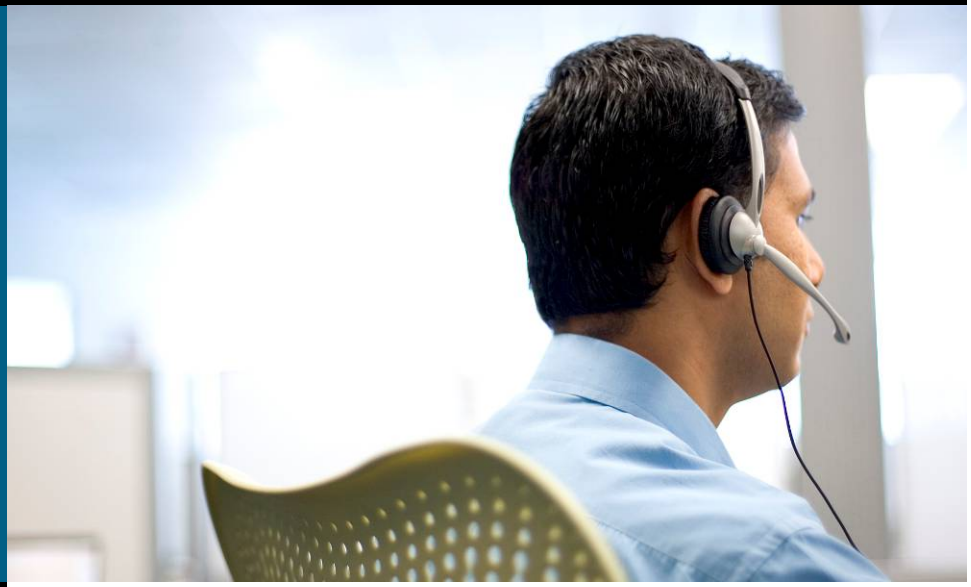
Enterprise Class Teleworker (ECT)



Plamen Nedeltchev, Ph. D.
Member of Technical Staff, ECT Architect

The Cisco Network Infrastructure

We Face the Same Challenges as Our Customers

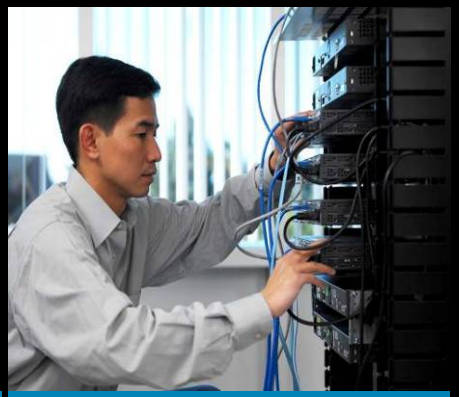
Versatility

Functionality

Performance

Total Cost of Ownership

Security



Simplicity - Ease of Deployment and Management

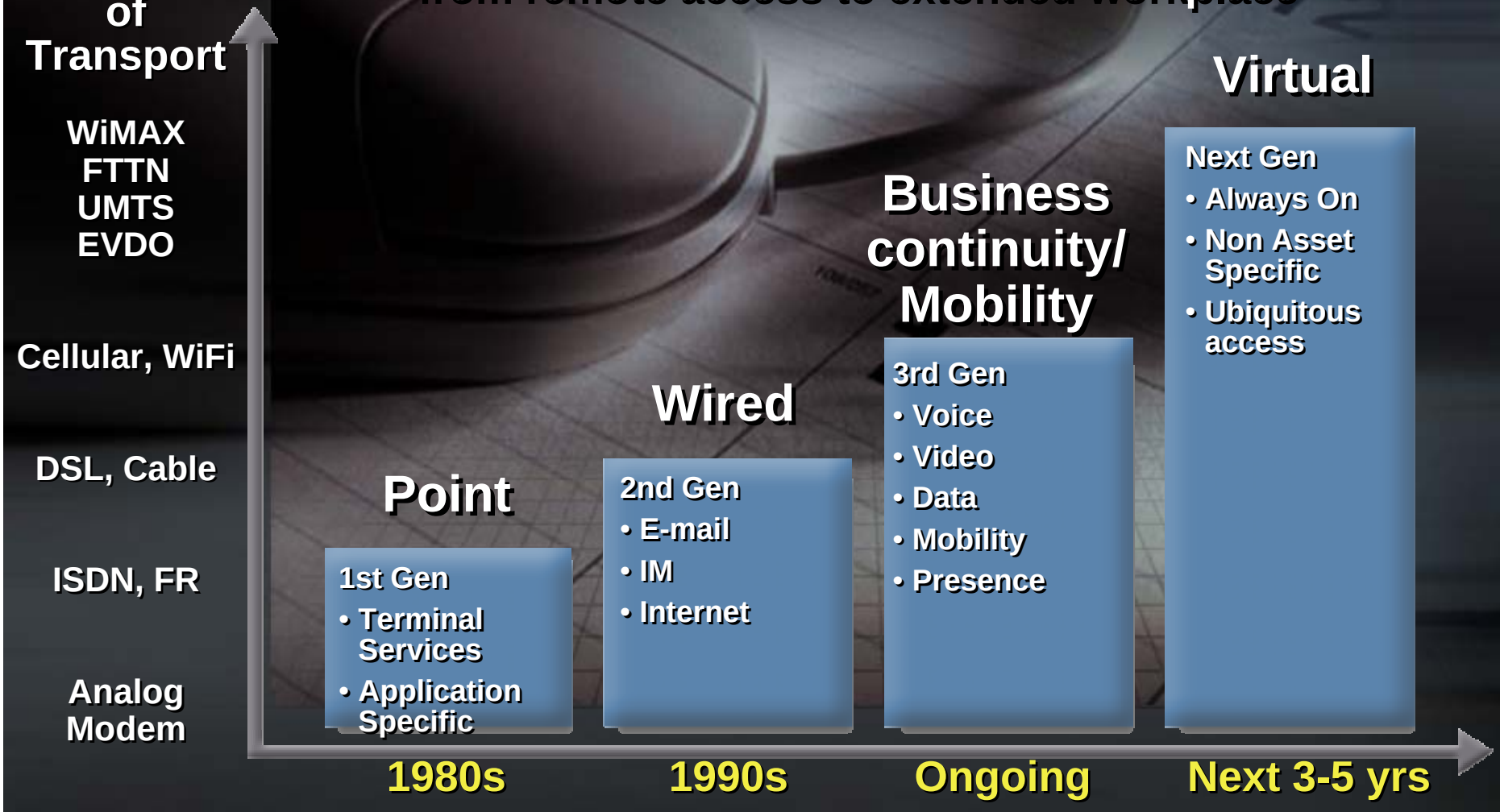
How Big is Cisco?

- 312 locations in 90 countries
- 400 buildings
- 50 data centers and server rooms
- 1000+ labs worldwide (500+ in San Jose)
- 50,000 employees
- 30,000 contractors
- 20,000 channel partners
- 110+ application service providers
- 210+ business and support development partners

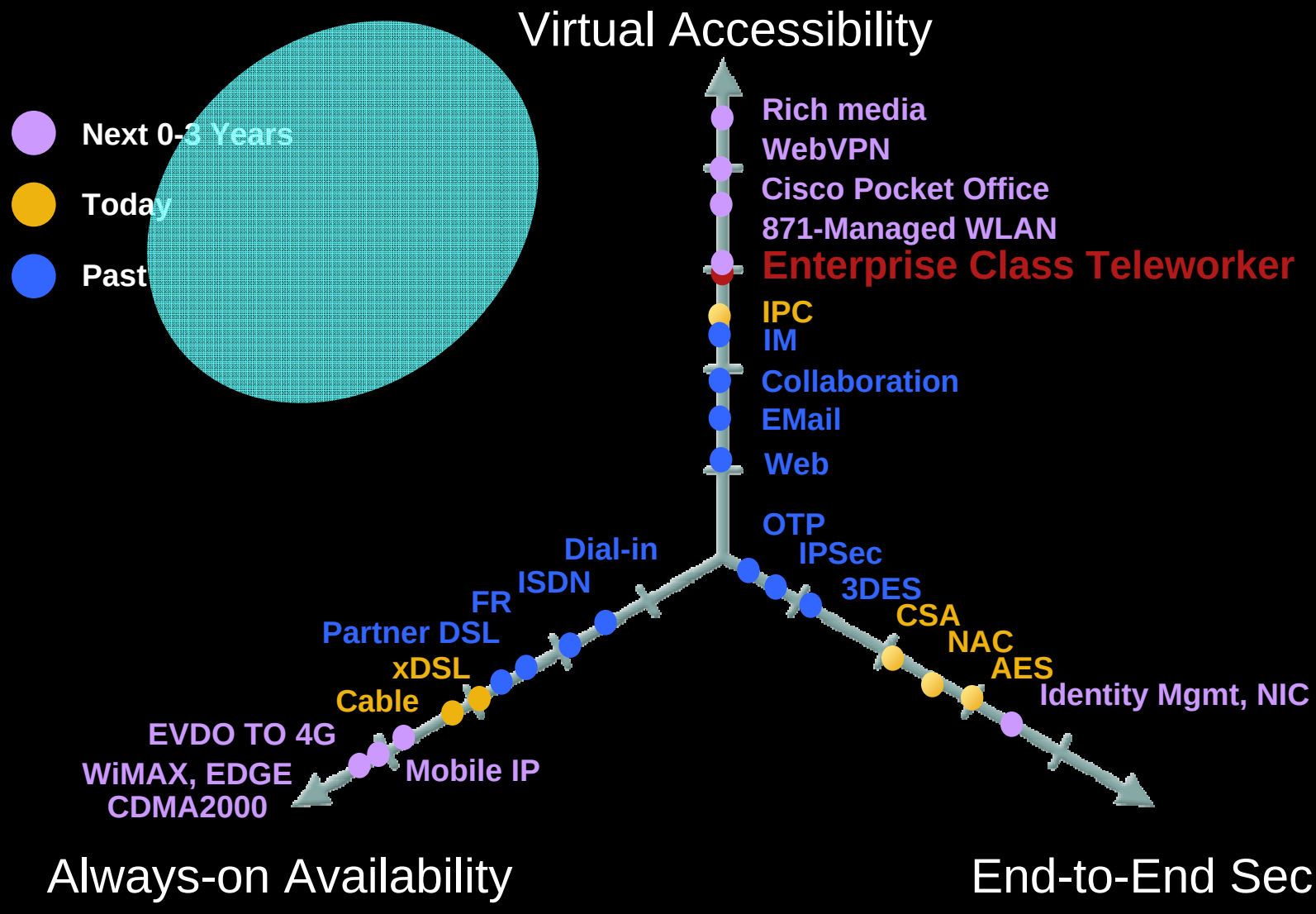
Over 150,000 People around the World in the Extended Cisco Family

Remote Access: Where were we, where are we, where are we going?

Remote Access has evolved from business convenience to business critical, from technology to service, from remote access to extended workplace



Cisco's Path to Managed Remote Service. ECT positioning for Home, Branch, ISP, SMB

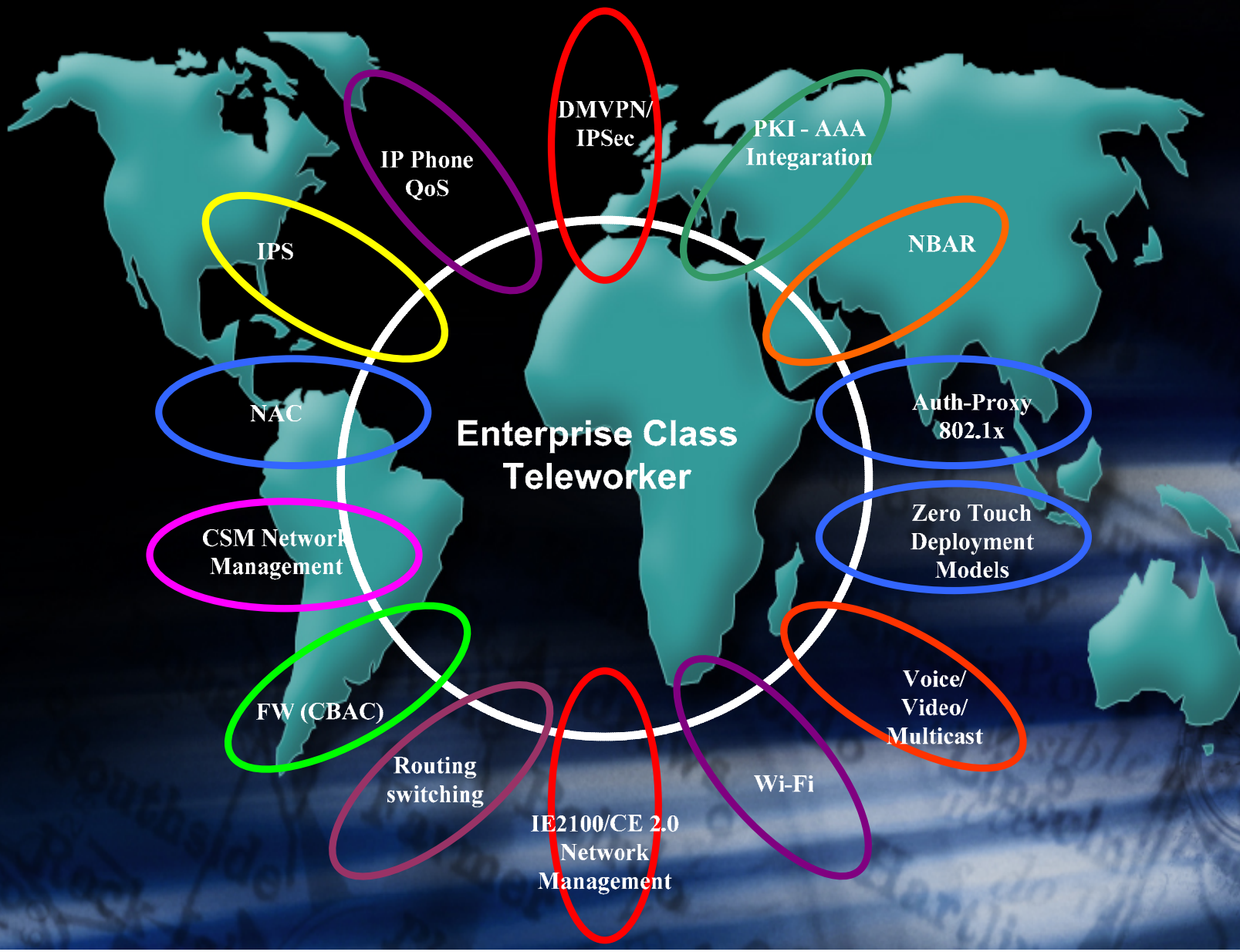


The Broadband Explosion

- Over the past year, the number of broadband subscribers increased 33% from 136 million in June 2005 to 181 million in June 2006.
- In June 2006, six countries (Denmark, the Netherlands, Iceland, Korea, Switzerland, and Finland) led the broadband penetration, each with at least 25 subscribers per 100 inhabitants. Denmark penetration rate of 29.3 /100 inhabitants.
- Fibre to the home is becoming increasingly important for broadband access. Japan leads fibre-to-the-premises (FTTP) with 6.3 million fibre subscribers in June 2006.
- The breakdown of broadband technologies in June 2006 is as follows: DSL 63%; Cable modem 29%; Satellite, Fibre and Fixed Wireless 8%.
- The United States has the largest total number of broadband subscribers at 57 million. Canada continues to lead the G7 group of industrialized countries in broadband penetration.

- SOURCE - Organization for Economic Co-operation and Development; www.oecd.org/sti/ict/broadband

Next Generation ECT Feature Set



ECT and End-to-End VPN Model and TCO

ECT Framework

End-to-End Security

Device and User Authentication and Anti-theft Protection

- Secure RSA Lock Key
- Secure ARP-proxy
- Auth-Proxy
- AAA IEEE 802.1X-AAA.

IOS-based PKI

- Certificate Server (CA&RA, Sub-CS modes)
- PKI-AAA Integration
- Auto-enrolment
- Multiple Trust Points

Underlying Security Features

- IPSec (3DES or AES)
- Stateful Firewall
- NBAR and IDS

End-to-end Connectivity

DMVPN

- Failover/Load-balancing
- Dynamic routing
- Full-mesh and partial-mesh topologies
- Hub-to-spoke and spoke-to-spoke tunnels. Permanent and on-demand tunnels
- mGRE, IPSec, NHRP. Transport and Tunnel modes
- Multiple DMVPN clouds per head-end router. Resiliency

Full Support of IP Applications

- Data
- VoIP
- QoS
- Wi-Fi
- Multicast
- Video

End-to-end Deployment

Configuration Automation Cisco Security Manager (CSM)

Cisco CNS 2100 Series Intelligence Engine:

- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Engine

Automated Zero Touch Deployment (ZTD)

- BootstrapConfiguration and PKI certificates (EzSDD)
- Off-line (ISC CA Proxy)
- In-house (RA engineer)

Automated Policy Deployment, Re-deployment and Audit

- DMVPN/ IPSec
- Firewall
- QoS
- NAT
- NBAR and IDS

End-to-end Management

Ongoing Management Cisco Security Manager (CSM)

Cisco IE2100-based CNS Notification Engine

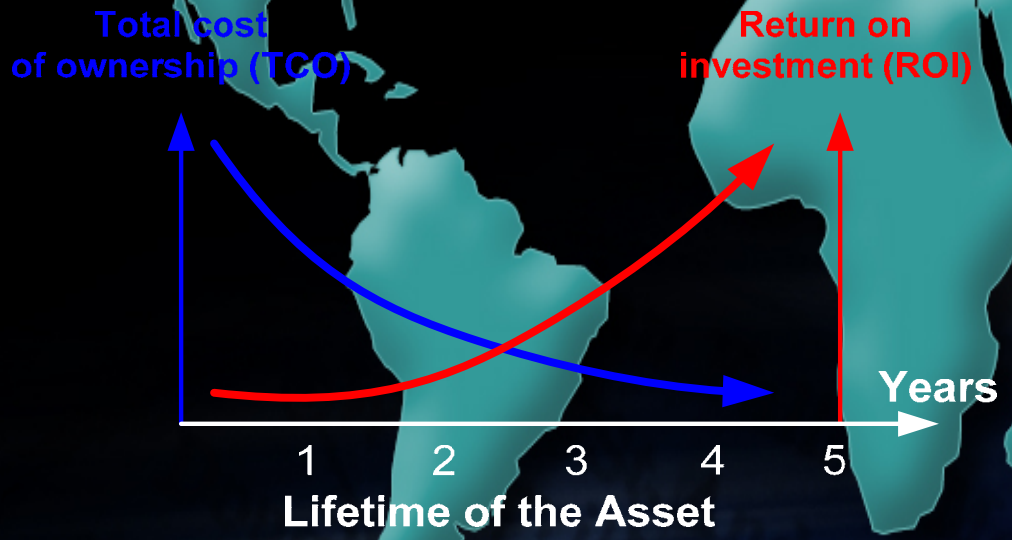
- CNS Configuration Engine
- CNS Notification Engine
- CNS Image Management Engine

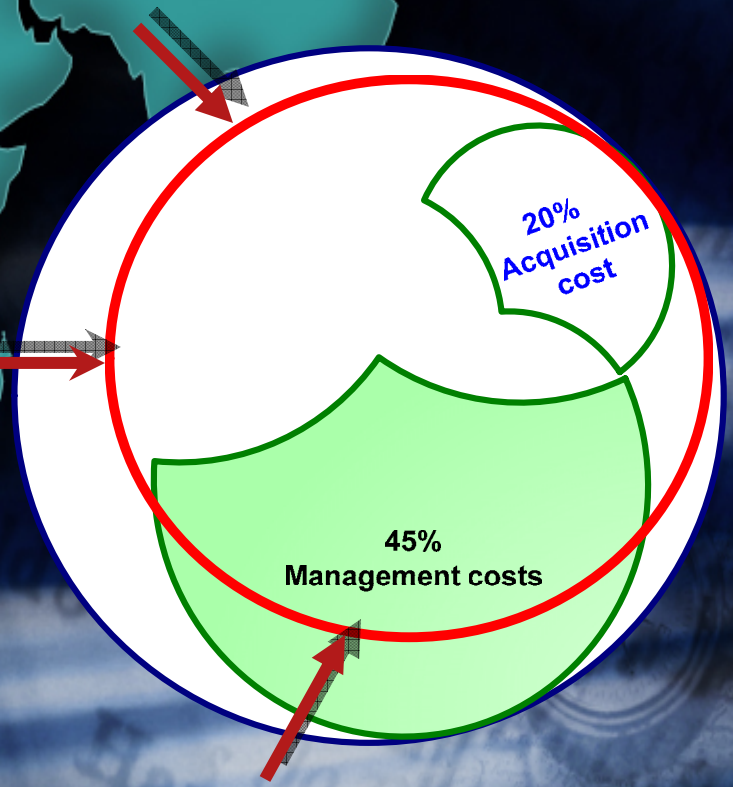
EMAN Framework Integration

- Automated user service application and entitlement
- Automated configuration/pre-configuration and audit
- Automated image management
- Automated control, monitoring and security management
- Interactive/Automated decision making and service termination
- Anti-virus, anti-worm and DoS protection (per identification)
- Automated event log management

End-to-end VPN Model Reduces TCO

Total cost of ownership (TCO) is the sum of acquisition costs, plus all the operational and support costs over the lifetime of an asset - generally 3-5 years. As TCO decreases, ROI improves TCO components.





Maintaining low TCO:

- Use Integrated Security Routers
- Maintain low cost of deployment
- Maintain low cost of management
- Use reusable components

ECT Not Only End-to-end but Global

Cisco IT Deployment
5 management hubs
11 pairs of data hubs
30,000+ expected users

Phase I Policies
DMVPN, FW
Auth-Proxy,
QoS, NAT

Phase II Policies
NAC, IPS,
NBAR, 802.1x

ECT Hub Environment
SMG1 – Cat65K (7206VXR, 3845)
SDG1, SDG2 – 7206VXR, 7301,
7600, Server Load Balancing
CERT1, REG1, and CERT2 – 3845
Cisco Secure Manager
Linux-based IE2100
ACS AAA server
EMAN Provisioning

Cisco Integrated Services Routers

The Right Router for Every Office

Markets

Enterprise

Medium Business

Small Business

Performance and Services Density

3800 Series

Highest Density and Performance for Concurrent Services

2800 Series

1800 Series

Modular

Fixed

800 Series

New Models for Small Offices

Embedded, Advanced Voice, Video, Data and Security Services

High-Performance Integrated Security and Data

Secure Broadband and Wireless Connectivity

Office Size

Enterprise Branch Office

Small Branch

Small Remote Offices

Teleworker

Single-Site Small Business

Cisco 870 Series Integrated Services Router

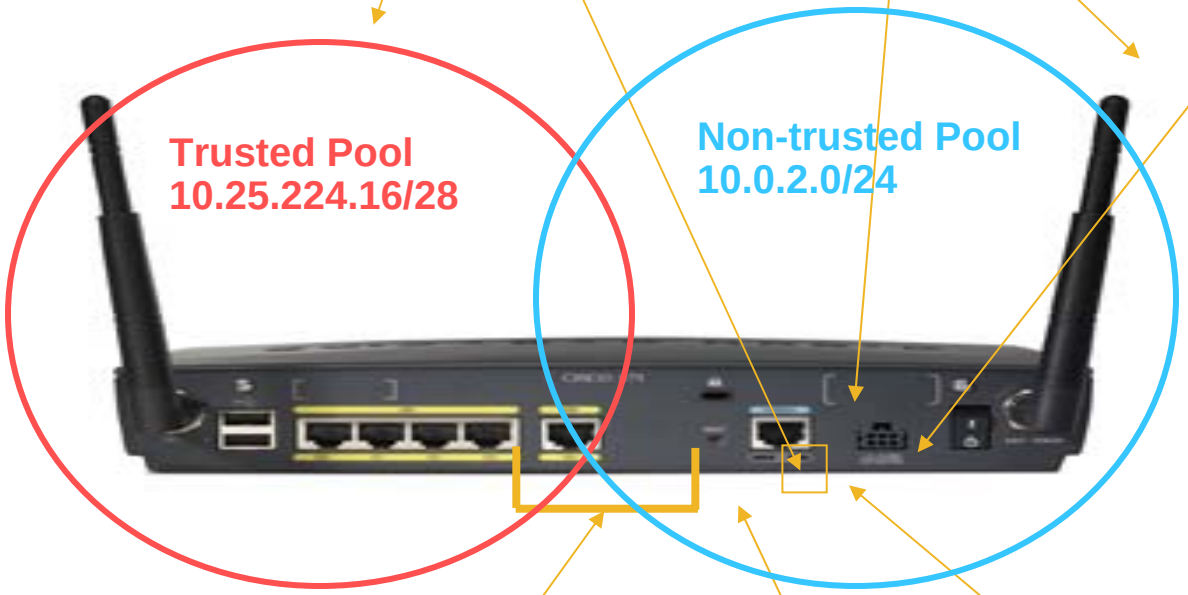
WAN Port:
871 = 100 MB Ethernet
876 = ADSL over ISDN
877 = ADSL
878 = G.SHDSL (4-wire)

Dual, Removable Antennae

ISDN S/T Port (876 and 878 Only)

Security Cable Lock

Console Port/Virtual AUX Port



Memory
Flash
Default: 24 MB
Max: 52 MB

DRAM
Default: 128 MB
Max: 256 MB

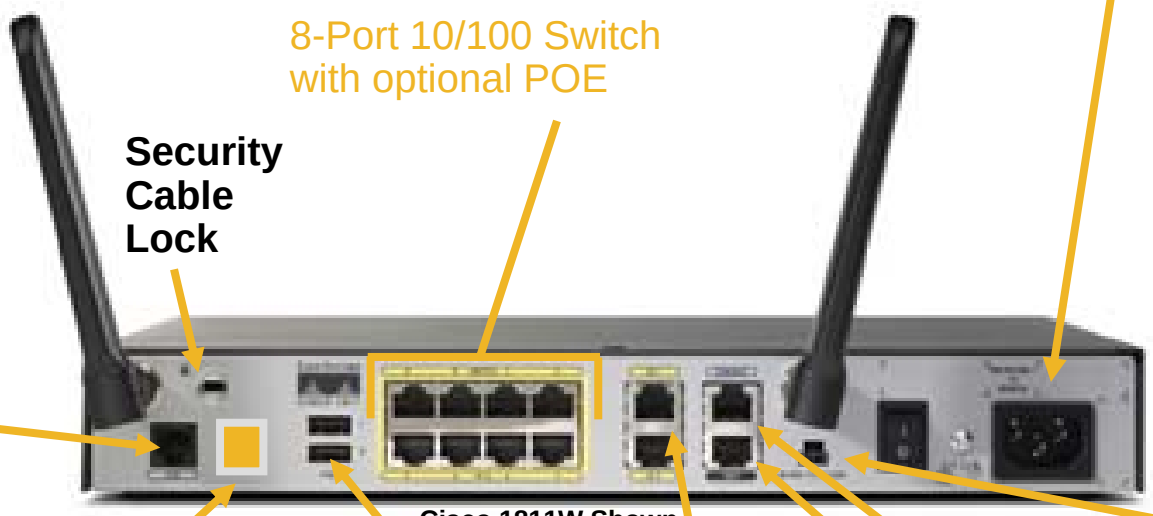
4-Port 10/100 Managed Switch

WAN Port:

Reset

Cisco 1800 Series Fixed Configuration Integrated Services Routers (Cisco 1811W shown)

Antenna Options



Dual, Replaceable Antennas

Internal Power Supply

8-Port 10/100 Switch with optional POE

Security Cable Lock

Memory
Flash
Default: 32 MB
Max: 128 MB

DRAM
Default: 128 MB
Max: 384 MB

ISDN S/T (1801, 1802, 1803, 1812) or Analog Modem (1811) for Backup and Out-of-Band Management

PoE Power Input

Cisco 1811W Shown

DSL WAN Port:
- **ADSL (1801)**
- **ADSL over ISDN (1802)**
- G.SHDSL (1803)

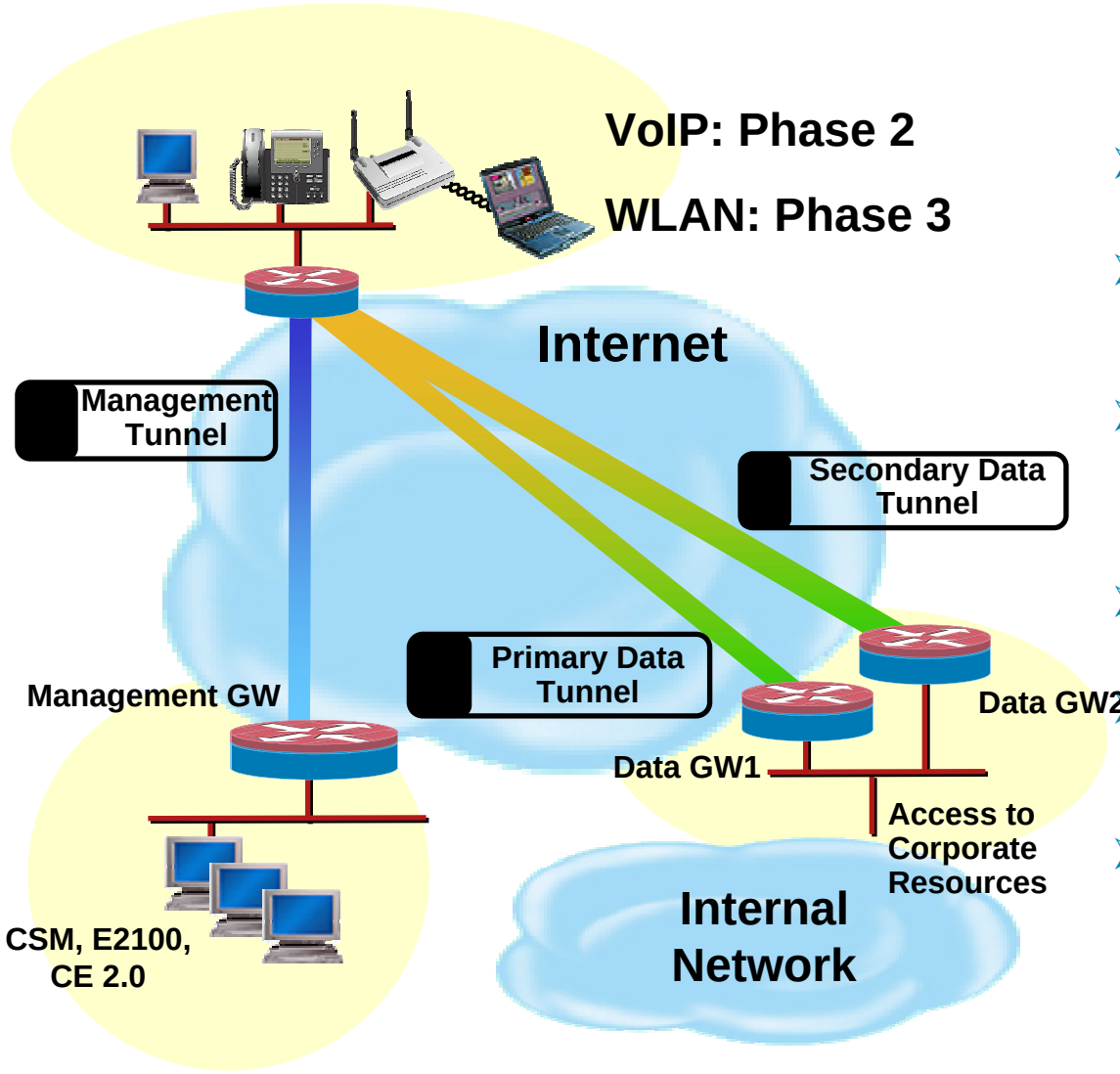
USB 2.0 Ports for Security Tokens (1811/1812)

Dual 10/100 FE WAN Ports (1811, 1812)

Console Port

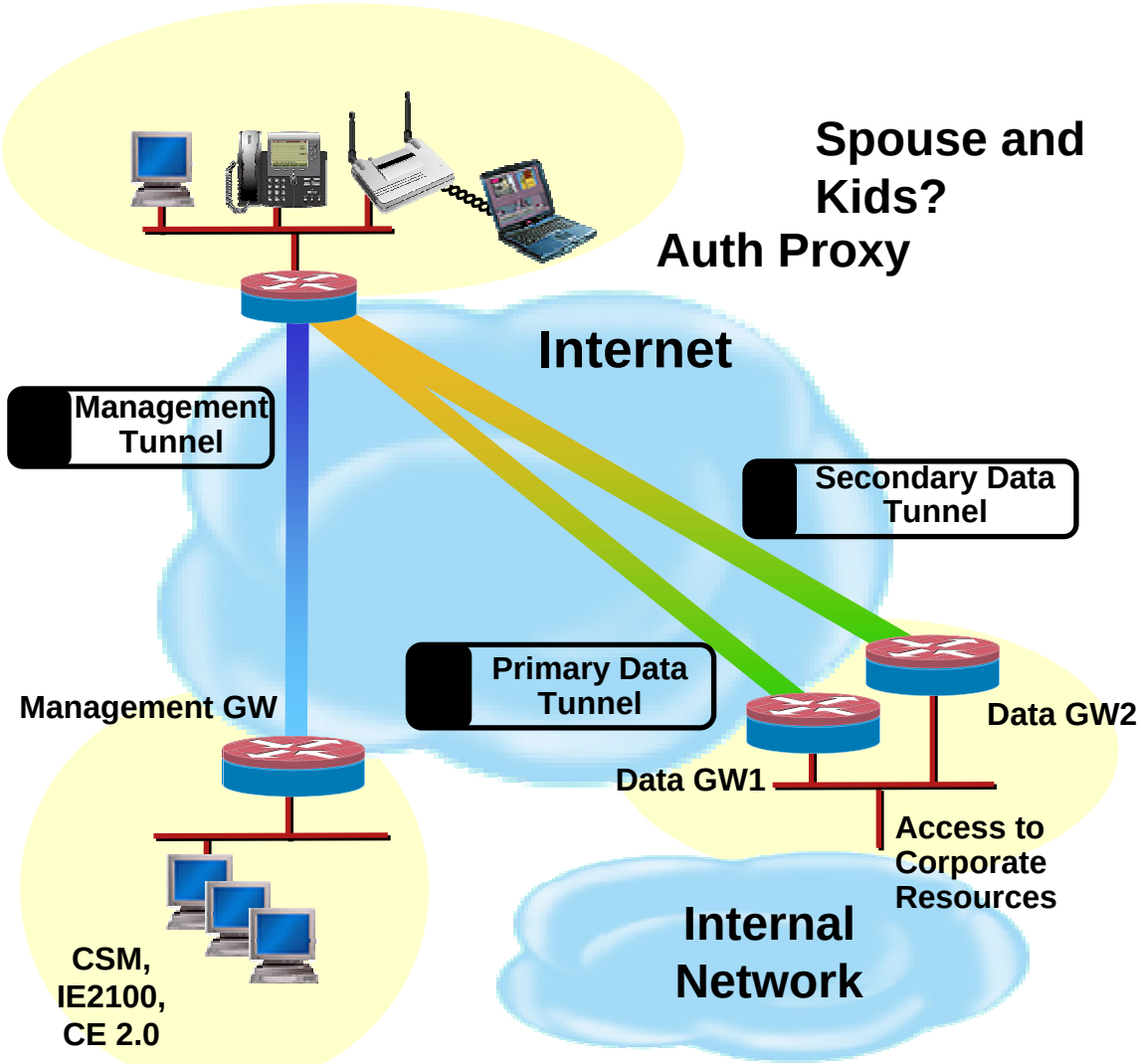
AUX Port

ECT CPE Zero Touch Deployment (ZTD)



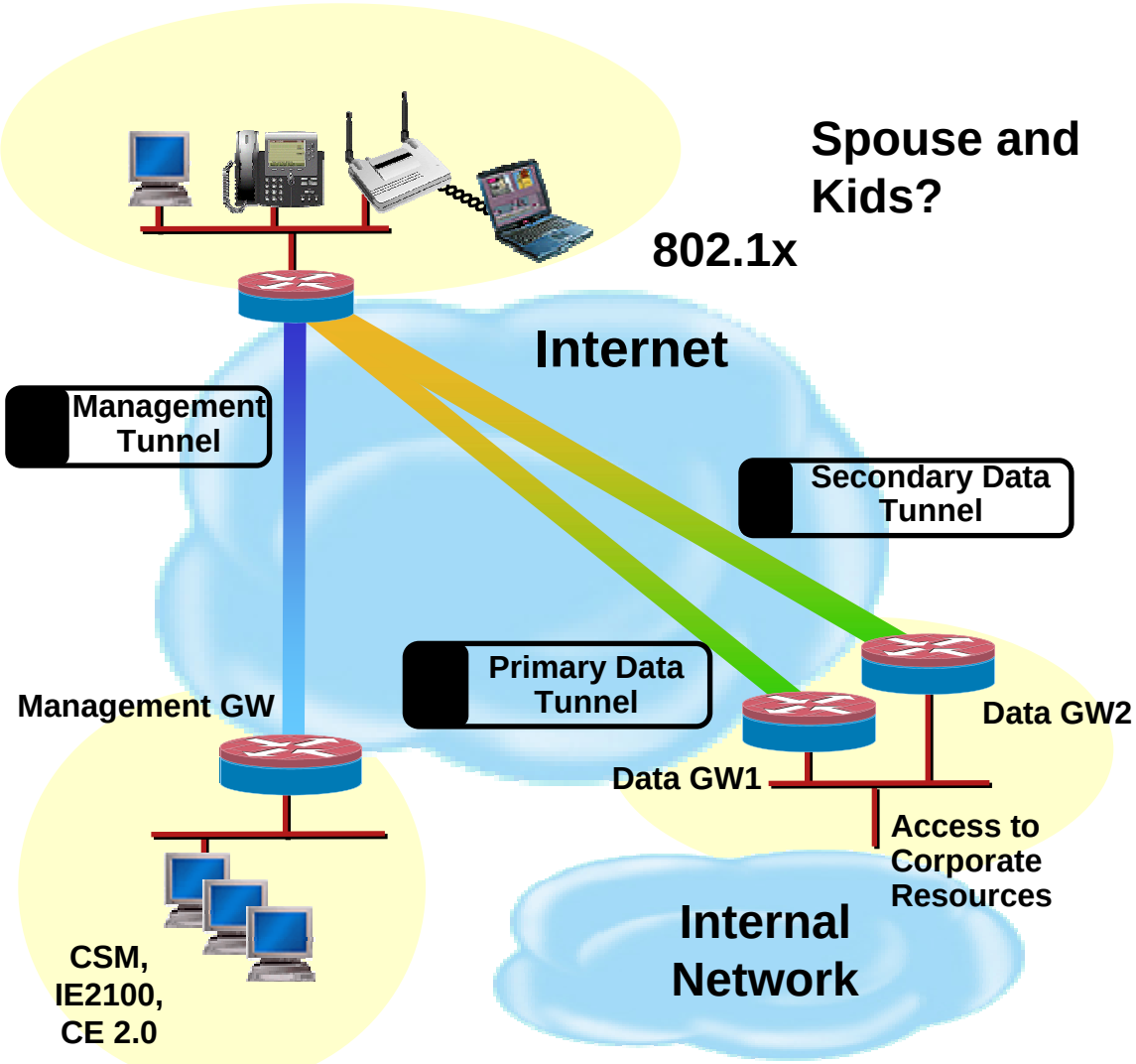
- Spoke router performs EzSDD and obtains keys and certificates
- Management GW authenticates spoke router using PKI-AAA integration
- Spoke router establishes mgmt tunnel, “calls home” and sends CNS “connect” event to CNS Engine and ISC
- ISC pushes & audits policy over management tunnel
- Spoke router establishes VPN tunnel w/Data GW1, gains access to corporate resources
- VPN tunnel established w/Data GW2 and stays active for failover (15 seconds)

ECT Architecture-Today-Auth Proxy



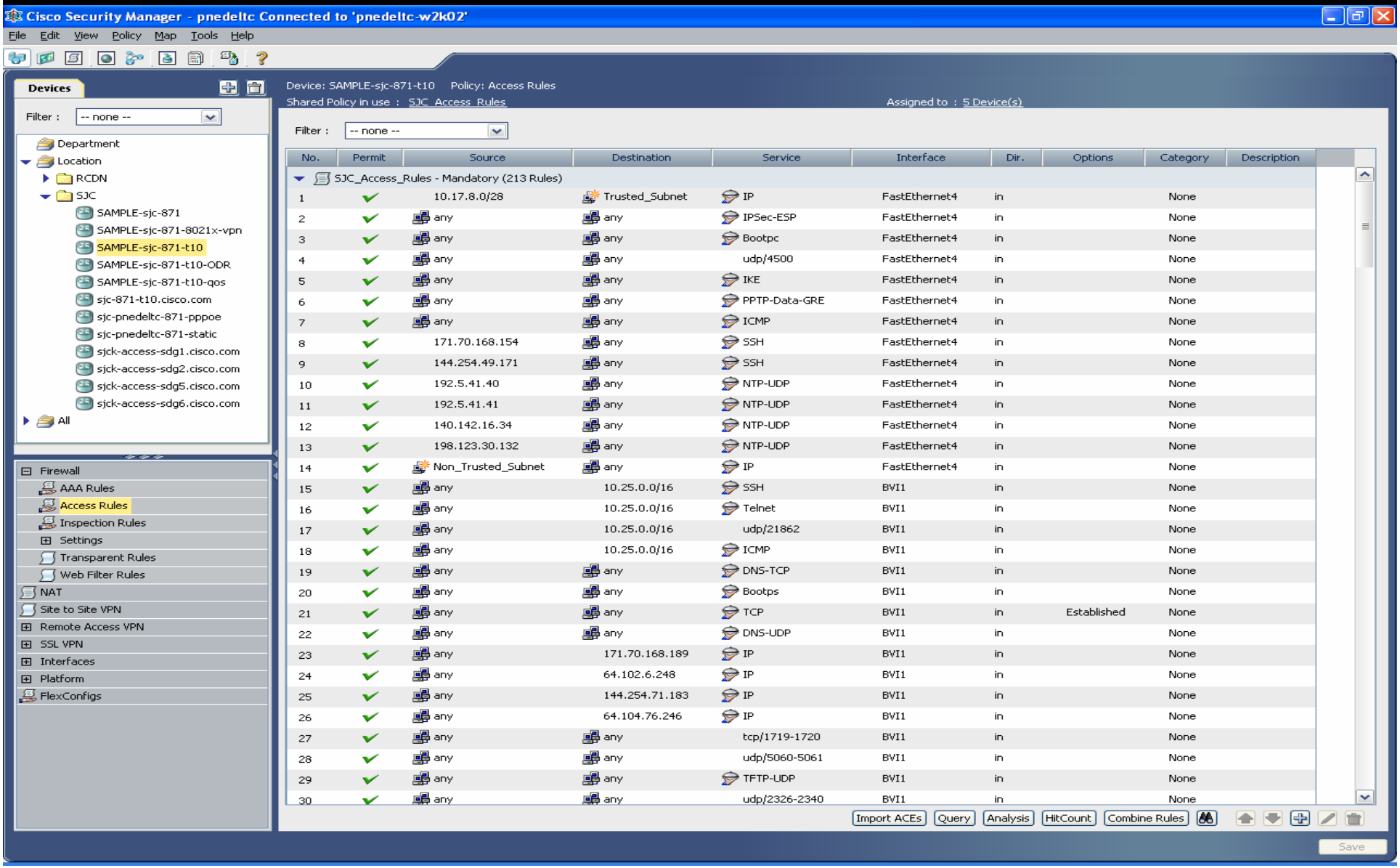
- Today the ECT solution uses 'Auth Proxy' to authorize PC's to corporate resources
- Auth Proxy uses a userid and Active Directory (AD) password through a browser
- Once the user has successfully authenticated, corporate resources (email, IM, etc.) can be accessed
- If the authorization is not successful, the PC can still access the Internet

ECT Architecture-Q3-802.1x

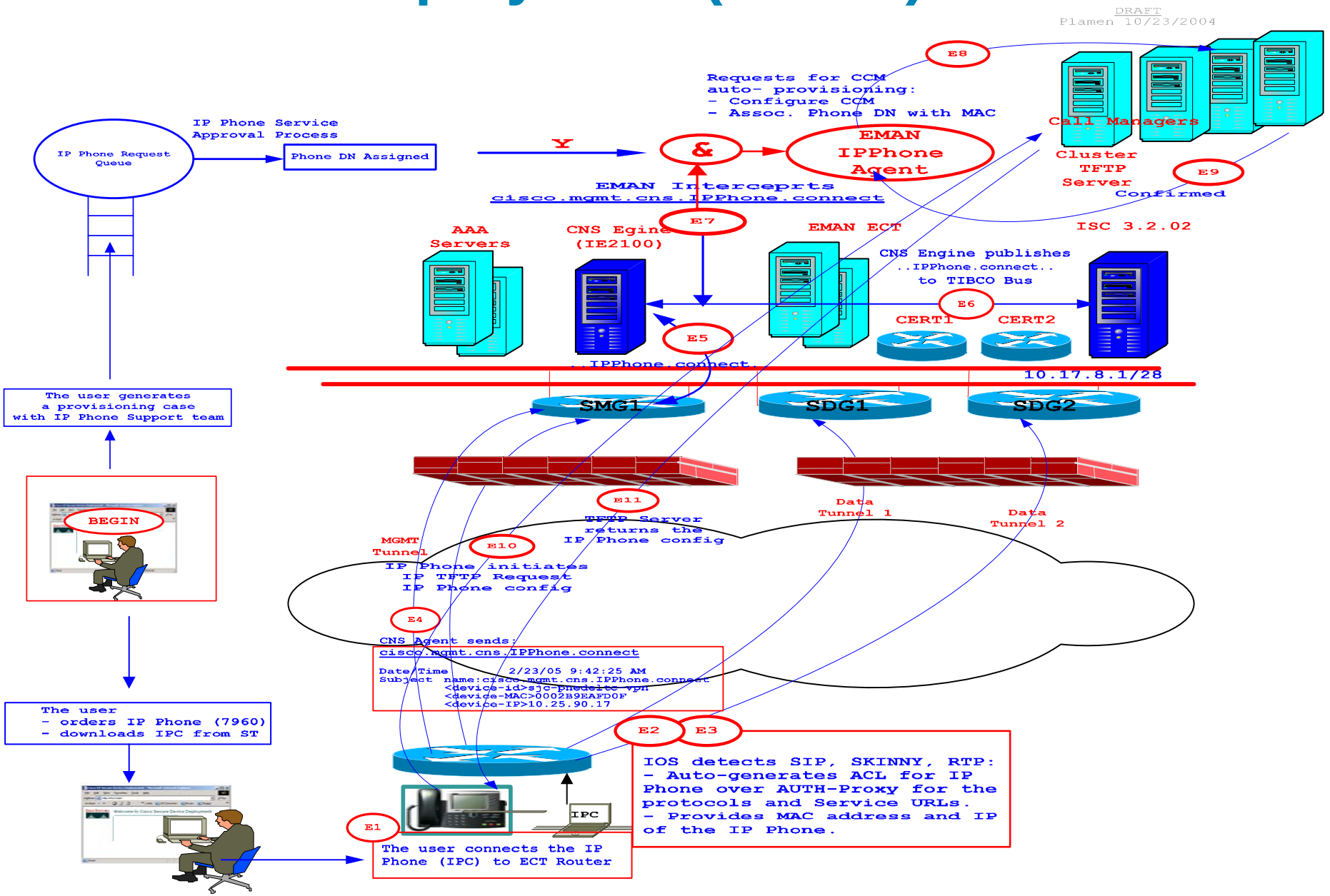


- 802.1x utilizes a client certificate to authenticate it as a 'trusted' device
- By utilizing a client certificate on a corporate PC, the auth proxy solution is no longer required to authenticate the device
- Client access to corporate resources from a corporate PC is seamless
- If the PC does not have a certificate, the PC can still access the Internet

Cisco Security Manager Integrated into EMAN

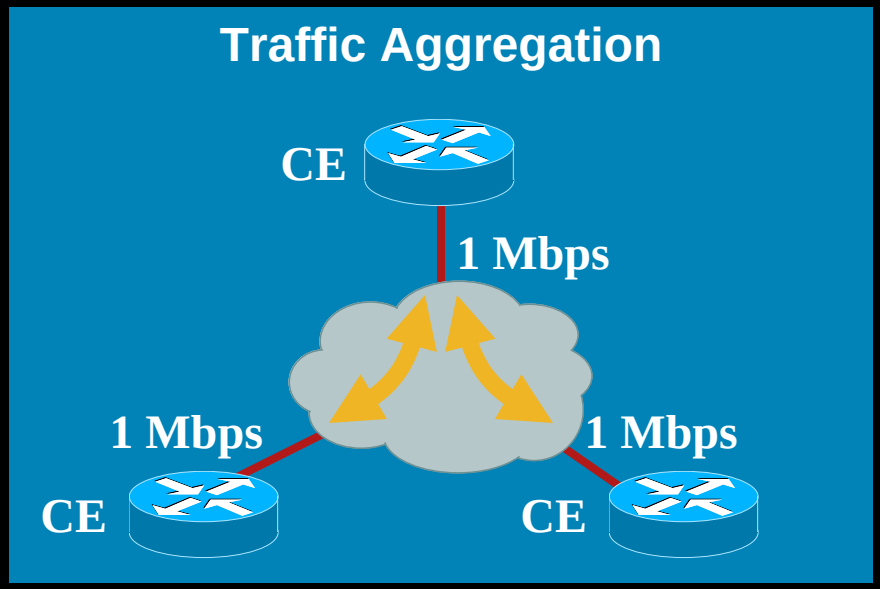


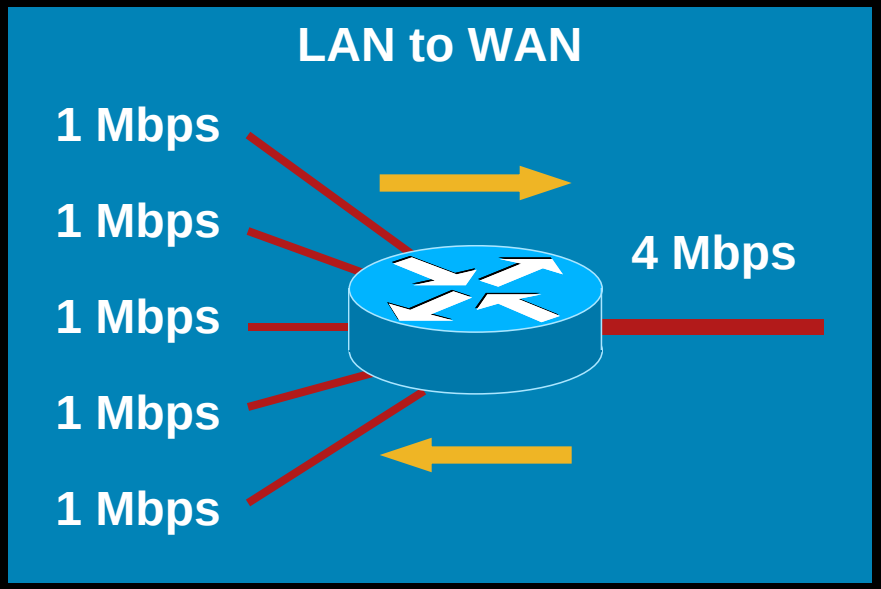
ZTD IPT Deployment (HOME)

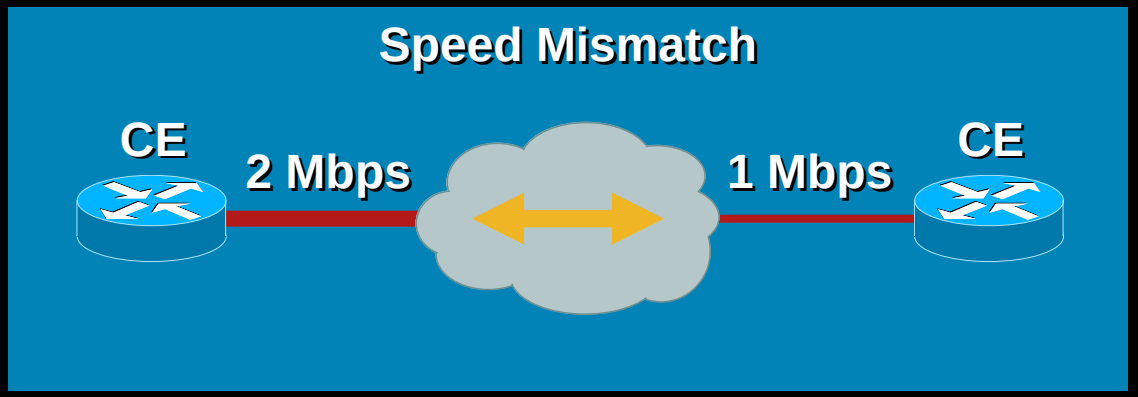


Teleworker QoS
What Do We Want from ISP?

Congestion Scenarios



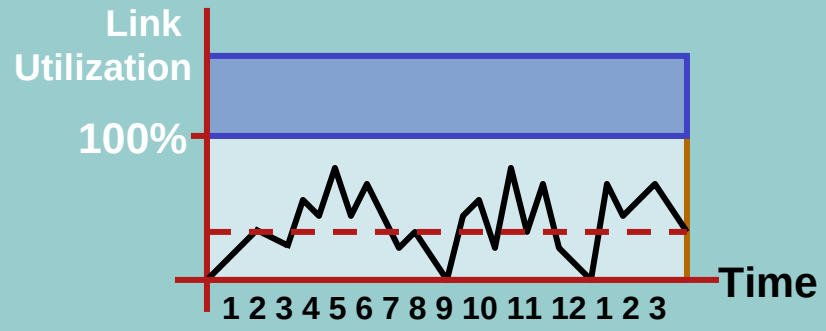




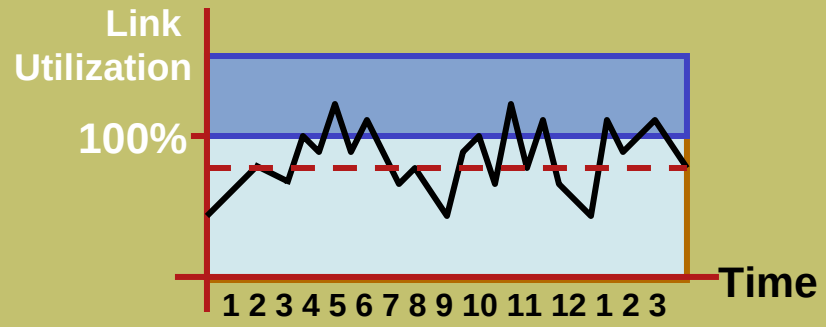
What Is QoS?

- **Quality of service:** A term which refers to a **set of performance parameters that characterize the traffic over a given connection**
- **Quality of service: A measurable set of parameters that define the level of service that a service provider can be held accountable for**
- **Quality of service:** Defined as the **measure of performance for a transmission system that reflects its transmission quality and service availability**
- Service availability is a crucial foundation element of QoS. Before any QoS can be implemented successfully, the network infrastructure must be designed to be highly available. (The target for high availability is 99.999 percent uptime, with only five minutes of downtime permitted per year.)
- The transmission quality of the network is determined by the following factors: Loss, Delay, Delay Variation (jitter), Throughput/Contracted BW

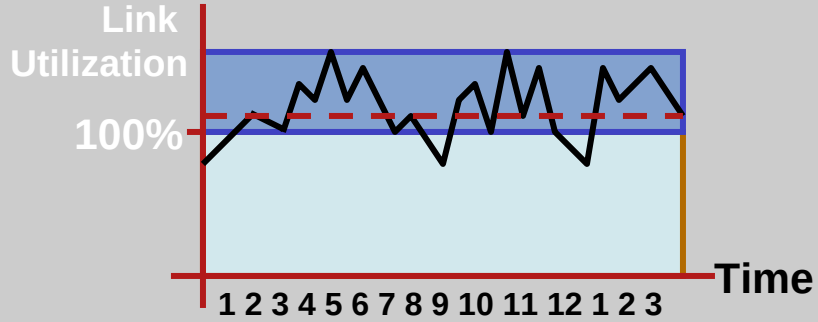
How Much Can QoS Help?



- Link overprovisioned
- May not be cost effective
- No QoS required but a safety net



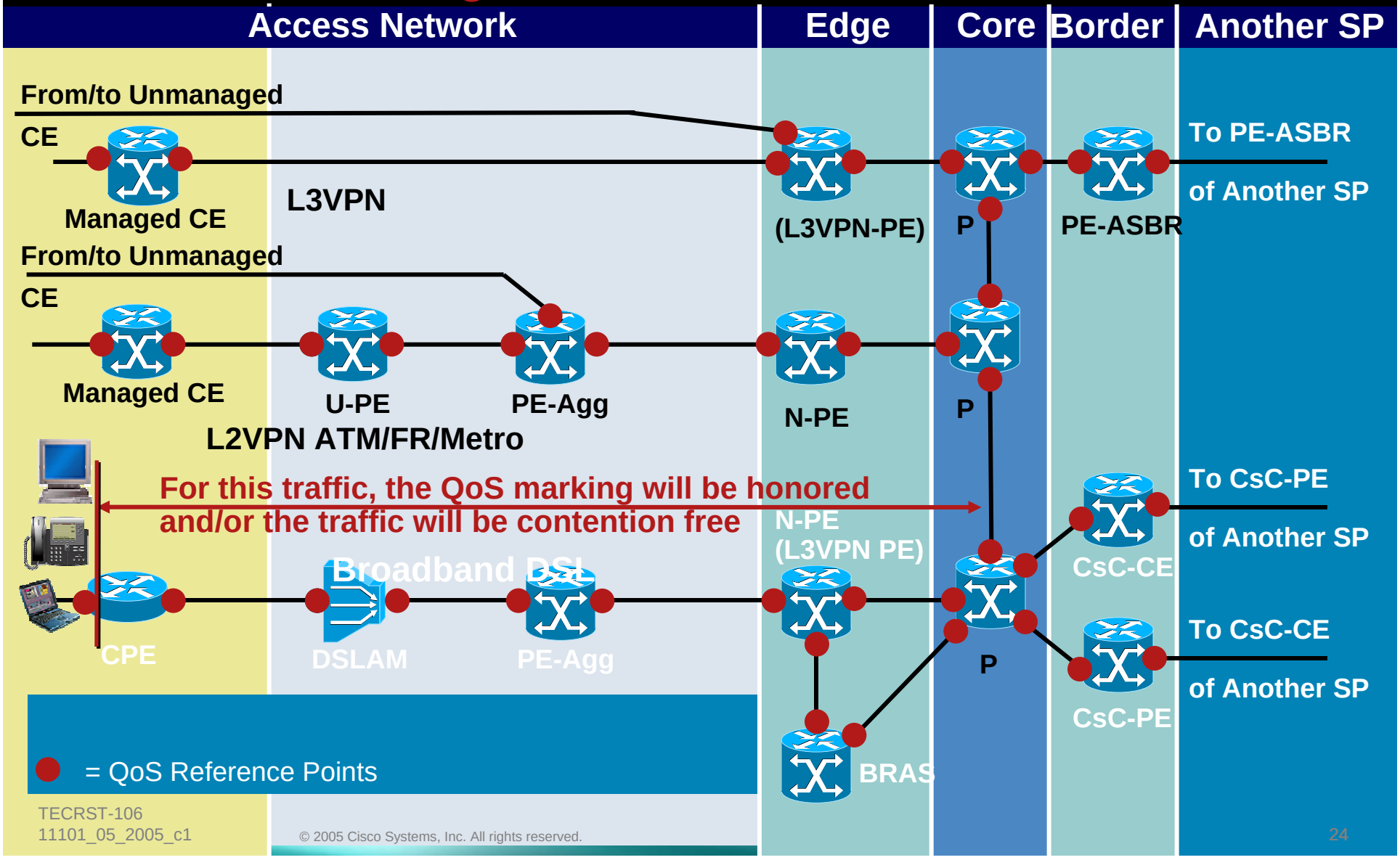
- Transient congestion
- QoS most useful



- Link highly oversubscribed
- QoS somewhat useful but more bandwidth required

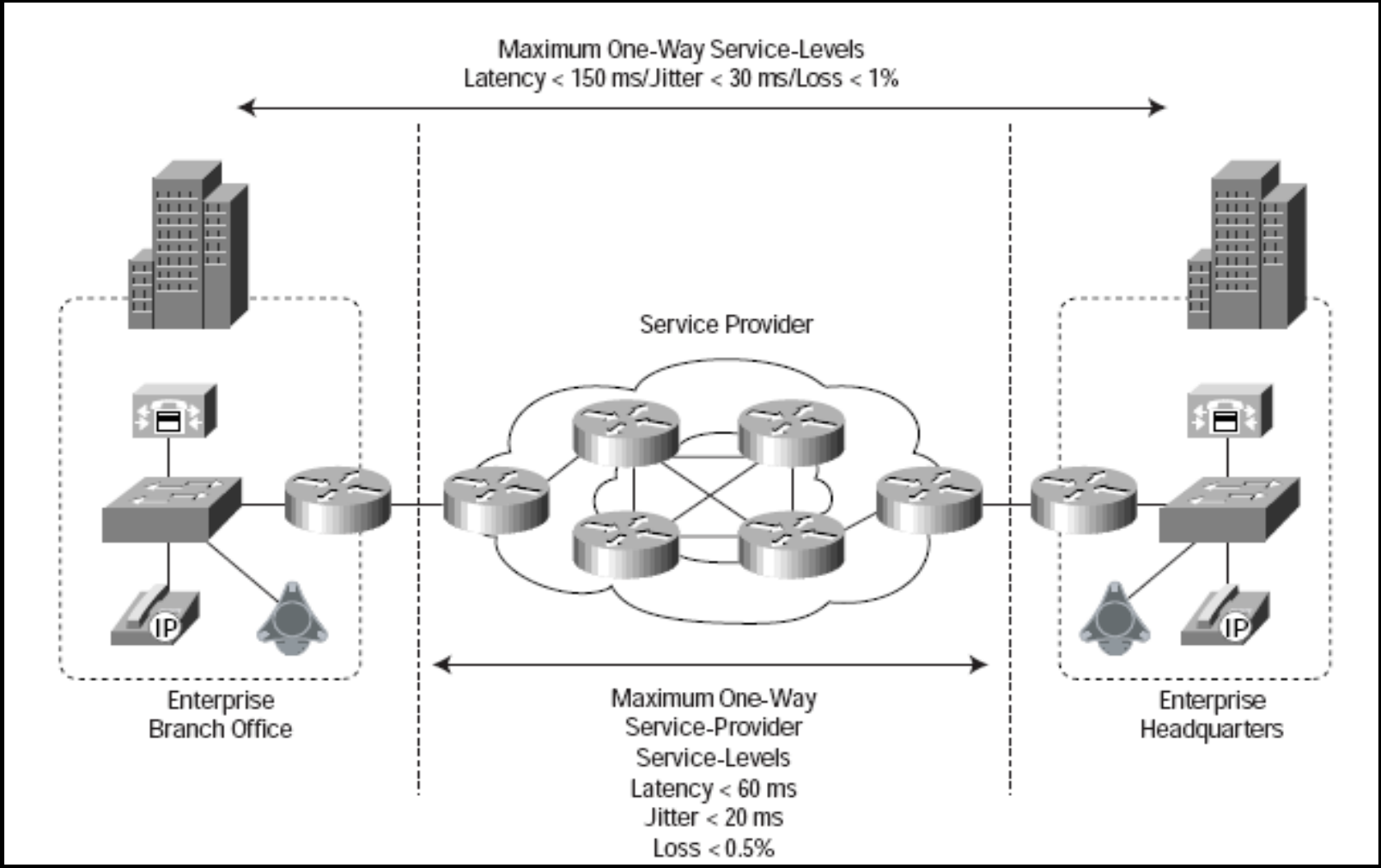
‘Diamond’ Service in Service Provider’s DSL Network

The service is as good as its weakest link



Teleworker
QoS and IP SLA

First Three Requirements: Latency, Jitter and Loss



SLA Metrics

Minimum SLA Attributes Related to QoS	Other SLA Attributes Related to QoS
Latency (Delay)	Availability
Packet Loss	Mean Time to Repair (MTTR)
Delay Variation (Jitter)	Mean Time Between Failure (MTBF)
Contracted Bandwidth	Per-Flow Packet Sequence Preservation
Throughput	Admission Control Criteria
Contention Ratio	ISP supported QoS at the edge
SLA measurement/reporting tools - measurement points, methodology, reporting methodology (web, e-mail) reporting interval, report contents, failure criteria and penalty clauses.	

Minimum SLA Requirements

Applications with similar QoS requirements are grouped into a traffic class (e.g., Voice, Interactive Video as real-time)

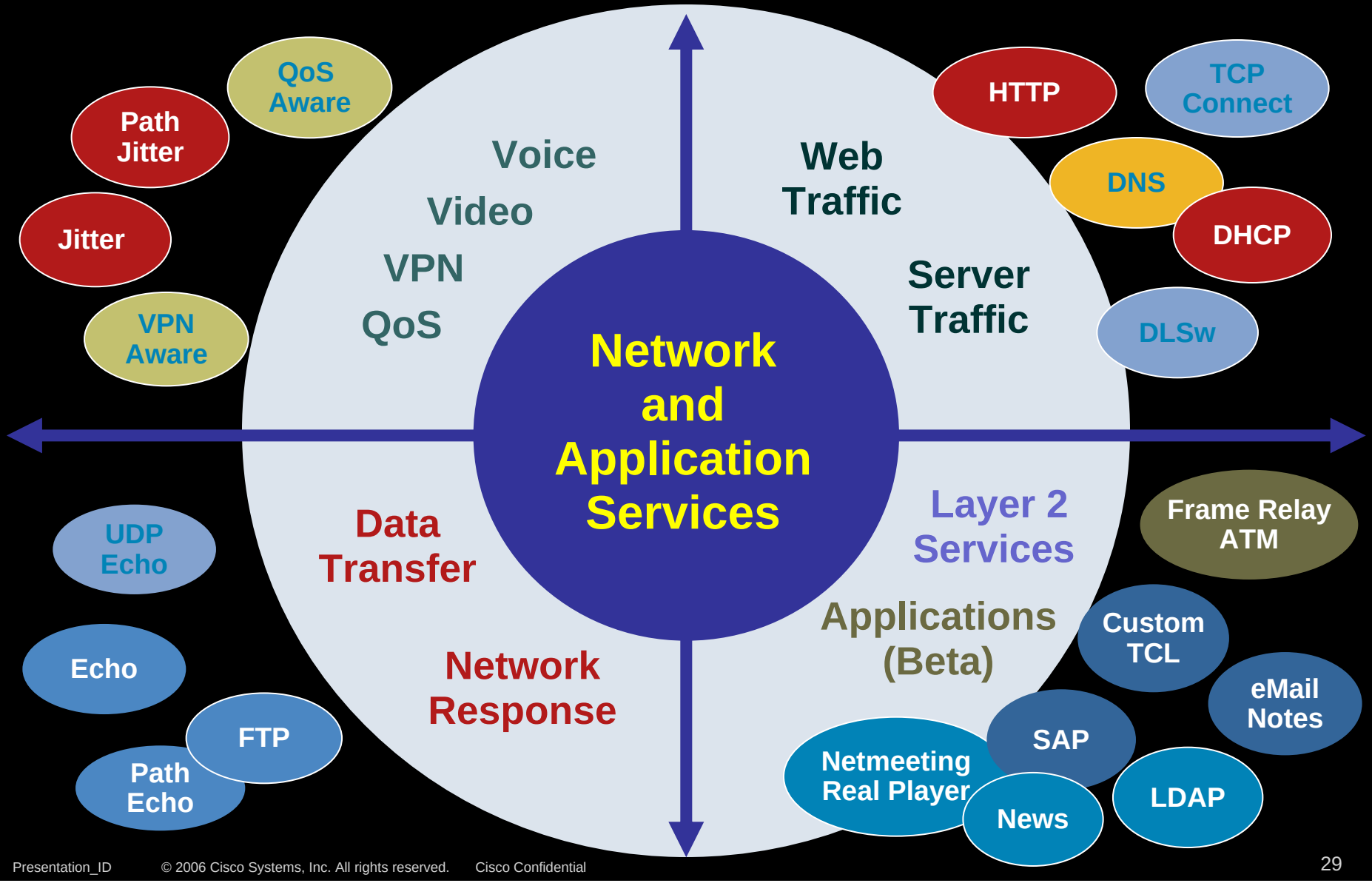
Traffic Classes will have separate loss, latency, and jitter requirements:

- Time-sensitive applications—Voice, Interactive Video
- Business critical class—Oracle, SAP
- Best effort—Internet access, file transfer

SLA attribute guarantees are per traffic class

	PoP-to-PoP			End-to-End		
	Real Time	Business	BE	Real Time	Business	BE
Loss	✓	✓	✓	✓	✓	
Delay	✓	✓	✓	✓	✓	
Jitter	✓			✓		
Availability	✓	✓	✓	✓	✓	✓
Contracted BW (cBW)				✓	✓	✓

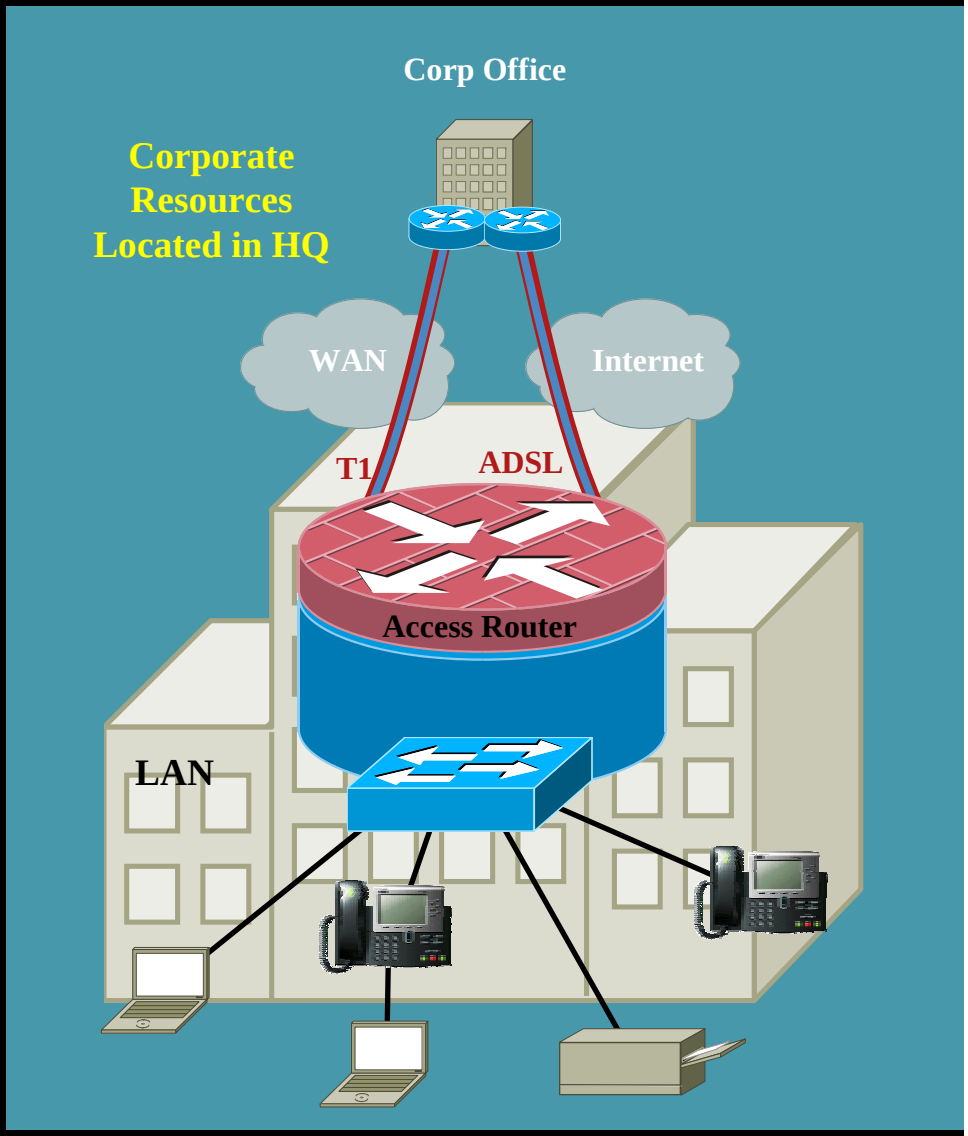
IP SLA Probe Types



Small and Very Small FSO
One Size Fits All: Yes or No?
Business Continuity

Single Tier Branch

- Networked Infrastructure Components
  - Access Router
  - Integrated LAN Switch
  - Laptops, Phones, Printers
- WAN Services
  - Internet Deployment Model
  - T1 Primary Link
  - ADSL Secondary Link
- LAN Services
  - Integrated L2 Switch
- Network Fundamentals
  - Routing—EIGRP
  - High Availability—Floating Statics, T1 w/ aDSL
  - WAN backup
  - QoS—Shaping, Policing, Scavenger Class (applied to both switch and router)



Many Types of Events Can Prevent Employees From Coming To Work

Transit Strike

Pandemic

Terrorism

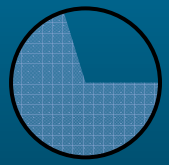
Natural Disasters

Increased Workforce Resilience:
Key to Business Continuity

Power Outage

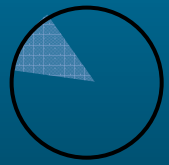
88% of Enterprises Prepared

Failure of Server, Host, Application, Software



70% of Enterprises Prepared

Workforce Disruption



13% of Enterprises Prepared

Only 13% of Enterprises Today Are Prepared for a Major Disruption in Workforce Operations

Communications Requirements Drive Solutions
Cisco ECT and Full Office Replication

Solution Suite	Communications Services
Cisco Anywhere Office	Data Connectivity
Cisco ECT	Voice & Data Connectivity
	Full Office Replication