© 2002, Cisco Systems, Inc. All rights reserved. 13

Levels of interworking identified by **GSM Association**

Cisco.com

- **Common billing customer care**
single relationship with user



© 2002, Cisco Systems, Inc. All rights reserved. 14

Many competing solutions addressing the roaming requirement:

Cisco.com

Solution \ Impact on	Client	Roaming Network
Adjungo Prop tunnel to HPLMN	Proprietary	No impact
Cisco EAP-SIM/802.1x	Standards based 802.1x	Standards based AP supporting 802.1x
Mobility Networks EAP-SIM/PPPoE	Standards based PPPoE	Proprietary
Nokia EAP-SIM/PPPoE	Proprietary	Proprietary
Transasys GSM MM/IP	Proprietary	Proprietary

Minimum impact on clients

Minimum impact on Roaming partners

© 2002, Cisco Systems, Inc. All rights reserved. 15

Roaming Models: What is the requirement placed on the visited network?

Cisco.com

- **Minimum set includes**
 - 802.1x on AP for EAP support**
 - Allows a users supplicant to be authenticated against a home AAA EAP method
 - RFC 2548 VSA for Key exchange (or similar)**
 - Allows session keys to be exchanged between the Home operator and the Access operator
- **Value added set includes**
 - L2TP tunnelling between Access Network into Home Operator**
 - Allows home operator to offer seamless service to users when roaming on WLAN (NOT vanilla Public Internet access)

© 2002, Cisco Systems, Inc. All rights reserved. 16

WLAN Integration in Mobile Networks

The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security
- Network Architecture
- Summary

© 2002, Cisco Systems, Inc. All rights reserved. 17

Authentication

Cisco.com

Different approaches for client to network

Clientless, no software required by user

- Easy call center support, no partner required
- WEB based authentication with automatic user redirection

Client / Server

Requires installation of user software and support must be minimised

Methods :

- PPPoE client (standard) (Mobility Networks)
- GPRS GMM (standard but proprietary clients) (Transat / Comfone)
- EAP-SIM client (Cisco – Nokia):
 - » 802.1x (Cisco with Microsoft support)
<http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/secwireless.asp>
 - » Proprietary (Nokia NAAP client)
- EAP-TLS
- PEAP

© 2002, Cisco Systems, Inc. All rights reserved. 18

Authentication

Cisco.com

Different approaches for IP traffic in core network

Native IP traffic : **Local/Visited Services**

– Everybody

Tunneled traffic : **Home Services**

Methods :

PPP client (standard)

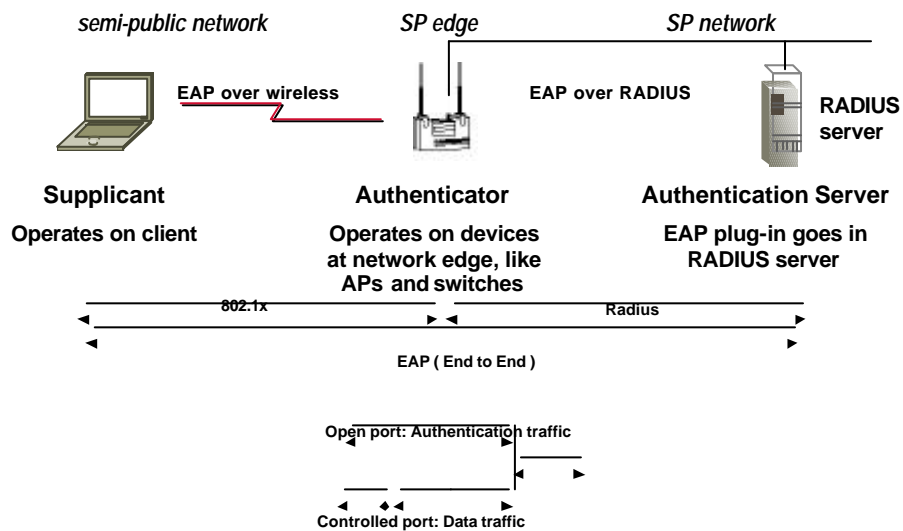
L2TP/PPP (standard)

GTP (standard but only one vendor : Mobility Networks). Also GTP is not suited for high capacity traffic flows

© 2002, Cisco Systems, Inc. All rights reserved. 19

General Description of IEEE 802.1x Terminology

Cisco.com



© 2002, Cisco Systems, Inc. All rights reserved. 20

Client Implementation for GSM SIM Why not later for CDMA RUIM

Cisco.com

Login Credentials and algorithms

- A smart card is required to store the GSM identity and key Ki
- Smart card reader required :
 - » Built in smart card reader built in WLAN device
 - » External smart card reader (USB Dungle, PCMCIA, ...)
 - » Any PC/SC reader compliant



A single WLAN / GPRS PCMCIA card with built in SIM reader

- Most laptops now have built in WLAN !
- A PCMCIA format not convenient for PDA! Also true for Cisco (investigation of Pocket PC format !)
- Symbol Pocket PC much better suited than Cisco card on HP Jornada, same for IPAQ.
- GPRS connectivity can be coupled with Bluetooth to a phone, drawback is no simultaneous voice + data

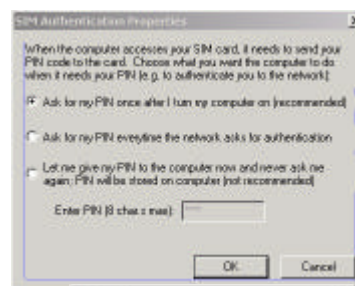
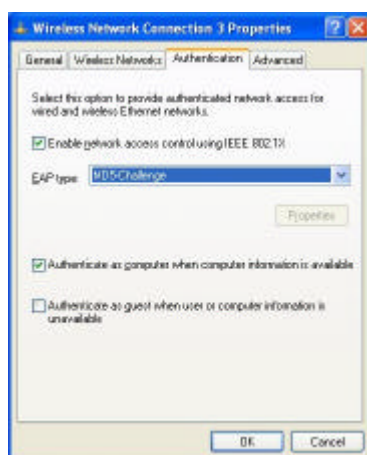
Most easy client support follows standardisation :

- IEEE 802.1x, allows for other authentication options : EAP-TLS / PEAP / EAP-MD5
- IETF EAP
- Microsoft support <http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/secwireless.asp>
- Gemplus SIM card support for security or standard SIM depending on A3/A8

© 2002, Cisco Systems, Inc. All rights reserved. 21

Windows XP Authentication screen shot

Cisco.com



© 2002, Cisco Systems, Inc. All rights reserved. 22

WLAN Integration in Mobile Networks

The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security / Encryption
- Network Architecture
- Summary

© 2002, Cisco Systems, Inc. All rights reserved. 23

The #1 Concern for Enterprise about Wireless: Security

Cisco.com

THE WALL STREET JOURNAL.
© 2001 Dow Jones & Company, Inc. All Rights Reserved.
WEDNESDAY, FEBRUARY 14, 2001
WALL STREET JOURNAL
HOSPITALITY
WIRELESS

Hackers Can Penetrate Wireless Network

By James H. ...
... of the ...
... of ...

The weakness is another reminder of the difficulty in implementing effective network security.

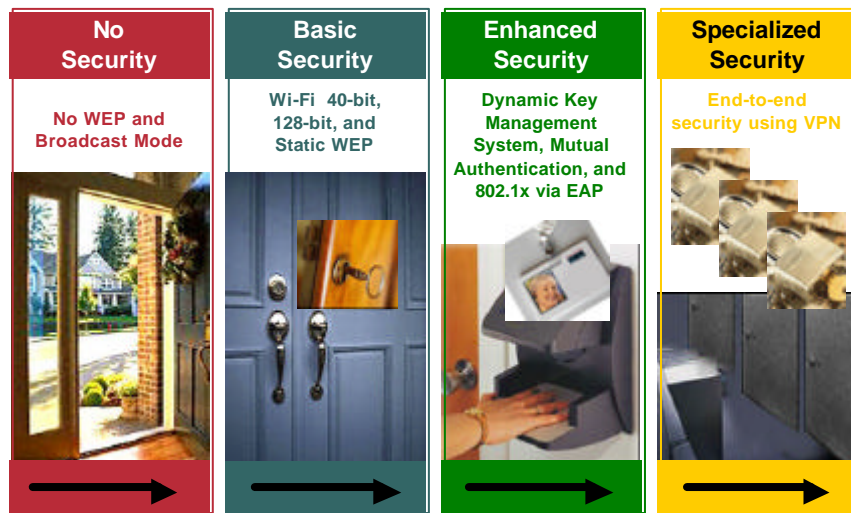
... of ...
... of ...
... of ...

Source: WSJ, 2/5/01

© 2002, Cisco Systems, Inc. All rights reserved. 24

Wireless Security

Cisco.com



© 2002, Cisco Systems, Inc. All rights reserved. 25

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.
- ICV : CRC-32 linear → bad choice again ! No Keyed MIC

© 2002, Cisco Systems, Inc. All rights reserved. 26

Cisco Solutions against WEP weaknesses

Cisco.com

- Per user session key derived from authentication, key generation based on one way function, key distribution method built in 802.1x
- Renewal of the session key
- Compliance to the successor of WEP (WEP2 / TKIP(Temporal Key Integrity)) in order to have a stronger encryption algorithm
 - Broadcast key rotation
 - Key hashing : against Airsnort
 - WEP frame integrity : MIC : to enhance CRC32 weakness
- Following standard and availability of AES (Future)
- End to end encryption using IPSEC

Solution: IEEE standard-in-progress for port-based network access control
802.1x Leverages existing standards: EAP (Extensible Authentication Protocol), RADIUS

© 2002, Cisco Systems, Inc. All rights reserved. 27

Sniffing Hackers' sites...

Cisco.com

"Has anyone had any luck with snorting against a Cisco 340 Access Point with 11.07? I have been running against one all day and according to Capture I have 60 billion encrypted packets but 0 interesting packets."

Toby Bearden, hacker, in posting to "AirSnort Forum"

"Thus the Cisco products cannot be attacked with AirSnort. Cisco is a little more secure than the rest of the world."

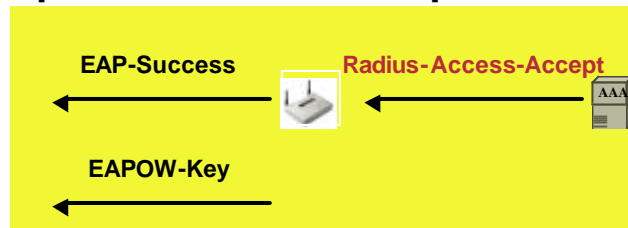
Jerry Bruestel, inventor of "AirSnort"

© 2002, Cisco Systems, Inc. All rights reserved. 28

Per user per session key exchange

Cisco.com

- Requires agreement between Home operator and visited operator



- Contains MS-MPPE-Send-Key attribute per RFC2548.
- This WEP session key has already been delivered/derived by the supplicant in the authentication phase. It is delivered here to the AP.

© 2002, Cisco Systems, Inc. All rights reserved. 29

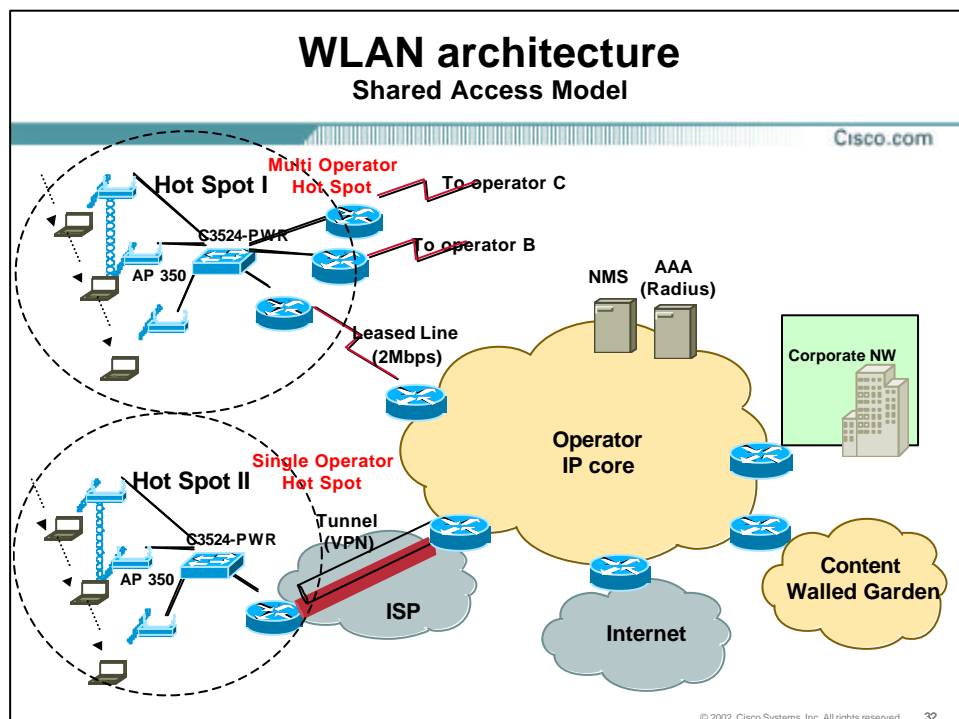
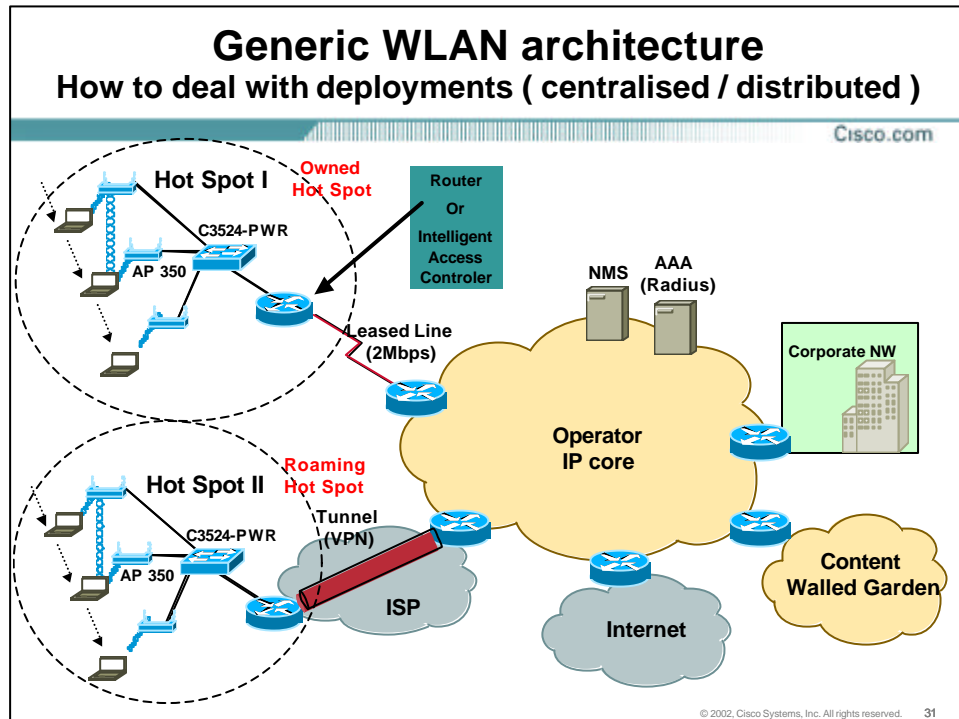
WLAN Integration in Mobile Networks

The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security / Encryption
- Network Architecture
- Summary

© 2002, Cisco Systems, Inc. All rights reserved. 30



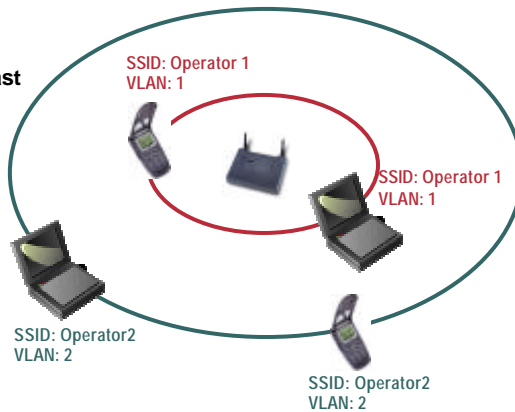
Shared Access Model

VLAN support on Access Point
Summer 2002

Cisco.com

VLAN support : Cisco Proprietary

- WLAN user groups with broadcast containment
- Support for 802.1p/q VLANs for end-to-end integration
- Support for 25 SSIDs with mapping to VLANs
- Private VLANs to prevent inter-client communication

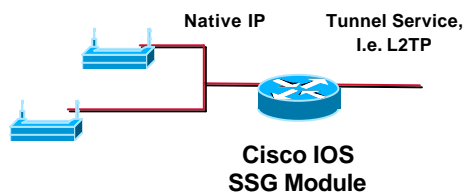


© 2002, Cisco Systems, Inc. All rights reserved. 33

Converged Service Control with CMX: For the WLAN Access Provider

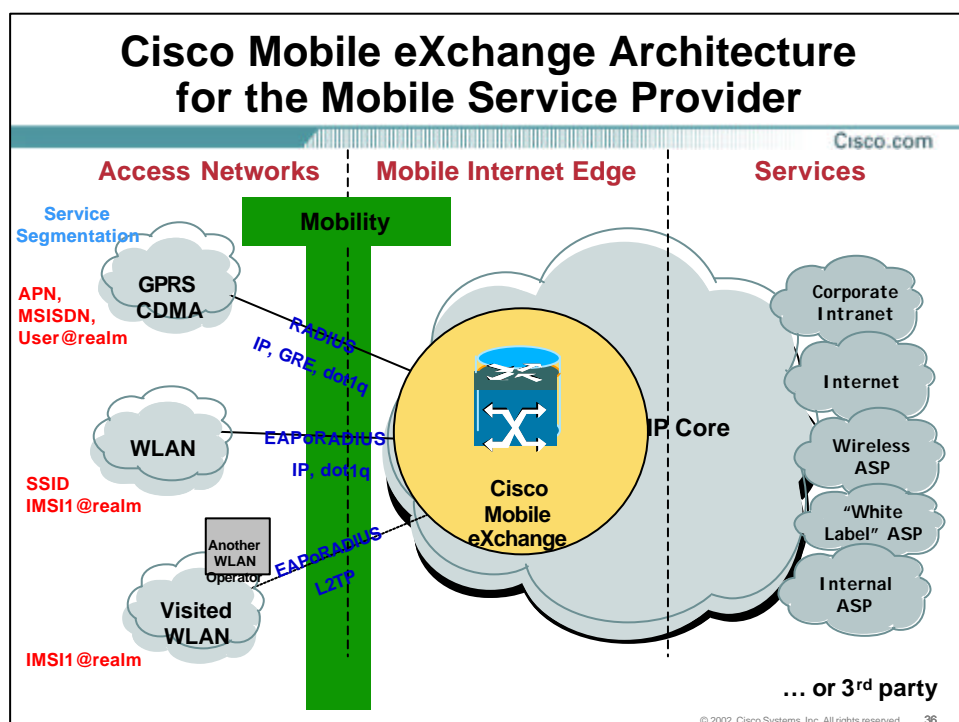
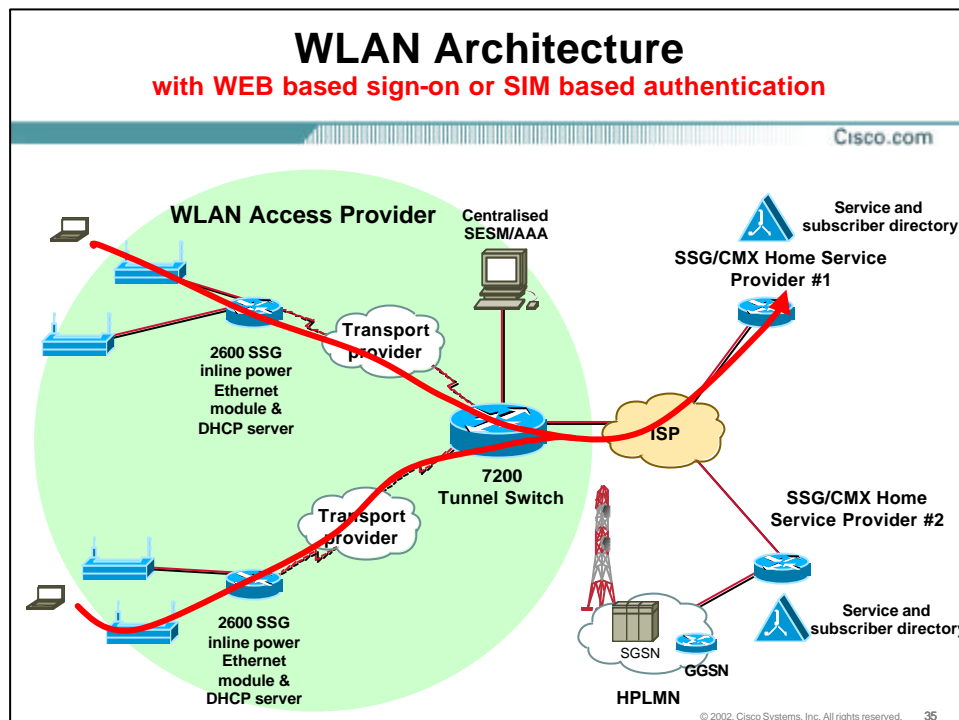
Cisco.com

- Cisco Mobile eXchange performs per subscriber control within the NETWORK layer



Tunnel service object can be triggered after web based log in or automatically via RADIUS exchange

© 2002, Cisco Systems, Inc. All rights reserved. 34



WLAN Integration in Mobile Networks

The IP Mobility Challenge

Cisco.com

- The Wireless Technologies & WLAN
- The WLAN Mobile Operator Concerns
 - Roaming
 - Authentication
 - Security / Encryption
- Network Architecture
- **Summary**

© 2002, Cisco Systems, Inc. All rights reserved. 37

Cisco: Accelerating the WLAN roaming market with open, standards based WLAN

Cisco.com

Solution \ Impact on	Client	Roaming Network
Adjungo Prop tunnel to HPLMN	Proprietary	No impact
Cisco EAP-SIM/802.1x	Standards based 802.1x	Standards based AP supporting 802.1x
Mobility Networks EAP-SIM/PPP/E	Standards based PPPoE	Proprietary
Nokia EAP-TLS	Proprietary	Proprietary
TI G	Proprietary	Proprietary

Minimum impact on clients

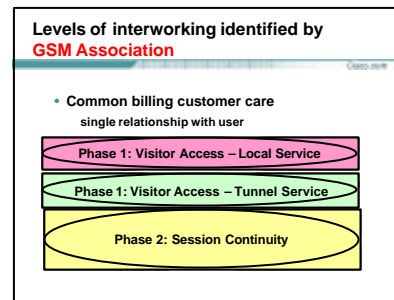
Minimum impact on Roaming partners

© 2002, Cisco Systems, Inc. All rights reserved. 38

Hierarchy or roaming types to meet different interworking requirements

Cisco.com

- **EAP-SIM/TLS/PEAP Authentication**
Simple 802.1X support in roaming network
- **Kc/ESN based encryption**
RADIUS RFC 2548 based per user per session key exchange
- **L2TP based subscriber control**
Value-added service provided by WLAN Access Provider allowing Orange to offer same look and feel when roaming over WLAN and GPRS
- **Web Based Authentication**



© 2002, Cisco Systems, Inc. All rights reserved. 39

CMX Based Service Control Cost Versus subscriber Control

Cisco.com

- CMX framework provides a truly access agnostic solution for per user service control
- CMX framework provides a common look at feel for WLAN and GPRS users
- Policy can be set as either being independent or dependent on the access technology
- Rating can be set as either being independent or dependent on the access technology
- Two options for a WLAN Hot Spot :
 - Low grade Access Points : reduced cost but no global roaming nor subscriber control, service is a bit pipe
 - Value Add Access Point : slightly higher cost but ...

© 2002, Cisco Systems, Inc. All rights reserved. 40

