DESIGNING VOICE ENABLED IPSEC VPNS FOR TELEAGENTS

VVT-2004

Recuerde siempre:

- Apagar su teléfono móvil/pager, o usar el modo “silencioso”.

- Completar la evaluación de esta sesión y entregarla a los asistentes de sala.

- Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.

- Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.

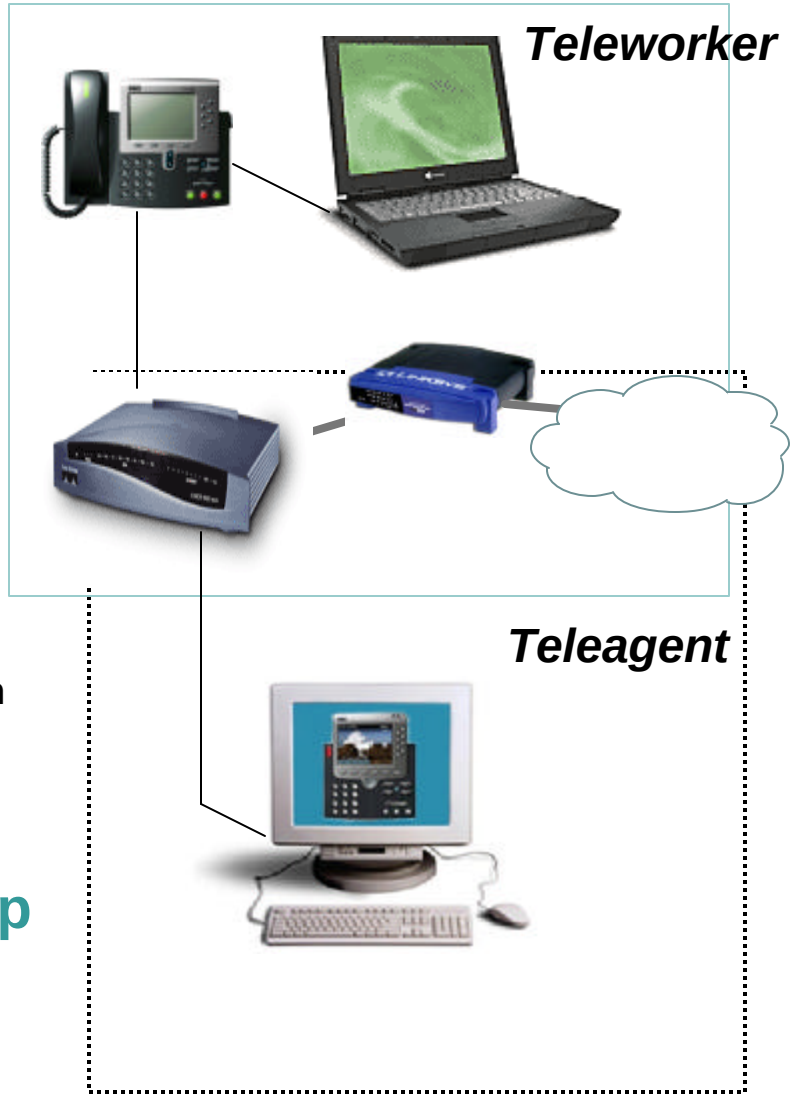
Agenda

- Overview
- Bandwidth Requirements
- VoIP / IPCC
- QoS
- IPSec
- Authentication and Segmentation
- Provisioning (Configuration Management)
- Voice Quality Management (Fault Management)
- Head-end Topology - Backup and Redundancy
- Performance
- Lessons Learned
- Summary
- Appendix

OVERVIEW

Definitions

- **Teleworker**
  - Day-extension, Full or Part Time Telecommuter
  - Workstation and Phone use not tightly coupled
  - Phone used for both inter and intra enterprise calling
  - Knowledge Worker - Professional and Technical
- **Teleagent**
  - Primary Job – Customer Service
  - Full Time Work at Home
  - Agent status and call routing determined by Cisco IP Contact Center (IPCC) or equivalent application
  - Agent receives calls only after logging in workstation and application
  - Seasonal workforce in many industries



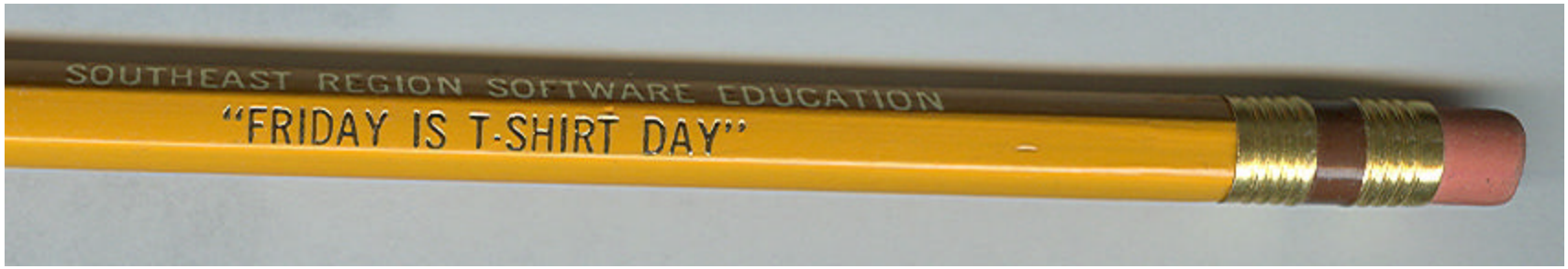
High Degree of Requirements Overlap Between Teleworker / Teleagent

Motivations

Work is an activity not a place

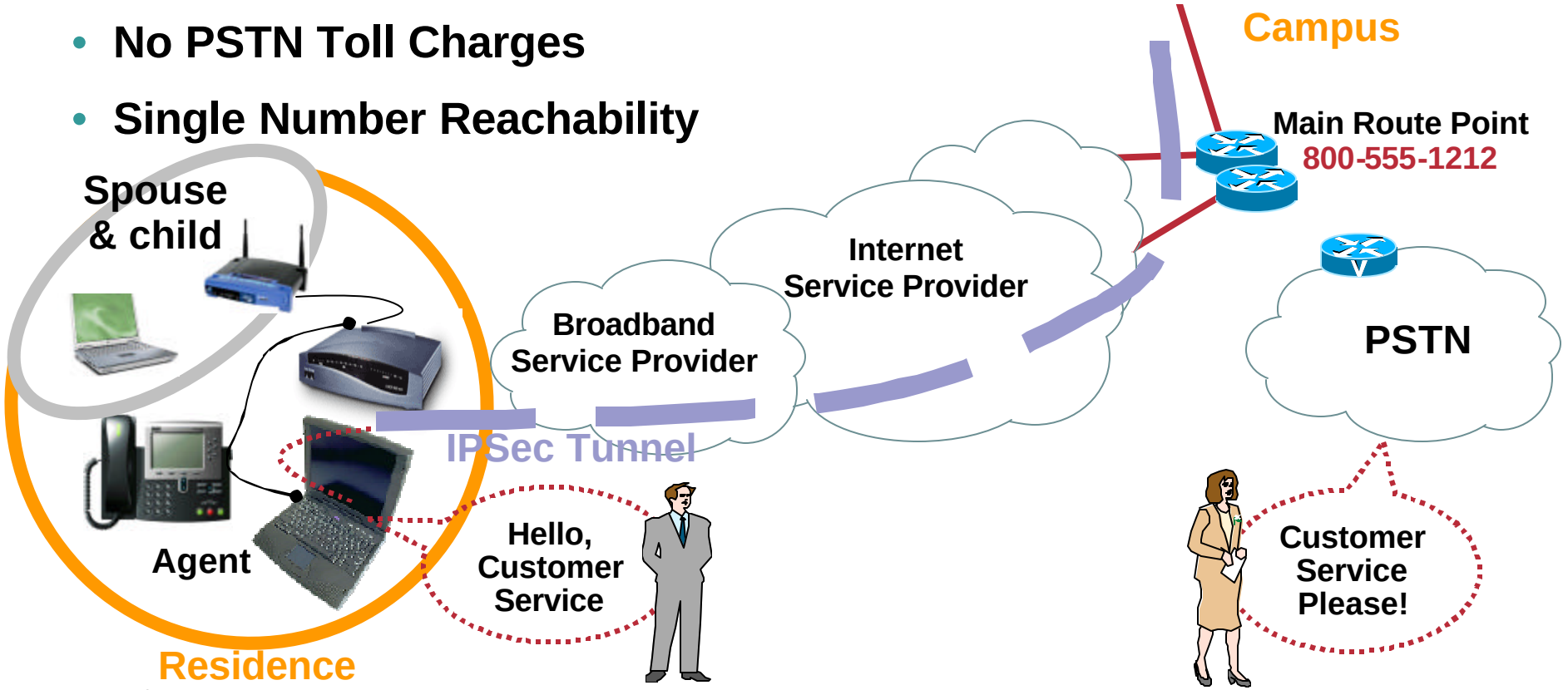
- **Improved job satisfaction and employee retention**
- **Business continuity and Disaster planning**
- **Employee responsiveness**
- **Greater flexibility - better work/life balance**
- **Harness talent across geographical boundaries**
- **Reduce commute time for employees**
- **Work opportunities for people with disabilities**

Cost Savings



Call Center Home Agent over Broadband Features and Requirements

- HW Accelerated 3DES crypto
- Quality of Service (QoS)
- Dynamic Addr DHCP/PPPoE
- No PSTN Toll Charges
- Single Number Reachability
- Spouse & Child co-exist with Agent
- VPN 'always' on
- No Home PSTN required



BANDWIDTH REQUIREMENTS

Bandwidth Requirements

- **Broadband costs decreased and available bandwidth increased in past 2 years - COMPETITION**
- **Bandwidth to Residence - single biggest influence in audio quality after hardware encryption acceleration**
- **Increased Broadband Bandwidth to Residence …**

  Eliminates Serialization (Blocking) Delay Issues

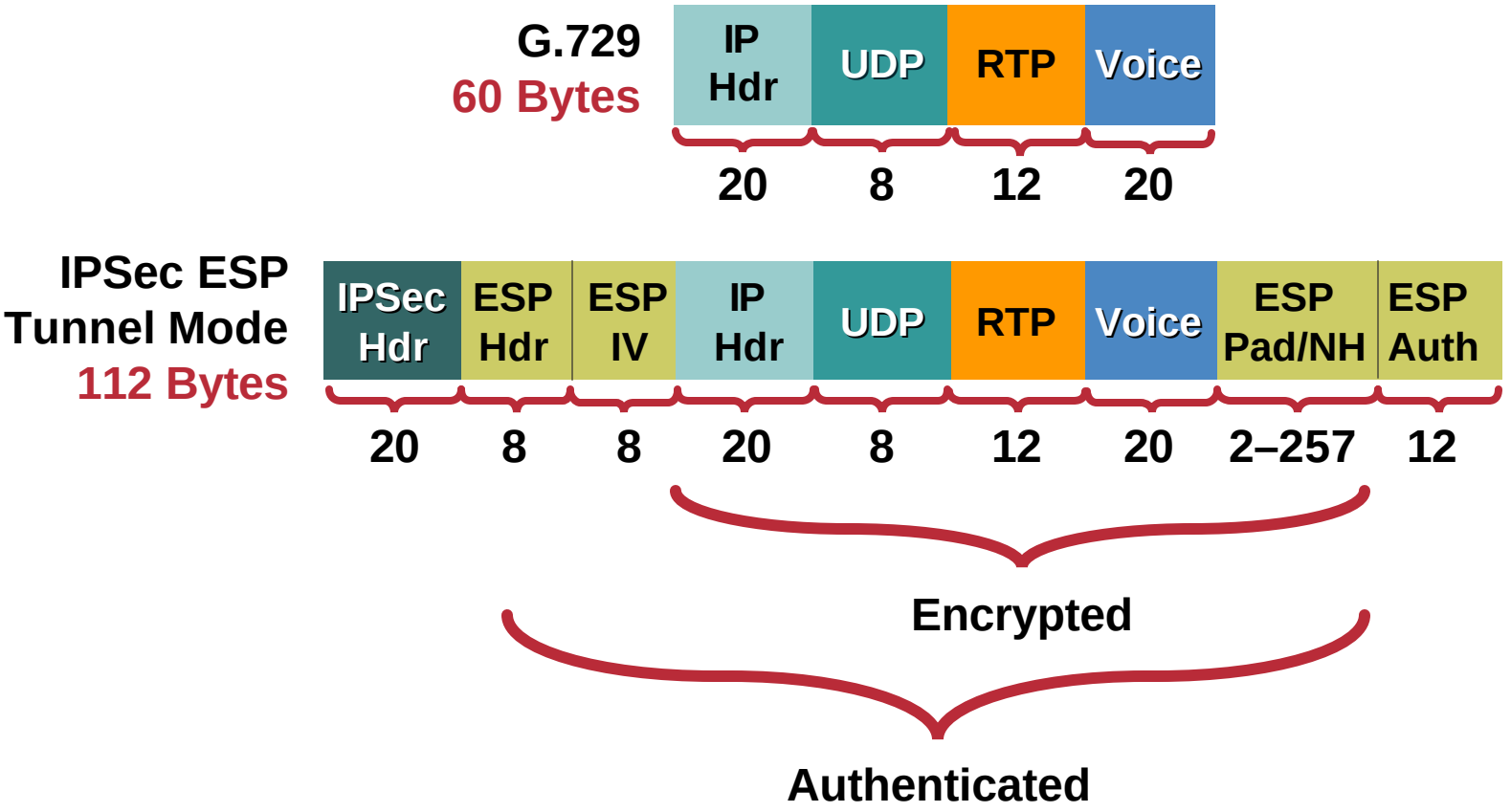
  Minimizes Jitter

  Decreases Latency

  Allows use of G.711 vs G.729 CODEC (Better Audio Fidelity)

  Provision for Remote (Silent) Monitoring of Home Agent

G.729 CODEC Direct IPSec - No GRE



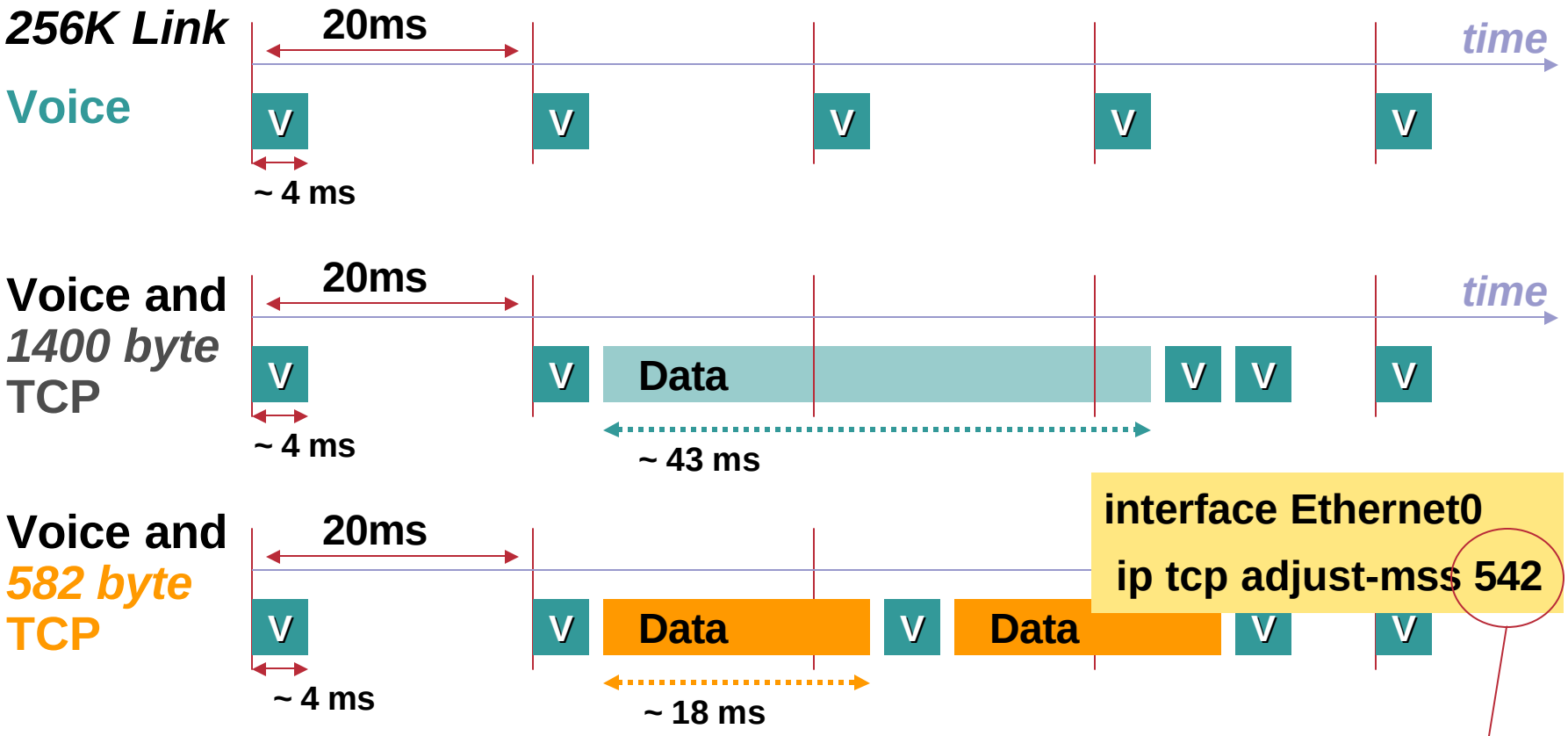
G.729 Packet DSL PPPoE IPSec has 40 bytes of AAL5 padding – adding GRE or NAT-T does not increase BW

VoIP + IPSec Bandwidth Calculation

esp-3des esp-sha-hmac		GRE and IPSec Tunnel Mode	IPSec Tunnel Mode	Adding Layer 2 Overhead
CODEC	pps			
G.711	50	280 Bytes per Packet 112,000 Bits/Sec	256 Bytes per Packet 102,400 Bits/Sec	114K to 128K Bits/sec
G.729	50	136 Bytes per Packet 54,400 Bits/Sec	112 Bytes per Packet 44,800 Bits/Sec	56K to 64K Bits/Sec

Serialization (Blocking) Delay
Influence Data Packet Size at Layer 4

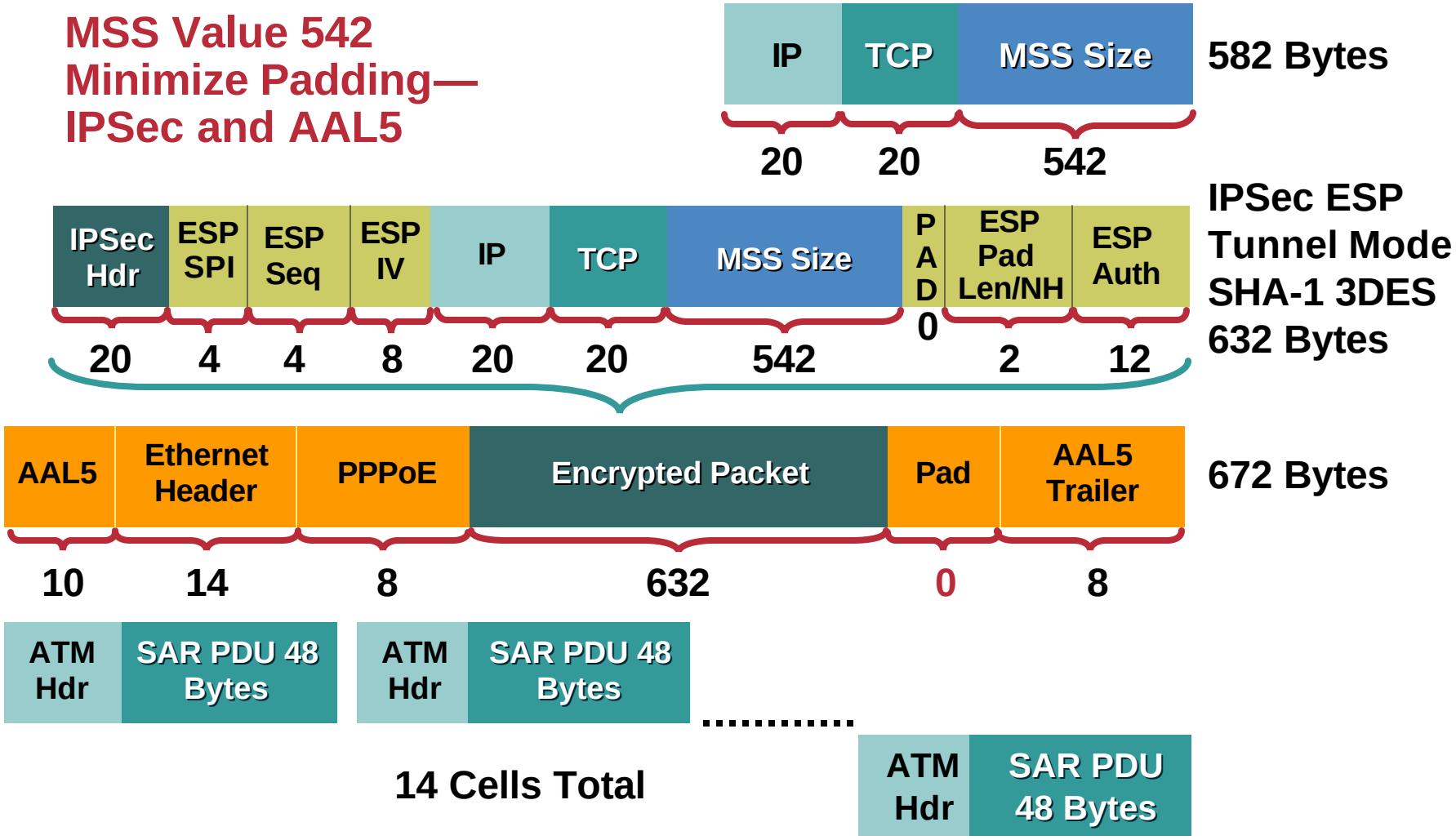
Links below 768K with no Layer 2 Fragmentation and Interleaving support - Teleagent router can override TCP MSS parameter – Reduces size of TCP packets – Decreases jitter and latency



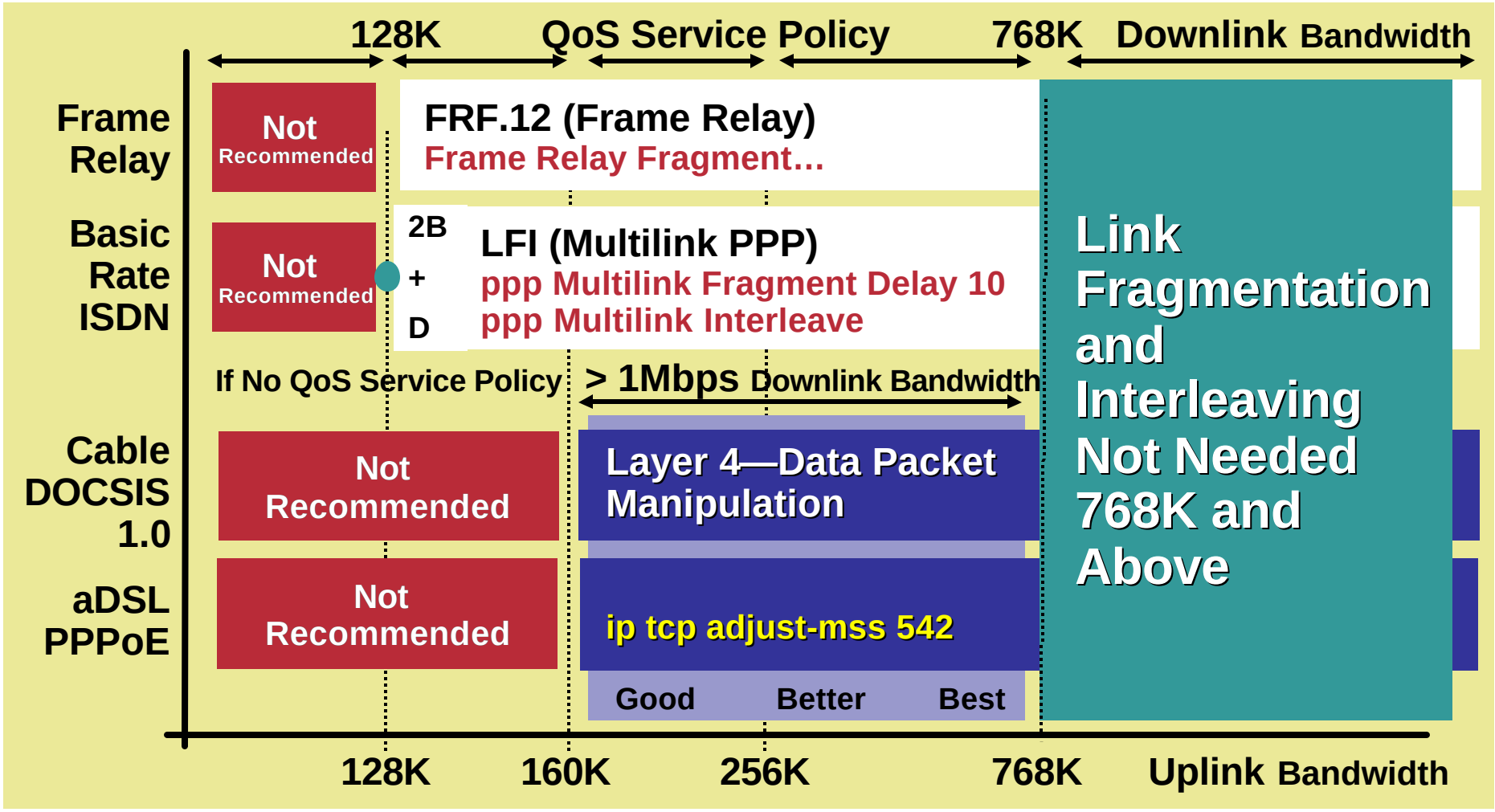
IP TCP Adjust-MSS Value
DSL/PPPoE

Cisco.com

MSS Value 542
Minimize Padding—
IPSec and AAL5



Encrypted VoIP—Voice Quality
Recommended Bandwidth Ranges



Compilation of Low-Speed Data Rates by Layer 2 Technology

Service Offerings
Research Triangle Park, NC

	Data Rate Up / Down	Monthly Rate	Comments
DSL	256K / 1.4M Residential	$53	DSL experiences have been good. DSL provider and Cisco RTP peer with same Tier 1 ISP. Very low latency.
Cable	768K / 3M Business	$75	Uplink rates are burst not guarantee on UBR. Generally thruput 80-90% advertised rate. Majority of RTP employees on cable
	384K / 5M Residential	$40	

For a few dollars more a month Serialization Delay is a non-issue

Voice over IP (VoIP) and Cisco IP Contact Center (IPCC) IPCC

VoIP and IPCC

- Voice over IP Network Requirements
- Home Agent Bandwidth by Application
- Software Phone Components
- SRTP Positioning

Voice over IP

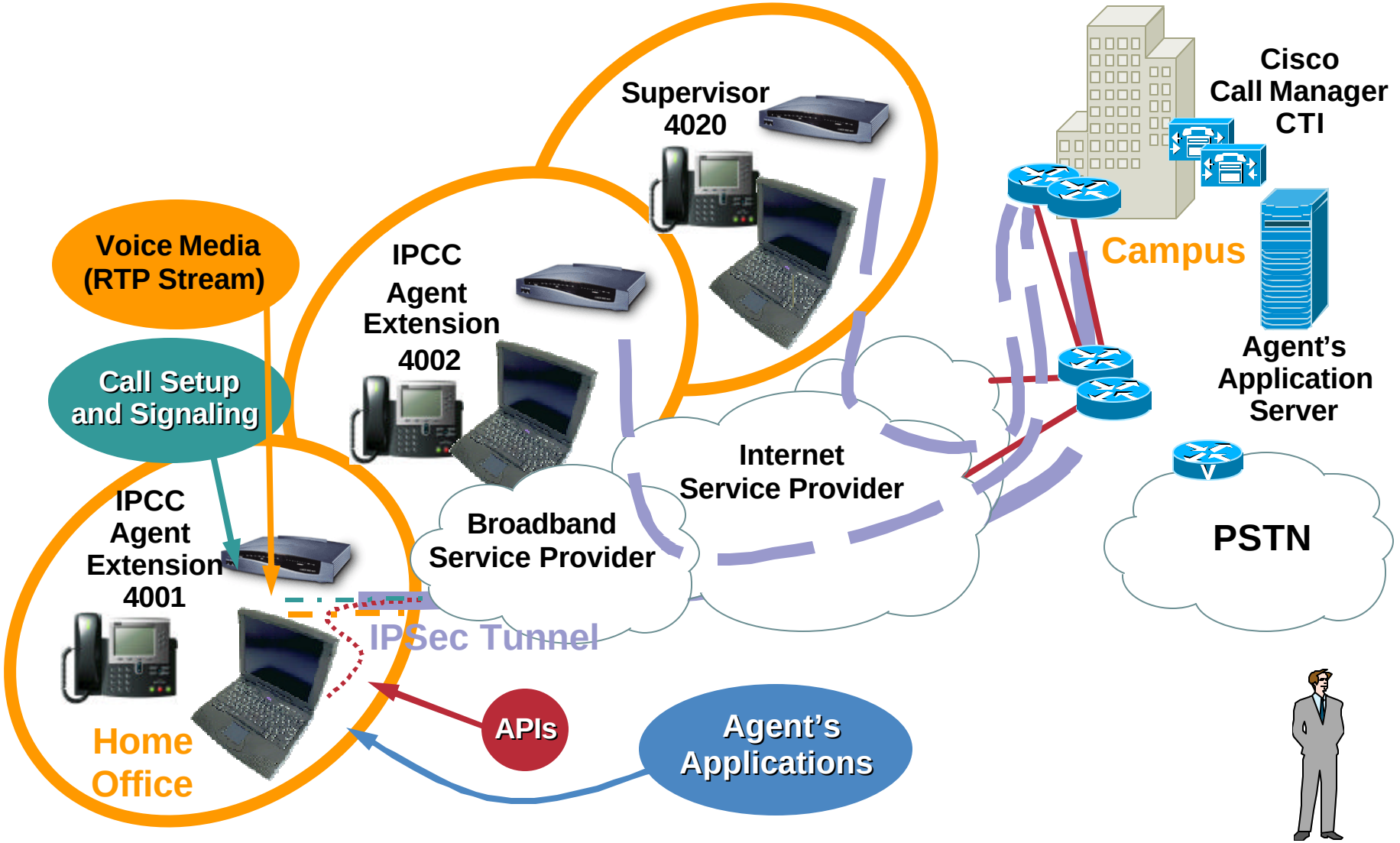
An Application with Special Requirements

- **Packets arrive at a constant rate**
  - **UDP stream with no upper layer flow control**
- **Arrival rate in “per call” increments**
  - **Typically 50 packets per second**
- **Quality a function of**
  - **Latency—over 250 ms people will speak at same time**
  - **Jitter—jitter buffer manages reasonable jitter**
  - **Drops—less noticeable when spread over time**
  - **Consistency—does performance level vary widely**
- **(Call Admission Control) CAC**
  - **Additional call can’t degrade existing calls**

Media Stream UDP Packets with DSCP Value of EF

50 pps

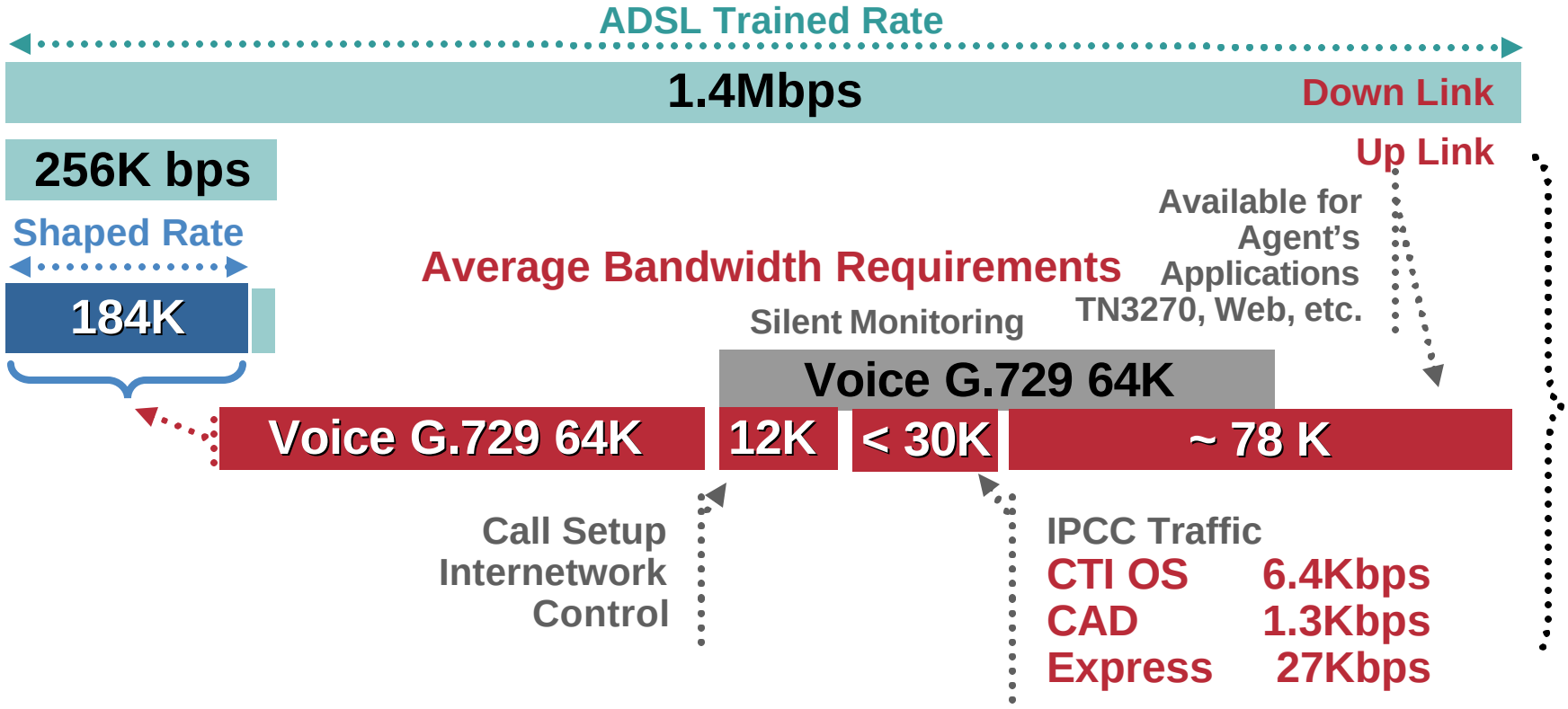
Home Agent Bandwidth Considerations



Home Agent Bandwidth Considerations
Encrypted

IPCC Is Simply an APPLICATION that Integrates Voice

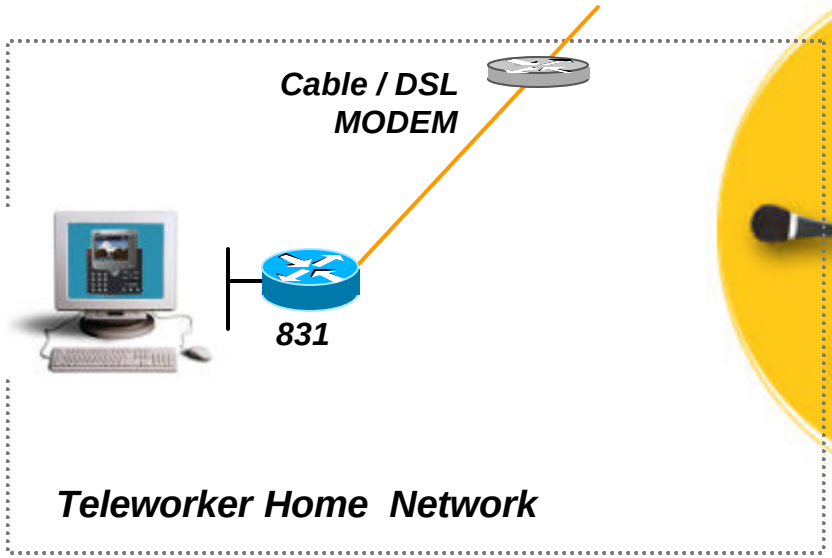
Remote Agent Desktop and Voice Data



Internal IPCC Testing Used Teleworker Traffic Profile Agent Applications and IPCC Traffic in Same Bandwidth Class

Cisco IP communicator

… our testing indicates that IP comm behaves very well even under heavy CPU load on the host machine...



Datasheets and info for IP communicator from CCO

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps5475/index.html

Plantronic DSP-400 headset

http://www.plantronics.com/north_america/en_US/productSearch/prod440042

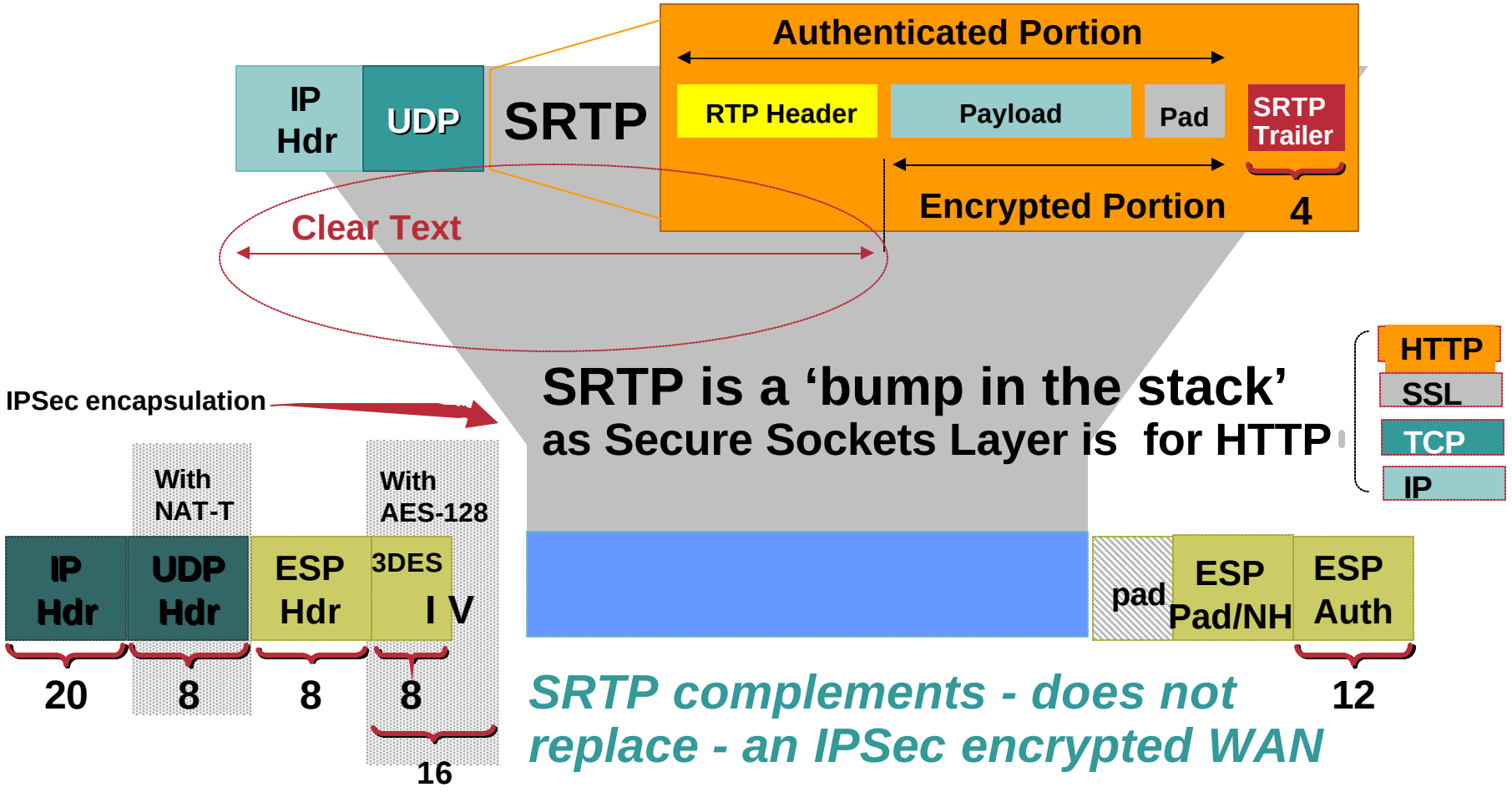
Deployment Model

- IPSec providing voice and data security
- Centralized call processing model — All IPCC Enterprise/Express servers at central site
- Hardware IP phone recommended - don't forget the power supply
- All remote IPCC enterprise supervisor functions supported
- Remote agent transfers, conferences supported
- Silent monitoring—agent desktop via switch port on IP phone
- Remote supervisor can monitor remote and campus agents

Positioning
IPSec and Secure Real-time Transport Protocol (SRTP)

SRTP provides Signaling and Media Encryption and Authentication

SRTP only increases latency by 15 microseconds



SRTP complements - does not replace - an IPSec encrypted WAN

Quality of Service (QoS)

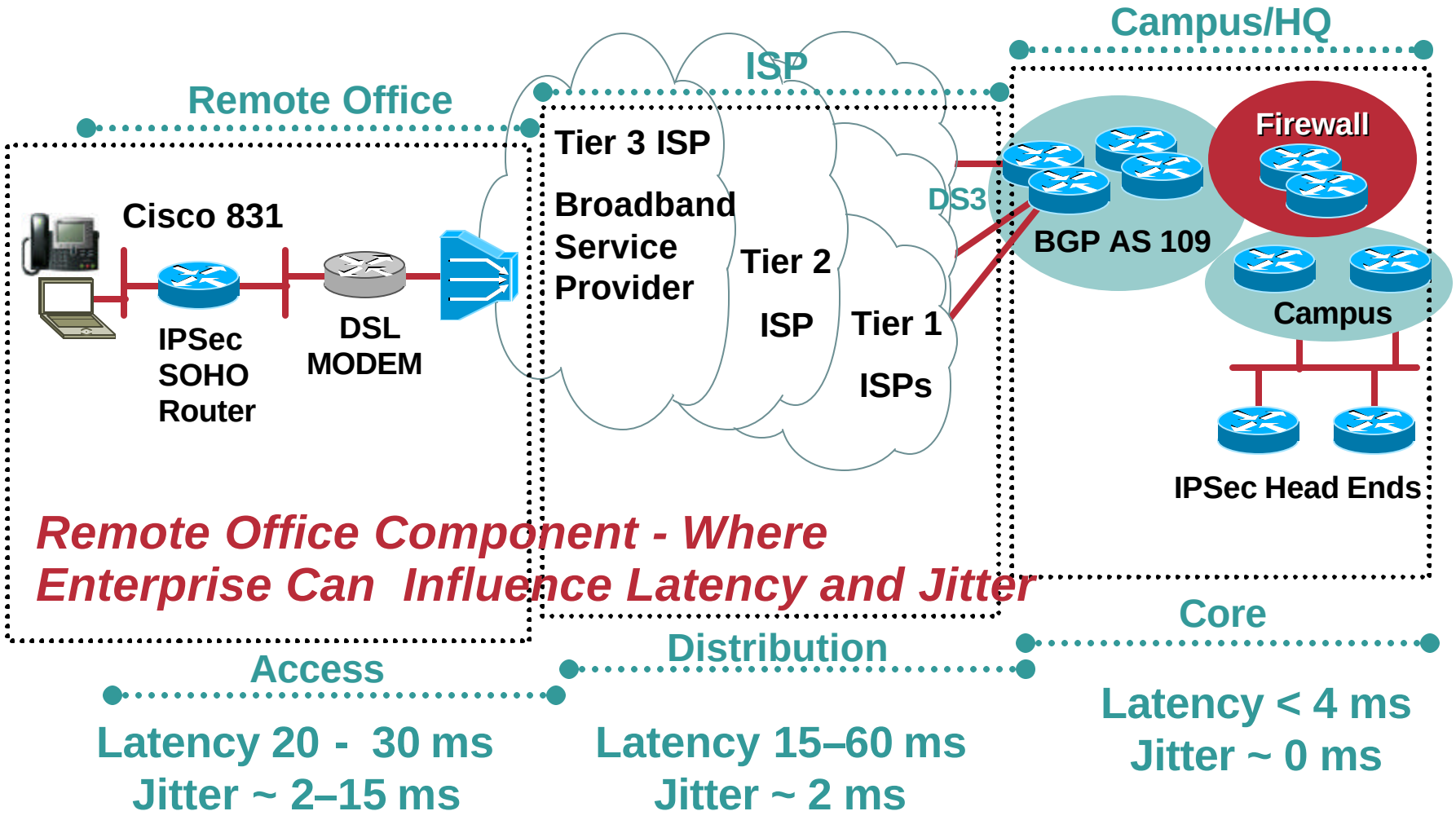
Quality of Service (QoS)

- QoS needed most where probability of congestion is the highest – Broadband uplink.
- No free lunch – a QoS configuration to optimize VoIP quality will require some concessions on data throughput.
- ISP: QoS in the core less important than high availability
- Netflow extremely useful to determine characteristics of packets in building a QoS Service Policy

Drops, Latency, and Jitter

- Voice packet loss (drops) in testing or Internet deployments rarely are an issue—rather outages
- Latency as an absolute number (ideally < 250 ms) can be addressed by practical design and minimum bandwidth recommendations
- Jitter—relative latency of one packet to the next; however:
  - Different tools measure jitter differently
  - Generally higher absolute latency will also experience higher jitter values
- Within a geography (i.e. North America) the largest positive influence (after hardware encryption) to latency and jitter is the amount of bandwidth to the remote site

Latency and Jitter by Network Component



ToS Byte for VoIP Applications

IP Phones—
7960, etc.

IP
communicator

Voice GW

MEDIA

DSCP = EF

(IP Precedence 5)

SIGNALING

DSCP = AF31

or CS3 [*]

(IP Precedence 3)

```
class-map match-all VOICE
 match ip dscp ef
```

```
class-map match-any
                    CALL-SETUP
 match ip dscp af31
 match ip dscp cs3
```

Configurable …Verify

```
dial-peer voice 10 voip
 ip qos dscp ef media
 ip qos dscp CS3 signaling
```

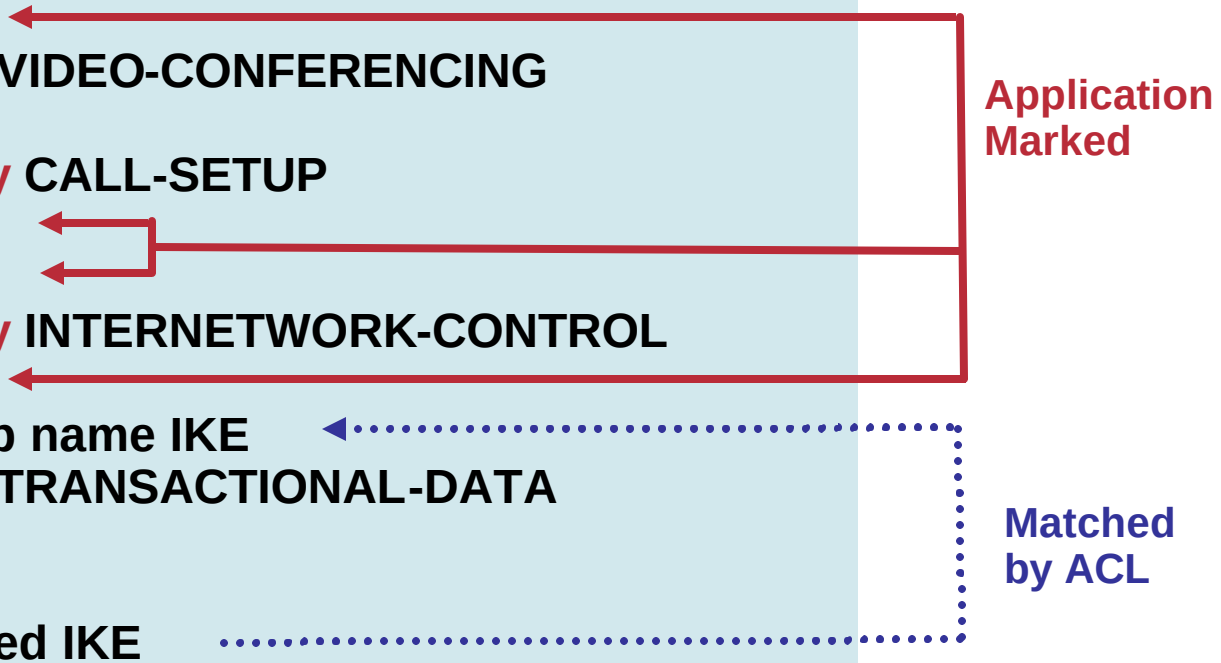
[*] Depends on Firmware - CSCdy33281 integrated releases Use CS3

Additional Information in Appendix

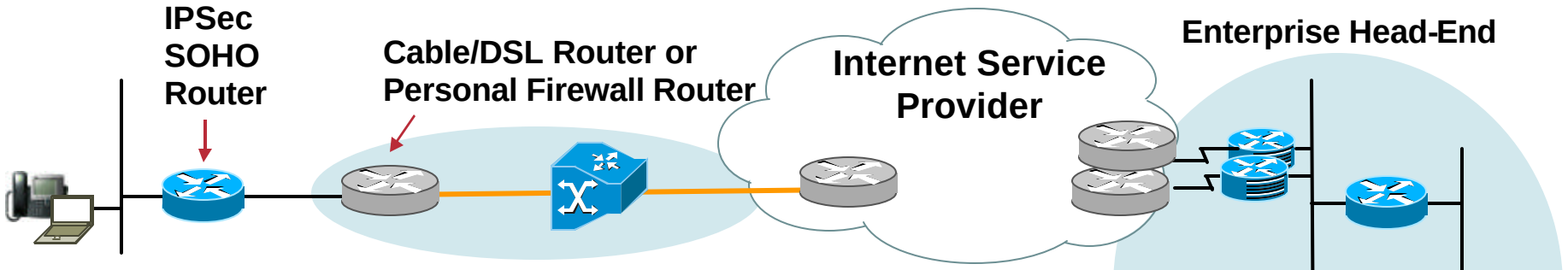
CLASS MAP

Either the Application Will Mark Traffic or the Router Will Select via an ACL and Optionally Re-Mark Packets

```
class-map  match-all VOICE
  match ip dscp ef
class-map match-all VIDEO-CONFERENCING
  match ip dscp af41
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
ip access-list extended IKE
 permit udp any eq isakmp any eq isakmp
```



CBWFQ Hierarchical Class-Based Weighted Fair Queuing
Shaper Provides Congestion Feedback



Broadband (Cable or DSL) Service Provider

```
policy-map V3PN-teleworker
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
  class VOICE
    priority 128
  class class-default
   fair-queue
   random-detect
policy-map Shaper
  class class-default
   shape average 182400 1824
   service-policy V3PN-teleworker
!
```

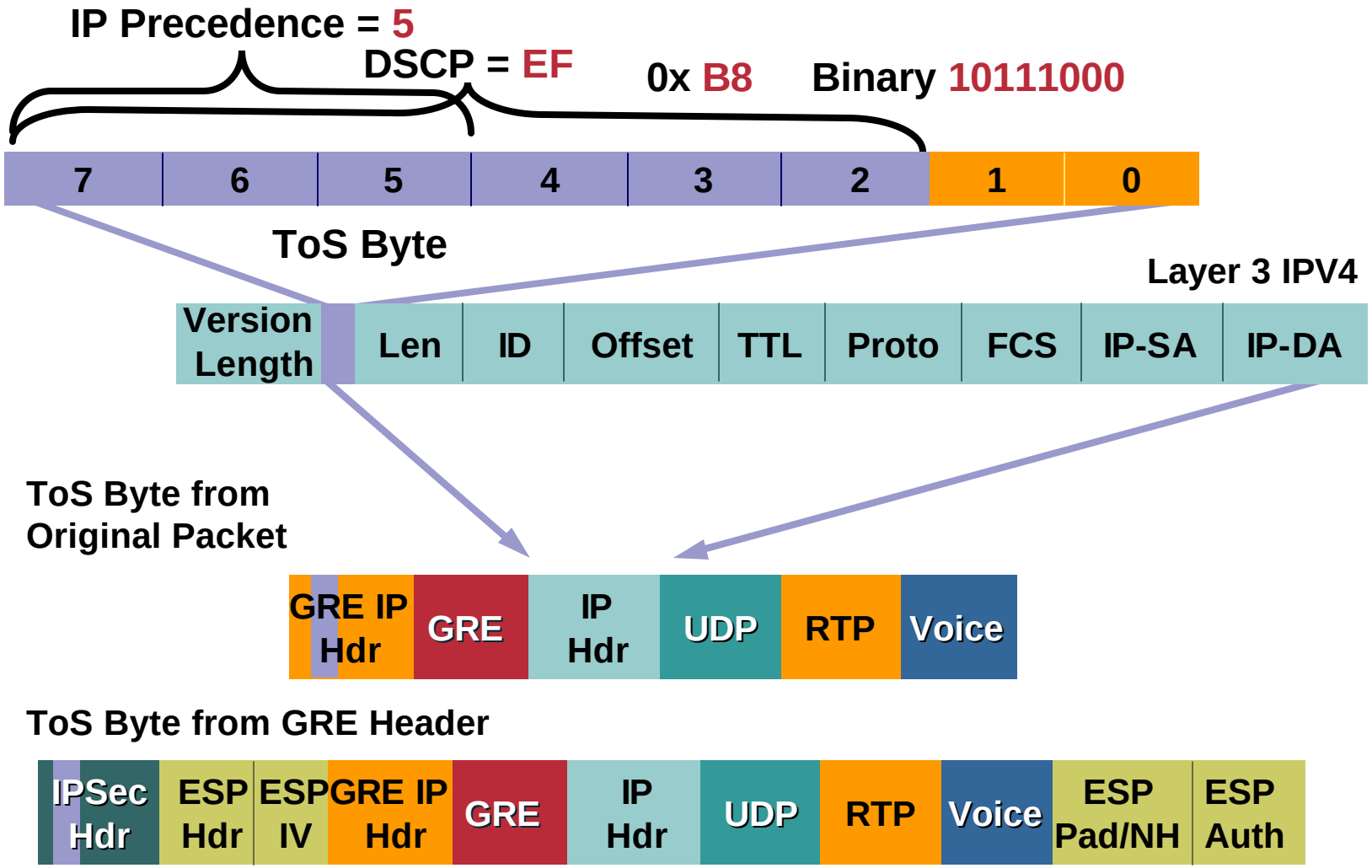
Shape at % of Estimated Rate with Interval of 10ms

```
!
interface Ethernet 0
 ip address 10.81.7.0 255.255.255.240
 ip route-cache flow
 ip tcp adjust-mss 542
 ip inspect CBAC in
!
interface Ethernet 1
 description Outside
 ip address dhcp
 ip access-group INPUT_ACL in
 service-policy output Shaper
 ip route-cache flow
 ip tcp adjust-mss 542
 duplex auto
 no cdp enable
 crypto map TELEWORKER
```

Because LFI not Available

Additional Information in Appendix

ToS Byte Copy for GRE and IPSec



IP Security (IPSEC)

Voice-Enabled IPSec VPNs

No Changes from a Typical VPN Deployment

Implement

- **Hardware Encryption Acceleration**
- **Diffie-Hellman Group 2 (1024 bit) for IKE**
- **Long keys (IOS "K9" images 3DES or AES-128,192 or 256)**
  - **870 Series supports AES in HW, 830 Series does not**
- **Secure hash algorithm (SHA) - HMAC**
- **Tunnel or transport mode**
- **Default lifetimes for**
  - **IKE (24 hr)**
  - **IPSec (1 hr)**
- **Enable qos pre-classify**

Encryption and Tunneling Configuration Options
Which Crypto Is Right for You?

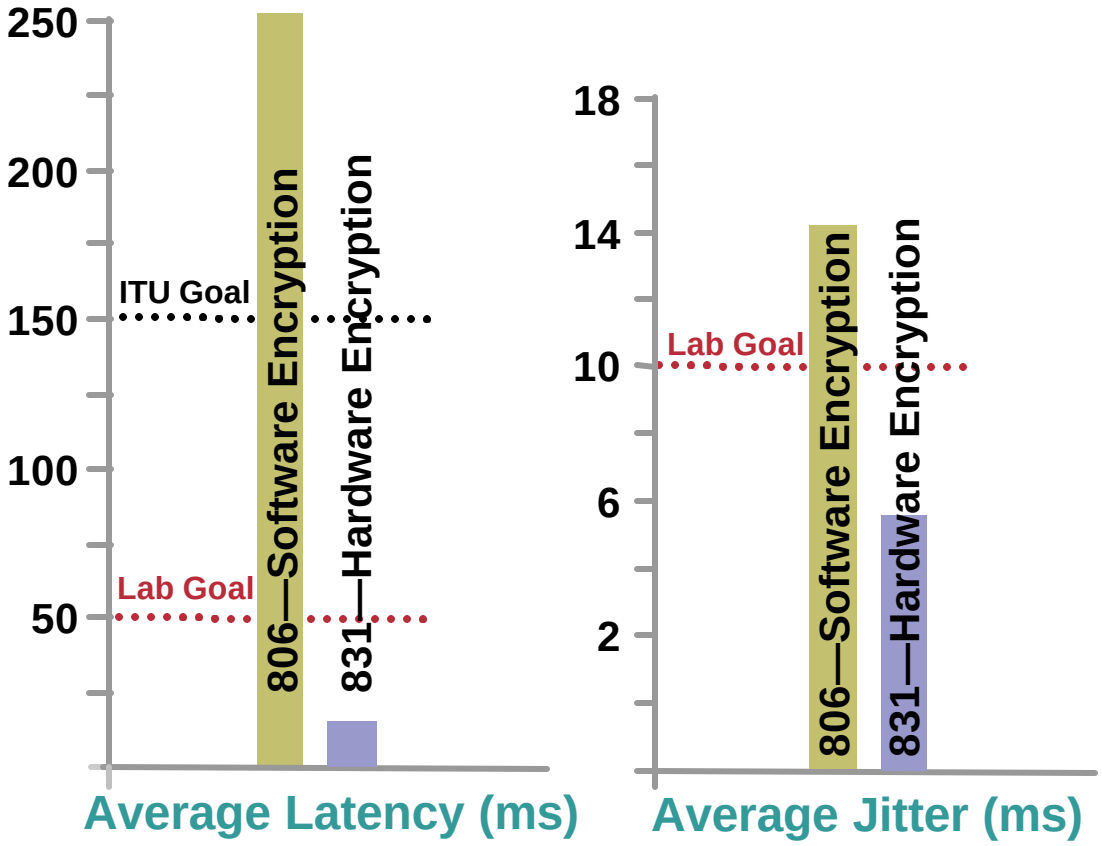
Cisco.com

	IP Mode	Restrictions	Keepalive
IPSec Static Crypto Map	Unicast	No IPmc	IKE DPD
IPSec Dynamic Crypto	Unicast	No IPmc	IKE DPD
IPSec Dynamic Crypto with GRE	IP Multicast/ Multiprotocol	None	IKE DPD /GRE/RP
DMVPN	IP Multicast [hub – spoke only]	VoIP Hub and Spoke Only	IKE DPD / RP NO GRE KEEPALIVE
EZVPN	Unicast	Softphone May Require Network Extension Mode	IKE DPD
IPSec High Availability	Unicast	No IPmc	IKE DPD /HSRP
IPSec/GRE High Availability	Multicast/ Multiprotocol		IKE DPD /HSRP

Hardware Encryption Acceleration

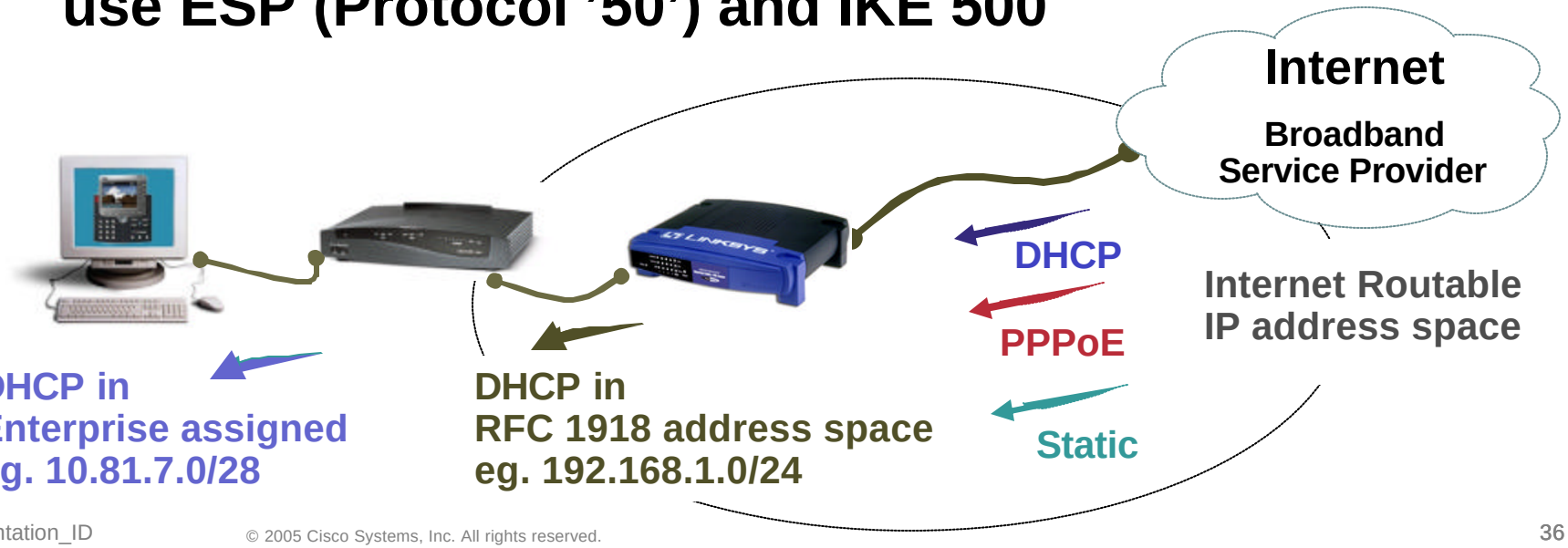
Minimize Impact of Crypto's CPU Consumption Always Implement Hardware Acceleration

- Software encryption exceeds both ITU and Cisco lab testing goals
- Voice (VoIP) quality demands low latency and jitter
- Supported in all products, 830 through 6500



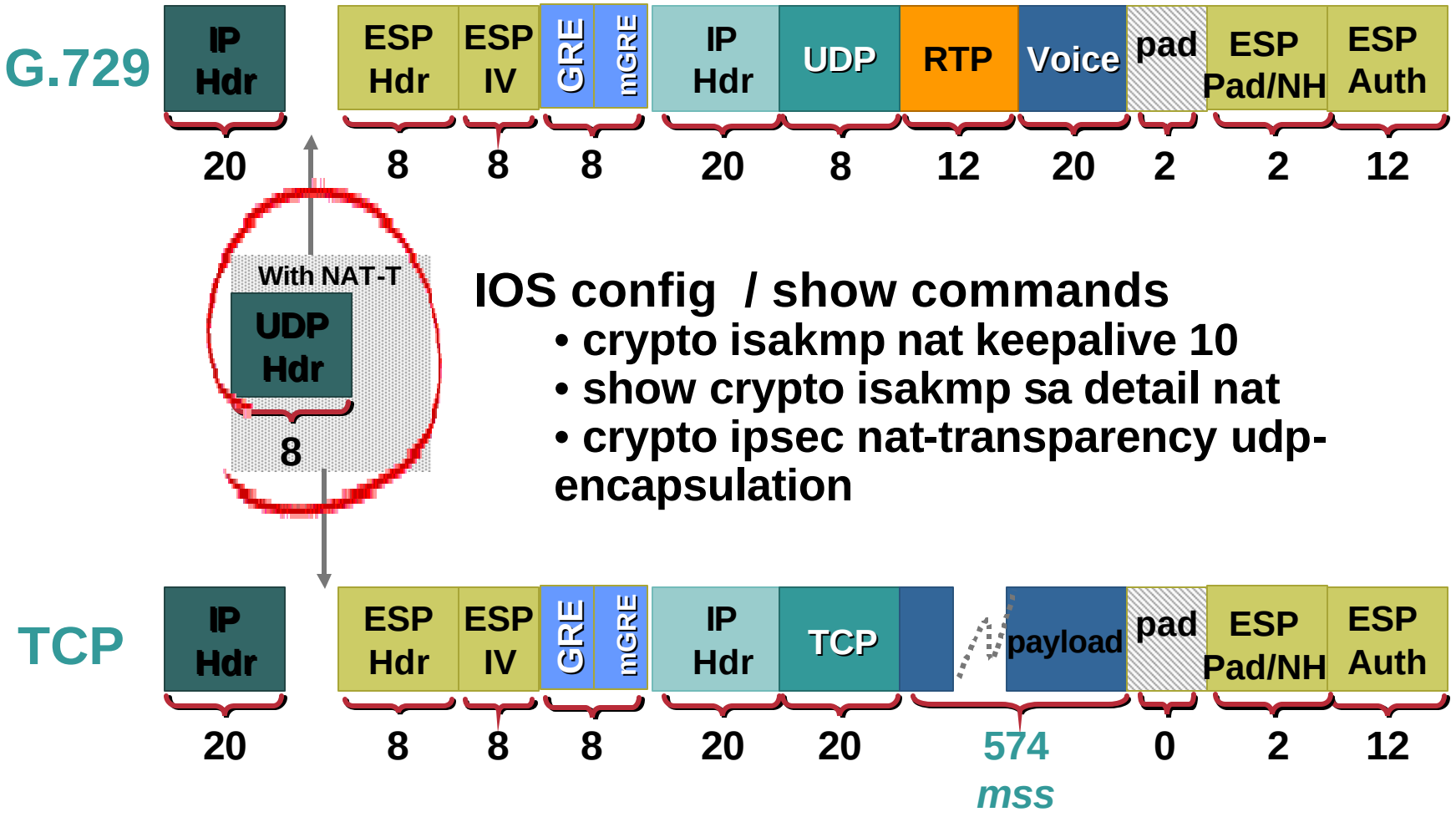
NAT-Traversal (RFC3947) [1/2]

- NAT/pNAT router typical for residential broadband
- Facilitates deployment – Outside Interface of VPN router always DHCP regardless of how service provisioned
- With NAT-T enabled and no NAT/pNAT device, will use ESP (Protocol ’50’) and IKE 500



NAT-Traversal (RFC3947) [2/2]

Additional 8 byte UDP Header



IOS config / show commands

- crypto isakmp nat keepalive 10
- show crypto isakmp sa detail nat
- crypto ipsec nat-transparency udp-encapsulation

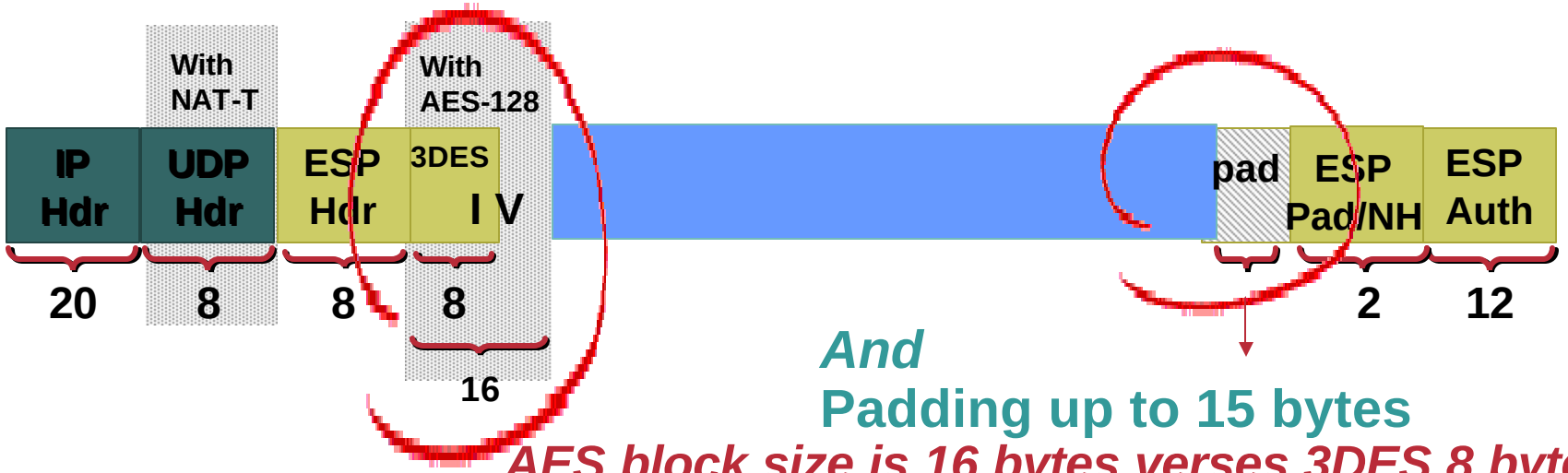
Advanced Encryption Standard (AES) - Rijndael

Slightly More Bandwidth Consumed Than 3DES

AES-128 192 256 and 3DES Similar Hardware Accelerated* Performance

However

AES Initialization Vector (IV) is 16 bytes



And

Padding up to 15 bytes

AES block size is 16 bytes verses 3DES 8 bytes

*** AES not HW accelerated on 830 Series***

Authentication and Segmentation

Authentication and Segmentation

- **Authentication –** ***validation of identity of device and end-user***

Device

- **Digital certificate / public key (PKI)**
- **Initiate IKE Aggressive Mode - with central pre-shared key repository**

User

- **EZVPN Remote Phase II**
- **Authentication Proxy / 802.1x**

Requirements:

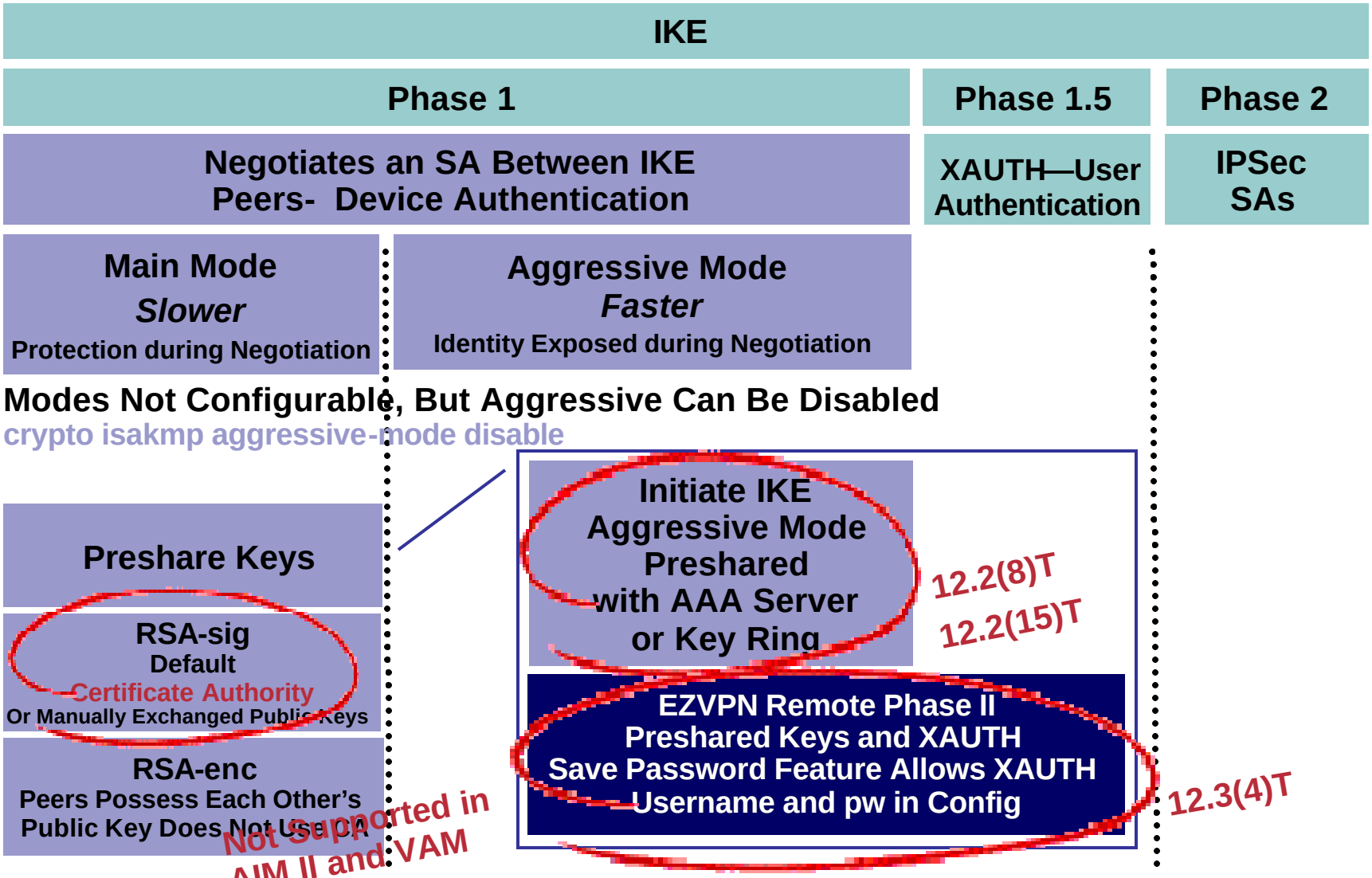
- **Support Dynamic Addressing**
- **Must scale and be manageable**

- **Segmentation –** ***separation between enterprise and family network resources***

  - **Physical Segmentation**
  - **DMZ port**
  - **VLANS**

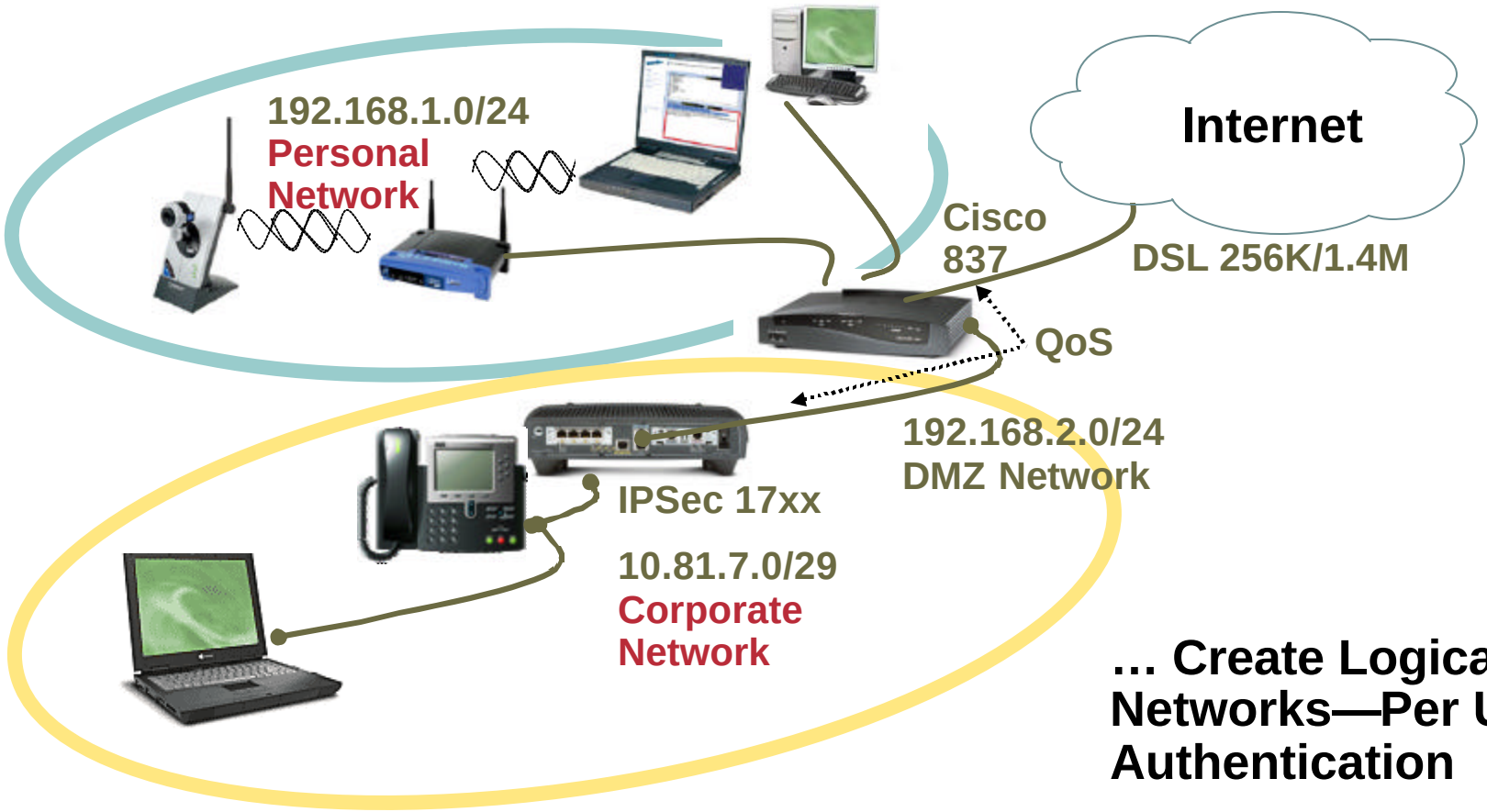
Authentication Methods Device (Router)

Three Practical Choices for Teleagent Deployments



Case Study—Home Network Connection
Physical Separation of Spouse and Children

Eliminate One Router to Reduce Costs …



… Create Logical Networks—Per User Authentication

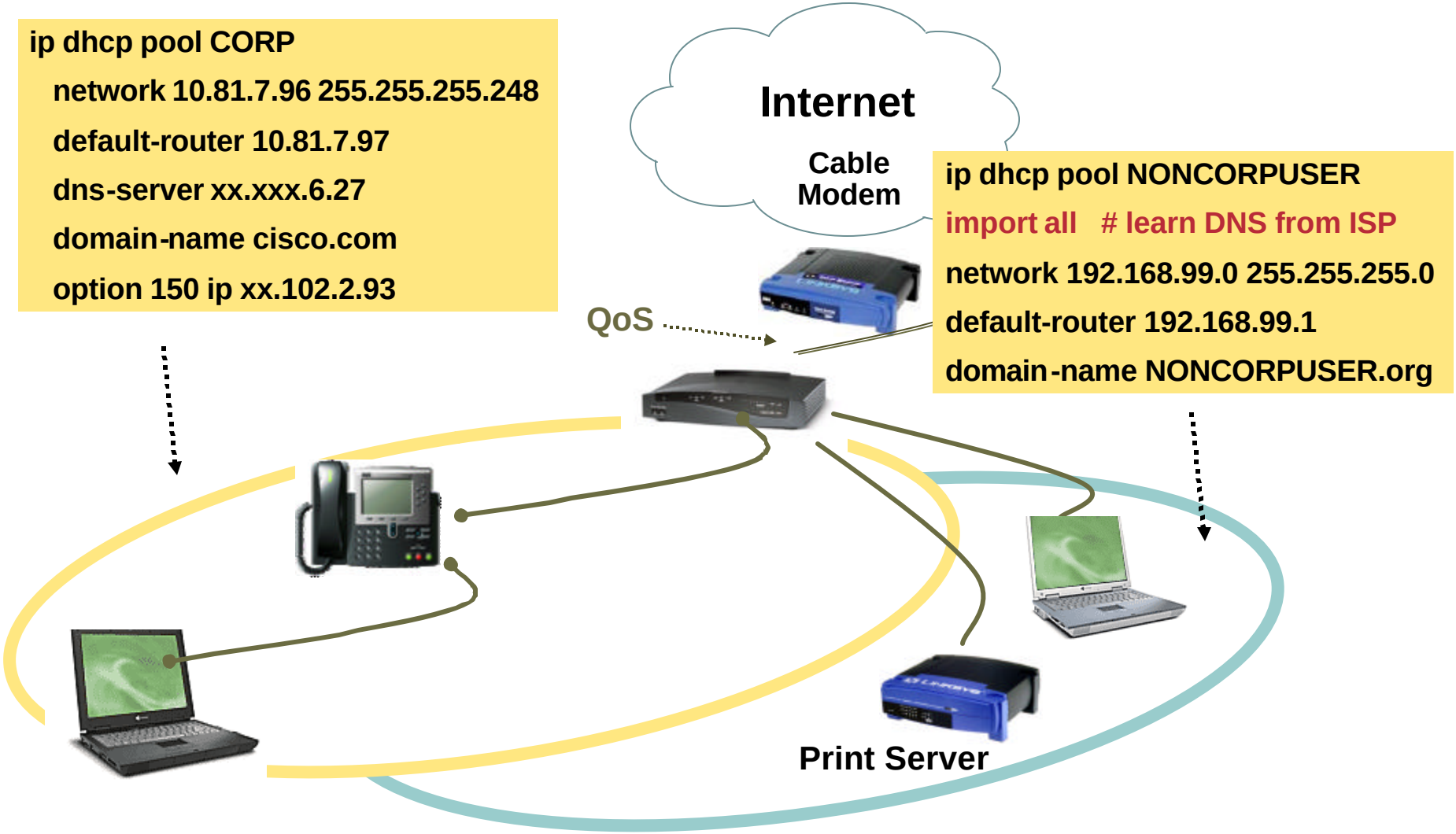
Cisco IOS Firewall Authentication Proxy

- HTTP/HTTPS initiated authentication via web browser
- Valid for all types of application traffic
- Provides dynamic, per-user authentication and authorization via TACACS+ and RADIUS protocols
- Works on any interface for inbound or outbound traffic
- Router's ACL must permit IP Phone access without authentication – IP Phone either static IP address or DHCP pool with only one IP address
- Spouse and children's PC will be NAT/pNAT'ed to the Internet
- QoS Service Policy (output) can prioritize Enterprise vs. Internet packets

IEEE 802.1x for Cisco 830

Enables Logical Separation of Spouse and Children


```
ip dhcp pool CORP
   network 10.81.7.96 255.255.255.248
   default-router 10.81.7.97
   dns-server xx.xxx.6.27
   domain-name cisco.com
   option 150 ip xx.102.2.93
```



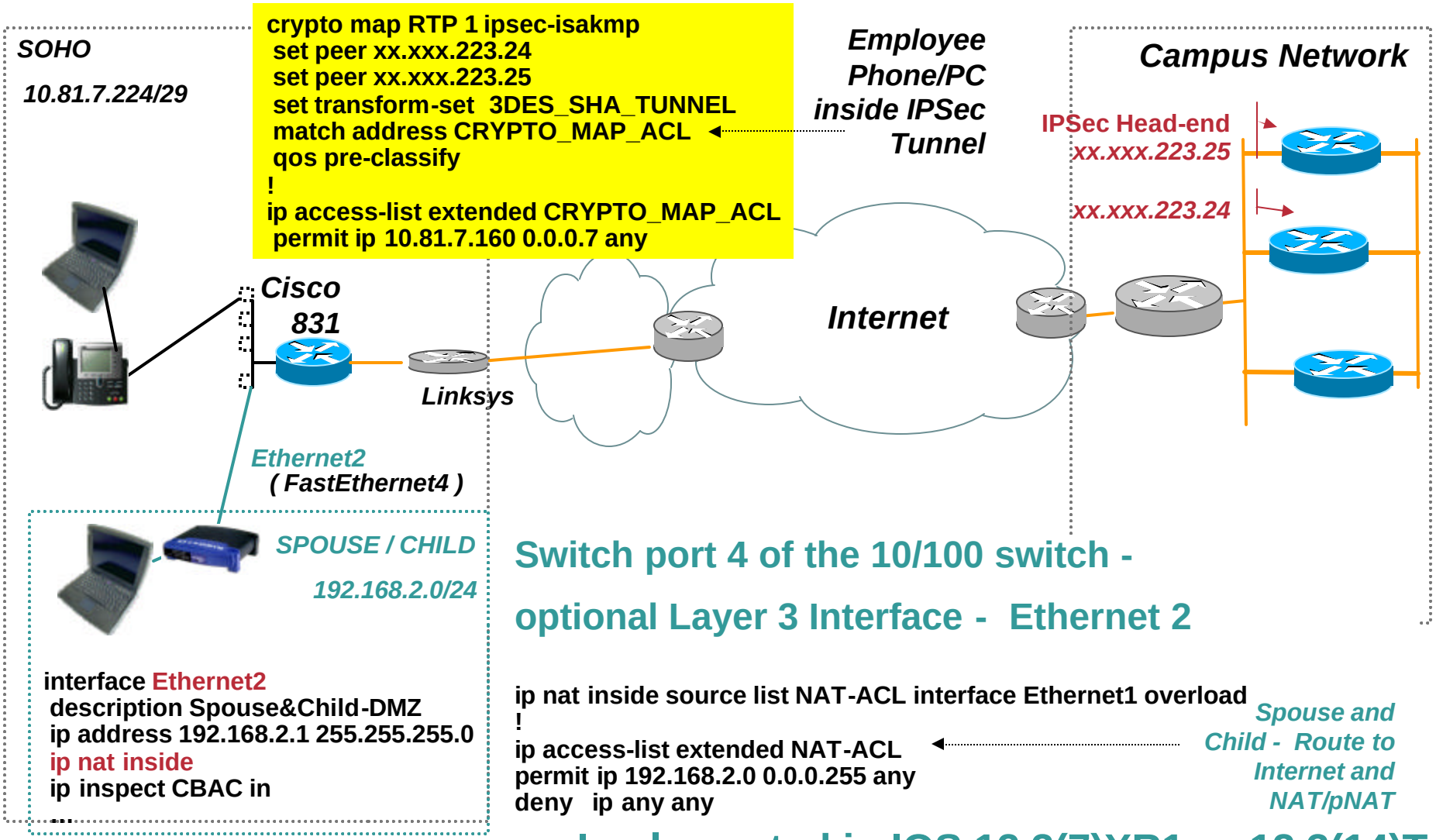

```
ip dhcp pool NONCORPUSER
import all   # learn DNS from ISP
network 192.168.99.0 255.255.255.0
default-router 192.168.99.1
domain-name NONCORPUSER.org
```

IEEE 802.1x for Cisco 830 Spouse and Child

Cisco.com

- User credentials sent Layer 2—login prompt on PC
  - EAPOL (Extensible Authentication Protocol over LAN)
- Unauthenticated users allowed access to Internet
- Logical Separation: 2 IP Networks—2 DHCP Scopes
- CDP used for IP phone discovery
  - device authorize type cisco ip phone
- By default, sharing between home devices permitted—allows print and file sharing
- PCs with static IP addresses must also authenticate
- PC must have IEEE 802.1x supplicant (client) code

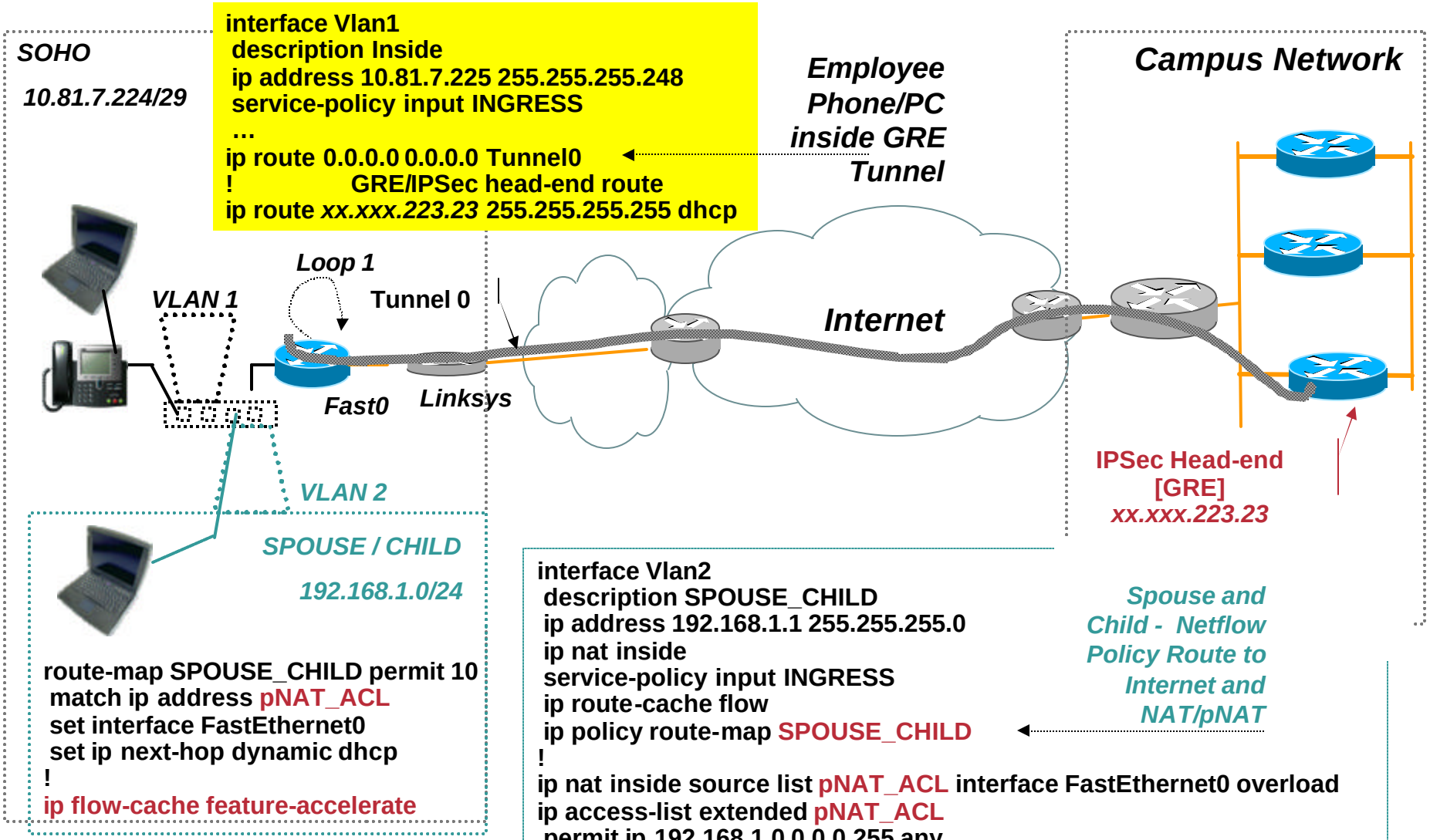
Demilitarized Zone (DMZ) port
Cisco 830 series routers



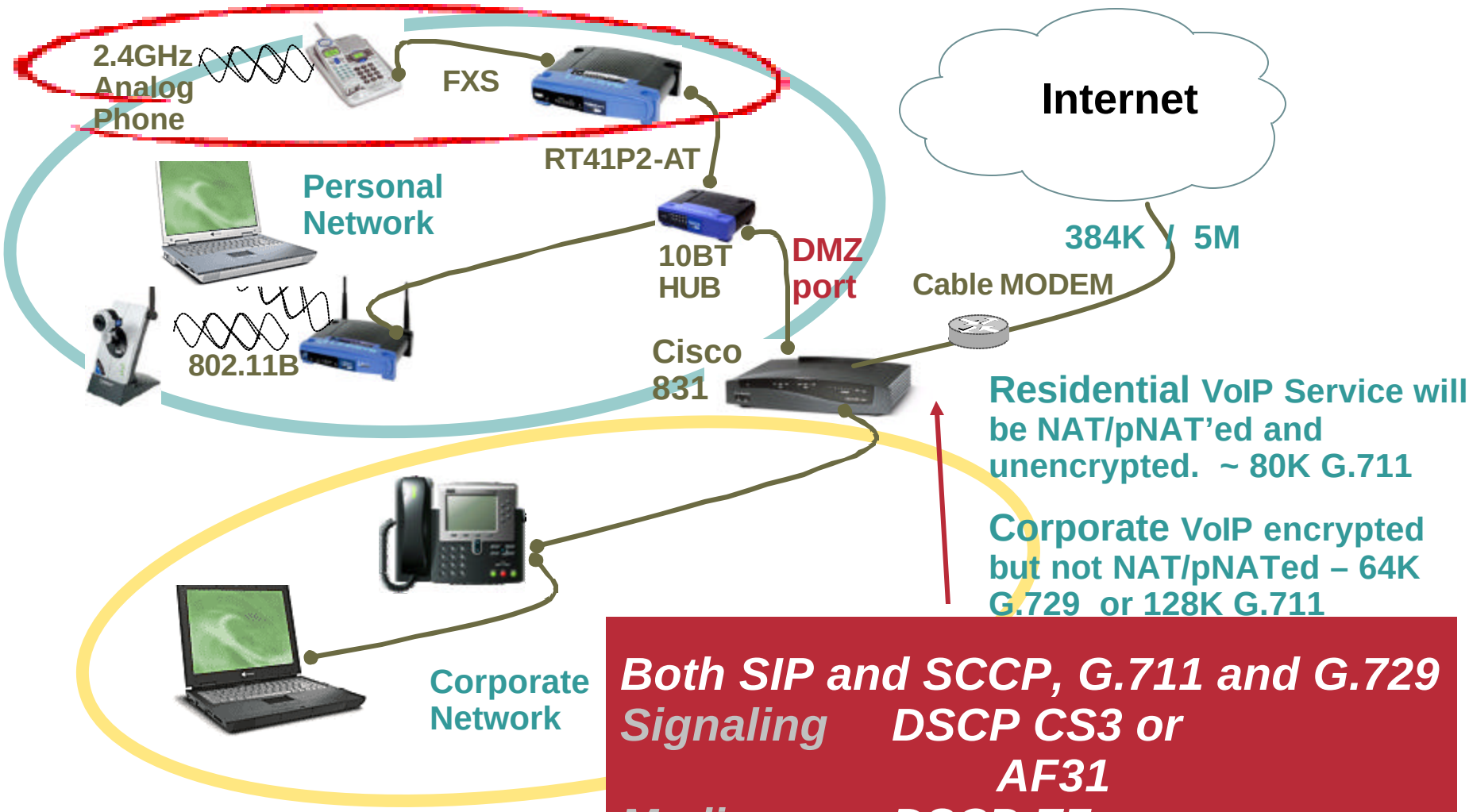
VLAN SOHO Routers

Cisco 87x and 1711 or 12 and 17xx/18xx with WIC-4ESW

Cisco.com



Residential VoIP Service
Topology and QoS Configuration



Residential VoIP Service will be NAT/pNAT'ed and unencrypted. ~ 80K G.711

Corporate VoIP encrypted but not NAT/pNATed – 64K G.729 or 128K G.711

Both SIP and SCCP, G.711 and G.729

Signaling ***DSCP CS3 or AF31***

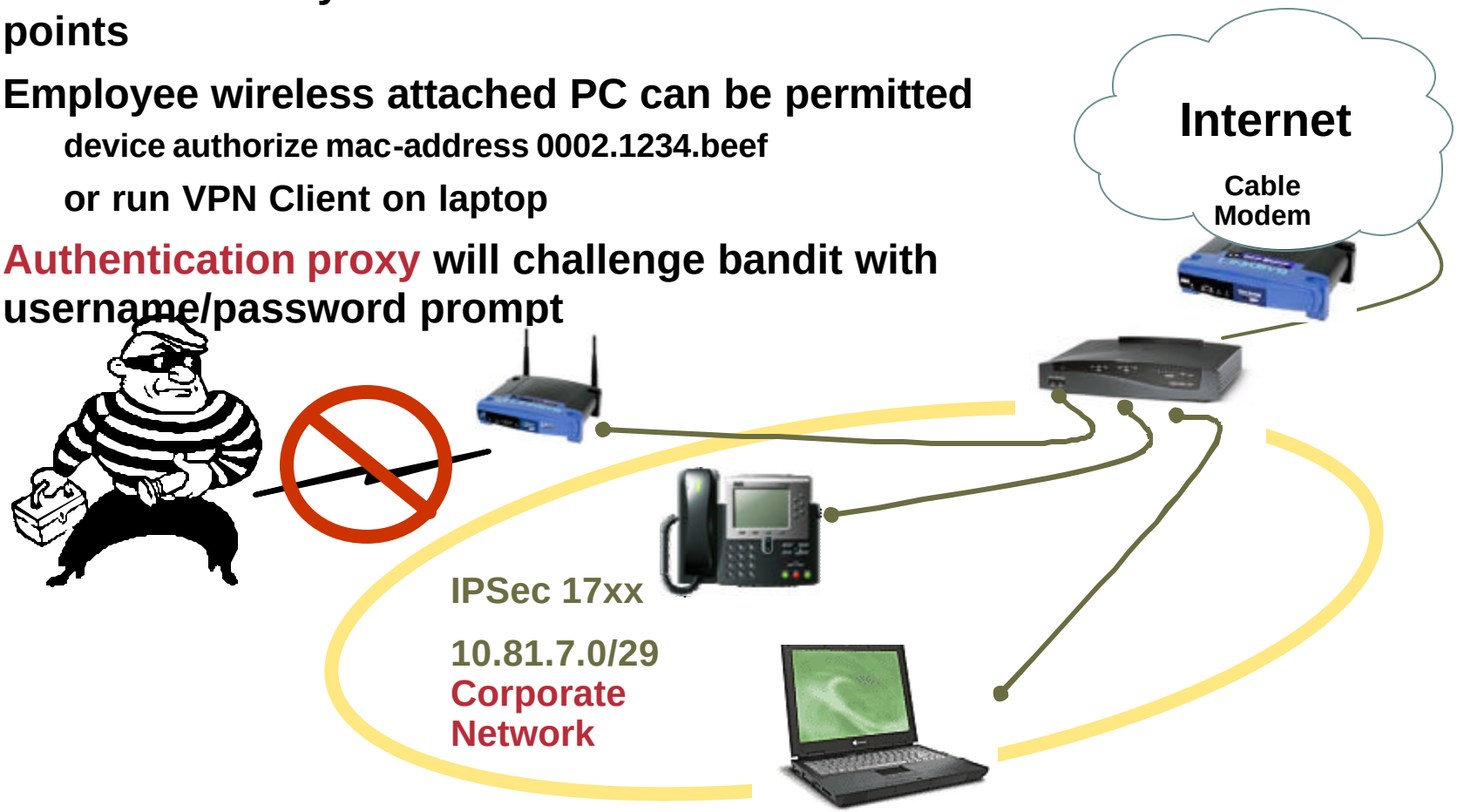
Media ***DSCP EF***

Home Wireless for Voice enabled Teleworker

Today's Deployment Capability—User Authentication

Cisco.com

- **802.1x for 830 EAP over LAN (EAPoL) Packets not forwarded by switches or wireless access points**
- **Employee wireless attached PC can be permitted**
  - **device authorize mac-address 0002.1234.beef**
  - **or run VPN Client on laptop**
- **Authentication proxy will challenge bandit with username/password prompt**

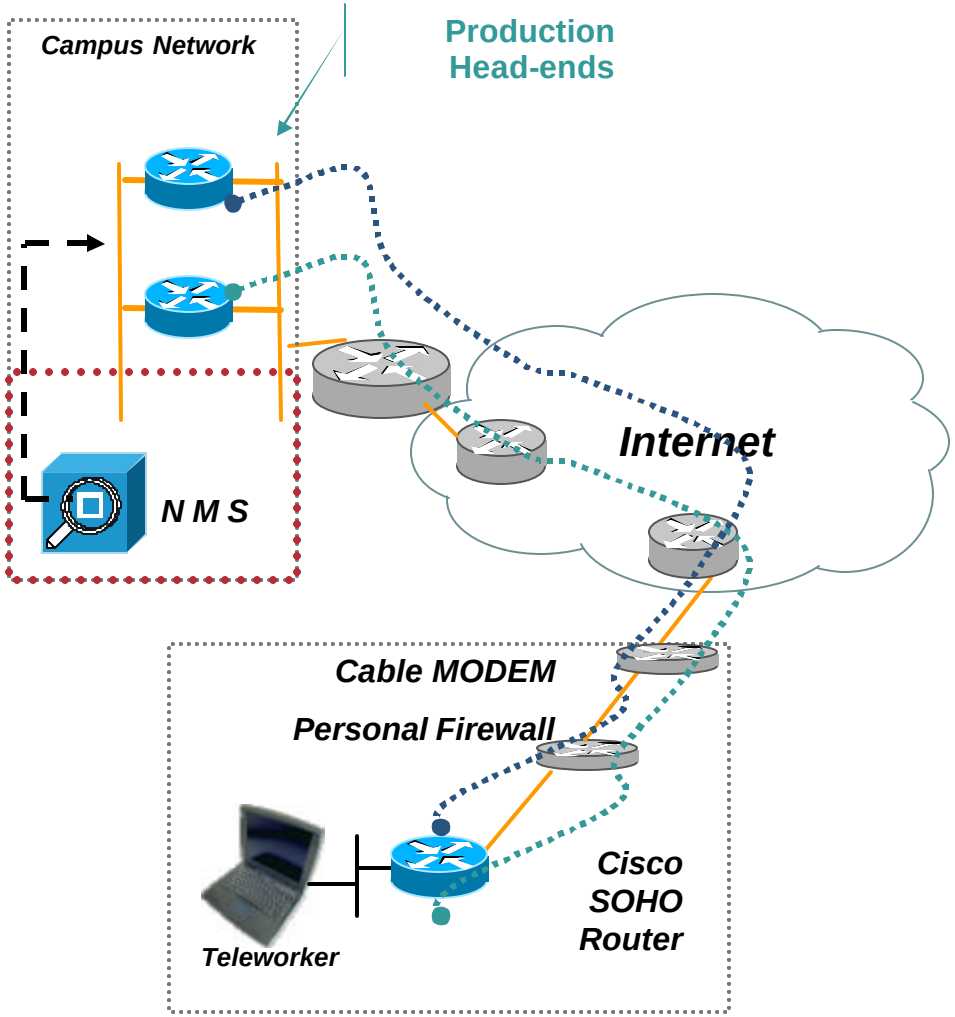


Provisioning (Configuration Management)

Deployment and Provisioning Challenge

- Large number of remote nodes – deployment targets range from 1,000 to 10,000 teleagents
- Each teleagent requires:
  - Broadband MODEM / Personal Firewall
  - QoS and VPN Router
  - Workstation / Personal Computer
  - Hardware or Software IP Phone
- Goal - Efficiency in deployment and configuration
- Provisioning Models
  - *CENTRALIZED*
  - *TOUCHLESS (for IT Staff)*

Deployment and Provisioning
Centralized Provisioning Model



Deployment Steps:

- Factory ships router to IT
- IT sets up:
  - Load IOS Code
  - Enroll Certificate
  - Load Config (from template)
  - Enter user parameters
- IT validates and ships to user
- User plugs in and uses

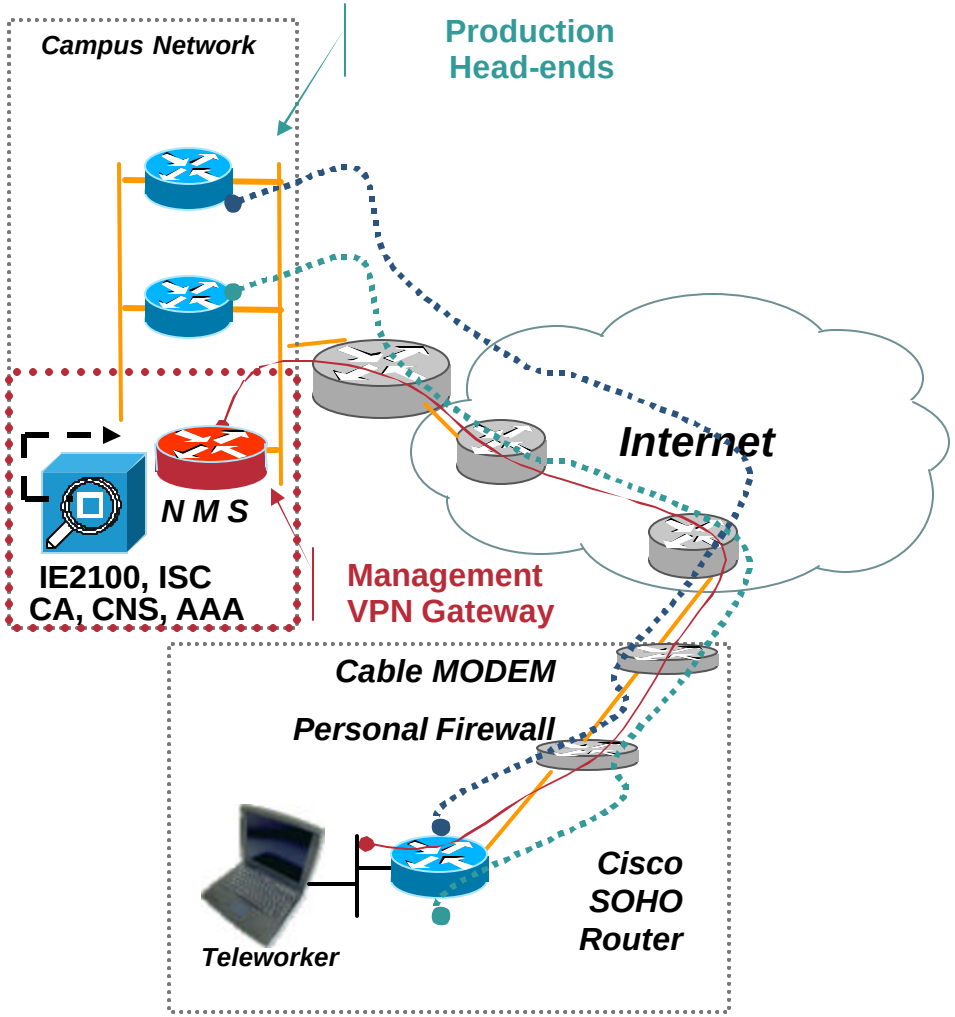
Management Steps:

- Ongoing config management same as any other router in network - IP Solution Center (ISC), CiscoWorks, etc.

Centralized Provisioning Model
Pros/cons

- **Plug ‘n Play for End User**
- **End User Receives All Necessary Equipment in One Shipment - Cisco Router, IP Phone, Laptop, Cables, Power supplies.**
- **Router’s configuration and connectivity is tested before shipment. *Show Interface and Show Log* will identify most problem during install.**
- **IT staff (intern?) to unbox, load IOS, configure and test. Scripts to automate this process will minimize keyboard time – Unpacking and Packing labor intensive. Perhaps one manhour per router.**
- **5,000 user deployment at $30/hr = $150,000**
- **High probability of successful deployment for non-technical end users.**

Deployment and Provisioning
"Touchless" Provisioning Model



Deployment Steps:

- Factory ships router to user
- User follows "script" to establish first-time connection
- CRWS with EzSDD or EZVPN
- Setup:
  - Cert Enrollment
  - Config (from template)
  - User parameters
- User continues to use

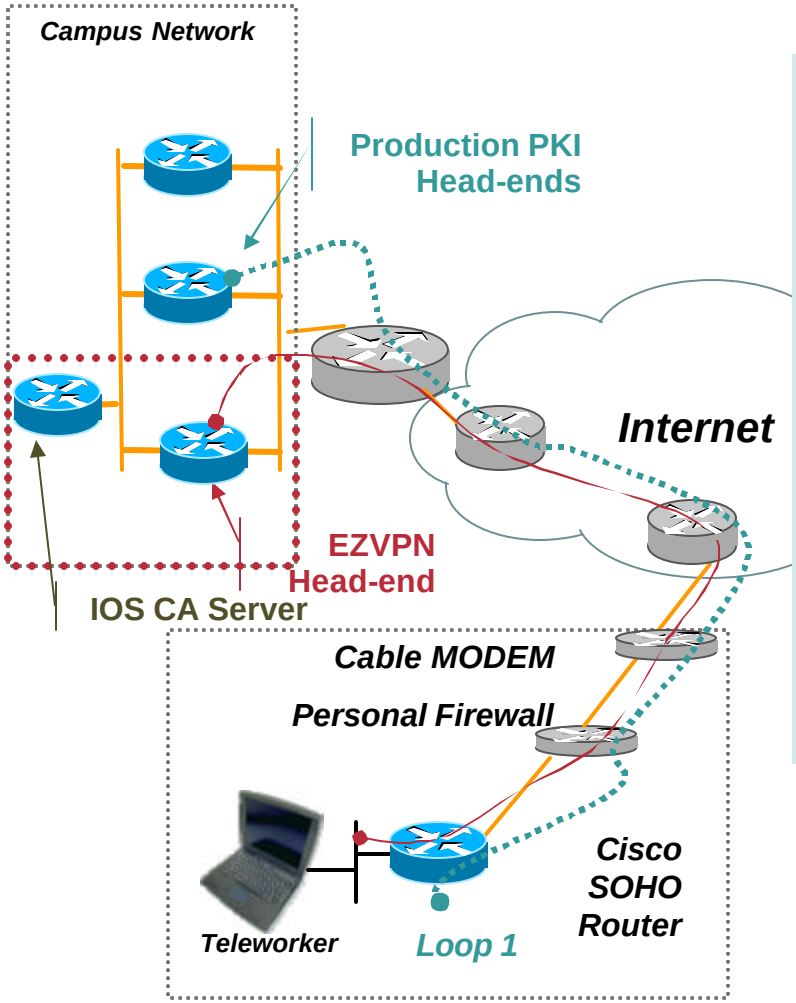
Management Steps:

- Management Subnet/ Tunnel
- IP Solution Center (ISC) ongoing configuration management

Case Study
Provisioning using EZVPN

- **Assume User has the ability to connect to console using some terminal emulator over the console port.**
- **User will ‘cut-n-paste’ an initial configuration to bring up an EZVPN IPSec tunnel.**
- **Central site will access remote router via EZVPN tunnel for certificate enrollment and final configuration.**
- **This method works behind personal firewall as remote router initiates connection and can use NAT-T.**

EZVPN BOOTSTRAP



1. Remote User Enters Minimal EZVPN
2. IPSec tunnel established to mgt net
3. PKI Certificate configured
4. Basic Crypto / GRE configured
5. Both EZVPN and IPSec/GRE UP
6. Router mgt subnet thru GRE
7. Change IP address of Remote NET
8. Reconnect via Remote NET
9. Remove EZVPN from Interfaces
10. Complete configuration via GRE
11. Ongoing management thru GRE

"Touchless" Provisioning Model
Pro/Cons

- **Router shipped directly to end-user, no unpacking and packing at central location**
- **Cisco IOS installed at factory must be level to support initial deployment**
- **EZSDD Browser version / configuration**
- **With PCs, every user a System Administrator, every user a Network Administrator**
- **End User and IT Help Desk Bear the Effort of Deployment**
- **Installation must be carefully thought out and documented. Software development at IT for user enrollment**

Case Study
Cisco IT deployment

Cisco.com

- **Cisco Internal deployment of Enterprise Class Teleworker uses *"Touchless" Provisioning Model***
- **End User Deployment Steps**

  Order Home Broadband – *Monthly Approved VPN reimbursement below $75 do not require receipts – expenses submitted monthly and direct deposited.*

  Order Cisco 831

  Register for ECT service – *Web page with Mgr Approval*

  Install Hardware – *Cisco Router Web Set-up (CRWS)*

  Initial Software Configuration – *Easy Secure Device Deployment (EzSDD)*

  Full Configuration - *IP Solution Center (ISC)* using Management VPN tunnel

- **On-going Management**

  ***IP Solution Center (ISC)* using Management VPN tunnel**

Quick Start Checklist
Cisco IT deployment

Cisco.com

VPN Hardware (ECT)

Quick Start Checklist

Support / Feedback

Follow these steps to get you up and running quickly with ECT:

ECT Quick Start Checklist		
☐	**1.**	Determine whether the ECT solution fits your needs.
☐	**2.**	Discuss this with your manager and get their approval to request the service and order the ECT equipment.
☐	**3.**	Establish/order a high-speed Internet connection for your home. If you're intending on connecting your IP telephone, please not that you will need at least a 256k upload speed from your ISP and that support will only be on a best effort basis.
☐	**4.**	Register for ECT Your manager receives an auto-generated e-mail request for approval from the service request system. See the registration process section for details.
☐	**5.**	Order the 831 router (pending your manager's approval), following the appropriate process for your region
☐	**6.**	Receive ECT hardware and use the following resources to complete installation.
	☐ **a.**	Follow the Hardware Setup Guide for physical installation instructions.
	☐ **b.**	Follow the ECT Installation and Configuration Guide - Cisco Router Web Setup (CRWS) to connect your ECT router to the Internet (via your ISP).
	☐ **c.**	Follow the ECT Installation and Configuration Guide - Easy Secure Device Deployment (EzSDD) to complete your ECT router configuration and connect to the Cisco corporate network.
☐	**7.**	Refer to the ECT web site for resources and support information to enhance your ECT service experience.

User Enters Specific Parameters
Cisco IT deployment

This information will be used to configure your home router. If this is incorrect your router will not work.:

***Service Provider:**	(Enter only, if 'Other')
***Service Type:**	
***Download Service Speed:**	
***Upload Service Speed:**	128k
Modem manufacturer and model name: ***(Eg: Motorola Surfboard..)***	
Will ECT router sit behind NAT/PAT router? ***(Eg: Linksys)***	(more info) [New Window]
***IP Address Assignment for ECT Router (E1 interface)**	(more info) [New Window]

'*' indicates a must entry field.

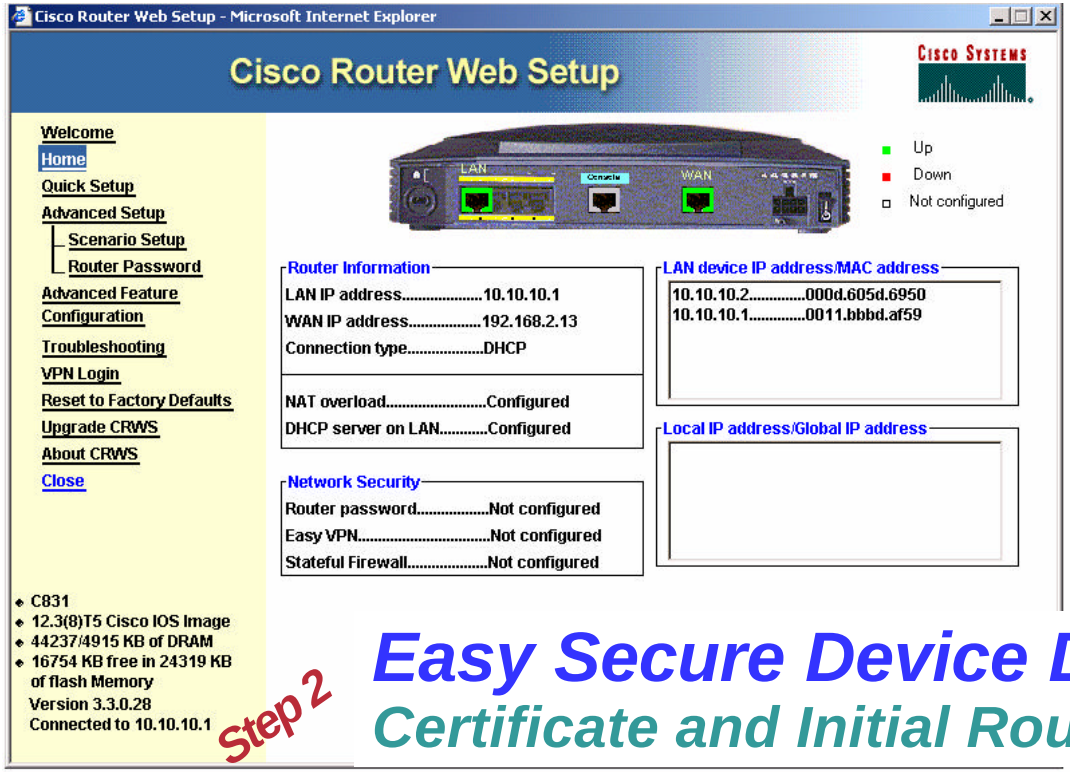
Continue Cancel

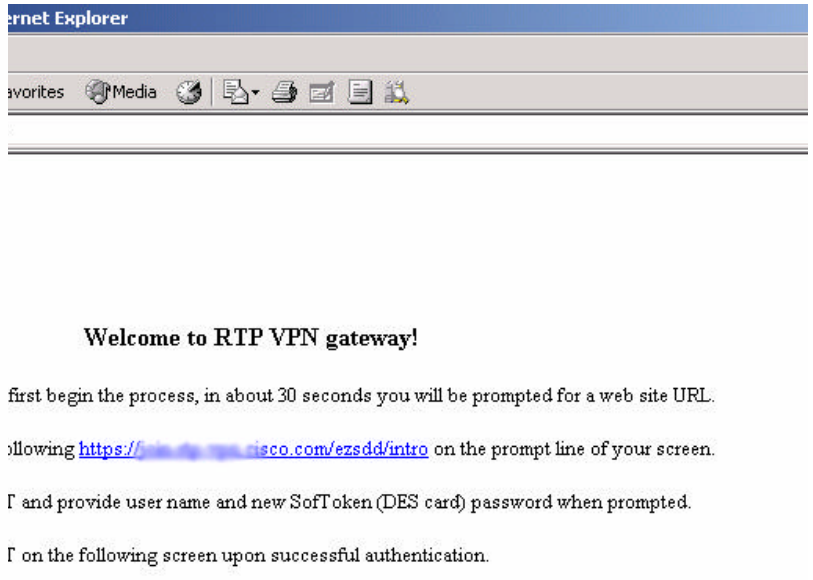
User Initiated Provisioning
Cisco IT deployment

Cisco.com

Step 1

Cisco Router Web Setup
Hardware Installation and Network Connectivity





Step 2

Easy Secure Device Deployment (EzSDD)
Certificate and Initial Router Configuration

Step 3

Full Configuration – IP Solution Center (ISC)

Voice Quality Management (Fault Management)

Troubleshooting, Monitoring, Test Tools

Cisco.com

- Proactive Monitoring is a Requirement to verify voice quality meets expectations
- Customer Requirement to Monitor and Rank Voice Quality of Teleagents
- Call Center Supervisor may mark agent unavailable if network faults will impact voice quality
- Validate SLA of Broadband / Internet Service Provider
- Case Study - Demonstrate Network Management Tools / Processes

  Service Assurance Agent (SAA) SAA renamed to IP SLA

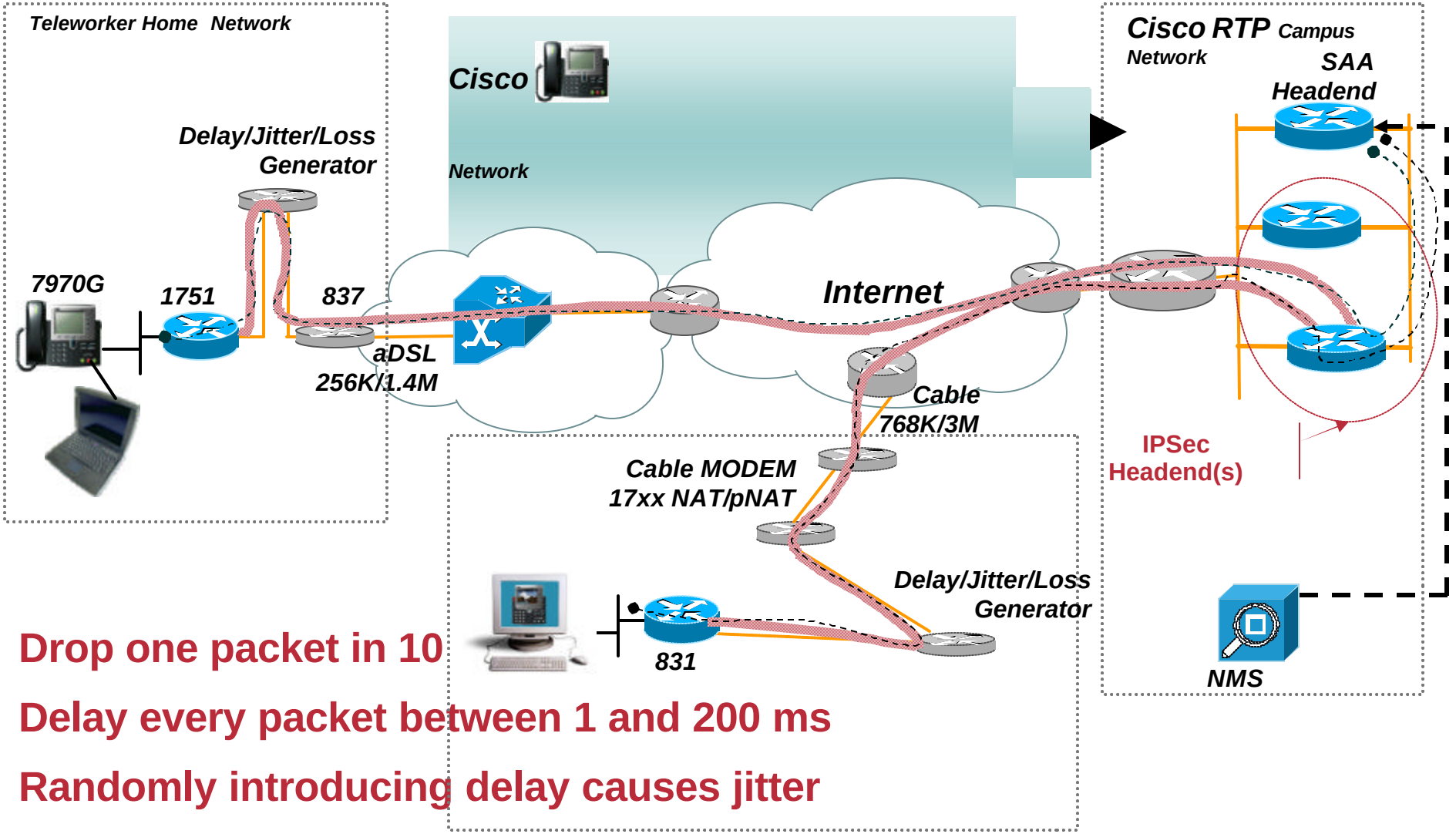
  www.cisco.com/go/saa www.cisco.com/go/ipsla

  CiscoWorks Internetwork Performance Monitor (IPM)

  www.cisco.com/go/ipm

  Packet loss, delay and jitter will be introduced artificially

Topology
Introduce Extreme Loss, Delay and Jitter

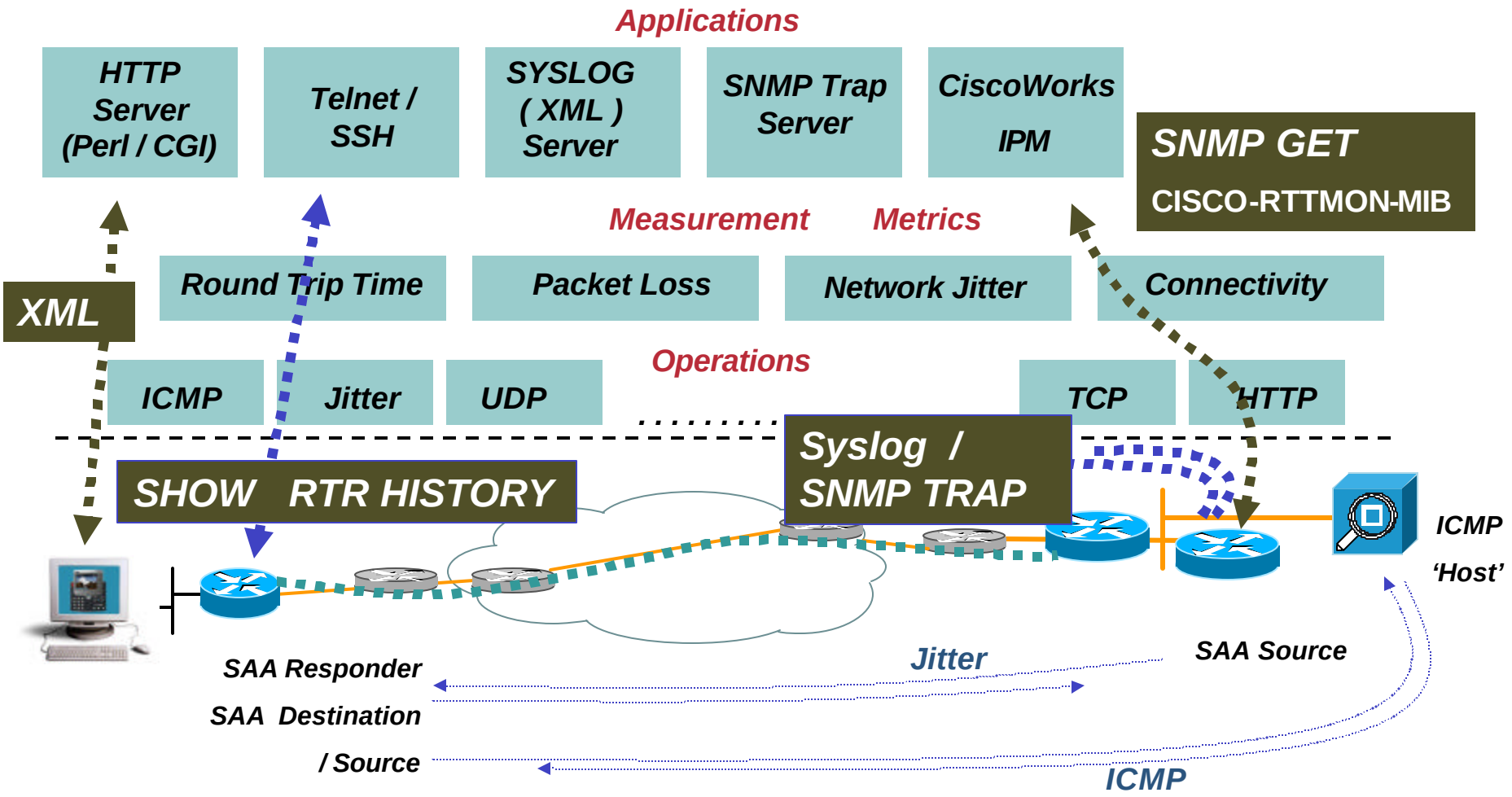


Drop one packet in 10

Delay every packet between 1 and 200 ms

Randomly introducing delay causes jitter

Service Assurance Agent (SAA)
VoIP Proactive Monitoring



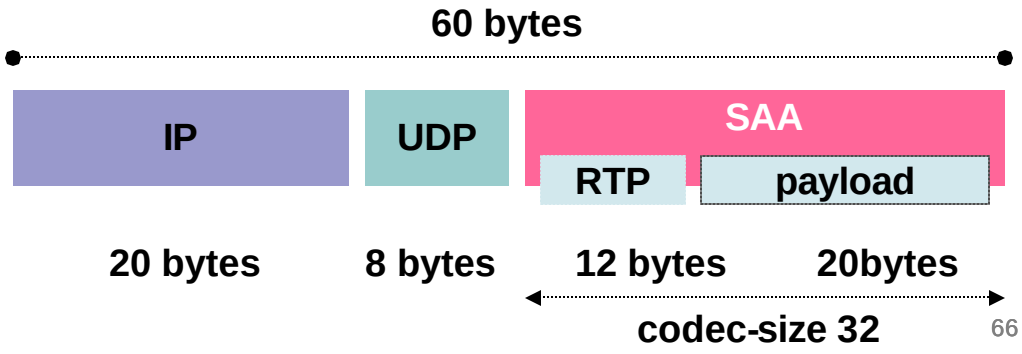
Additional Information in Appendix

IPM Generates a SAA Probe

Create a probe to measure jitter and latency, consume a minimum amount of bandwidth and pps rate, and proactively alert network manager to voice quality issues

```
rtr 4614
 type jitter dest-ipaddr 10.81.7.1 dest-port 16400 num-packets 20
 tos 160
 threshold 300
 owner 37|ipm-rtpnml-chi-Unknown
 tag ESE-IPTDemo
rtr reaction-configuration 4614 threshold-falling 100 threshold-type consecutive 3 action-type
trapOnly
rtr schedule 4614 life forever start-time now ageout 3600
```

Tests indicate an additional 26K allocated to the LLQ would be sufficient to place this traffic in the LLQ along with voice and not impact agent's voice quality.



Allocate Bandwidth in LLQ for SAA

Cisco.com

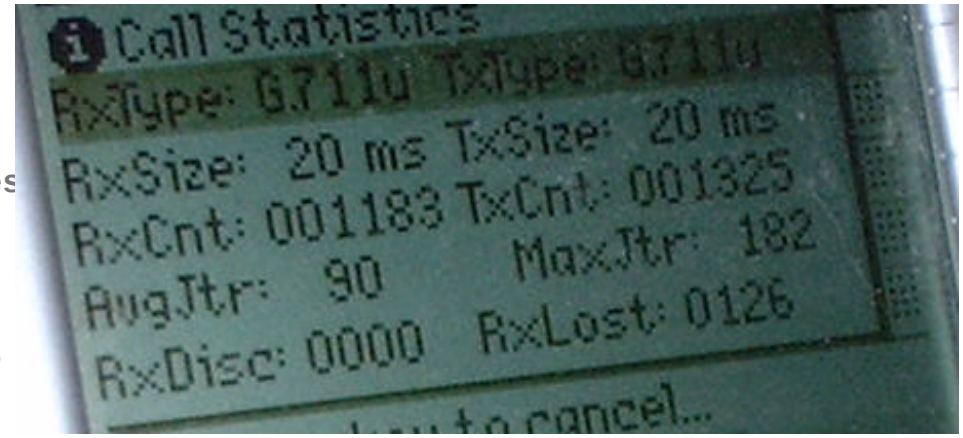
```
policy-map V3PN-teleworker
 description Note LLQ for ATM/DSL G.729=64K, G.711=128K
  class CALL-SETUP
   bandwidth percent 2
  class INTERNETWORK-CONTROL
   bandwidth percent 5
   set dscp cs6
  class VOICE
   priority 154
  class class-default
   fair-queue
   random-detect
policy-map Shaper
  class class-default
   shape average 182400 1824
   service-policy V3PN-teleworker
```

Allocating ~26K additional for SAA probe

During testing verified for IPcommv113-G711
- The voice stream is marked 0xB8 in both directions..
- Call setup is marked 0x68 in the phone to Call Manager direction,
- From Call Manager to IP Communicator, 0x00.

Delay/Jitter/Loss Generator Enabled aDSL 256K/1.4M


```
rtp-esevpn-saa#show rtr op 18
Entry number: 18
…
Latest RTT (milliseconds): 301
Latest operation start time: 14:59:52.344 es
Latest operation return code: OK
Voice Scores:
ICPIF Value: 55 MOS score: 1.0
RTT Values:
NumOfRTT: 15    RTTAvg: 401     RTTMin: 356
RTTSum: 6029    RTTSum2: 2431389
Packet Loss Values:
PacketLossSD: 4 PacketLossDS: 1
PacketOutOfSequence: 0  PacketMIA: 0    PacketLateArrival: 0
InternalError: 0        Busies: 0
Jitter Values:
MinOfPositivesSD: 25    MaxOfPositivesSD: 87
NumOfPositivesSD: 3     SumOfPositivesSD: 139   Sum2Posit
MinOfNegativesSD: 15    MaxOfNegativesSD: 18
NumOfNegativesSD: 6     SumOfNegativesSD: 99    Sum2Negat
MinOfPositivesDS: 1     MaxOfPositivesDS: 67
NumOfPositivesDS: 8     SumOfPositivesDS: 111   Sum2Posit
MinOfNegativesDS: 3     MaxOfNegativesDS: 35
NumOfNegativesDS: 5     SumOfNegativesDS: 80    Sum2Negat
Interarrival jitterout: 0       Interarrival jitterin: 0
….
```



One way latency

170 – 220 ms

MOS 1.0

10% packet loss

Jitter 25 – 87 ms

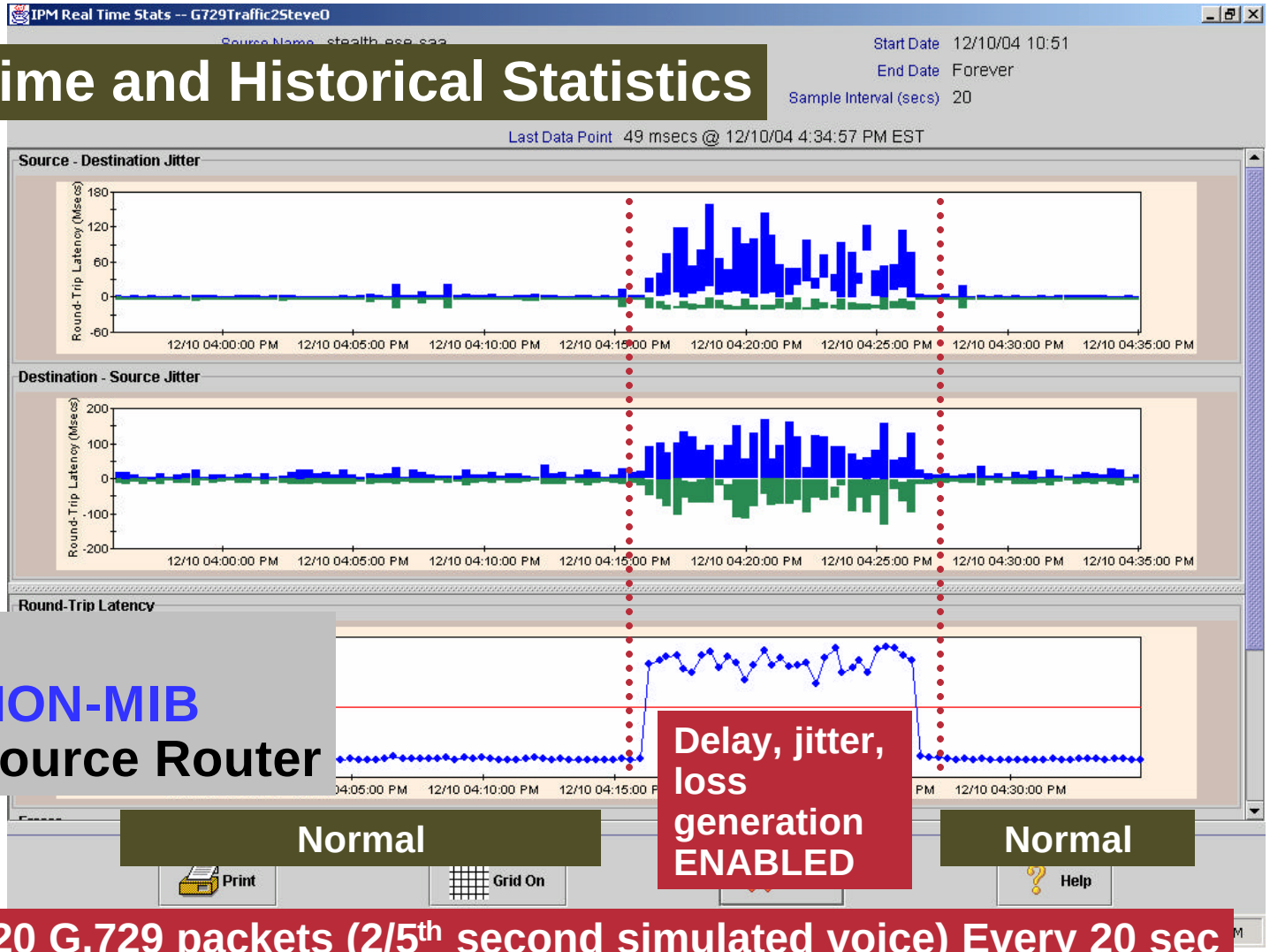
Normal (Good) Values are 40-50ms One Way Latency, 1-7 ms Jitter, No packet loss, MOS of 3.3

Internetwork Performance Monitor (IPM)

www.cisco.com/go/ipm

Cisco.com

Both Real Time and Historical Statistics



SNMP GET
CISCO-RTTMON-MIB
of the SAA Source Router

Normal

Delay, jitter, loss generation ENABLED

Normal

SAA generates 20 G.729 packets (2/5th second simulated voice) Every 20 sec

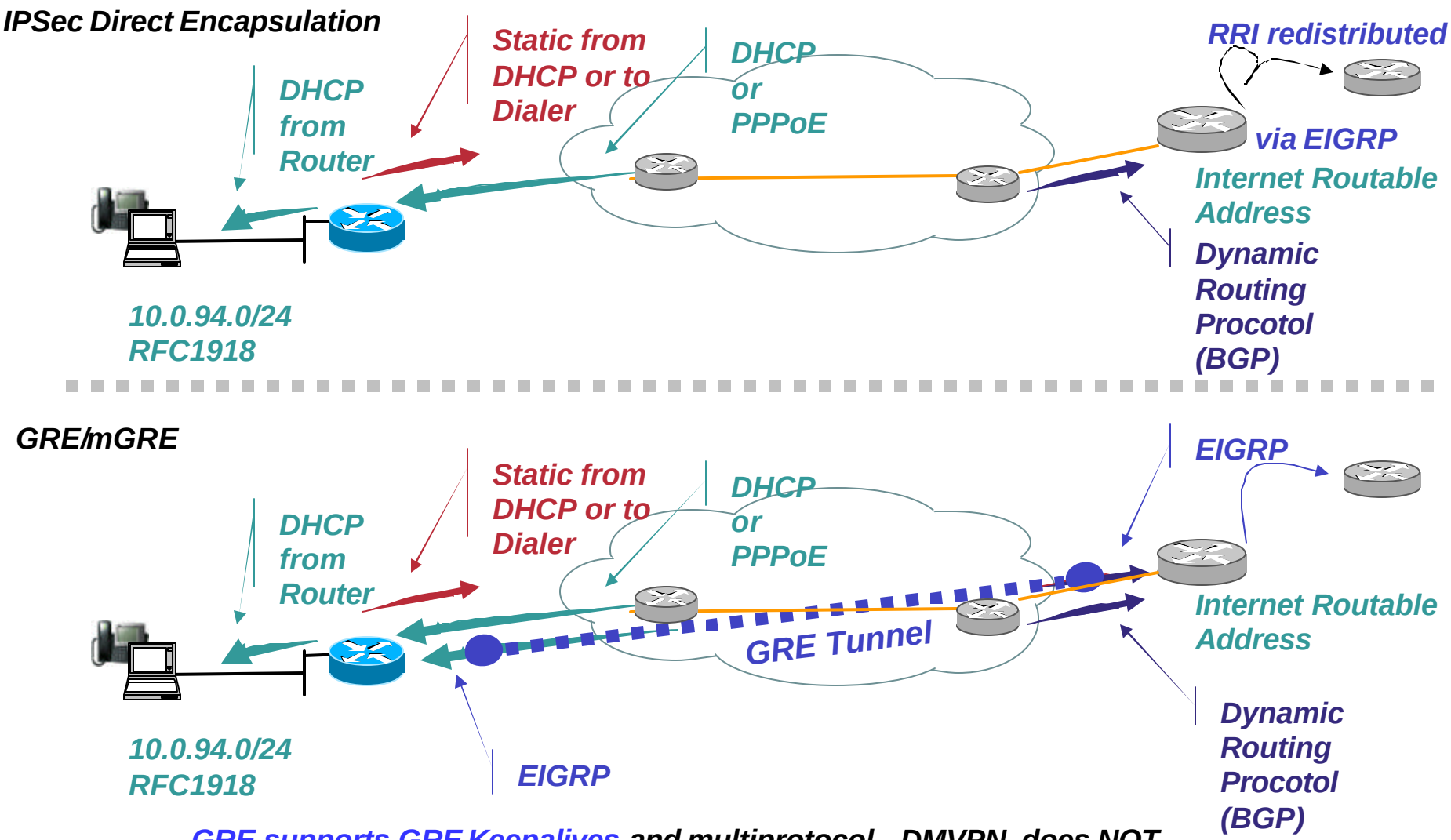
HEAD-END TOPOLOGY BACKUP and REDUNDANCY

HEAD-END TOPOLOGY BACKUP and REDUNDANCY

- Detecting and recovery from failure can range from as little as 1–3 seconds or as high as 60 seconds
- GRE tunnels, shadow GRE tunnels (GRE keepalive) IKE keepalive/Dead Peer Detection (DPD) and Reliable Static Routing Backup Using Object Tracking provide detection and recovery
- During head-end failure and recovery, active voice call may not drop, but registration with call manager often does
- In general, Internet deployments will see slightly higher incidence of link flaps (especially for teleworkers) than Frame Relay networks

Routing Information Sources
IPSec Direct Encapsulation and GRE/mGRE

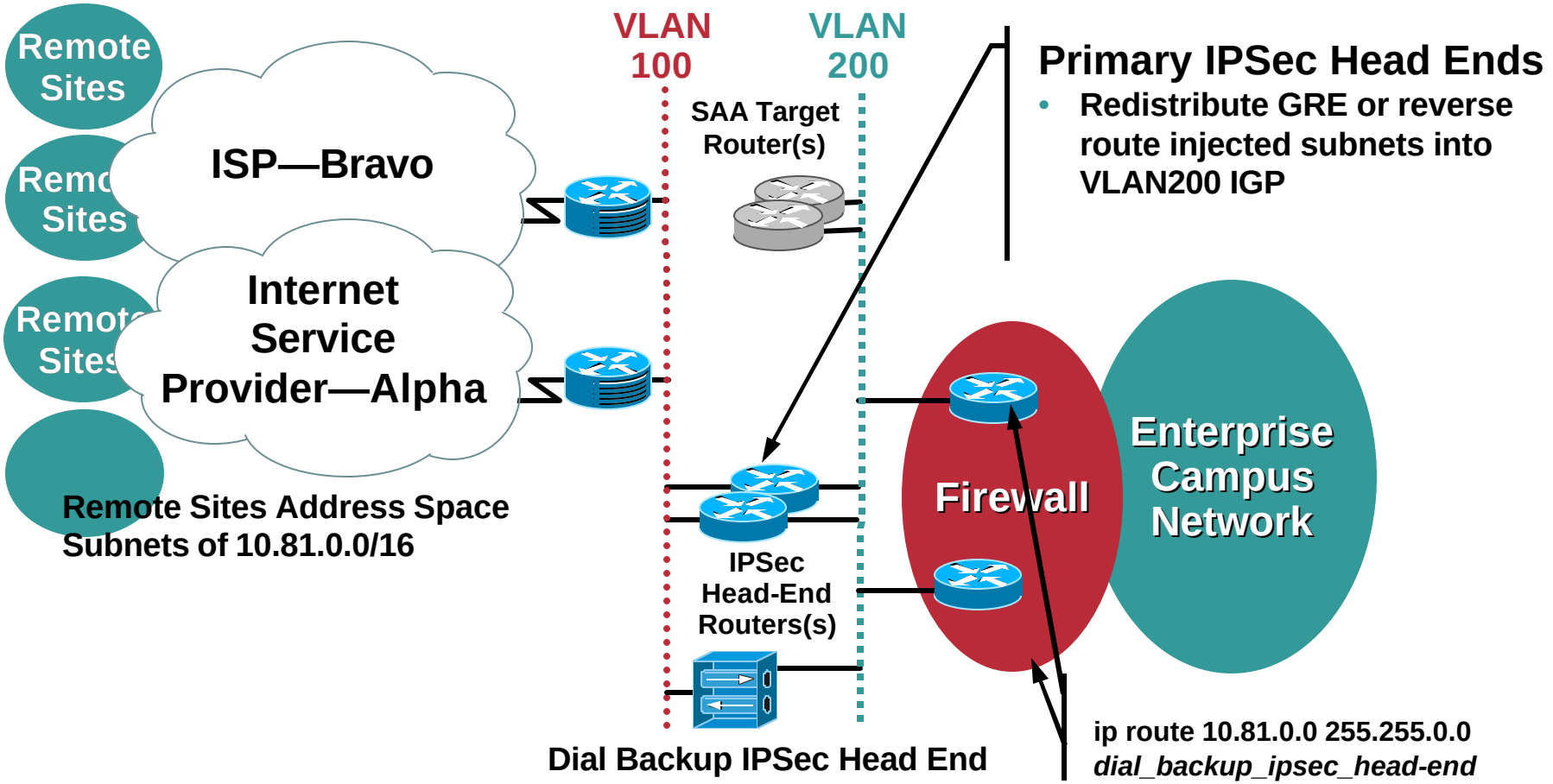
Cisco.com



GRE supports GRE Keepalives and multiprotocol - DMVPN does NOT

Head-End Topology
Stateless—GRE or IPSec Direct Encapsulation

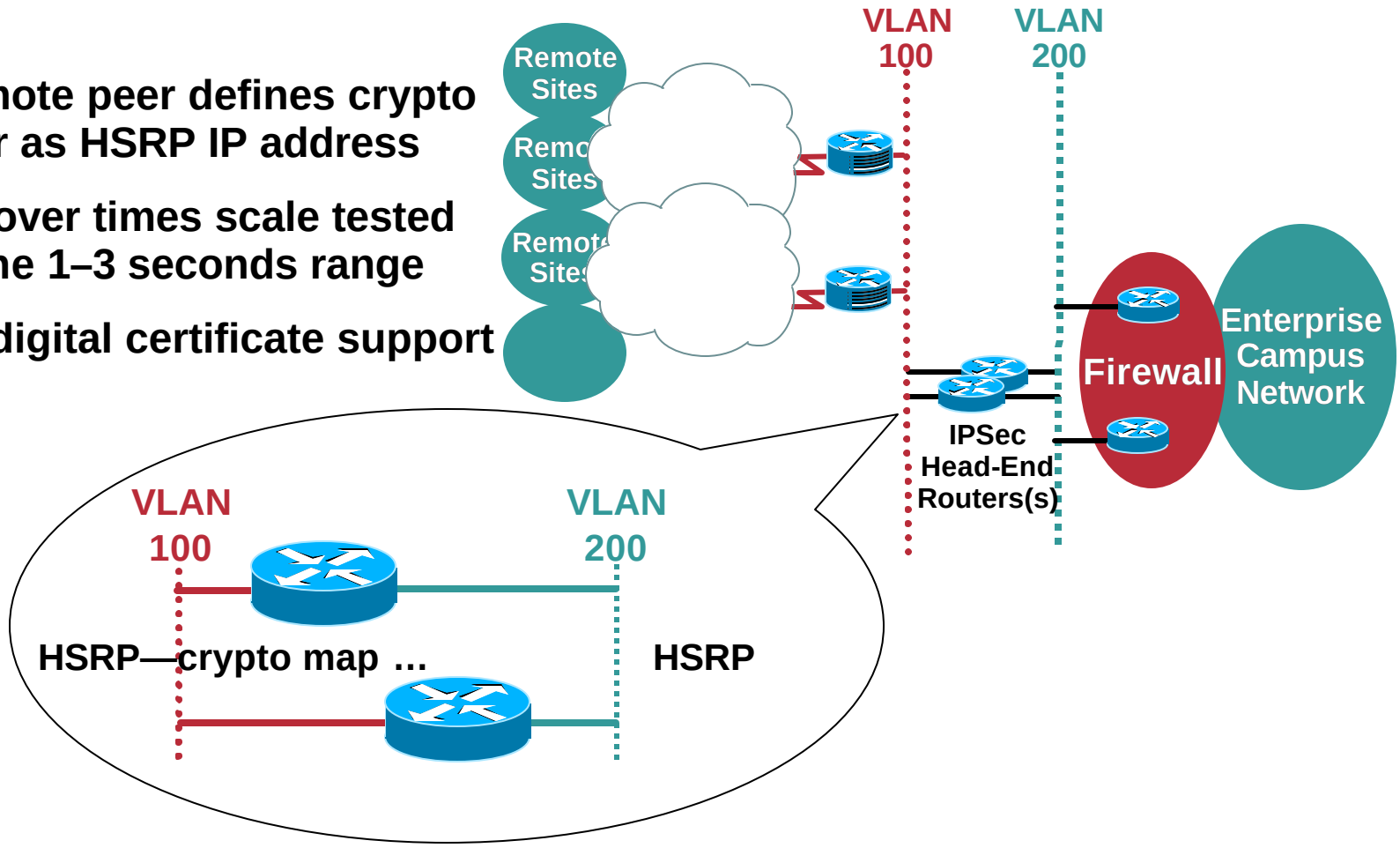
Cisco.com



Reliable Static Routing Backup Using Object Tracking feature: Deploy a Pair of SAA Routers and Use a HSRP Address as the Remote Router's Destination IP Address—Could Be IPSec Head Ends

Head-End Topology
High Availability—Stateful

- Remote peer defines crypto peer as HSRP IP address
- Failover times scale tested in the 1–3 seconds range
- No digital certificate support

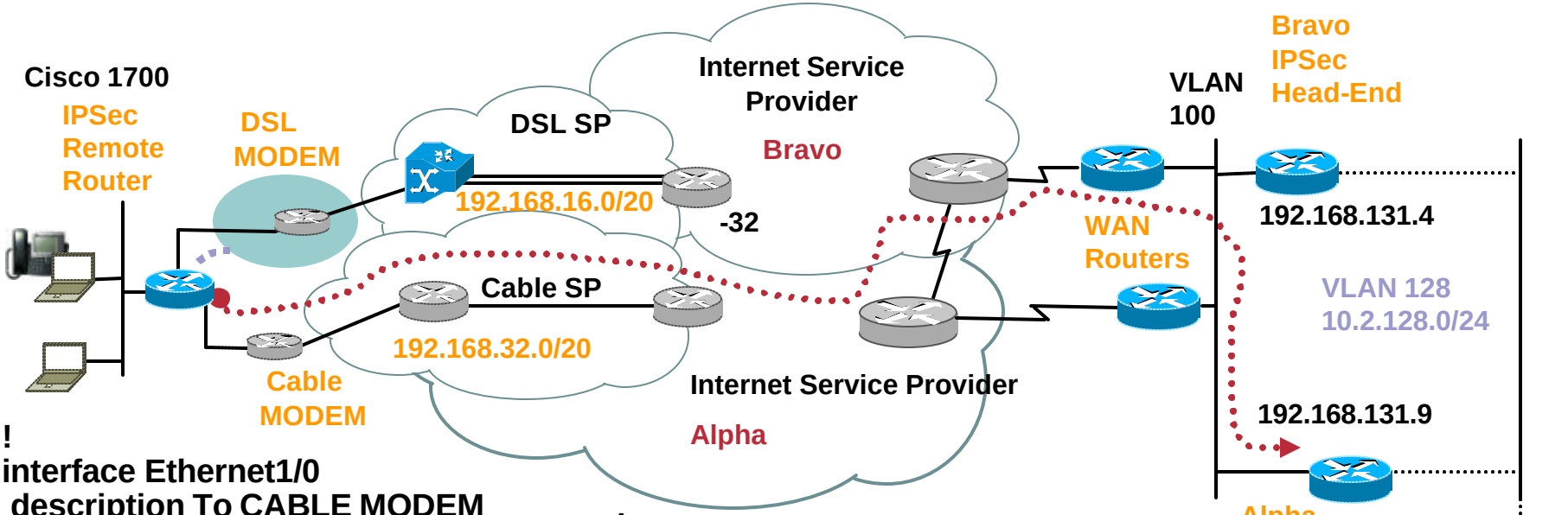


Hot Standby Router Protocol

Load Sharing—Dual Broadband

Load Sharing between Cable and DSL Links

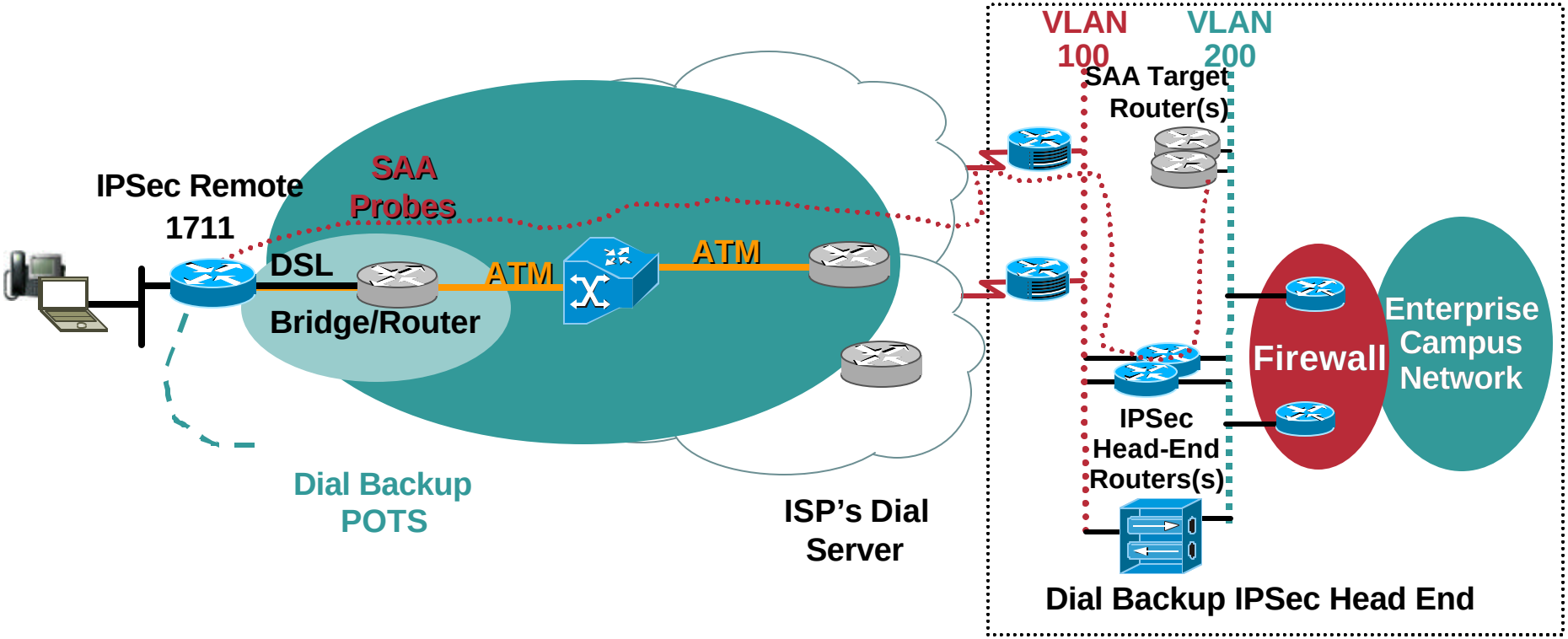
Cisco.com




```
!
interface Ethernet1/0
 description To CABLE MODEM
 ip dhcp client route track 123
 ip address dhcp
 ...
 crypto map ISP_Alpha
!
crypto map ISP_Alpha 1 ipsec-isakmp
 description ISP Alpha Connection
 set peer 192.168.131.9
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
!
```

```
!
interface Dialer1
 description To DSL MODEM
 ...
 crypto map ISP_Bravo
!
crypto map ISP_Bravo 1 ipsec-isakmp
 description ISP Bravo connection
 set peer 192.168.131.4
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL
 qos pre-classify
```

Dial Backup



- Dial service can terminate on either an SP access server or an Enterprise-owned access Server—Reliable Static Routing Backup Using Object Tracking feature
- B-ISDN capable of encrypted voice transport—1 G.729 call
- Async dial bandwidth insufficient for encrypted voice transport

Additional Information in Appendix

PERFORMANCE

Performance

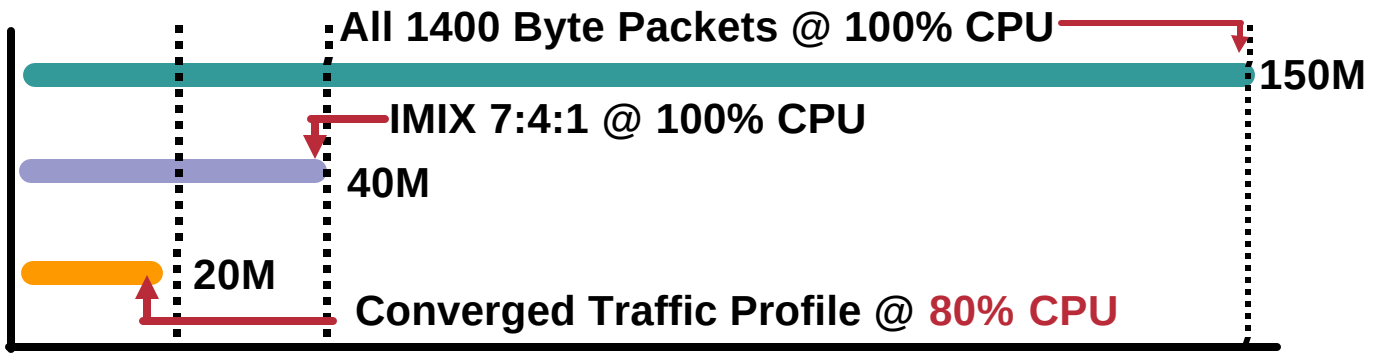
- Reported Performance Generally Inaccurate Due to
  - Interests of Marketing
  - Inadequate Test Tools
- Performance of the Teleagent Router Generally Not an Issue
- Head-end Performance Requirements Based On
  - Topology
  - Redundancy Requirements
  - Geographic Dispersion of Teleagents
  - IPSec Direct Encapsulation or IPSec Encryption of GRE/mGRE
  - Erlang – Ratio of Concurrent Voice Calls to Teleagents

Voice over IP and Encryption Performance

Most Common Mistake Deploying Encrypted Voice

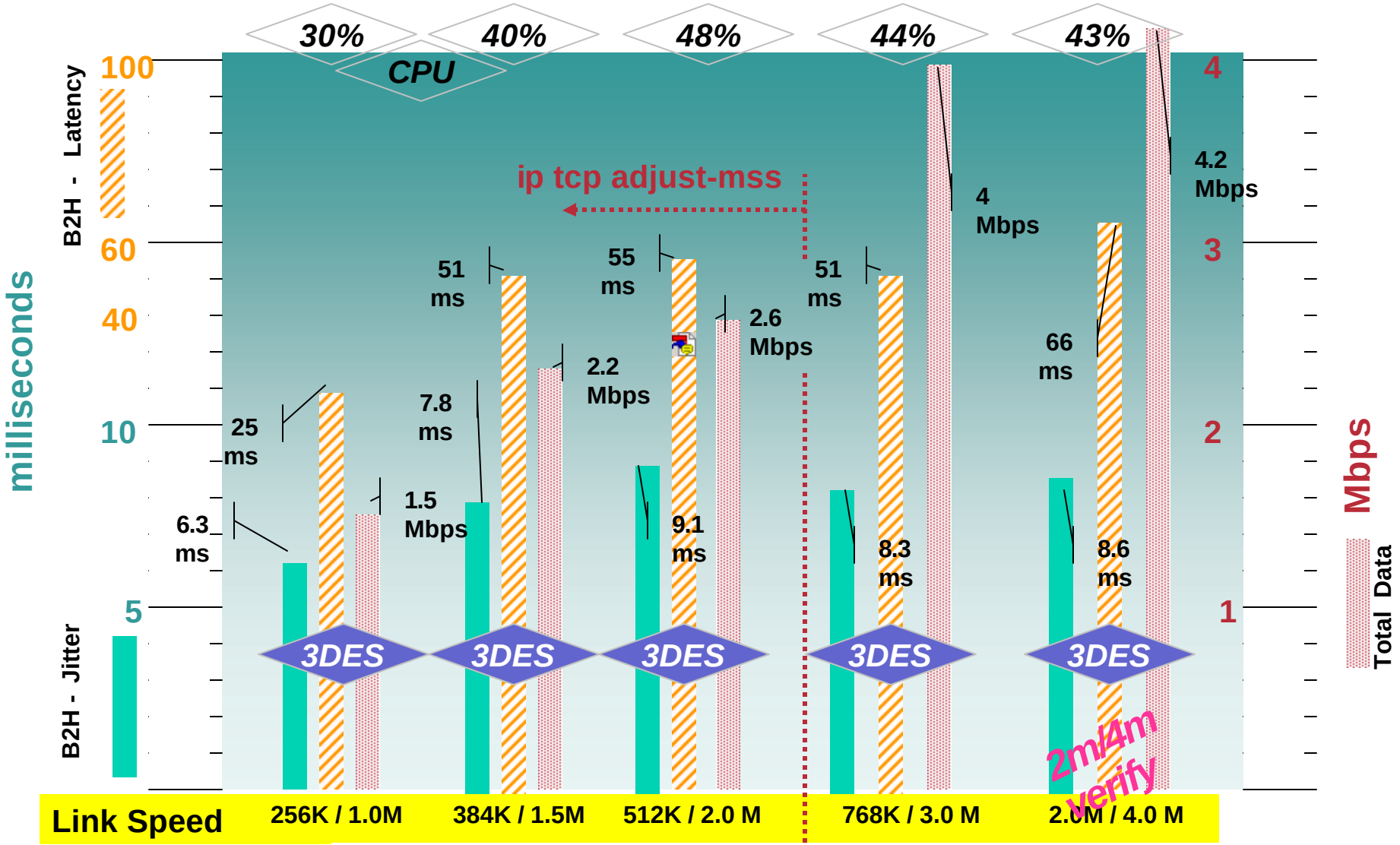
- All vendors state crypto performance in megabits per second at 100% CPU with all MTU-sized (~1400 byte) packets; *why? Shows the best marketing numbers*
- Voice packets are of a fixed size and a constant—and higher—rate than data applications
- Average packet size in some profiles < 100 bytes

Crypto Performance Measured in Packets per Second Is a More Accurate Indicator for VoIP



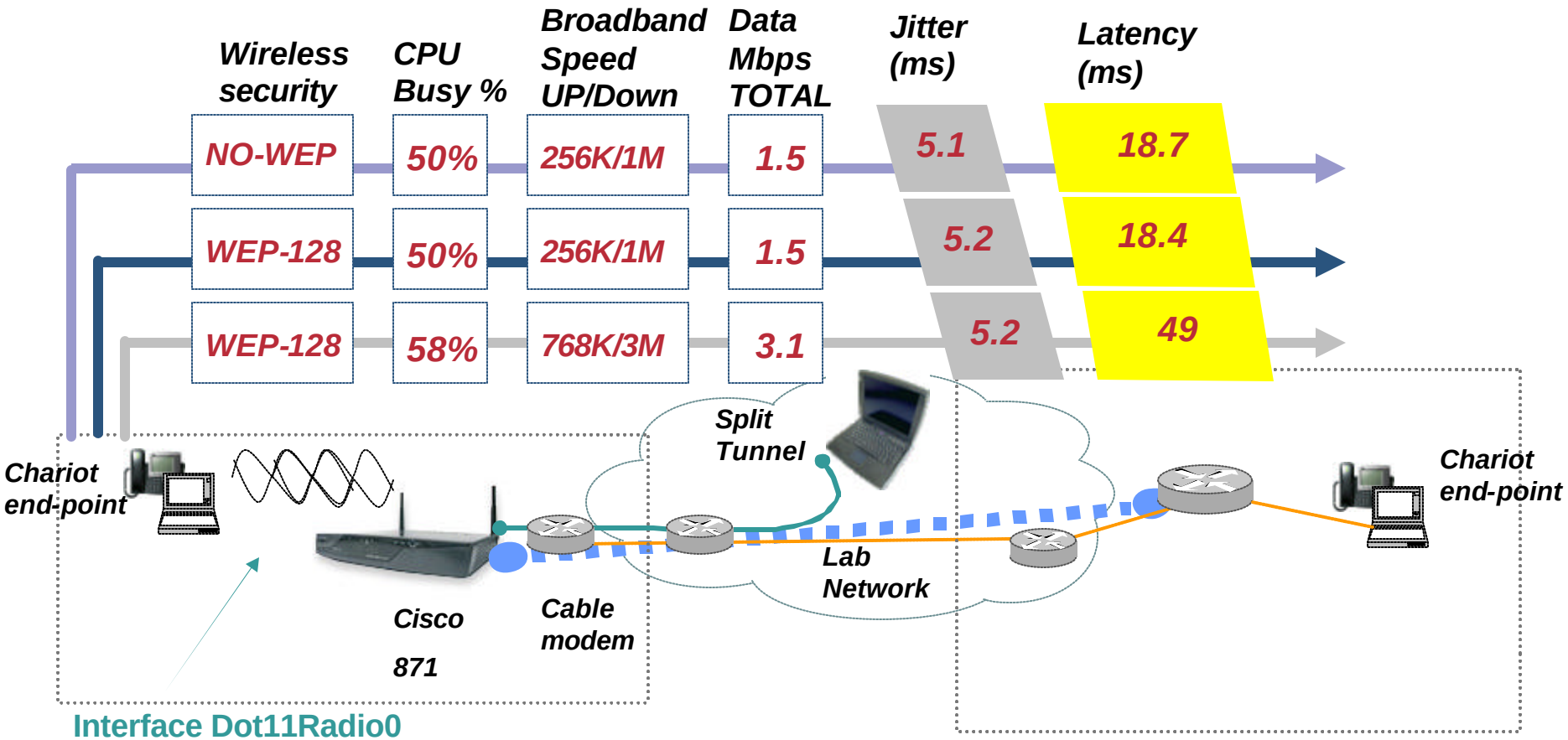
Crypto Performance in Megabits per Second over Various Traffic Profiles

871 Performance Chart - Teleworker Chariot Profile, 1 G.729 voice call plus data – Split Tunnel – IOS FW and IPS



Cisco 870 Series Wireless LAN Test

1 G.729 voice call plus data – Split Tunnel – IOS FW and IPS




```
Interface Dot11Radio0
!                50mW power with a 40db attenuation
 power local cck 50
 power local ofdm 20
```

Latency and Jitter are reported from branch to head-end. Packet loss approaches zero.

IPSec Direct Encapsulation with DPD / RRI
Performance Summary

	Spokes	Bi-Directional Traffic (Mbps)	Bi-Directional Traffic (kPPS)	CPU Utilization %	Stopping Point
3745 (AIM-II)	120	22.5	14.5	80	CPU
PIX535 (VAC+)	500	167	84	89	CPU
3080 (SEP-E)	138	39.4	19.6	52	CPU
7200 NPE-400 (VAM1)	1040	71.7	31.7	88	CPU
7200 NPE-G1 (2xVAM1)	1040	106.7	48.1	81	CPU
7200 NPE-G1 (2xVAM2)	1040	108.7	48.7	77	CPU
Cisco Catalyst® 6500 (VPNSM)	1040	1029.3	488.7	N/A	VPNSM

Additional Information in Appendix

Lessons Learned

Pitfalls/Lessons Learned [1]

- **Certificate lifetimes**
  - Need to consider re-enrollment strategy (auto-enrollment)
- **Teleworker address space**
  - Recommend /28 (255.255.255.240) a /29 should be sufficient, but re-provisioning users from a /29 to a /28 is tedious
- **Remote router input ACL should permit SSH (TCP port 22)**
  - Inevitably help desk will want to connect to the remote router without the IPSec tunnel being active
- **Exclude addresses from DHCP pool**
  - Users, especially engineers, will have some need for accessing home devices from work—pre-defining several address in the pool eliminates re-provisioning
- **Minimum bandwidth policy**
  - Establishing a minimum broadband connection data rate policy will eliminate at least 30% of your teleworker support problems

Pitfalls/Lessons Learned [2]

- **Standard configuration template should include an SAA (Service Assurance Agent)/ IP SLA probe**
  - **Builds and maintains IPSec tunnels to dynamic crypto maps and provides latency (and jitter) history**
- **Deploy a head-end IP SLA router and EZVPN server**
  - **With IPM (Internetwork Performance Monitor) or manually configured SAA probes, can assist with troubleshooting ISP issues**
  - **Permits creating temporary IPSec tunnel for troubleshooting and manual certificate enrollment**
- **NetFlow enabled on head-end IPSec routers**
  - **Capacity planning (peak call rates)**
  - **Identification of infected hosts on remote networks**
  - **Troubleshooting**

Pitfalls/Lessons Learned [3]

- **Contiguous ISP**

  For site to site deployments, single ISP preferred—eliminates inter-ISP routing issues and connectivity failures

- **Use your remote access head-end (VPN3000) device to support dial backup**

  Using a distinct IPSec head-end for supporting IPSec tunnels during dial-backup simplifies head-end routing configuration

- **Run IPM/IP SLA for historical data trending**

  Voice latency and jitter will change as ISP's network changes

- **Troubleshoot all Teleworker devices**

  For cable the frequency filter—for DSL the DSL filter and the cable and DSL MODEM are often the source of the problem

Pitfalls/Lessons Learned [4]

- **Pilots, define the scope and duration of pilot**

  End-users will not want to give up a teleworker router—its like a microwave, you don't fully understand the convenience until you use one for a week

- **Factor in additional skill set in troubleshooting**

  Site to Site VPNs will save the enterprise money, but the network managers will need to learn new skills and improve troubleshooting ability

- **Test applications for MTU related issues**

  Common problem within Cisco Internal Deployments My PC hangs when I boot; see…

  Microsoft Knowledge Base Article 244474—How to Force Kerberos to Use TCP Instead of UDP

SUMMARY

Summary / Reference Material

Cisco.com

- **Updates and errata will be posted at:**
  - ftp://ftp-eng.cisco.com/vvt-2004/index.html
- **Solution Reference Network Design**
  - http://www.cisco.com/go/srnd
    - **Voice and Video Enabled IPSec VPN (V^{3}PN) SRND**
    - **Business Ready Teleworker SRND**

Associated Sessions

SEC-2011 Deploying Site-to-Site IPSec VPNs
SEC-4010 Advanced IPSec Deployments and Concepts of DMVPN Networks
SEC-2010 Deploying Remote Access IPsec and SSL VPNs
TECRST107 Deploying QoS to Protect Voice, Video and Critical Data in the Enterprise
NMS-3043 Advanced Network Performance Measurement with Cisco IOS IP SLA
NMS-3132 Advanced Netflow Usage
NMS-1601 Zero Touch Image and Configuration Management
NMS-1011 Principles of Fault Management
VVT-2013 QoS Design for Service Provider Voice over VPN

Complete Your Online Session Evaluation!

Help us improve this session !

Please Complete your session evaluation form and give it to the room monitors.

MUCHAS GRACIAS !

Appendix

Agenda

- Overview
- Bandwidth Requirements
- VoIP / IPCC
- QoS
- IPSec
- Authentication and Segmentation
- Provisioning (Configuration Management)
- Voice Quality Management (Fault Management)
- Head-end Topology - Backup and Redundancy
- Performance
- Lessons Learned
- Summary
- Appendix / Supplemental Material

APPENDIX: BANDWIDTH

(supplemental slides)

Serialization Delay

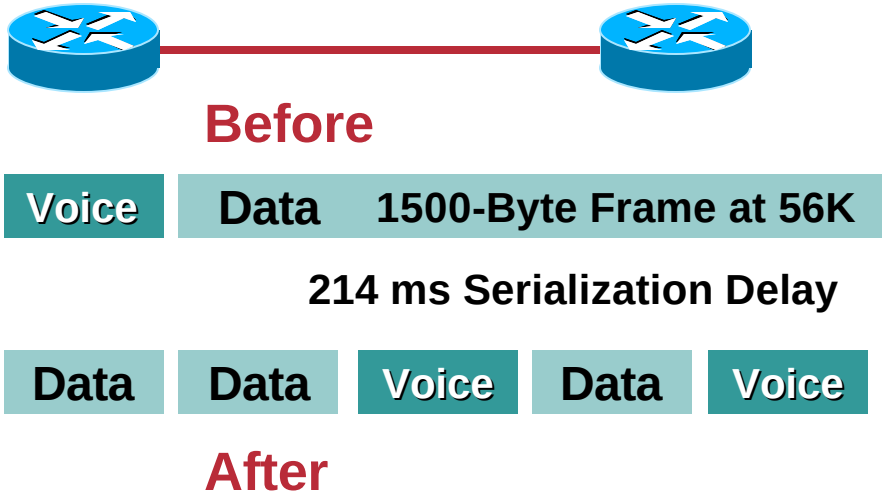
Why Bandwidth to the Remote Site Is So Important

- **Fragmenting large data packets and interleaving voice packets between the data fragments minimizes the serialization delay**
- **Addressed by Layer 2 technologies:**
  - **Link fragmentation and interleaving (LFI): multilink PPP**
  - **FRF.12: Frame Relay**

However, the Predominate Service Offering of DSL Providers Is PPPoE which Has No LFI Standard

Assuming Most Cable Providers Are DOCSIS 1.0 or DOCSIS1.0+ which Has No LFI Either

DOCSIS 1.1 Provides Fragmentation and QoS



Serialization Delay

How Can You Influence Data Packet Sizes without a Layer 2 Fragmentation Technique?

Use Layer 4—Transport Layer

Before

214 ms Serialization Delay

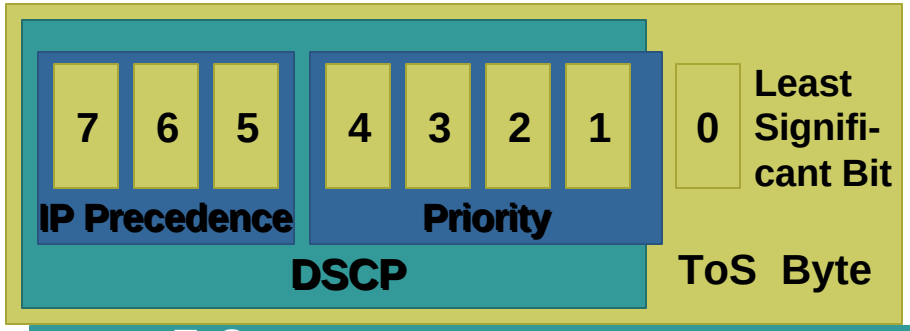
After

Router Can Override the TCP MSS (Maximum Segment Size) and Reduce Data Packet Size

```
interface Ethernet0
 ip tcp adjust-mss 542
```

APPENDIX: QoS (supplemental slides)

ToS Byte
DSCP Reference Chart

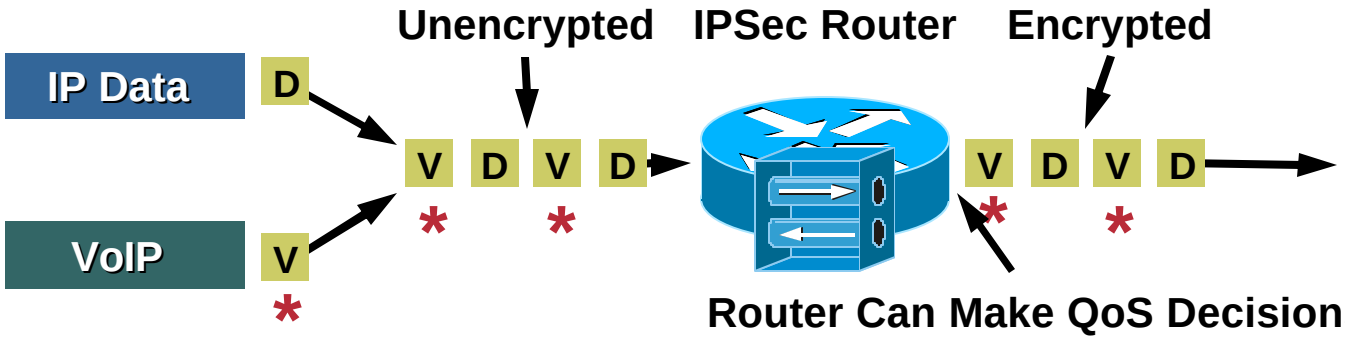


ToS Hex	ToS Decimal	IP Precedence	Class-map Name	DSCP	Binary
E0	224	7 Network Control		56 CS7	11100000
C0	192	6 Internetwork Control	INTERNETWORK-CONTROL	48 CS6	11000000
B8	184		VOICE	46 EF	10111000
A0	160	5 Critical		40 CS5	10100000
88	136		VIDEO-CONFERENCE	34 AF41	10001000
80	128	4 Flash Override		32 CS4	10000000
68	104		CALL-SETUP	26 AF31	01101000
60	96	3 Flash	CALL-SETUP	24 CS3	01100000
48	72		TRANSACTIONAL-DATA	18 AF21	01001000
40	64	2 Immediate		16 CS2	01000000
20	32	1 Priority		8 CS1	00100000
00	0	0 Routine		0 Dflt	00000000

QoS Preclassify

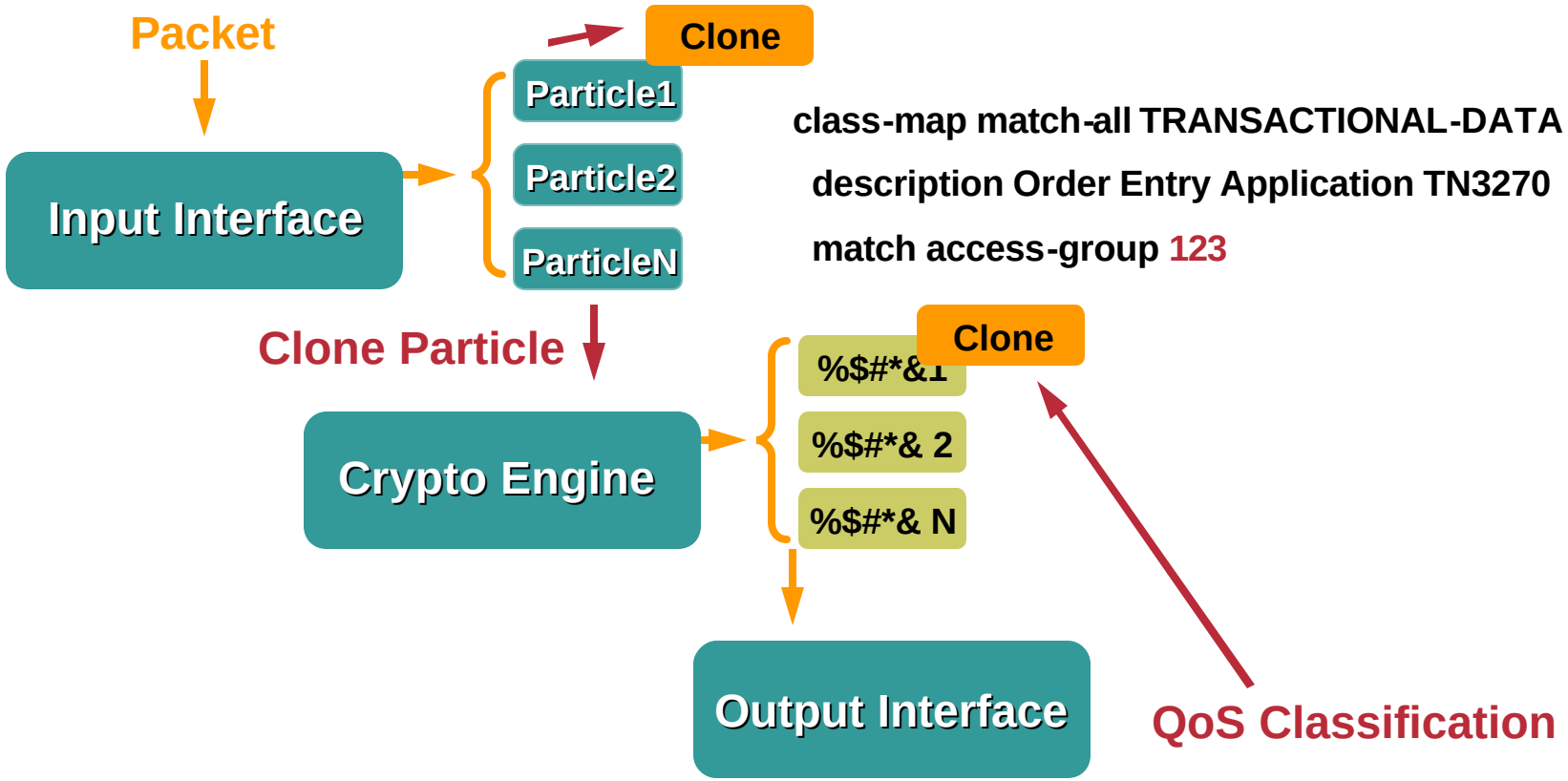
- Independent of ToS byte copy to IPSec IP header
- Maintains preencapsulated IP header for output QoS policy—port, protocol, src/dst IP address, etc.
- Apply to both crypto map and IP GRE tunnel—or just crypto map if no IP GRE tunnel

```
!
crypto map static-map 10 ipsec-isakmp
 qos pre-classify
!
interface Tunnel1
 ip address 10.62.139.198 255.255.255.252
 qos pre-classify
 delay 60000
 tunnel source 192.168.91.2
 tunnel destination 192.168.252.1
 crypto map static-map
!
```



Router Can Make QoS Decisions Based on Encrypted Elements in the Packets

QoS Preclassify



access-list 123 permit tcp any host 10.45.15.1 eq telnet

Encrypted Packet

Shaping Values for Cable and DSL

Example

```
policy-map shaper
  class class-default
   shape average 182400 1824
```

mean-rate burst-size

1/100th = 10ms

shape average *mean-rate burst-size*

Upstream Link Rate	Cable	DSL
128K	122,000 1,220	91,200 1,000[*]
160K	152,000 1,520	114,000 1,140
256K	243,200 2,432	182,400 1,824
384K	364,800 3,648	273,600 2,736

Shaped Rate for Cable = Upstream Link Rate * 95

Shaped Rate for DSL = (Upstream Link Rate * 75) * 95

[*] Minimum Configurable Value—128K Not Recommended—Shown for Illustrative Purposes Only

Shaping Illustration (184,200 bps)

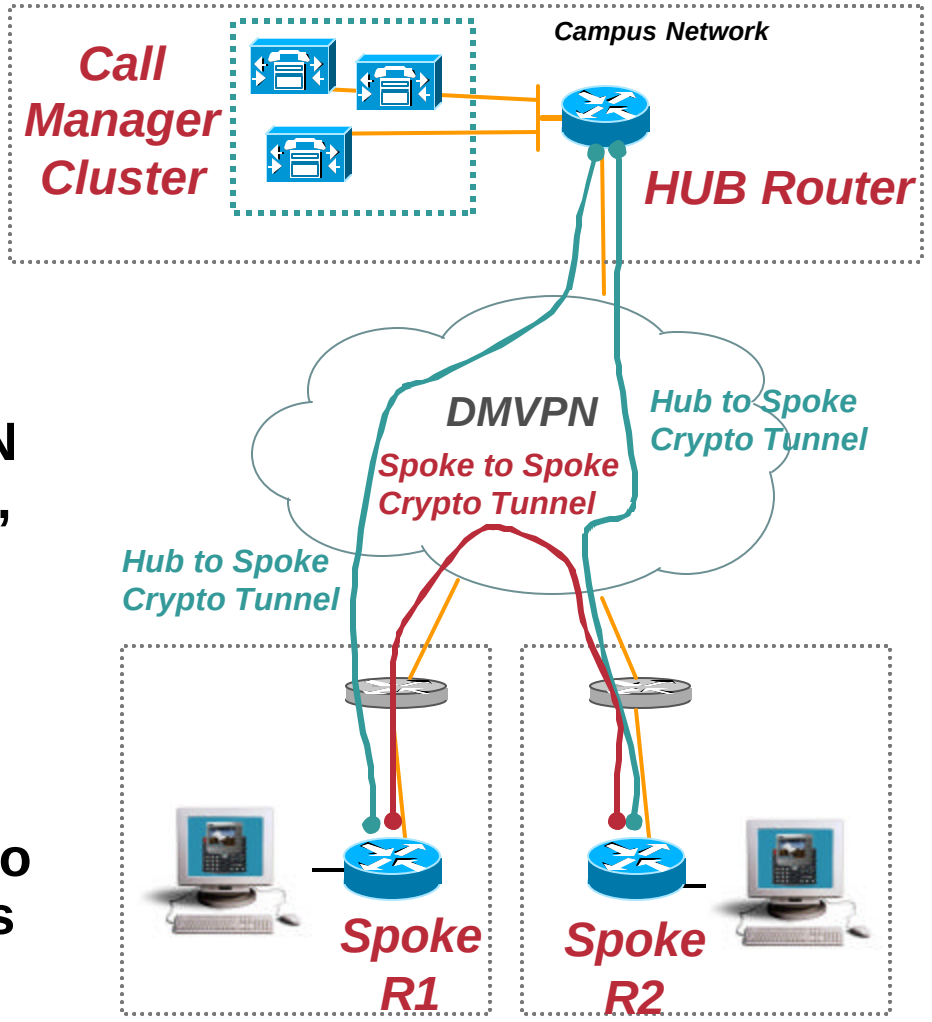
G.729 Call—831 Behind Cable MODEM

This Graph Is the View from the PC's Perspective, Note How the Throughput Increases when the Call Completes; 128K + 56K = 184K

APPENDIX: IPSEC (supplemental slides)

DMVPN (Dynamic Multipoint VPN)
Spoke to Spoke Calling – Voice Quality

- **Phone R1 calls Phone R2**
- **Media (RTP) flows between R1 and R2 only if R2 phone is answered**
- **RTP packets trigger establishment of Spoke to Spoke Path**
- **R1 knows R2 is attached to DMVPN net, but has no valid CEF adjacency, no direct crypto path to R2.**
- **RTP packets process switched via Hub while spoke to spoke crypto tunnel is built.**
- **Cut over of RTP stream from Hub to Spoke to Spoke to Spoke introduces out of order packets. This delta in latency impacts voice quality.**



SSL VPN (WebVPN)
How does it apply to Teleworker?

Cisco.com

- **Client to Gateway (Remote Access) Solution**
- **No UDP support, thus no VoIP**
- **Server side**

  VPN 3000 V4.1 or higher

  IOS 12.3(14)T or higher
- **Client (browser) side**

  SSL V3.0 and JAVA V1.4
- **SSL VPN is not a packet encapsulation technology like IPSec –rather an “encrypted/authenticated web proxy”**

Static Crypto map and EZVPN Backup Authentication Method for Management

It is possible to configure both a static crypto map and an EZVPN remote on the same router.

This could be on two different outside interfaces or on the same outside interface. However, be aware of

CSCeg08541

Different IKE Authentication methods wont work at Easy VPN Remote

Integrated in - 12.3(12.04)T

Crypto Config Example
Certificates/EZVPN

Example: 1712 Using Certificates on the Primary Interface to a 2691 and

EZVPN to a VPN3080 on the Dial-Backup interface

```
ip host ect-msca 172.26.179.237
!
crypto ca trustpoint ect-msca
 enrollment mode ra
 enrollment url http://ect-msca:80/certsrv/mscep/mscep.dll
 revocation-check none
 source interface Vlan1
!
crypto ca certificate chain ect-msca
 certificate 5DA1A8EE00000000003D
 certificate ca 113346B52ACEE8B04ABD5A5C3FED139A
!
crypto isakmp policy 20
 encr 3des
 group 2
crypto isakmp keepalive 10
!
crypto ipsec transform-set 3DES_SHA_TUNNEL
                              esp-3des esp-sha-hmac
!
crypto ipsec client ezvpn VPN3080
 connect auto
 group SOHO key point_of_sale
 mode network-extension
 peer xx.xx.131.30  Internet routable IP address
 username site100 password  cisco123
!
crypto map IOS_2691 10 ipsec-isakmp
 set peer xx.xx.131.4  Internet routable IP address
 set transform-set 3DES_SHA_TUNNEL
 match address CRYPTO_MAP_ACL  Matches Vlan1 subnet
 qos pre-classify
!
interface BRI0
...
crypto ipsec client ezvpn VPN3080


interface Vlan1
...
 crypto ipsec client ezvpn VPN3080 inside
!
interface Dialer1
 description Outside to DSL (PPPoE)
...
crypto map IOS_2691
!
...
!                    Aliases to aid in verification
alias exec xa crypto ipsec client ezvpn xauth
alias exec ca sh cry eng conn act
alias exec cc crypto ipsec client ezvpn connect VPN3080
alias exec cz clear crypto ipsec  client ezvpn VPN3080
alias exec sz show cry ipsec client ezvpn
```

Example of Static Crypto map and EZVPN Backup Authentication Method for Management

Cisco.com

```
crypto ca trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 crl optional
 source interface FastEthernet0/0
!
crypto ca certificate chain rtp5-esevpn-ios-ca
 certificate 2F
 certificate ca 01
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto ipsec client ezvpn BOOTSTRAP
 connect auto
 group EZVPN_Group key xxx
 mode network-extension
 peer xx.xxx.223.3
 username FOO password BAR
!
crypto map Encrypt_GRE 10 ipsec-isakmp
 set peer xx.xxx.223.23
 set transform-set 3DES_SHA_TUNNEL
 match address Encrypt_GRE
!
interface Loopback1
 ip address 10.81.7.214 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback1
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination 64.102.223.23
!
interface Ethernet0/0
 ip address dhcp
 crypto map Encrypt_GRE
 crypto ipsec client ezvpn BOOTSTRAP
!
interface FastEthernet0/0
 ip address 10.81.2.1 255.255.255.248
 no keepalive
 crypto ipsec client ezvpn BOOTSTRAP inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route xx.xxx.223.0 255.255.255.224 dhcp
!
ip access-list extended Encrypt_GRE
 permit gre host 10.81.7.214 host xx.xxx.223.23
!
alias exec xa crypto ipsec client ezvpn xauth
!
ntp server 10.81.254.131 source FastEthernet0/0
end
```

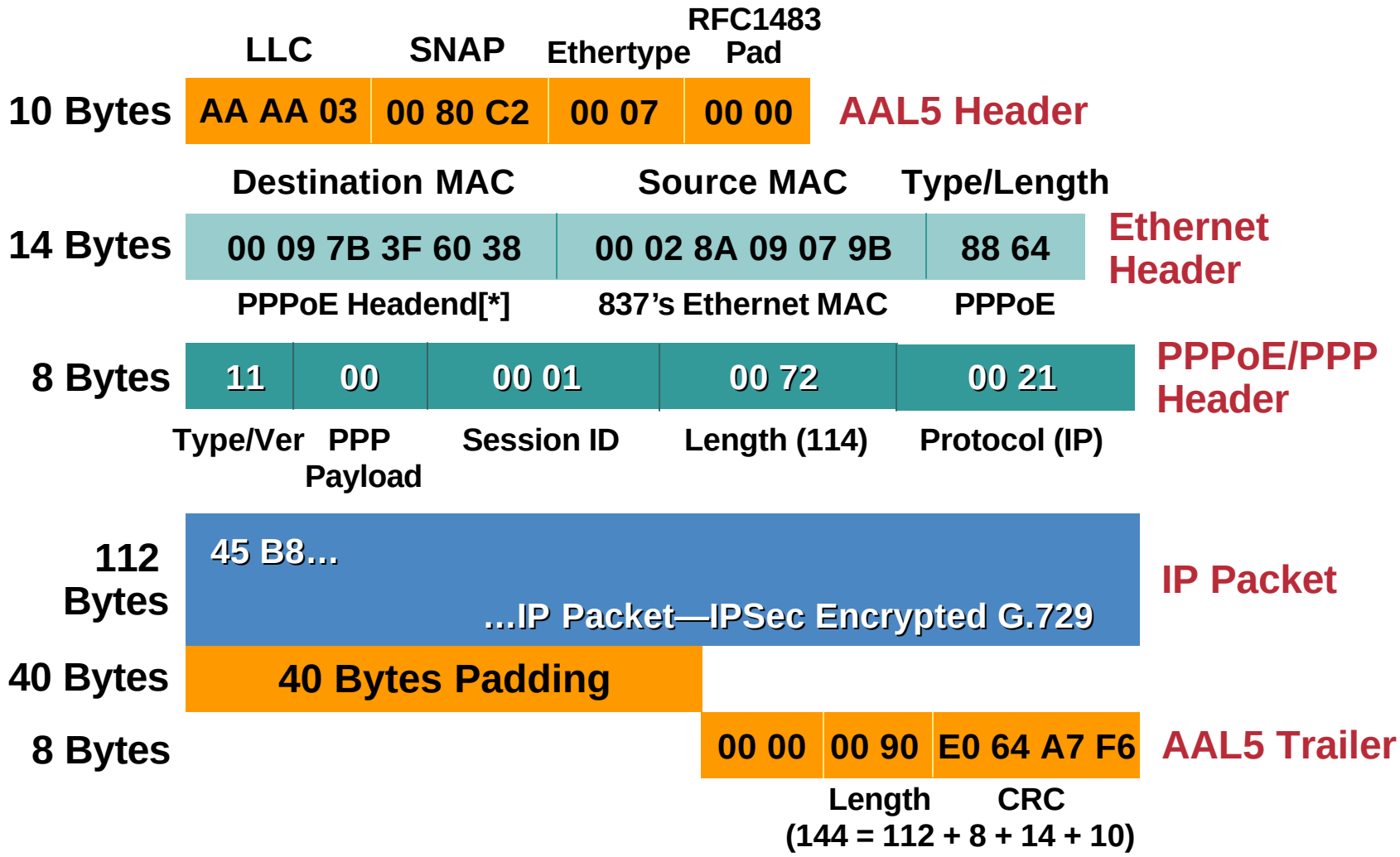
Benefit of ip tcp adjust-mss DSL 256K/1.4M

	Call Leg	Chariot Voice Drops %	Chariot RFC1889 Jitter	Chariot One-Way Delay
Cisco 831 mss 542	Branch -> Head	0 %	7.9 ms	67.5 ms
	Head -> Branch	0 %	7.6 ms	38.9 ms
Cisco 831 mss 1360*	Branch -> Head	0 %	12.8 m	74.8 ms
	Head -> Branch	0 %	13.4 ms	84.8 ms

Jitter Goal <= 8 ms

*Sun Netra's MTU Set at 1400 Bytes—Cisco IOS Not Overriding

G.729 Packet
DSL/PPPoE/IPSec



Total 192 Bytes/48 per Cell = 4 Cells = 53 * 4 = 212 Bytes **G.711 = 7 Cells**

APPENDIX: Authentication and Segmentation

(supplemental slides)

Cisco 830 Auth Proxy Configuration Sample


```
!--- Define what will be authenticated
 aaa new-model
!
 aaa authentication login default local group radius
 aaa authorization auth-proxy default group radius
 aaa session-id common
 !--- Set the router name to appear as the banner
 ip auth-proxy auth-proxy-banner
 !
!--- Set the proxy name, (PXY), activate via http
!--- Set ACL entries to timeout after 8 hours
!--- And set the ACL for interesting auth-proxy traffic
 ip auth-proxy name PXY http auth-cache-time 480
  list Data-Only_Vpn
 ip audit notify log
 !--- Define the auth-proxy server
 radius-server host 10.68.18.1
 radius-server key cisco
 !--- Source the request from inside (for VPN support)
 ip radius source-interface Ethernet0
```

```
interface Ethernet0
  IP address 10.1.2.1 255.255.255.248
!---Apply the access list to the interface
  ip access-group Ipt-Vpn_Internet in
  !--- Apply the auth-proxy list name
  ip auth-proxy PXY
 !
 !--- Enable http server and authentication
 ip http server
 ip http authentication aaa
 !
 !--- This is the access list for auth-proxy
 !---It requires auth-proxy to access tcp to 10.1.0.0/16
ip access-list extended Data-Only_Vpn
 permit tcp 10.1.2.0 0.0.0.7 10.1.0.0 0.0.255.255
!
! This ACL stops what proxy passes, and allows all else
Ip access-list extended Ipt-Vpn_Internet
 deny tcp 10.1.2.0 0.0.0.7 10.1.0.0 0.0.255.255
 permit  ip 10.1.2.0 0.0.0.7 any
```

Assume IP Phone(s) Match this Entry

802.1x for Cisco 830 Configuration


```
dot1x system-auth-control
!
identity profile default
 description 802.1x configuration
 template Virtual-Template1
 device authorize type cisco ip phone
!
interface Loopback0
 description NONCORPUSER inside interface
 ip address 192.168.99.1 255.255.255.0
!
interface e0
 ip nat inside
 dot1x port-control auto
!
interface e1
 ip nat outside
 ip inspect CBAC out
!
ip nat inside source list NatACL interface e1  overload
!
ip access-list extended NatACL
 permit ip 192.168.99.0 0.0.0.255 any
!
interface Virtual-Template1
 description This will spawn a virtual-access for each non-authorized non-CORPUSER
 ip unnumbered Loopback0
 ip nat inside
!
```

```
ip radius source-interface e0

ip host radius-server 10.81.0.19

radius-server host 10.81.0.19 auth-port 1645 acct-port
1646 key cisco

radius-server authorization permit missing Service-Type
```

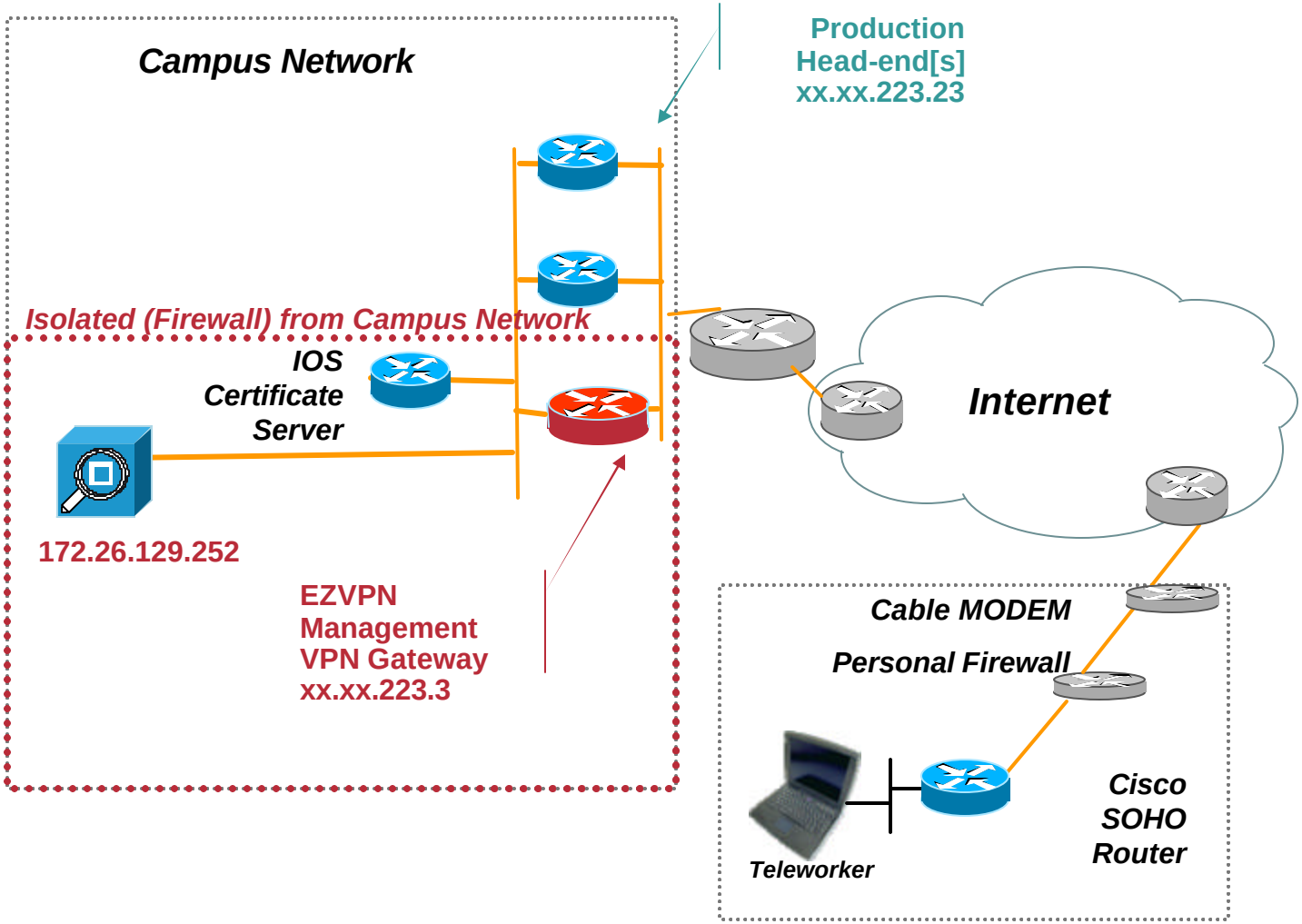
```
Remark This ACL Is a Filter of Which Traffic Is to Be NAT/Pnat for the Internet
Remark Only the Spouse Will Be Allowed to the Internet Directly,
the Employee  Will Go to the HQ Location to Get Internet Access
```

APPENDIX: Provisioning (Configuration Management)

EZVPN BOOTSTRAP (supplemental slides)

EZVPN BOOTSTRAP Head-end Topology

Cisco.com



EZVPN BOOTSTRAP
Remote Router Initial config (1751)

Remote User Enters Initial Config

```
!
hostname Router
!
crypto isakmp nat keepalive 10
!
crypto ipsec client ezvpn BOOTSTRAP
 connect auto
 group EZVPN_Group key cisco
 mode network-extension
 peer 64.102.223.3
!
interface Ethernet0/0
 ip address dhcp
 no shut
 crypto ipsec client ezvpn BOOTSTRAP
!
interface FastEthernet0/0
 ip address 10.81.2.1 255.255.255.248
 no keepalive
 no shut
 crypto ipsec client ezvpn BOOTSTRAP inside
!
alias exec xa crypto ipsec client ezvpn xauth    # Ideally run an IOS version the permits storing uid
ntp server 10.81.254.131 source f0/0
clock timezone est -5
clock summer-time edt recurring
line vty 0 4
pass cisco
exit
enable pass cisco
end
```

Console Access

EZVPN BOOTSTRAP
Initial Tunnel UP

You would really like to have an IOS version that allowed the storing of username and password in the config. But if not.

Nov 21 05:45:45.615: EZVPN(BOOTSTRAP): Pending XAuth Request, Please enter the f ollowing command:
Nov 21 05:45:45.615: EZVPN: crypto ipsec client ezvpn xauth

Router#xa
Username: EZVPN_Test_user
Password: my-password
Router#

Verification:

Router#show cry ipsec client ezvpn
Easy VPN Remote Phase: 2

Tunnel name : BOOTSTRAP
Inside interface list: FastEthernet0/0
Outside interface: Ethernet0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
DNS Primary: 64.102.6.247
DNS Secondary: 171.68.226.120
Default Domain: cisco.com

The above is goodness.

Console Access

EZVPN BOOTSTRAP
Certificate Enrollment


```
video1751-vpn#config t
Enter configuration commands, one per line.  End with CNTL/Z.
ip domain-name cisco.com
clock timezone est -5
clock summer-time edt recurring
cry key generate rsa
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]

ip host rtp5-esevpn-ios-ca 10.81.0.27
crypto ca trustpoint rtp5-esevpn-ios-ca
 source interface f0/0
 enrollment mode ra
 enrollment url http://rtp5-esevpn-ios-ca:80
 crl optional
 exit
cry ca authenticate rtp5-esevpn-ios-ca
Certificate has the following attributes:
        Fingerprint: xxx xxx xxx xxx

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
video1751-vpn(config)#cry ca enroll rtp5-esevpn-ios-ca
%
% Start certificate enrollment ..
...
show cry ca cert
```

Campus Telnet - EZVPN tunnel

EZVPN BOOTSTRAP
Build a GRE tunnel to the Campus

Cisco.com

```
ip access-list extended Encrypt_GRE
permit gre host 10.81.7.214 host 64.102.223.23
!
int loop 1
ip address 10.81.7.214 255.255.255.255
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto map Encrypt_GRE 10 ipsec-isakmp
 set peer 64.102.223.23
 set transform-set 3DES_SHA_TUNNEL
 match address Encrypt_GRE
!

interface Tunnel0
 ip unnumbered Loopback1
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination 64.102.223.23
int e 0/0
crypto map Encrypt_GRE
```

Campus Telnet - EZVPN tunnel

EZVPN BOOTSTRAP
EZVPN and Encrypted GRE tunnel both up

Cisco.com

```
Mar  1 18:14:32.416: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up
video1751-vpn#show crypto engine conn act

 ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
  78 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C        0        0
  79 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C        0        0
 200 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C        0      343
 201 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C      357        0
 202 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C        0       15
 203 Ethernet0/0         192.168.2.43    set    HMAC_SHA+3DES_56_C       10        0

video1751-vpn#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.2.43    YES DHCP   up                    up
FastEthernet0/0            10.81.2.1       YES NVRAM  up                    up
Loopback1                  10.81.7.214     YES NVRAM  up                    up
Tunnel0                    10.81.7.214     YES TFTP   up                    up

video1751-vpn#who
  Line       User       Host(s)              Idle       Location
   0 con 0                 idle                 00:04:10
*  6 vty 0                 idle                 00:00:00 172.26.129.252
```

Campus Telnet - EZVPN tunnel

EZVPN BOOTSTRAP
EZVPN Clean-up

ip route 172.26.129.252 255.255.255.255 tu 0
int f0/0
ip address 10.81.7.137 255.255.255.248

Connectivity is lost as the telnet destination IP address has been eliminated

'telnet 10.81.7.137'

Remove the EZVPN statements from the interfaces.

int e 0/0
no crypto ipsec client ezvpn BOOTSTRAP
int f 0/0
no crypto ipsec client ezvpn BOOTSTRAP inside

Campus Telnet telnet 10.81.2.1 - EZVPN tunnel

EZVPN BOOTSTRAP
Basic config – finish via GRE tunnel

Cisco.com

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname video1751-vpn
!
enable password cisco
!
memory-size iomem 25
clock timezone est -5
clock summer-time edt recurring
ip domain name cisco.com
ip host rtp5-esevpn-ios-ca 10.81.0.27
!
ip cef
ip audit po max-events 100
!
crypto ca trustpoint rtp5-esevpn-ios-ca
 enrollment url http://rtp5-esevpn-ios-ca:80
 crl optional
 source interface FastEthernet0/0
!
crypto ca certificate chain rtp5-esevpn-ios-ca
 certificate 2F
 certificate ca 01
!
crypto isakmp policy 100
 encr 3des
 group 2
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-
sha-hmac
!
!
crypto ipsec client ezvpn BOOTSTRAP
 connect auto
 group EZVPN_Group key cisco
 mode network-extension
 peer 64.102.223.3
!
crypto map Encrypt_GRE 10 ipsec-isakmp
 set peer 64.102.223.23
 set transform-set 3DES_SHA_TUNNEL
 match address  Encrypt_GRE
!
interface Loopback1
 ip address 10.81.7.214 255.255.255.255
!
interface Tunnel0
 ip unnumbered Loopback1
 keepalive 10 3
 tunnel source Loopback1
 tunnel destination 64.102.223.23
!
interface Ethernet0/0
 ip address dhcp
 crypto map Encrypt_GRE
!
interface FastEthernet0/0
 ip address 10.81.7.137 255.255.255.248
 no keepalive
!
ip route 172.26.129.252 255.255.255.255 Tunnel0
!
ip access-list extended Encrypt_GRE
 permit gre host 10.81.7.214 host 64.102.223.23
!
alias exec xa crypto ipsec client ezvpn xauth
!
ntp server 10.81.254.131 source FastEthernet0/0
end
```

EZVPN BOOTSTRAP
Sample EZVPN HEAD-END CONFIG

Cisco.com

```
hostname    rtp5-EZVPN-gw1
!
boot system flash c3725-advsecurityk9-mz.123-8.T5
!
username EZVPN_Test_user password xxxx
aaa authentication login RTP_ezvpn_user local
aaa authentication ppp default if-needed group radius
aaa authorization network RTP_ezvpn_group local
!
crypto isakmp policy 10
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
crypto isakmp client configuration address-pool local dynpool
crypto isakmp xauth timeout 60
!
crypto isakmp client configuration group EZVPN_Group
 key cisco
 dns 64.102.6.247 171.68.226.120
 domain cisco.com
 pool dynpool
 save-password
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
!
crypto dynamic-map DYNOMAP 10
 set transform-set 3DES_SHA_TUNNEL
 reverse-route
!
!
crypto map EZmap local-address Loopback0
crypto map EZmap client authentication list RTP_ezvpn_user
crypto map EZmap isakmp authorization list RTP_ezvpn_group
crypto map EZmap client configuration address respond
crypto map EZmap 10 ipsec-isakmp dynamic DYNOMAP
!
interface Loopback0
 description Public address
 ip address 64.102.223.3 255.255.255.255
!
interface FastEthernet0/0
 description Private
 ip address 10.81.0.3 255.255.255.248
 crypto map EZmap
!
ip local pool dynpool 10.81.2.8 10.81.2.15
end
```

APPENDIX: Voice Quality Management (Fault Management)

(supplemental slides)

SHOW RTR HISTORY

Cisco.com

For Dynamic Crypto Maps Builds/Maintains IPSec SAs

```
rtr 12
 type echo protocol ipIcmpEcho 172.26.1.2 source-ipaddr 10.81.2.1
 request-data-size 164
 tos 192
 frequency 90
 lives-of-history-kept 1
 buckets-of-history-kept 60
 filter-for-history all
rtr schedule 12 start-time
    now  life forever
```

Every 90 Seconds Source an ICMP off the Inside Interface ToS Is *Internetwork Control*

show rtr history tabular

```
joeking-vpn#show rtr operational-state 12
Entry number: 12
Modification time: 16:29:55.298 est Wed Mar 5 2003
Number of operations attempted: 5559
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: FALSE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): 44
Latest operation start time: 11:26:55.301 est Tue Mar
Latest operation return code: OK
RTT Values:
RTTAvg: 44      RTTMin: 44      RTTMax: 44
NumOfRTT: 1     RTTSum: 44      RTTSum2: 1936
```

SYSLOG / SNMP Traps

Configuration

logging host 172.26.157.11 xml

...

rtr reaction-configuration 18 react jitterSDAvg threshold-value 6 5 threshold-type immediate action-type trapOnly

SYSLOG XML Trap

Apr 4 13:51:47 rtp5-esevpn-saa.cisco.com 150: <ios-log-msg><facility>RTT</facility> <severity>3</severity><msg-id>SAATHRESHOLD</msg-id><time>Apr 4 14:11:36.313 edt</time> <args><arg id="0">18</arg><arg id="1">exceeded</arg><arg id="2">jitterSDAvg</arg></args></ios-log-msg>

SNMP Trap Packet Detail

Apr 4 14:28:05.761 edt: %RTT-3-SAATHRESHOLD: RTR(18): Threshold exceeded for jitterDSAvg
Apr 4 14:28:05.777 edt: SNMP: Queuing packet to 172.18.86.92
Apr 4 14:28:05.777 edt: SNMP: V1 Trap, ent ciscoSyslogMIB.2, addr 10.81.0.26, gentrap 6, spectrap 1
clogHistoryEntry.2.67 = RTT
clogHistoryEntry.3.67 = 4
clogHistoryEntry.4.67 = SAATHRESHOLD
clogHistoryEntry.5.67 = RTR(18): Threshold exceeded for jitterDSAvg
clogHistoryEntry.6.67 = 993229411

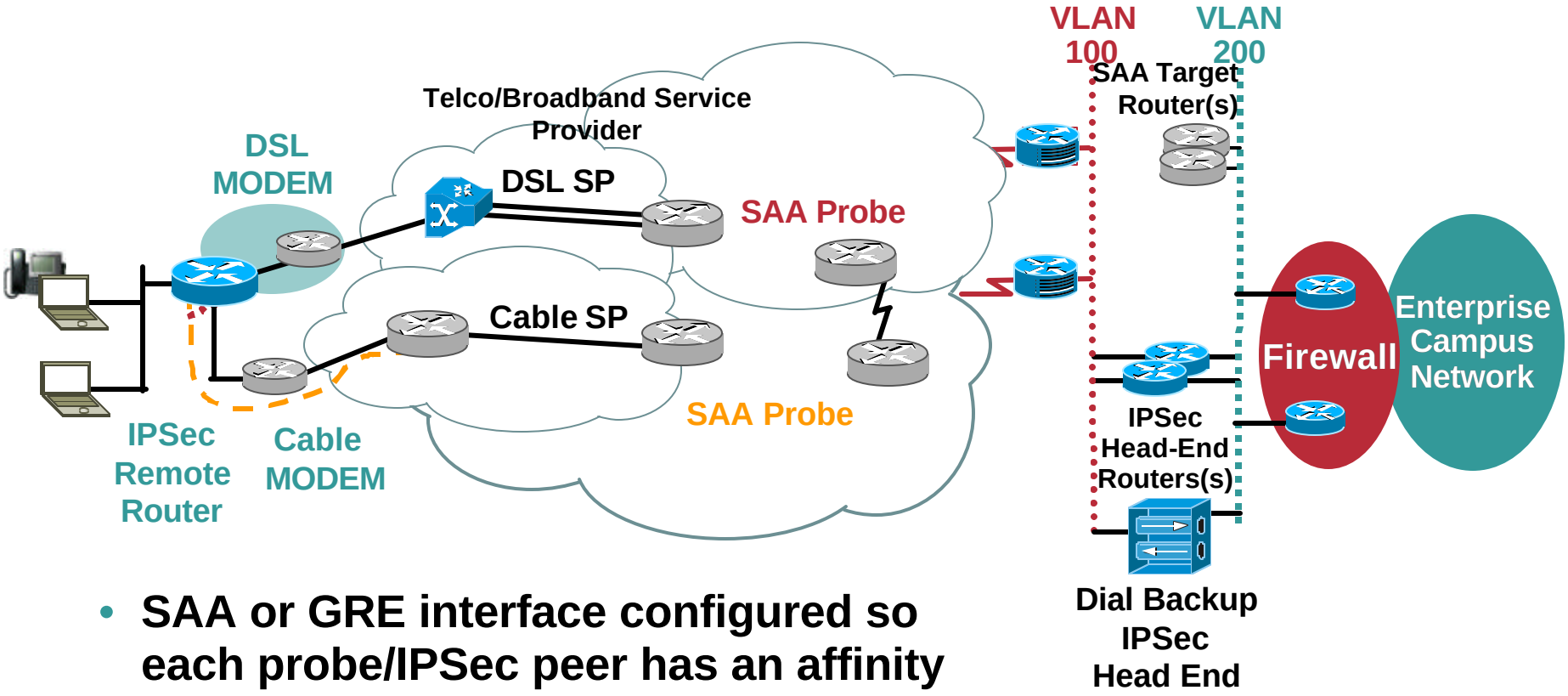
APPENDIX: Head-end Topology - Backup and Redundancy

(supplemental slides)

Load Sharing—Dual Broadband

Load Sharing between Cable and DSL Links

Cisco.com

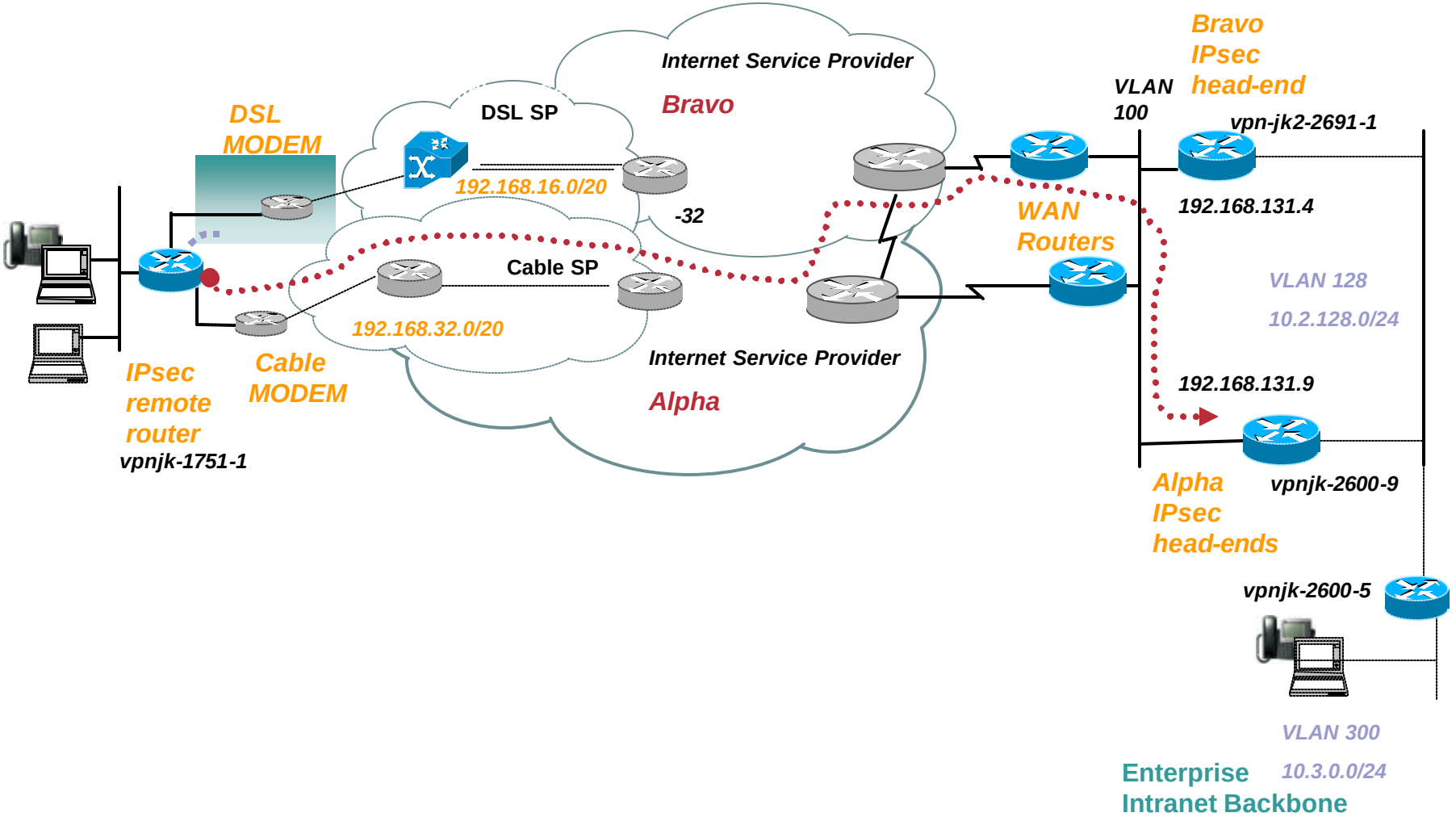


- SAA or GRE interface configured so each probe/IPSec peer has an affinity to a particular interface
- Floating static / ‘tracked’ routes provide load sharing and backup for failed path

Load Sharing - Dual Broadband

Load Sharing Between Cable and DSL Links

Cisco.com



APPENDIX: Performance

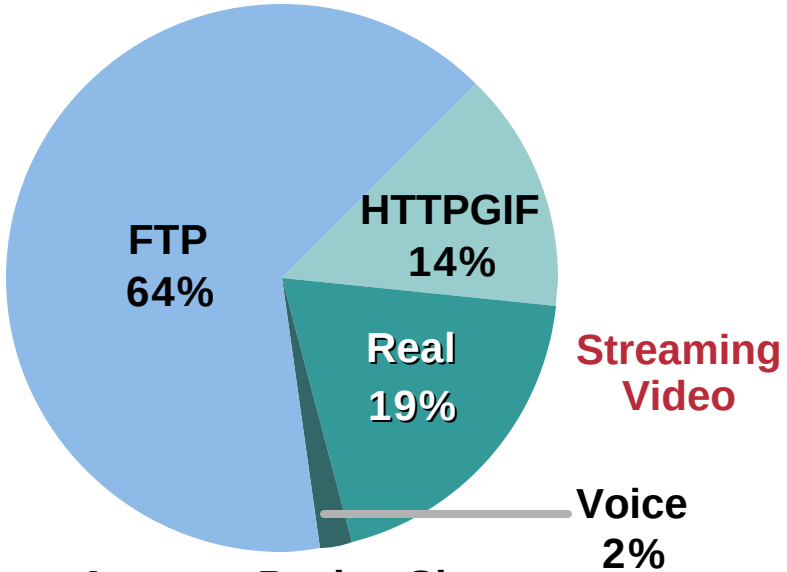
(supplemental slides)

Teleworker Traffic Split Tunnel Excludes IPSec Headers/Trailers

Percent of Bytes

Downstream

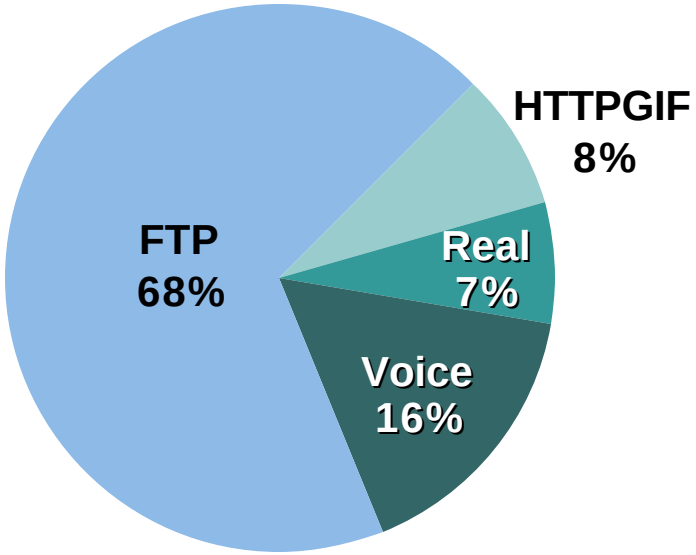
80.4 Megabyte in 10 Minutes
1.0 Mbps



Average Packet Size
= 425 Bytes

Upstream

11.3 Megabytes in 10 Minutes
Shaped to 243 Kbps



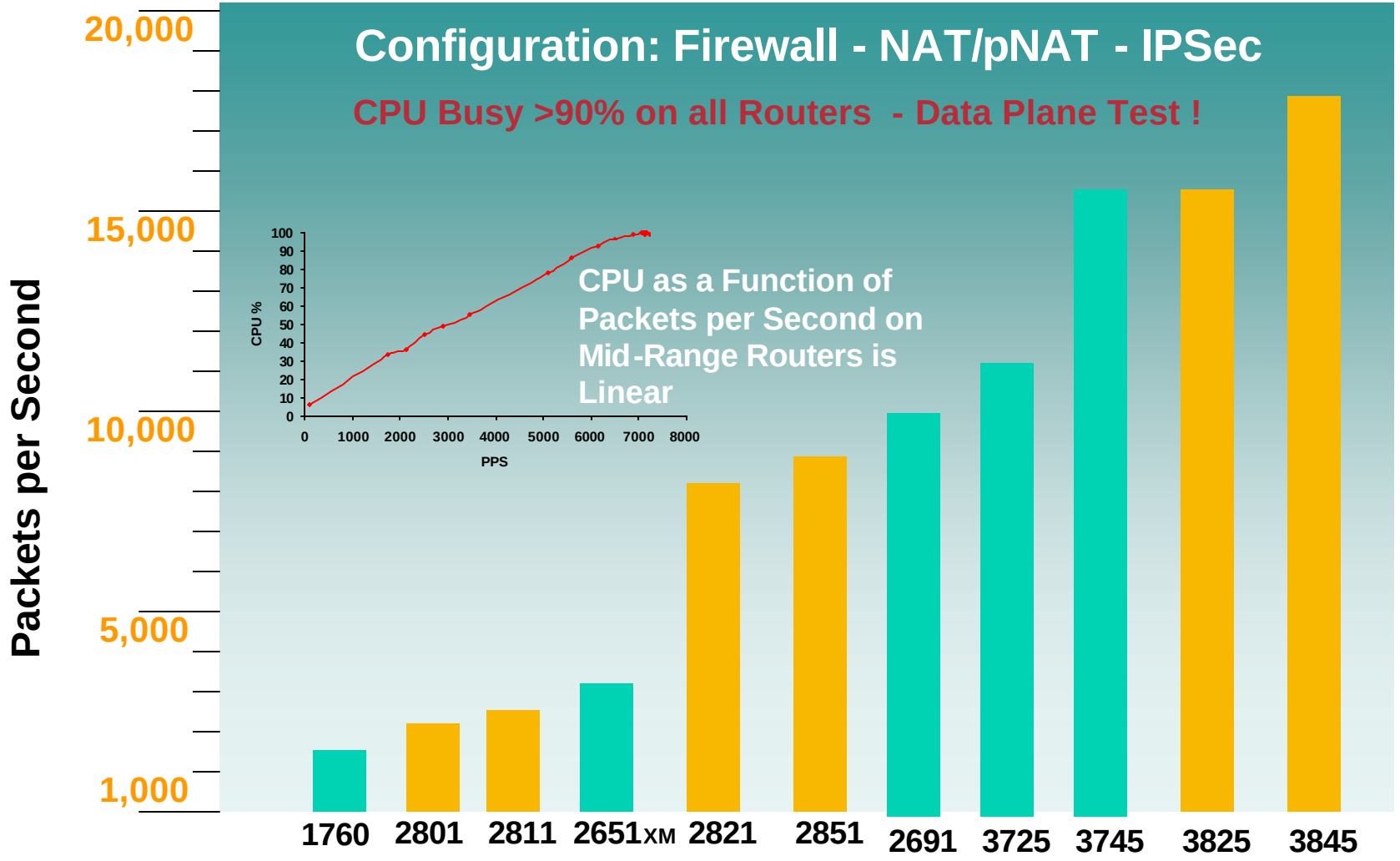
Average Packet Size
= 94 Bytes

NetFlow™ Ten-Minute Chariot Test 831 on Cable 256K/1.0M

ip tcp adjust-mss 542

ICMP DNS TN3270 Call-Setup POP3 HTTP Text—Represents 1% in Both Cases

Performance Comparison
Integrated Services Routers



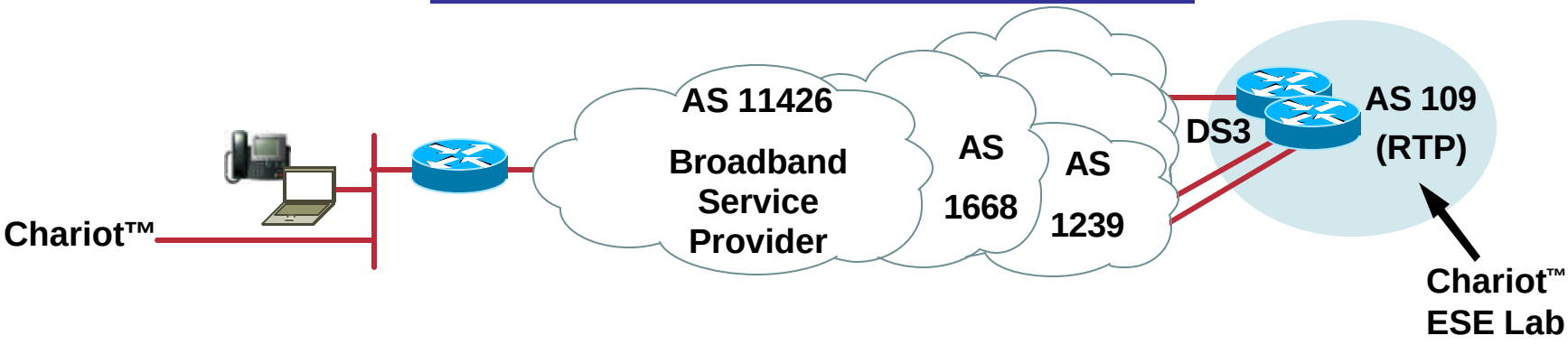
Case Study

Cisco 1711—Chariot Branch Profile Test Business Class Cable

Link Rate (K) Up/Down Media	Platform	Number of G.729 Calls	MSS Value	Jitter (ms) B2H	Jitter (ms) H2B	Latency (ms) B2H	Latency (ms) H2B	Mbps Data	Total CPU	pps Data/Voice
768K/ 3072K Business Cable	1711	1	N/A*	5.4	4.5	34	33	2.4	59%	395/100

Voice Drops < .2%

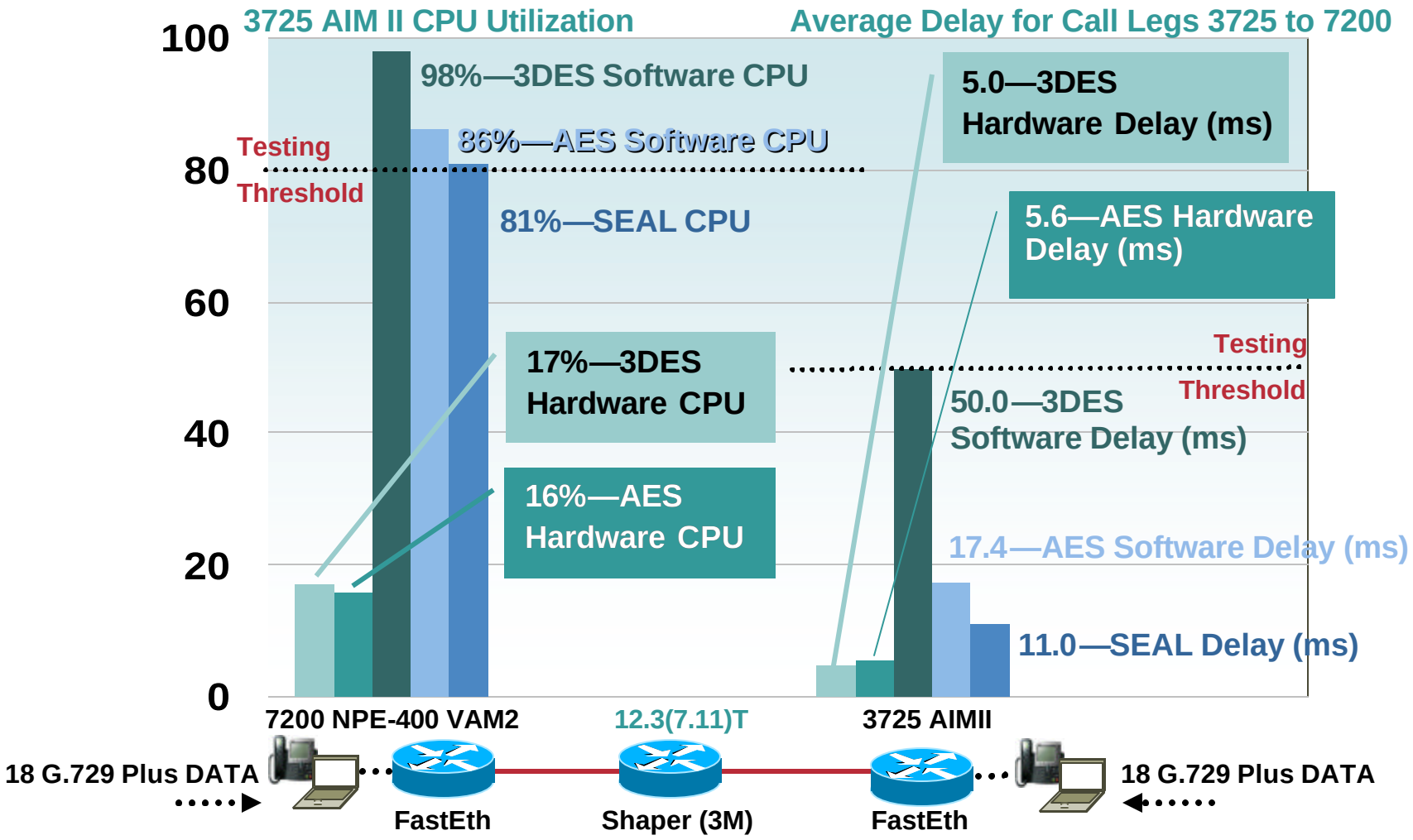
Mission Critical Response Time .11 Sec



*Serialization Delay Not an Issue on 768K Link—B2H = Branch to Head—H2B = Head to Branch

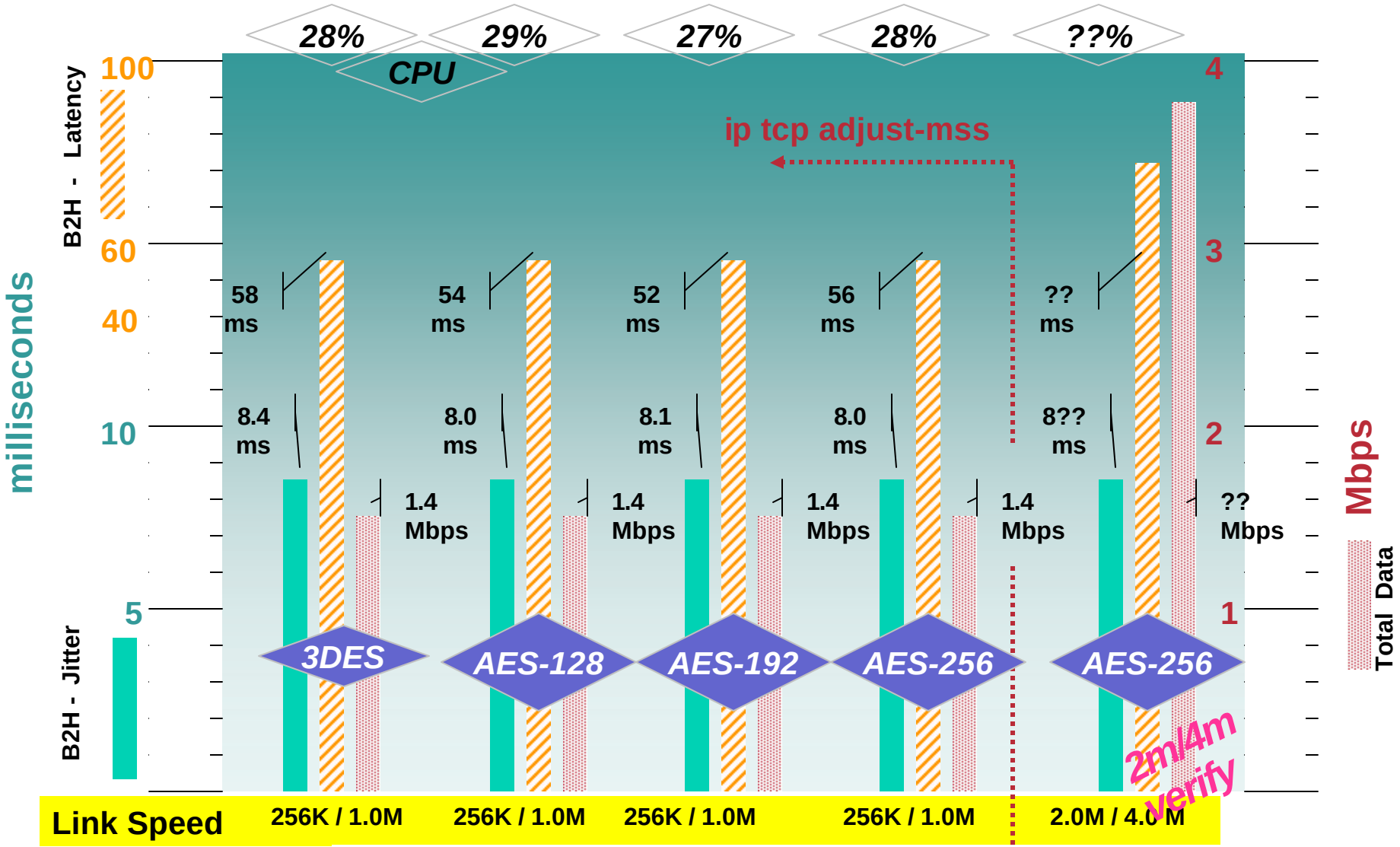
AES 128bit vs. 3DES vs. SEAL[1]

VoIP PLUS Data



Note 1: SEAL Is a Software-Efficient Stream Cipher—Not Ideal for Hub and Spoke

871 Performance Chart – 3DES _ AES-128 _ AES-192 _ AES-256



Remote Router Performance
aDSL Various Data Rates

Cisco.com

Link Rate (K) Up/Down	Platform	Number of G.729 Calls	MSS Value	Jitter B2H	Jitter H2B	Latency B2H	Latency H2B	Mbps Data	Total CPU
256/1408	831	1	542	8.0	7.2	67	37	.9	54%
384/1536	831	1	542	6.7	9.0	54	74	1.2	67%
512/2048	831	1	542	5.1	5.8	71	52	1.6	81%
768/3072	831	1	542	3.7	5.1	51	64	2.1	92%
	1751	1	542	3.8	3.6	86	28	2.0	70%
	831	1	1360*	8.8	7.9	53	38	2.3	73%
	1751	1	1360*	8.4	7.6	54	37	2.3	50%

Jitter Increases, but Still < 10ms—Larger Data Packets Decrease pps Rate and CPU Decreases Accordingly

Voice Drops Not Shown, < .5% in All Cases—*Workstation MTU Set at 1400

Complete Your Online Session Evaluation!

Cisco.com

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session ID: VVT-2004

DESIGNING VOICE ENABLED IPSEC VPNS FOR TELEAGENTS