

Voice and Video Enabled IPsec VPN (V3PN)

Presented by

Dr. Peter J. Welcher, Chesapeake Netcraftsmen



Slide 1

About the Speaker

- **Dr. Pete Welcher**
 - Cisco CCIE #1773, CCSI #94014, CCIP
 - Network design & management consulting
 - Stock quotation firm, 3000 routers, TCP/IP
 - Second stock quotation firm, 2000 routers, UDP broadcasts
 - Hotel chain, 1000 routers, SNA
 - Government agency, 1500 routers
 - Teach many of the Cisco courses
- **Enterprise Networking Magazine articles**
 - <http://www.netcraftsmen.net/welcher/papers>



Slide 2

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- Managing V3PN
- Wrap-up

Why Do We Care?

- Many organizations are trying to use IPsec VPN to reduce costs and simplify new connections
- VPN allows
 - Shared Internet and Enterprise access
 - Reduced access line costs
 - Ease of provisioning, flexibility
 - Increased security
- Using IPsec introduces some potential challenges for QoS for Voice and Video
 - But some nice Cisco features for V3PN address the issues and make this work well!



IPSec V3PN Benefits

- **Enhanced productivity and reduced support costs: extend central site voice, video, data resources and applications to all corporate sites**
- **Voice, Video, data transported securely and transparently over IPSec tunnels with QoS enabled**
- **Standard IP Telephony features including codecs, SRST preserved**
- **IPSec VPN design provides resiliency**
- **Integrated branch routers provide ISP connection, VPN termination, IPT gateway, and Cisco IOS Firewall functionality**
- **Tested scalability and performance numbers**



Slide 5

Agenda

- **Introduction and Motivation**
- **IPSec Review**
- **Enterprise IPSec VPN**
- **QoS Review**
- **V3PN**
- **Managing V3PN**
- **Wrap-up**



Slide 6

IPSec Basics

- **IPSec uses a Security Association (SA) and crypto key to encrypt selected data between a pair of sites**
 - This key is used with the DES, 3DES, or AES forms of encryption to both encrypt and decrypt data
- **The key is automatically established, changed, and managed by IPSec devices using IKE (Internet Key Exchange), a.k.a. “ISAKMP”**
- **Before a key can be established, IKE does authentication**
 - Shared secret or Certificate Authority are two ways to do this
- **IKE uses public key crypto to securely do its job**
 - Public and private keys, either encrypts, the other decrypts
 - Diffie-Hellman is the technique used to securely exchange encryption keys

Message Hashing

- **Message Hashing is used to detect altered messages**
 - Message bits a secret key are combined into short hash code
 - Hash code sent in header
 - If received message hash doesn't match, message was altered
 - Two forms: SHA and MD5
 - SHA is a bit stronger

IPSec Protocols

- **IPSec comes in two forms**

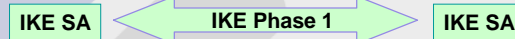
- AH provides a keyed hash and authentication data
 - Ensures data comes from peer router (authentication)
 - Detects alterations (keyed hash)
 - But does not encrypt for confidentiality
- ESP encrypts
 - Two sub-modes: tunnel and transport
 - In tunnel mode, the new IP header hides source and destination addresses: keeps server address confidential
 - Keyed hash for detecting alterations
 - Authentication
 - Encryption

The 4 Steps of IPSec SA Establishment

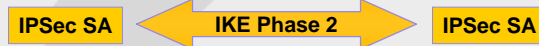
1. Host A sends interesting traffic for Host B



2. Router A and B negotiate an IKE Phase 1 session and authenticate



3. Router A and B negotiate an IKE Phase 2 session and exchange key



4. Information is exchanged via IPSec tunnel



What to Encrypt

- **The crypto map you configure references an access list for “interesting packets”**
 - What to encrypt (outbound)
 - What to decrypt (inbound)
- **If the router encrypts or decrypts the wrong packet, it gets nonsense and a bad checksum → discarded packet!**

IPSec Troubleshooting Tips

- **The two ends have to agree on the various choices**
 - How to do IKE (IKE policy)
 - Authentication method, shared secret or CA, etc.
 - AH versus ESP
 - Tunnel versus transport
 - Message hashing scheme
- **You need routing to be able to deliver packets**
- **IPSec source address at one end must match destination at the other**
- **You need consistent crypto access lists!!!**
 - The two endpoint ACL's need to mirror each other
- **Use the 4 steps to troubleshoot**

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- Managing V3PN
- Wrap-up

Design Assumptions

- High availability and failover with fast convergence
- Support for dynamic routing
- Ability to carry diverse traffic, including IP multicast, multi-protocol
- Conservative CPU levels
- Router-based (versus VPN concentrator)

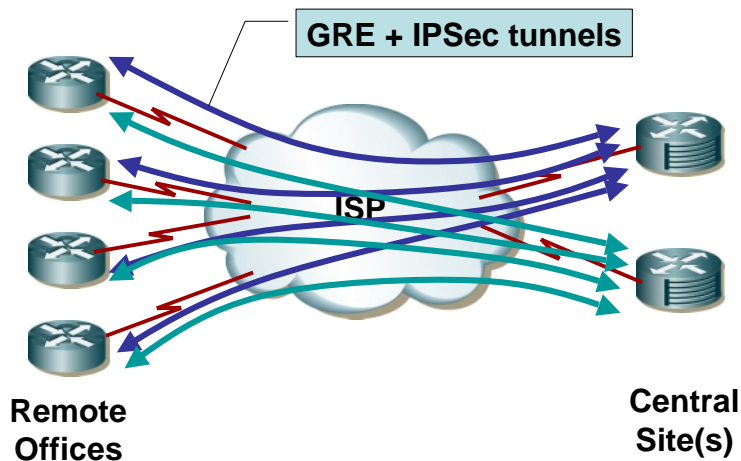
Key Design Components

- **Cisco VPN routers as head-end VPN termination**
- **Cisco access routers as branch termination**
- **Use hardware IPsec acceleration**
- **IPsec ESP Tunnel mode**
- **GRE tunnels, dual star to two head-end routers**
 - At HQ or two head-end sites for geographic diversity
- **Internet services from an ISP**



Slide 15

Enterprise IPsec VPN



Slide 16

Why GRE with IPSec?

- Dynamic routing and support of multicast and non-IP protocols
- Side effect: simpler implementation and troubleshooting
- If you're not building in redundancy, you can leave out the GRE and the dynamic routing and reduce overhead, at the price of doing a bit more configuration

Overhead

- **Cost (GRE + IPSec): 24 more bytes of header (overhead)**
- Total headers added: 76 bytes

IPSec Tunnel IP Header	ESP Header	GRE IP Header	GRE Header	IP Header	Payload
20 B	32 B, variable	20 B	4 B	20 B	

Avoiding Fragmentation

- **We want to avoid fragmenting the IPsec packets**
 - They have to be re-assembled at the termination router to be decrypted
 - Re-assembly is process switched
 - Slow + CPU impact
 - So create fragments BEFORE IPsec encrypts!
 - Reduce GRE tunnel MTU to 1400+ Bytes
 - Consider enabling Path MTU Discovery on the tunnels

Path MTU Discovery

- **Path MTU Discovery is used by current and recent UNIX and Windows servers**
 - They send large packets with DF set
 - Intervening routers needing smaller MTU send back ICMP message with option indicating desired frame size
- **Problem: some web / server sites block all ICMP packets**
 - Result: large web images, FTP file transfers mysteriously fail, but only to some sites
 - Use router default, tunnels not doing P-MTU-D
 - Use router default: Cisco GRE and IPsec tunnels reset DF=1 to DF=0 and fragment
 - “Cisco Pre-Fragmentation for IPsec VPN” feature
 - This plus GRE MTU of 1400 means no P-MTU-D issues even with web traffic via IPsec + GRE tunnels

Which Router?

- Cisco tested ESP tunnels with GRE to 2 head-end sites, 240 branch routers
- Recommendations are based on 55-65% CPU for a specific traffic mix.
- This is a summary: see the Cisco documents for details. In particular, specific models within a product family may have lower performance than that shown. Your Mileage May Vary.

Router	H/w Accel	Max bps	Recommended	Role(s)
7200	ISA or VAM	140 M	40 M	Central
7100	ISM, VAM	140 M	30 M	Central
3600	AIM	38 M	16 M	Large/medium branch
2600	AIM	14 M	3 M	Large/medium branch
1700	VPN Module	3 M	2.5 M	Medium/small branch
800	N/a	384 K	100 K	Small office

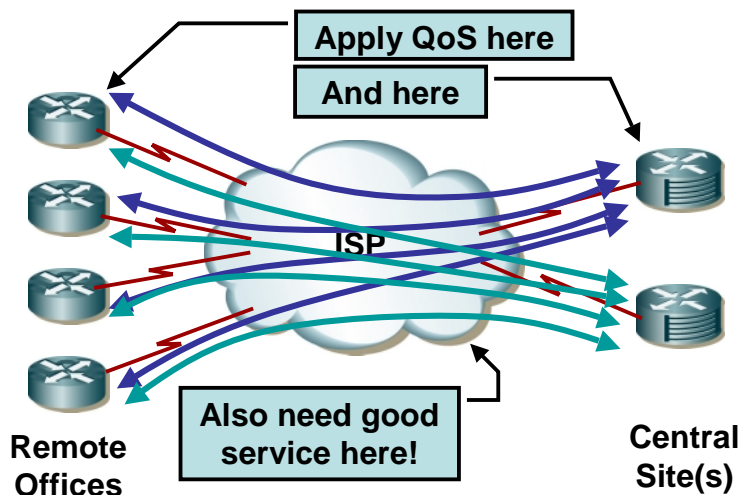
Other Recommendations

- **Have a summarizable addressing scheme**
 - It can makes crypto ACL's simpler, less of an issue with GRE
 - Use route summarization
- **For central DHCP, use helper addresses remotely**
- **Use IPSec Tunnel Mode with 3DES**
- **Don't use IKE keepalives**
- **Base number of head-end devices on number of remote sites and throughput**
- **Use appropriate (recent) Cisco IOS releases**
- **Avoid IPSec through NAT points**

IPSec Sequence Numbers

- **IPSec also uses sequence numbers for anti-replay protection**
 - Out-of-order packets can lead to dropped packets!
 - Conclusion: priority queuing and load-balancing can lead to drops in an IPSec environment!
- **Make one GRE tunnel primary with single preferred path for each remote site**
 - Dynamic routing failover preserved
 - Can use interface delay parameter to prefer one GRE tunnel over the other (if both head end routers at same site)

Service Provider



Service Provider – 2

- **Many or even most ISP's do not honor the L3 QoS markings**
 - Your voice traffic may experience unacceptable delay or jitter
- **Whenever possible, you need SLA's**
 - Covering overall delay and jitter, repair time, etc.
 - Or for QoS-aware service guaranteeing certain delay and jitter levels for various classes of traffic, based on agreed-upon markings
 - Otherwise, you can deploy and later discover your IPsec VPN isn't working very well: no recourse!
- **Multiple ISP's is harder**
 - SLA's generally only apply within a single ISP's network
- **Beware: some home cable & DSL services block IPsec unless "business grade" service is paid for**



Slide 25

SLA's

- **CPN Multi-service VPN standards:**
 - Jitter – less than or equal to 20 msec
 - Delay – less than or equal to 60 msec one way
 - Packet Loss – less than or equal to 0.5 percent

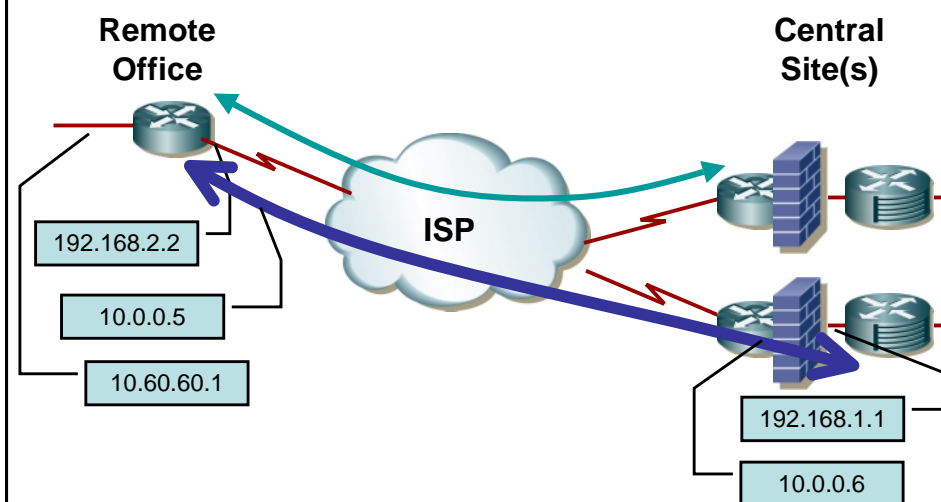


Slide 26

Configuration Steps

- **Step 1: Configure IKE policy**
- **Step 2: Specify IPSec transform and protocol**
- **Step 3: Create access lists (ACL's) for encryption**
- **Step 4: Configure crypto map**
- **Step 5: Apply crypto map**

Enterprise IPSec VPN



Sample: IKE Policy

Head End Router

```
interface FastEthernet1/0
ip address 192.168.1.1
 255.255.255.0
!
crypto isakmp policy 1
encr 3des
authentication pre-share
crypto isakmp key mybigsecret
  address 192.168.2.2
```

Branch Router

```
interface s0/0
ip address 192.168.2.2
 255.255.255.0
!
crypto isakmp policy 1
encr 3des
authentication pre-share
crypto isakmp key mybigsecret
  address 192.168.1.1
```



Slide 29

Sample: IPsec Transform and Protocol

Head End Router

```
crypto ipsec transform-set
vpn-t-test esp-3des
  esp-sha-hmac
```

Branch Router

```
crypto ipsec transform-set
vpn-t-test esp-3des
  esp-sha-hmac
```



Slide 30

Sample: Encryption ACL's

Head End Router

```
ip access-list extended
vpn-static-1 permit gre
host 192.168.1.1 host
192.168.2.2
```

Branch Router

```
ip access-list extended
vpn-static-2 permit gre
host 192.168.2.2 host
192.168.1.1
```



Slide 31

Sample: Crypto Map

Head End Router

```
crypto map static-map-pjw1
local-address
FastEthernet1/0
crypto map static-map-pjw1 1
ipsec-isakmp
set peer 192.168.2.2
set transform-set vpn-t-test
match address vpn-static-1
```

Branch Router

```
crypto map static-map-pjw2
local-address Serial0/0
crypto map static-map-pjw2 1
ipsec-isakmp
set peer 192.168.1.1
set transform-set vpn-t-test
match address vpn-static-2
```



Slide 32

Sample: Apply Crypto Map

Head End Router

```
interface Tunnel1
ip address 10.0.0.5
 255.255.255.252
tunnel source 192.168.1.1
tunnel destination
 192.168.2.2
crypto map static-map-pjw1
!
interface FastEthernet1/0
ip address 192.168.1.1
 255.255.255.0
crypto map static-map-pjw1
```

Branch Router

```
interface Tunnel1
ip address 10.0.0.6
 255.255.255.252
tunnel source 192.168.2.2
tunnel destination 192.168.1.1
crypto map static-map-pjw2
!
interface Serial10/0
bandwidth 1536
ip address 192.168.2.2
 255.255.255.0
crypto map static-map-pjw2
```



Slide 33

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- Managing V3PN
- Wrap-up

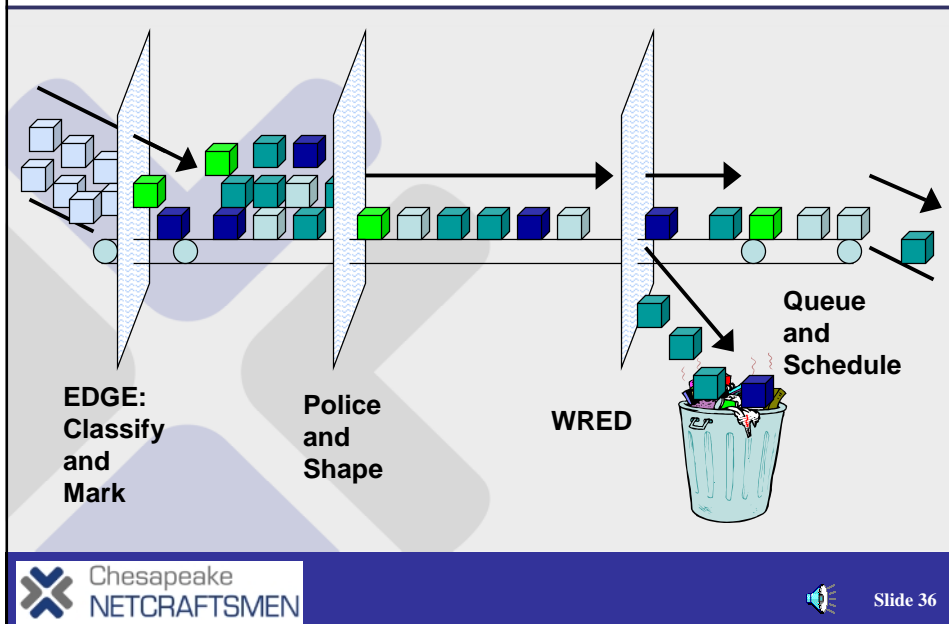


Slide 34

Purpose of QoS

- **Allow different kinds of application traffic (data, voice, video, etc.) to share links while meeting their needs**
- **Needs might include**
 - Low latency and jitter
 - Low drop rate

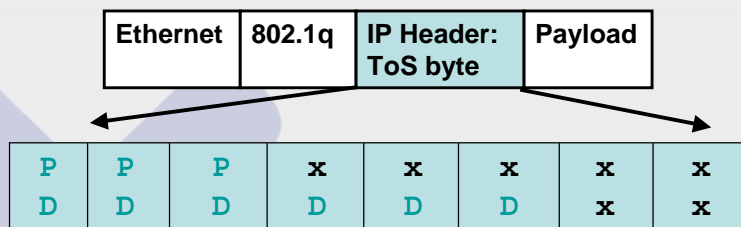
The Operations of QoS



QoS Operations

- **Classify and mark for different types of handling**
 - L2 frames: CoS bits (in trunk headers or 802.1p only)
 - L3 packets: IP Precedence or DSCP bits
- **Rate enforcement: limit traffic rate**
 - Policing: drop or mark down the excess
 - Shaping: queue or delay the excess
- **Low latency queuing**
 - Prioritize critical traffic to reduce latency & jitter
- **Guaranteed minimum bandwidth**
- **Congestion avoidance**
 - Selectively drop less important traffic to reduce congestion

Layer 3 Marking



- **IP header ToS byte used for IP marking**
- **IP Precedence: 3 bits, 0-7**
 - 6 & 7 reserved for system use
- **Diff Serv: 6 bits, 0-63**
 - Backwards compatible with IP Precedence
- **Purpose: allow downstream devices to quickly determine importance of traffic and desired handling**

QoS Operations for WAN

- **On slow links (< 768 Kbps)**
 - Need to use the bandwidth frugally
 - Link Fragmentation and Interleaving (LFI)
 - Consider compressed RTP (cRTP)
 - Consider Voice Activity Detection (VAD)
 - Consider lower bandwidth VoIP codecs
- **On FR, ATM**
 - Shape to CIR or effective bandwidth, so data bursts don't cause dropped VoIP

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- Managing V3PN
- Wrap-up

Best Practices

- **See earlier list of IPSec VPN practices**
- **Beware performance limits of devices**
- **Use hardware encryption**
- **Use QoS Pre-Classify (see below)**
- **Use G.729 codec to save bandwidth (IPSec + GRE overhead are bad enough!)**
- **Use a Cisco Powered Network SP designated as “IP Multi-service VPN Provider”**
- **Consider separate head-end WAN router(s), offloads routing and QoS**



Slide 41

Limitations

- **Not fully addressed or tested for first release of the current Cisco design guide:**
 - Video
 - IP multicast
 - Dynamic Multipoint VPN
 - AES encryption
- **PIX-based VPN design guide coming**
- **Several newer features also not considered or tested yet**
 - Voice Activity Detection (VAD)
 - Survivable Remote Site Telephony (SRST)
 - Dynamic Multi-point VPN (DMVPN)
 - IPSec stateful failover, digital certificates
 - LZS compression, GRE tunnel keepalives, EIGRP stubs



Slide 42

IPSec QoS Issues

- **Much increased packet overhead**
 - Using G.729 helps get the bandwidth consumption down some
 - G.711 + IPSec + GRE → 114 Kbps w/ FR headers
 - G.729 + IPSec + GRE → 56 Kbps w/ FR headers
 - This makes VAD also attractive, but perceived quality can drop with VAD
- **Need hardware encryption**
 - Software encryption is subject to CPU-derived delay and jitter
- **cRTP incompatible with IPSec**
 - Headers encrypted before cRTP stage

IPSec QoS Issues – 2

- **Delay budget for VoIP**
 - Testing yields 2-5 msec for encryption or decryption
 - 10 msec total is pretty much a non-issue
- **Spoke-spoke crypto delay**
 - Traffic via the hub requires 2 ISP hops ...
 - This is where DMVPN or partial meshing might be attractive

IPSec QoS Issues – 3

- **Crypto engine FIFO queue**
 - Prior to 12.2(13) T, crypto engine used single FIFO queue
 - After that, traffic from LLQ gets LLQ treatment in the crypto queue
 - Testing suggests the router CPU bogs down before this is an issue for hardware crypto anyway
 - Except for software crypto, which still has just FIFO queue
- **Anti-replay sequencing failures**
 - Altered packet order can result in out of sequence hence dropped packets
 - Minimal effect in tested scenarios
 - Voice OK, it's data that will get dropped
 - Can tune queue depth to more aggressively drop excess data before sending it

General WAN QoS – 1

- **FR: continue using LFI, FRF.12**
- **Use CBWFQ LLQ, but for no more than 33% of the total traffic**
- **FR / ATM: consider shaping to 95% of carrier CIR / SCR if conservative**
- **When doing FRTS, do not do BECN adaptation**

General WAN QoS – 2

- **Make sure to plan the number of concurrent calls**
 - Quick rule of thumb: 1 call per 6 people (1:6)
 - Depends on what people at the office do
 - Could be 1:4 to 1:10
 - Better: do BHCA and Erlang design for VoIP
- **Strongly consider Call Admission Control (CAC)**
 - CallManager Locations (hub & spoke!)
 - Or H.323 gatekeeper functionality in routers



Slide 47

QoS Pre-Classify

- **GRE and IPSec preserve the ToS byte bearing IP Precedence or DSCP markings automatically**
 - Otherwise, this byte would be in the encrypted payload, inaccessible for QoS purposes
 - However, source/destination, protocol, and port info is encrypted and inaccessible outbound
- **QoS pre-classify command on output interface causes unencrypted clone of IP header to be available**
 - Can fully classify, mark, and do QoS on outbound interfaces on the encrypting router, if desired
 - Not needed if packets already marked before this!



Slide 48

Sample: EIGRP Summary and Delay

Head End Router

```
interface Tunnell
! Advertise "This way to rest of
network 10/8."
ip summary-address eigrp 1
10.0.0.0 255.0.0.0 5
```

Branch Router

```
interface Tunnel0
ip summary-address eigrp 1
10.60.60.0 255.255.255.0 5
ip hold-time eigrp 1 25
```

```
interface Tunnell
! Advertise just local subnet(s)
ip summary-address eigrp 1
10.60.60.0 255.255.255.0 5
ip hold-time eigrp 1 25
delay 60000
!
router eigrp 1
passive-interface Serial0/0.1
passive-interface Ethernet0/1
network 10.0.0.0
no auto-summary
eigrp log-neighbor-changes
```



Slide 49

QoS: Trust Boundary

- **QoS: we are assuming IP Precedence set by IP phone and/or edge switch with L3 classification capability**
- **QoS at Branch: small branch switch may only be L2-capable (CoS-only)**
 - In which case, the branch router needs to use an ACL or NBAR to classify traffic and mark it with IP Precedence



Slide 50

Sample Branch Router QoS

- May need to map IP Precedence or DSCP to CoS if branch switch is L2-only
- Requires trunk from branch router to switch

```
class-map match-all call-setup
  match ip precedence 3
class-map match-all voice
  match ip precedence 5
class-map match-all all-
mission-critical
  match ip precedence 2
  match ip precedence 6
```

```
policy-map output-L3-to-L2
  class voice
    set cos 5
  class call-setup
    set cos 3
  class mission-critical
    set cos 2
!
interface FastEthernet0/1.201
  encapsulation dot1Q 201
  ip address 10.60.60.1
  255.255.255.0
  service-policy output output-L3-
to-L2
```



Slide 51

Sample Configuration: FR

```
policy-map 512kb-divvy
  class call-setup
    bandwidth percent 5
  class mission-critical
    bandwidth percent 22
  class voice
    priority 168
  class class-default
    fair-queue
policy-map 512kb-shaper
  class class-default
    shape average 480000 1920 0
  service-policy 512kb-divvy
```

```
interface Serial2/0/0/10:1
  no ip address
  encapsulation frame-relay
  no fair-queue
interface Serial2/0/0/10:1.102 point
  ip address ...
  frame-relay interface-dlci 102
  class frts-512kb
!
map-class frame-relay frts-512kb
  no frame-relay adaptive-shaping
  service-policy output 512kb-shaper
  frame-relay fragment 640
```



Slide 52

Sample Configuration: FRF.12 & FRTS

```
interface Serial1/0.1 point-to-point
  bandwidth 512
  ... <as before>
  class ts-branch
  crypto map static-map-pjw1
  map-class frame-relay ts-branch
  frame-relay cir 486400
  frame-relay bc 4864
  frame-relay be 0
  frame-relay mincir 486400
  no frame-relay adaptive-shaping
  service-policy output llq-branch
  frame-relay fragment 640
```

QoS Pre-Classify

- Up to here, fairly vanilla WAN QoS...
- Do need to add “**qos pre-classify**” to GRE tunnel interfaces and crypto maps if applying QoS policy outbound

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- **Managing V3PN**
- Wrap-up

Cisco VPN Network Management Tools

- **CiscoWorks VPN / Security Management Solution (VMS) includes**
 - Management Center (MC) for IDS Sensors
 - Management Center for VPN Routers
 - Management Center for PIX Firewalls
 - Centralized configuration and management of devices
 - Monitoring Center for Security
 - Central IDS event software, w/ correlation, notification, reports
 - VPN Monitor
 - Track status of VPN devices, w/ drill-down reporting
 - IDS Host Sensor
 - Auto-Update Server
 - Pull model of distribution of images and configurations
 - Resource Manager Essentials (RME), CiscoView, Common Services

Agenda

- Introduction and Motivation
- IPsec Review
- Enterprise IPsec VPN
- QoS Review
- V3PN
- Managing V3PN
- Wrap-up

See Also

- AVVID Enterprise Site-to-Site VPN Design
 - http://www.cisco.com/application/pdf/en/us/guest/netso/ns142/c649/ccmigration_09186a00800d67f9.pdf
- Voice and Video Enabled IPsec VPN (V3PN) Solution Reference Network Design Guide
 - http://www.cisco.com/application/pdf/en/us/guest/netso/ns241/c649/ccmigration_09186a0080146c8e.pdf
- IPsec support page
 - http://www.cisco.com/cgi-bin/Support/PSP/psp_view.pl?p=Internetworking:IPSec

Summary

- Use GRE + IPsec in a hub and spoke design for easily managed IPsec VPN with redundancy and failover
- Cisco has tested performance under load for 240 remote branch routers going to 2 central routers
- Add QoS configuration and “qos pre-classify” to support voice and video
- Use G.729 VoIP to conserve WAN bandwidth
- Fragment before IPsec for much better performance

Disclaimer: this presentation touches on most of the high-level issues, but it definitely does not cover all the details of QoS or V3PN planning.



Slide 59

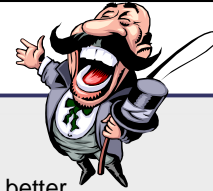
Questions?

THANK YOU !



Slide 60

A Word From Us ...



- **We can provide**
 - Network design review: how to make what you have work better
 - Periodic strategic advice: what's the next step for your network or staff
 - Network management tools & procedures advice: what's right for you
 - Implementation guidance (your staff does the details) or full implementation
- **We do**
 - Small- and Large-Scale Routing and Switching (design, health check, etc.)
 - IPsec VPN and V3PN (design and implementation)
 - QoS (strategy, design and implementation)
 - IP Telephony (preparedness survey, design, and implementation)
 - Call Manager deployment
 - Security
 - Network Management (design, installation, tuning, tech transfer, etc.)



Slide 61

Cisco Certifications

Chesapeake Netcraftsmen is certified by Cisco in:

- IP Telephony
- Network Management
- Wireless
- Security
- (Routing and Switching)



Slide 62