

nortelnetworks.com



## **Understanding the Four Ps of Mobile Security**

**John Gray - Security Product Manager, Nortel Networks**

**Tuesday May 11, 2004**

# What's the Secure Mobility Challenge?

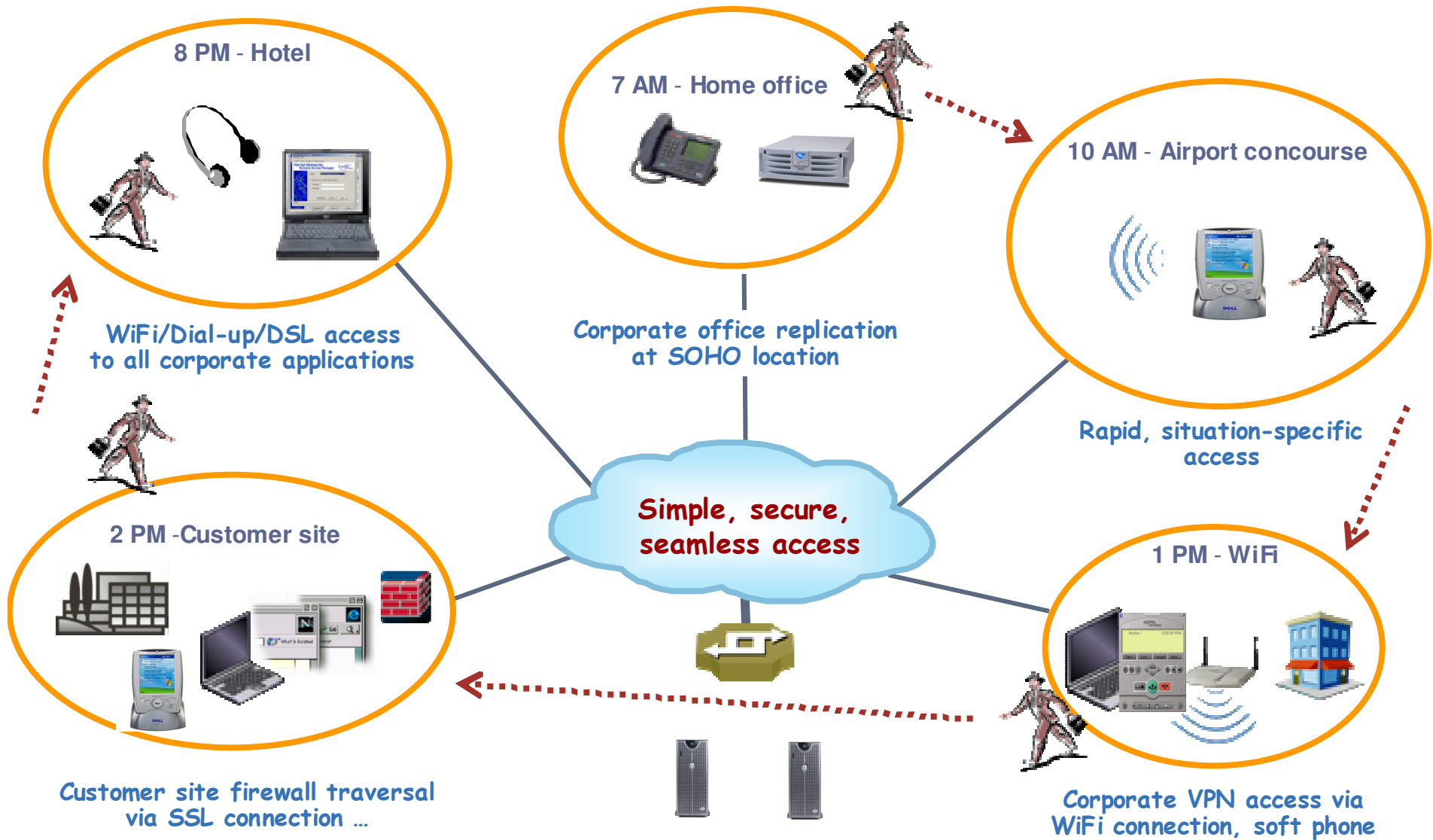
- **Making IP Mobile**
  - IP does not inherently support mobility (*or security for that matter*)
- **Taking Security “along for the ride”**
  - Security begins to break down when we go mobile
  - Extending “wired security” to a “wireless” paradigm not simple as 1+1
- **Managing the L2 connection & applications**
  - What is the best, faster, closest or lowest cost connection?
  - What happens when the applications time-out?
- **Lots of solutions aimed at solving this challenge**
  - Make applications mobile – Mobile FTP, Mobile SIP
  - Deal with it at the data link layer (Mobile drivers)
  - What about SSL VPN as a possible solution?
  - Focus on the network layer – make IP Mobile

But what's the **REAL** Challenge?

Convincing your boss that you didn't respond to them because you weren't "*connected*" to the network ...

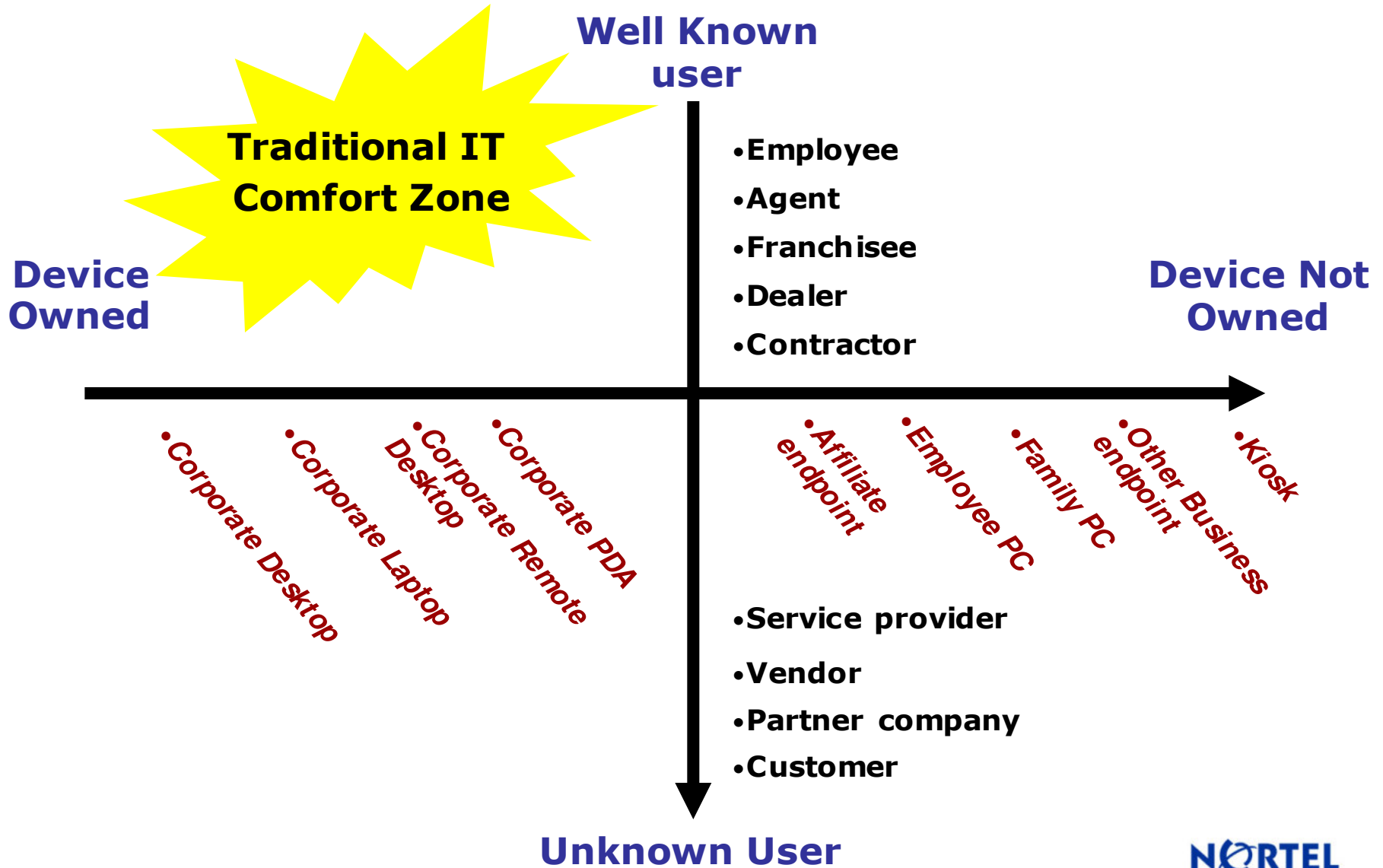
*... After your IS group deploys a "Secure Mobility" solution*

# A day in the life of a mobile worker



***Work is an activity – NOT a place***

# Securing the “Extended Enterprise”?



# The Evolving Wireless Landscape

**Wireless Wide Area Network**

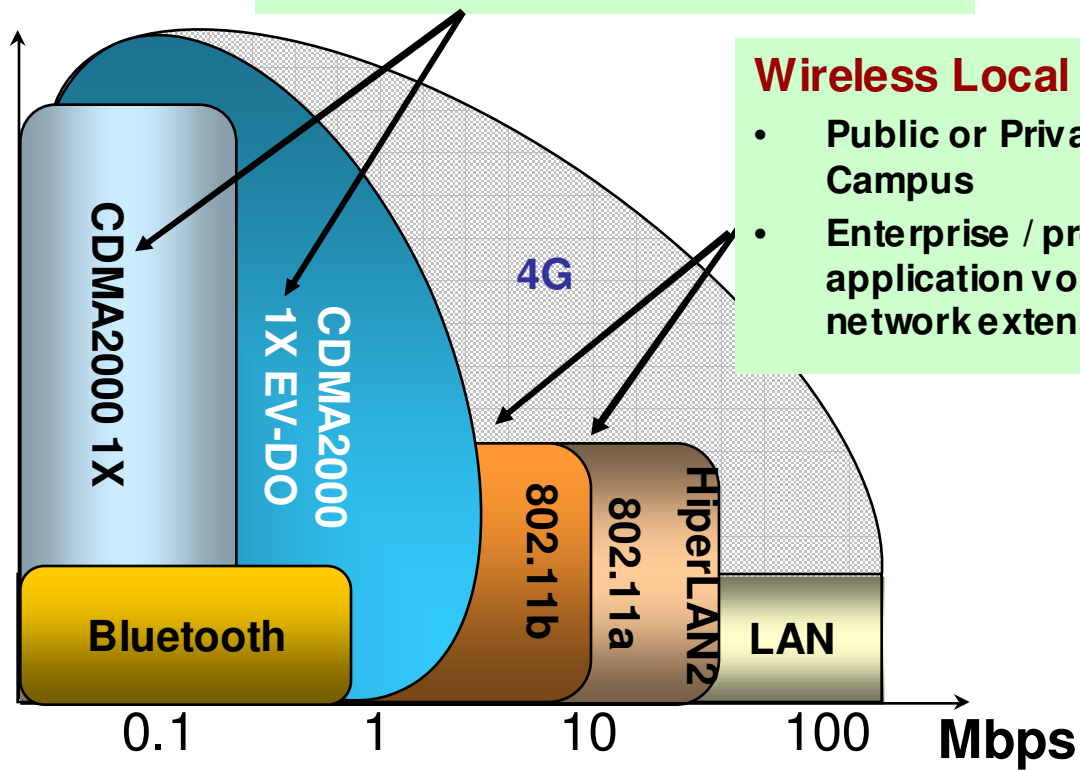
- Metro/Geographical area
- “Always On” Services
- Ubiquitous public connectivity

**Wireless Local Area Network**

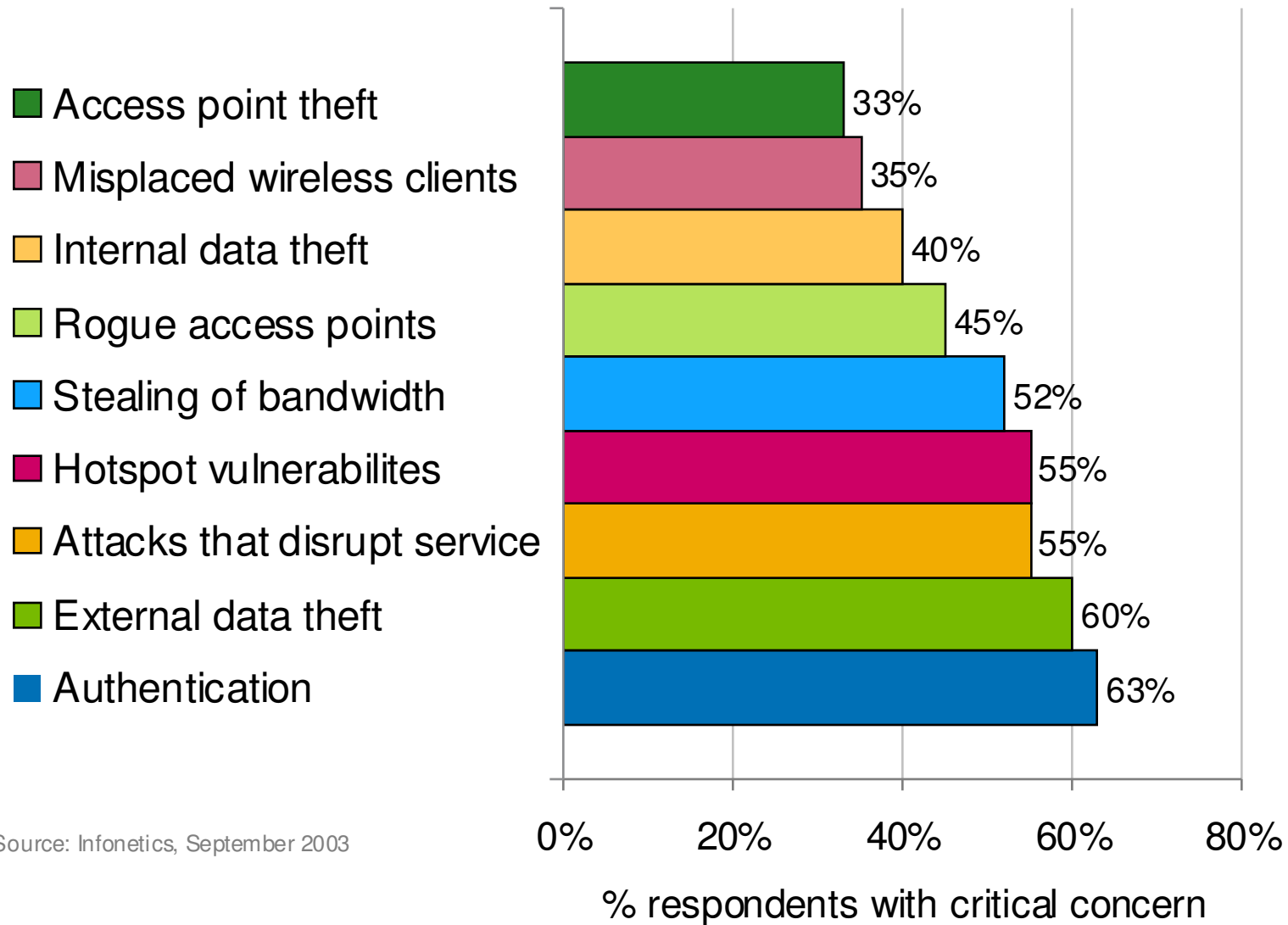
- Public or Private Site or Campus
- Enterprise / premises application voice & data network extension

**Mobility**

Outside Campus	Vehicle
	Walk
	Fixed
Within Campus	Walk
	Fixed/ Desktop



# Perceived WLAN security threats



Source: Infonetics, September 2003

# Intranet “Secure” Roaming is a Reality

Private WLAN



Public Cellular



**SECURITY OPTIONS:**

- ✓WPA (TKIP) & 802.1X
- ✓RADIUS (ESSID)
- ✓Unauthorized AP Detection
- ✓Network Design-DMZ



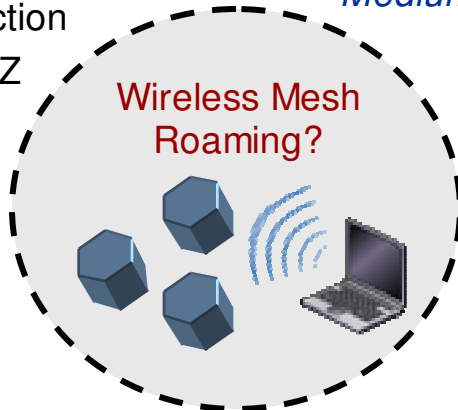
**SECURITY OPTIONS:**

- ✓IPsec & SSL VPN
- ✓Stateful Firewall, NAT
- ✓Network Based Svcs.
- ✓End to End Security



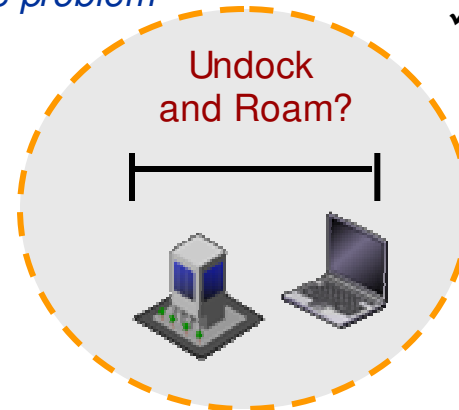
*Going mobile between these Mediums is the problem*

Wireless Mesh Roaming?



Public WLAN

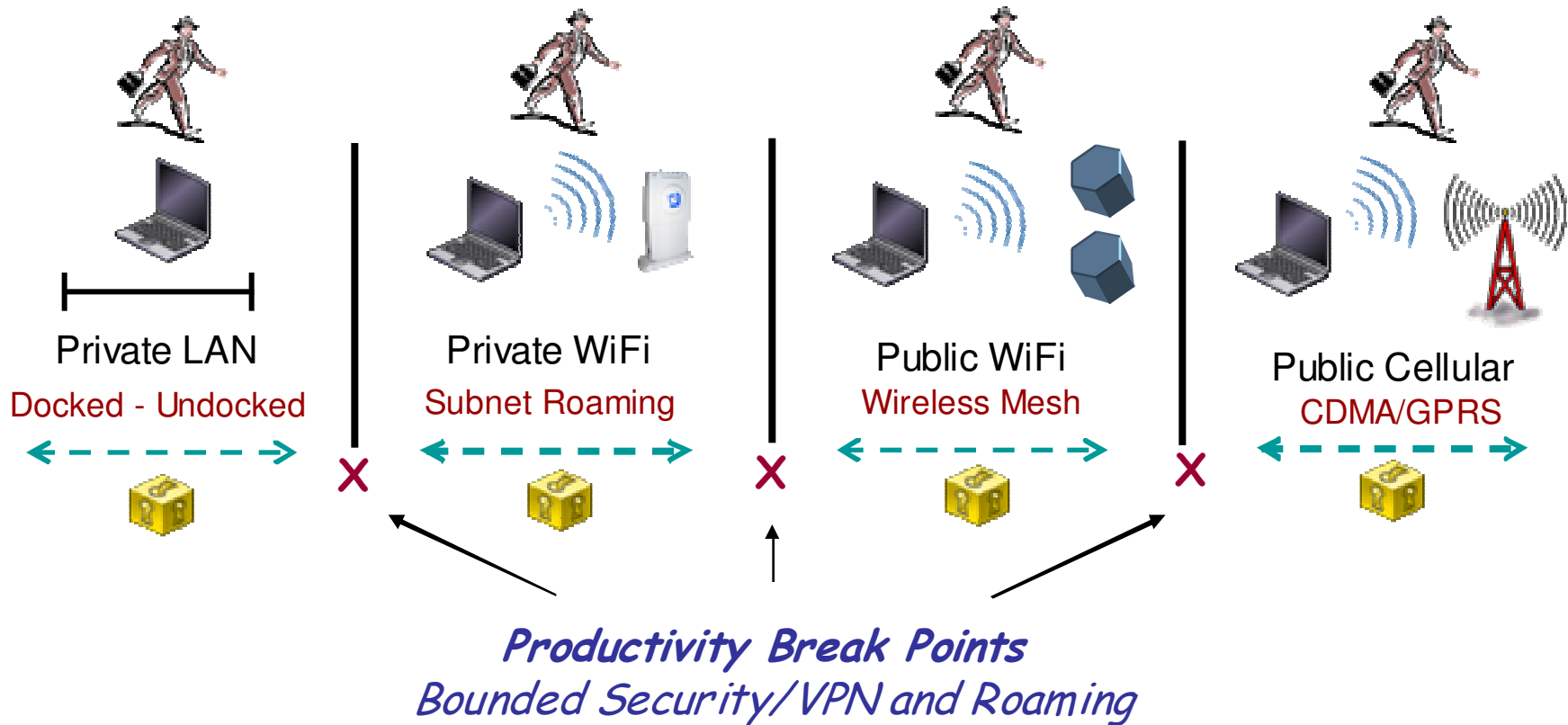
Undock and Roam?



Private LAN



# True “Secure Mobility” Remains Elusive



## ➤ Current mobility deployment challenges:

- Roaming limited to specific use case (eg., no roaming across private to public access)
- User Security/VPN connections “break” forcing them to re-login in and restart applications

# IP Mobility Architectures / Options

IP

Mobile Overlay

Mobile

- Mobile IP – Wireless Provider Deployment Model (RFC 3344)
- Additional client, servers & infrastructure needed
- **Still requires security** (VPN for end to end security)

IP

Value Added Overlay

Mobile

- 3<sup>rd</sup> Party Value Added (Security/VPN application persistence)
- Enterprise deployment model (cost, features, management)
- **Requires additional clients, servers & infrastructure**

Application

Application Layer Mobility

Mobile

- Not dependant on L3 IP addressing to function – small device support
- Browser based ubiquity – no “clients” to manage
- **Application support & End-point security?**

Mobilizing

VPN Deployments

IPsec

- Extends IPsec VPN (security) with mobility
- Tracks to IKEv2/MOBIKE effort – but available today
- **Allows installed VPN to become “Mobilized”**

# IEFT Standards Activity

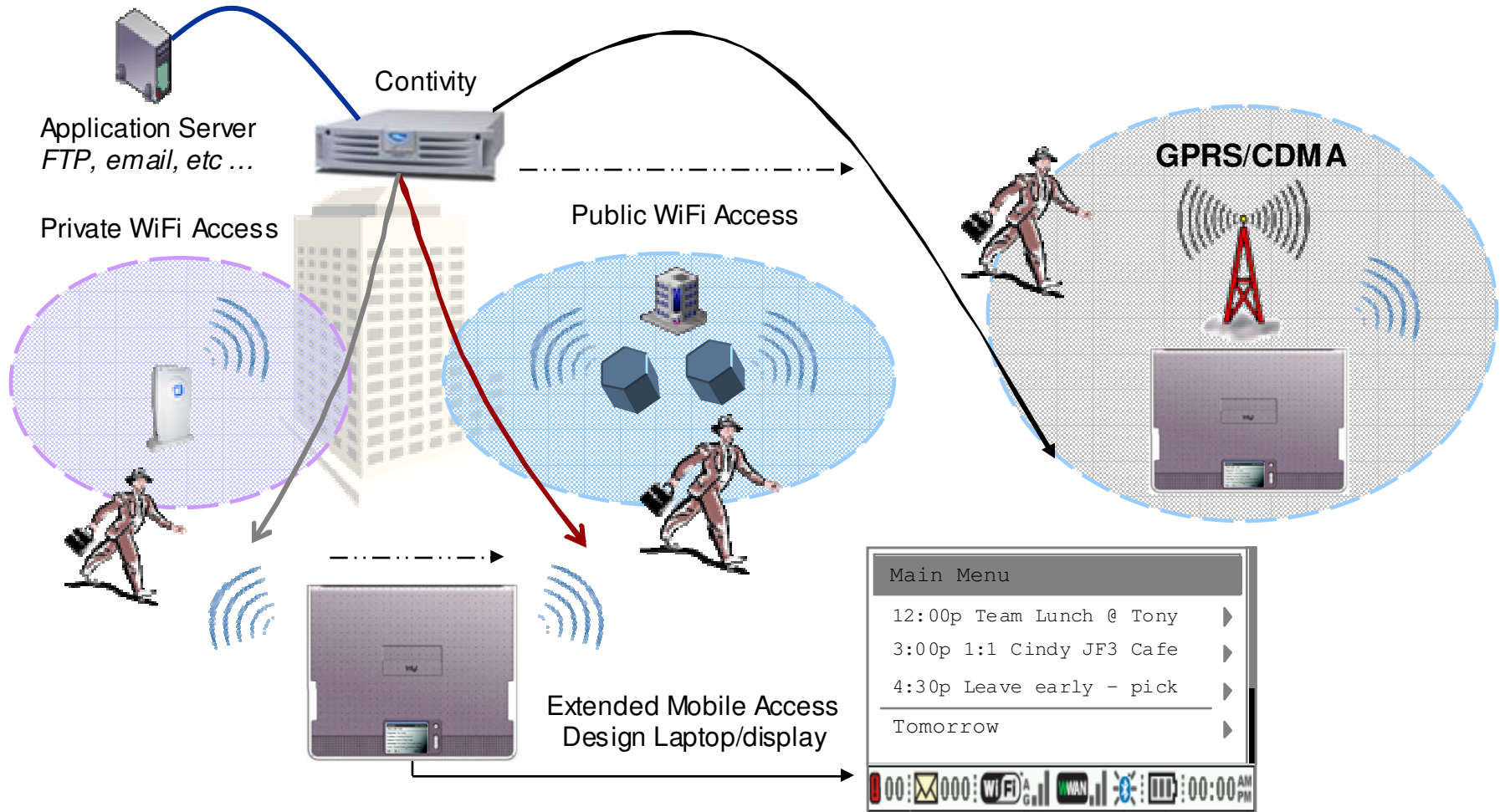
**IKEv2** – a simpler and more efficient version of IKE - the key management protocol for IPsec - that is being worked through IEFT. Current proposal does **not** include mobility extensions.

**MOBIKE** – IKEv2 Mobility and Multi-homing IETF Working Group – IEFT group chartered to **address IKEv2 lack of roaming, mobility**, and multihoming support. Collective IKEv2/Mobility effort *still 12-18 months away from RFC*.

**IKEv1** – currently deployed key exchange protocol standard for millions of IPsec remote access VPN clients and gateways. **No new enhancements** being accepted for IKEv1 at the IETF.

**IPsec Mobility** – Nortel Network IPsec implementation design to “mobilize” existing installed base of IPsec remote access deployments by leveraging currently deployed IKEv1 IPsec infrastructures. **Provides an immediate solution for customers today.** Nortel Networks will implement IKEv2/MOBIKE when it becomes a standard.

# “Closed-Lid, Fully Operation” Secure Access



**Private** ← ----- **Persistent IPsec VPN Tunnel** ----- → **Public**

- ✓ Persistent & Secure VPN Tunnel, No user re-login required when roaming
- ✓ Laptop stays operation (while closed) user applications/services stay active

# Mobility, VPN & Security Solution Offerings



## WLAN Security

- Key deployment attributes:**
- ✓WiFi RF and Security requirement
  - ✓WPA (TKIP) & 802.1X
  - ✓Unauthorized AP Detection
  - ✓Wireless Voice & Data
  - ✓Subnet Roaming



## VPN (IPsec) Gateway

- Key deployment attributes:**
- ✓IPsec VPN based access
  - ✓End to End L3 VPN Model
  - ✓RAS – SoHo – Branch VPN
  - ✓Employee RAS support
  - ✓Routing, WAN Access




## Secure Remote Access


- Key deployment attributes:**
- ✓SSL VPN based needs
  - ✓Client-less access requirement
  - ✓Web/Portal base applications
  - ✓Partners & customers access

## Software Based Mobile Security Solutions


← **Mobility, VPN, Security & IP Services** →



Wireless Security & Roaming



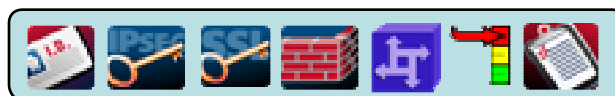
AAA, VPN, Access Control, REPS



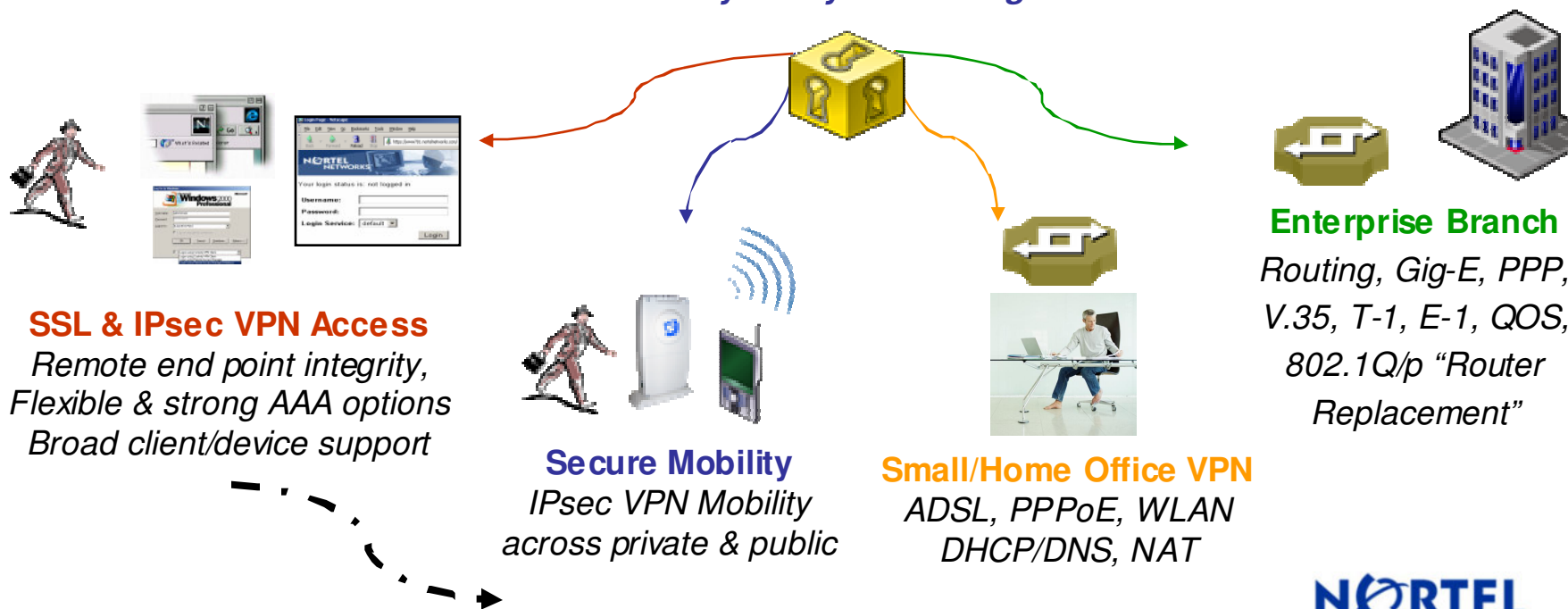
Client and Client-less access

# “Universal” Secure Mobility Gateway

Common Secure IP & Mobility Services



**AAA, VPN, Firewall, Routing/WAN, QoS,  
Security Policy and Management**



# Secure Mobility - Summary

Many solutions solving (aspects) the problem slightly different

Focus on the use case first - rather than the technology

Users, devices, applications, security and roaming/mobility requirement

Use what you already have in place *as it makes sense*

-IPsec and SSL VPN, security policies, AAA, defense in depth network design

-Add additional security as required - rogue AP detection, end point security etc ...

Be mindful of altering the “user’s experience”

-Not to mention how it impacts the security and your administration effort

Develop an “acceptable use policy” for your mobile users