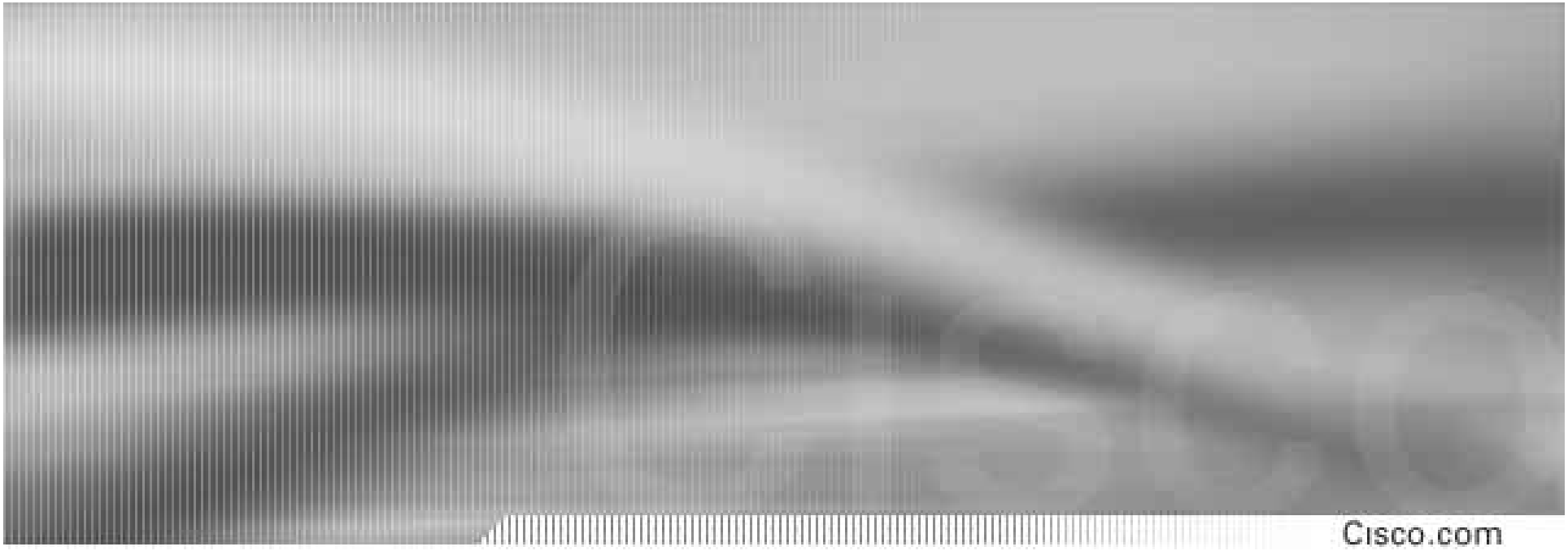


Cisco Enterprise Mobility

Overview of Technical Solutions

Nathaly Landry

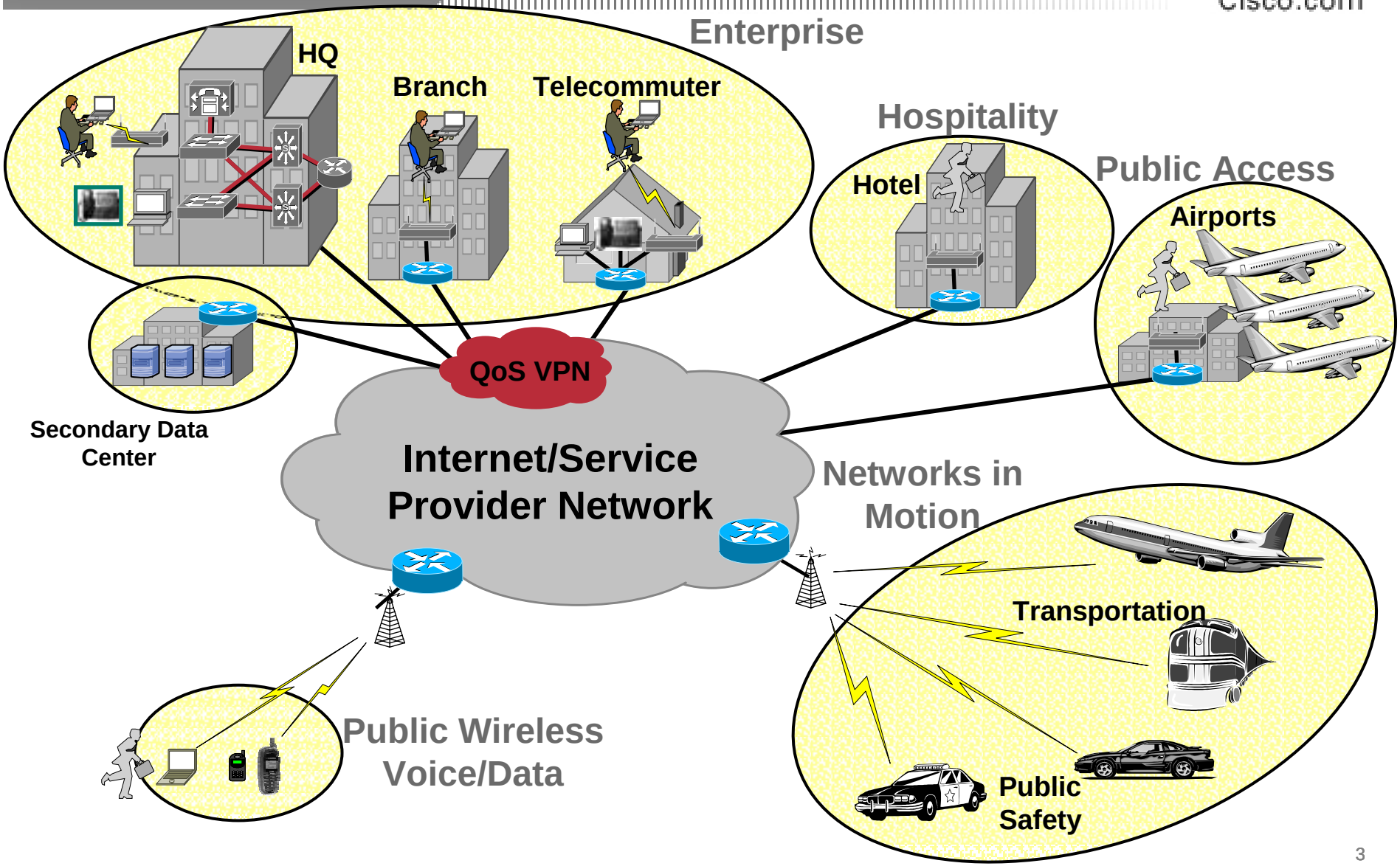
lnathaly@cisco.com

Agenda

- Cisco Enterprise Mobility Direction
- **Mobility Solutions Technical Overview**
- **Jon Coxworth – Intel – Centrino Technology**
- **Shawn Winter –Bell - AccessZone**

Today's Enterprise Workplace

Highly Distributed/Mobile Workforce



Today's Enterprise Productivity Challenges

While away from the Corporate Desk

On-Campus Productivity
Productivity degrades when away from desk (Meetings, Common Areas etc)

Corp Office NY
212-555-1212

New York

"I'll send out mtg minutes when I am back at my desk"

Internet

PSTN

I'm working from home today, call me at (212) 444-5678

Can I use the Phone now?

I'll be in DC today
Call me at
610-222-1234

Home Office

Philadelphia

Baltimore

Wash DC

Use of VPN client "dialer" to access Corp resources

Off-Campus Productivity
Degraded Data and Voice access when away from Corporate office

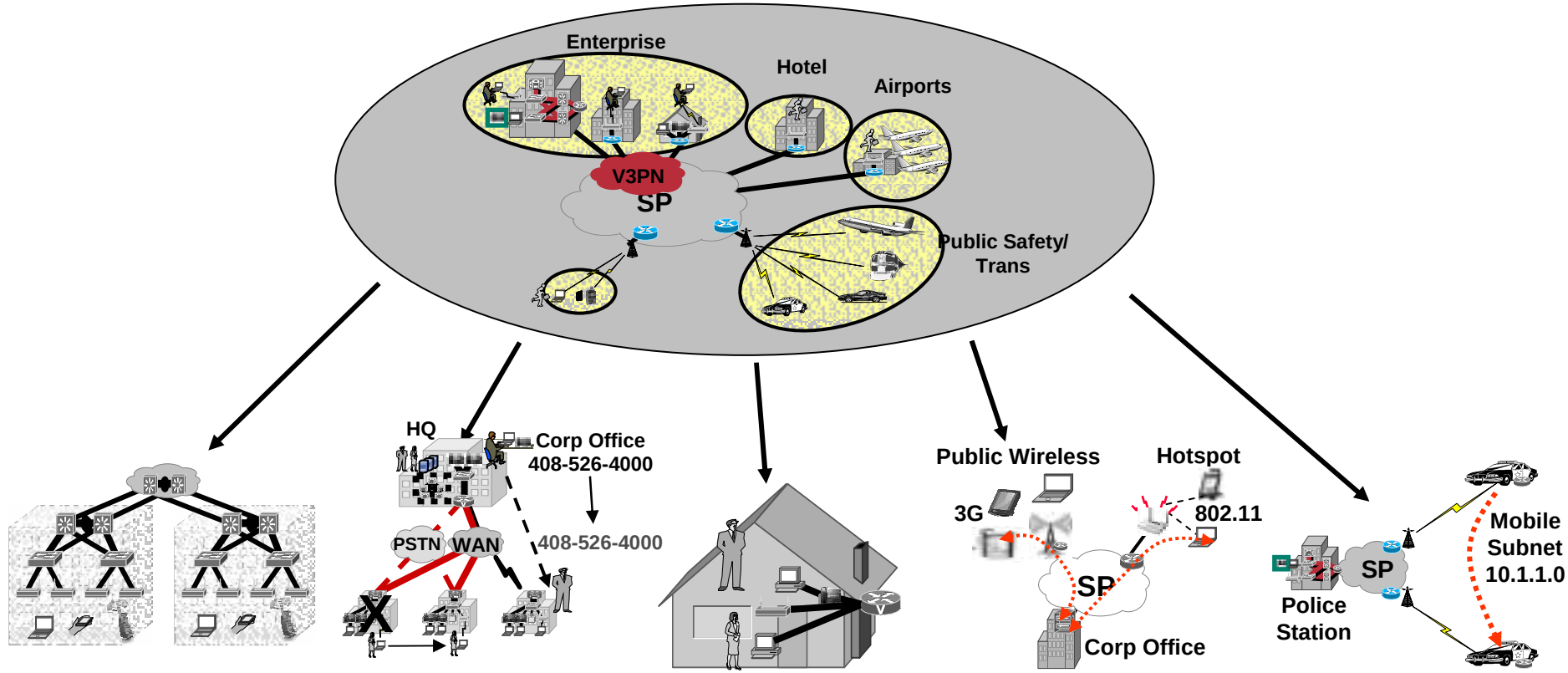
Where Does Increased Productivity Come From?

- **Steal 5 minutes at the beginning of meetings**
  - **Often meetings don't start on time**
  - **Instead of wasting time with idle chit-chat, get work done**
  - **3-4 meetings/day x 5 min./meeting = 15-20 min. productivity savings/day**
- **Eliminate *"I'll do it when I get back to my desk"* syndrome**
  - **Share files, PowerPoint presentations instantly**
  - **Arrange meetings using your online calendar**
  - **Saves 15-20 min./day for knowledge workers who don't sit at desks all day**
- **Use Instant Messaging as a corporate app**
  - **Great for quick communications; get answers without disturbing meeting**
  - **Only works if employees are connected to the network**
- **The "Connected Meeting"**
  - **Send presentations during meeting to all conf. call participants via email**
    - **Conf. calls are more productive when everyone is looking at same info**
  - **Follow presentations on your PC even if no projector in meeting room**

Cisco Enterprise Mobility Vision

Increasing Workday Productivity

Cisco.com

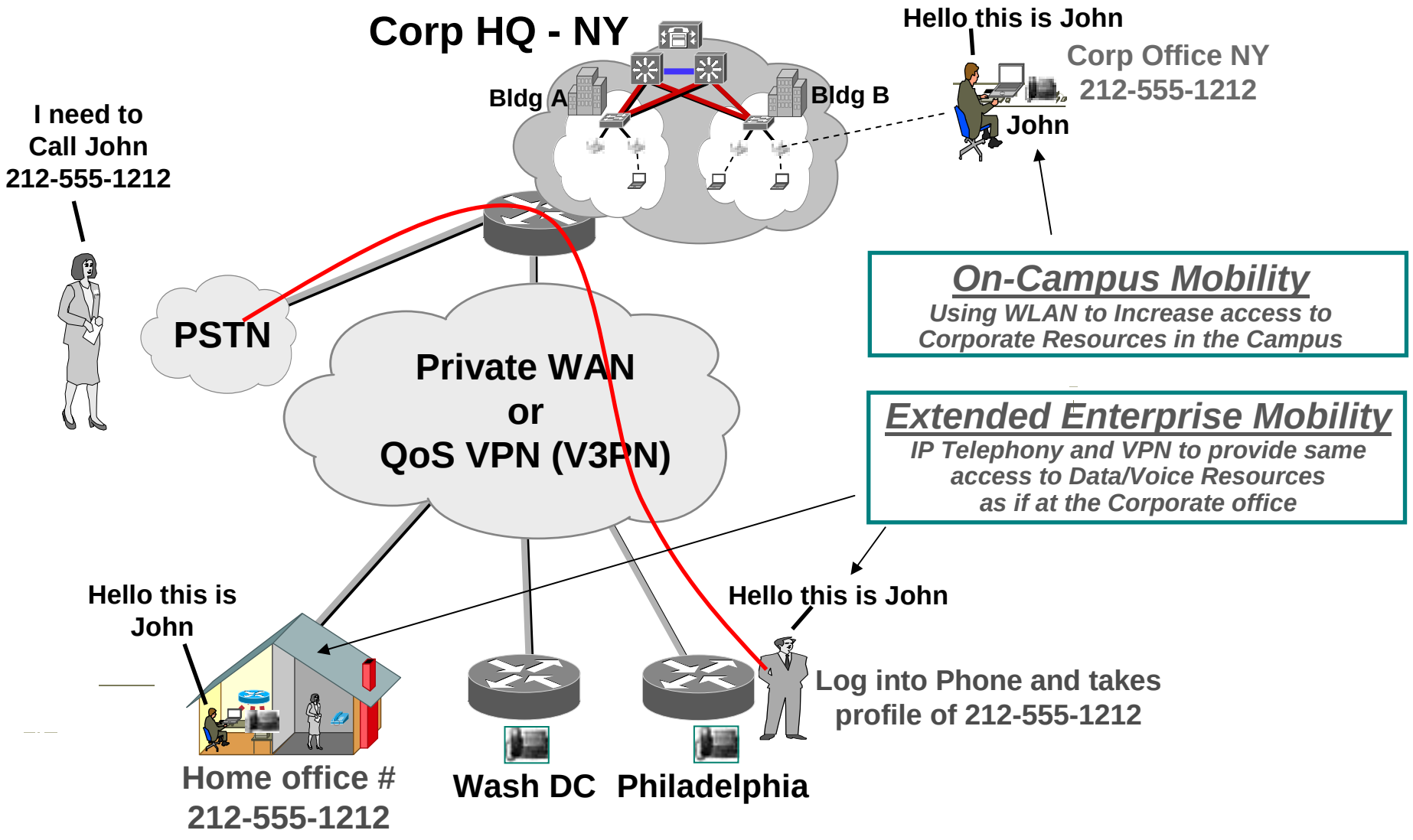


Campus WLAN	Branch Mobility	Teleworker	Users on the Move	Networks in Motion
• Secure WLAN Access • Rogue AP Prevention • WLAN IP Telephony • User Policies – Identity • Guest Access – Identity	• Rapid Deployment V3PN Pt to Pt Wireless • Extension Mobility – IP Tel	• IP Telephony (V3PN) • 802.1x User Authentication Spouse and Kids – Identity	• Hot Spot Access • PDA device access • Public Wireless Access	• Networks in Motion (Mobile IP – Mobile Router) • Public Safety • Transportation

Cisco Enterprise Mobility Solutions

Using Network Solutions to Deliver Increased Business Productivity

Cisco.com



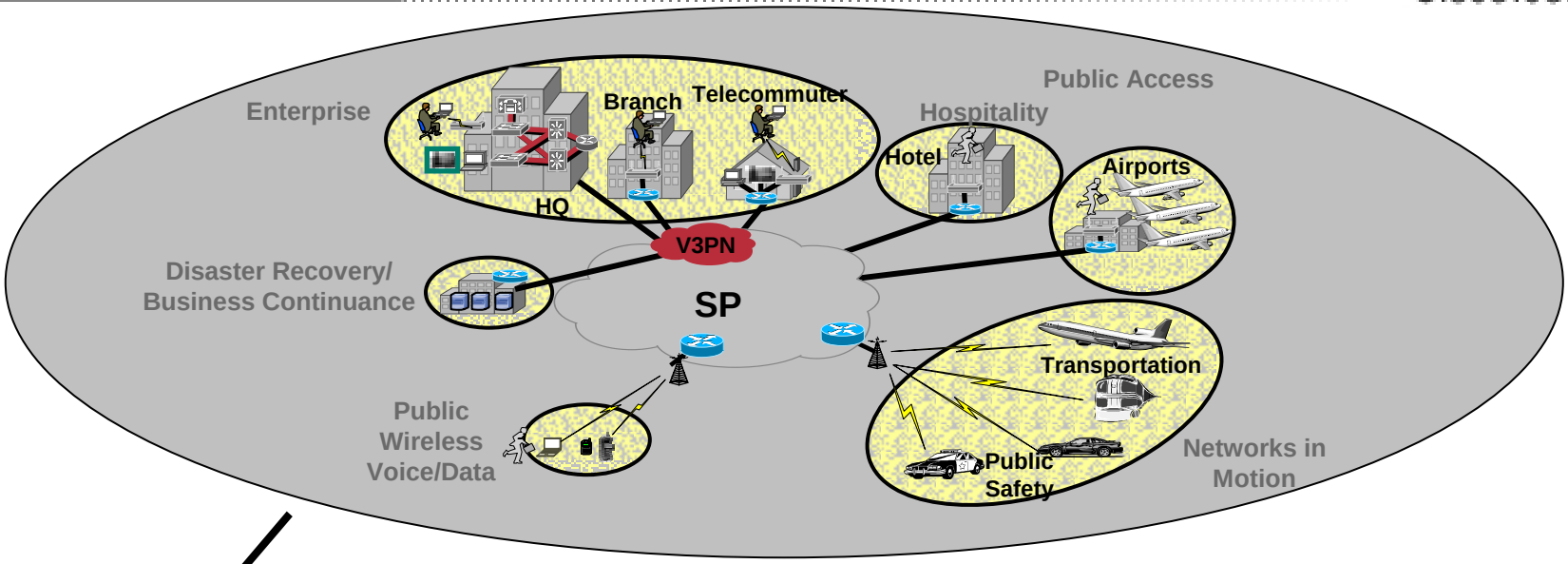
Agenda

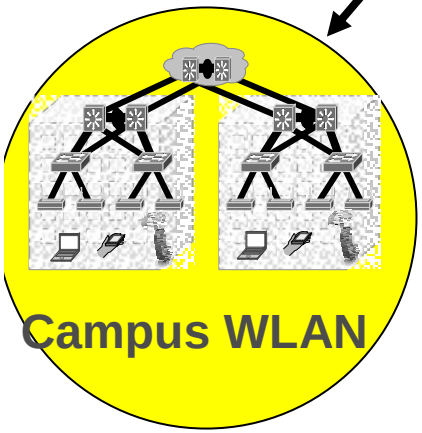
- **Cisco Enterprise Mobility Direction**
- **Mobility Solutions Technical Overview**
- **Jon Coxworth – Intel – Centrino Technology**
- **Shawn Winter –Bell - AccessZone**

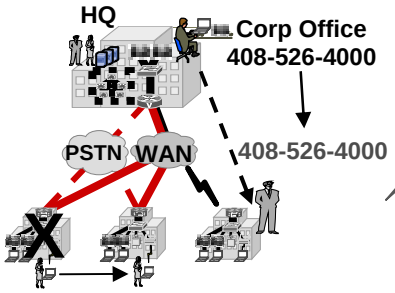
Cisco Enterprise Mobility Solutions

Campus WLAN Mobility

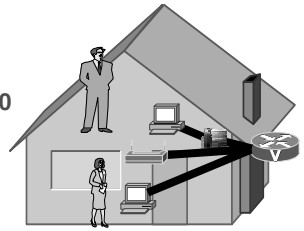
Cisco.com



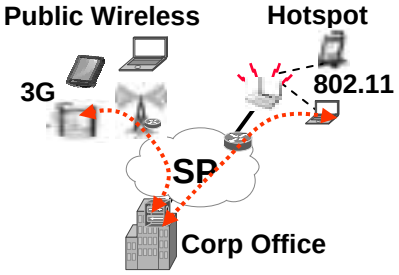




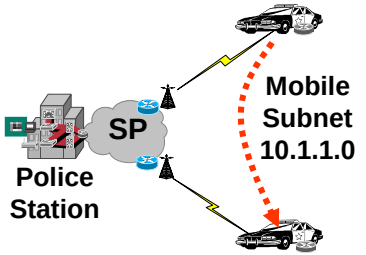
Branch Mobility



Teleworker



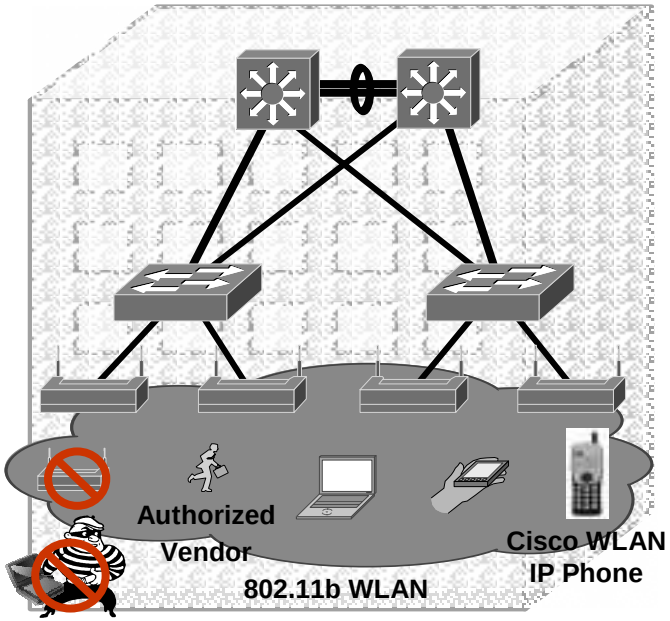
Users on the Move



Networks on The Move

Campus WLAN Mobility

Solution Overview



Solution Timeline

Today

Phase 1	Phase 2	Phase 3
LEAP + 802.1x Security	Rogue AP/QoS/VLANs Standard PEAP Security	WLAN IP Phone (CY Q2 '03)

Featured Elements

- **Large % of customers have insecure Rogue AP deployments today**
  - *Rogue AP prevention and detection with 802.1x*
  - *Properly Secured deployment enables Enterprise class WLAN*
- **Segmentation of Authorized users and prevention of Un-Authorized users**
  - *User based Access Policies with 802.1x*
  - *Authorized Guest/Vendor VLAN Access*
- **Lower Productivity when not at desk**
  - *WLAN Access to Business Apps*
  - *Cisco WLAN IP Telephony with QoS and Campus Roaming*

Wireless LAN Technologies

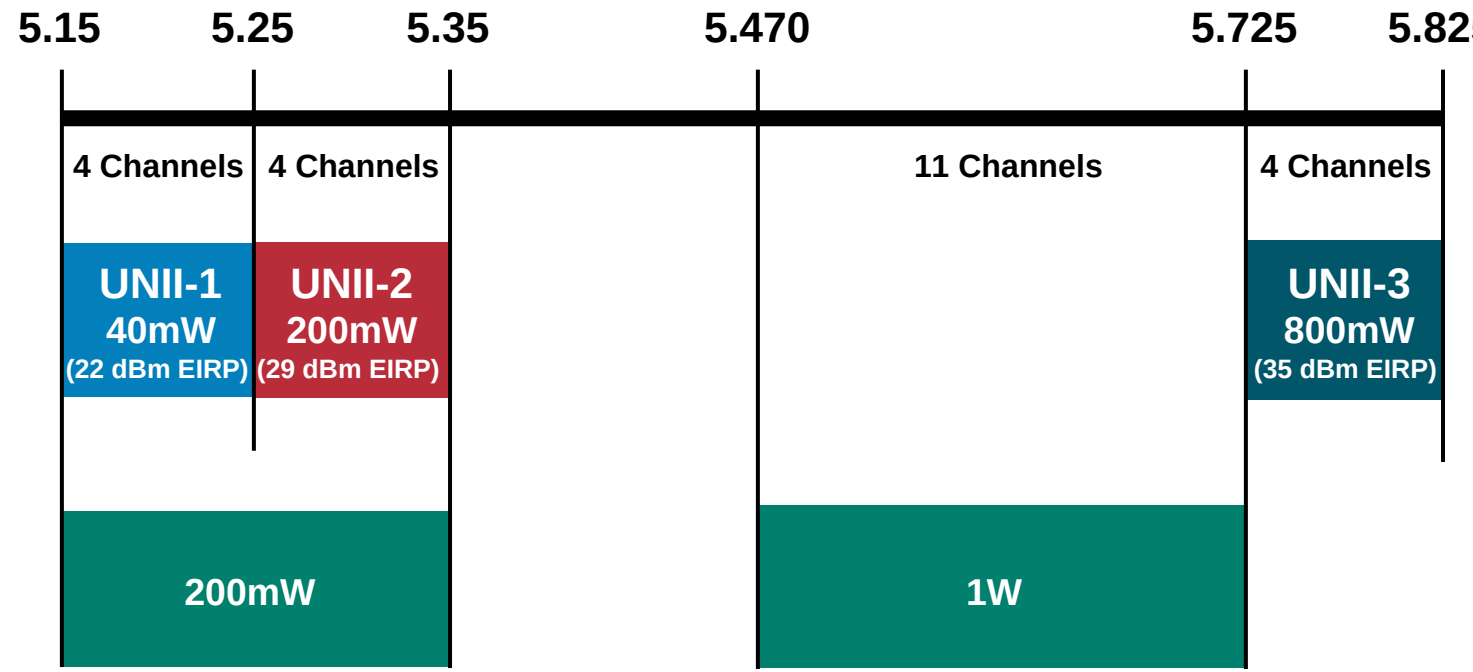
	802.11b	802.11g	802.11a
Freq. Band	2.4 GHz	2.4 GHz	5 GHz
Data Rate	1-11 Mbps (now)	<54 Mbps (mid '03)	6-54 Mbps (now)
# non-overlapping channels	3	3	8
Wi-Fi	Yes	Anticipated	Yes

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

Understanding the 5 GHz Spectrum

5 GHz UNII Band



US (FCC)
12 Channels
(*can use up to 6dBi gain antenna)

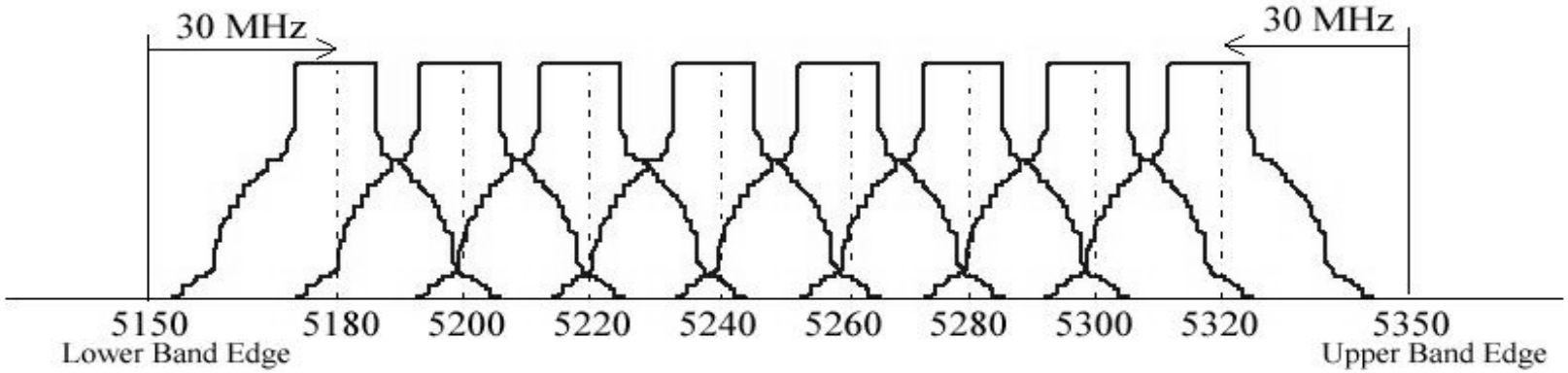
Europe
19 Channels
(*assumes no antenna gain)

UNII-1: Indoor Use, antenna must be fixed to the radio
UNII-2: Indoor/Outdoor Use, fixed or remote antenna
UNII-3: Outdoor Bridging Only (EIRP limit is 52 dBm if PtP)

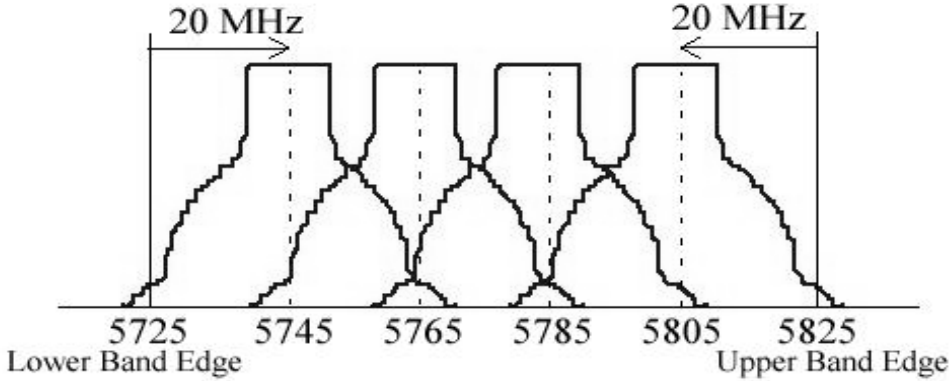
if you use a higher gain antenna, you must reduce the transmit power accordingly

802.11a UNII-1 & UNII-2 ISM Channels

Lower and Middle U-NII Bands: 8 Carriers in 200 MHz / 20 MHz Spacing



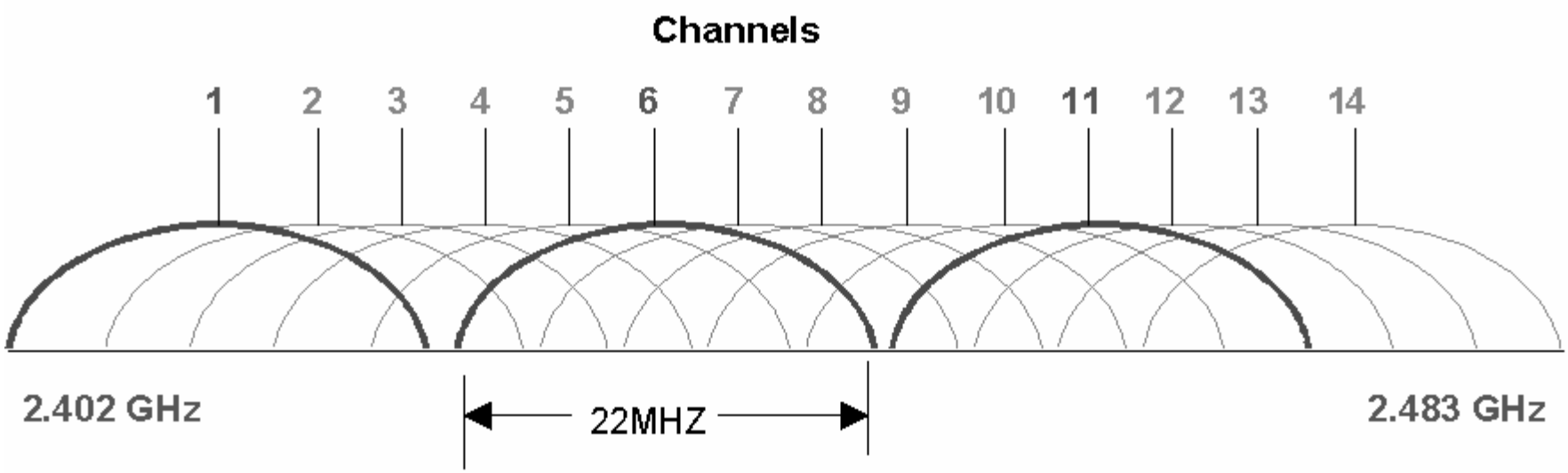
Upper U-NII Bands: 4 Carriers in 100 MHz / 20 MHz Spacing



802.11a

- **Data rates supported: 54, 48, 36, 24, 12, and 6 Mbps**
  - **Client will automatically "downshift" to lower data rate when it gets further from AP**
- **15 Countries have approved the use of today's 802.11a products:**
  - **U.S. Australia Poland Denmark France Sweden New Zealand Ireland**
  - **U.K. Germany Japan Singapore Canada Belgium Netherlands**
- **802.11h will ultimately permit worldwide usage of WLAN's @ 5 GHz**
  - **Transmit Power Control (TPC)**
  - **Dynamic Frequency Selection (DFS)**
- **5 GHz band has more channels than 2.4 GHz band**
  - **UNII-1 + UNII-2 = 8 channels (vs. 3 channels for 2.4 GHz)**
  - **However, depending on distance between APs, you may only be able to use half of the 5 GHz channels due to adjacent channel interference**
- **5 GHz band subject to less interference than 2.4 GHz band**
  - **However, 2.4 GHz interference not a major problem in most business environments**

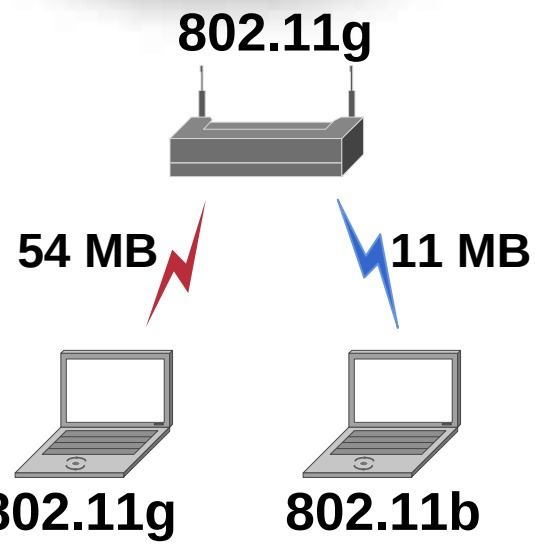
802.11b/g Channel Usage
Comparing WLAN Technologies



- **(14) 22 MHz wide channels (11 under FCC/ISTC)**
- **3 non-overlapping channels (1, 6,11)**

What Is IEEE802.11g

- **Provides higher data rates @ 2.4 GHz**
- **54 Mbps (same as 802.11a)**
- **Backward compatible 802.11b**
- **Same modulation as 802.11a—OFDM**
- **Should be ratified towards the end of CY03**



WLAN Security Hierarchy

Open Access

No Encryption,
Basic Authentication

Public "Hotspots"

Basic Security

40-bit or 128-bit
Static WEP Encryption

Home Use

Enhanced Security

802.1x,
TKIP Encryption,
Mutual Authentication,
Scalable Key Mgmt., etc.

Enterprise

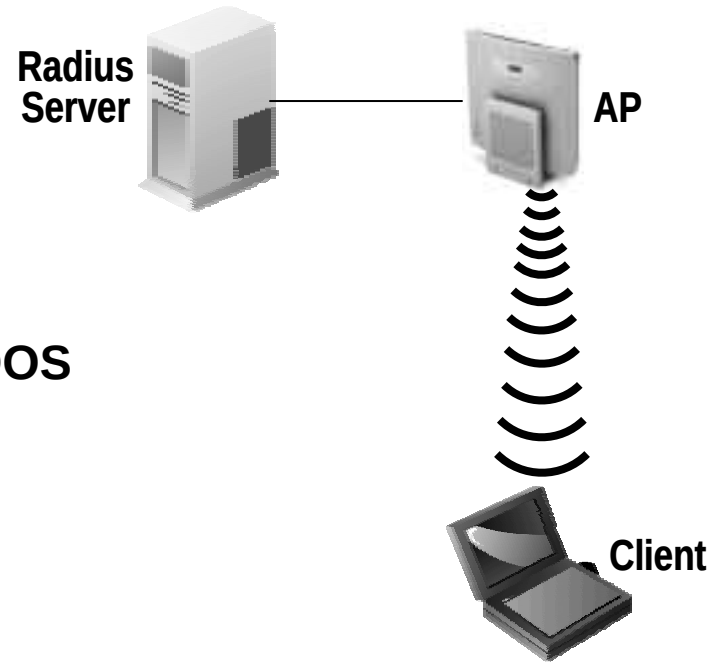
Remote Access

Virtual Private Network (VPN)

Business Traveler, Telecommuter

WLAN Security: 802.1X Authentication

- **Mutual Authentication**
- **LEAP**
  - **“Lightweight” EAP**
  - **Nearly all major OS’s supported:**
    - **WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS**
- **EAP-TLS**
  - **EAP-Transport Layer Security**
  - **Mutual Authentication implementation**
- **PEAP**
  - **“Protected” EAP**
  - **Establishes secure tunnel (similar to VPN)**
  - **Supported by Cisco, Microsoft, & RSA**
  - **Option: One-Time Passwords (“OTP”)**



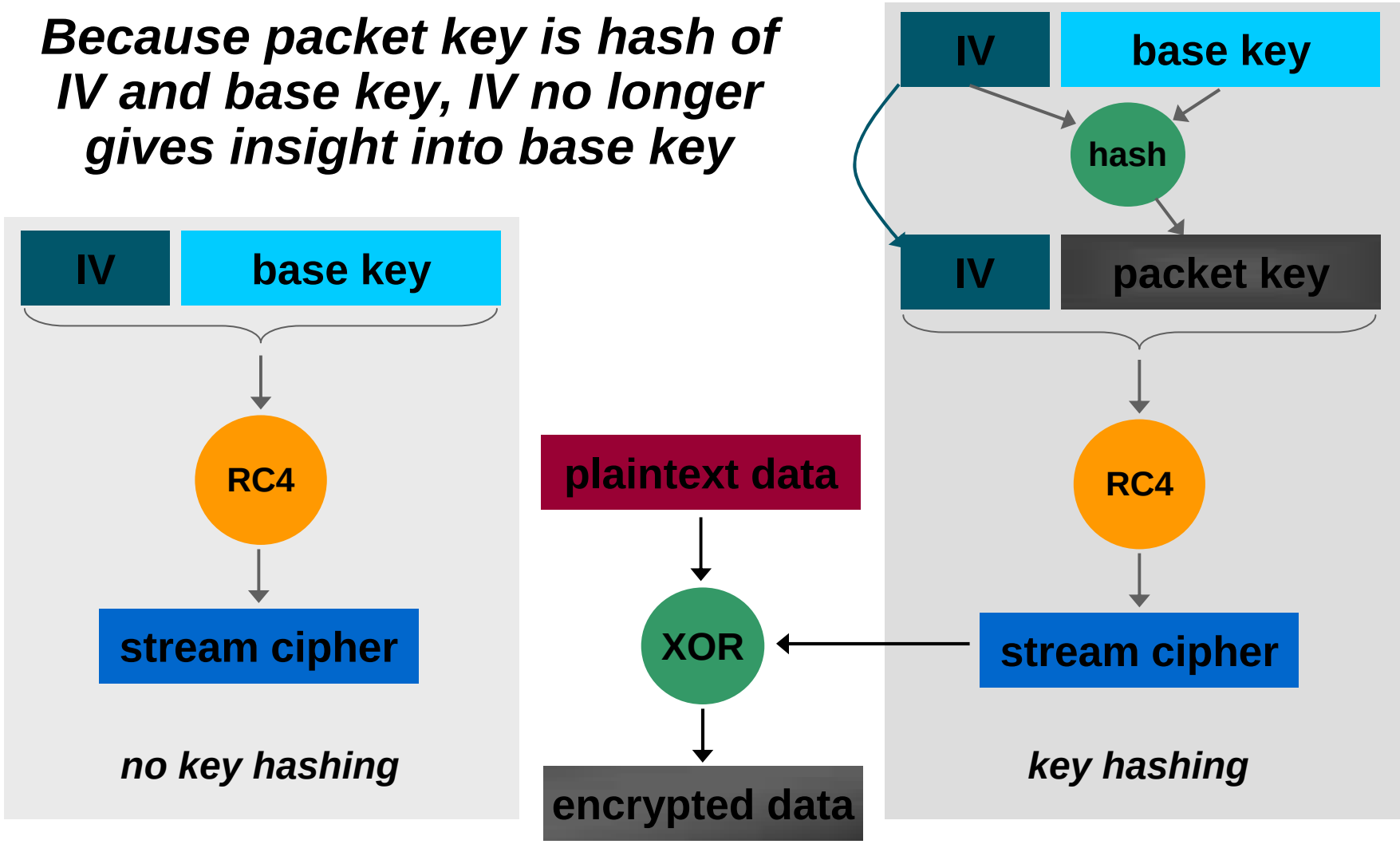
Cisco Systems

RSA SECURITY

Microsoft®

TKIP: Change Encryption Keys for Every Packet

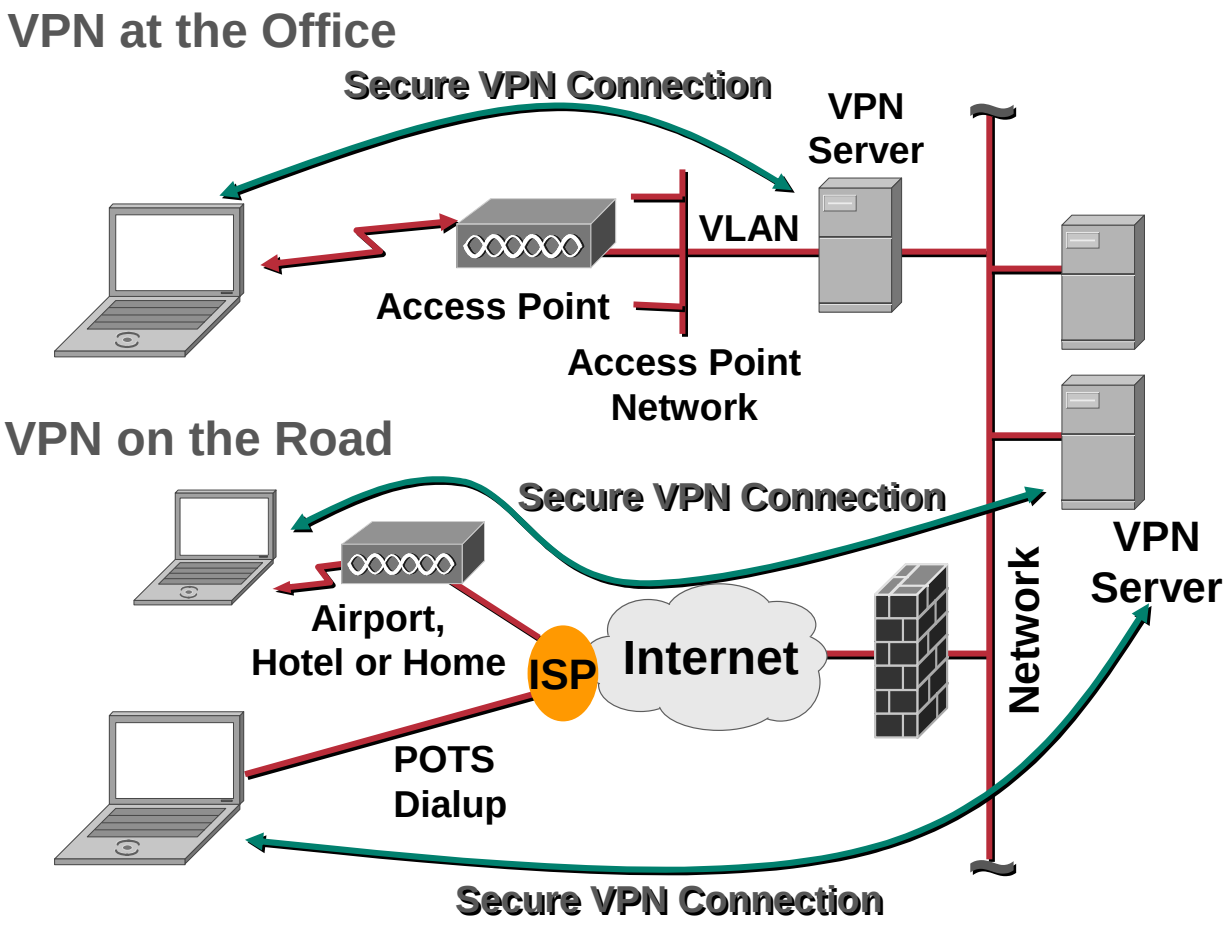
Because packet key is hash of IV and base key, IV no longer gives insight into base key



Wi-Fi Protected Access (WPA)

- **WPA is the biggest thing to happen to WLAN security since Cisco LEAP**
- **802.11i-standard TKIP + 802.1X authentication**
  - **There is a non-802.1X version of WPA for home use which is unsuitable for enterprises**
- **All new products after Aug.'03 MUST have WPA**
  - **Existing products are grandfathered**
- **Cisco has supported the base technologies of WPA longer than any other vendor**
- **Cisco will be implementing WPA across-the-board this summer '03**

Virtual Private Network



- Deployable today
- VPNs already in use in many IT organizations
- Scalable to large number of clients
- No key management issues
- Centrally managed
- Consistent user interface with remote access
- Re-initialize VPN connection when roaming

VPN Security for WLANs

Remote Access

Dialing into Corporate Network from Home, Hotel, Airport, etc.

VPN is the Best Solution!

On-Campus Access

Accessing Corporate Network while inside the Enterprise

?

VPN may not be the Best Answer

VPN/WLAN On Campus – Pros

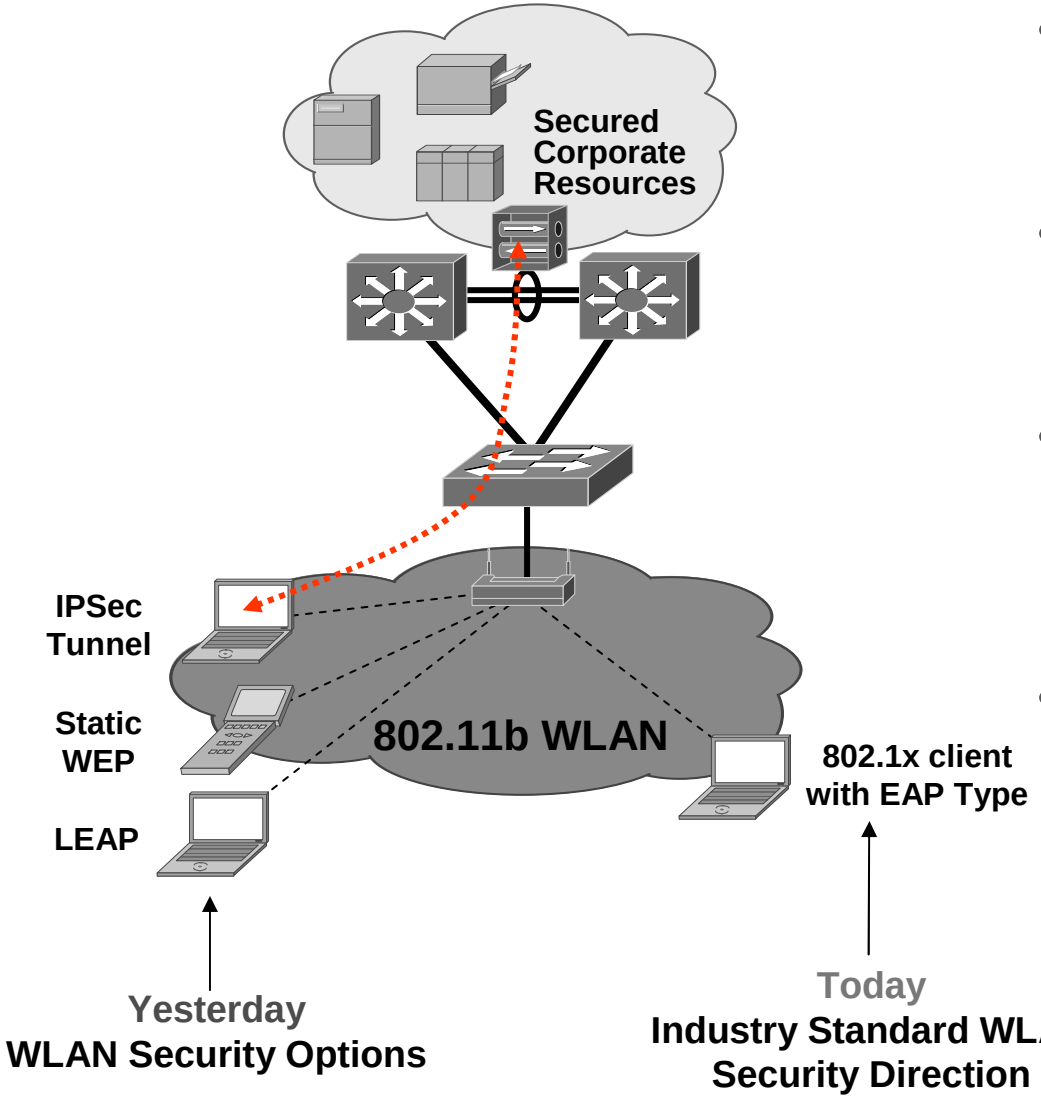
- **Familiar**
  - Is in use at most enterprises
  - Makes user interface consistent for both WLAN & remote access
- **Trusted for authentication & privacy**
  - Supports central security management
  - Ensures 3DES encryption from client to concentrator
- **Compatible with wide range of client devices from multiple vendors**

VPN/WLAN On Campus – Cons

- **Cost:** Requires VPN concentrators behind APs
- **Performance:** Client software encryption lowers throughput
- **Roaming:** Roaming between VPN concentrators forces application restarts
- **QoS:** All traffic is IPSec traffic; no QoS, multicast, or multiprotocol support
- **Client Devices:** Not supported on phones, scanners, or other specialized devices
- **Convenience:** Additional steps required beyond Windows logon

Campus WLAN Mobility

Secure WLAN Access



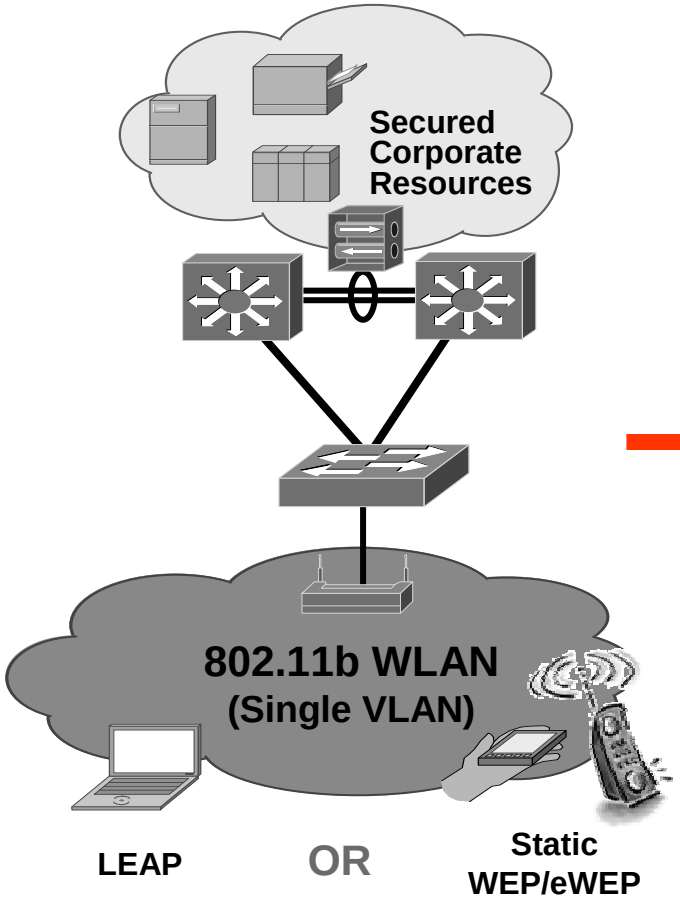
- **Several secure deployment options - LEAP, IPSec VPN with Auto Initiation, and eWEP**
- **802.1x with PEAP provides industry standard future direction for WLAN Security**
- **VLAN support in AP's provide co-existence/migration from current installed based security models to PEAP/802.1x**
- **Provides security equal to that of wired Ethernet (higher if customer is not using 802.1x on wired Ethernet)**

Campus WLAN Mobility

Multiple AP VLAN Support – Co-existence and Migration

Yesterday

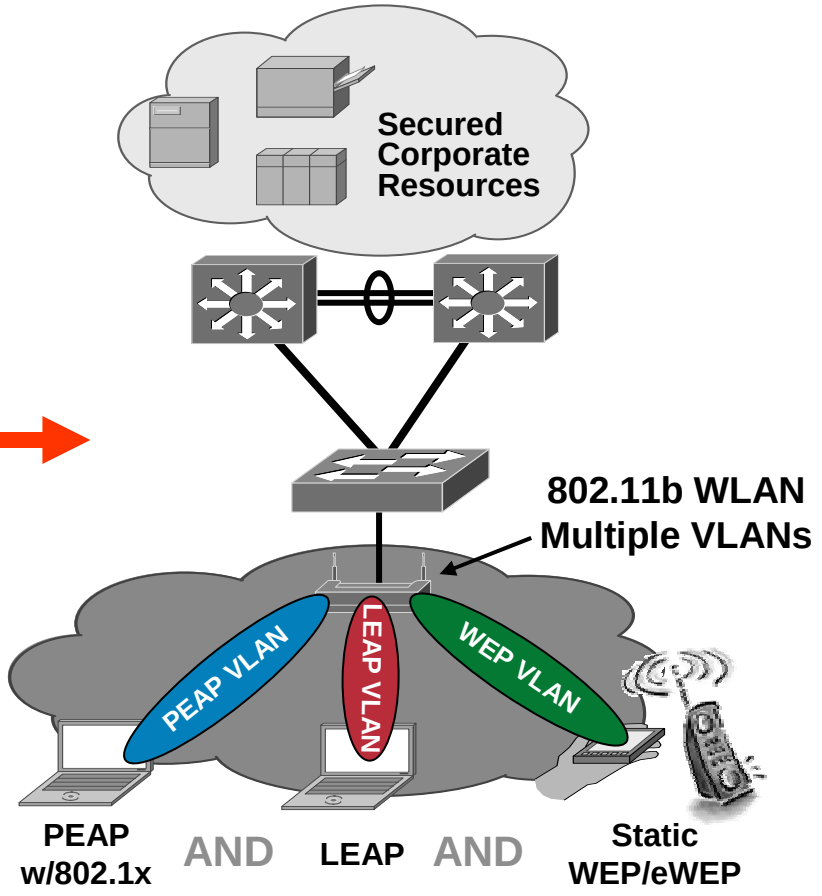
One VLAN - One Security Model at a time per AP



Note – VPN can use LEAP or WEP/eWEP

Today

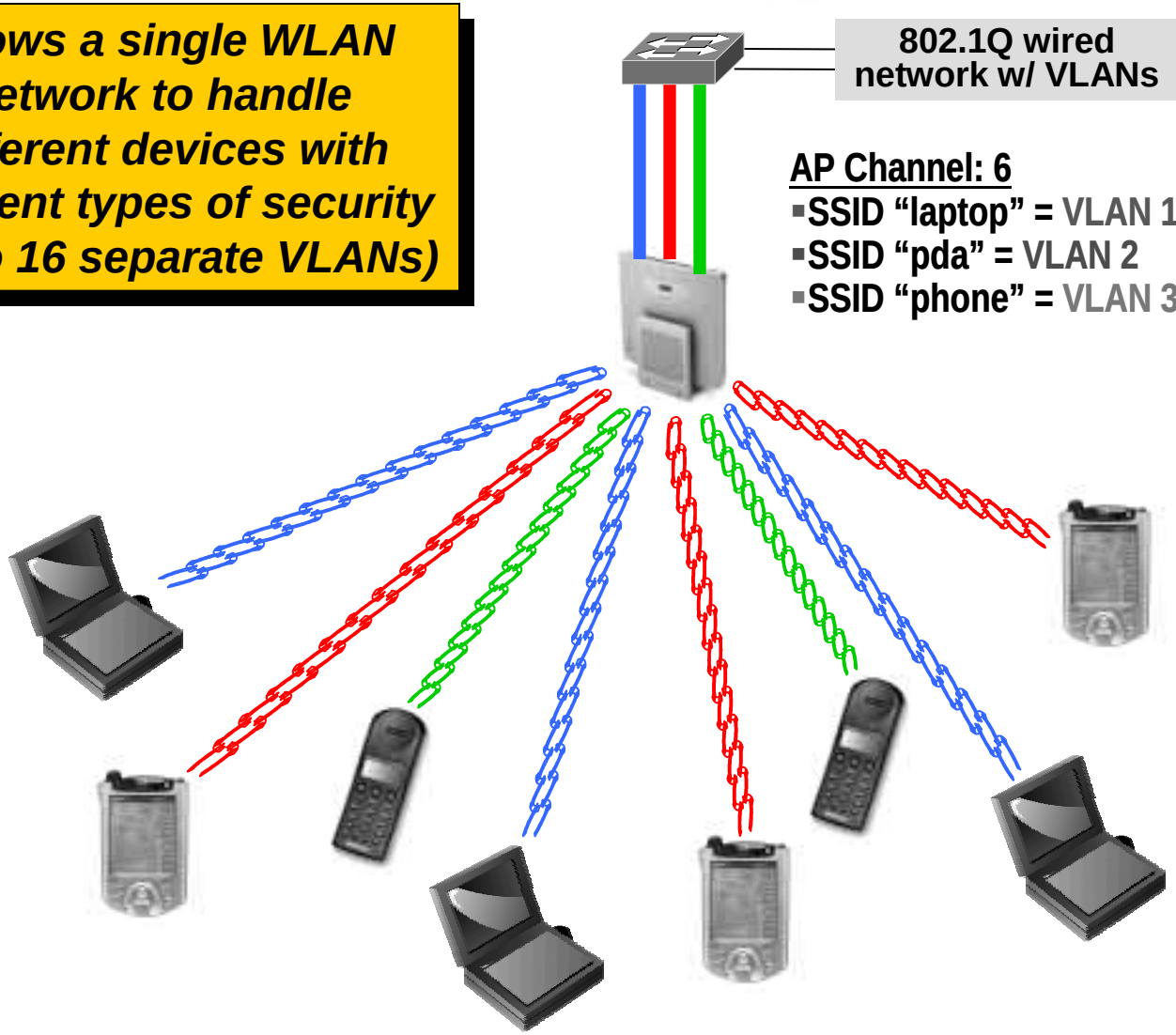
Extension of the Wired Ethernet Network

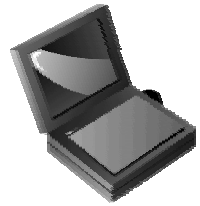


AP VLAN's facilitate Multiple WLAN Security Model co-existence and migration to PEAP w/802.1x

Client Differentiation with VLANs

Allows a single WLAN network to handle different devices with different types of security (up to 16 separate VLANs)





SSID: laptop
Security: PEAP + AES

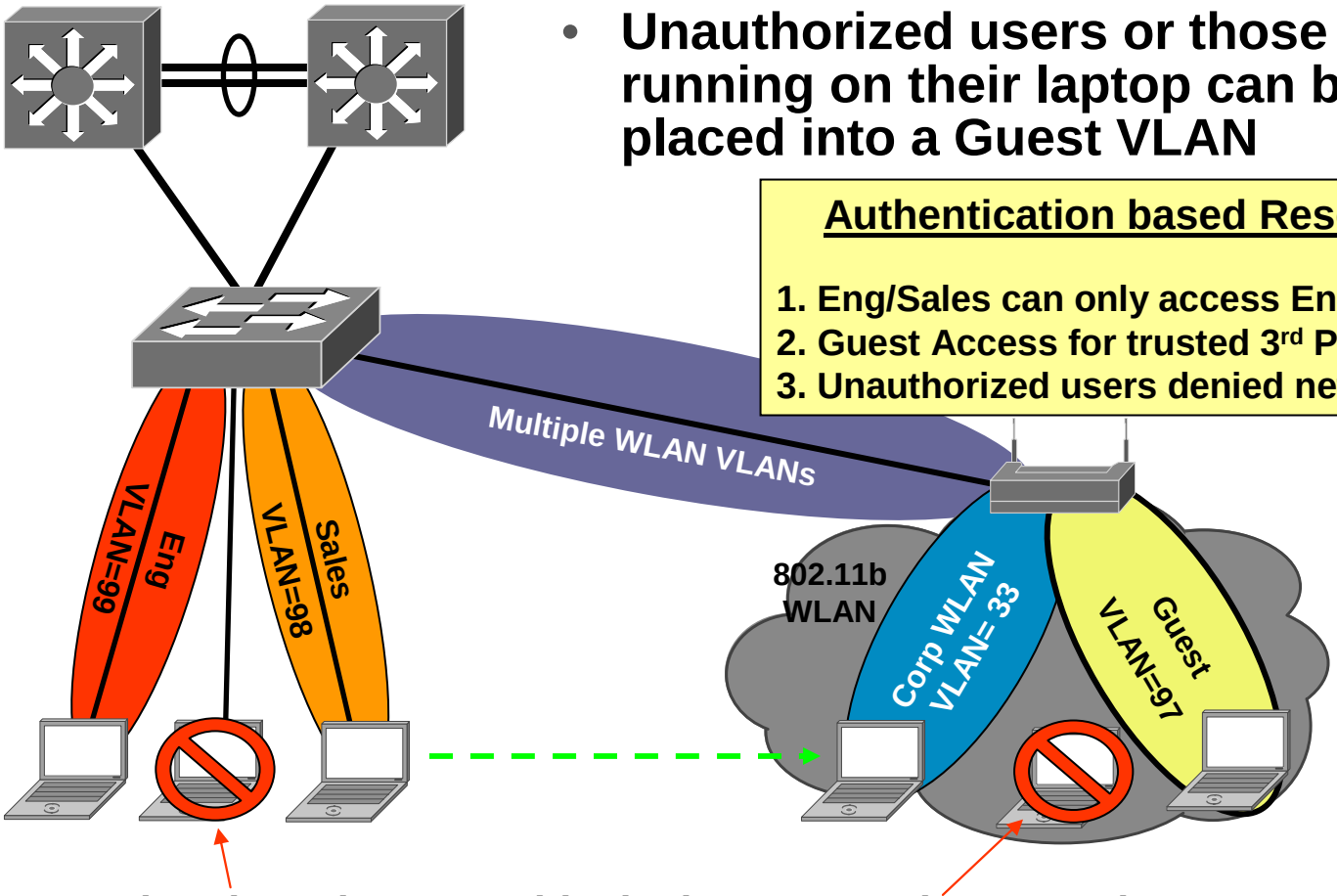
SSID: pda
Security: LEAP + TKIP

SSID: phone
Security: LEAP + WEP

Campus WLAN Mobility

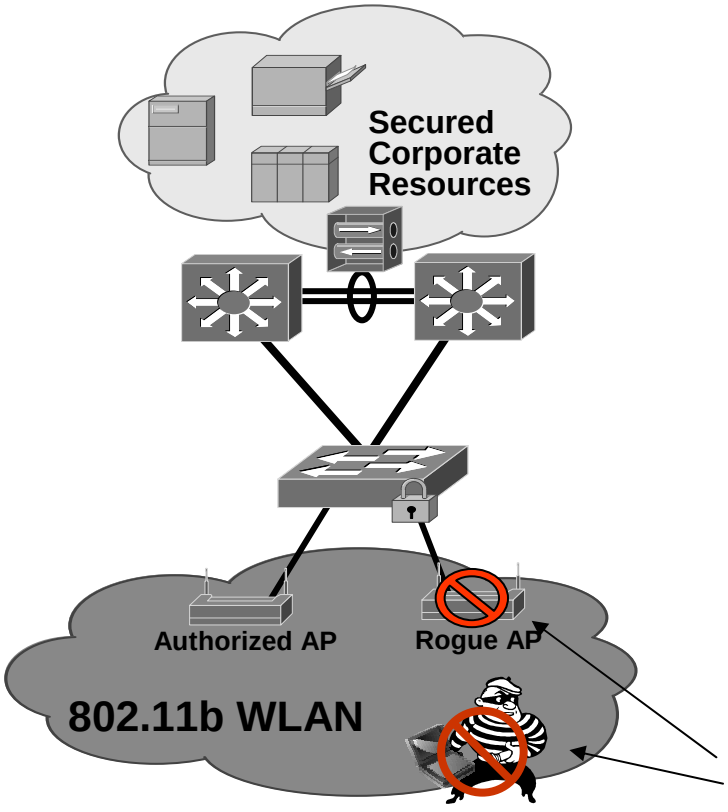
User based Network Access (User Identity)

- **Based upon user's credentials via 802.1x (User Identity)**
- **Unauthorized users or those without 802.1x running on their laptop can be denied or placed into a Guest VLAN**



Campus WLAN Mobility

Rogue AP Detection and Mitigation



- ***Detecting Rogue APs*** **- Use of wireless analyzer to look for WLAN signals**

  Boingo, Netstumbler etc.

- ***Preventing Rogue APs*** **– 802.1x switched infrastructure**
- **Un-Authorized AP's are therefore locked out**

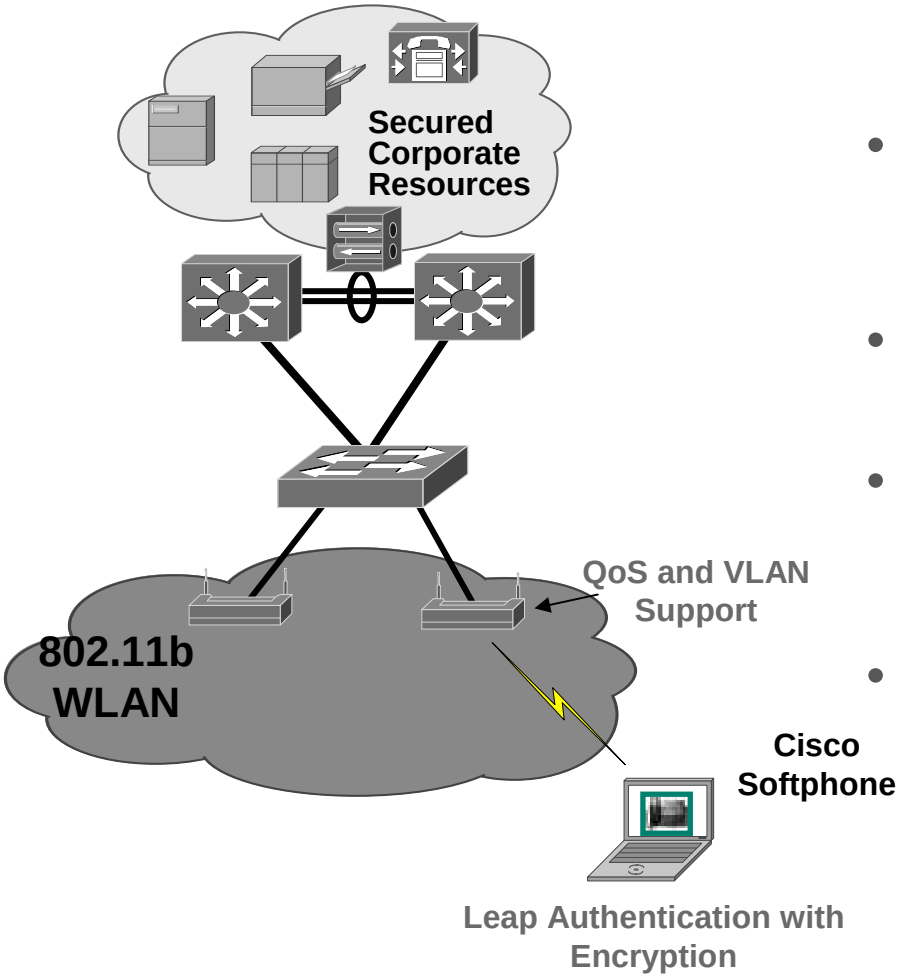
Enables IT to control WLAN activities and promotes sanctioned WLAN deployments – Inherently Reducing rogue WLAN activities

Rogue AP Prevention Summary/Strategy

- **Fact - You probably already have a WLAN deployment in your corporate network (whether you know it or not)**
- **An IT deployed and supported WLAN is the best way to prevent insiders from installing their own APs**
- **802.1x on switched infrastructure prevents *Rogue Devices***
  - **Effective against unauthorized access**
  - **Allows identity based policy on switch port**
- **Use a combination of scripts and wireless analyzers to regularly audit for rogue APs**

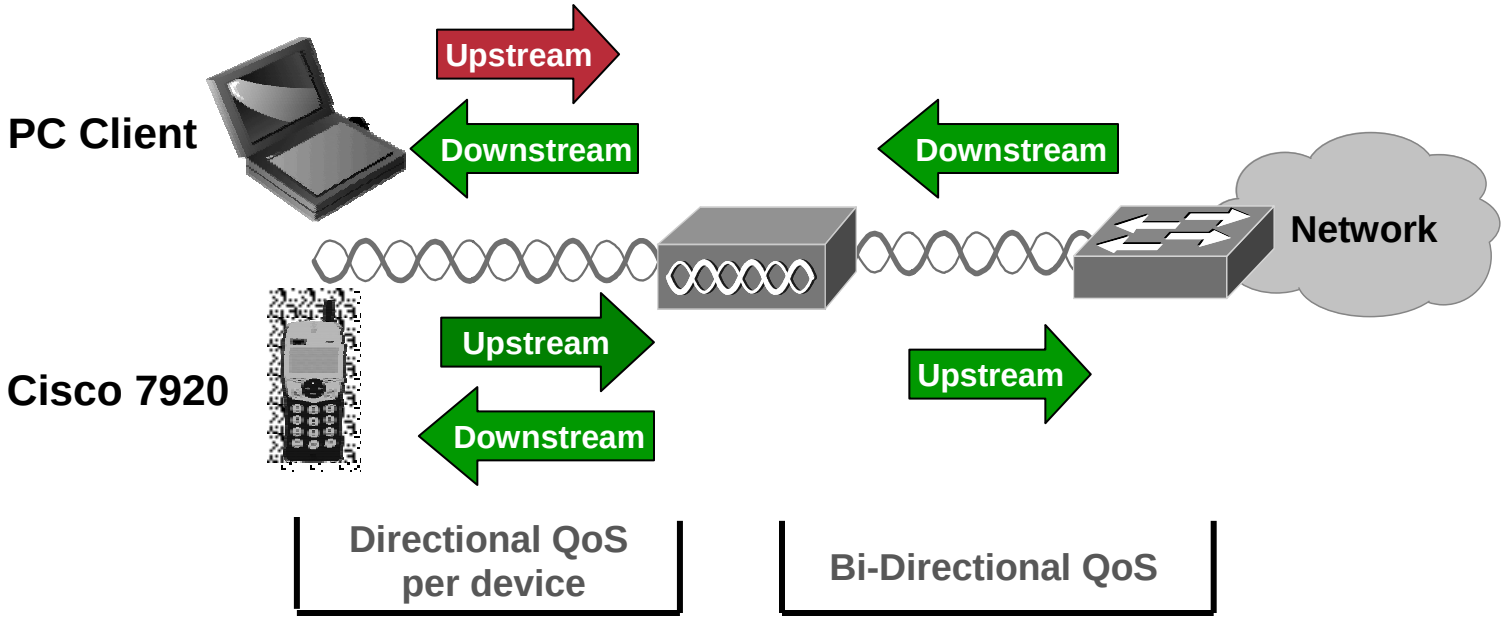
Campus WLAN Mobility

Cisco WLAN QoS



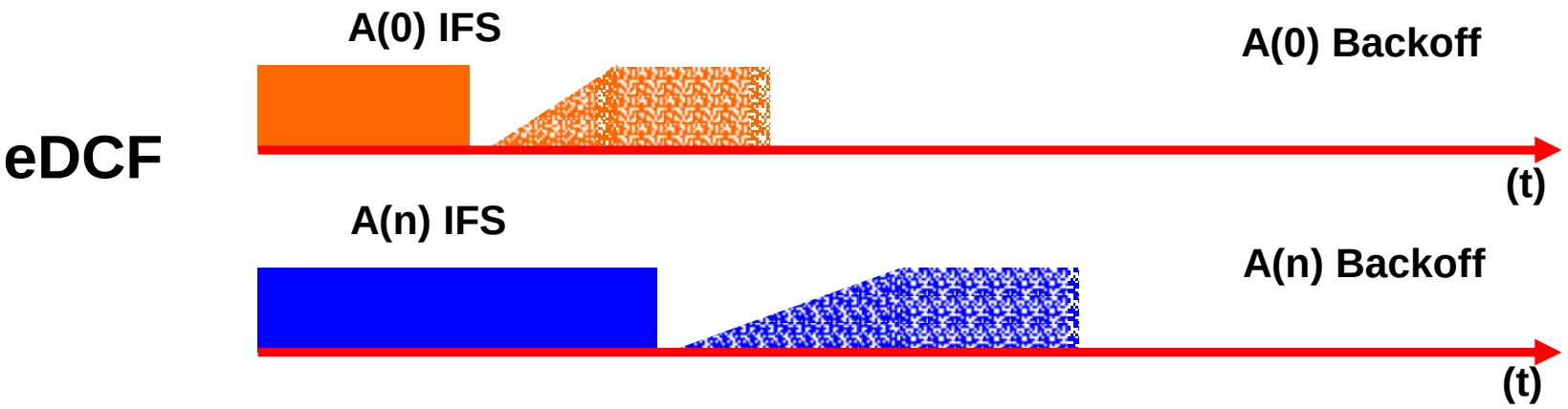
- **WLAN QoS that provides preferential treatment of higher priority traffic**
- **Cisco IP Telephony Endpoints such as the Cisco Softphone**
- **Latency sensitive applications that have the ability to classify higher priority traffic**
- **Only downstream QoS. With future 802.11e, QoS upstream and downstream**

WLAN QoS Challenges



- **WLAN QoS is based on a model of preferred access to the RF medium.**
- **QoS is statistical, not guaranteed.**

WLAN QoS



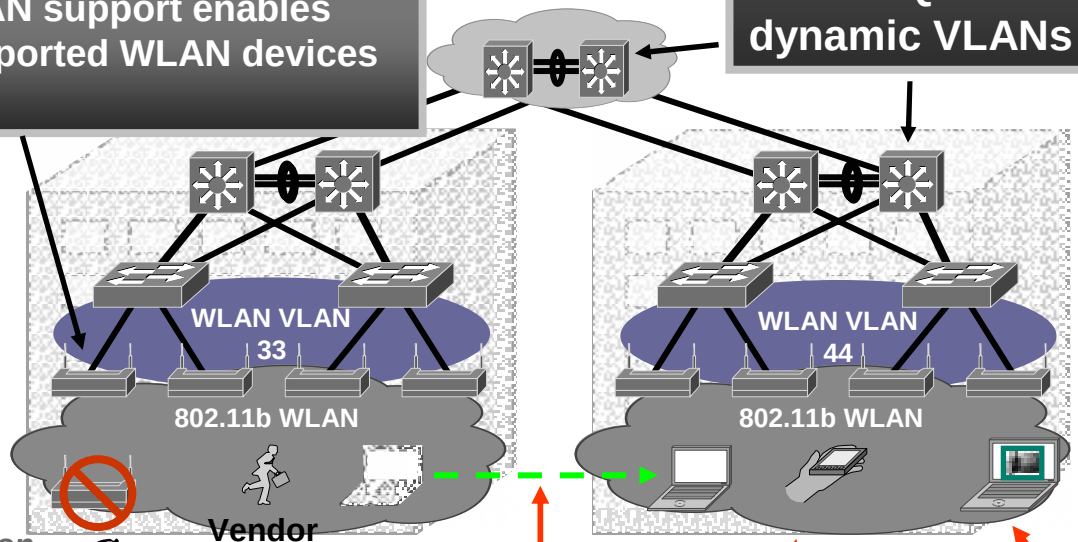
What is eDCF?

- Enhanced Distributed Coordination Function
- eDCF allows high priority traffic first access to the media by having a smaller random backoff timer

Cisco Delivers End-to-End, Secure QoS Enabled WLAN Network Solutions

Cisco Wireless Access Points
802.1x enabled to provide Secure QoS WLAN access; VLAN support enables wider range of supported WLAN devices and access types

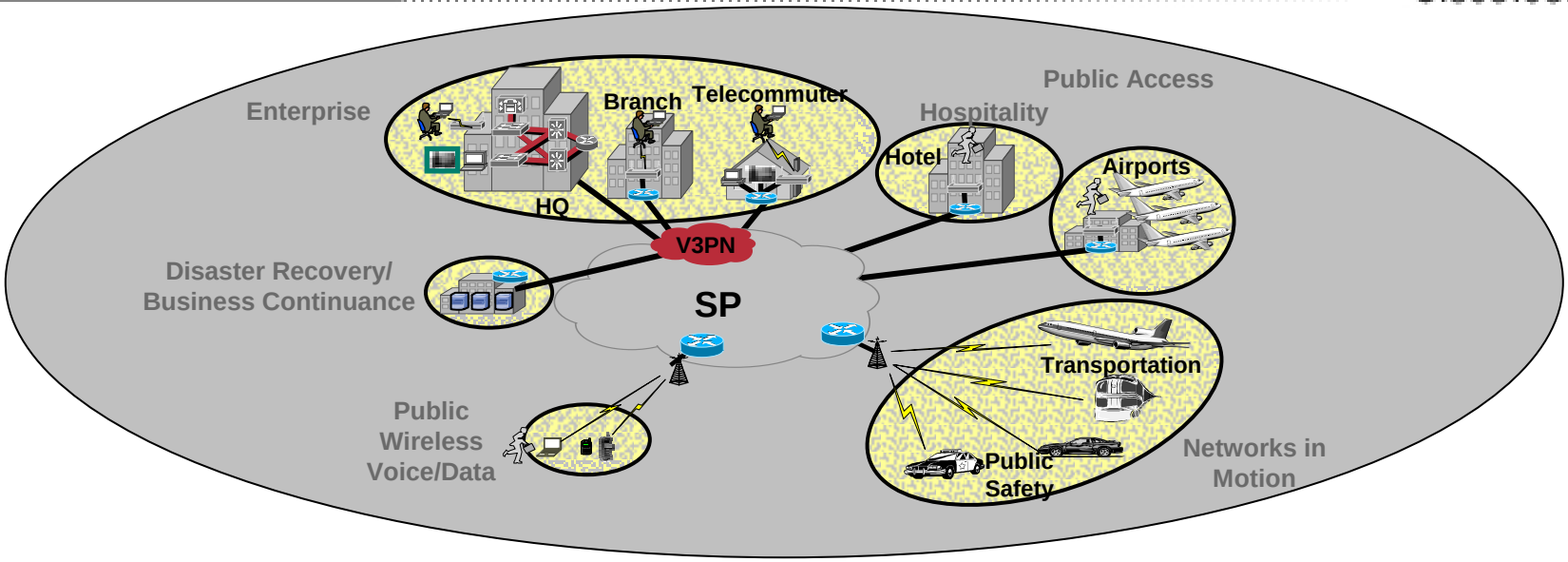
Cisco Catalyst Switches
Secure QoS enabled access; 802.1x, dynamic VLANs with AP's

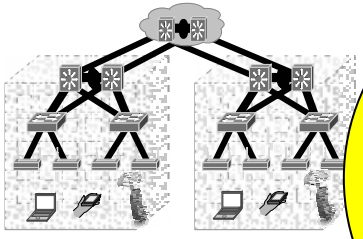


Network Management
Wireless LAN Solution Engine (WLSE) and Ciscoworks

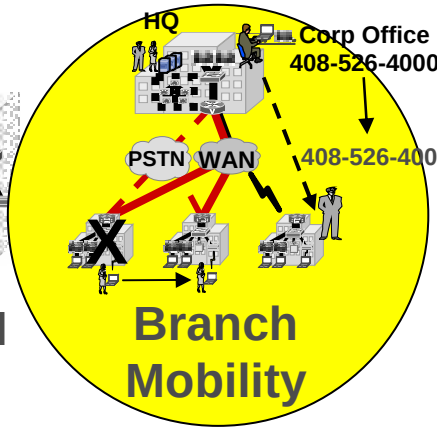
WLAN QoS AP Capability
Integrated QoS for latency sensitive applications

Enterprise Branch Mobility

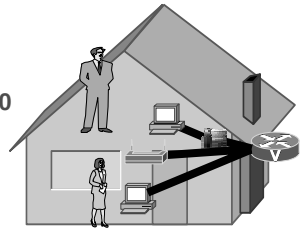




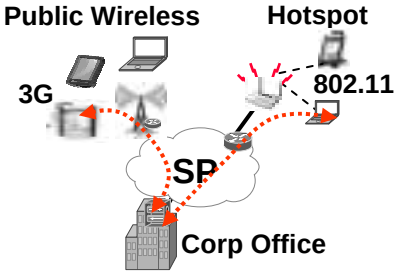
Campus WLAN



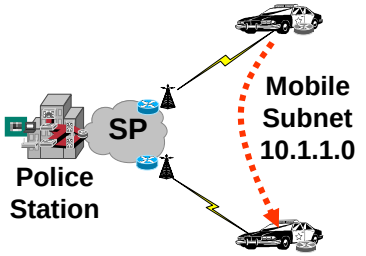
Branch Mobility



Teleworker

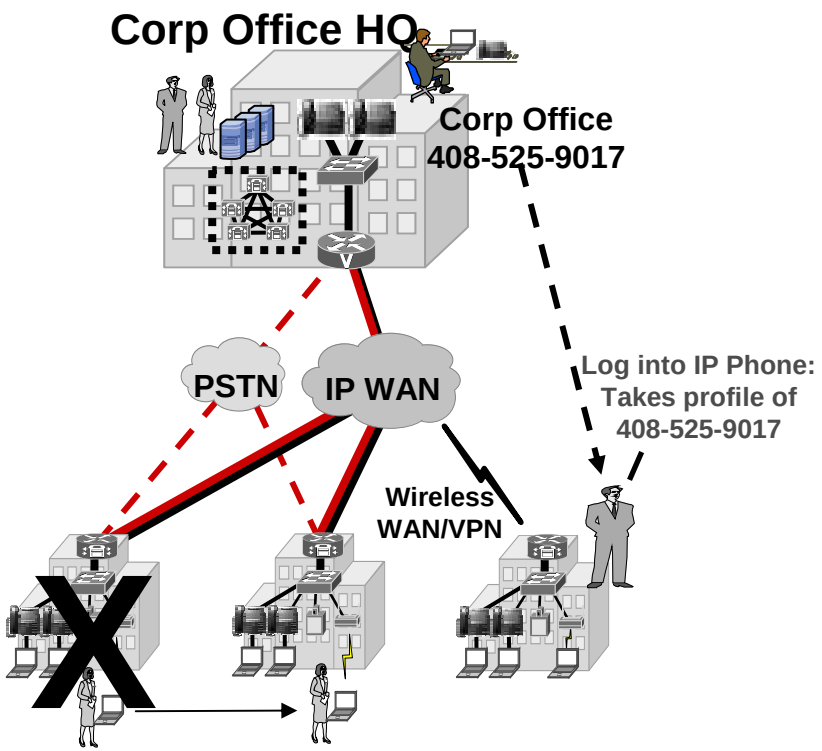


Users on the Move



Networks on The Move

Branch Mobility
Solution Overview



Solution Timeline

Today

Phase 1
Extension Mobility
IP Telephony

Phase 2
V3PN

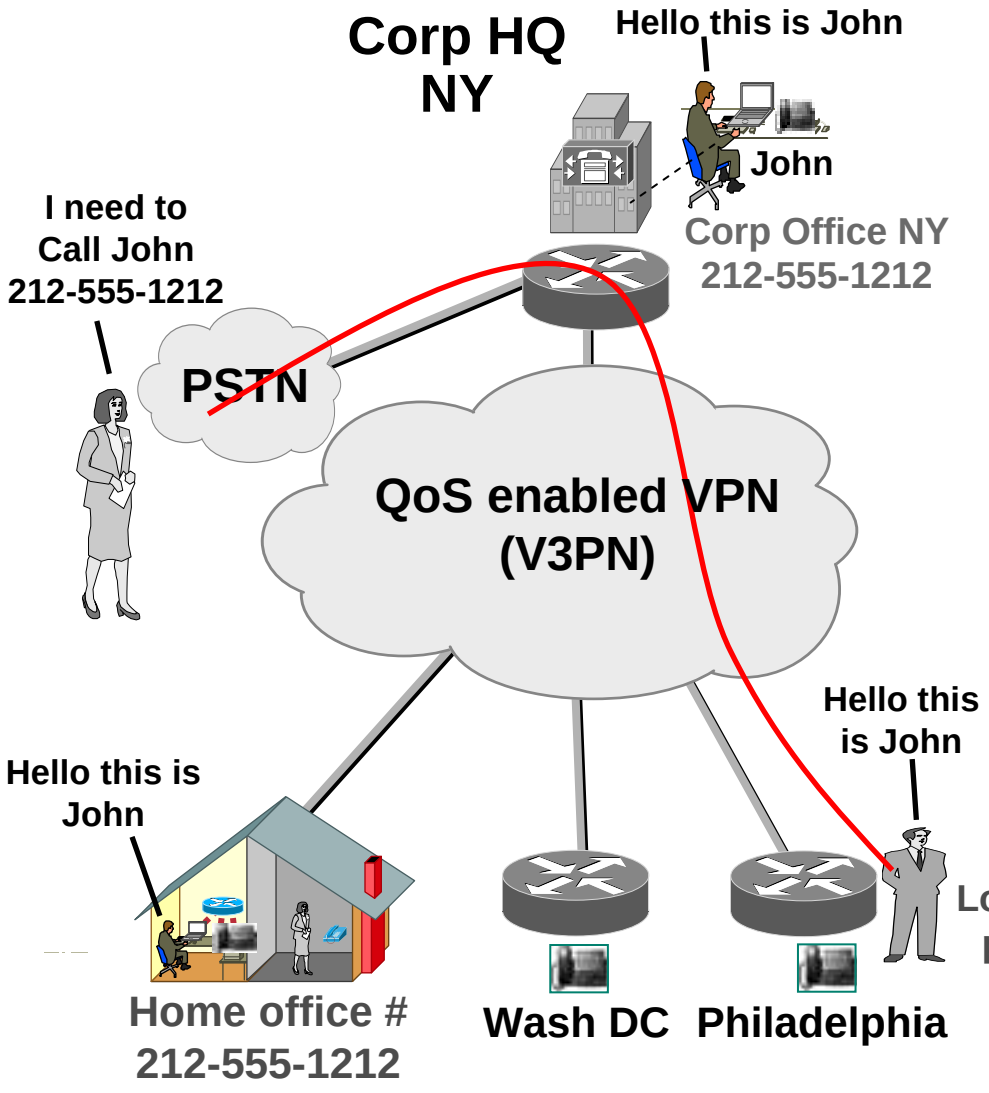
Phase 3
Pt to Pt Wireless
With QoS
(CY Q1 '03)

Featured Elements

- **Preparing for Business Resilience - Rapid Branch Deployment or Redeployment**
  - *Rapidly deployable WAN Alternatives such as VPN and Pt to Pt Wireless*
  - *WLAN enabled user PC's to minimize relocation time*
  - *IP Telephony - Allows for geographically diverse users, PSTN Gateways and Call Processing*
- **Enterprises continually striving to lower operating costs**
  - *Lower cost WAN Alternatives such as VPN and Pt to pt Wireless*
- **Employee productivity decreases when away from Corp office**
  - *IP Telephony - Extension Mobility to provide transparent Corp Office IP Phone Extension*
  - *Used during normal user Mobility or during unplanned displacement*

Combining IP Telephony and VPN

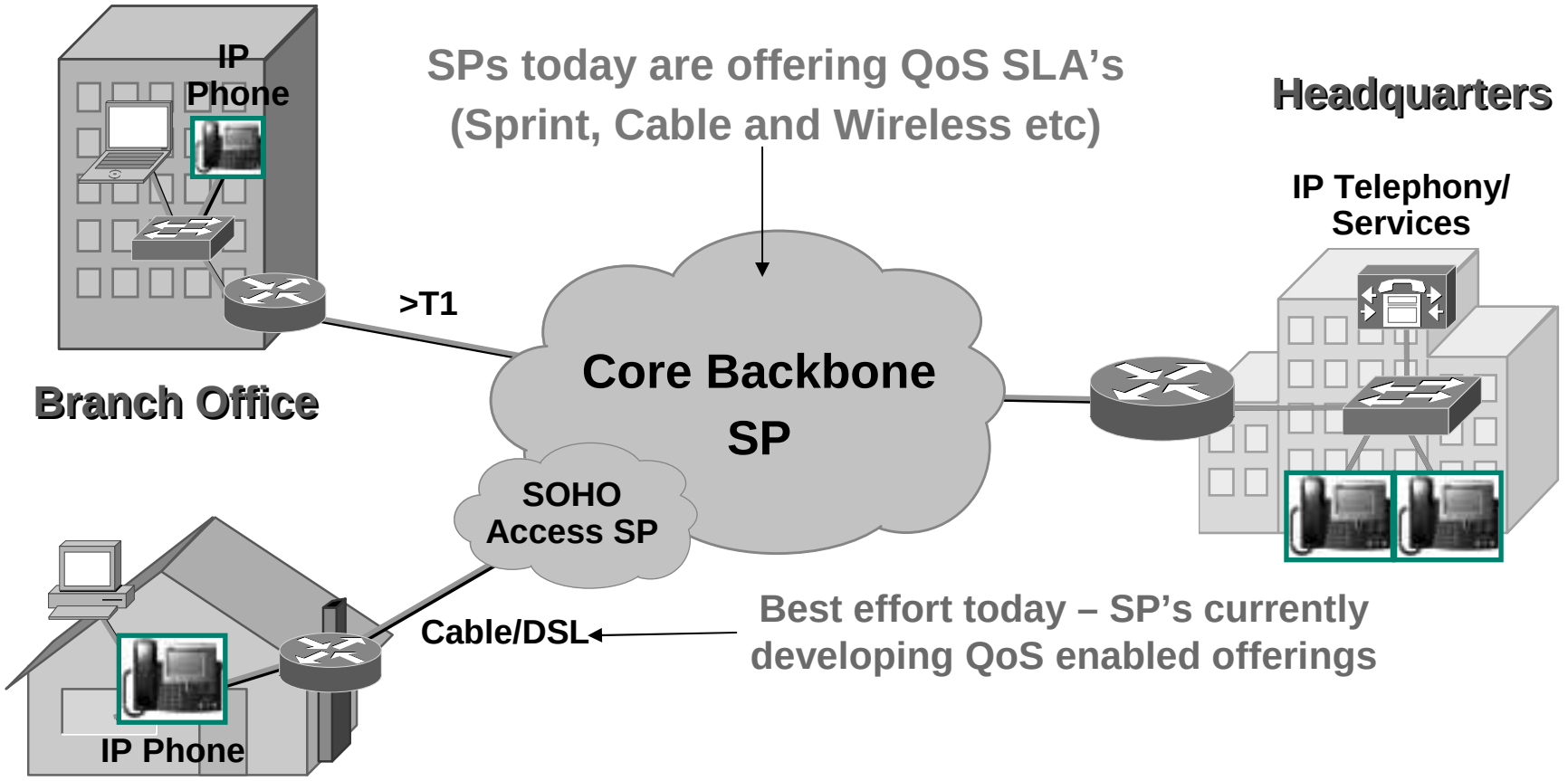
Voice and Video Enabled VPN – V^{3}PN



V3PN Solutions

- **Lowers WAN Cost and Increases Teleworker Productivity**
- **Cisco Powered Network (CPN) Service Provider Partners carry Voice/Video with Toll quality SLA's**
- **Same network connectivity in home as in Corp office (Voice, Video and data)**

V³PN Service Provider Partners



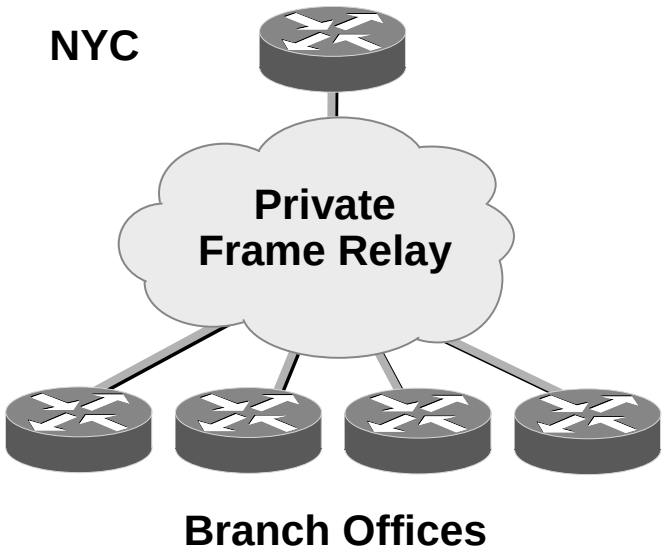
Cisco Powered Network SP Partners

http://www.cisco.com/pcgi-bin/cpn/cpn_pub_bassrch.pl

V³PN Business Justification

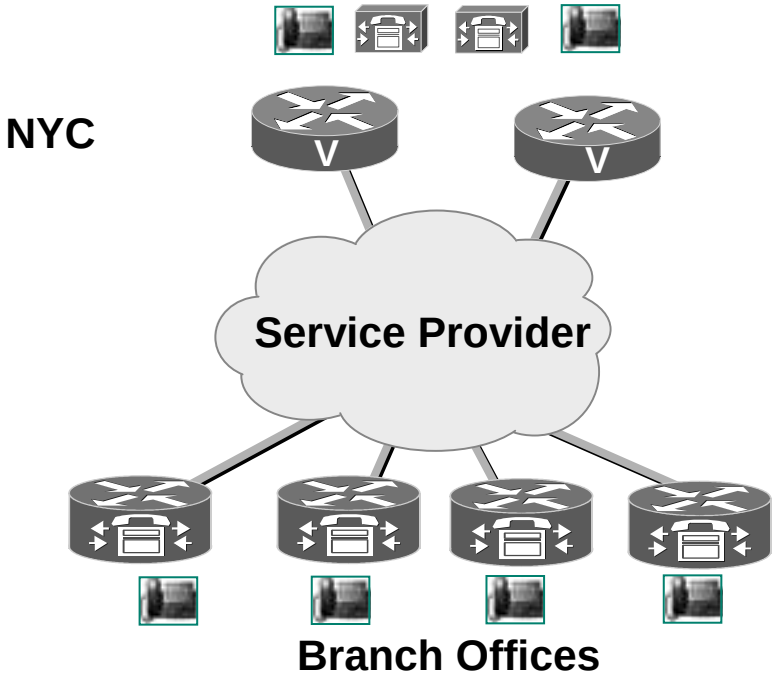
Lexent, Inc. (NYC) – NYC HQ w/20 remote offices

Alternative 1: Managed Frame Relay



- 20 sites – >$45,000 per month
- 3 year commit, >$1.5M total

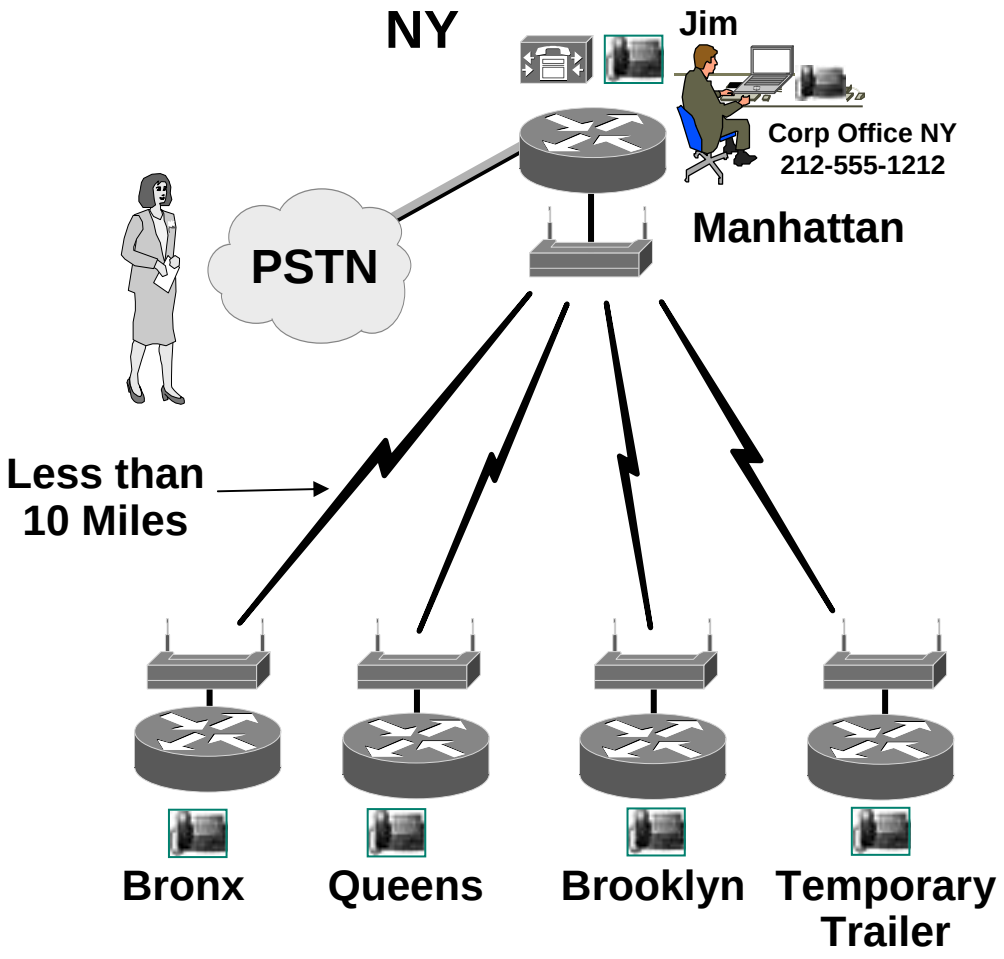
Alternative 2: Voice and Video enabled VPN



- 20 sites – <$20,000 per month
- 1 year commit, <$250K total

Branch Office Mobility

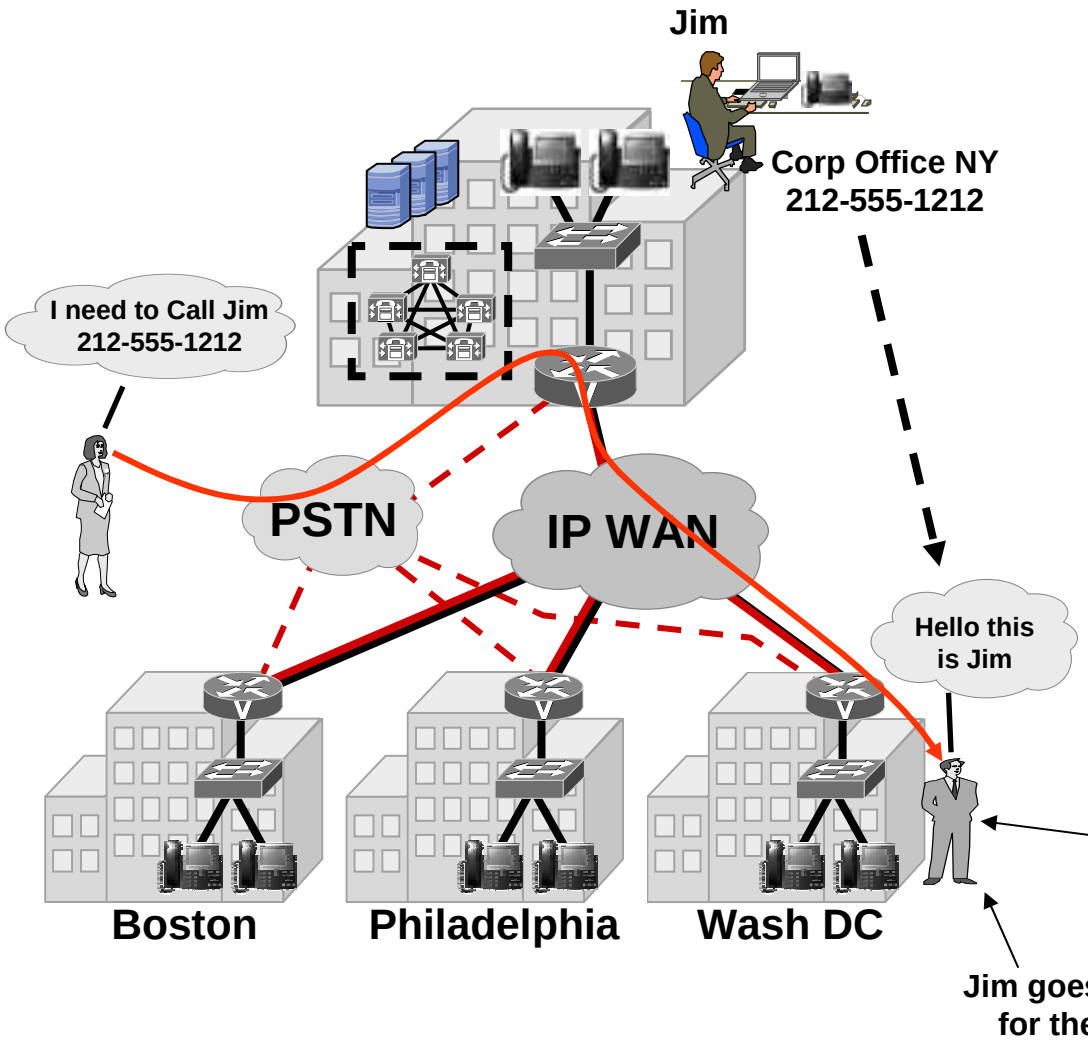
Pt to Pt Wireless



- **Allows for rapid office setup for permanent and temporary settings**
- **Saves on circuit cost for short haul distances**
- **QoS enabled IP Telephony and Video support option available**

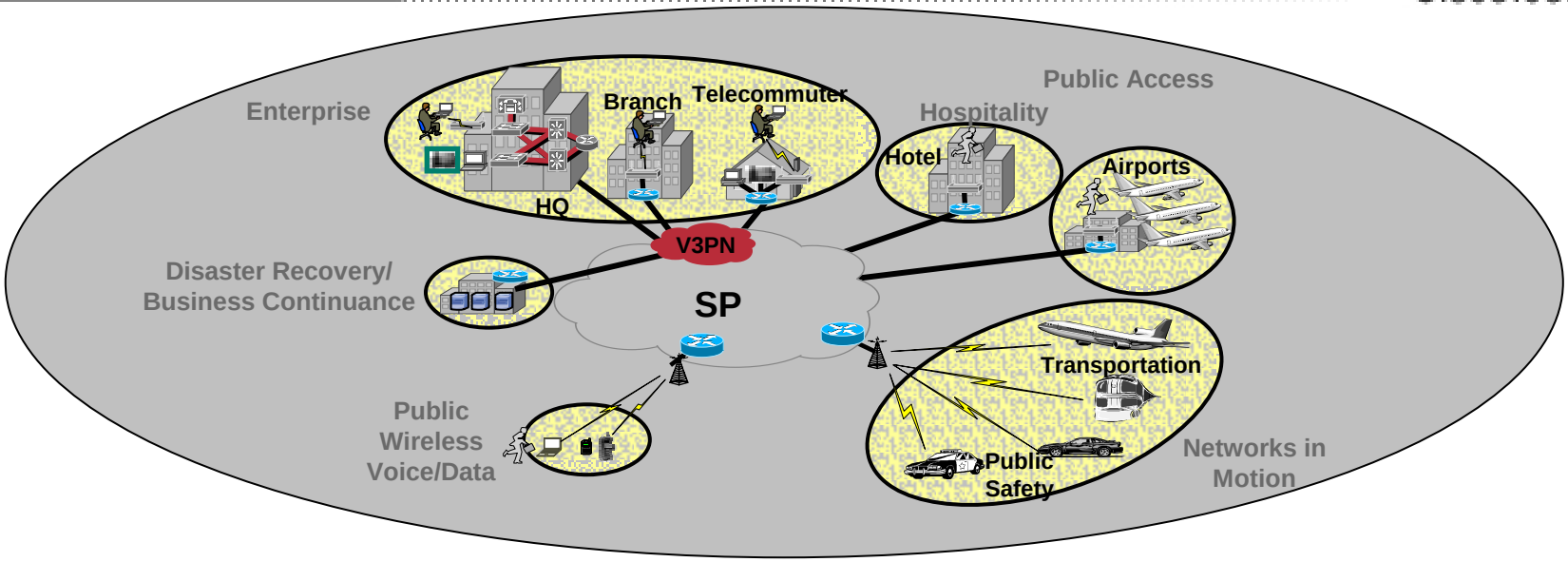
User Mobility

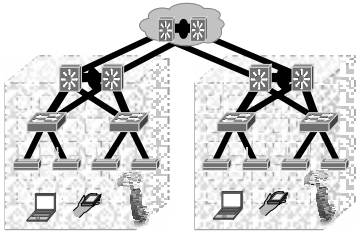
CallManager Extension Mobility



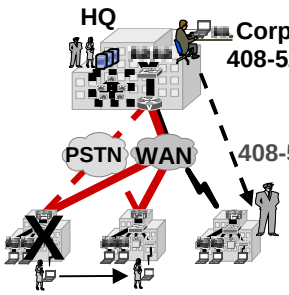
- **Supported with Centralized Call Processing**
  - **Allows users to log into remote IP Phone and have "home" profile follow them**
- **Supported with WLAN IP Phone**
  - **Need to ensure proper branch bandwidth to not exceed Call Admission Control bandwidth settings**

Enterprise Teleworker Mobility

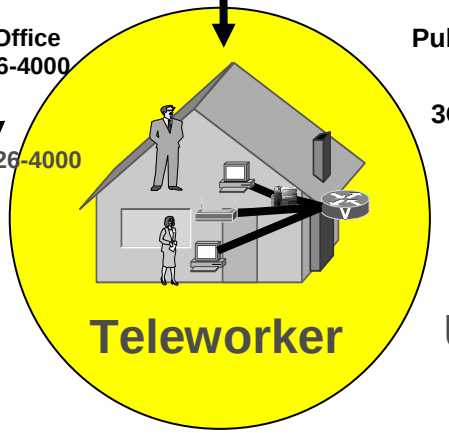




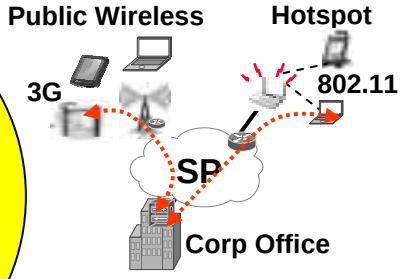
Campus WLAN



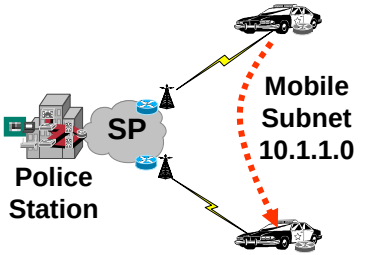
Branch Mobility



Teleworker



Users on the Move



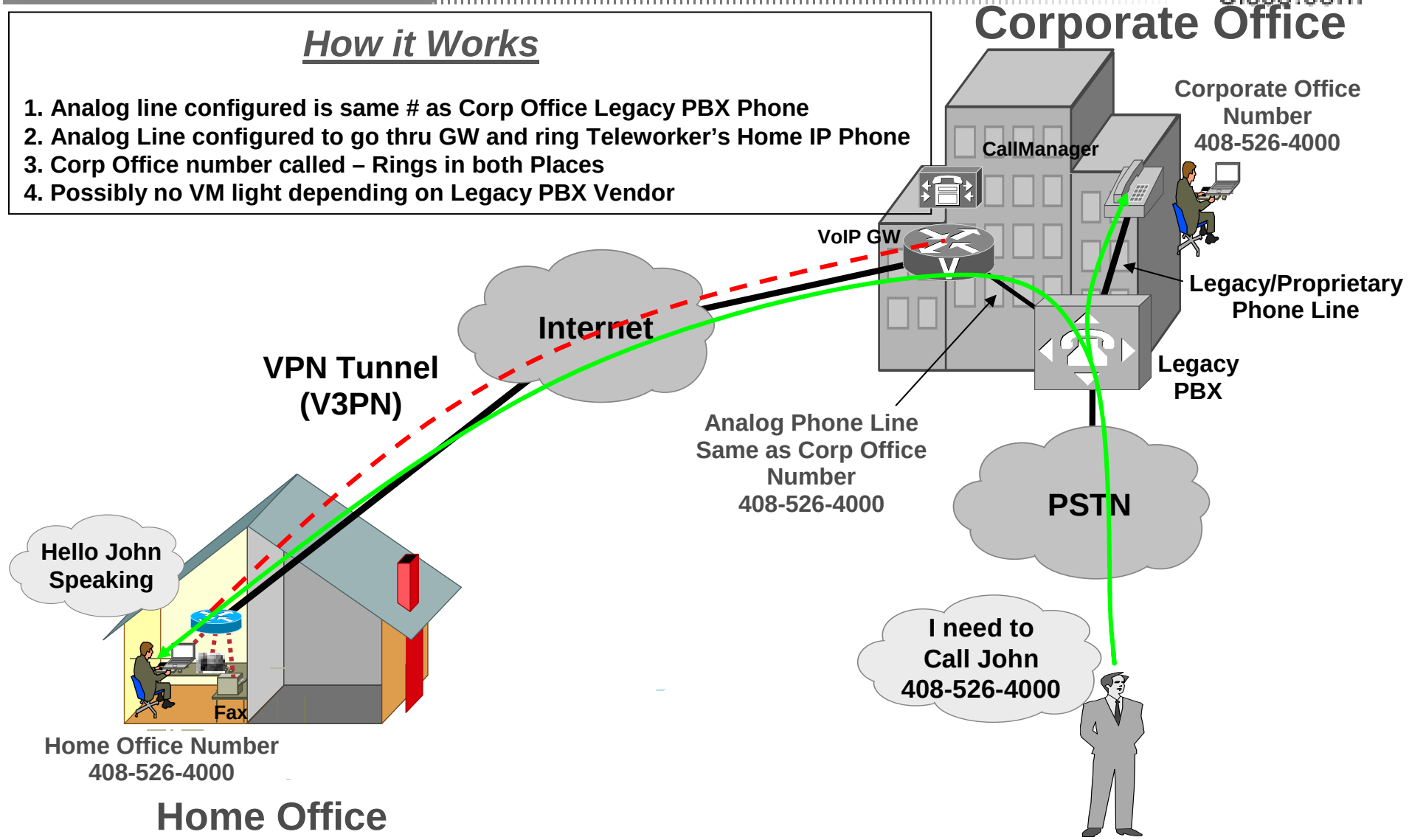
Networks on The Move

IP Telephony for Teleworker

For Legacy PBX Environments

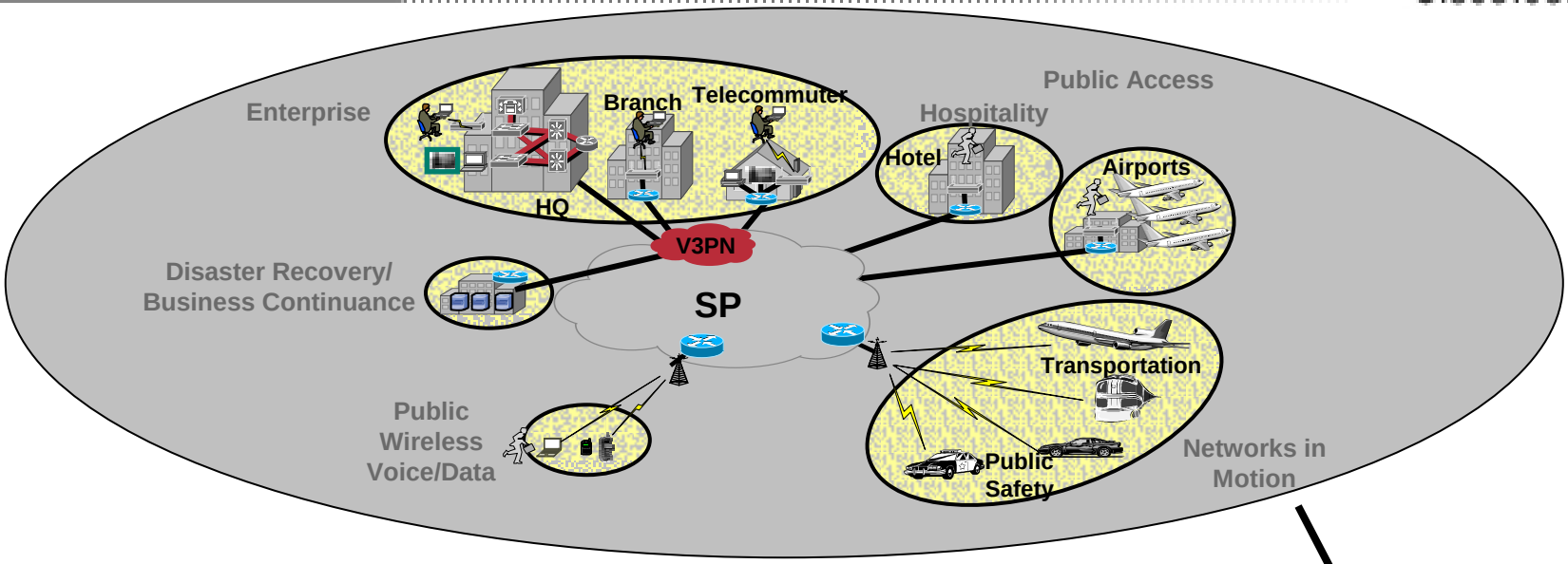
How it Works

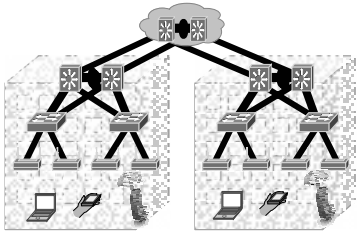
1. Analog line configured is same # as Corp Office Legacy PBX Phone
2. Analog Line configured to go thru GW and ring Teleworker's Home IP Phone
3. Corp Office number called – Rings in both Places
4. Possibly no VM light depending on Legacy PBX Vendor



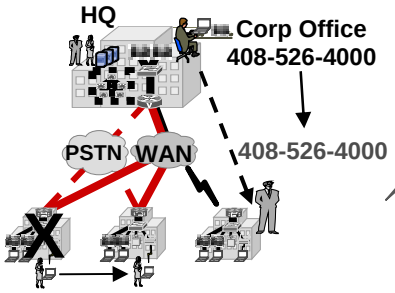
Networks in Motion

Cisco.com

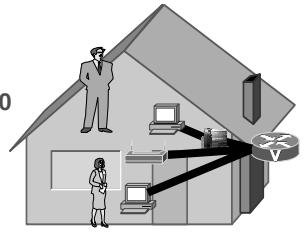




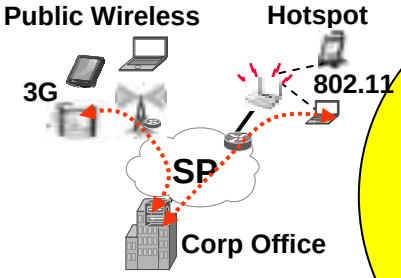
Campus WLAN



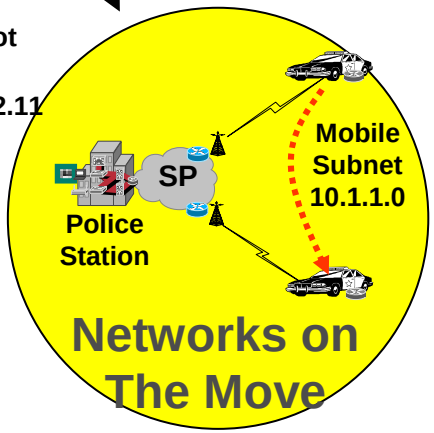
Branch Mobility



Teleworker



Users on the Move

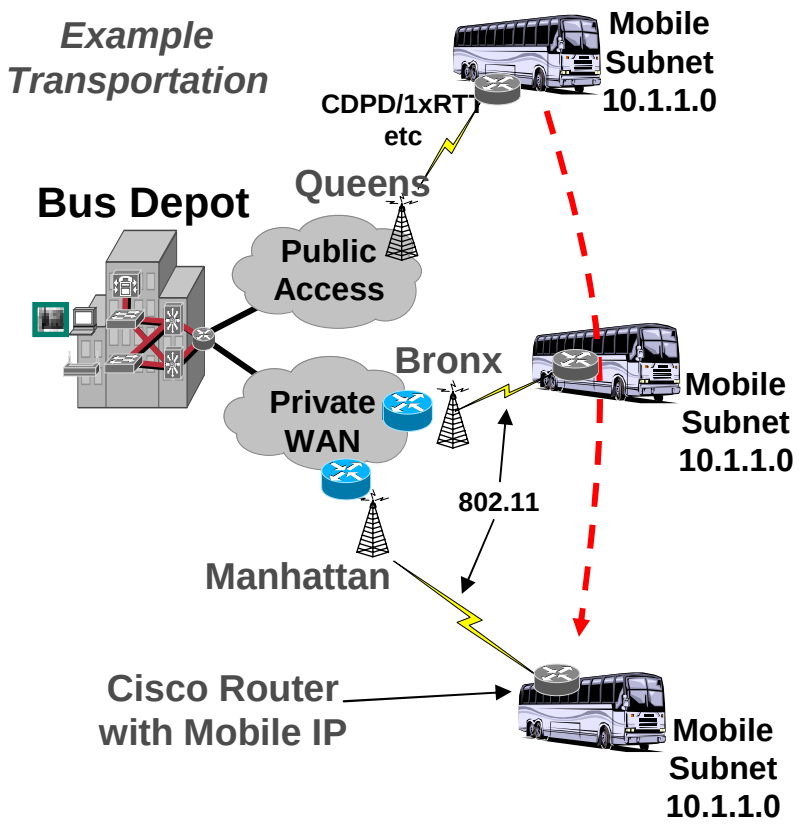


Networks on The Move

Networks in Motion – Solution Overview

Solution Overview – Transportation and Public Safety

Cisco.com



Solution Timeline

Today

Phase 1	Phase 2	Phase 3
Proof of Concept/Trials	Stationary Wireless Access (CY 2H 03)	Wireless Roaming Access

Featured Elements

- **Reducing OpEx to increase Productivity + Profitability - Today many non-standard applications each with their own communication system**
- **Applications Example - Fare Collection, Video Surveillance + Storage, Telemetry, Maintenance Apps, GPS etc.**

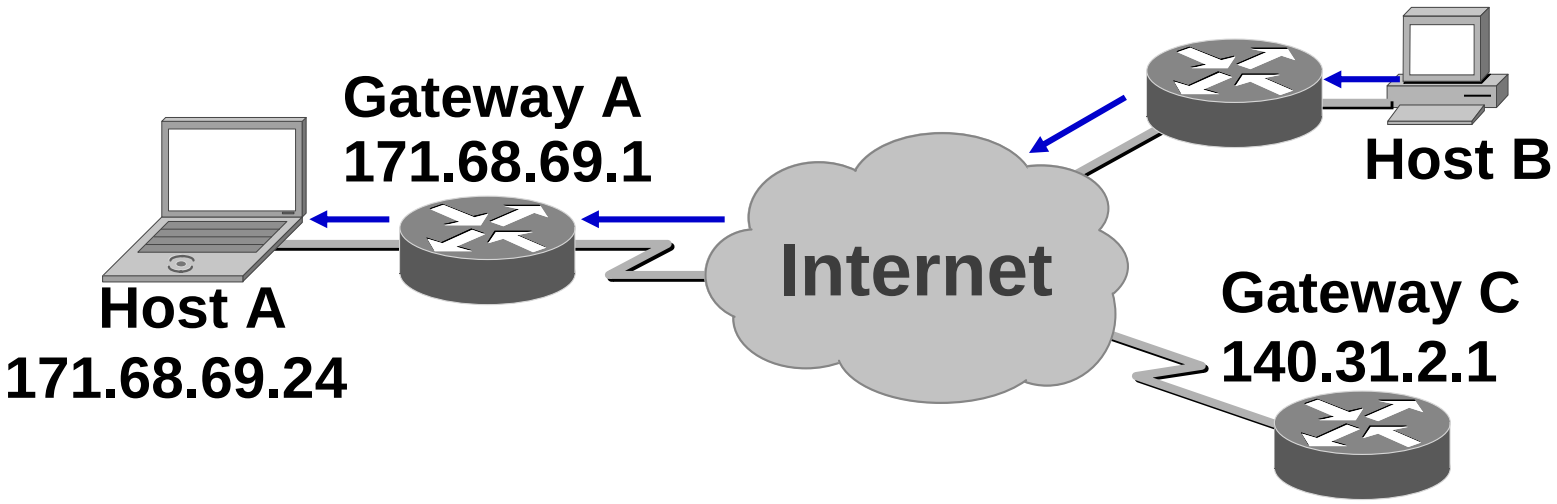
  Standard network infrastructure for multiple industry applications with IP based Ethernet access

  Vehicle maintains network connectivity while in motion using the the MAR 3200 Mobile Router and a combination of Private and Public Wireless access media

- **Continuous strive to create new revenue streams**

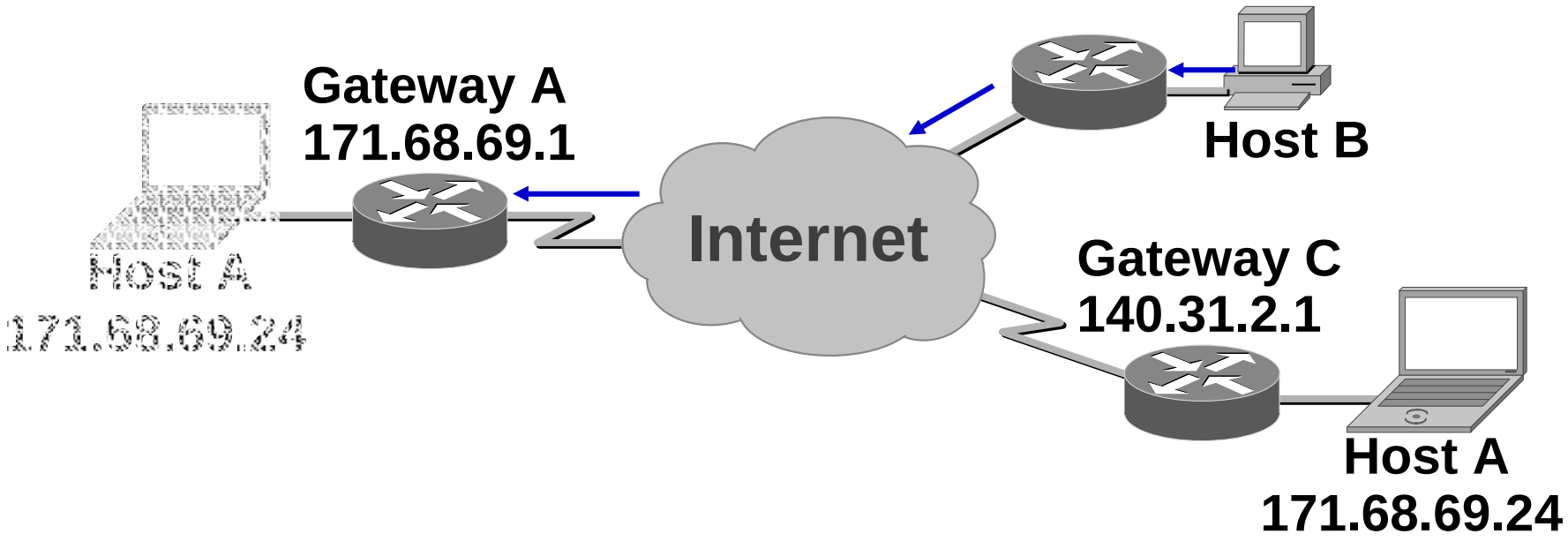
  Internet Access for passengers provides added revenue stream potential

Basic Concept



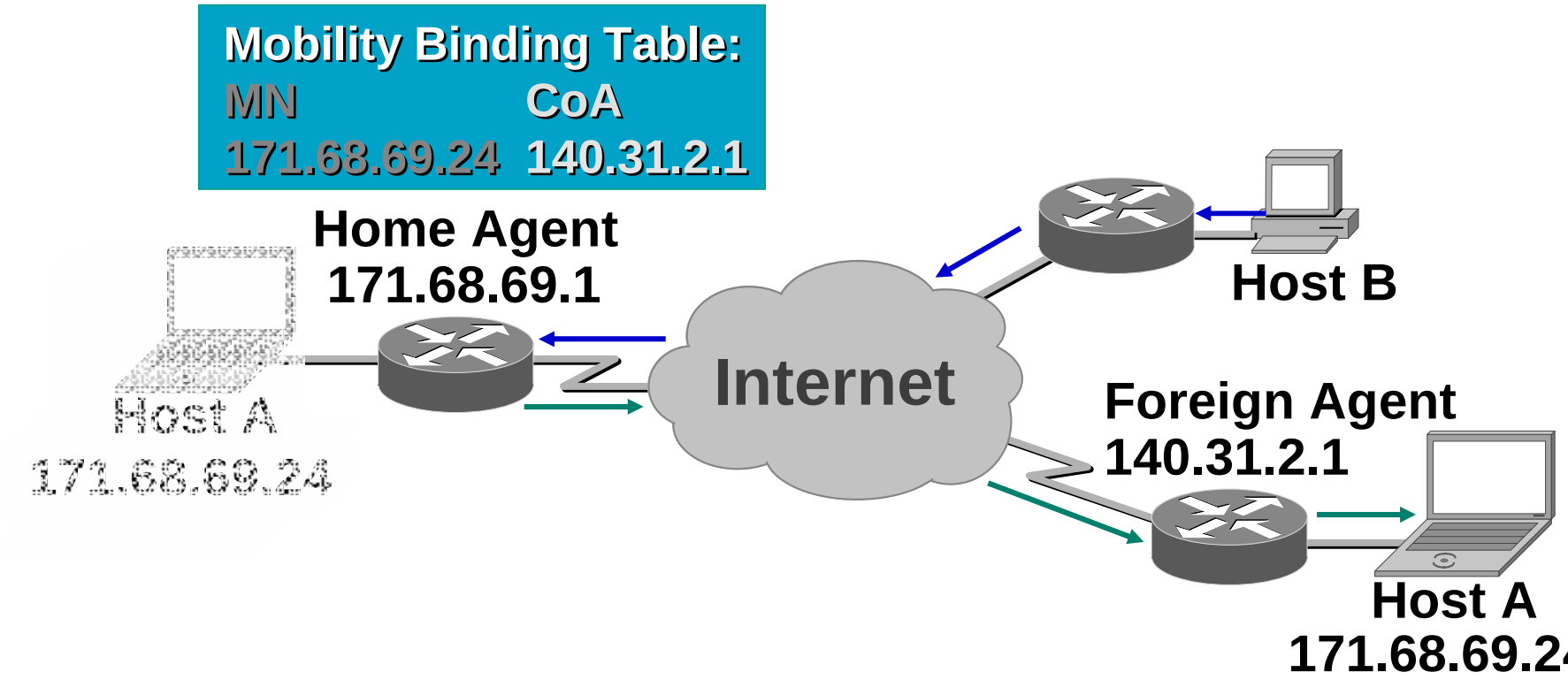
- **Host A receives packets from Host B through normal routing**

Basic Concept



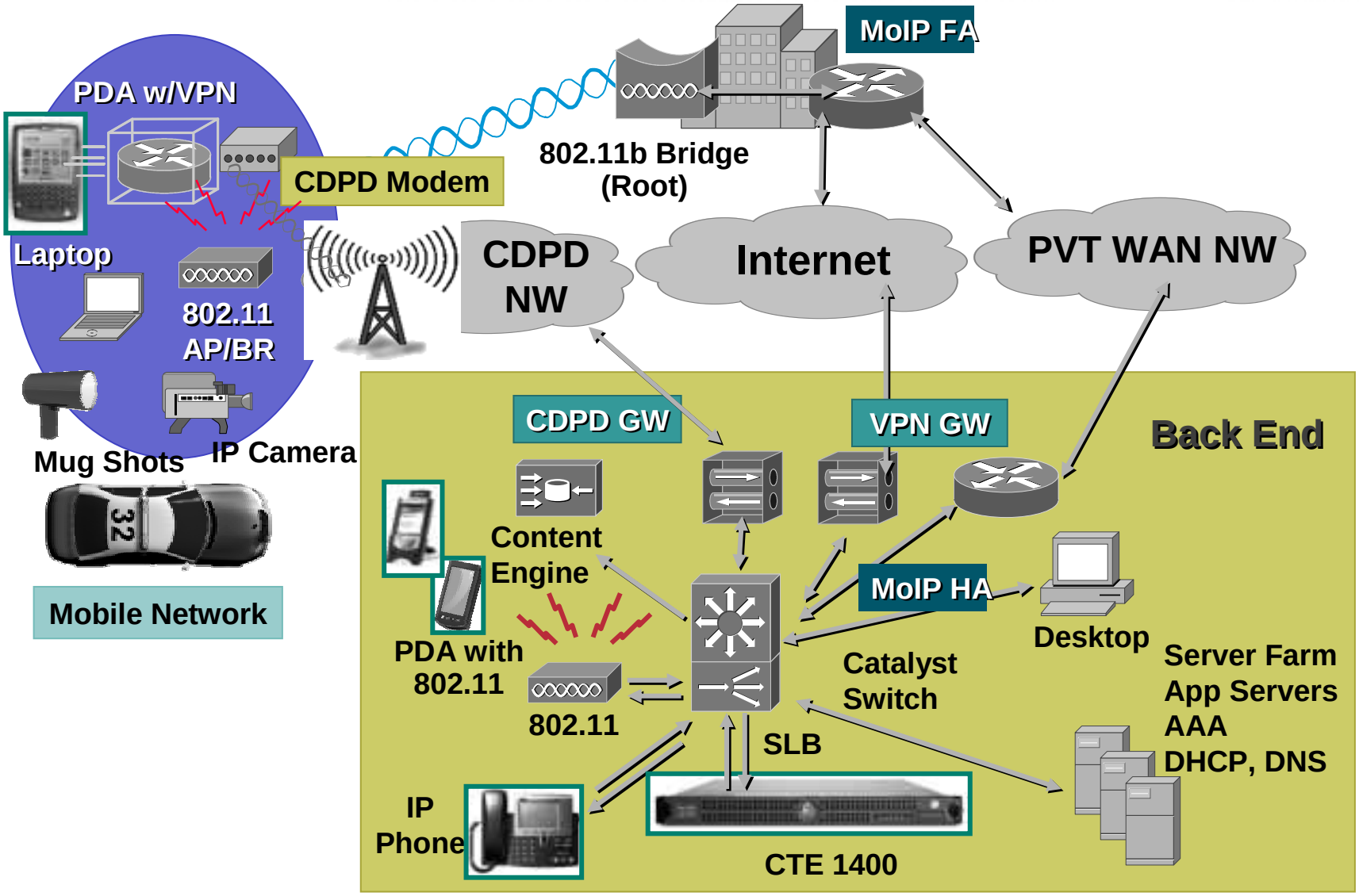
- Gateway A replies to Host B with an ICMP unreachable
- Gateway C blocks host A by rejecting ARP

Basic Concept

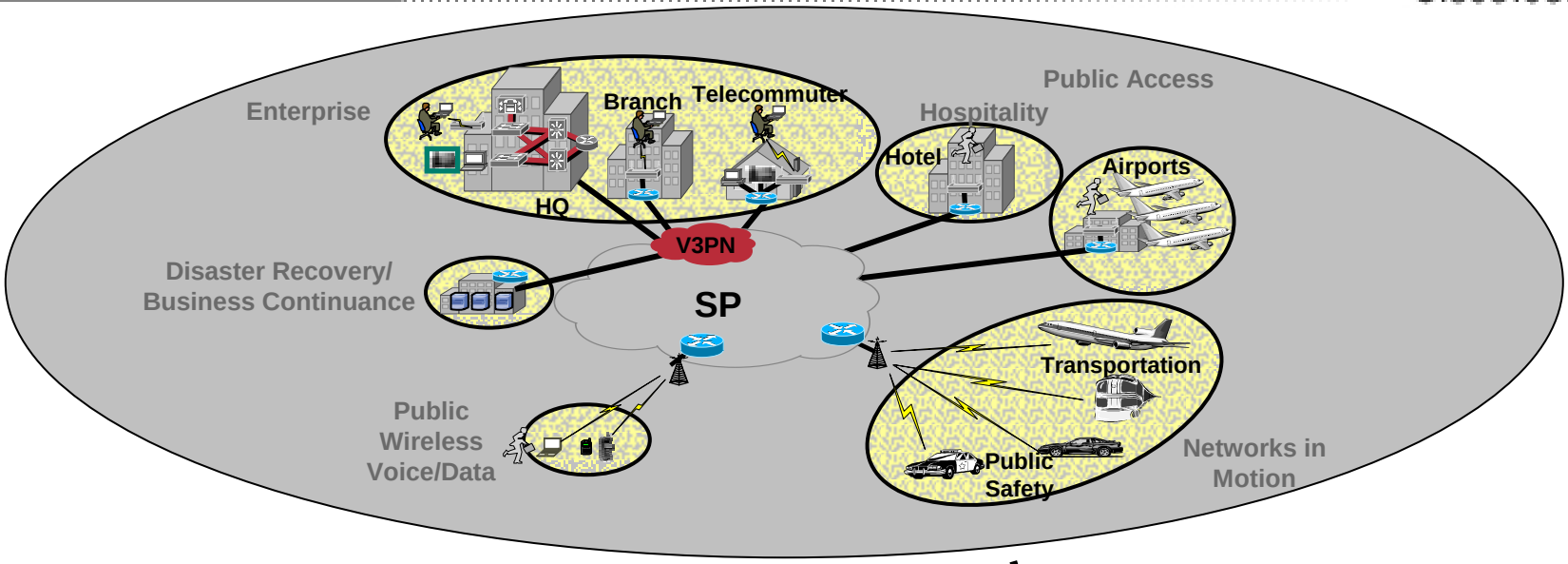


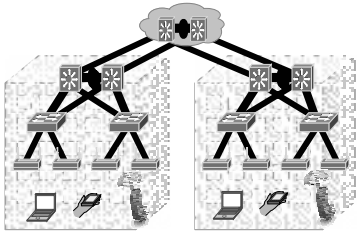
- Home Agent [HA] forwards packets to Host A (Mobile Node [MN]) via Care of Address [CoA]
- CoA is updated via Registration Request [RRQ] from MN

Example End to End Law Enforcement Mobility Solution

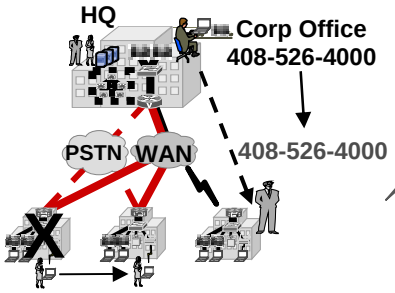


Users on the Move

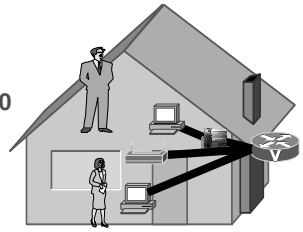




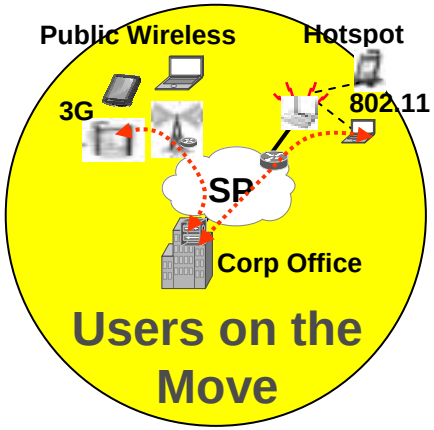
Campus WLAN



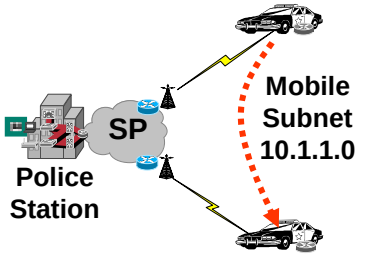
Branch Mobility



Teleworker



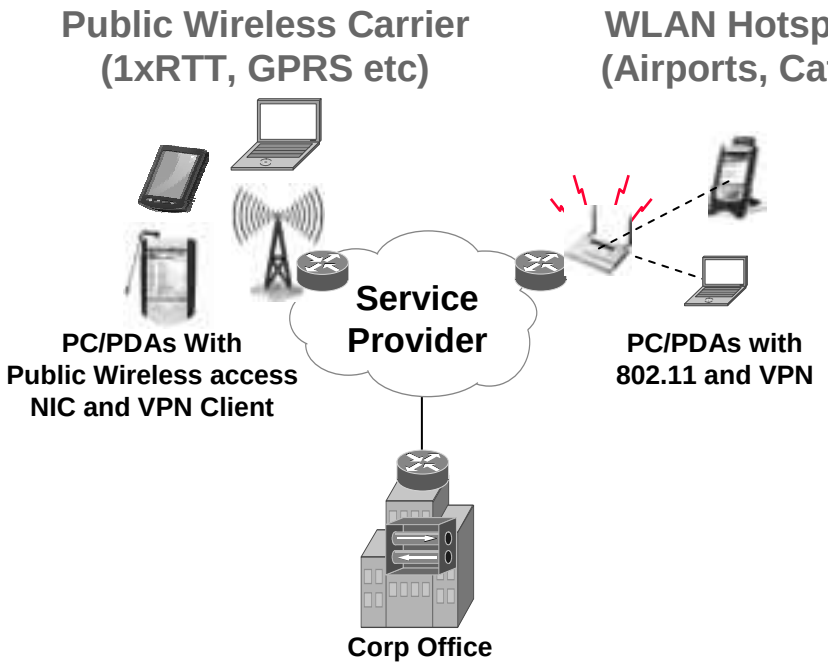
Users on the Move



Networks on The Move

Users on the Move

Solution Overview



Solution Timeline

Phase 1	Phase 2	Phase 3
WLAN Hotspot Public Carrier Access - PCs	Content Transformation For PDAs	Secure PDA Access With Smartcards

Featured Elements

- **Many users require access to corporate Business applications when on the road and in public locations**
  - ***Wireless LAN with Hotspot Access***
  - ***1xRTT/GPRS/CDPD Public Wireless Carrier Access***
- **Pervasiveness of handheld devices such as PDA with requirements to access Business Applications**
  - ***Secure Wireless VPN Client access Certificate or Smartcard VPN Integration***
  - ***PDA Access to corporate resources with Content Transformation***

Intel/Bell

- **Jon Coxworth – Intel – Centrino Technology**
- **Shawn Winter –Bell - AccessZone**