



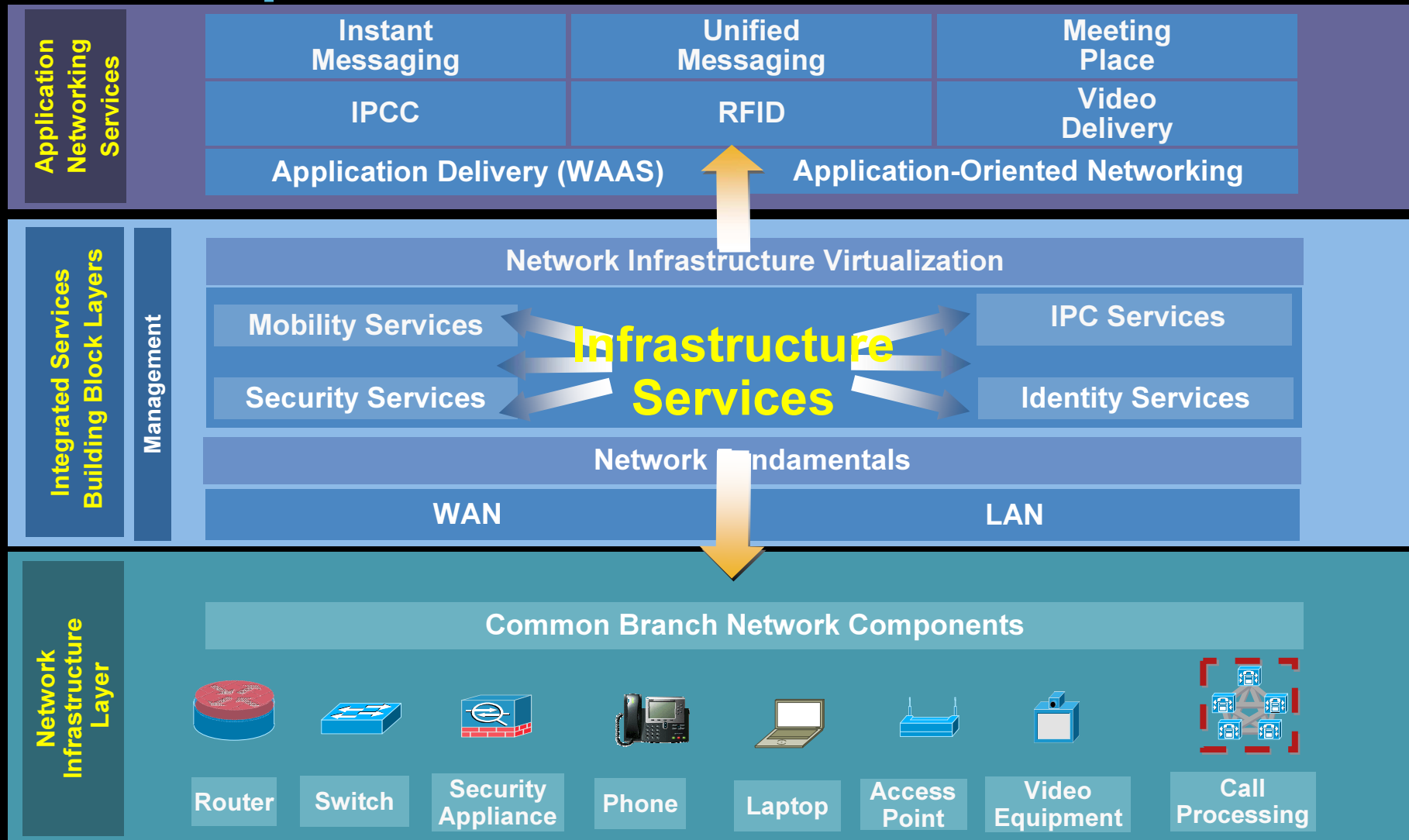
Enterprise Branch



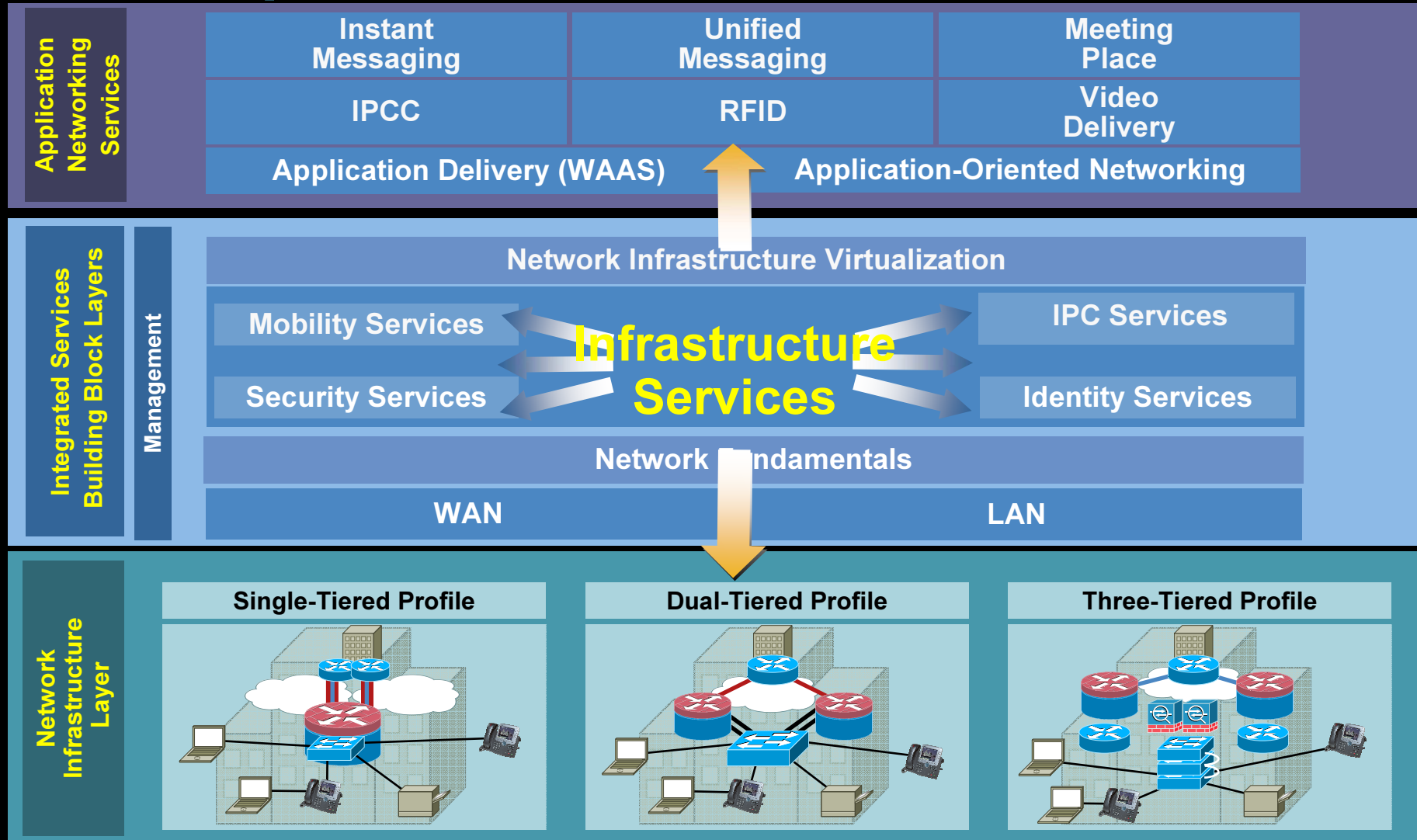
Farel Kuswanda

Product Manager
Cisco 800-3800 Series
Integrated Service Router

Enterprise Branch Architecture



Enterprise Branch Profiles



Single Tier Branch

- **WAN Services**

- Internet Deployment Model
 - T1 Primary Link
 - ADSL Secondary Link

- **LAN Services**

- Integrated L2 Switch

- **Network Fundamentals**

- QoS—Shaping, Policing, Scavenger Class (applied to both switch and router)
 - CoPP (Control Plane Policing)

- **Security Services**

- Integrated Stateful Firewall, IDS, IPS, High performance IPSec.

- **IPC Services**

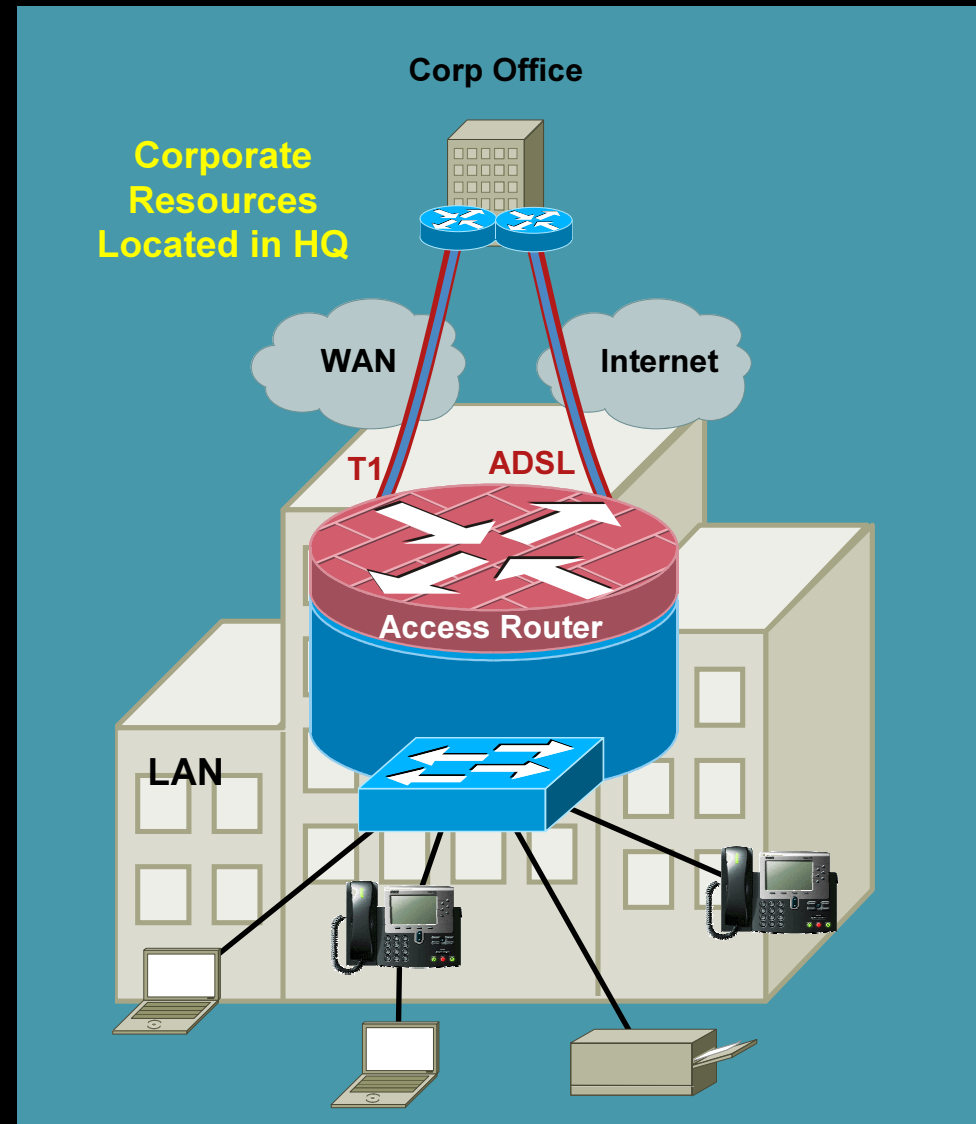
- Integrated Call Manager (IP-PBX), Voicemail

- **Mobility Services**

- Integrated Wireless

- **Identity Services**

- 802.1x, NAC



Empowered Branch



Cisco ISRs - Strong Market Acceptance

2 million integrated services routers

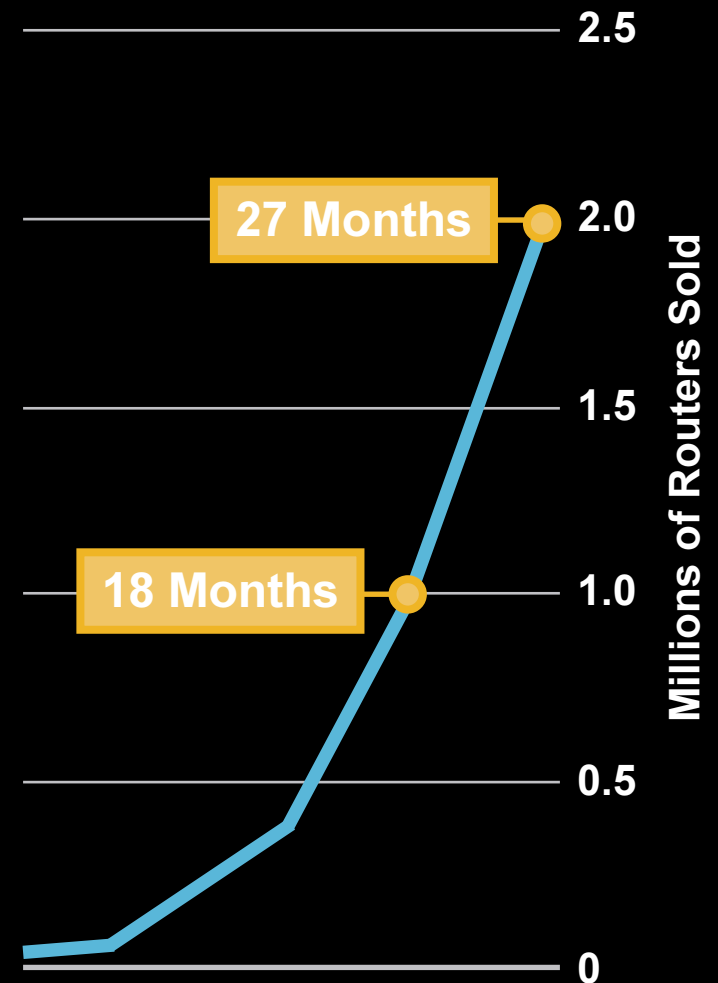
1 million routers
in 18 months

2 million routers
9 months later

More than 50%
shipped with
Advanced Services

3x higher service
attach rate over
previous generation

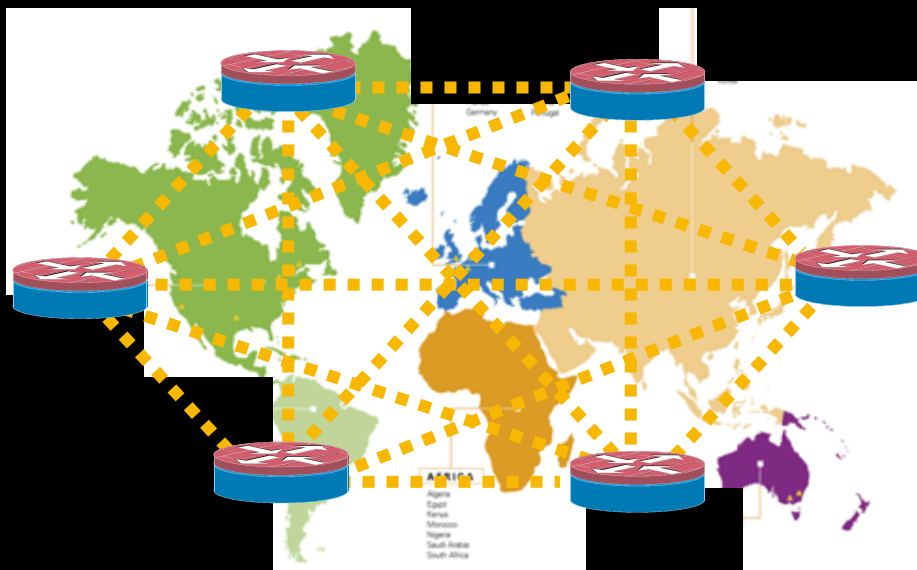
Customers adopting integrated services



Tunnel-less VPN based on Group Encrypted Transport (GET) Enabling Any-to-Any Secure Connectivity

NEW
Ideal for Large
Enterprise Branch

GET is a next-generation WAN security technology that eliminates the trade-off between network intelligence and encryption on WANs



Secures any-to-any branch
connectivity over WAN

Travels the network without a tunnel overlay

Key Benefits

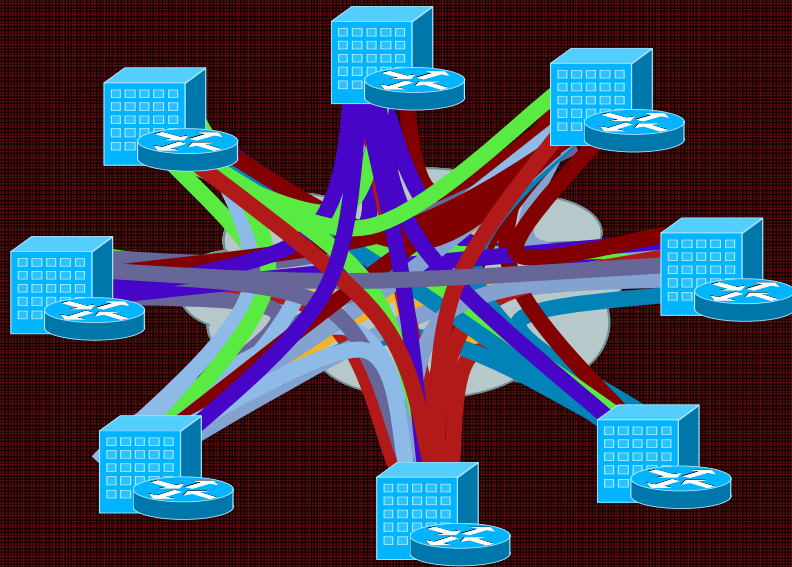
- Easy-to-manage, high-scale any-to-any encrypted communications
- Secured packets use existing routing infrastructure without tunnels
- Networkwide QoS and Multicast capabilities preserved; improves application performance
- Offers flexible span of control among subscribers and providers

VoIP/Video Applications Scale and QoS Marking Preserved

Tunnel-less VPN - A New Security Model

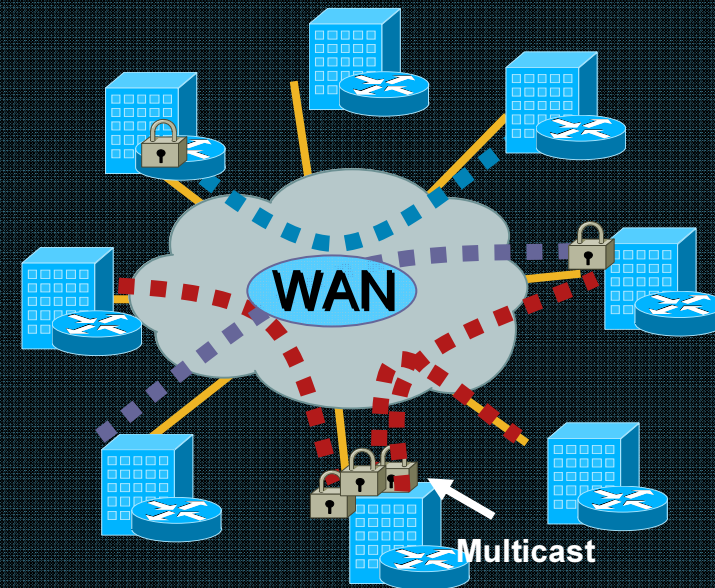
Any-to-Any encryption

IPsec Point-to-Point Tunnels



- Scalability—an issue (N^2 problem)
- Any-to-any instant connectivity can't be done to scale
- Overlay routing
- Limited advanced QoS
- Multicast replication inefficient

Tunnel-less VPN



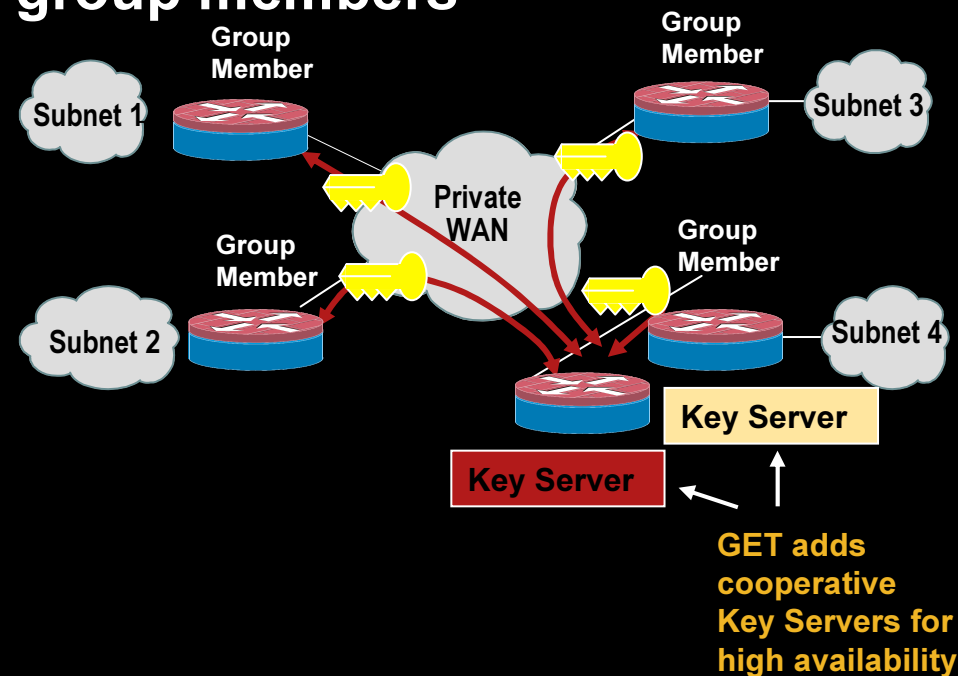
- Scalable architecture
- Any-to-any instant connectivity to high-scale
- No overlays – native routing
- Advanced QoS
- Efficient Multicast replication

How Cisco GET VPN Works

GET simplifies security policy and key distribution by using Group Domain of Interpretation (GDOI)

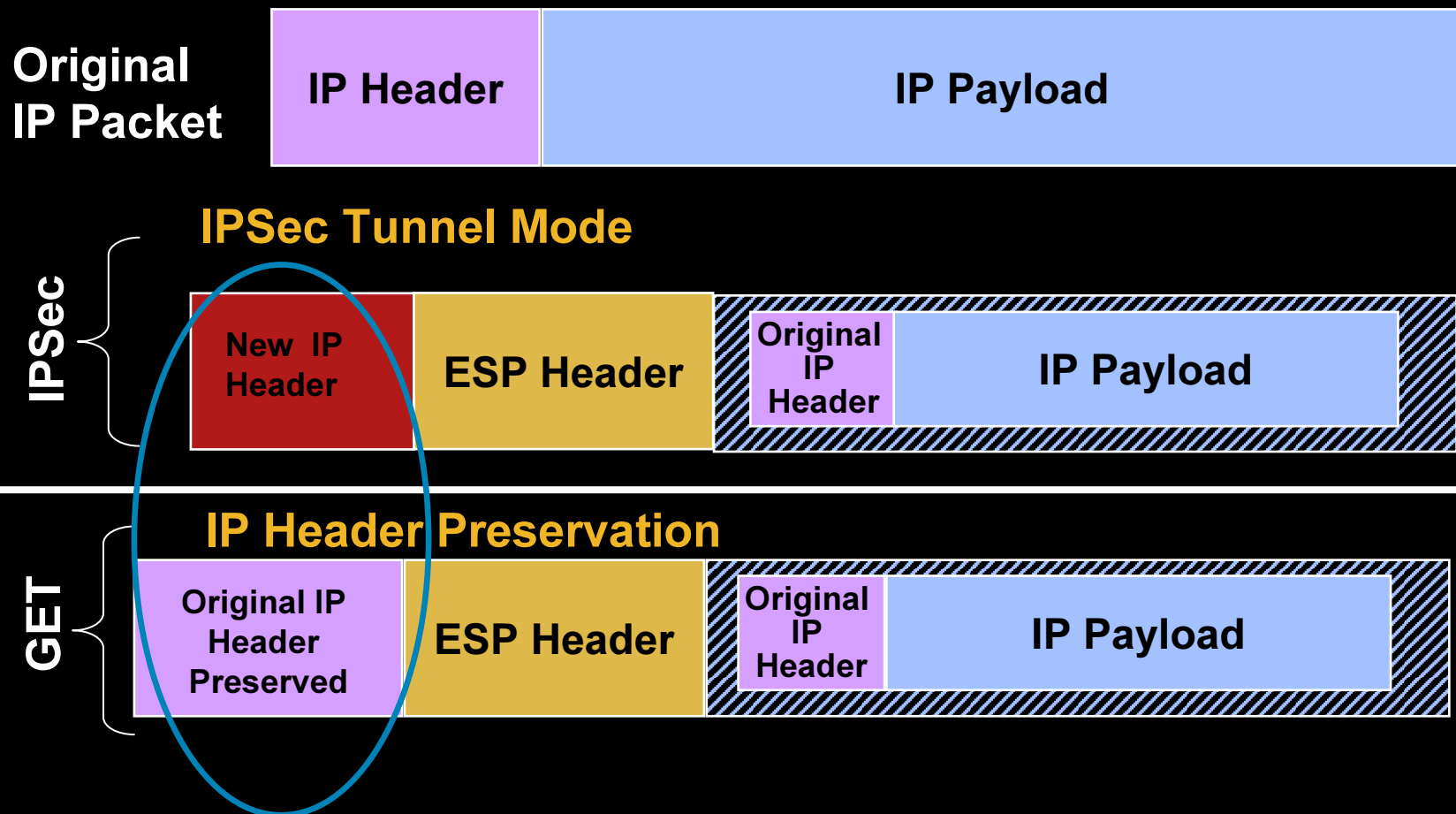
- GDOI:
 - A key distribution mechanism
 - Group Key Model
 - Standards-based (RFC 3547)
- GET uses GDOI and adds:
 - Cooperative Key Servers for high availability & geographic distribution
 - Secure Unicast/Multicast control/data plane via encryption
 - Unicast/Multicast key distribution

Key Server: Authenticates group members, distributes keys and policies; group member provisioning is minimized. Application traffic is encrypted by group members



How GET VPN Prevents Overlay Routing

Cisco GET VPN uses IP header preservation to mitigate routing overlay and to preserve QoS and multicast capabilities



Example Customer - Banking

Large, National U.S. Bank with MPLS Network

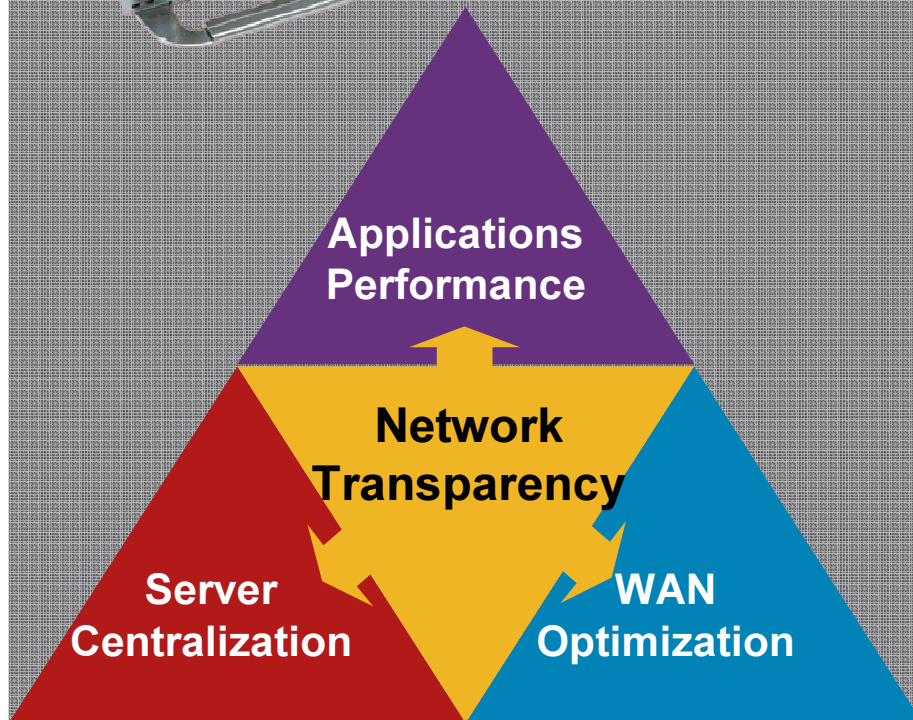
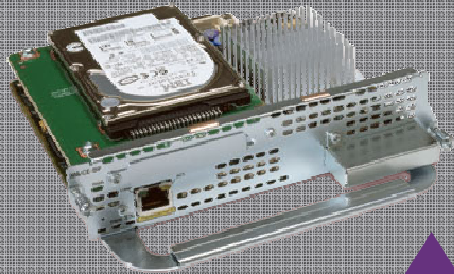
Concerned about security:

- **Compliance:** Need to comply with SOX, payment card industry regulations—Visa rules state that if more than one carrier is used for MPLS, bank must encrypt
- **Concern for provisioning errors:** Confidential customer data can be leaked; in that case, customers would have to be notified, and fines would be levied
- **Management:** Not encrypting today because of management complexity

Benefits of Cisco IOS GET VPN

Previous Limitations	New Feature and Benefits
Multicast traffic encryption through IPsec tunnels: <ul style="list-style-type: none">– Not scalable– Difficult to troubleshoot	Encryption supported for Native Multicast and Unicast traffic with GDOI <ul style="list-style-type: none">– Allows higher scalability– Simplifies Troubleshooting– Extensible standards-based framework
Overlay VPN Network <ul style="list-style-type: none">– Overlay Routing– Sub-optimal Multicast replication– Lack of Advanced QoS	No Overlay <ul style="list-style-type: none">– Leverages Core network for Multicast replication via IP Header preservation– Optimal Routing introduced in VPN– Advanced QoS for encrypted traffic
Full Mesh Connectivity <ul style="list-style-type: none">– Hub and Spoke primary support– Spoke to Spoke not scalable	Any to Any Instant Enterprise Connectivity <ul style="list-style-type: none">– Leverages core for instant communication– Optimal for Voice over VPN deployments

WAAS –Transparent WAN Optimization

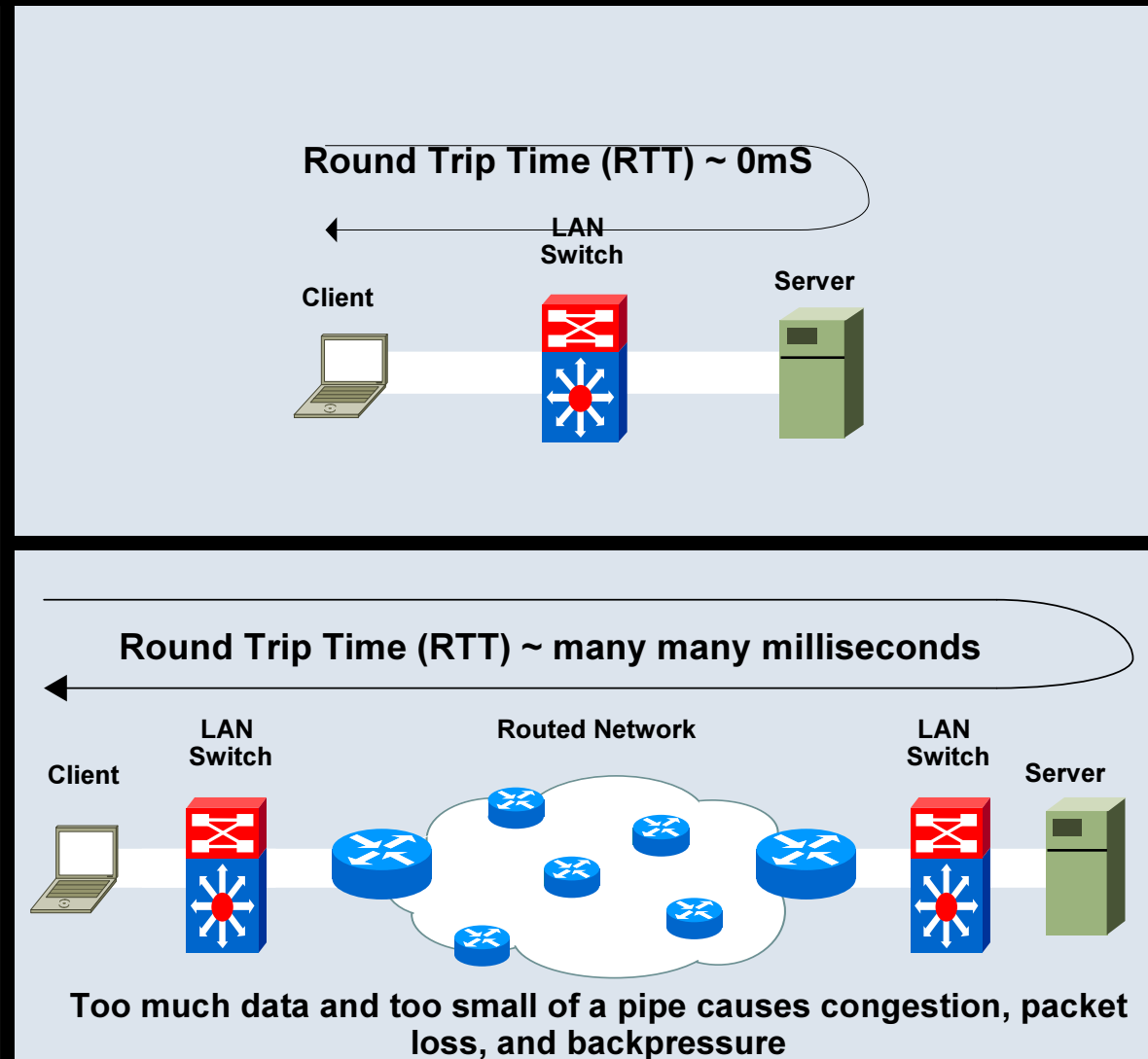


- **WAN Optimization**
 - Compression
 - Caching - store commonly used data close to the user
- **Application response time**
 - TCP optimization overcomes latency
 - Application-specific optimizations
 - Support Quality of service
- **Server Centralization**
 - Centralized file/print/storage
 - IT efficiency
 - End-user response time
- **Network Transparency**
 - Supports security and advanced QoS
 - Network visibility and monitoring

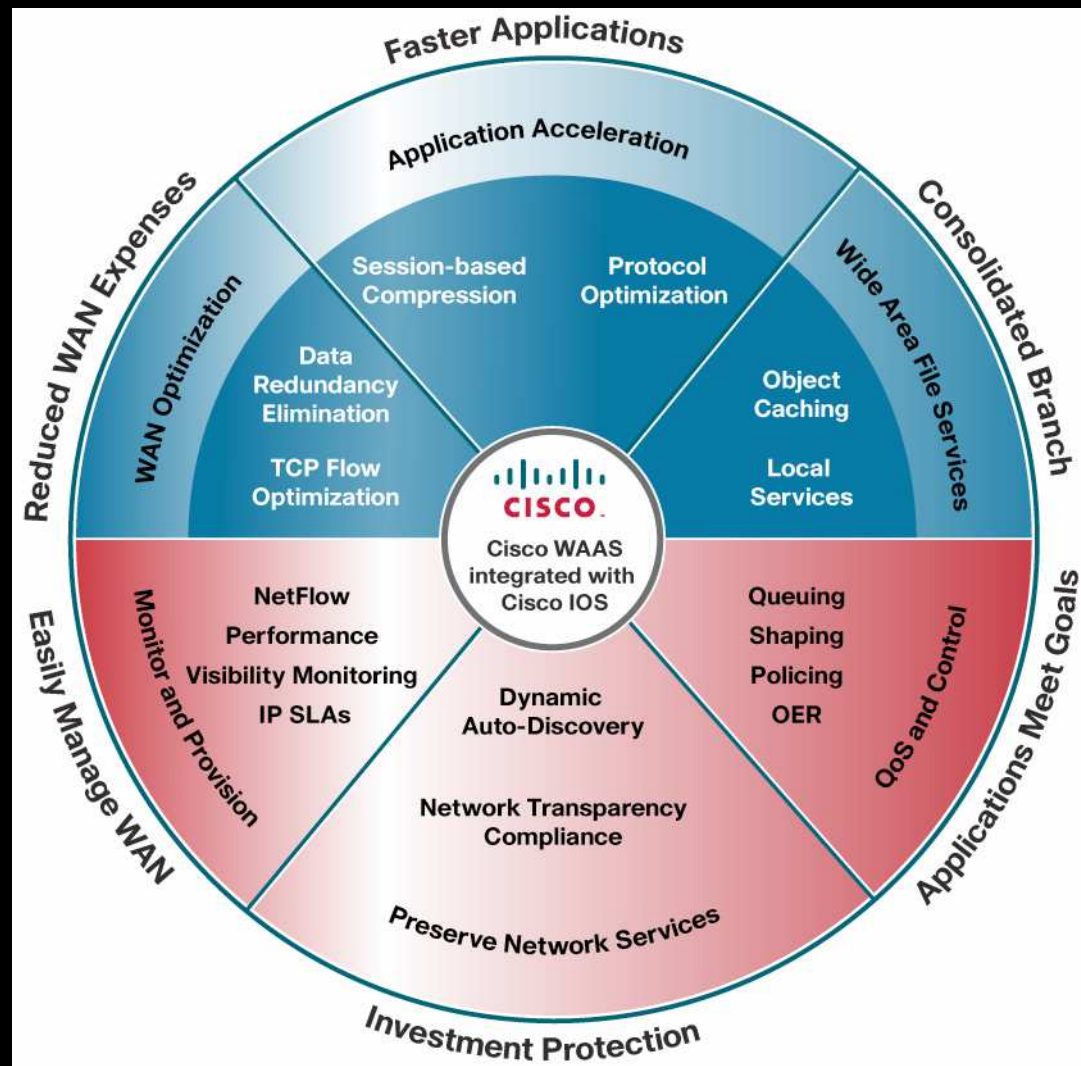
Delivering the Power of the Routed Network

The WAN Is A Barrier To Consolidation

- Applications are designed for LAN environments
 - High bandwidth
 - Low latency
 - Reliability
- WAN characteristics hinder consolidation
 - Already congested
 - Low bandwidth
 - Latency
 - Packet Loss



Cisco WAAS Optimization Architecture

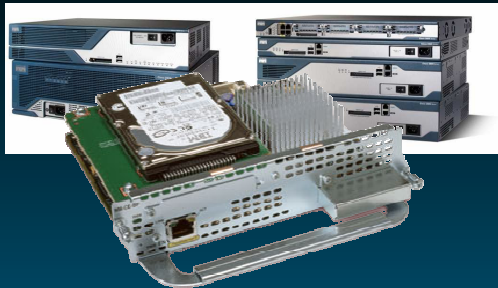


WAAS Accelerates Broad Range of Applications

Application	Protocol	Typical Improvement
File Sharing	<ul style="list-style-type: none"> Windows (CIFS) UNIX (NFS) 	<ul style="list-style-type: none"> 2X-100X
Email	<ul style="list-style-type: none"> Exchange (MAPI) SMTP/POP3, IMAP Notes 	<ul style="list-style-type: none"> 2X-50X
Internet and Intranet	<ul style="list-style-type: none"> HTTP, HTTPS, WebDAV 	<ul style="list-style-type: none"> 2X-50X
Data Transfer	<ul style="list-style-type: none"> FTP 	<ul style="list-style-type: none"> 2X-50X
Software Distribution	<ul style="list-style-type: none"> SMS Altiris 	<ul style="list-style-type: none"> 2X-100X
Database Applications	<ul style="list-style-type: none"> SQL Oracle Notes 	<ul style="list-style-type: none"> 2X-10X
Data Protection	<ul style="list-style-type: none"> Backup Applications Replication Applications 	<ul style="list-style-type: none"> 2X-10X
Other	<ul style="list-style-type: none"> Any TCP-based Application 	<ul style="list-style-type: none"> 2X-10X

*** Performance improvement varies based on user workload, compressibility of data, and WAN characteristics and utilization. Actual numbers are case-specific and results may vary.**

Remote Office Hardware Platforms



NME-WAE
Router-Integrated Network Module
for the Cisco Integrated Services Router



WAE-512
Remote Office Appliance

■ NME-WAE

Lowest CapEx / OpEx, ISR integrated,
addresses 80% of remote offices

NME-WAE-302-K9

Supports 2Mbps WAN connections
250 optimized TCP connections
80GB drive

NME-WAE-502-K9

Supports 2Mbps WAN connections
500 optimized TCP connections
120GB drive

Bundles for ISR 2800 and 3800 available now

■ WAE-512 Appliance

Remote office appliance platform

Supports 20Mbps WAN connections

1500 optimized TCP connections

250GB RAID-1 disk capacity

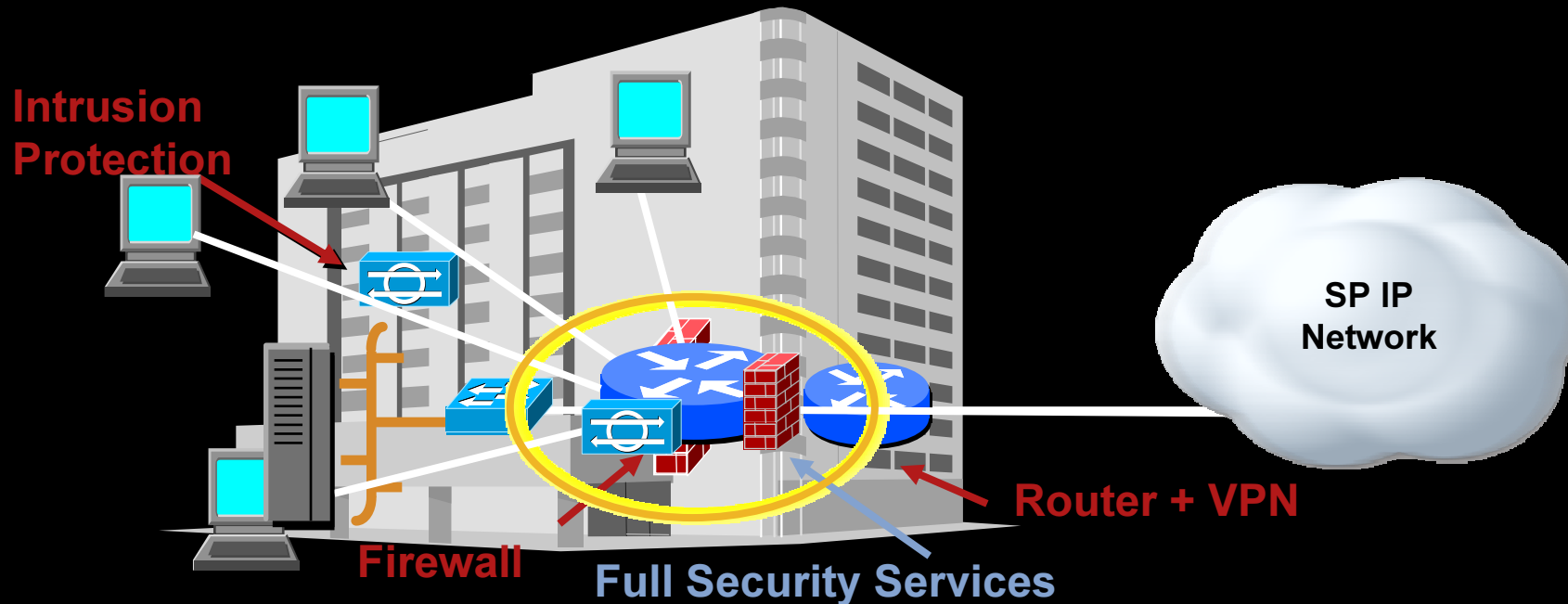
Cluster w/ WCCPv2, PBR, CSM/ACE

Single-tier Branch



- A. Wide Area Network (WAN)
- B. Local Area Network (LAN)
- C. Network Fundamentals
- D. Security Services
- E. IPC Services
- F. Mobility Services
- G. Identity Services

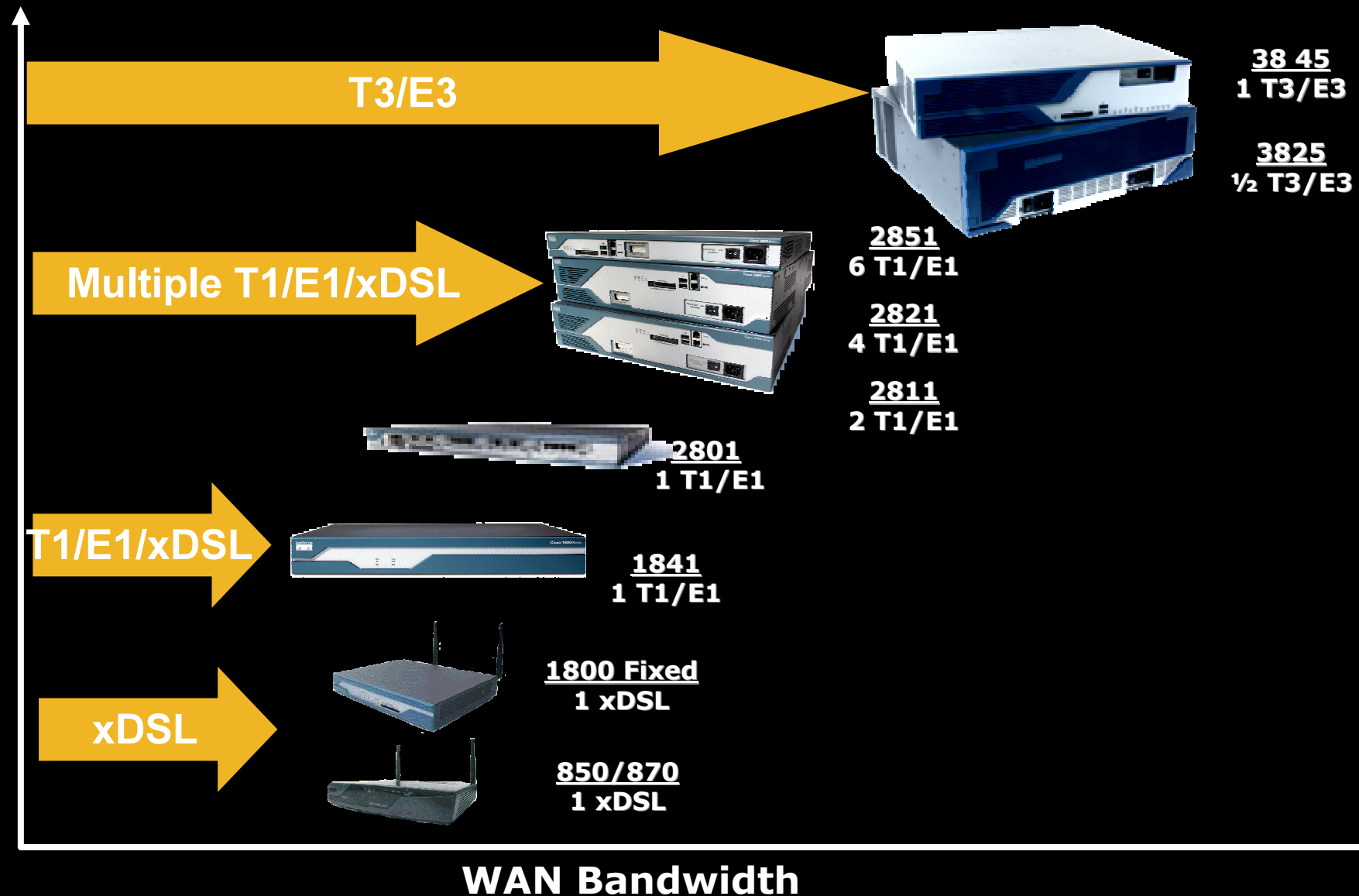
Single Tier implementation



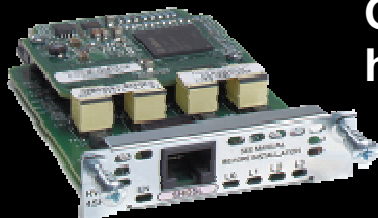
- Many devices → High CAPEX
- Labour intensive operation → extending CPE lifecycle
- Different services coming from different providers / vendors → Lower CAPEX
- Lack of consistency in Security Policy → Less "truck-roll" and devices to manage
- Lower OPEX

Better Model for higher volume deployment

Cisco Integrated Services Routers Performance with Concurrent Services in Traditional Access Networks



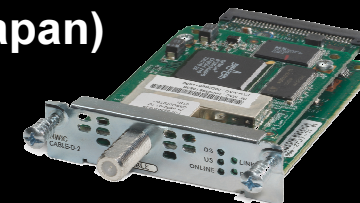
A Unmatched WAN Flexibility



G.SHDSL symmetric high-bit rate DSL HWICs

- Symmetric bandwidth = E1/T1 replacement
- 2-pair/4-wire and 4-pair/8-wire options
- Flexible bonding, wire pairing (IMA/ M-pair)
- Scalable provisioning from 2.3–16 Mbps
- Extensive ATM CoS and IP QoS support

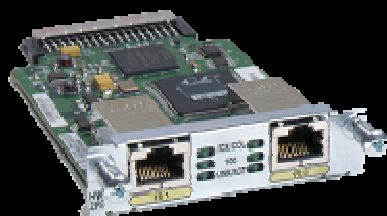
Cable Modem HWIC (U.S./Canada, Europe, Japan)



- Integrated DOCSIS/Euro-DOCSIS WAN interface
- Up to 40 Mbps throughput
- Advanced QoS and WAN traffic management
- Enables managed services for SMB market

Coming Soon

- Frees network module slot
- Enables Metro Ethernet services delivery
- Up to 8 additional Fast Ethernet ports



1- and 2-port routed Fast Ethernet HWICs

- VSAT indoor unit (IDU) integrated on a Network Module
- Integrated TCP/HTTP acceleration
- Ku and Extended Ku, C & Extended C band
- Works with GILAT-SkyEdge compatible hub
- Supports up to 10 mbps of data in outbound direction (hub to VSAT)

NM-1VSAT-GILAT



B New Modules for Integrated Services Routers EtherSwitch Service Module

- **Four form factors** – 16, 24, 48 and 24 + StackWise interfaces
- New generation EtherSwitch modules provide full software feature parity with Catalyst 3750
- **802.3af POE** & Cisco inline power on all ports
- Switch will run it's own IOS image (12.2S train) allowing easier management & support
- L3 WAN Router connectivity to all Switch's in a Ring; for the first time a router can plug directly into a 32-Gbps fault tolerant bi-directional stack ring
- **High Availability:** IP Routing, HSRP, STP enhancements, 802.1s/w, IGMP snooping
- **Security:** ACL, port security, MAC address notify, RADIUS/TACAC+, 802.1x, SSH, SNMPv3, IPv6
- **Layer 2–4 QoS** with CoS/DSCP, shaped round robin, strict priority queuing



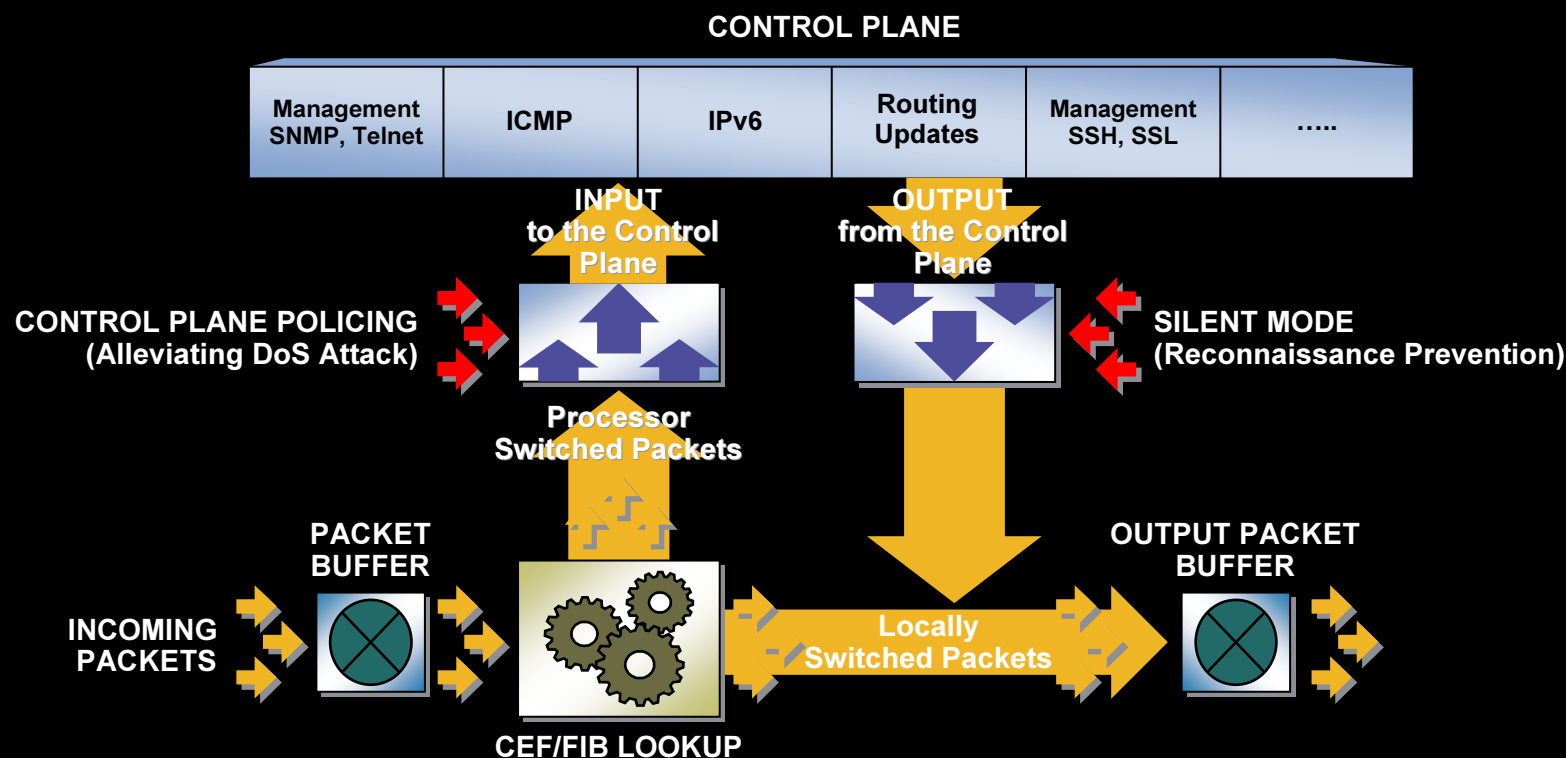
New! 24 and 48-port
EtherSwitch modules



New! 16 and 24 Port that
includes 2 StackWise
interfaces



Cisco Control Plane Policing



- Packets destined to the control plane consume valuable route processor resources
- Router can be attacked by sending large amount of traffic (like Internet Control Message Protocol (ICMP)) to be punted to the route processor (Control Plane)
- Incoming traffic can be policed to the control plane (route processor), reducing the incoming traffic rate and thus alleviating the DoS attack

D Typical Customer Requirements

Business **Services** Need Continuous **Connectivity**,
Requiring the Network to be **Secure** and **Available**

Secure Connectivity

- Encrypted VPN between sites or partners
- Secure remote access
- High ROI Leased line/Frame Relay to VPN migration

Data and Identity Protection

- Network segregation into trusted and untrusted zones
- Defense against worms, viruses, trojans and hacks
- Policy-based network access

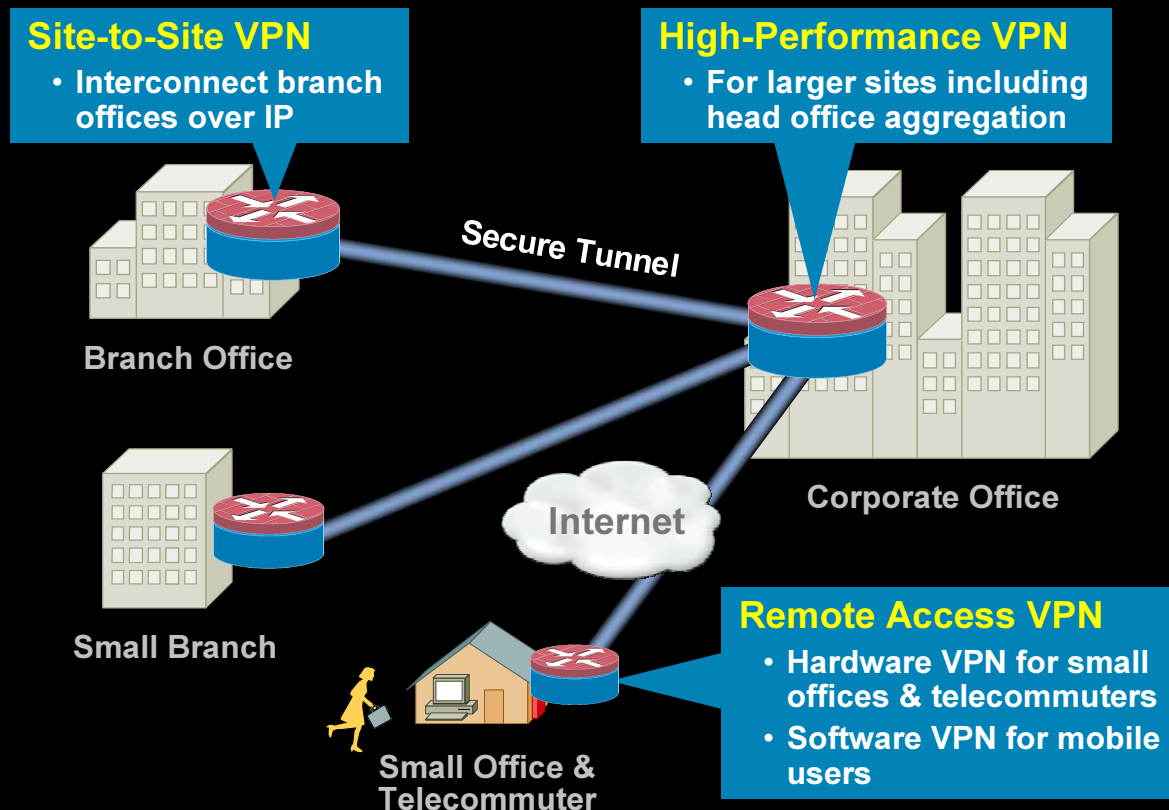
Infrastructure Protection

- Protect the Infrastructure
- Maintain network Transport continuity and availability

D Secure Connectivity Overview

Business Requirements

- Encrypted VPN connectivity between sites or partners
- Secure remote access
- High ROI of Leased line/Frame Relay to VPN migration



Value of Integrated Network Security

Site-to-Site VPN

- Scalable full / partial mesh (DMVPN)
- Simplified cookie-cutter deployment (IPSec VTI)
- Simplified PKI deployment (CA Server, USB eTokens)
- Network intelligence (routing, QoS, multicast) enables Voice, Video & Data

Remote Access VPN

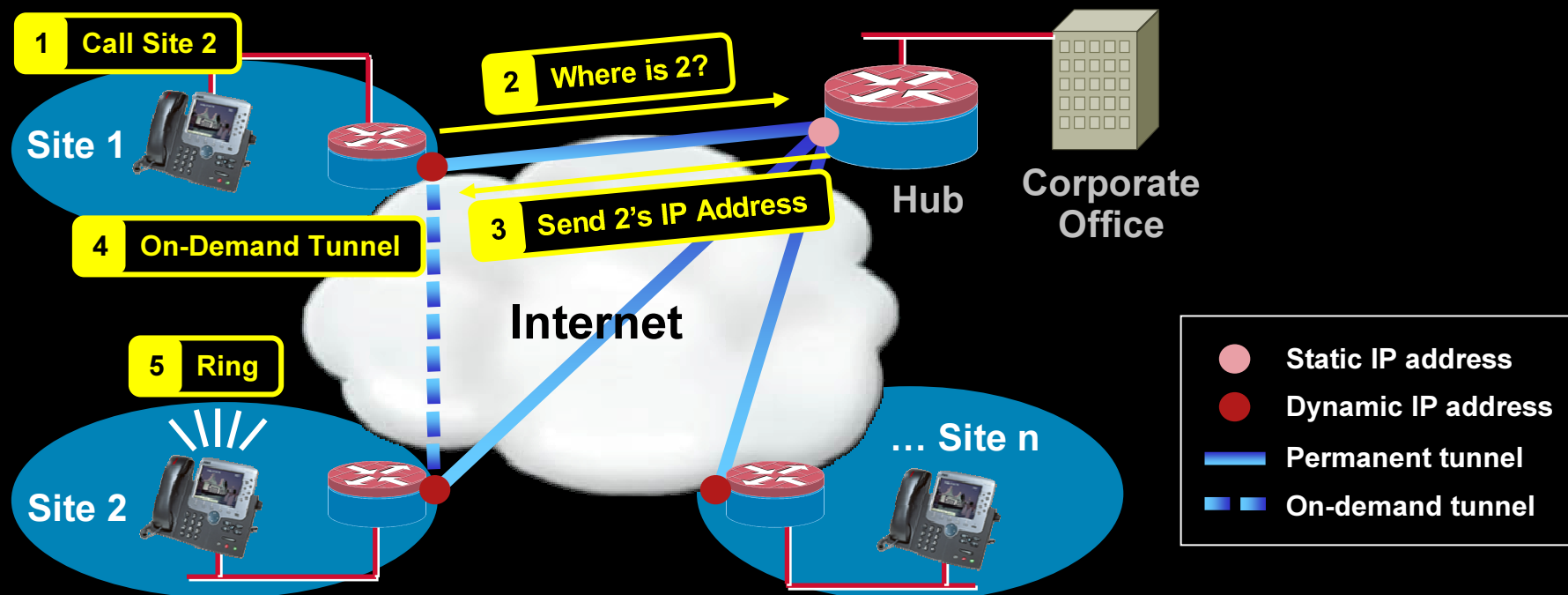
- Centralized policy-based management & full service network access (Easy VPN)
- Clientless secure access (SSL VPN)

High Performance VPN

- Strongest hardware-accelerated encryption (AES)

D Scalable Partial/Full Mesh: Dynamic Multipoint VPN

- Scalable full mesh—on-demand tunnels torn down after use
- Reduced latency and jitter for voice—avoids double hop over hub
- Improved throughput—avoids encrypt and decrypt at hub
- Easy to deploy and maintain—on-demand tunnels are automatic, minimal hub configuration and change management



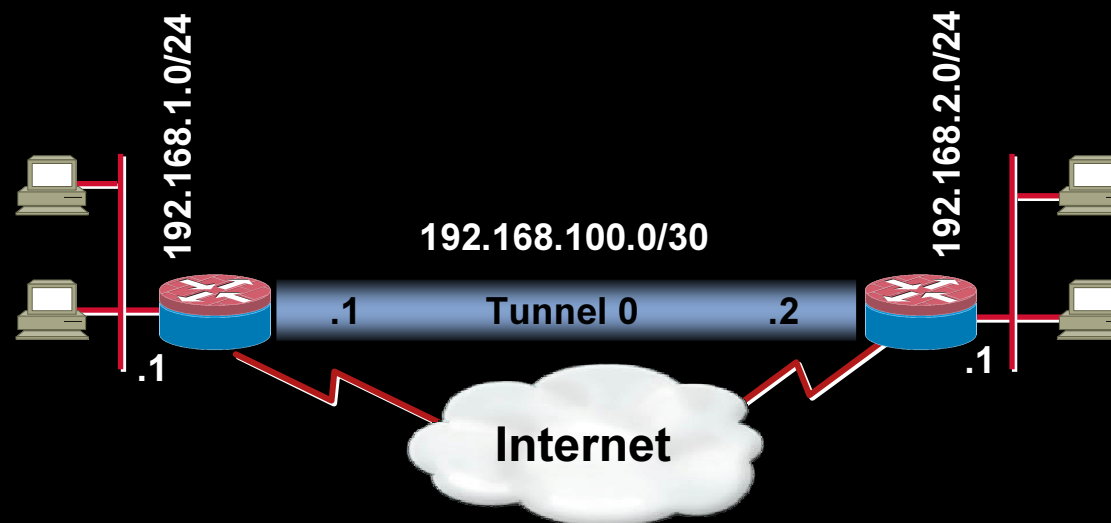
Slide 26

AN1

- * Replaced with Comm BDM version
 - * Previous one was 3 yrs old, this is the latest
- Anand Nuggihalli, 1/19/2006

D Simplified Cookie-Cutter Deployment: IPSec Virtual Tunnel Interface (VTI)

- Simplifies VPN configuration by eliminating crypto maps, ACLs, GRE
- Simplifies VPN design
 - 1:1 relationship between tunnels and sites with dedicated logical interface
- Scales better than Generic Route Encapsulation (GRE)
 - Supports QoS, multicast, and other functions that previously required GRE
- Improves VPN interoperability with other vendors



D Simplified PKI Deployment: **USB Secure Token and Flash Storage**

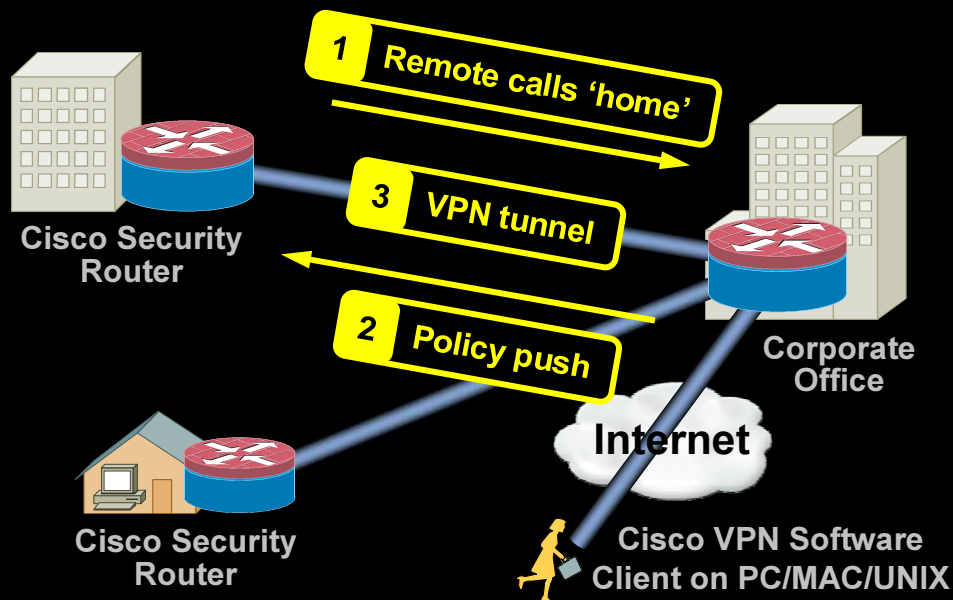
- Distribution and Storage of VPN Credentials
Encryption keys are securely stored and removable
- Zero-Touch Deployment
Easy to provision and distribute encryption keys
- Bulk Flash for Image Distribution/Storage
Alternative to Compact Flash deployment
- 2 USB Ports: Cisco® 3800, 2851, 2821, 2811, 1811, 1812, 871 ISRs
- 1 USB Port: Cisco 2801, 1841 ISRs



Available from Aladdin

D Centralized Policy-Based Management: Easy VPN

- Enables Small or Large Deployments without User Intervention
 - Enforces consistent VPN policy on all remote devices
 - No head-end changes when adding extra devices
- Supports Dynamic Connections with VPN
- Interoperability Across Cisco® Access and Security Devices
 - Cisco VPN client is the only FIPS-certified client in the industry



- 1 Remote router contacts central site, provides authentication credentials
- 2 If credentials are valid, central site “pushes” configuration policies securely to remote device
- 3 VPN is established



Network-Embedded SSL VPN Remote Access: **Cisco IOS WebVPN**

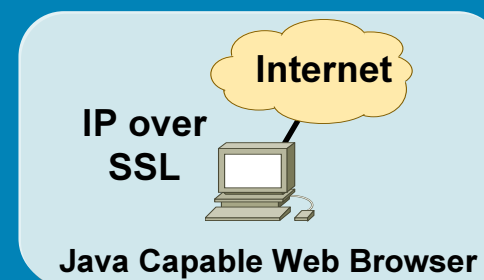
NEW

Clientless Access



- Web-based + Application helper
- Browser-based (clientless)
- Gateway performs content transformation
- File Sharing (CIFS), OWA, Citrix
- Java Based application helper

Full Network Access



- IP-based applications
- Application Agnostic
- Tunnel Client dynamically loaded
- No re-boot after installation
- Client may be permanently installed or removed dynamically

- **Cisco Router and Security Device Manager** – Simple GUI based provisioning and management with step by step Wizards for turn key deployment
- **Cisco Secure Desktop** – Prevents digital leakage, Protects user privacy, Easy to implement & manage, Works with desktop guest permissions
- **Virtualization and VRF awareness** – Pool resources while masking the physical attributes and boundaries of the resources

D Comprehensive Endpoint Security for SSL VPN: Cisco Secure Desktop

Complete Pre-Connect Assessment

- Location assessment – managed or unmanaged desktop?
- Security posture assessment – AV operational/up-to-date, personal firewall operational, malware present?

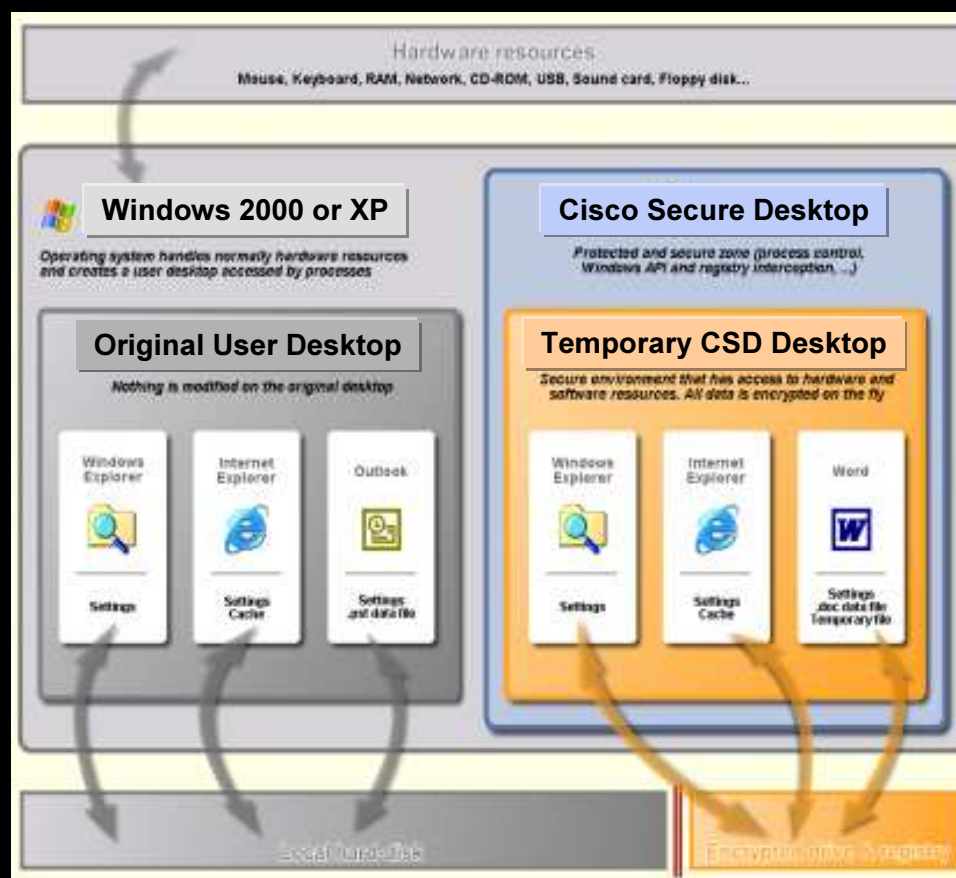
Comprehensive Session Protection

- Data sandbox and encryption protects every aspect of session
- Malware detection with hooks to Microsoft free anti-spyware software

Post-Session Clean-Up

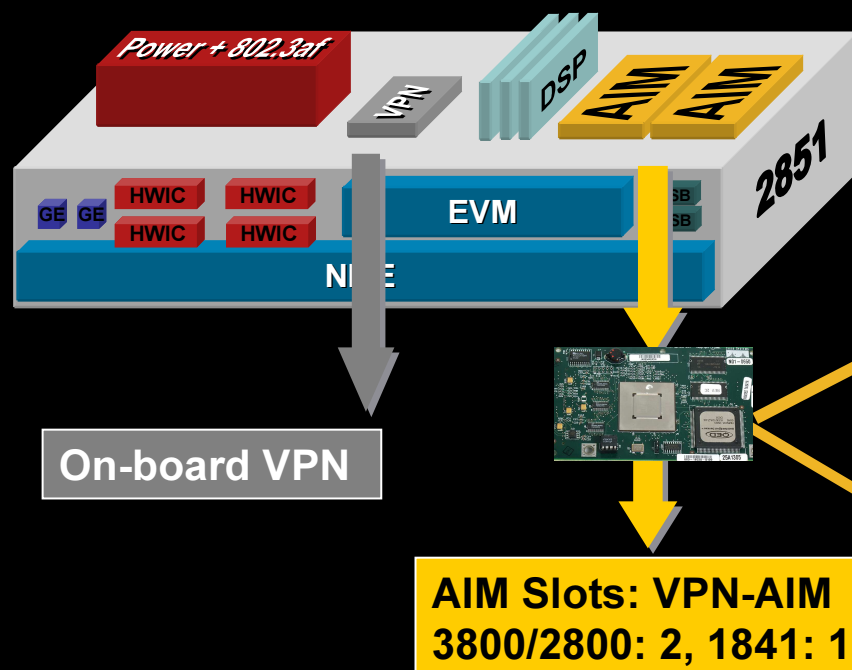
- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history and cookie overwrite
- File download and email attachment overwrite
- Auto-complete password overwrite

Works with Desktop Guest Permissions No Admin Privileges Required





New VPN + SSL Module for ISR 1841, 2800, 3800 *AIM-VPN/SSL (IPSec & SSL Encryption)*




**Investment Protection
with Performance**

- On-board VPN Accelerator supports IPSec 3DES and AES (up to 256 bit)
- AIM-VPN Modules Series Provides IPSec DES/3DES/AES encryption and IPSec IPPCP compression
- The new AIM-VPN/SSL Features:
 - SSL & IPSec Encryption in one Card
 - Supports IPPCP HW Compression Ratios are 2:1 to 3:1
 - Support 2x current SW SSL user counts and Performance
 - Maintains IPSec performance of Previous PLUS AIM and Improves IPsec VPN Hub Performance in 3800
- Part Numbers
 - AIM-VPN/SSL-1, for 1800
 - AIM-VPN/SSL-2, for 2800
 - AIM-VPN/SSL-3, for 3800
- FCS: Sept 2006

AIM-VPNII and AIM-VPN EoS announcements:

http://www.cisco.com/en/US/partner/products/ps5855/prod_eol_notice0900aecd802d3d0b.html

http://www.cisco.com/en/US/partner/products/hw/routers/ps282/prod_eol_notice0900aecd8042e674.html



Scalable Performance

- Up to 1.1Gbps F/W*
- Up to 185 Mbps IPsec
- Up to 425 Mbps IPS**
- Up to 2,500 Tunnels

Performance and Service

- Up to 1.1Gbps F/W*
- Up to 185 Mbps IPsec
- Up to 425 Mbps IPS**
- Up to 2,500 Tunnels

1.1 Gbps F/W
185 Mbps IPsec VPN
425 Mbps IPS
2500 Tunnels

855 Mbps F/W
175 Mbps IPsec VPN
325 Mbps IPS
2,000 Tunnels

530 Mbps F/W
145 Mbps IPsec VPN
250 Mbps
1500 Tunnels

455 Mbps F/W
140 Mbps IPsec VPN
200 Mbps IPS
1500 Tunnels

130 Mbps F/W
130 Mbps IPsec VPN
70 Mbps IPS
1500 Tunnels

127 Mbps F/W
100 Mbps IPsec VPN
65 Mbps IPS
1500 Tunnels

125 Mbps F/W
95 Mbps IPsec VPN
60 Mbps IPS
800 Tunnels

Cisco 3845

Cisco 3825

Cisco 2851

Cisco 2821

Cisco 2811

Cisco 2801

Cisco 1841

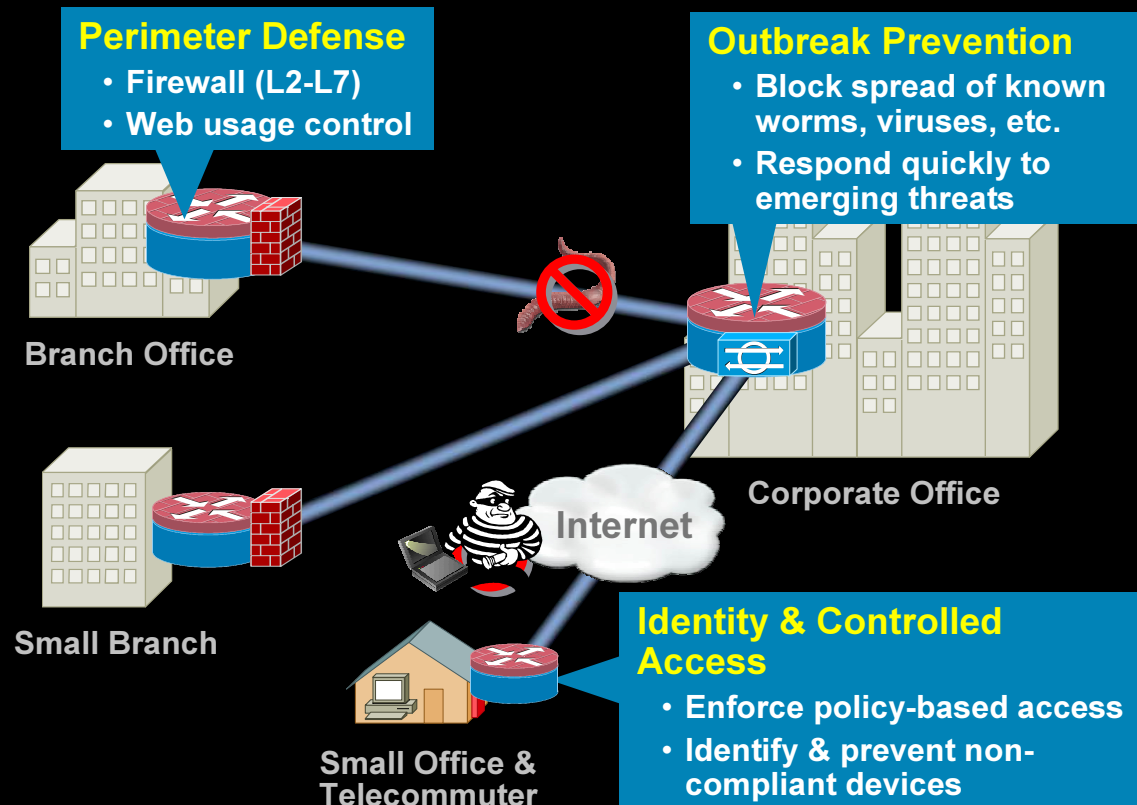
* Stated performance is with NAT and logging enabled

**** Branch scenario when tested with optimal traffic conditions**

D Data and Identity Protection Overview

Business Requirements

- Segregate network into trusted & untrusted zones
- Defense against worms, viruses, trojans & hacks
- Policy-based access to network assets



Value of Integrated Network Security

Perimeter Defense

- Segregate network assets into trusted and untrusted zones
- Application-aware inspection and defense against port 80, IM, P2P misuse (Application Firewall)
- Web usage control & monitoring (URL Filtering, Integrated Content Security)

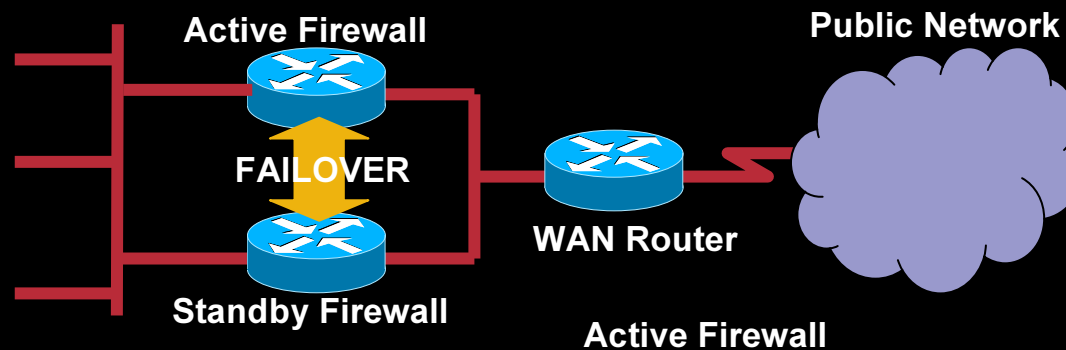
Outbreak Prevention

- Network-based protection against viruses, worms & trojans (IPS)
- Distributed network protection at minimum cost (DTM)
- Rapid response to emerging threats (ICS)

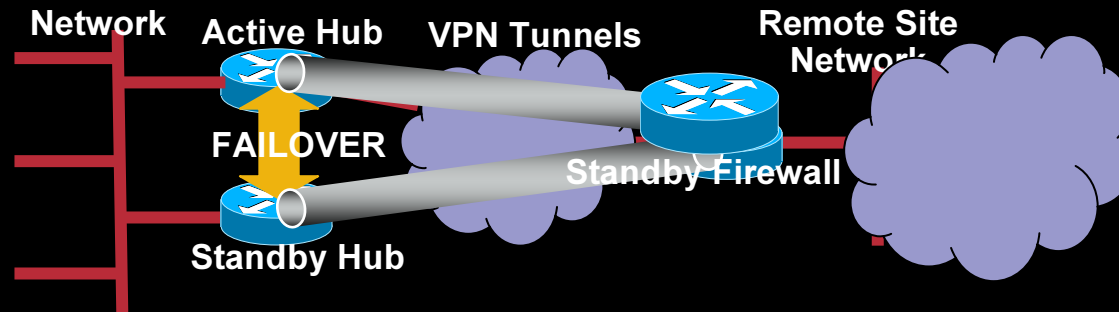
D Cisco IOS Firewall Stateful Failover

- Supports both LAN/VPN interfaces
- Active/Standby configuration
- Maximizes Firewall uptime for mission critical Enterprise applications

Protected Network



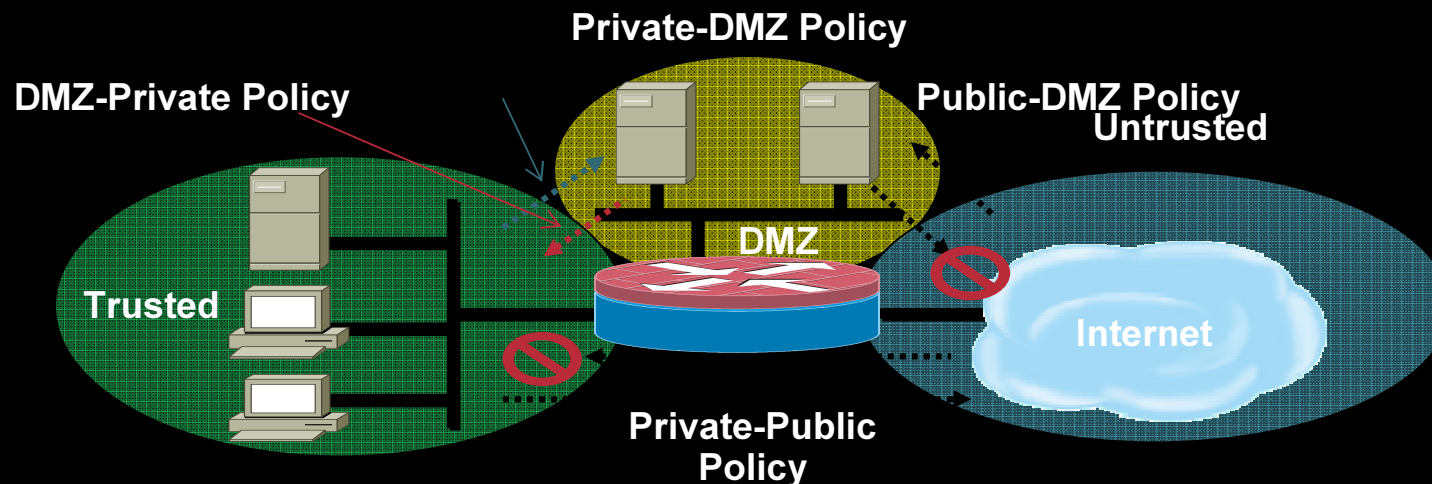
Head End Network





Zone Based Policy Configuration for Cisco IOS Firewall

- Allows grouping of physical and virtual interfaces into zones
- Firewall policies are configured on traffic moving between zones
- Adding or removing interfaces and integration into firewall policy is also simplified



E Business-Ready IP Communications: **CallManager Express and Unity Express**

Business Problem

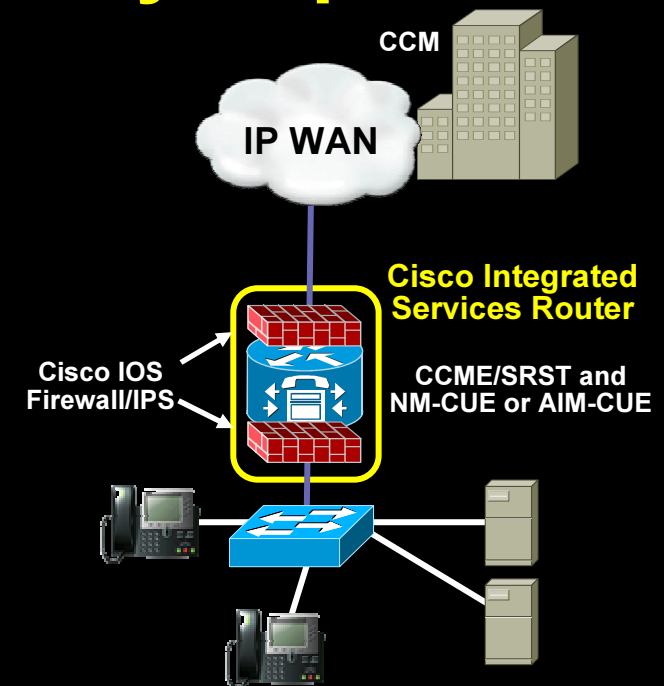
- Affordable and robust IP communications for Enterprise branches and small to medium-sized businesses

Solution

- Cisco® CallManager Express (CME) with Cisco Unity® Express
- Cisco Survivable Remote Site Telephony (SRST)

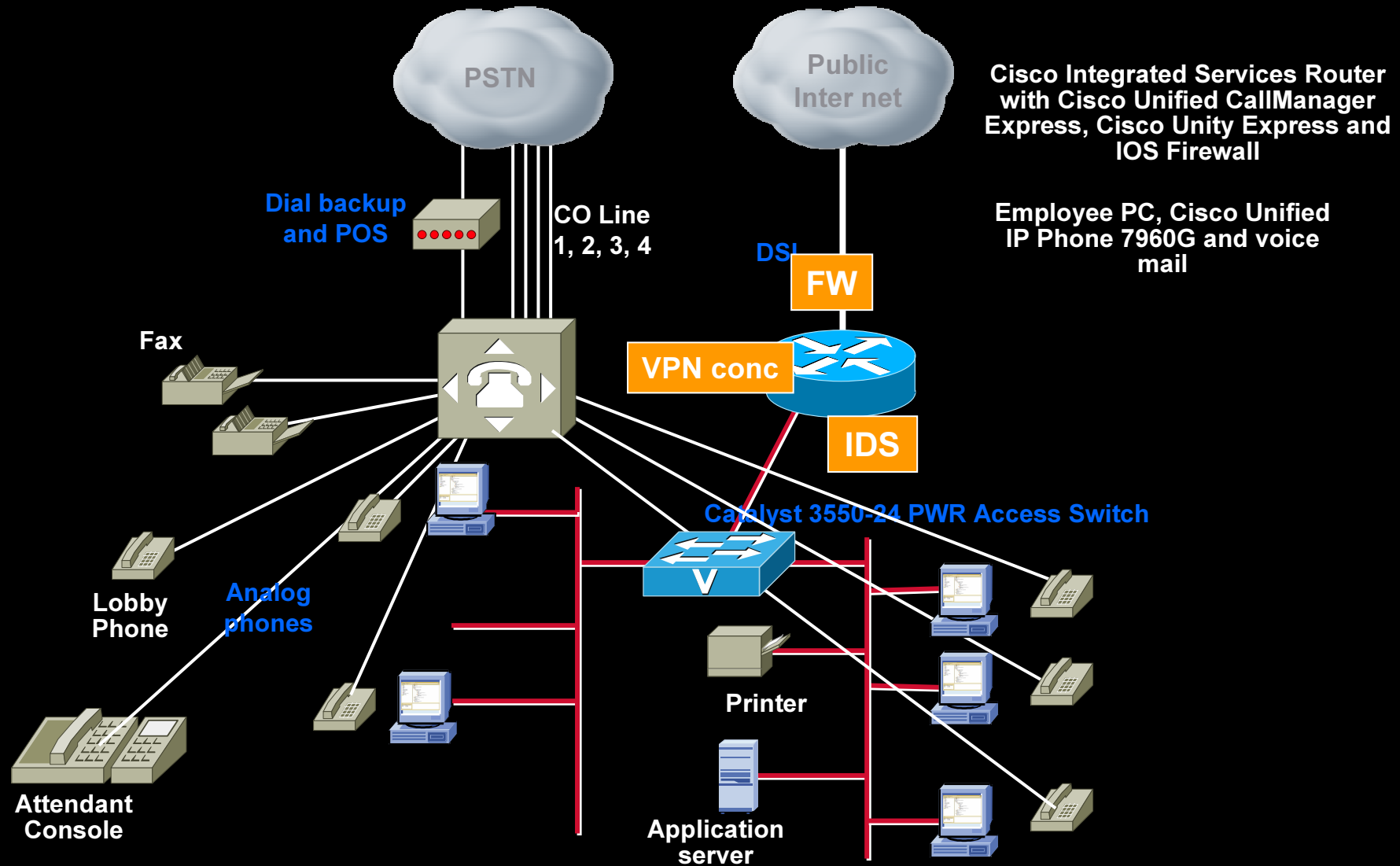
Benefits

- Localized call processing with Cisco CallManager Express (CME) for up to 240 phones!
- Optional distributed voicemail via Cisco Unity Express (NM-CUE or AIM-CUE)
- EtherSwitch® module for line-powering IP phones
- Centralized DSP resources for voice connectivity
- Higher digital and analog voice densities



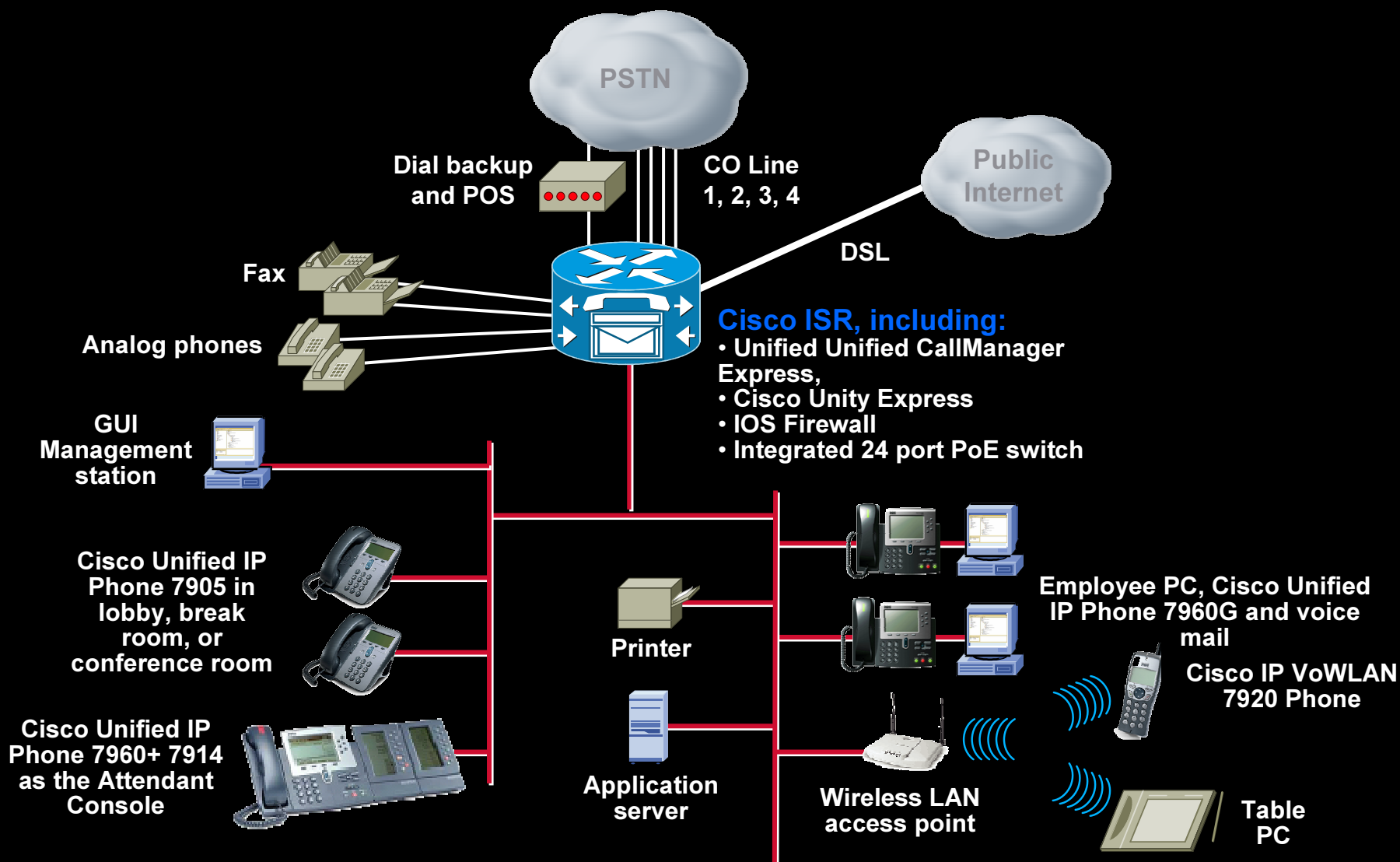
- Cisco IOS Firewall/IPS secures branch call processing
- SRTP encrypts voice calls (SRST)
- TLS encrypts signaling, protects called number, pins, encryption keys (SRST, CME*)
- V³PN between enterprise branch or small to medium business sites

E Traditional Business Solution: Separate Voice and Data Infrastructure





Cisco Unified Communications Express Application: Small Standalone Office Deployment

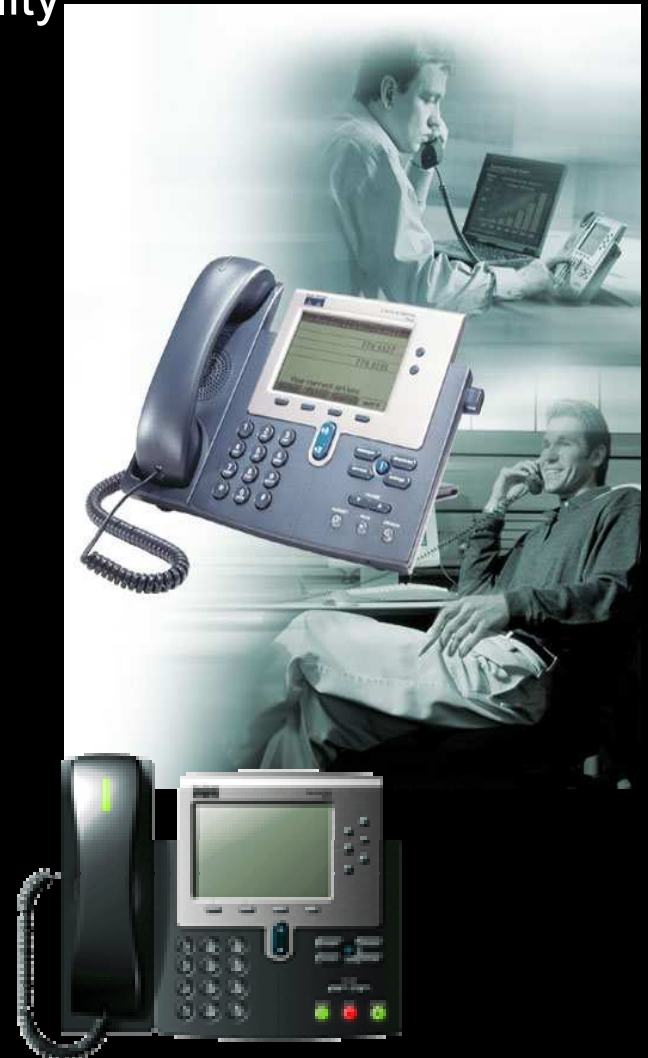




Cisco Unified Call Manager Express

Key Call Control Features

- Support for Either PBX or Key System Functionality
- **Legacy Telephony Features:**
 - Call Transfer, Paging, Intercom, Call Coverage
 - Call Park, MOH, Night Bell
 - Hunt Groups, Basic ACD and Reporting
 - Ad Hoc & “Meet Me” conferencing
 - DID / Operator Console
- **Converged IP Communications Features:**
 - Video Telephony
 - Wireless (802.11) Integration
 - Soft Phone support
 - Desk Top Integration
 - SIP Support



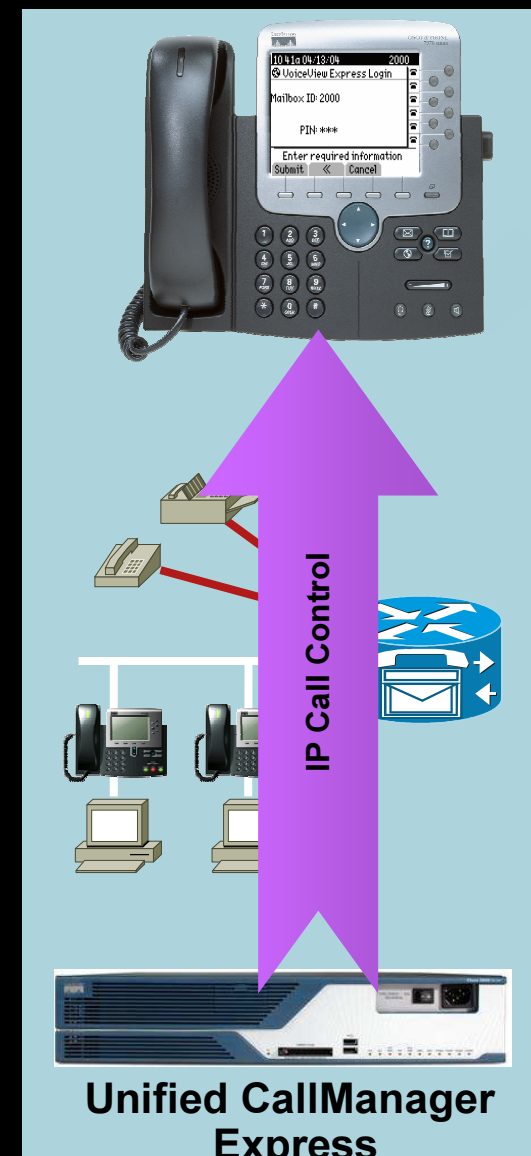


Cisco Unified CallManager Express Version 4.0 Enhancements to Legacy Telephony Features



- **ACD, AA & Hunt Group Enhancements**
 - Dynamic registration with Huntgroups
 - Huntgroup logon / logoff (normal calls still allowed)
 - Improved waiting call notification
 - Enhanced B-ACD Reporting in EXCEL Format
- **Conferencing Enhancements**
 - Retain conference call when conference initiator drops
- **Call Forwarding, Park, Transfer Enhancements**
 - Night Service Call Forwarding
 - Park Call Recall
 - Dedicated Park Slot per extension
 - Call Transfer blocking
 - Class of Restriction: Forced Authorization for Toll calls
- **Enhanced Phone Features**
 - Distinctive Ring Patterns for Internal or External Calls
- **Integration with Legacy PBX**

Support for QSIG protocols to communicate with TDM-based PBX's



E Cisco Unity Express Modules



NM-CUE or NM-CUE-EC

- Voice message storage: 100 hours
- Session/port capacity – 8 or 16
- Up to 250 mailboxes supported
- Hard Drive – 20GB, 500 MHz processor, 256MB/512MB DRAM



AIM-CUE

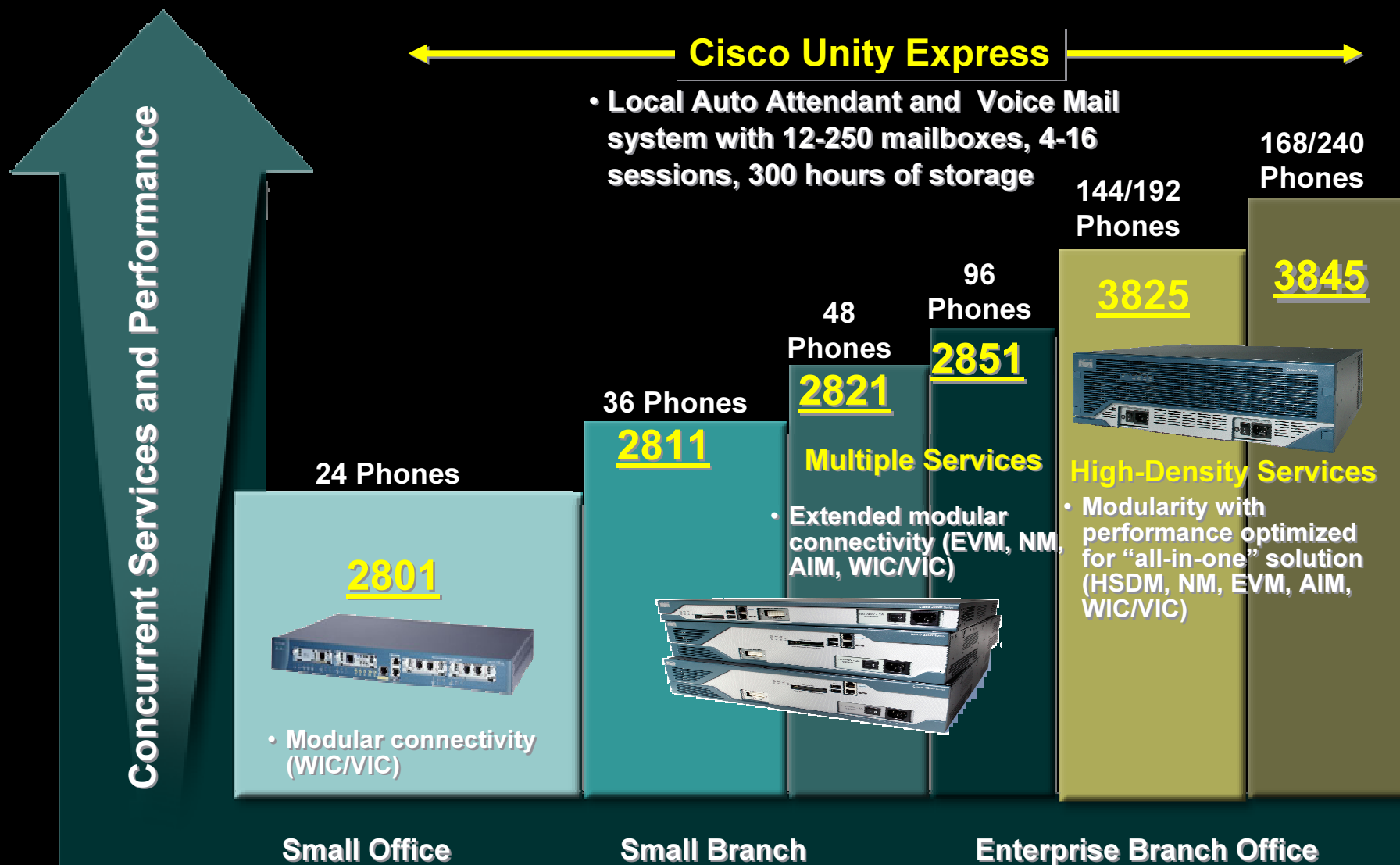
- Voice message storage: up to 14 hours beginning with release 2.0
- Session/port capacity 4 or 6 depending on router
- Up to 65 mailboxes supported
- Industrial Grade Compact Flash –1 GB beginning release 2.0 – 300 MHz processor, 256MB DRAM

E Cisco Unity Express Sizing Options

		12 Mboxes	25 Mboxes	50 Mboxes	100 Mboxes	150 Mboxes	200 Mboxes	250 Mboxes
# Total M'boxes		17	35	65	120	175	225	275
NM-EC	# Hrs Storage	300	300	300	300	300	300	300
	# Ports	16	16	16	16	16	16	16
NM	# Hrs Storage	100	100	100	100	not supported	not supported	not supported
	# Ports	8	8	8	8	not supported	not supported	not supported
AIM-1G	# Hrs Storage	14	14	14	not supported	not supported	not supported	not supported
	# Ports	4/6	4/6	4/6	not supported	not supported	not supported	not supported



IP Communications Express Product Portfolio



F Integrated Wired/Wireless LAN Access

Business Problem

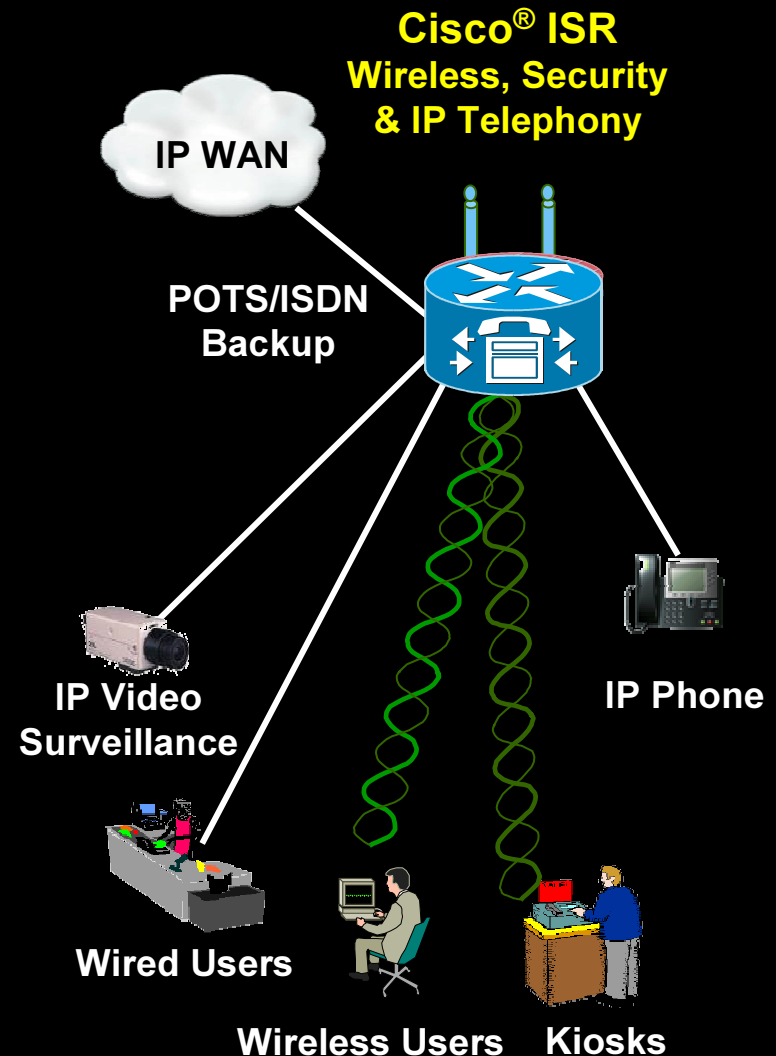
- Mobile access to critical applications and data throughout the site, while maintaining security

Solution

- Integrated Wireless Access Points and Structured Wireless Aware Networks

Benefits

- Convenient, easy-to-deploy integrated access points
- Rogue access point detection to protect against unauthorized access
- Authentication: 802.1x Cisco LEAP, PEAP-MSCHAPv2, PEAP-GTC, EAP-TLS, and EAP-FAST
Local LEAP authentication takes over if RADIUS server is down
- Encryption: TKIP encryption and support for static & dynamic 802.11 WEP keys
- State-of-the-art network management via CiscoWorks Wireless LAN Solution Engine





Controlled Access to Network Assets:

802.1X

- New NME 16, 24 and 48 port EtherSwitch modules support 802.1x authentication and NAC

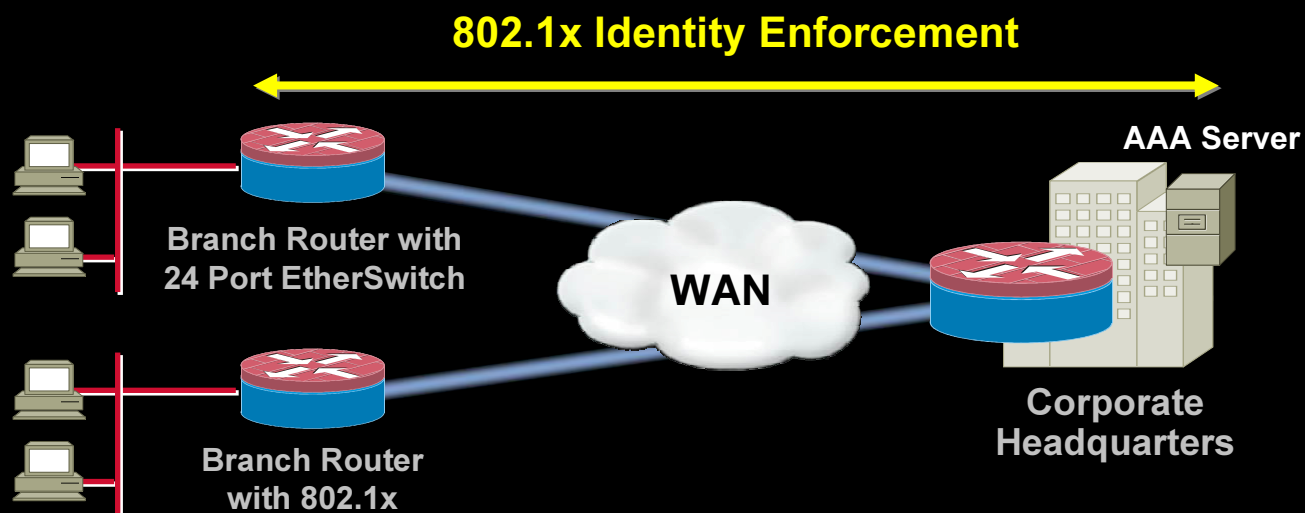
Smaller port density HWIC4-9 supports only basic 802.1 authentication and L3 NAC in router

- Plus Power over Ethernet (POE) 802.3af
- Controls who gets access to the network



NME-ESW

16, 24 and 48 Port
10/100 EtherSwitch

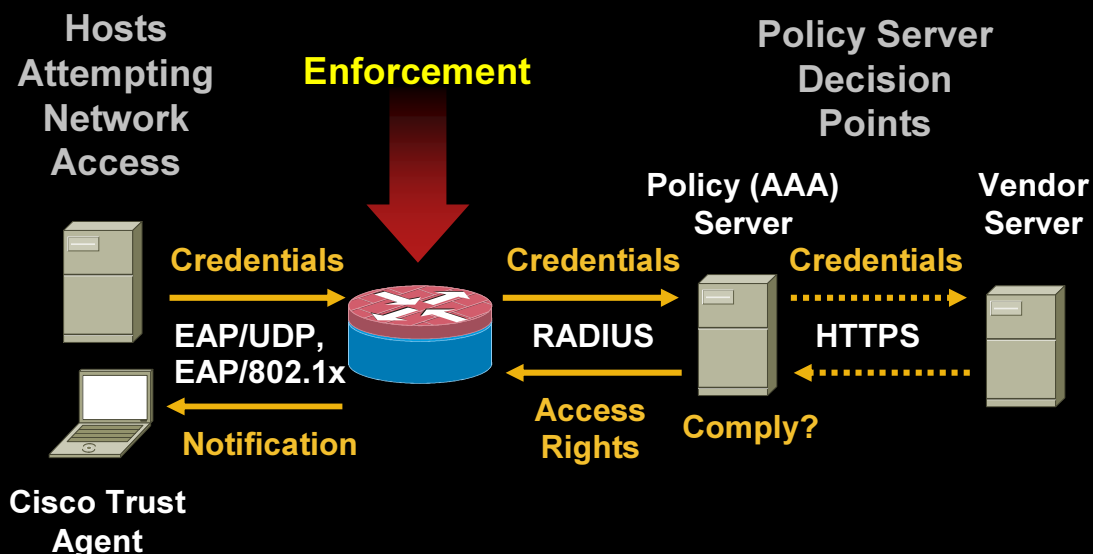




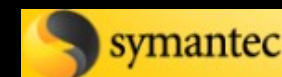
Detection and Isolation of Noncompliant Devices: **Network Admission Control**

- Enforces access privileges based on endpoint security posture
 - Allows compliant, trusted endpoints only
 - Restricts network access by noncompliant devices
- Limits damage from viruses and worms
- Supports multiple AV vendors and Cisco® Security Agent
- The Cisco 3800, 2800, and 1800 ISR Security Bundles ship with NAC capability

**Winner Network Magazine
2005 Innovation Award**



Coalition of Market-Leading Vendors



www.cisco.com/go/nac

Q and A



