ENTERPRISE CLASS TELEWORKER VPNS: DYNAMIC MULTIPOINT VPN

SECURITY TECHNOLOGY GROUP
NOVEMBER 2004

ENTERPRISE CLASS TELEWORKER (ECT) VPNS OVERVIEW

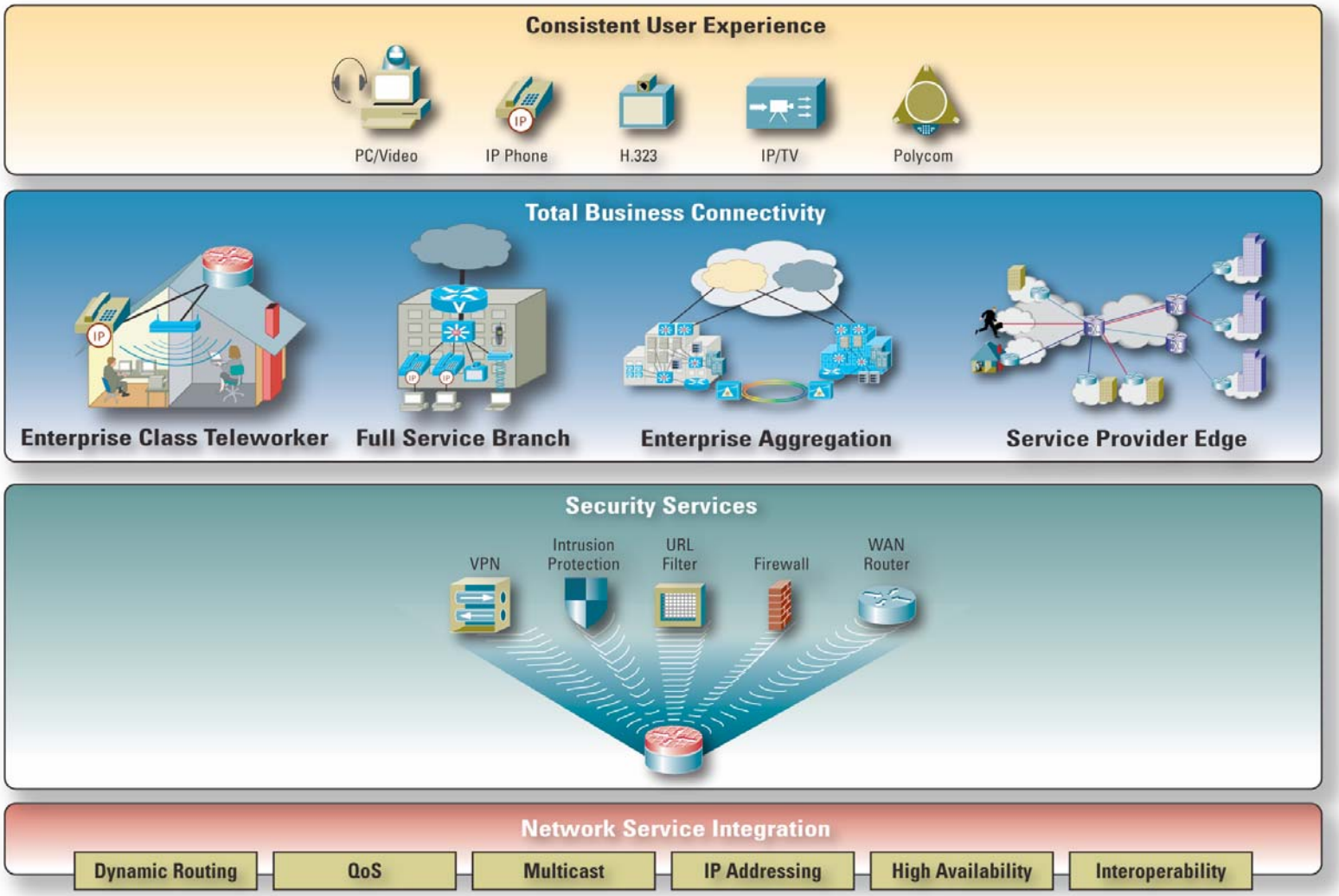
What is “ECT”?

- Cisco IOS® VPN connectivity solution that focuses on layers of security, network integration, and management
- Site-to-site VPN applications:
  - Frame Relay to IP VPN migration
  - IP VPN as alternative to ISDN backup
- SOHO / Telecommuter VPN applications:
  - V3PN-enabled connectivity

Requirements Addressed

- Encryption of voice, video and all multimedia applications
- Solution based on Public Key Infrastructure (CA)
- End-to-end solution that work well for both spoke-to-hub and full mesh (spoke-to-spoke - future functionality) scenarios
- Covers the remote access and site-to-site solution in one box
- A single box that can provide all the features and services (Security, VPN, IP Services)
- Central management network that can fully manage and deploy a full functionality, end-to-end solution
- Secure solution that can deploy and manage seamlessly
    - Lowers TCO by eliminating end-user intervention

The Vision Behind ECT ....



ECT Technology Overview

Cisco.com

ECT

Connectivity

Enterprise Class Teleworker

- Cisco 830 Router, Cisco 1700 Series

Full Service Branch

- Cisco 1700, 2600, 3700 Series Router

Enterprise Aggregation

- Cisco 3700 and 7200 Series

Service Provider Edge

- Cisco 7200 Series

Security

Public Key Infrastructure

- PKI-AAA Integration
- Auto Enrolment
- Multiple Trust Points
- Secure RSA Private Key

Device and User Authentication

- Secure ARP
- Authentication Proxy/802.1x

Stateful Firewall

Intrusion Protection

Network Integration

DMVPN

- Dynamic Addressing for Spoke-to-Hub
- On-Demand Spoke-to-Spoke Tunnels (future)

V^{3}PN

- QoS
- VoIP
- Video
- Multicast

Resiliency

- Self-Healing and Load Balancing

Scalability

- Full Mesh up to 700 Sites

Management

Touchless Provisioning (ISC)

- Bootstrap PKI Certificates
- Dynamic Addressing and Call Home
- Policy Push for IPsec, QoS, Firewall, IDS, NAT, Routing
- Hub-and-spoke, full and partial mesh topologies

Ongoing Management (ISC)

- Management Tunnel
- Configuration Change Notification
- Audit Checks

ECT Benefits – IT

- Centralized management of services running on remote devices (ie: IP Routing, QoS, IPsec, Firewall)
- Single deployment model fits site-to-site and remote access VPN — SOHO thru Branch thru HQ
- Allows phased migration from existing WAN infrastructure

Reduced complexity and costs

ECT Benefits – End Users

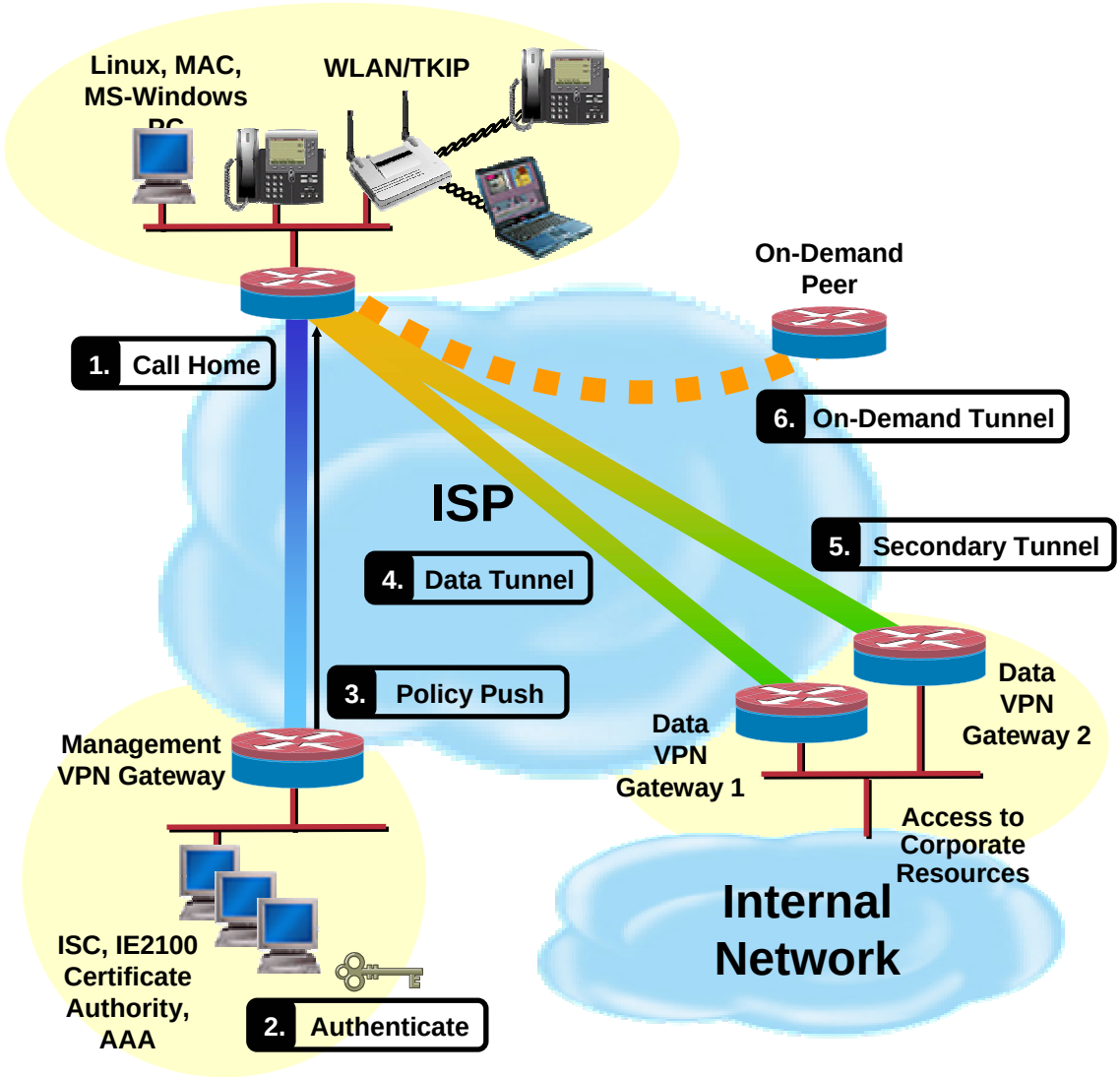
- Collaborative voice, video, and data applications made possible
- Consistent user experience whether at branch, SOHO, or headquarters
- Layers of security and authentication provides worry-free environment

Increased security and productivity

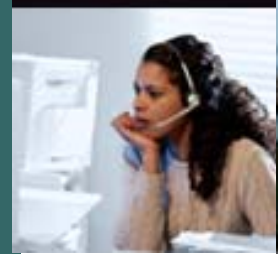
ECT Connectivity Cross-Section

1. Remote routers “call home” and management tunnel is set up
2. Management server authenticates remote router using certificate authority and AAA servers
3. Management server pushes policy including new certificate
4. Remote router establishes primary data tunnel, access to corporate resources
5. Secondary tunnel established, stays active for instant failover
6. When required, remote router establishes direct spoke-to-spoke tunnel with other authorized remotes

   Tunnel torn down after use



SECURITY



ECT Security Overview

- **Support for Public Key Infrastructure (PKI) and shared passwords**
- **Protection against router being stolen or hacked into**
- **Stateful firewall and IDS included**
  - **Supports off-board URL filtering**
  - **Supports authentication proxy/802.1x for wireless / split tunnel**
- **AAA database integration**

ECT – Layers of Security

Feature	Benefit
CNS Bootstrap Call Home	Forces newly provisioned remote routers to “call home” to management server
Public key infrastructure support	Digital certificates can be used to authenticate routers, providing greater scalability
Secure management tunnel	Proactive notification if configuration has been tampered with. Also allows periodic audit checks
Secure RSA private key	Guards against router being stolen or misused—private key is erased if password recovery attempted
PKI—AAA integration	Credentials stored centrally on AAA server, allowing quick addition and deletion of devices with a single entry
Authentication proxy/802.1x	User-level authentication especially useful in split-tunnel scenarios
IOS Stateful Firewall	Deep packet inspection maintaining state information per application, off-board URL filtering support
Intrusion Protection (IOS IDS)	101 signatures, combines with IOS stateful firewall to perform deep packet inspection with a single lookup

New!

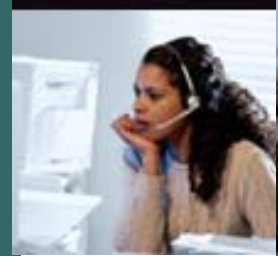
Auth Proxy / 802.1x Port-Security Solution

- **Auth Proxy prompts the user for login/passwd when attempting to connect to the corporate network via http/ftp and telnet**
- **802.1x based authentication mechanism is extended to allow employee and family to share the same access router**
- **When a PC is connected to the spoke router, user will be prompted for credentials**
  - **User with right credential will be allowed to go to Intranet**
  - **Other users will only have access to Internet**

802.1x Phase-2

- Phase 2 will support EAP-TLS (certificates) apart from the EAP-MD5 which is already supported
- Larger platforms will be supported (ie: Cisco 3600 Series Router)

NETWORK INTEGRATION



ECT - Network Integration Overview

- **DMVPN**

  Virtual full mesh – IPSec with dynamically configured routing protocols

  Dynamic spoke-to-spoke tunnels allows solution to scale, supports distributed applications

  Dynamic discovery of spoke-to-hub tunnels allows painless addition of new spokes

- **V^3PN**

  IP telephony over VPN through integration of VPN, Voice and QoS

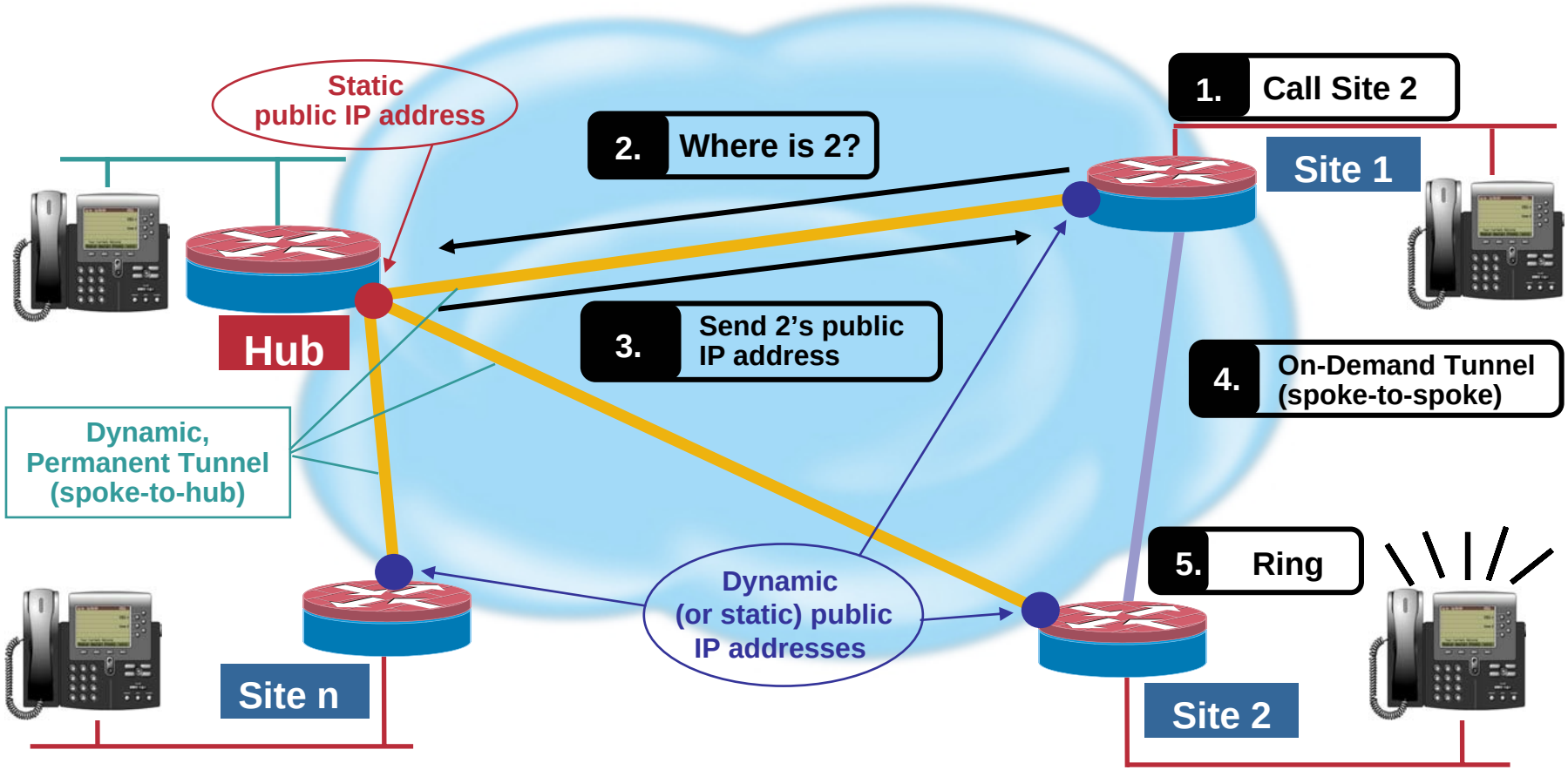
- **Resiliency**

  Load balancing and self healing

DMVPN

Feature	Benefit
Virtual full mesh	Industry first—Allows IPSec with routing protocols to be dynamically configured
On-demand spoke-to-spoke tunnels	Industry first—Optimizes performance, reduces latency for real-time traffic
Dynamic discovery of spoke-to-hub tunnels	Minimizes hub configuration and maintenance
QoS, multicast support	Latency-sensitive applications e.g. voice and video
Tiered DMVPN	Allows preferential treatment of users, simplifies configuration, improves scalability
Enhanced scalability	Load balancing doubles price-performance, single hop spoke-to-spoke, tiered DMVPN

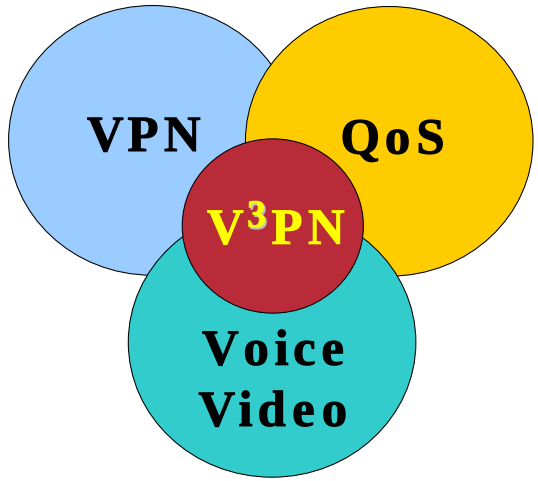
DMVPN: Automeshing with Dynamic Routing



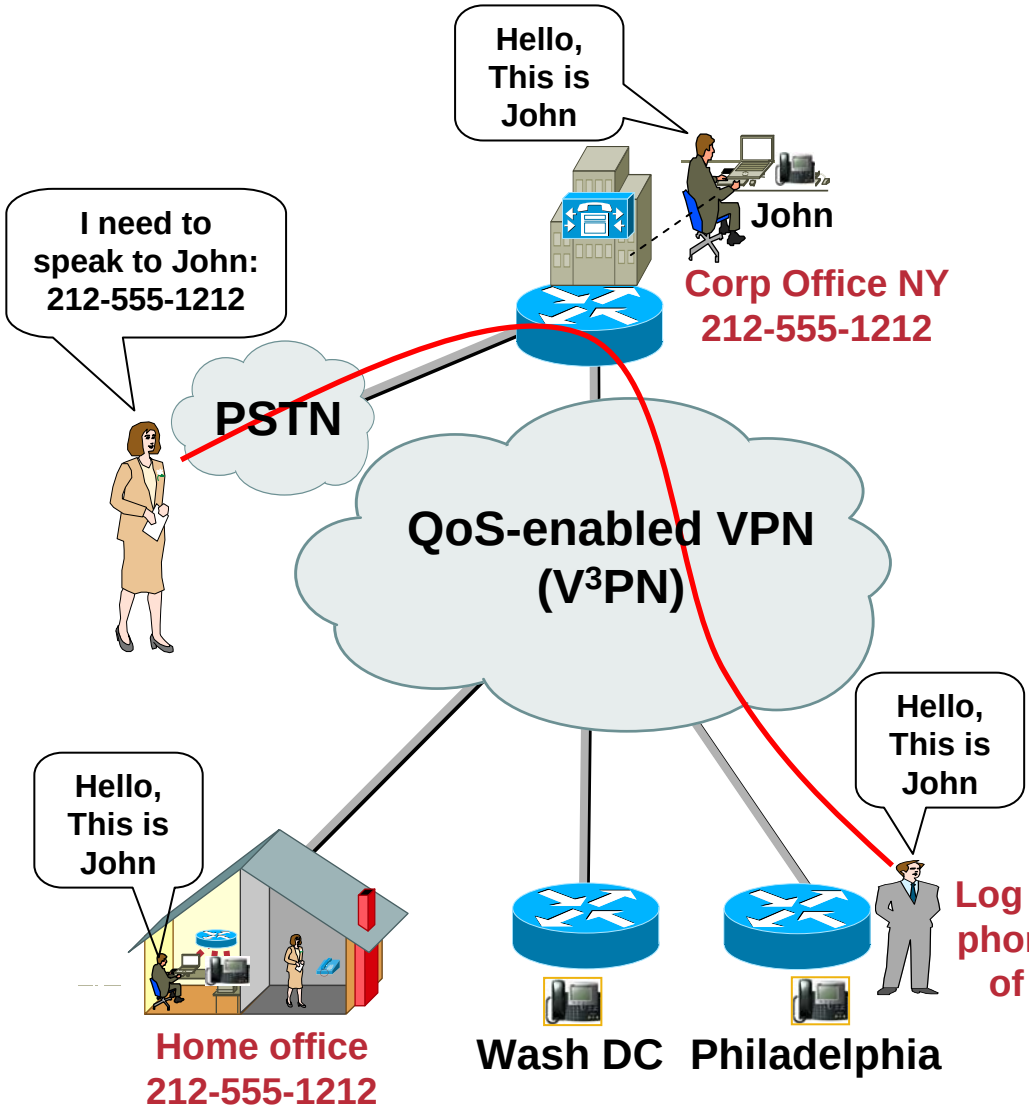
- Reduced latency and jitter
- Improved performance
- Increased scalability
- Easy to deploy and maintain

V³PN—Voice and Video Enabled VPN

- **Fully functional, cost-effective remote working environments**
  - Securely extend the corporate PBX to home offices for full-featured teleworker solutions
  - Deliver secure IP video for videoconferencing and training
- **Enhanced security for voice and video traffic over the WAN**
  - Encryption of voice and video streams, authentication of gateways
- **IP telephony + VPNs = Greater cost savings**
  - Combining IP telephony and video with VPNs reduces bandwidth and telephony expenses
  - Extending converged communications to remote sites or users increases productivity



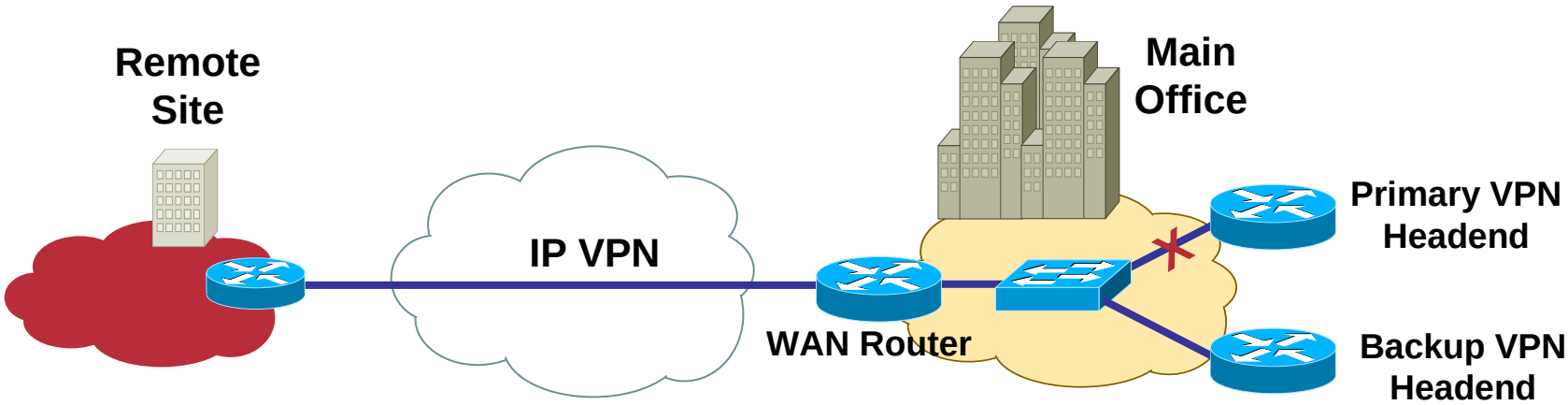
V³PN—Voice and Video Enabled VPN



- **Consistent user experience**
  - Same network connectivity at home as in corporate office (data, voice and video)
- **Lowers costs and increases teleworker productivity**
- **Service provider partners with networks built with Cisco products carry voice and video with toll-quality SLAs**

ECT – Failover/Resiliency

Non-stop VPN Connectivity

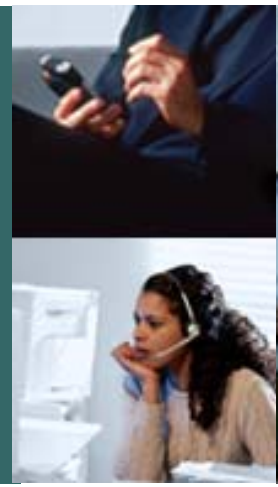


Feature	Benefit
DMVPN load balancing	Doubles performance at given price point while providing resiliency
DMVPN self-healing	Reroutes around link failures, maximizes uptime

New!

New!

MANAGEMENT

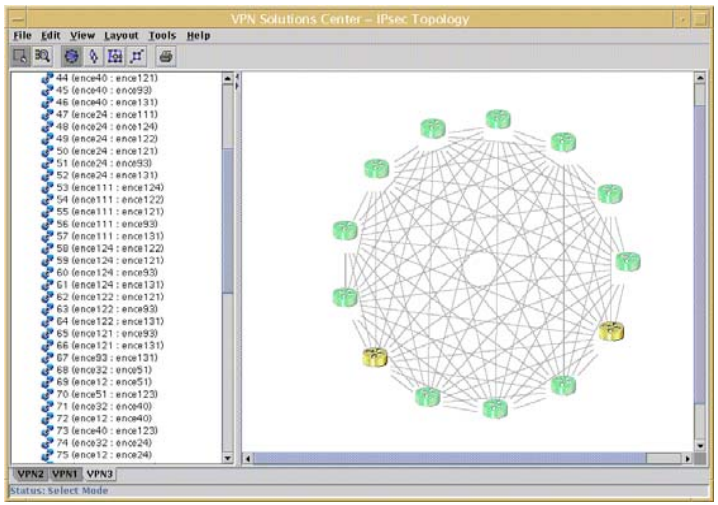


ECT - Management Overview

- **Touchless provisioning of DMVPN, IKE/IPSec, NAT, QoS, Firewall, IDS**
  - **Including split tunnel, redundant configurations**
- **Bootstrapping and call home**
  - **Automatic registration and policy push, no user intervention**
- **Management tunnel facilitates outsourcing of management**
- **Dynamic discovery of spoke-to-hub tunnels**
  - **Add spokes without changing hub configuration**
- **Dynamic spoke-to-spoke tunnels**

Cisco VMS- IP Solution Center 3.1: Carrier-Class Network and Service Management

Cisco.com



- Site–to-site VPN
- Remote Access VPN
- DMVPN
- Easy VPN
- Managed firewall
- NAT
- Managed IDS
- Network-based IPSec

Device Abstraction Layer

IOS Router | PIX® Appliance | VPN 3000 | IDS

New!

- Hub-and-spoke, full and partial mesh topologies (DMVPN)
- Design and deploy complex firewall rules
- Cisco IOS IDS provisioning and tuning
- Integrated routing—OSPF, EIGRP, RIP
- Automate provisioning of failover and load balancing
- QoS provisioning
- Massive NAT configuration deployment
- PKI-based end-to-end authentication and audit checks

Cisco VMS IP Solution Center 3.1 – Carrier Class Network and Service Management

- **Provisions and manages Cisco IOS Software, PIX, 3K devices and their services**
- **Multiple transport mechanisms**
  - **Telnet / tftp / ftp**
  - **SSH**
  - **CNS-CE**
- **CNS-CE Features**
  - **Asynchronous provisioning: if router is inaccessible during provisioning, provisioning resumes automatically when router becomes accessible**
  - **Asynchronous notification of events: config-change, connect, disconnect, etc.**

Cisco VMS IP Solution Center 3.1 – Carrier Class Network and Service Management

- Generates Bootstrap Configs; downloads to startup-config
- Image management – copies images to flash
- Reloads
- Sophisticated Templates for provisioning enhancements
- Scales to a very large number of devices
- Provides SLA provisioning, collection, and reporting

Cisco VMS IP Solution Center 3.1 – Carrier Class Network and Service Management

- **Migrates existing users to ISC**
- **Uploads/downloads from/to many devices concurrently via groups**
- **Adds/removes/modifies existing services on multiple devices in one operation**

Cisco VMS IP Solution Center 3.1 – Carrier Class Network and Service Management

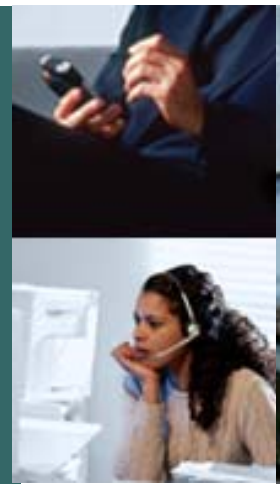
Fully managed solution

- Optional per device
- Keeps track of last event (connect/disconnect)
- Email is sent for connect/non-isc-config-change event
- Audit is triggered for connect/non-isc-config-change event
- Successful audit – done
- Failed audit:email with payload is sent
- Failed audit: unix script is optionally called

Cisco VMS IP Solution Center 3.1 – Carrier Class Network and Service Management

- **Fully Managed fully protects HQ from router breakins, intrusions, etc.**
- **Fully Managed continuously ensures router integrity**
- **Fully Managed takes immediate action upon improper operation**
- **Fully Managed disconnects mis-behaving router/user from HQ**

CISCO IT DEPLOYMENT



Cisco Internal ECT Solution

IT Operations Requirements

- **Touchless deployment: eliminate end-user involvement**
- **Maximum security and authentication: protect against theft or tampering with remote device**
- **Centralized management of remote devices: all services including routing, QoS, IPSec, firewall, etc.**
- **Future migration of branches to VPN using same design: spoke-to-hub and full mesh spoke-to-spoke**

Reduced complexity and risk for operations staff

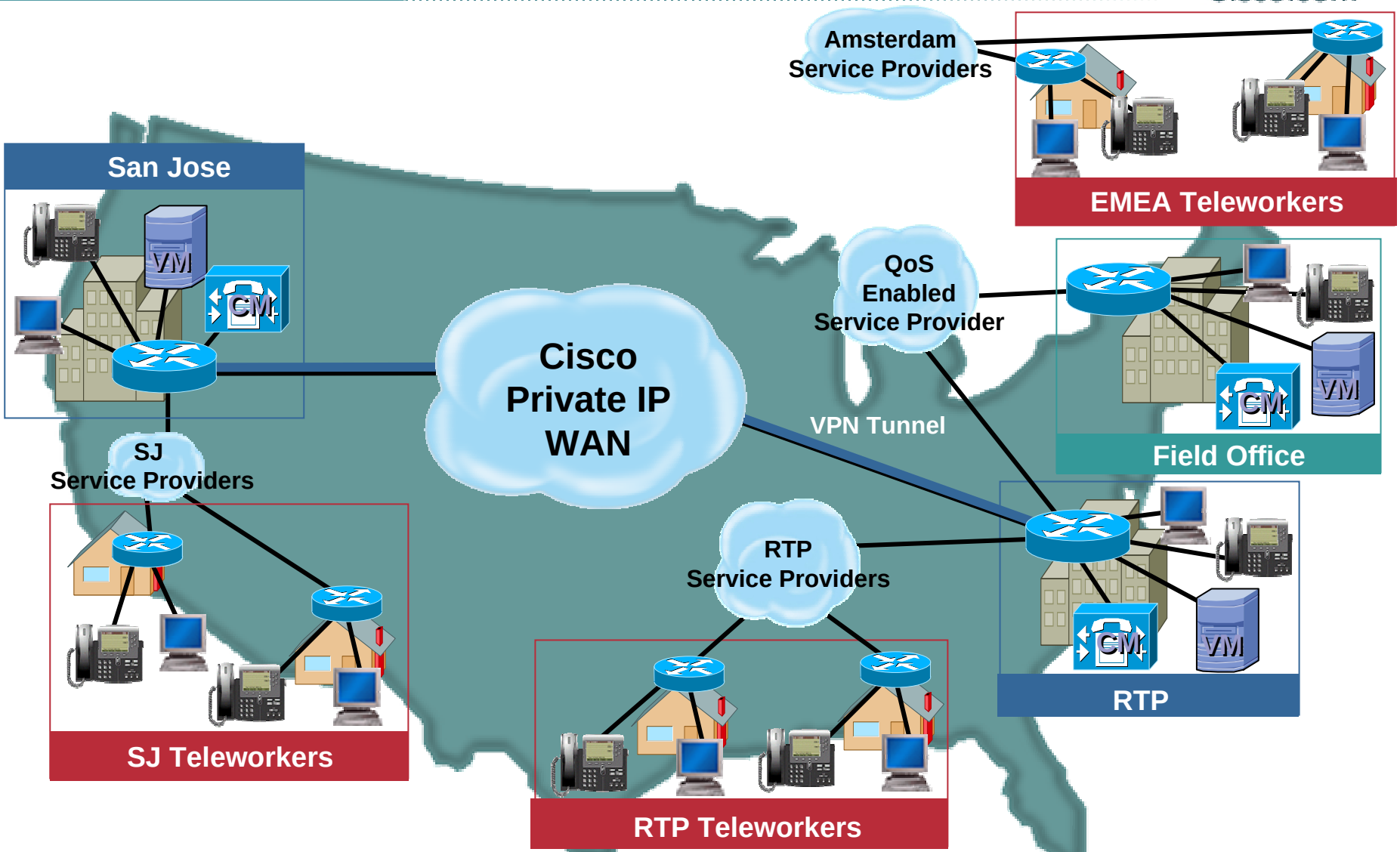
Cisco Internal ECT Solution

End-user requirements

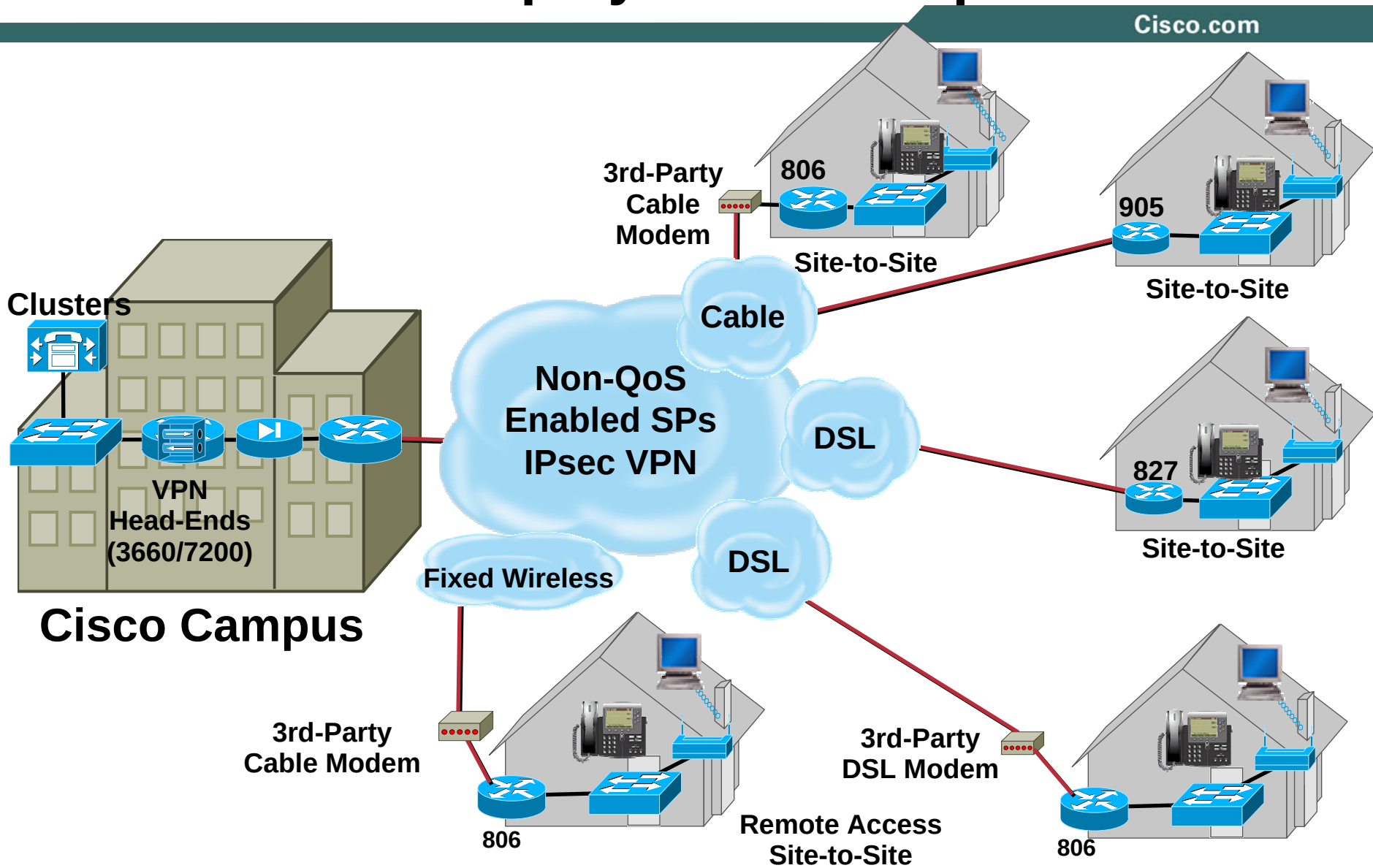
- **Regular Users**
  - **Need consistent access to content at home or work**
  - **Includes Windows and non-Windows devices**
- **Full-time telecommuters**
  - **Require the same IP telephony as at corporate site**
  - **Includes executive assistants, senior management, TAC, engineering, marketing personnel**
  - **Avoid hassles of expensing home phone bills**

Increased workday productivity
Lowered expenses for home telephony

ECT Global Deployment



Cisco Teleworkers
Current ECT Deployment Examples



ECT - USA ISPs Tested

Cisco.com

1. AT&T Cable Modem
2. Sprint Broadband
3. Earthlink DSL
4. SBC/PacBell DSL
5. DirectTV DSL
6. Telocity DSL
7. Speakeasy IDSL
8. UUNET DSL
9. Charter Communications
10. Time Warner/Road Runner Cable
11. Verizon DSL
12. Cox Cable
13. Covad Communications
14. Starband Satellite Network
15. Verizon Online
16. Qwest DSL
17. Prexar
18. Guadalupe Valley Telephone Coop - DSL (CPN)
19. SBCIS DSL

ECT - EMEA ISPs Tested

1. France Telecom Netissimo/Wanadoo DSL – France: DSL (PPPoE)
2. PT Prime/Telecom – Portugal: DSL (PPPoE) and Cable [DHCP]
3. KPN MxStream – Netherlands: DSL (PPPoA)
4. Belgacom (Skynet, ADSL service 1M/128K) – Belgium: DSL (PPPoE)
5. Telenor Nextra – Norway: DSL (PPPoE)
6. Telecom Italia – Italy: DSL (PPPoE)
7. Telefonica – Spain: DSL (PPPoA)
8. Deutsche Telecom – Germany: DSL (PPPoE)
9. British Telecom - United Kingdom: DSL (PPPoE)

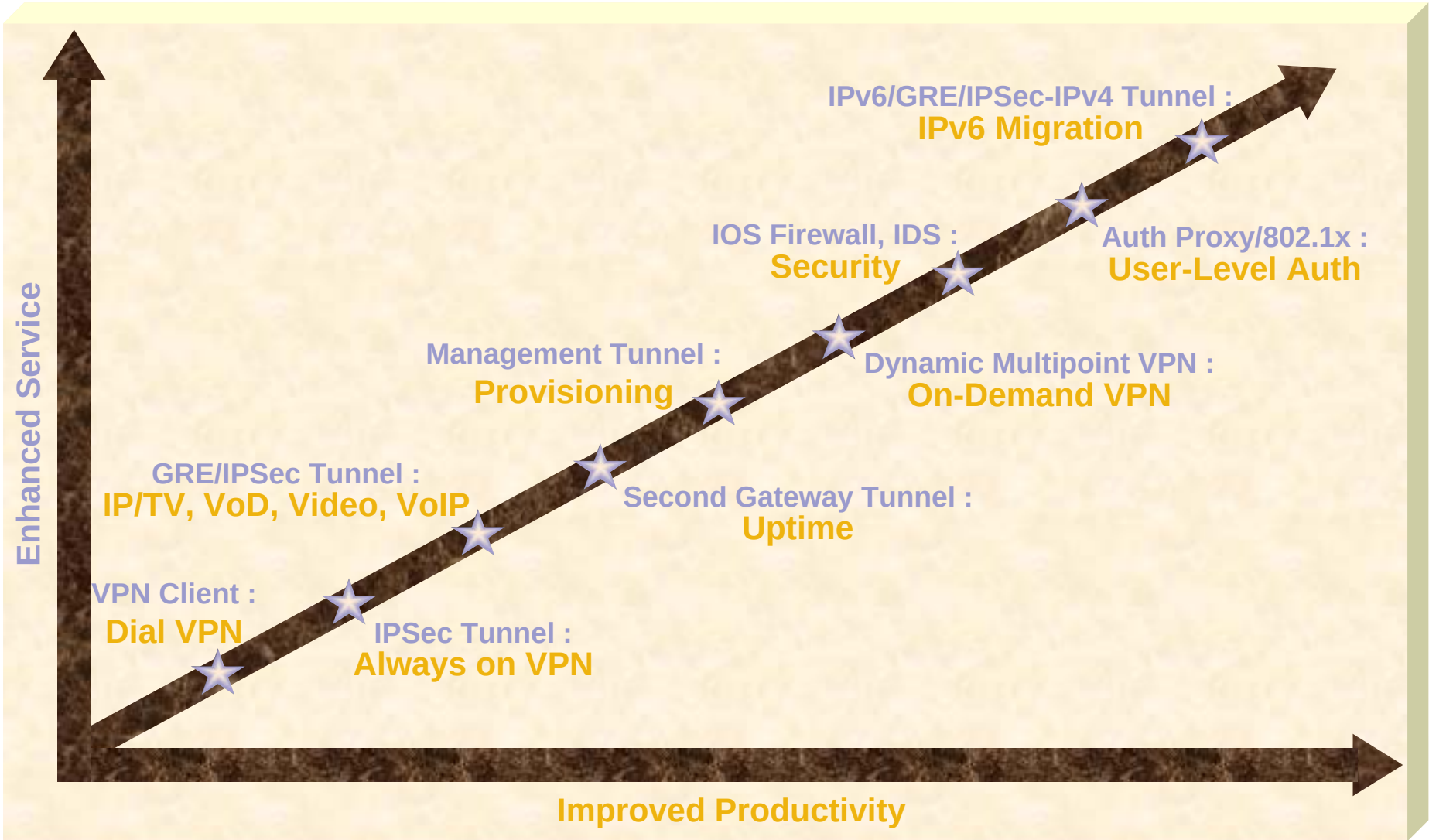
   Currently under deployment

ECT - Hardware Deployed

- **Hardware tested on the SOHO**
  - **Cisco 1710, 1751, 1760 Routers,**
  - **Cisco 2600 and 3600 Series Routers**
  - **Cisco 831, 836, 837 Routers**
- **Hardware tested on the Gateway**
  - **Cisco 3725, 3745 Routers**
  - **Cisco 7200 VXR (with VAM-2) Router**
- **End devices already tested**
  - **Computers – PCs, Laptops, Macintosh**
  - **IP phones (hardware, wireless and Cisco SoftPhones)**
  - **Wireless Access Points**
  - **UNIX and LINUX systems**

Services Evolution—Generating Increased Productivity

Cisco.com



Cisco Teleworker Solution ROI

Cost of Equipment

+ Installation
+ Infrastructure
+ Support
+ WLAN Client Adapter
+ Other

≈ $1500 (yr 1) + $900 (yr 2)

≈ $4 – $6 per day per user

Employee Time Savings

+ Salary
+ Benefits
+ Furniture, Equipment
+ Allocated Expenses
+ Other

≈ $120K – $300K / yr / user

≈ $1 – $3 per *minute* per user

Employee Productivity = Savings

ECT Roadmap

- **Continue production deployment to 1000+ users**
- **Expand features and scope using test network**

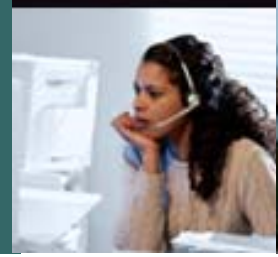
  Added capabilities include 802.1x authentication, Cisco IOS Software certificate server, Dynamic IDS/CNBAR support

- **Document and share best practices**

  ECT VPN Configuration Guide

  www.cisco.com/en/US/netsol/ns110/ns170/ns172/ns271/networking_solutions_implementation_white_paper09186a008012b60d.shtml

SUMMARY



ECT Summary

- **Same deployment model scales across HQ, branches, home / road warriors**
- **Cisco IOS ECT VPNs are NETWORKS**

  Fully supports voice, video and data with routing, multicast, high availability, QoS, and security
- **Low risk migration for VPN rollout leveraging existing infrastructure**

  Migration path from Layer 2 WANs, ISDN Backup
- **Same skills and experience for deployment, management and operational carry through to all network segments and devices; “small, medium, large and x-large”**
- **Scalable management solution gluing the system together**

QUESTIONS?