Secure Mobile Architecture 10/16/02

POTS, ISDN, ADMSL
GSM, CDMA, PCS
GPRS, VSAT, ...

Over Any Network

Web Content
Communications Data
Enterprise Data
Personal Data
Directory Data

Any Data
(to which the user is entitled)

To Any Device
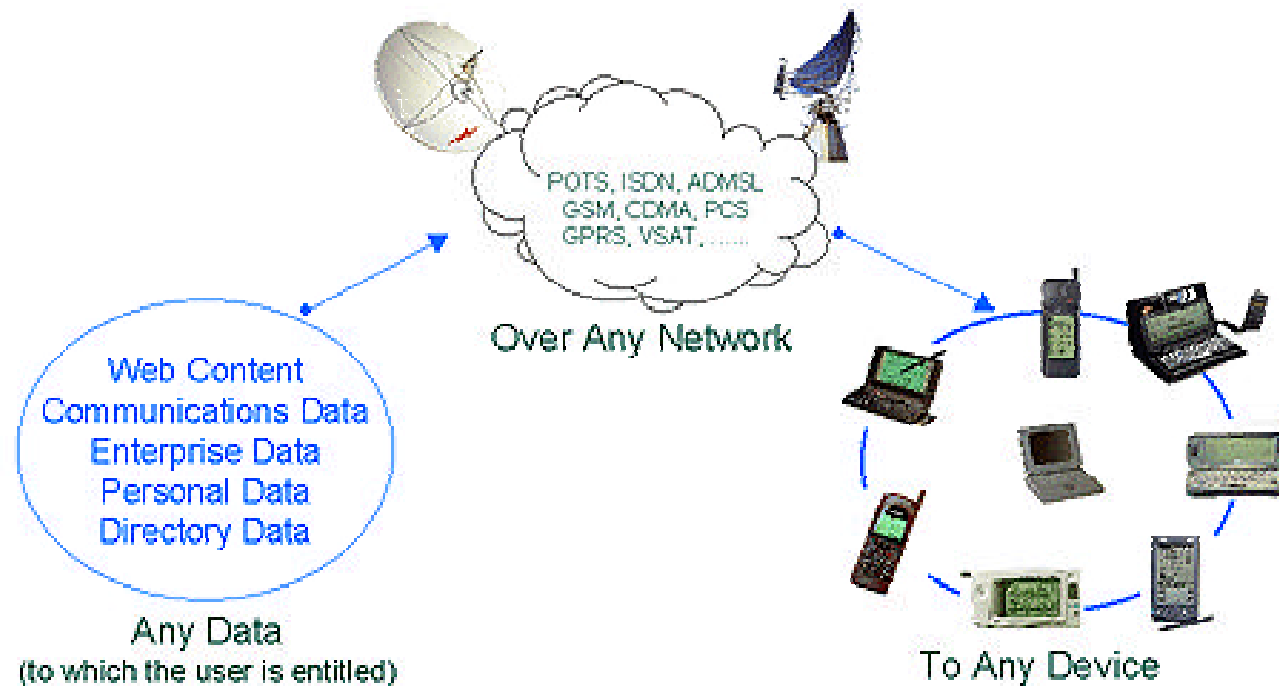
Richard H. Paine
Richard.h.paine@boeing.com
425.865.4921
Pager 206.797.4580
Cell 206.854.8199

www.mmforum .org

Agenda

- **Setting the Stage for a Secure Mobile Architecture**

  History of 2G, 3G, and 4G

  History of WLANs

  Convergence of Cellular and WLANs

- **Requirements for a converged Secure Mobile Architecture**

- **Principles of a Secure Mobile Architecture**

2000/2001 Deployment Scenarios

Secure Mobile Architecture Working Group
Mobile Management Forum

- **Evolution of 3G -- 3.5G and 4G programs**
  - Licensed spectrum
  - Wide area
  - High Mobility support -- vehicular speed mobility (and higher)
  - 20 - 200 Mbits/sec per sectored cell per channel

- **Hybrid: Digital Broadcast (DVB-T, DAB) outbound, cellular inbound**
  - European discussions as a near term Telematics application

- **W-LAN as Lower Mobility fill-in**
  - Inside - out deployment scenarios
  - EU program: 4G = 3G + HIPERLAN2   →   3G + IEEE 802.11
  - "Seamless mobility" between access networks
  - Seamoby
  - Use of unlicensed spectrum
  - Less geographic coverage per base site

Broadband Wireless Roadmap
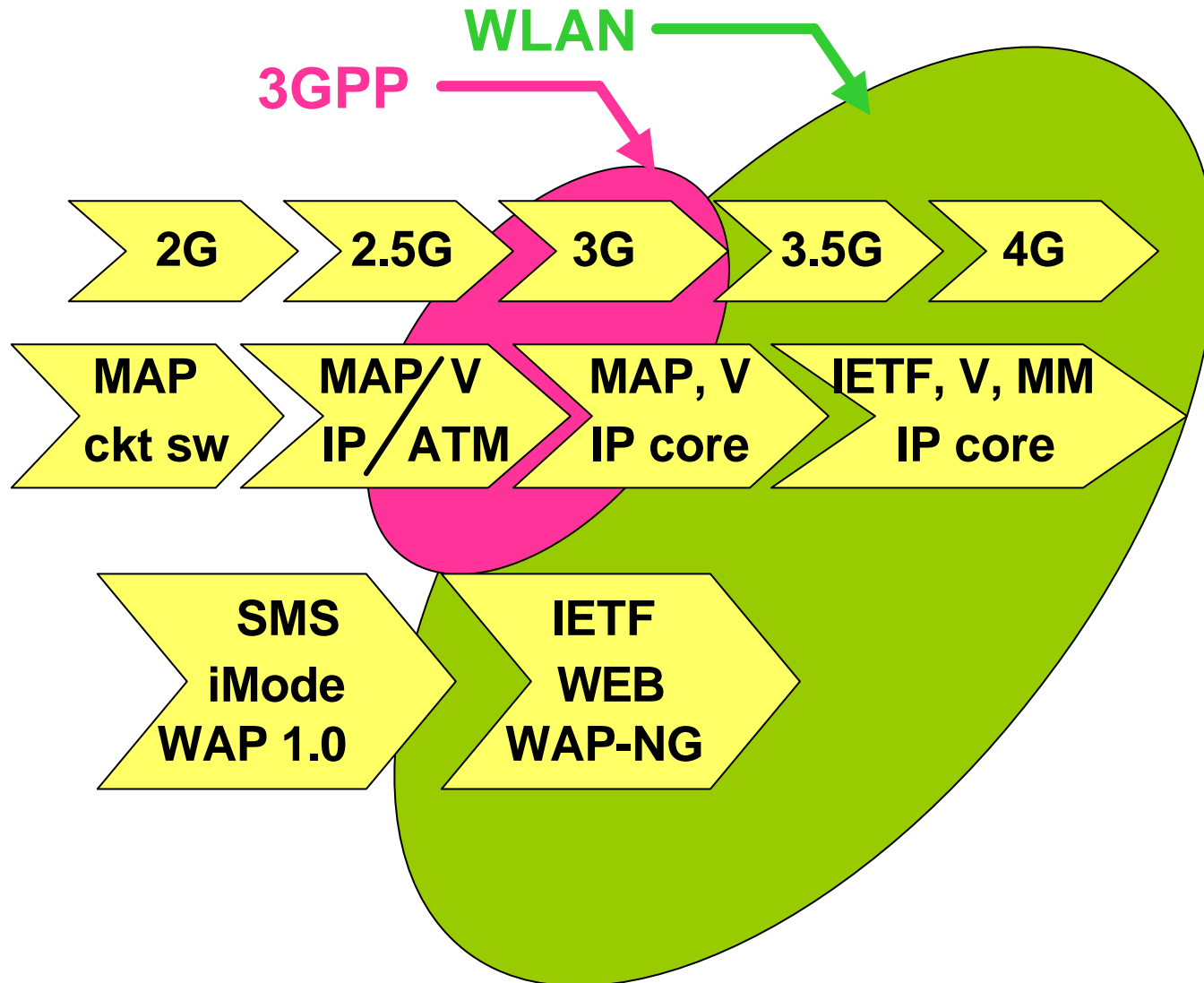
THE *Open* GROUP
... enabling enterprise integration

Secure Mobile Architecture Working Group
Mobile Management Forum

WLAN

3GPP

| 2G | 2.5G | 3G | 3.5G | 4G |

| MAP
ckt sw | MAP, V
IP/ATM | MAP, V
IP core | IETF, V, MM
IP core |

| SMS
iMode
WAP 1.0 | IETF
WEB
WAP-NG |

www.mmforum.org

Cellular Devices

THE *Open* GROUP
... enabling enterprise integration

Kyocera

Model 6035

Palm OS

CDMA

Kyocera's Smartphone

Neopoint

2000

CDMA

Handspring

Visor

Palm OS

IEEE 802.11b, Bluetooth, CDMA, GSM

VisorPhone
Learn more
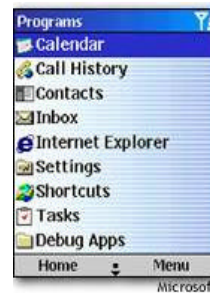
Microsoft "Stinger" Phone

WinCE

CDMA

PC-EPhone

Convergent
PC-EPhone
WinCE
CDMA

www.mmforum.org

What Is New With 3G/WLAN Devices

THE *Open* GROUP
... enabling enterprise integration

Devices
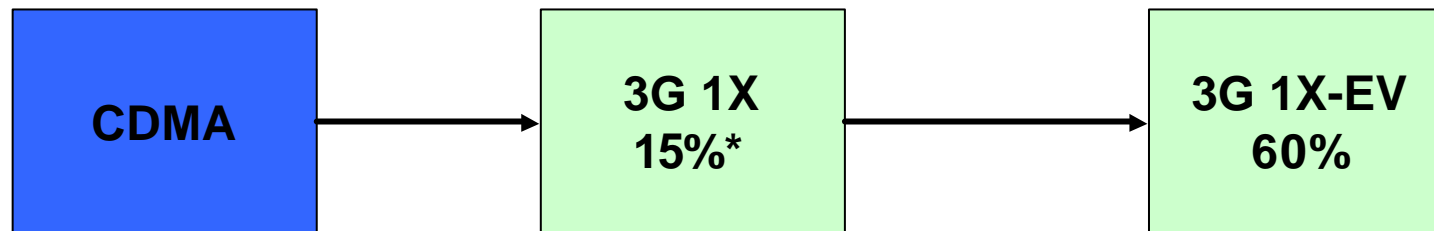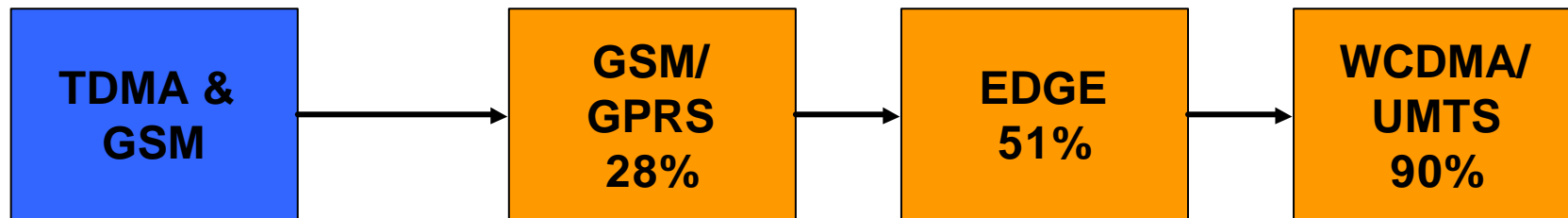
Screen size, storage capability improved

Multi-media

Video (stills and clips)

Music (download, store and play)

Increased speed

Faster File download / WEB browsing

Better Graphics

Improved mobile internet experience

www.mmforum.org

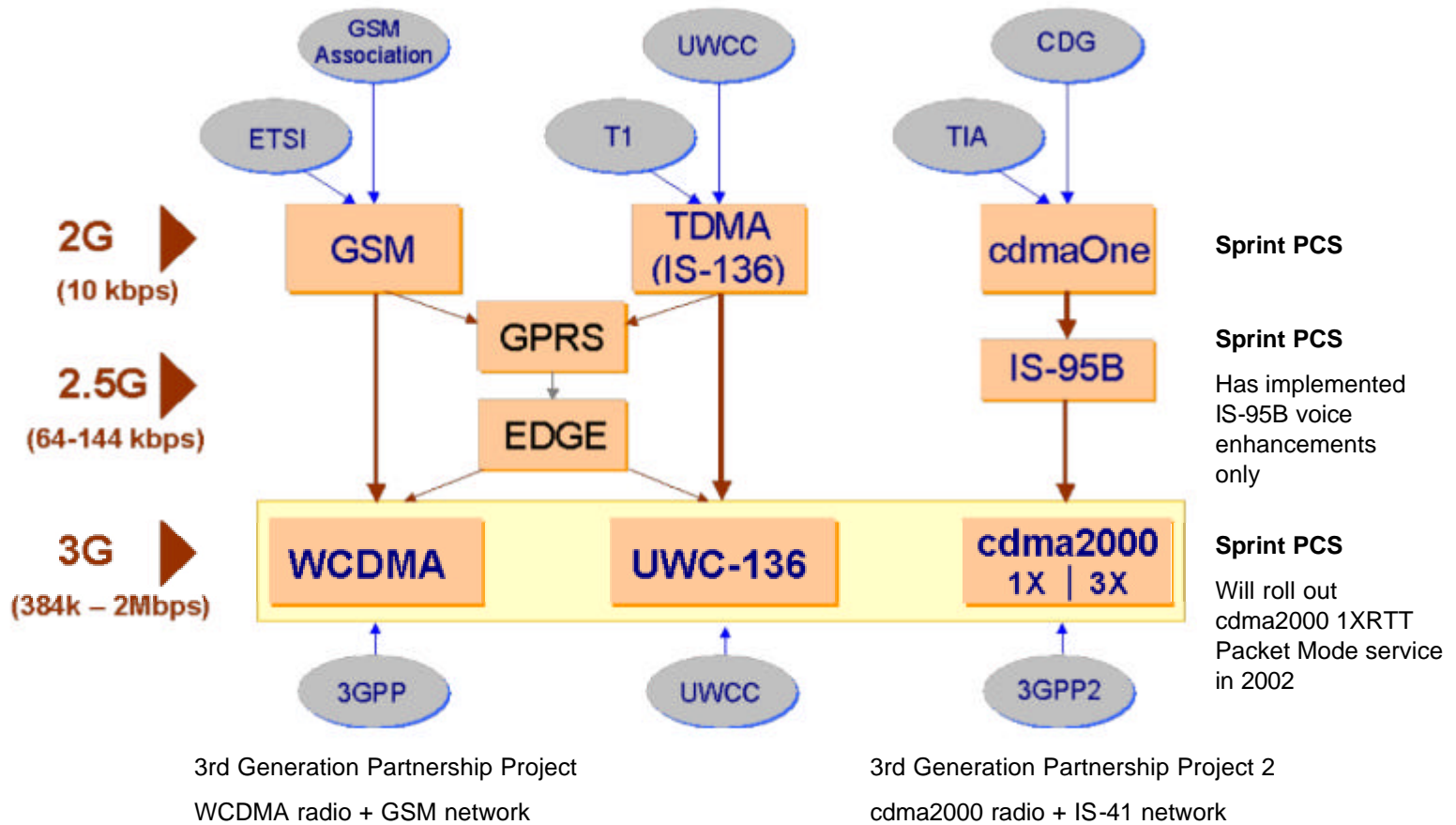# *3G Capital Costs*

Upgrade costs as a percent of 2G network cost.

Source: *Yankee Group*

The Road to IMT-2000

Secure Mobile Architecture Working Group
Mobile Management Forum

http://www.itu.int/imt/what_is/roadto/index.html

GSM Association		UWCC		CDG
ETSI		T1		TIA

2G
(10 kbps)

GSM | TDMA (IS-136) | cdmaOne — Sprint PCS

GPRS

2.5G
(64-144 kbps)

IS-95B — Sprint PCS

EDGE

Has implemented IS-95B voice enhancements only

3G
(384k – 2Mbps)

WCDMA | UWC-136 | cdma2000 1X | 3X — Sprint PCS

3GPP | UWCC | 3GPP2

Will roll out cdma2000 1XRTT Packet Mode service in 2002

3rd Generation Partnership Project

WCDMA radio + GSM network

3rd Generation Partnership Project 2

cdma2000 radio + IS-41 network

www.mmforum.org

WLAN Devices

WLAN History

- 1997 Standard 802.11 1 and 2Mbps

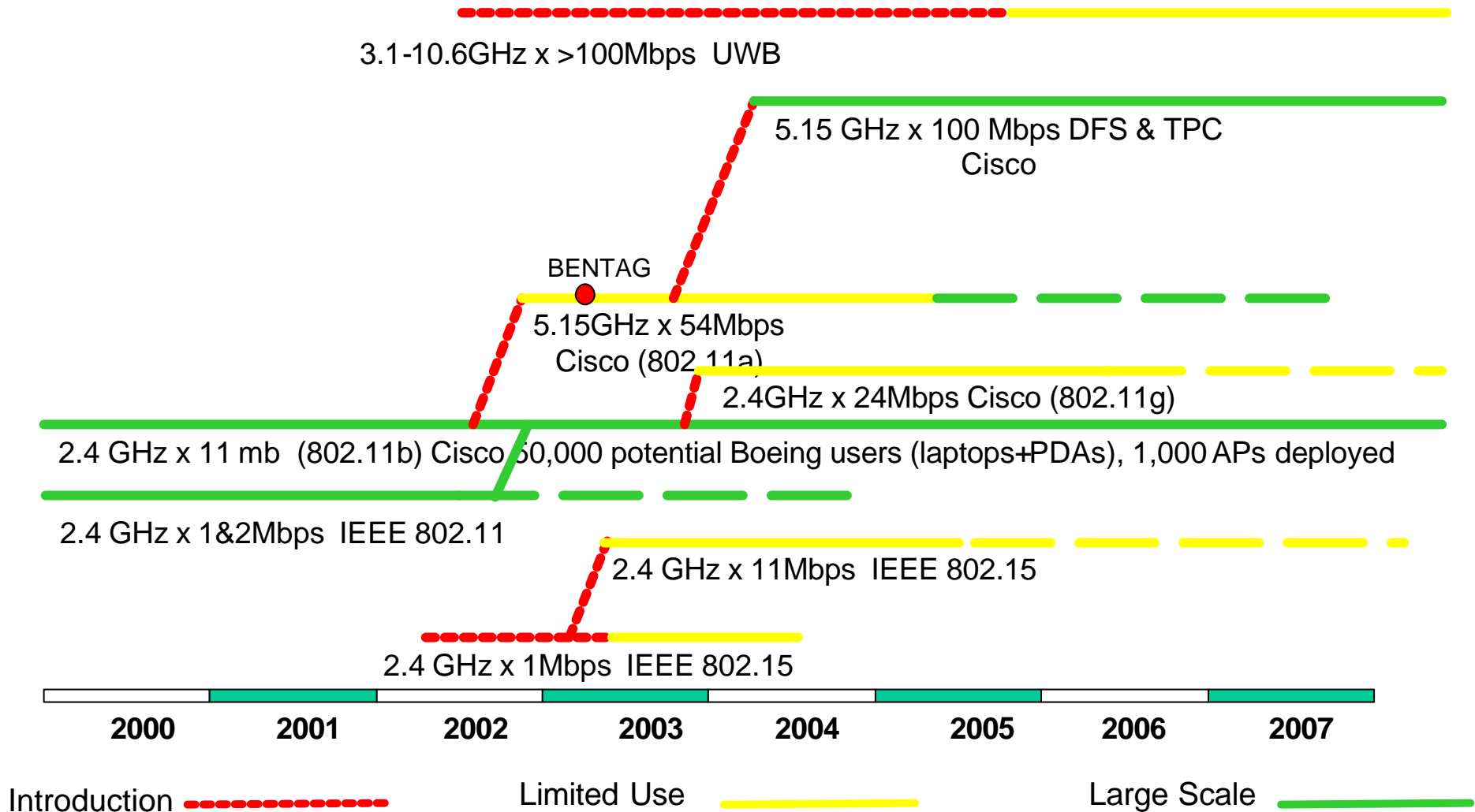- 1999 Standards 802.11a (54Mbps) and 802.11b (11Mbps)

- 802.11b Growth is astronomical (on the order of the Web growth)

- Microsoft Campuses (3700 APs and 37,000 PCMCIA cards)

- Boeing has approximately 1000 APs

- Security and QoS is being worked (802.11i and 802.11e)

- Radio Resource Measurement and High Throughput 802.11a in study groups

Boeing Wireless Railroad Chart

THE *Open* GROUP
... enabling enterprise integration

3.1-10.6GHz x >100Mbps UWB

5.15 GHz x 100 Mbps DFS & TPC
Cisco

BENTAG

5.15GHz x 54Mbps
Cisco (802.11a)

2.4GHz x 24Mbps Cisco (802.11g)

2.4 GHz x 11 mb (802.11b) Cisco 50,000 potential Boeing users (laptops+PDAs), 1,000 APs deployed

2.4 GHz x 1&2Mbps IEEE 802.11

2.4 GHz x 11Mbps IEEE 802.15

2.4 GHz x 1Mbps IEEE 802.15

| 2000 | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 |

Introduction   Limited Use   Large Scale

Mobile Collocation Comm Technologies

THE *Open* GROUP
... enabling enterprise integration

	1999	2000	2001	2002	2003

Wireless

WAN Satellite	DBS
MANs/CANs	analog(AMPS)
	Ricochet
	PCS
	SMR
LAN	IEEE 802.11 1 and 2Mbps
	IEEE 802.11b 10-25Mbps
	IEEE 802.11a 54Mbps
	IEEE 802.11a 100Mbps
Personal Area Networks	700Kbps
	2Mbps
	400Mbps
Pulse	

Wired

Home & Traveling	
	Dialed
	Cable (10M)
	Copper (6M)

Introduction ●●●●●●●●● Limited Use ▬▬▬▬ Large Scale ▬▬▬▬

Mobile Collocation Comm Technologies

THE *Open* GROUP
... enabling enterprise integration

	2002	2003	2004	2005	2006

Wireless

WAN Satellite   DBS
MANs/CANs   analog(AMPS)

         PCS
         SMR

LAN   IEEE 802.11 1 and 2Mbps
   IEEE 802.11b&g 10-25Mbps
      IEEE 802.11a 54Mbps
    IEEE 802.11l 100Mbps

Personal Area Networks
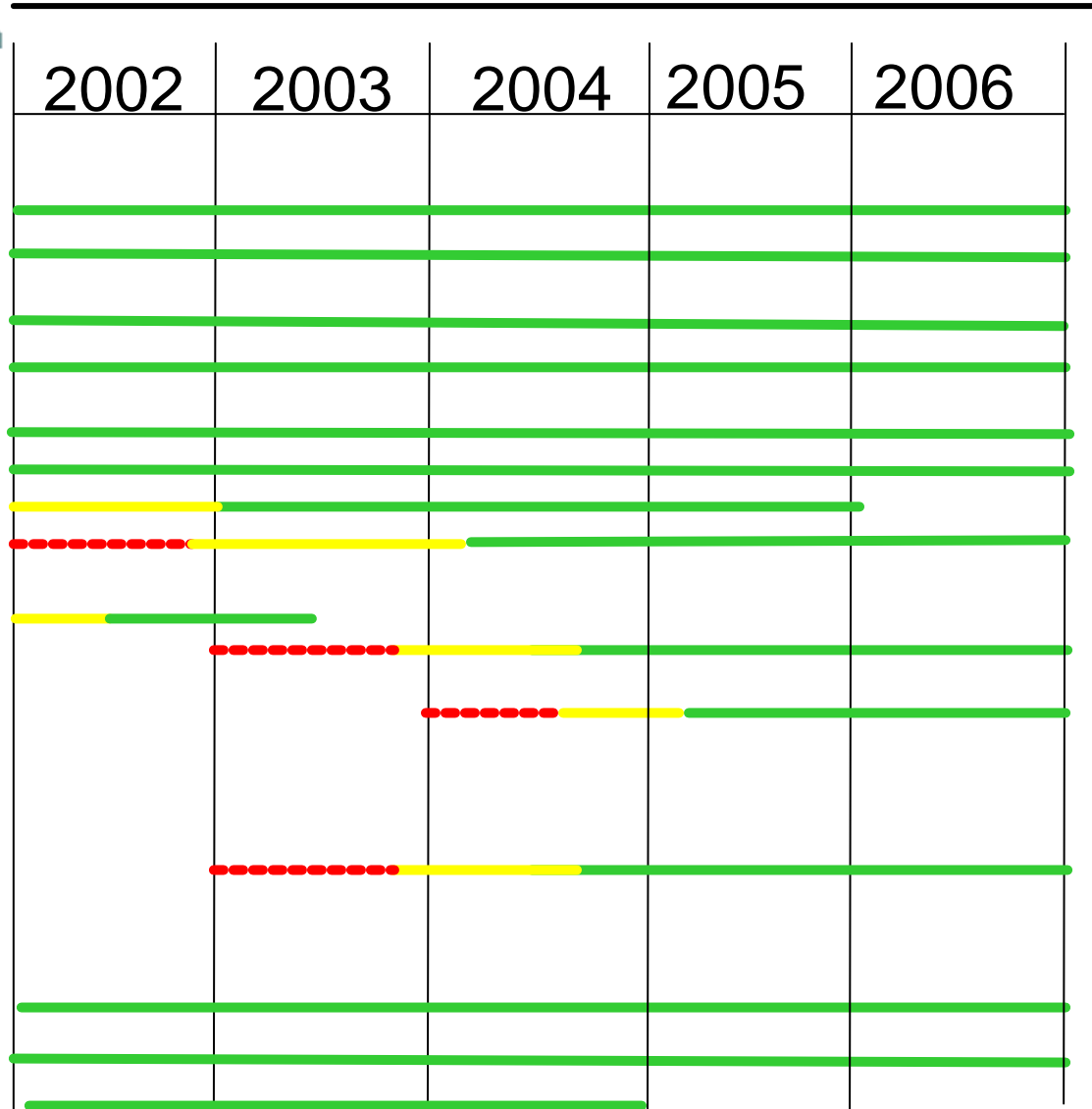   700Kbps
       2Mbps

       400Mbps
Pulse

Fixed WLAN to Homes
    IEEE 802.11b&g 10-25Mbps
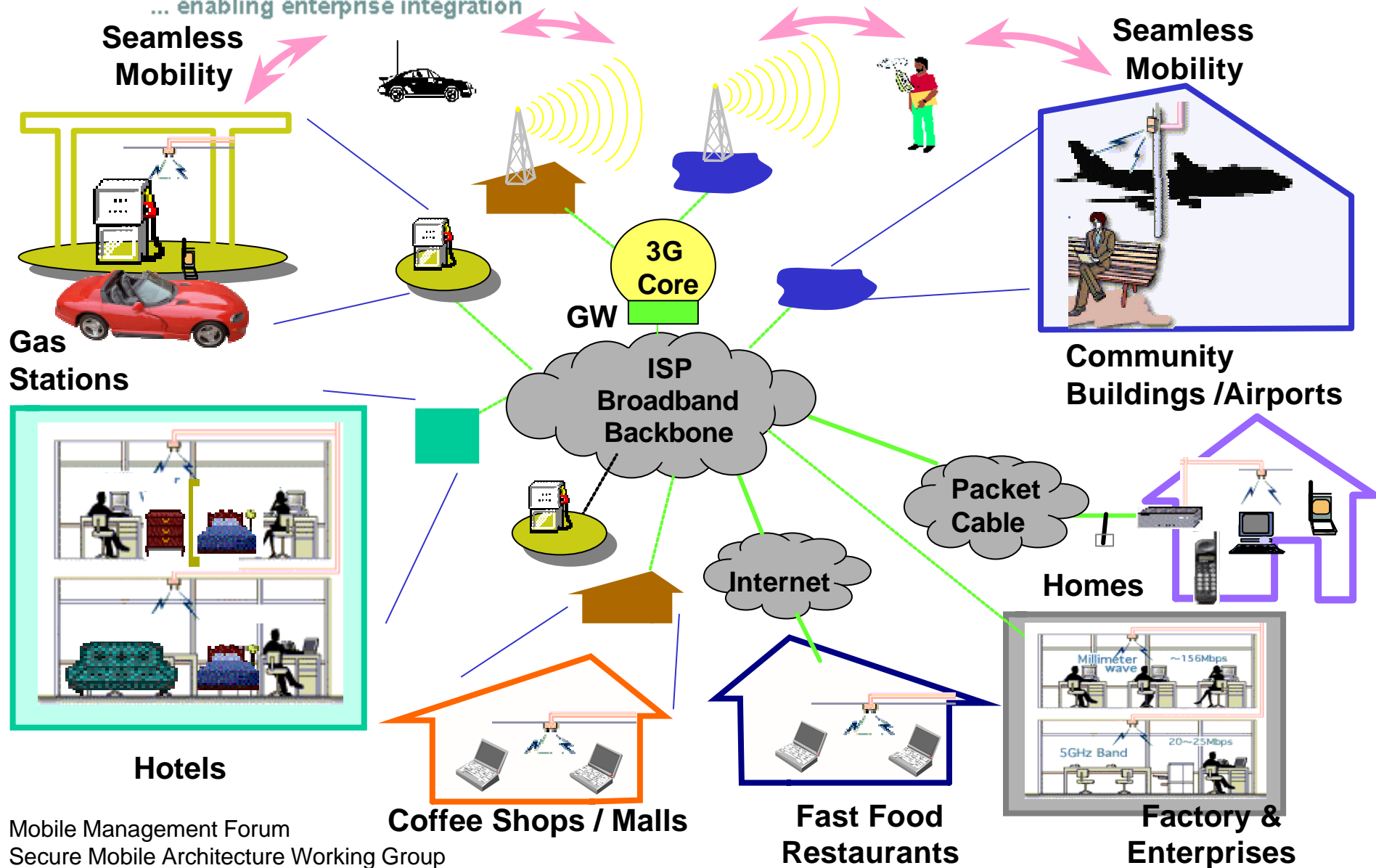
Wired

Home & Traveling
      Dialed

Cable (10M)

Copper (6M)

Introduction ▪▪▪▪▪▪▪▪▪▪▪ Limited Use ——————— Large Scale ———————

Convergence of Cellular and WLAN

THE Open GROUP
... enabling enterprise integration

Seamless Mobility

Seamless Mobility

3G Core

GW

ISP Broadband Backbone

Gas Stations

Community Buildings /Airports

Packet Cable

Homes

Internet

Hotels

Coffee Shops / Malls

Fast Food Restaurants

Factory & Enterprises

Millimeter wave ~156Mbps
5GHz Band 20~25Mbps

Convergence of Cellular and WLAN - Projects

- Project Rainbow – AT&T Wireless, Verizon, Intel, IBM, Cingular

- Voicestream – TMobile WLANs

- Sprint?

- Boingo – from wireless LAN to VOIP Service Provider
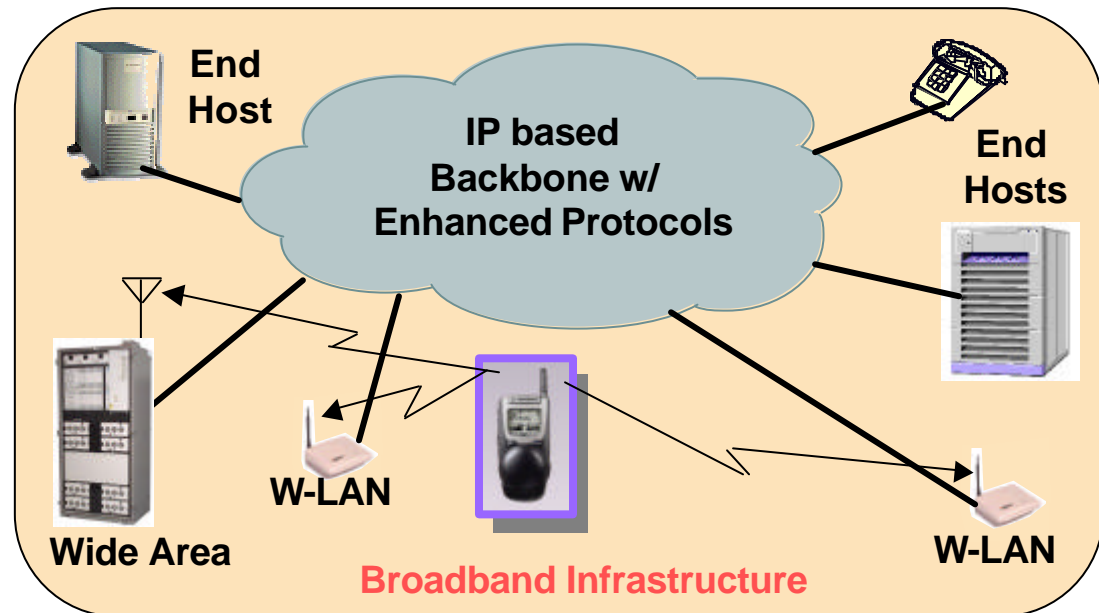
Seamless Mobility Deployment

THE Open GROUP
... enabling enterprise integration

GOAL: Distributed IP-based Infrastructure With Rapid Seamless Service Deployment

- Plug 'N Play Access Elements
- Mobility Across Access Domains
- Multimedia, Voice, Data
- Lower Costs

APPROACH:
Embrace Peer-to-Peer Networking
Functionality into End Points &
    Internet Protocols
Access Points Become
    IP-Addressable Gateways

End Host

IP based Backbone w/ Enhanced Protocols

End Hosts

W-LAN

Wide Area

Broadband Infrastructure

W-LAN

Recent Developments

- Research Architecture and Requirements Overview document
- IETF Activities - Underway
  - Standardization of IP enhancements required
  - Leadership in some key IEEE 802.11/IETF Working Groups

Resulting Capabilities

- Seamless services between W-LAN Enterprise and wide area environments
- Seamless integration of private system communications, including W-LAN
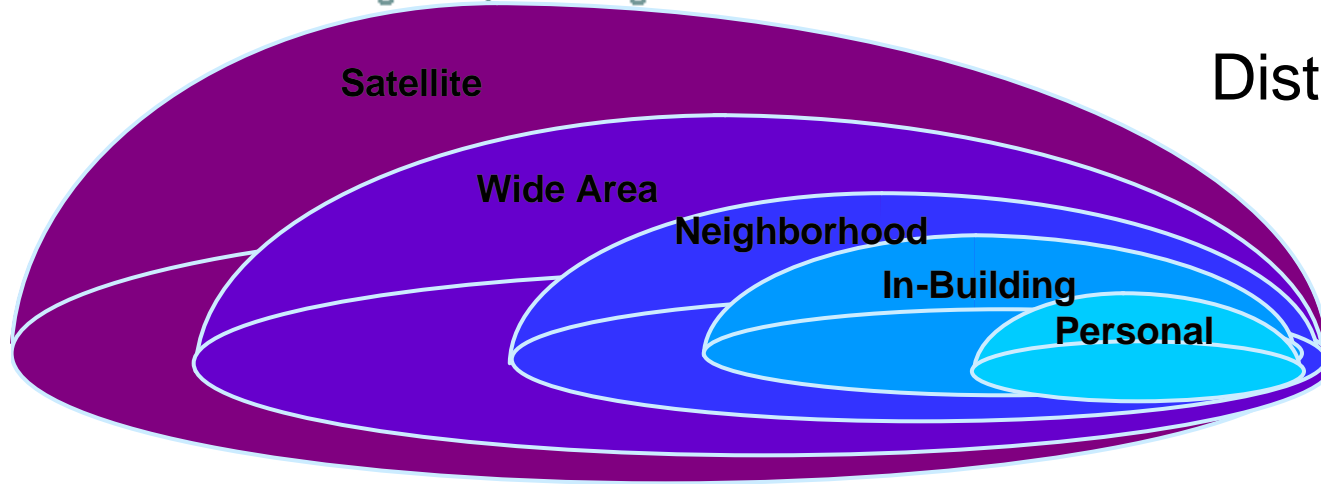- Little distinction between IP-based wireless and wired applications
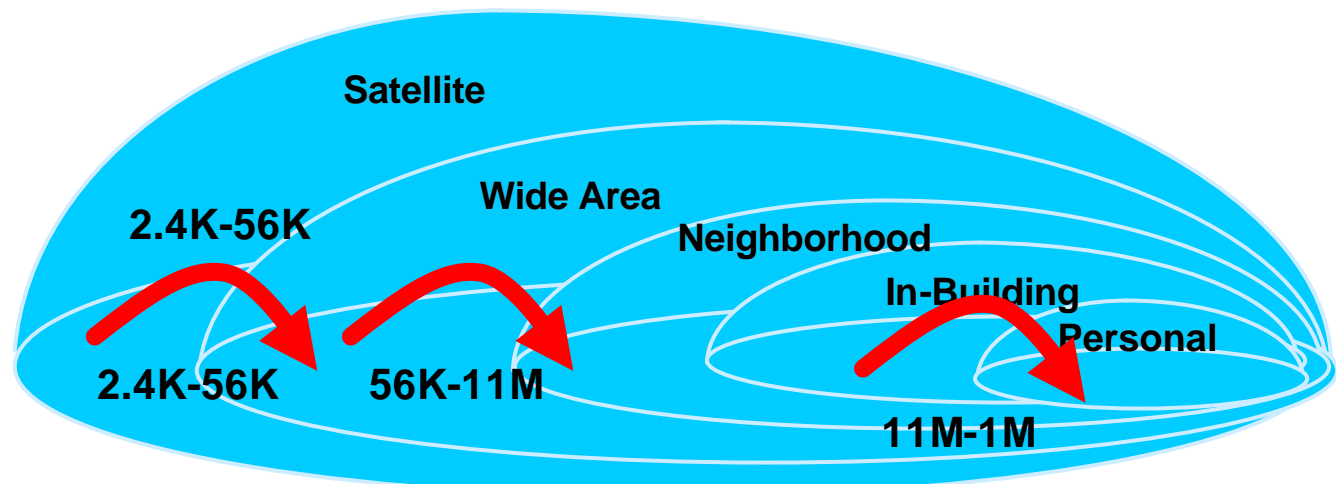
Secure Mobile Architecture Vision

THE *Open* GROUP
... enabling enterprise integration

Distinct Regimes

Satellite

Wide Area

Neighborhood

In-Building

Personal

Transparent Regime Selection

Satellite

2.4K-56K

Wide Area

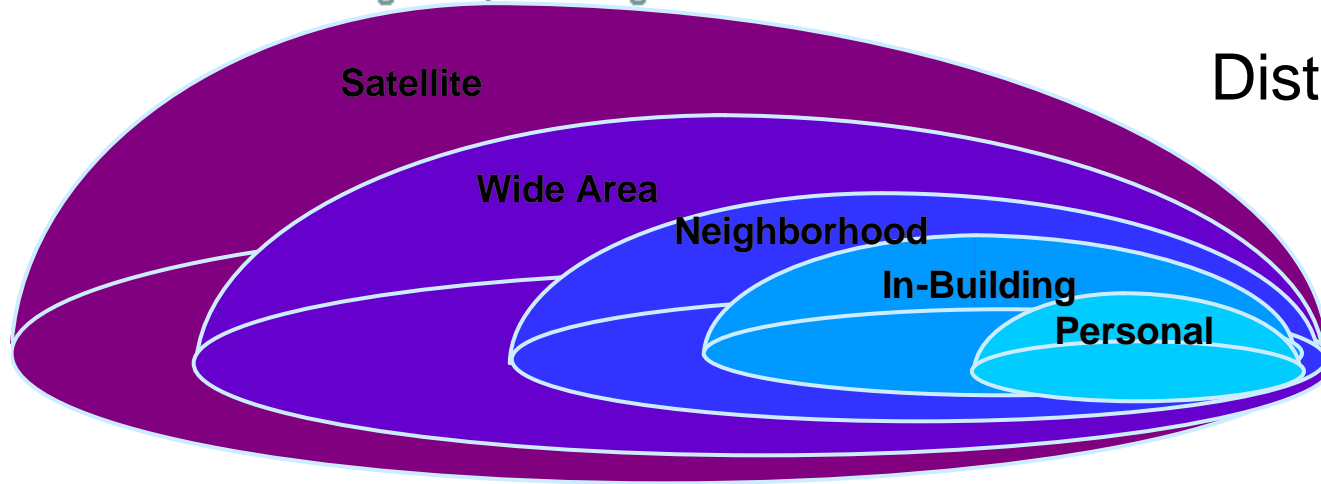Neighborhood

In-Building

Personal

2.4K-56K

56K-11M

11M-1M

Protocol-based Transparency

Single Transition Vision

THE *Open* GROUP
... enabling enterprise integration

Distinct Regimes

Satellite
Wide Area
Neighborhood
In-Building
Personal

Transparent Regime Selection

Satellite
Wide Area
Neighborhood
In-Building
Personal

56K-11M

Protocol-based Transparency

Wireless Voice and Data Technology Overlay
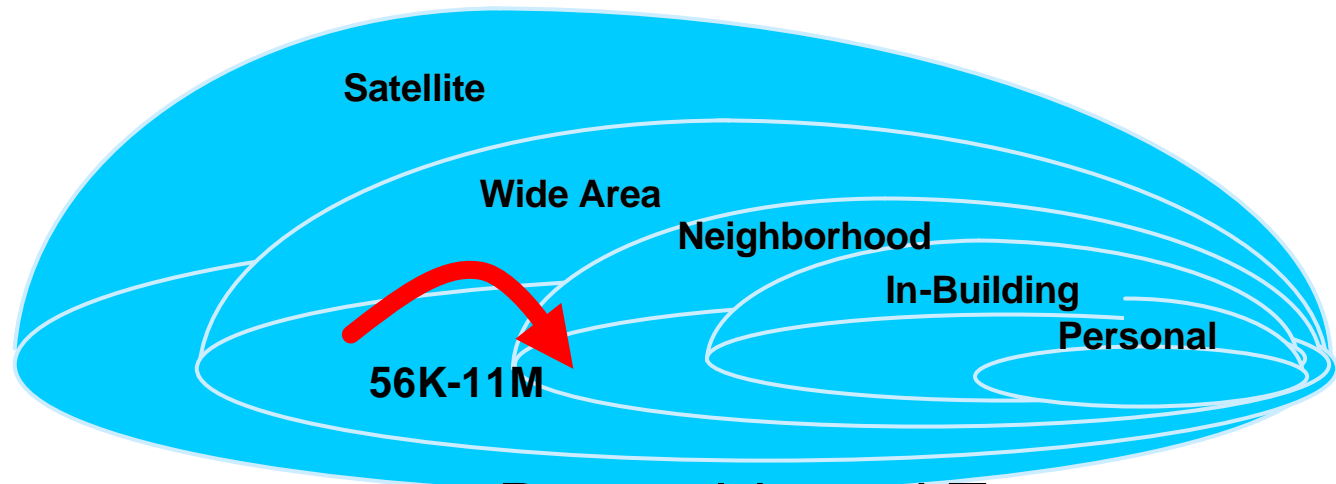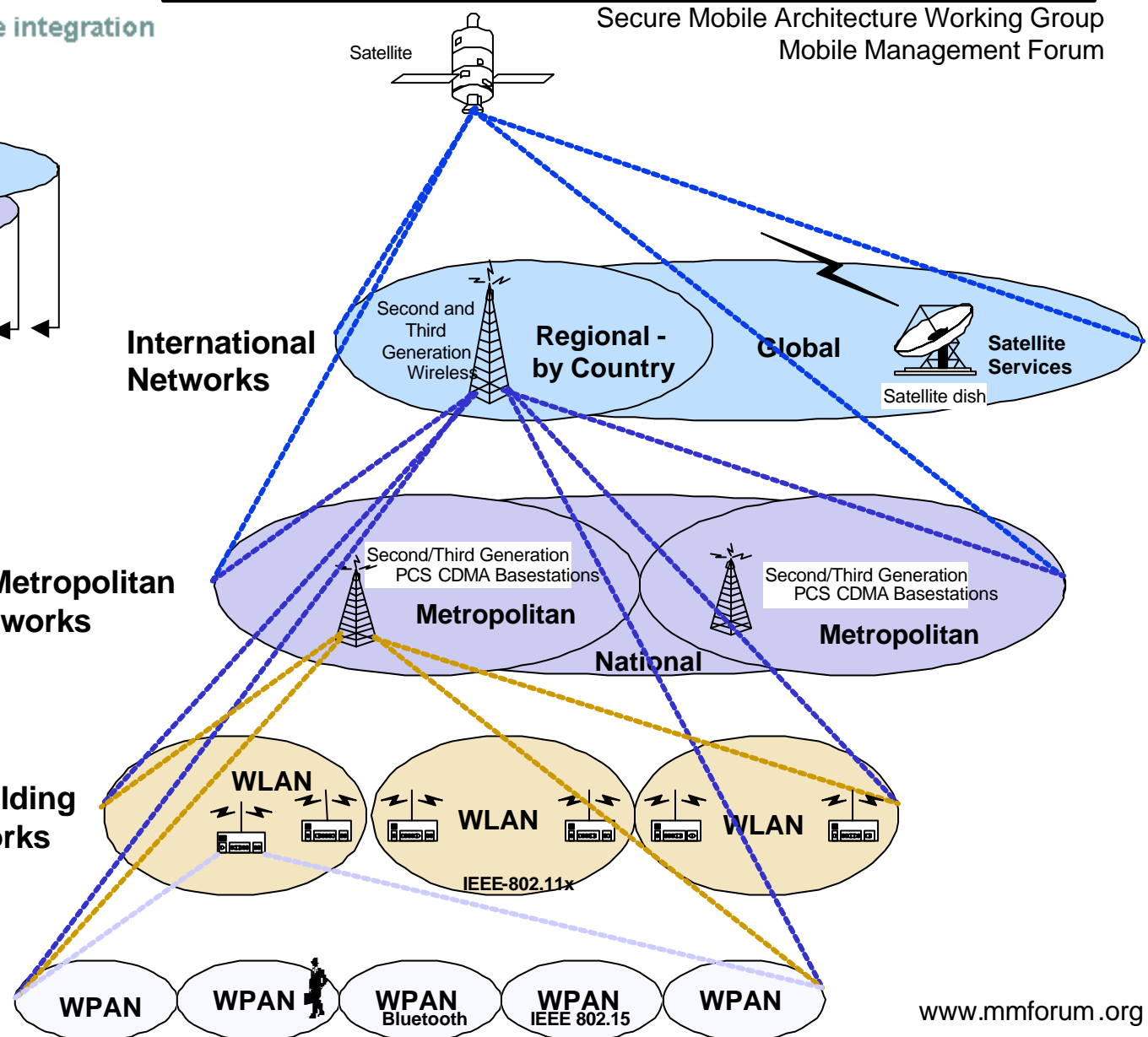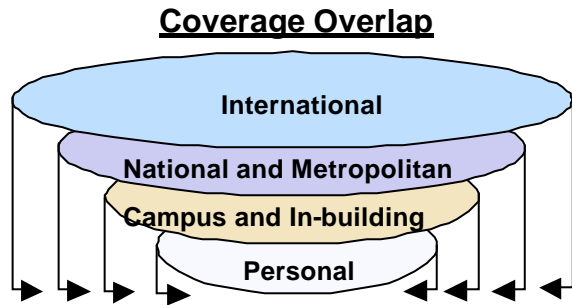
THE *Open* GROUP

... enabling enterprise integration

Secure Mobile Architecture Working Group
Mobile Management Forum

Satellite

Coverage Overlap

International

National and Metropolitan

Campus and In-building

Personal

International Networks

Second and Third Generation Wireless

Regional - by Country

Global

Satellite Services

Satellite dish

National and Metropolitan Wide Area Networks

Second/Third Generation PCS CDMA Basestations

Metropolitan

Second/Third Generation PCS CDMA Basestations

Metropolitan

National

Boeing Campus and In-Building Wireless Local Area Networks (WLANs)

WLAN

WLAN

WLAN

IEEE-802.11x

Boeing Wireless Personal Area Networks (WPANs)

WPAN

WPAN

WPAN Bluetooth

WPAN IEEE 802.15

WPAN

www.mmforum.org

Mobile Wireless Coverage Relationships

THE Open GROUP
... enabling enterprise int

International

Satellite 2.4-64 Kb/s

PCS CDMA 14 Kb/s -2 Mb/s

WLAN 1-54 Mbps, 300 feet

Metropolitan and National

WPAN 1-20 Mbps, 30 feet

www.mmforum.org
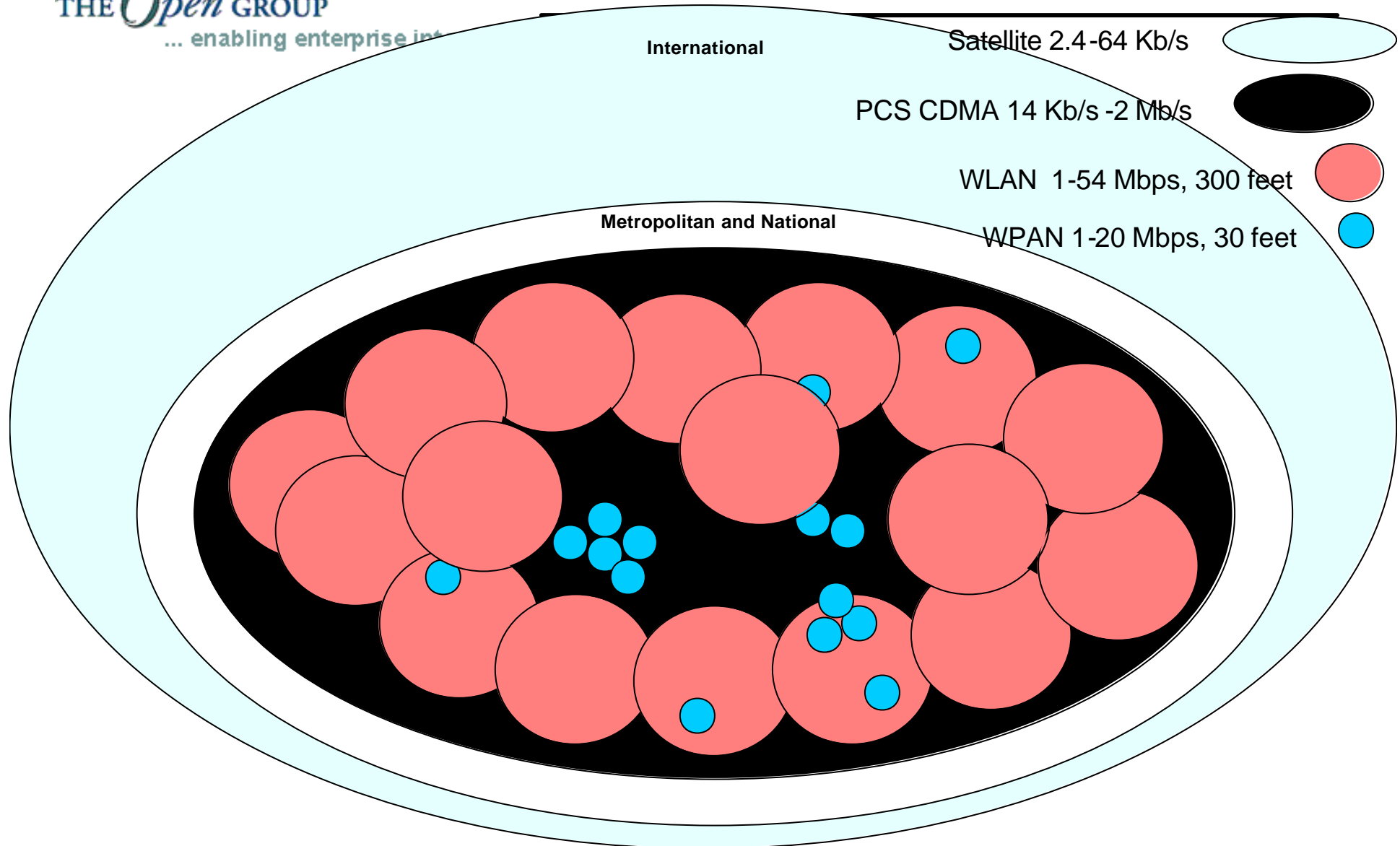
CDMA & WPAN Wireless Vision

THE *Open* GROUP
... enabling enterprise integration

Boeing
Telecom & Intranet
Networks

PDA

Notebook PC

WPAN

PC Card
(PCMCIA)
WPAN Radio

CDMA
Phone

WPAN
Synchronization

Two Way Paging,
Messaging & e-mail

Digital Voice,
Paging, Messaging,
& e-mail

Planned Security Envelope

WLAN Wireless Vision

THE *Open* GROUP
... enabling enterprise integration

Campus
LAN

LAN
Switch

WLAN
Access
Point

**VoIP Voice,
Paging, and Messaging**

Web Pad

Notebook PC

**Two Way Paging,
Messaging & e-mail**

Planned Security
Envelope
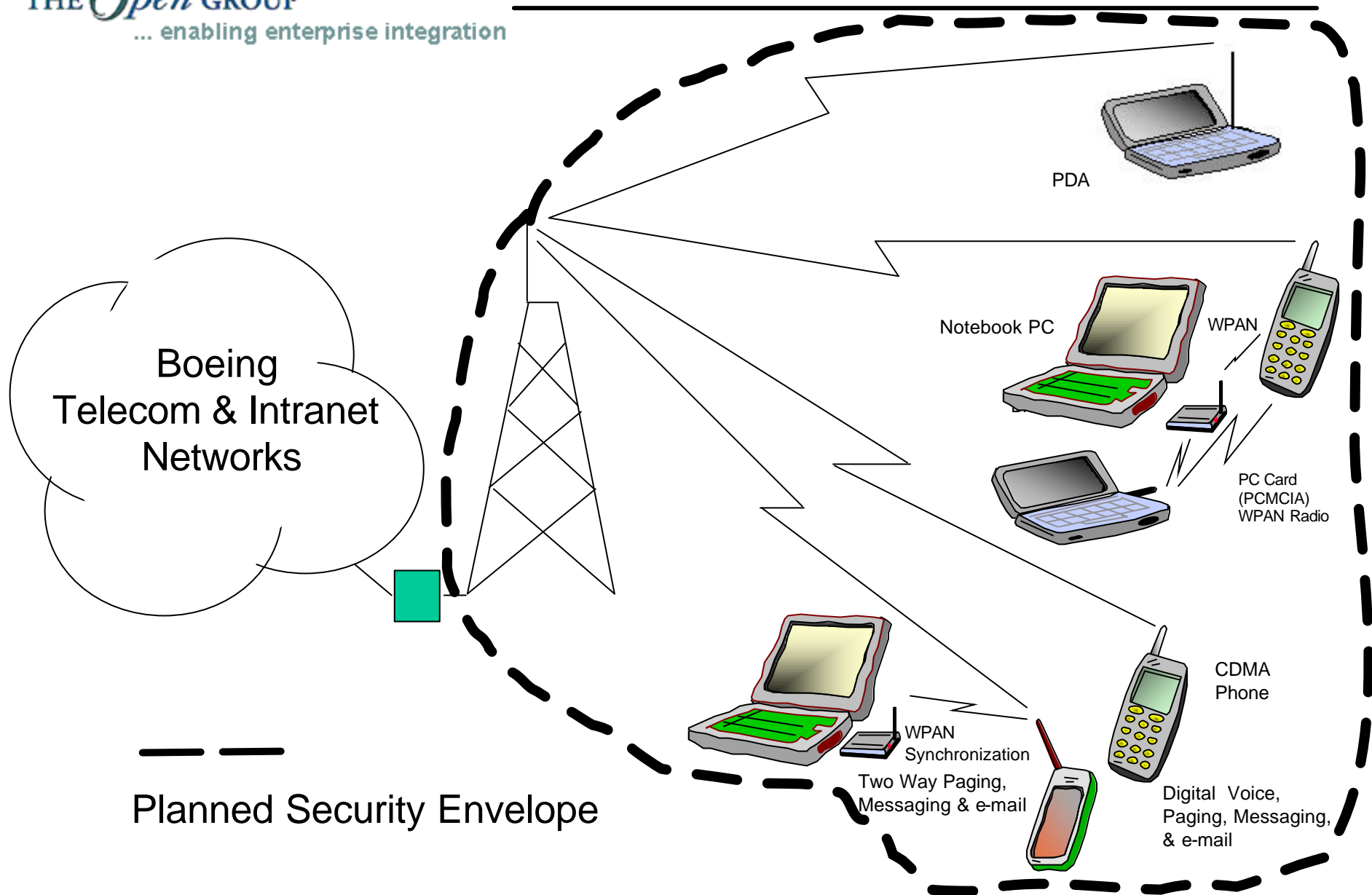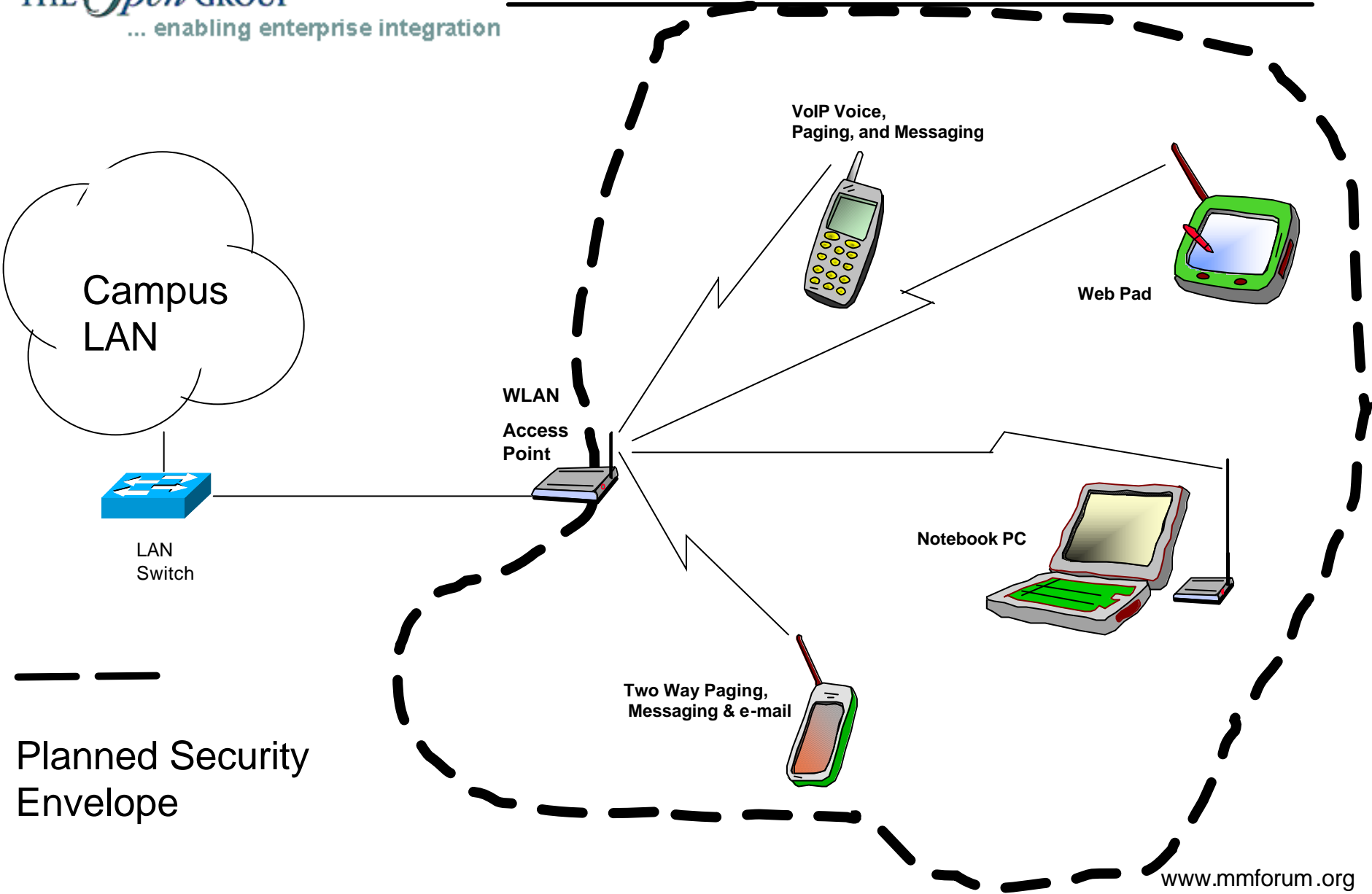
Inter-RAT Handoff Matrix

Secure Mobile Architecture Working Group
Mobile Management Forum

HANDOFF		to RAT								
		802.11a	802.11b	802.11g	HL2	MMAC	Bluetooth	W-CDMA	CDMA2K	GPRS
from	802.11a	N/A								
RAT	802.11b		N/A							
	802.11g			N/A						
	HL2				N/A					
	MMAC					N/A				
	Bluetooth						N/A			
	W-CDMA							N/A		
	CDMA2K								N/A	
	GPRS									N/A

- **6 different Handoff** scenarios to analyze for intra-802.11 operations.
- **12 additional Hando**ff scenarios to analyze for WIG interworking.
- **24 additional Hando**ff scenarios to analyze for other identified wireless data RATs.
- There may be certain reasons why some of these scenarios are not practical to standardize.
- Priorities and consensus scheduling needed to address completion of worktasks for each new RAT addressed by 802.11.

Requirements

- Policy Enabled
- Secure (AAA at least 2 level authentication)
- Seamless Cellular MAN/WAN to WLAN
- Common Information Model
- Macromobility
- Directory-Enabled Network + Real Time Mobility Info
- Discovery
- Event Handling
- Infrastructure for Radio Integration (Software Defined Radios)

Secure Mobile Architecture Requirements

THE *Open* GROUP

... enabling enterprise integration

- **Mobility management with both the server (Session Management) and protocols**

- **A secure protocol set to make seamless mobility viable**

- **Policy-based secure selection process for which location, network entitlements, bandwidth are delivered**

Issues

- Privacy
- Address transparency (E.164 to IP address)
- Mobile Security
- Lack of consensus on information model and how to use it
- Existing focus on static networks
- Mobile Network Architectures
- Network Management of Mobile Devices and Mobile Networks
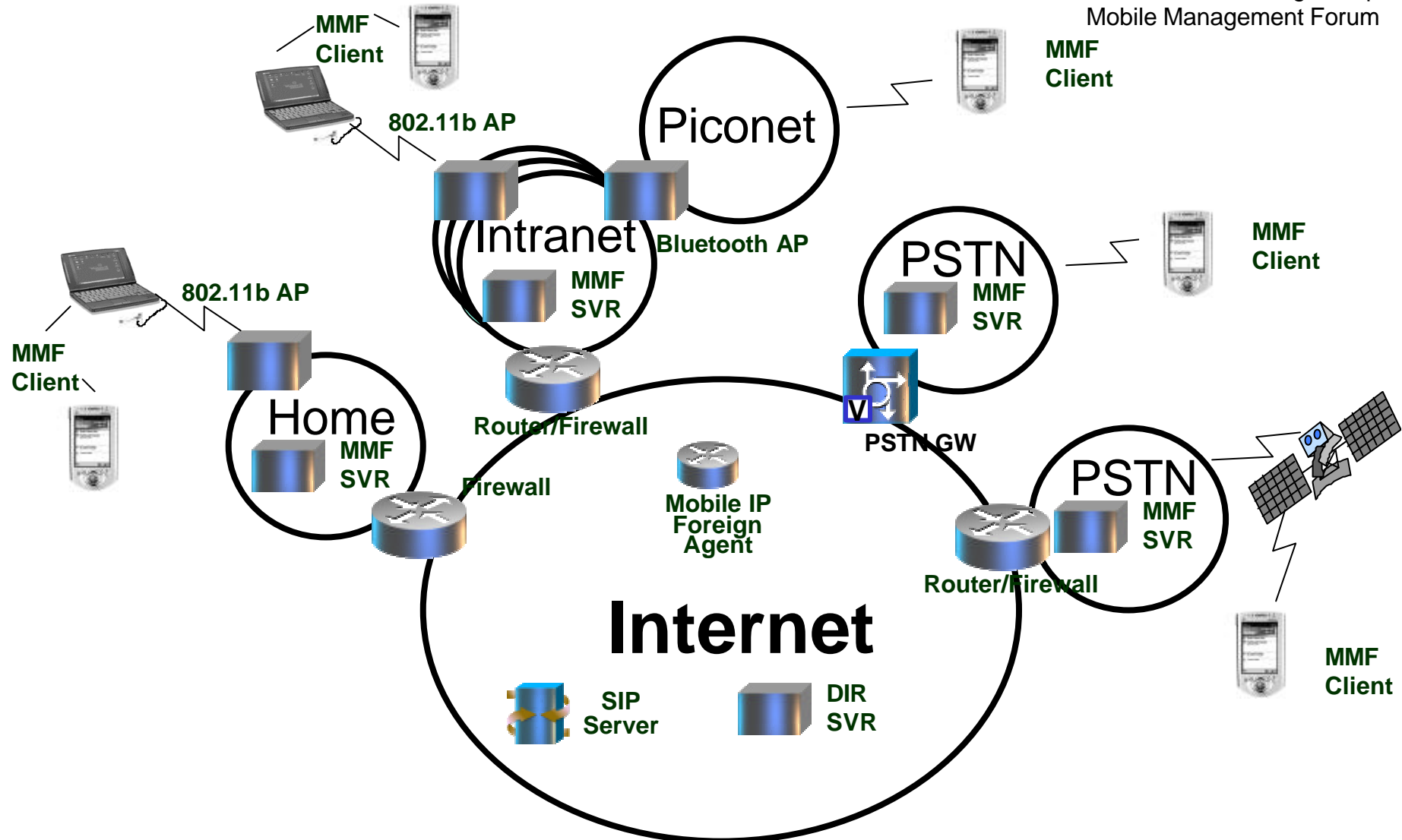- Mobile VOIP
- QoS in the Mobile Environment

Executive on the Move Requirements

- Secure Communications over:

  - WLAN in office (is there a PAN in the office?)

  - Cellular in taxi

  - Airport Airline Lounge WLAN

  - Airport Infrastructure WLAN

  - Airplane WLAN

Sessions Mgt Arch
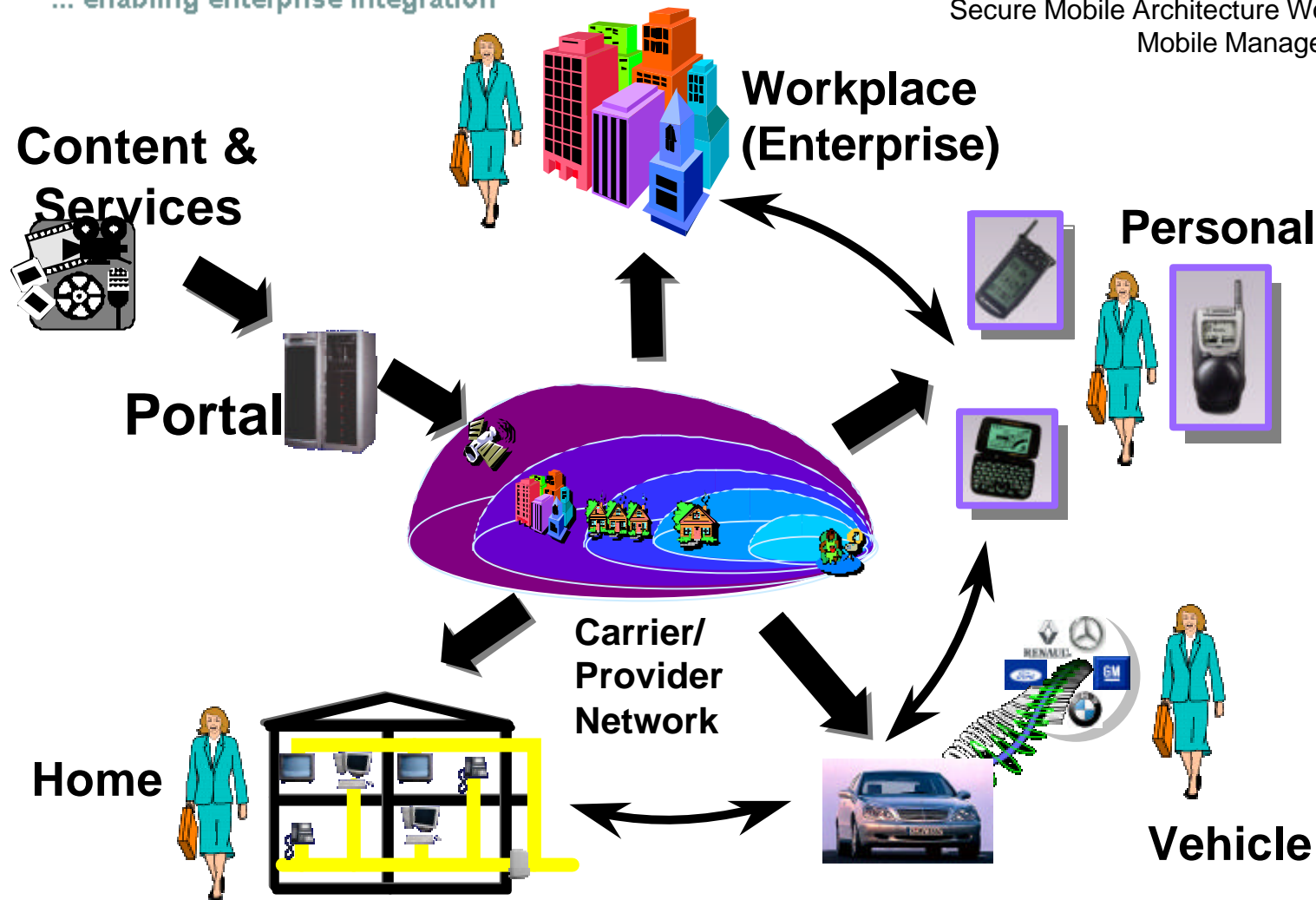
THE *Open* GROUP
... enabling enterprise integration

MMF Client

MMF Client

802.11b AP

Piconet

MMF Client

Intranet

Bluetooth AP

PSTN

MMF SVR

MMF SVR

802.11b AP

MMF Client

Home

MMF SVR

Router/Firewall

PSTN GW

Firewall

Mobile IP Foreign Agent

PSTN

MMF SVR

Router/Firewall

Internet

SIP Server

DIR SVR

MMF Client

Converged Cellular/WLAN Experience

Workplace (Enterprise)

Content & Services

Personal

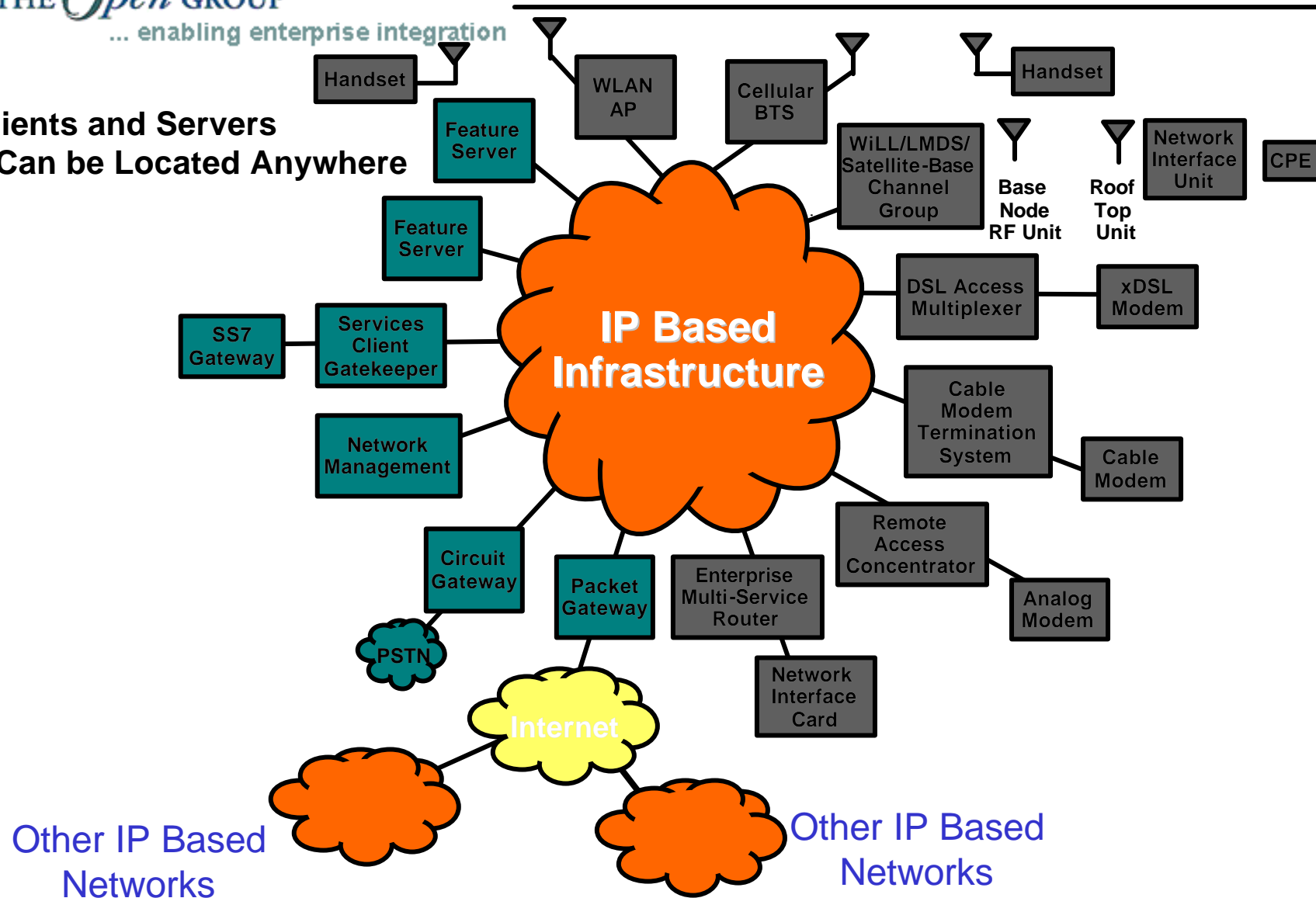**Portal**

Carrier/ Provider Network

Home

Vehicle

Converged Cellular/WLAN Infrastructure

THE *Open* GROUP
... enabling enterprise integration

-Clients and Servers
 Can be Located Anywhere

Handset

WLAN AP

Cellular BTS

Handset

Feature Server

WiLL/LMDS/ Satellite-Base Channel Group

Network Interface Unit

CPE

Base Node RF Unit

Roof Top Unit

Feature Server

IP Based Infrastructure

DSL Access Multiplexer

xDSL Modem

SS7 Gateway

Services Client Gatekeeper

Cable Modem Termination System

Cable Modem

Network Management

Remote Access Concentrator

Circuit Gateway

Packet Gateway

Enterprise Multi-Service Router

Analog Modem

PSTN

Network Interface Card

Internet

Other IP Based Networks

Other IP Based Networks

Multi-Layered Security
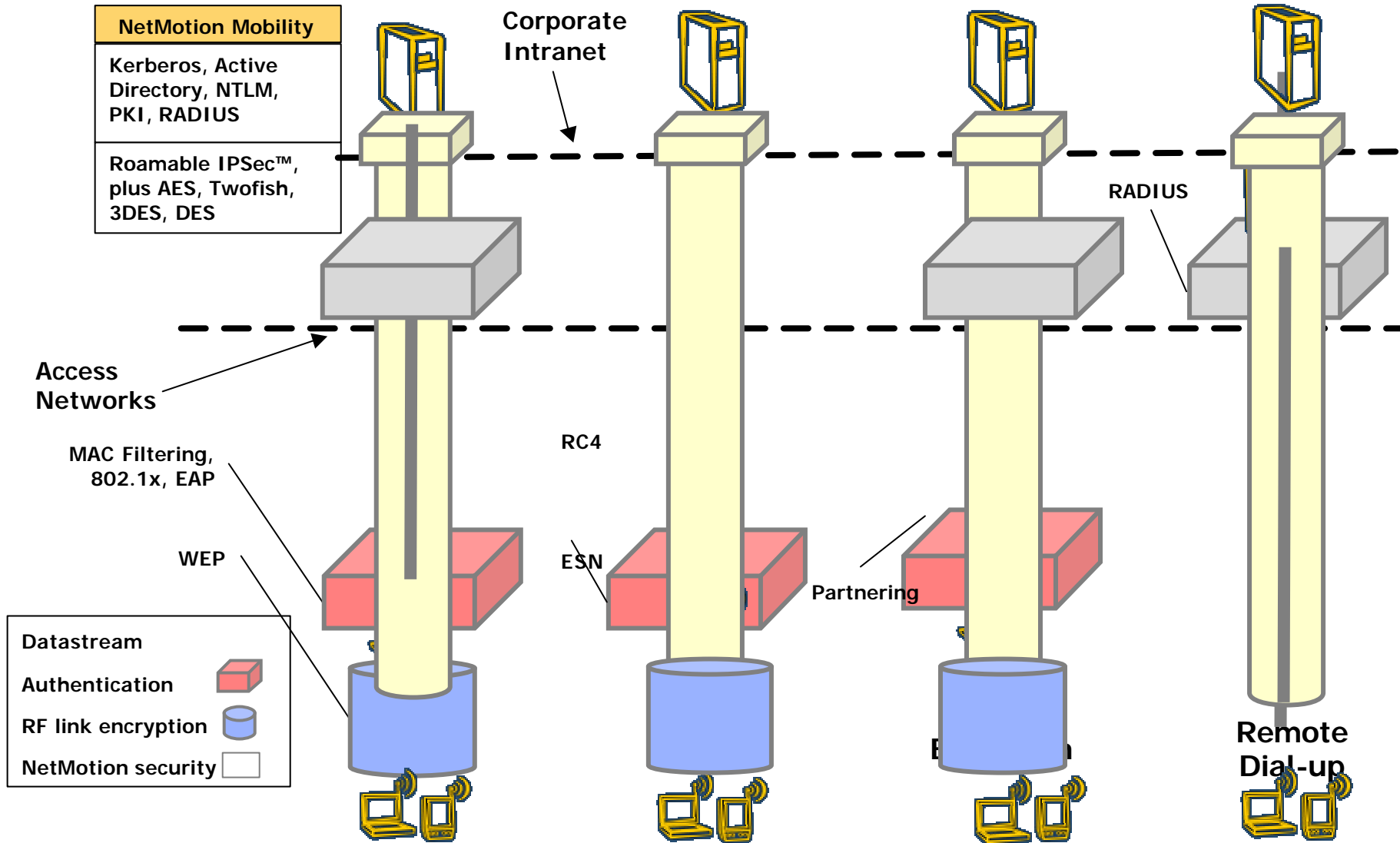
THE Open GROUP
... enabling enterprise integration

NetMotion Mobility
Kerberos, Active Directory, NTLM, PKI, RADIUS
Roamable IPSec™, plus AES, Twofish, 3DES, DES

Corporate Intranet

RADIUS

Access Networks

MAC Filtering, 802.1x, EAP

RC4

WEP

ESN

Partnering

Remote Dial-up

Datastream
Authentication
RF link encryption
NetMotion security

Secure Mobile Architecture Vision
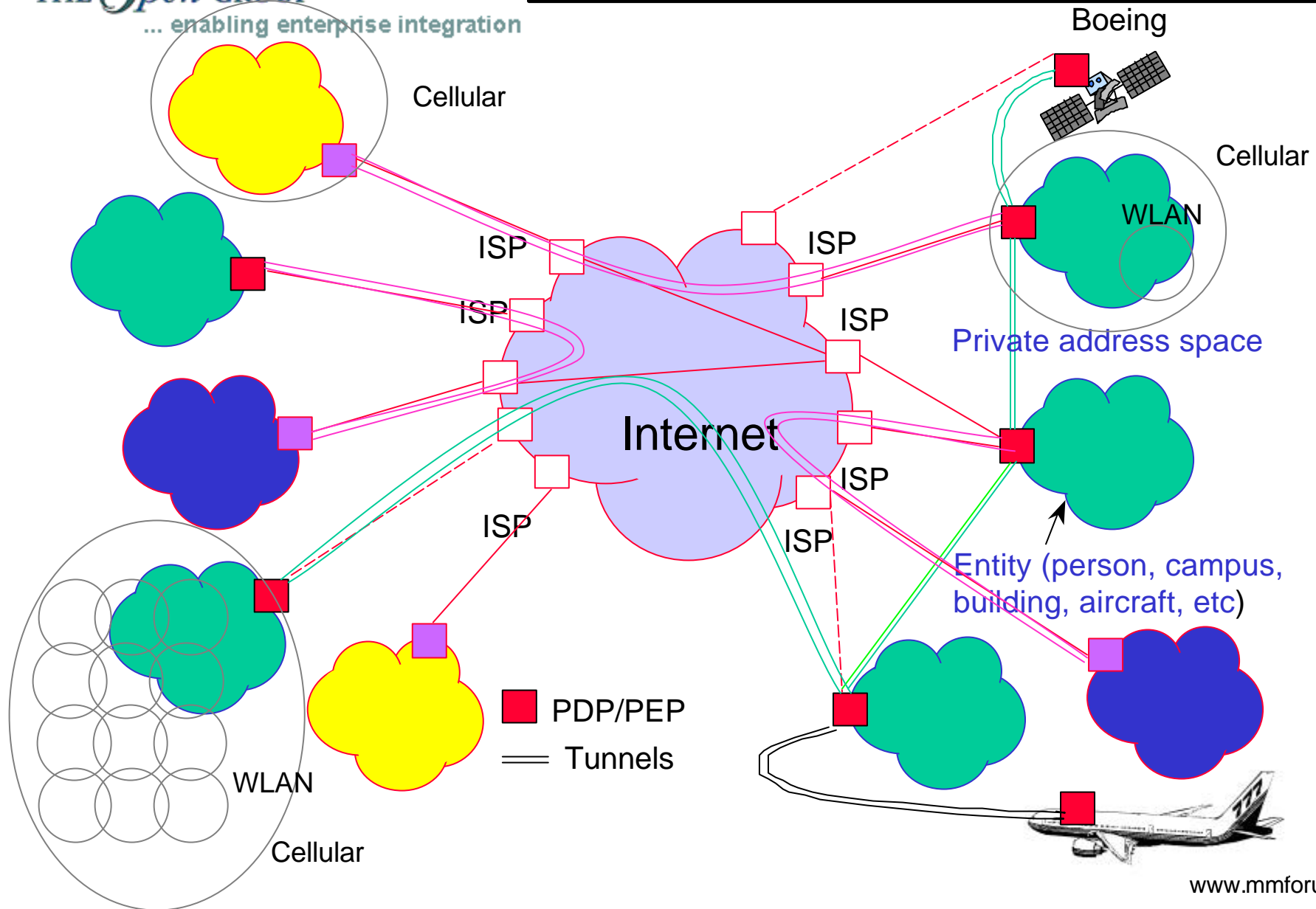
Principles
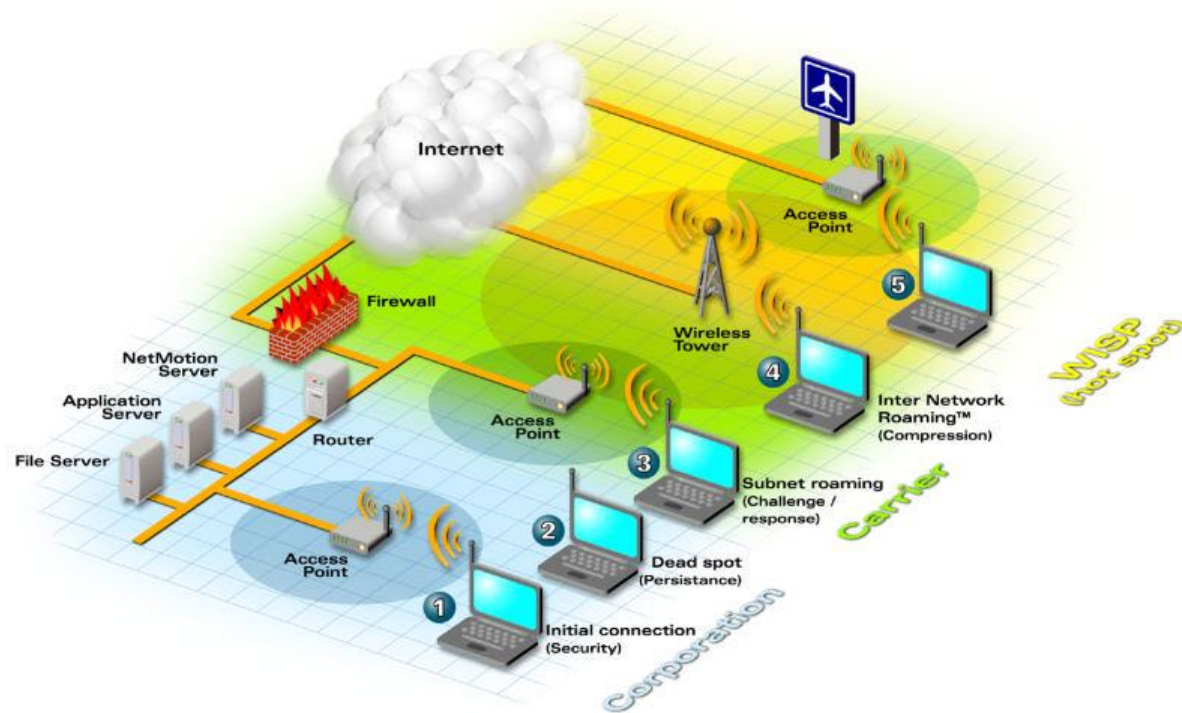
- **IP Only**
- **Policy-based**
- **Session Security**
- **AAA based on Standards-based Network Statistics**
- **SIP**
- **Personal Firewall on Every Device**
- **Host Identity Payload (HIP) – like (moving away from security based on MAC and IP address)**
- **Network Statistics are Standards-based**
- **Maximum data rate available**
- **WLAN (Hotspot+Hotzone) and WAN (MAN+Satellite) are Mobile**

Secure/Mobile Vision

THE Open GROUP
... enabling enterprise integration

Boeing

Cellular

Cellular

WLAN

Private address space

ISP

ISP

ISP

ISP

Internet

ISP

ISP

ISP

Entity (person, campus, building, aircraft, etc)

WLAN

Cellular

■ PDP/PEP

═ Tunnels

Security in Secure/Mobile

Secure

AAA

Authentication (strong)

Authorization (governmental, enterprise, personal)

Accounting (ISP, WISP, Cellular, Enterprise, Chargeback)

Identity

Identity Management

HIP

Certificates

HW

SW

Policies

COPS

RBAC (simple roles)

Personal Role – manage own security (with guidelines)

Governmental Role – government manages security

Enterprise Role – enterprise manages security

Mobility in Secure/Mobile

Mobile

Roaming across WLAN cells in a hotzone

Roaming from hotspot to cellular or 3GPP

Roaming from hotzone to cellular or 3GPP based on cost

Conclusions and Recommendations

THE *Open* GROUP
... enabling enterprise integration

- Secure Mobile Architecture undertaken with The Open Group

- Directory-Enabled Network (DEN) undertaken with DMTF

- Radio Resource Measurement undertaken with IEEE 802.11

- WLAN Security undertaken with IEEE 802.11i

- WLAN Secure IAPP undertaken with IEEE 802.11f

- Wireless Architecture under the Boeing WTWG

- VOIP Architecture under the Boeing VOIP TWG