

• NETWORKERS

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

1


CISCO SYSTEMS



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

2



Cisco.com

# Design Guidelines for Voice over IPsec VPN Deployments

Session VVT-216  
24 June—Revised

WT-216  
5172\_05\_2002\_c1 © 2002, Cisco Systems, Inc. All rights reserved. 3

## Agenda

Cisco.com

- **Overview**
- **Planning Considerations**
- **Design Guidelines**
- **Case Study**
- **Summary**

WT-216  
5172\_05\_2002\_c1 © 2002, Cisco Systems, Inc. All rights reserved. 4

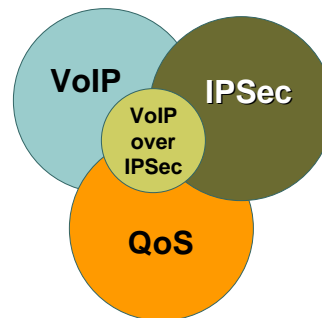
## Goal

Cisco.com

### Successfully Design and Implement Voice over an IPsec VPN

#### Components for VoIP over IPsec

- Voice over IP (VoIP)
- Quality of Service (QoS)
- IP Security (IPsec)



**Reduces Cost, Increases Productivity, Flexibility and Convenience**

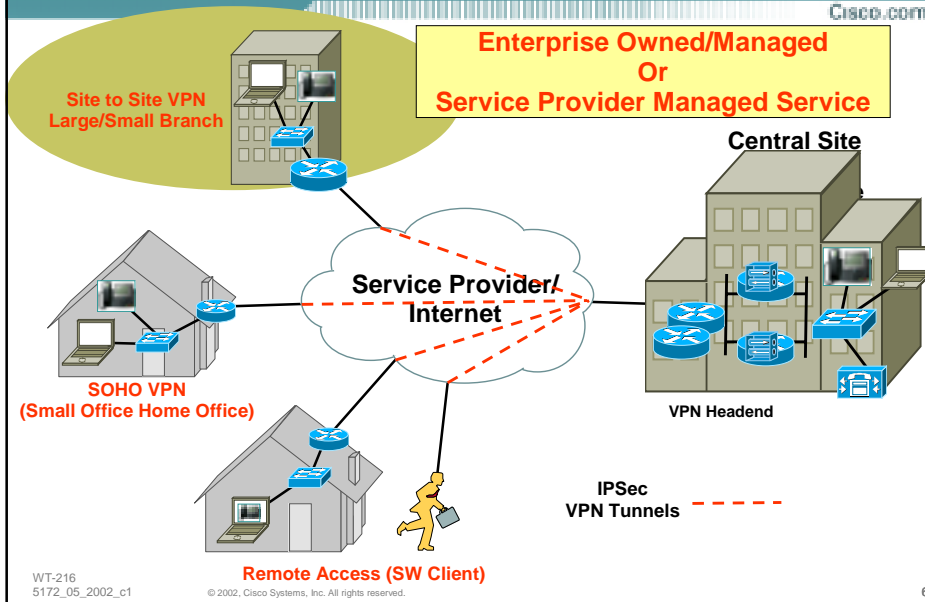
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

5

## QoS Enabling IPsec VPNs: What we are going to build

Cisco.com



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

6

## Companion Sessions

Cisco.com

- **SEC-210: Deploying and Managing Enterprise IPsec VPNs**
- **VVT-201: Designing Voice/Video Enabled SOHO IPsec VPN Telecommuter**
- **NSC-215: Deploying QoS in an Enterprise Environment**
- **PS-530: Building End-to-End IP Telephony Power Session**

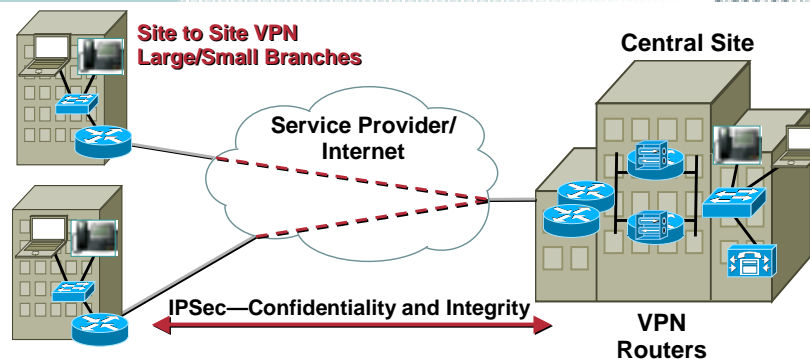
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

7

## Deployment Model: Site to Site VoIP VPN

Cisco.com



- **Hub and Spoke Topology**
- **VoIP support in IP Sec VPN**
  - IOS Routers
  - QoS capable WAN media (Pt to Pt, Frame Relay, etc.)
  - Service provider QoS based SLA for drop, delay and jitter, availability
- **“Gold Class” voice quality when implemented per design criteria**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

8

## Agenda

Cisco.com

- Overview
- **Planning Considerations**
- Design Guidelines
- Case Study
- Summary

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

9

## Planning Considerations

Cisco.com

- **Additional header and trailer overhead of IPSec and GRE (Generic Routing Encapsulation) with voice packets**
- **Routing protocol and GRE for best convergence**
- **Software crypto adds delay and jitter—  
Hardware crypto accelerators best practice**
- **Voice delay budget increased by crypto engine processing**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

10

## Planning Considerations (Cont.)

Cisco.com

- **CODEC (Coder-Decoder) G.711 vs. G.729**
- **QoS re-ordering of IPSec sequenced packets can lead to packet loss upon receipt**
- **Low Latency Queuing (LLQ) for Crypto Engine may be required for some traffic profiles**
- **Service providers as QoS-enabled transport**

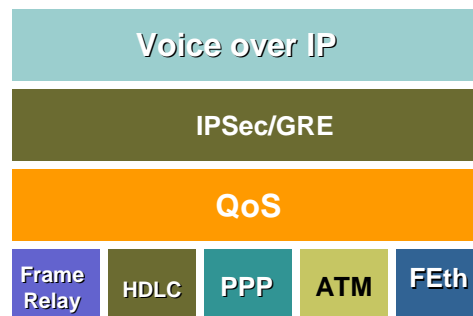
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

11

## WAN Media Considerations

Cisco.com



↑  
Configuration Examples Based on Frame Relay

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

12

# Agenda

Cisco.com

- Overview
- Planning Considerations
- **Design Guidelines**
- Case Studies
- Summary

WT-216  
5172\_05\_2002\_c1

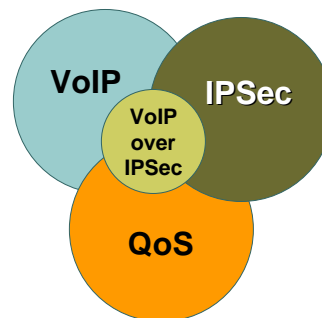
© 2002, Cisco Systems, Inc. All rights reserved.

13

# Design Guidelines

Cisco.com

- **General Design Characteristics**
- Voice over IP (VoIP)
- Quality of Service (QoS)
- IP Security (IPSec)
- Service Provider Considerations
- Solution Test Validation



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

14

## General Design Characteristics

Cisco.com

- **Strong (3DES) encryption—both voice and data**
- **Voice and data in same IPSec/GRE tunnel**
- **Hardware encryption modules**  
AIM-HP,EP,MP,BP SA-VAM/ISA 1751-VPN
- **Hub and spoke tunnel topology**  
IPSec/GRE Tunnels (GRE for IP Multicast, routing protocol, multi-protocol—IPX, AppleTalk)  
Routing protocol
- **Redundancy and availability—dual head-end**
- **QoS-enabled enterprise/service provider**

WT-216  
5172\_05\_2002\_c1

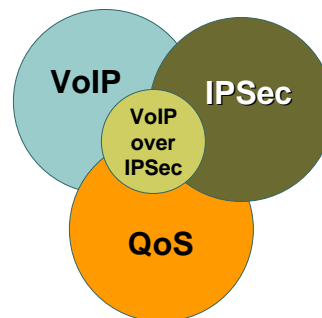
© 2002, Cisco Systems, Inc. All rights reserved.

15

## Design Guidelines

Cisco.com

- **General Design Characteristics**
- **Voice over IP (VoIP)**
- **Quality of Service (QoS)**
- **IP Security (IPSec)**
- **Service Provider Considerations**
- **Solution Test Validation**



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

16

## Voice over IP

Cisco.com

### An Application with Special Requirements

- Packets arrive at a constant rate
- Arrival rate in “per call” increments
- Quality a function of jitter/latency/drops
- Additional call can't degrade existing calls (Call Admission Control) CAC

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

17

## VoIP Design Parameters

Cisco.com

- G.729 CODEC (Coder-Decoder) recommended for  $\leq$  T1 links
- CAC same as FR implementations
- Link fragmentation and Interleaving for low speed ( $< 1024$ Kbps) links
- Hardware encryption accelerators required for predictable latency and jitter
- Frame Relay traffic shaping 10ms interval
- No changes required to CallManager or IP Phone
- Compressed RTP (cRTP) not compatible with encryption

WT-216  
5172\_05\_2002\_c1

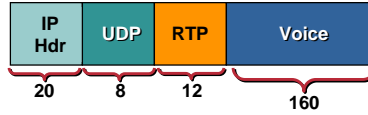
© 2002, Cisco Systems, Inc. All rights reserved.

18

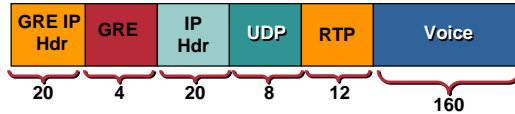
# G.711 CODEC with GRE and IPSec

Cisco.com

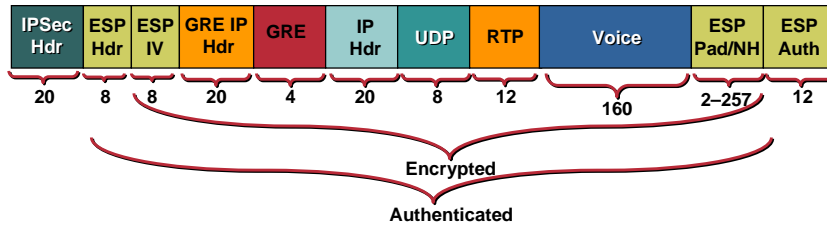
G.711  
200 Bytes



IP GRE  
224 Bytes



IPSec ESP  
Tunnel Mode  
280 Bytes



WT-216  
5172\_05\_2002\_c1

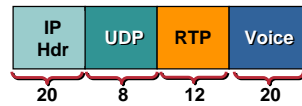
© 2002, Cisco Systems, Inc. All rights reserved.

19

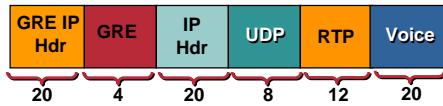
# G.729 CODEC with GRE and IPSec

Cisco.com

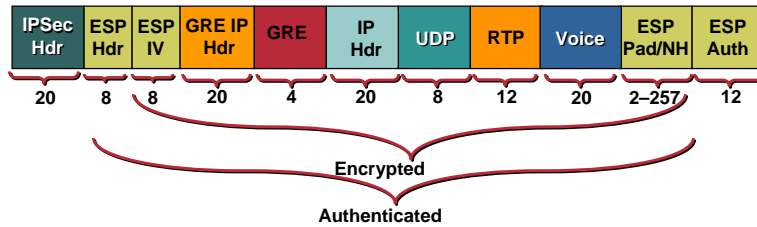
G.729  
60 Bytes



IP GRE  
84 Bytes



IPSec ESP  
Tunnel Mode  
136 Bytes



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

20

## VoIP + IPSec Bandwidth Calculation

Cisco.com

- IP GRE (Generic Routing Encapsulation)
- IPSec Tunnel Mode
- ESP (Encapsulating Security Protocol)
  - Encryption 3DES (esp-3des)
  - Authentication SHA-1 (esp-sha-hmac)
- G.729 = 136 bytes @ 50 pps = **54,400 bps**
- G.711 = 280 bytes @ 50 pps = **112,000 bps**

WT-216  
5172\_05\_2002\_c1

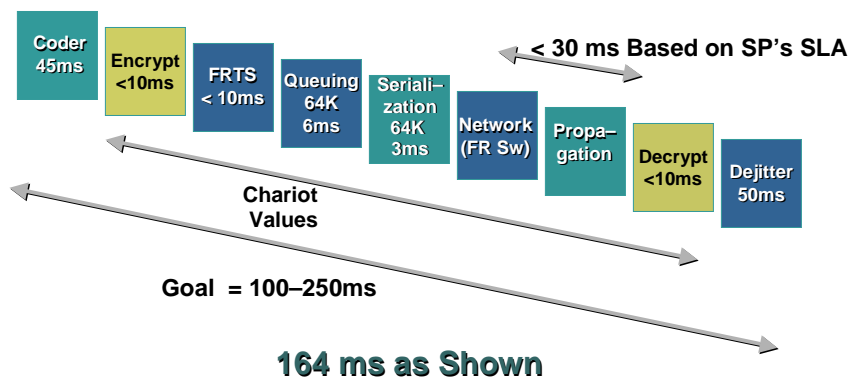
© 2002, Cisco Systems, Inc. All rights reserved.

21

## Delay Budget

Cisco.com

### IPSec Encryption Adds to Delay Budget



WT-216  
5172\_05\_2002\_c1

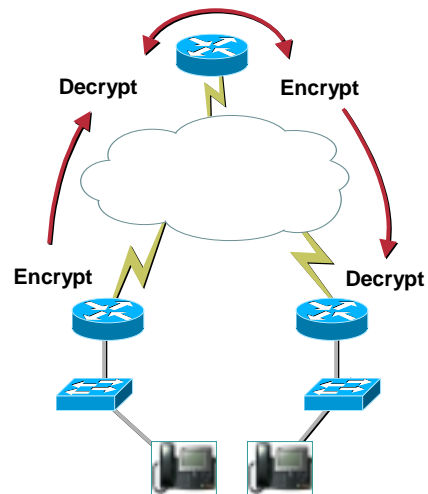
© 2002, Cisco Systems, Inc. All rights reserved.

22

## Spoke to Spoke Delay Budget

Cisco.com

- Doubles the delay budget outside coding and dejitter
- Full mesh issues similar to existing Frame Relay deployments



WT-216  
5172\_05\_2002\_c1

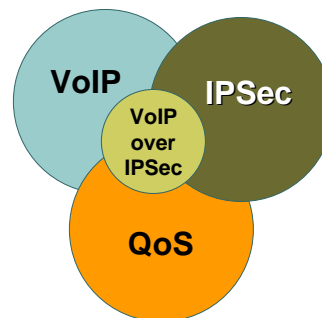
© 2002, Cisco Systems, Inc. All rights reserved.

23

## Design Guidelines

Cisco.com

- General Design Characteristics
- Voice over IP (VoIP)
- **Quality of Service (QoS)**
- IP Security (IPSec)
- Service Provider Considerations
- Solution Test Validation



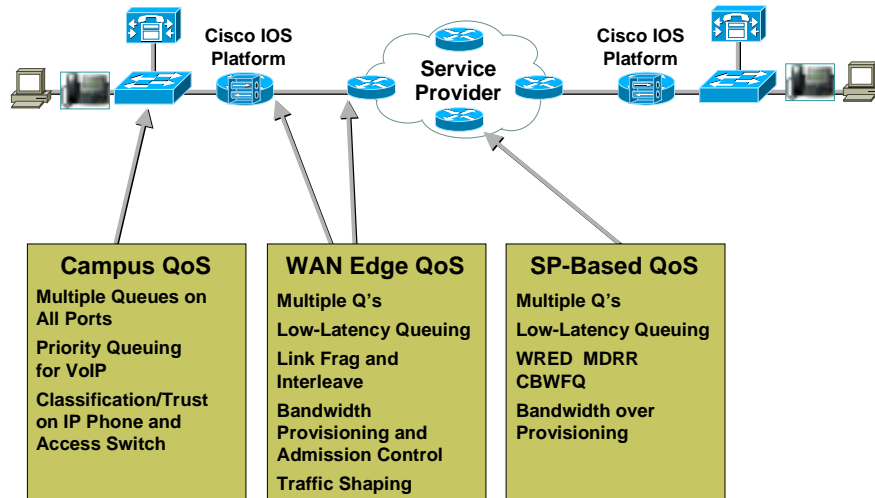
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

24

# QoS Requirements

Cisco.com



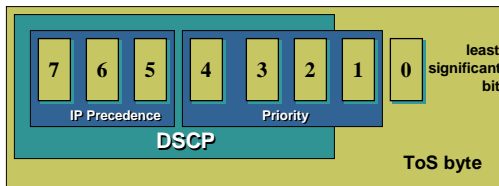
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

25

# ToS Byte—IP Precedence—DSCP Reference Chart

Cisco.com



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

TOS Hex	TOS Decimal	IP Precedence	Class-map Name	DSCP	Binary
E0	224	7 Network Control		CS7	11100000
C0	192	6 Internetwork Control	Mission-Critical	CS6	11000000
B8	184		Voice	EF	10111000
A0	160	5 Critical		CS5	10100000
80	128	4 Flash Override		CS4	10000000
68	104		Call-Setup	AF31	01101000
60	96	3 Flash		CS3	01100000
40	64	2 Immediate	Mission-Critical	CS2	01000000
20	32	1 Priority		CS1	00100000
00	0	0 Routine		Default	00000000

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

26

## Enterprise/SP Edge QoS

Cisco.com

- **Class-Based Weighted Fair Queuing  
CBWFQ/LLQ enabled on WAN interface**
- **Link Fragmentation and Interleaving  
(LFI /FRF.12) configured required**
- **Traffic shaping configured where required**
- **No support for cRTP for VoIP**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

27

## Bandwidth Allocation

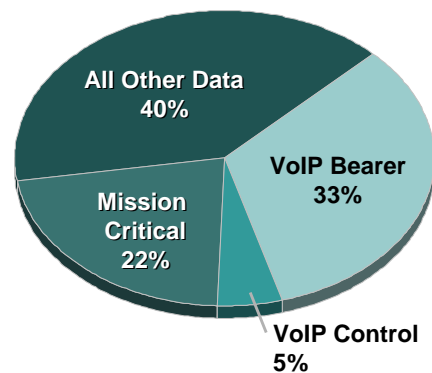
Cisco.com

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

**Voice Target  
33% of Link**

**Reasonable Number  
of Calls Given Speeds  
in Solution Testbed**

**Traffic Categories**



**Includes GRE and IPSec  
Headers/Trailers**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

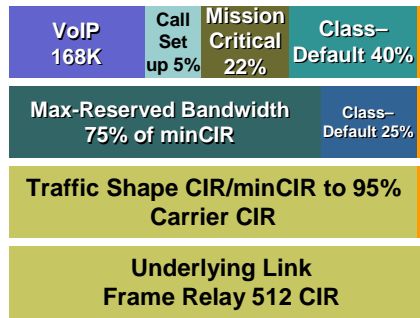
28

# Branch Router Policy-Map

Cisco.com

```

!
policy-map llq-branch
  class call-setup
    bandwidth percent 5
  class mission-critical
    bandwidth percent 22
  class voice
    priority 168
  class class-default
    fair-queue
!
    
```



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

29

# Bandwidth Allocations by Line Rate

Cisco.com

Line Rate Kbps	Max Number of G.729 Calls	Max Calls as a % of Line rate	Priority Kbps at 56k per Call	Call Set-Up 5% in kbps	Mission Critical 22% in kbps	Max-Reserved-Bandwidth
64	1	87.5	56	3	None	100
128	1	43.7	56	6	26	75
256	2	43.7	112	12	53	75
512	3	33	168	24	106	75
768	4	29	224	36	160	75
1024	6	33	336	48	213	75
1536	9	33	504	72	320	75

WT-216  
5172\_05\_2002\_c1

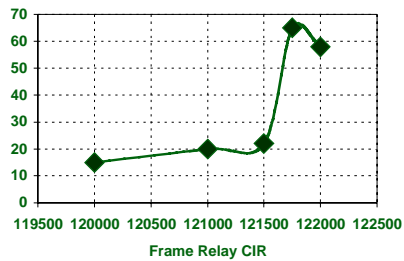
© 2002, Cisco Systems, Inc. All rights reserved.

30

## Frame Relay Traffic Shaping

Cisco.com

- Latency increases dramatically as offered rate approaches Carrier's Committed Information Rate (CIR)
- IOS FRTS does not include CRC FCS and flags
- Shape to 95% Carrier CIR



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

31

## Branch Frame Relay Traffic Shaping and LFI Parameters

Cisco.com

Line Rate Kbps	TS CIR/ minCIR	TS bc	LFI Bytes
64	60800	608	80
128	121600	1216	160
256	243200	2432	320
512	486400	4864	640
768	729600	7296	1000
1024	972800	9728	N/A
1536	1459200	14592	N/A

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

32

# WAN Edge QoS Configuration

Cisco.com

```

!
interface Serial0/0
  bandwidth 512
  no ip address
  encapsulation frame-relay
  frame-relay traffic-shaping
!
interface Serial0/0.100 point-to-point
  bandwidth 512
  ip address 192.168.1.1 255.255.255.252
  frame-relay interface-dlci 100
  class ts-branch
  crypto map GRE
!
map-class frame-relay ts-branch
  no frame-relay adaptive-shaping
  frame-relay cir 486400
  frame-relay bc 4864
  frame-relay be 0
  frame-relay mincir 486400
  service-policy output llq-branch
  frame-relay fragment 640
!

```

**Shape to 95% CIR** (points to `frame-relay cir 486400`)

**Fragment Size 10ms** (points to `frame-relay fragment 640`)

**Frame Relay Traffic Shaping required for FRF.12** (points to `frame-relay traffic-shaping`)

**Frame Relay Traffic Shaping Interval—10ms** (points to `no frame-relay adaptive-shaping`)

**Service Policy Calculated on mincir** (points to `frame-relay mincir 486400`)

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

33

# QoS Pre-Classify

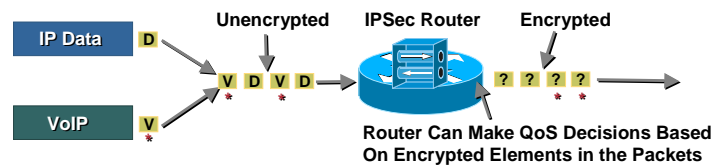
Cisco.com

- Independent of ToS byte copy to IPSec IP Header
- Maintains pre-encapsulated IP header for output QoS policy—port, protocol, src/dst IP address, etc.
- **Required** command for HW accelerators and service-policy on output interface until CSCdx08427
- 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
!

```



WT-216  
5172\_05\_2002\_c1

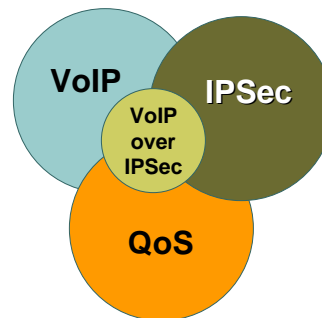
© 2002, Cisco Systems, Inc. All rights reserved.

34

## Design Guidelines

Cisco.com

- General Design Characteristics
- Voice over IP (VoIP)
- Quality of Service (QoS)
- **IP Security (IPSec)**
- Service Provider Considerations
- Solution Test Validation



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

35

## IKE and IPSec Assumptions

Cisco.com

- Strong (3DES) encryption for Internet Key Exchange (IKE) and IPSec
- IP GRE with IPSec Tunnel Mode
- Diffie-Hellman Group 2 (1024-bit) for IKE
- Secure Hash Algorithm (SHA)–HMAC
- Pre-shared keys
- Default lifetimes for IKE (24hr) and IPSec (1hr)

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

36

# Crypto IKE Configuration Sample

Cisco.com

```
!  
crypto isakmp policy 1  
  encr 3des  
  authentication pre-share  
  group 2  
crypto isakmp key bigsecret address 192.168.252.1  
crypto isakmp key bigsecret address 192.168.251.1  
!
```

Triple DES

Diffie-Hellman  
Group 2  
1024-bit

Pre-Shared  
Keys

Verify Using:  
show crypto isakmp policy

ISAKMP—Internet Security Association  
and Key Management Protocol

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

37

# Crypto IPsec Configuration Sample

Cisco.com

```
!  
crypto ipsec transform-set vpn-test c...  
!  
crypto map static-map local-address Serial0/0.1  
crypto map static-map 10 ipsec-isakmp  
  set peer 192.168.252.1  
  set transform-set vpn-test  
  match address vpn-static1  
  qos pre-classify  
crypto map static-map 20 ipsec-isakmp  
  set peer 192.168.251.1  
  set transform-set vpn-test  
  match address vpn-static2  
  qos pre-classify  
!
```

Encryption—Triple DES  
Authentication—SHA

Access-List Matches  
GRE Tunnel End-Points

Verify Using:  
show crypto map  
show crypto ipsec transform-set

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

38

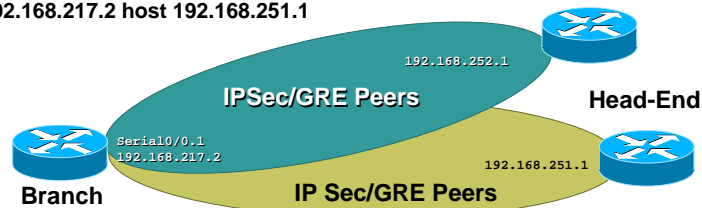
## Crypto Configurations Sample Branch Access-List

Cisco.com

```

!
interface Serial0/0.1 point-to-point
 ip address 192.168.217.2 255.255.255.252
!
ip access-list extended vpn-static1
 permit gre host 192.168.217.2 host 192.168.252.1
ip access-list extended vpn-static2
 permit gre host 192.168.217.2 host 192.168.251.1
!

```



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

39

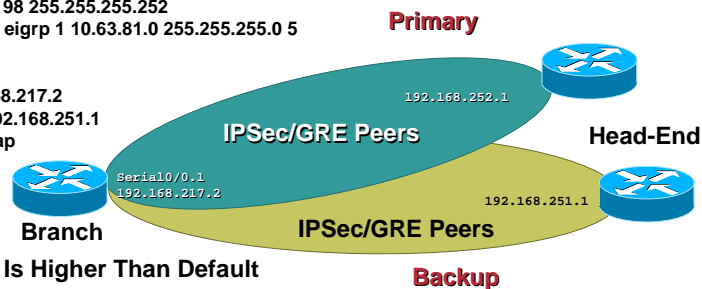
## Crypto Configuration Sample Branch GRE Tunnel Interfaces

Cisco.com

```

!
interface Tunnel0
 ip address 10.63.81.194 255.255.255.252
 ip summary-address eigrp 1 10.63.81.0 255.255.255.0 5
 qos pre-classify
 tunnel source 192.168.217.2
 tunnel destination 192.168.252.1
 crypto map static-map
!
interface Tunnel1
 ip address 10.63.81.198 255.255.255.252
 ip summary-address eigrp 1 10.63.81.0 255.255.255.0 5
 delay 60000
 qos pre-classify
 tunnel source 192.168.217.2
 tunnel destination 192.168.251.1
 crypto map static-map

```



WT-216  
5172\_05\_2002\_c1

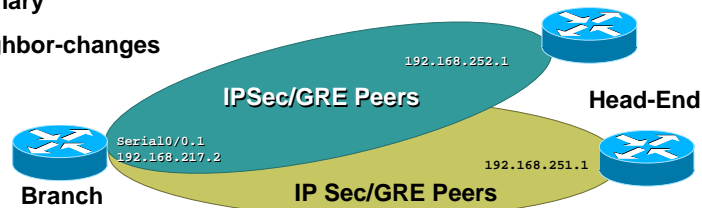
© 2002, Cisco Systems, Inc. All rights reserved.

40

## Crypto Configuration Sample Branch EIGRP

Cisco.com

```
!  
router eigrp 1  
  passive-interface Serial0/0.1  
  passive-interface Ethernet0/1  
  network 10.0.0.0  
  no auto-summary  
  eigrp log-neighbor-changes
```



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

41

## Anti-Replay Window

Cisco.com

- Designed to identify packet capture/replay by 3rd party—Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window
- Window marks packets as received or not
- Window moves to right to include higher sequence numbers
- Packets to the left of the window are dropped

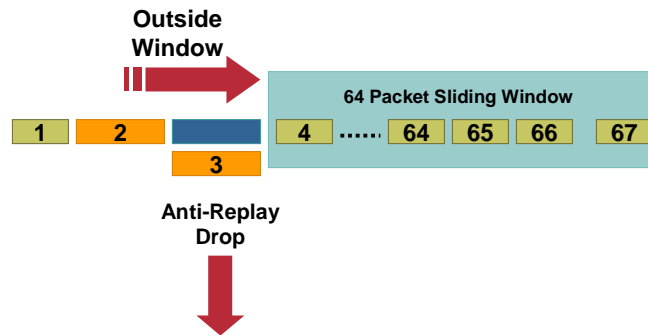
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

42

## Anti-Replay in Action

Cisco.com



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

43

## Anti-Replay Is Message Integrity

Cisco.com

```
crypto ipsec transform-set NOREPLAY esp-3des
crypto ipsec transform-set REPLAY esp-3des esp-sha-hmac
!
crypto map SKOOT 50 IPsec-isakmp
set peer 192.168.3.1
set transform-set REPLAY
match address 101
!
```

- **Message Integrity provided by ESP (Encapsulating Security Protocol) Authentication**
- **Defined in the IPsec *transform-set***
- **Either by SHA-1 or MD5 HMAC (Keyed-Hash Message Authorization Code)**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

44

## How to Identify Anti-Replay Drops

Cisco.com

Look at the **esp\_seq\_fail**  
**pkt\_replay\_err** counter

```
vpn18-2600-6#show crypto engine accelerator stat | include esp_seq_fail  
esp_prot_absent: 0 esp_seq_fail: 1775 esp_spi_failure: 0
```

```
vpn3-7200-2#show pas isa interface  
vpn3-7200-2#show pas vam interface
```

**Rate Limited  
Syslog Message on most  
platforms**

```
06:17:00: %HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet  
Encryption/Decryption error, status=4615
```

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

45

## Anti-Replay and QoS Interaction

Cisco.com

- **Voice packets (prioritized) not dropped, data (delayed) packets dropped**
- **Data packets transmitted, but dropped by receiving IPsec peer—wrong size of the link!**
- **Applications without flow control (UDP) drops persistent**
- **Networks with predominately TCP-based applications expect drop rate <1%**

WT-216  
5172\_05\_2002\_c1

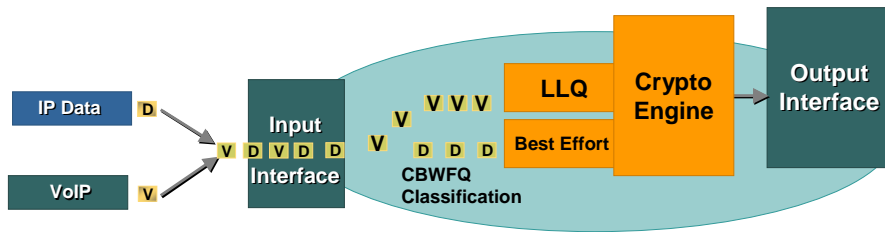
© 2002, Cisco Systems, Inc. All rights reserved.

46

# Crypto Engine QoS

Cisco.com

- Crypto engine is a half duplex internal interface
- Must process packets from multiple full duplex I/O interfaces
- Same input queue for encryption or decryption
- LLQ for crypto engine designed to minimize voice latency/jitter
- Enabled by presence of CBWFQ service policy
- Two queues—Low Latency Queue and best effort
- Not a pre-requisite to deploying Voice over IPsec today
- Applicable as CPU speed increases and/or high % of large packets



WT-216  
5172\_05\_2002\_c1

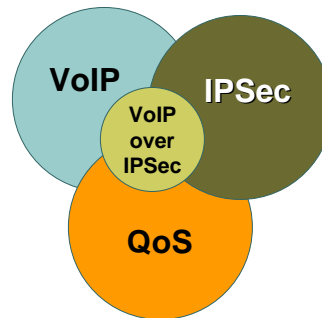
© 2002, Cisco Systems, Inc. All rights reserved.

47

# Design Guidelines

Cisco.com

- General Design Characteristics
- Voice over IP (VoIP)
- Quality of Service (QoS)
- IP Security (IPSec)
- **Service Provider Considerations**
- Solution Test Validation



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

48

## Roles and Responsibilities

Cisco.com

- **Enterprise**
  - SLA from the Service Provider?
  - Can the SP actually provide QoS across?
  - Contiguous or multiple Service Providers?
- **Service Provider**
  - QoS—on Service Provider edge and core
  - Bandwidth provisioning and SP boundary policing

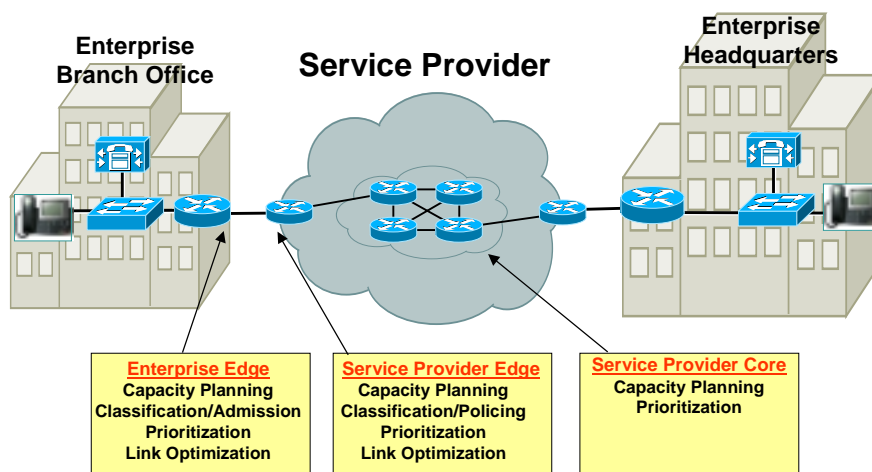
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

49

## Service Provider QoS Considerations

Cisco.com



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

50

# Service Provider Recommendations From Enterprise Edge to Edge

Cisco.com

- **Cisco Powered Network**  
Delivers end-to-end service level agreements to ensure voice/video quality  
[http://www.cisco.com/pcqi-bin/cpn/cpn\\_pub\\_bassrch.pl](http://www.cisco.com/pcqi-bin/cpn/cpn_pub_bassrch.pl)
- **Service Level Agreement**  
Packet Loss  $\leq$  .5%  
Delay  $\leq$  60ms One way Delay  
Jitter  $\leq$  20ms
- **Contiguous Cisco Powered Network SP Recommended**

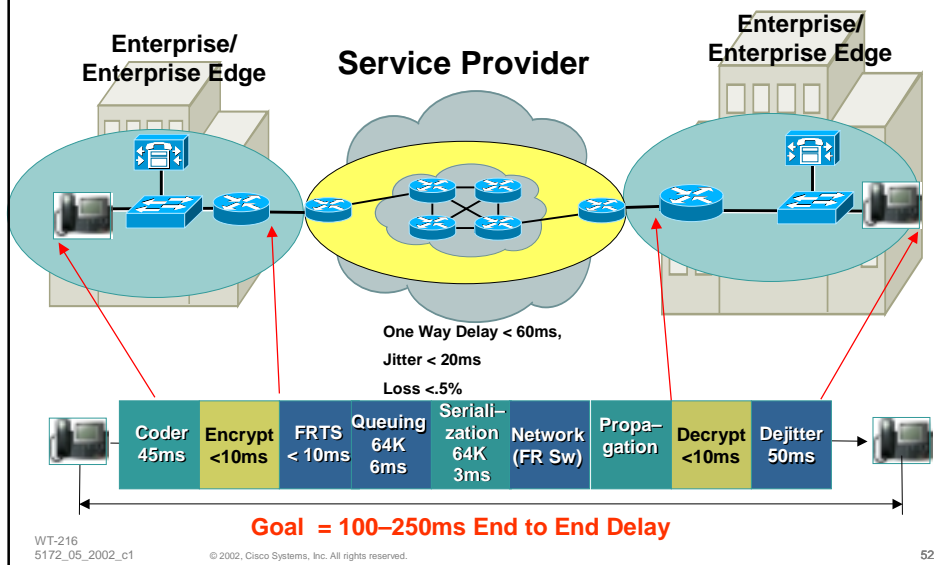
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

51

# Enterprise + Service Provider SLA Demarcations

Cisco.com



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

52

## Additional Things to Ask for From Service Providers

Cisco.com

### Service Provider Differentiation

- Handling of high priority traffic exceeding contracted rate?
- If multiple SP's involved – How is SLA achieved?
- Monitoring and Reporting on SLA statistics
- Availability of service and mean time to repair

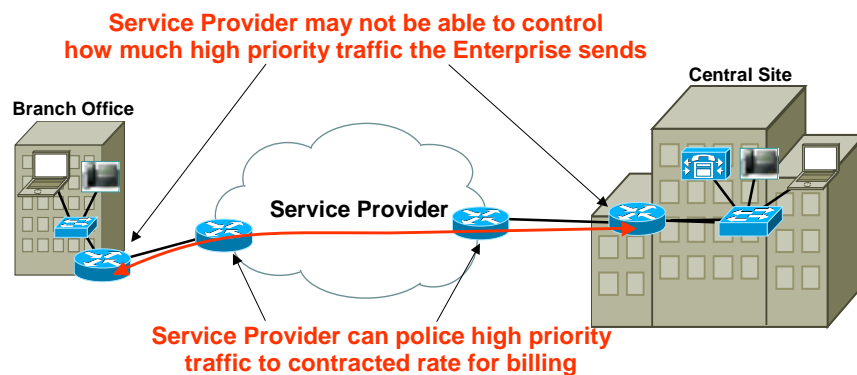
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

53

## Ent-SP Boundary Considerations *SP Policing high Priority BW from Enterprise*

Cisco.com



### Example

Enterprise Contracts for 5mbps high priority traffic  
SP Enforces to 5mbps - If exceeded charge extra or mark to lower priority

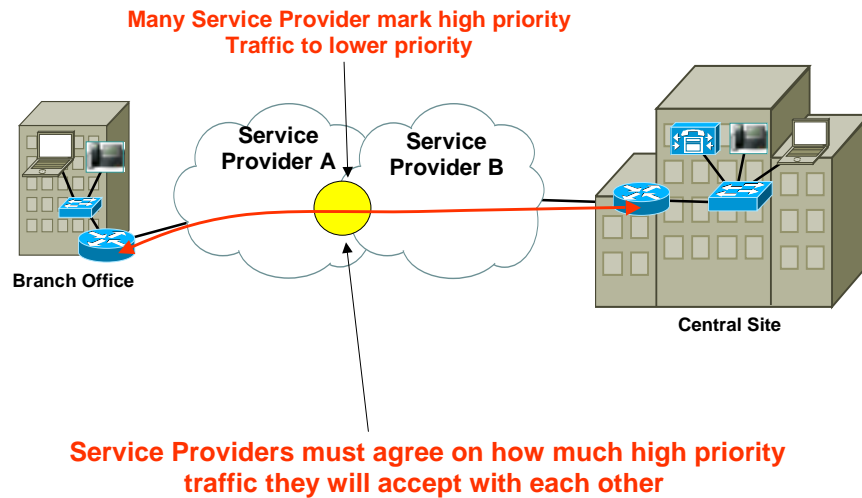
WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

54

## SP Considerations Cross Service Provider Boundaries

Cisco.com



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

55

## Enterprise SLA Requirements for Service Providers

Cisco.com

- **Bandwidth guarantee and provisioning**
- **Mirror customer's QoS at edge**
- **Delay guarantee**
  - 60ms one way between SP/Enterprise demarcation points
  - 150ms end to end (mouth to ear)
- **Jitter**
  - <20ms
- **Packet delivery  $\leq$  .5% packet loss**
- **Availability/Mean Time to Repair**
- **Notification of scheduled downtime/outages**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

56

## Cisco Powered Network

Cisco.com

- Cisco Powered Network on CCO  
<http://www.cisco.com/warp/public/779/servpro/cpn/>
- CPN multiservice description and requirements  
<http://www.cisco.com/warp/public/779/servpro/cpn/join/criteria.html>
- Search for a Cisco Powered Network Provider  
[http://www.cisco.com/pcqi-bin/cpn/cpn\\_pub\\_bassrch.pl](http://www.cisco.com/pcqi-bin/cpn/cpn_pub_bassrch.pl)

WT-216  
5172\_05\_2002\_c1

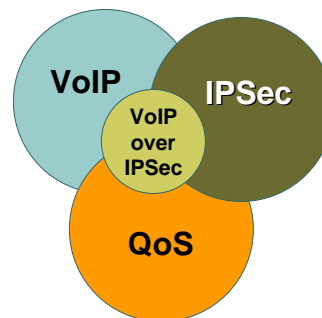
© 2002, Cisco Systems, Inc. All rights reserved.

57

## Design Guidelines

Cisco.com

- General Design Characteristics
- Voice over IP (VoIP)
- Quality of Service (QoS)
- IP Security (IPSec)
- Service Provider Considerations
- **Solution Test Validation**



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

58

## Voice over IPsec Solution Validation

Cisco.com

- Enterprise Solutions Engineering Test Lab
- Code Recommendation
- Scaling Considerations

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

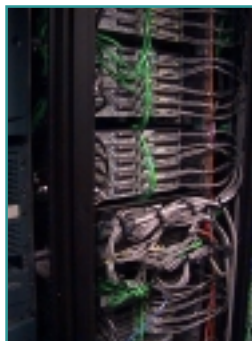
59

## Enterprise Solutions Engineering VPN Solution Testing Lab

Cisco.com

### Mission:

- Design, build, and test emerging technology solutions in a lab-simulated customer environment



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

60



# ESE VoIP Solution Test Chariot™ Traffic Profile

Cisco.com

## UDP

- RTP (VoIP G729) 33% of link (per call units, 50pps)
- DNS script—rate limited

## TCP

- HTTPtext script
- FTPGet and FTPPut script
- TN3270 script
- POP3 script

**HTTP and TN3270 Have Both IP  
Precedence 0 and 2 Traffic**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

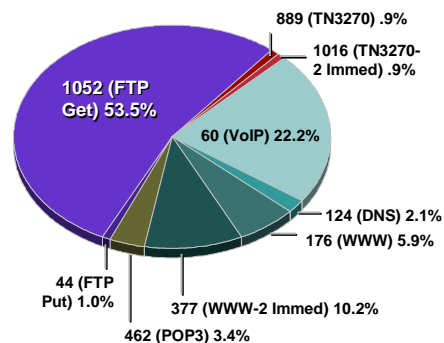
63

# ESE VoIP Solution Test Traffic Profile Excludes GRE and IPSec Headers/Trailers

Cisco.com

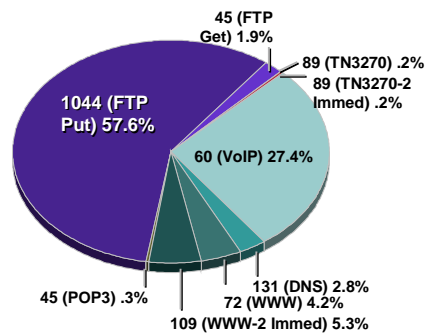
## Percent of Bytes with Average Packet Size

### Downstream



Average Packet Size = 188

### Upstream



Average Packet Size = 144

**NetFlow™ Protocol-Port-ToS Aggregation Exported and Summarized**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

64

## Code Recommendations

Cisco.com

Cisco Product Family	SW Release
Cisco 7200VXR VPN Routers	( 3DES IPsec Support) C7200-IK2S-M
Cisco 4200 Series VPN Routers	( 3DES IPsec Support) c4224-IK2O3SX3-M
Cisco 3600 Series VPN Routers	( 3DES IPsec Support) C3640-IK9O3S-M
Cisco 2600 Series VPN Routers	( 3DES IPsec Support) C2600-IK9O3S-M
Cisco 1700 Series VPN Routers	( 3DES IPsec Support) C1700-K9O3SY7-M
Cisco 800 Series VPN Routers	( 3DES IPsec Support) C806-K9OSY6-M

Please Refer to Account Team for Specific Release

<http://www.cisco.com/warp/customer/779/largeent/netpro/avid/srnd.html>

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

65

## Packet Fragmentation

Cisco.com

- Fragmenting router process switches to fragment
- Fragmentation done after encryption, before decryption
- End station re-assembles, could be decrypting router
- Process switching and huge buffer (18024 bytes) to re-assemble
- Use path MTU discovery, manually set MTU or look-ahead fragmentation

```
show ip traffic | include fragmented
```

```
530194 fragmented, 0 couldn't fragment
```

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

66

## IPSec Transport vs. Tunnel Mode

Cisco.com

- Transport mode an option when IPSec and GRE peers terminate on the same router
- Tunnel mode selected for Cisco solution lab testing to provide worst case performance numbers
- Look-ahead fragmentation—12.1(11)E
  - Feature implemented for IPSec Tunnel mode
  - GRE supported in IPSec Tunnel mode
  - Not implemented for IPSec Transport mode

WT-216  
5172\_05\_2002\_c1

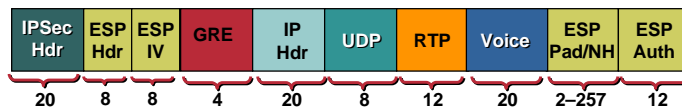
© 2002, Cisco Systems, Inc. All rights reserved.

67

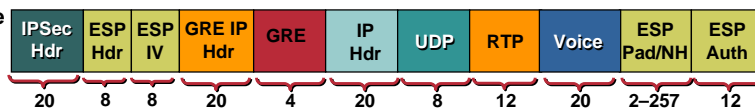
## Transport vs. Tunnel Size Delta for G.729 Packet

Cisco.com

IPSec ESP  
Transport Mode  
120 Bytes



IPSec ESP  
Tunnel Mode  
136 Bytes



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

68

## Solution Caveats—Testing Roadmap

Cisco.com

- Multilink PPP
- SRST—Survivable Remote Site Telephony
- Analog/digital voice modules installed in IPSec router
- IP compression with LZS algorithm
- OSPF
- IKE Keepalive/dead peer detection/reverse route injection
- LLQ for crypto engine
- Look-ahead fragmentation

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

69

## Agenda

Cisco.com

- Overview
- Planning Considerations
- Design Guidelines
- **Case Study**
- Summary

WT-216  
5172\_05\_2002\_c1

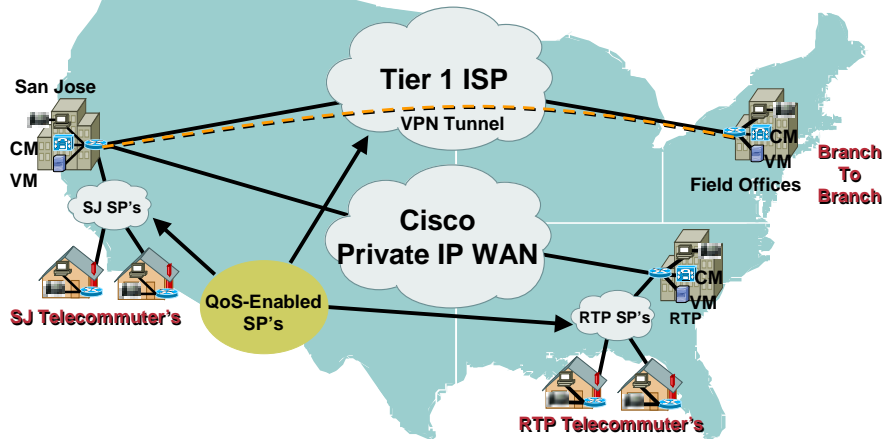
© 2002, Cisco Systems, Inc. All rights reserved.

70

# Cisco Internal VoIP VPN Deployment

Cisco.com

## Branch to Branch + Telecommuter



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

71

# Agenda

Cisco.com

- Overview
- Planning Considerations
- Design Guidelines
- Case Study
- **Summary**

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

72

## Summary

Cisco.com

- Design intersects three technologies

VoIP

QoS

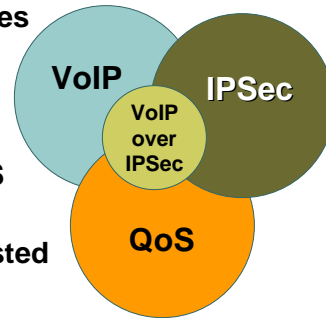
IPSec

- Possible today with Cisco VPN IOS routers
- Implementation must align with tested design guide

<http://www.cisco.com/warp/customer/779/largeent/netpro/avvid/srnd.html>

- Errata, updates and additional test results URL

<ftp://ftpeng.cisco.com/ftp/vvt216/voip-vpn.html>



WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

73

## Design Guidelines for Voice over IPSec VPN Deployments

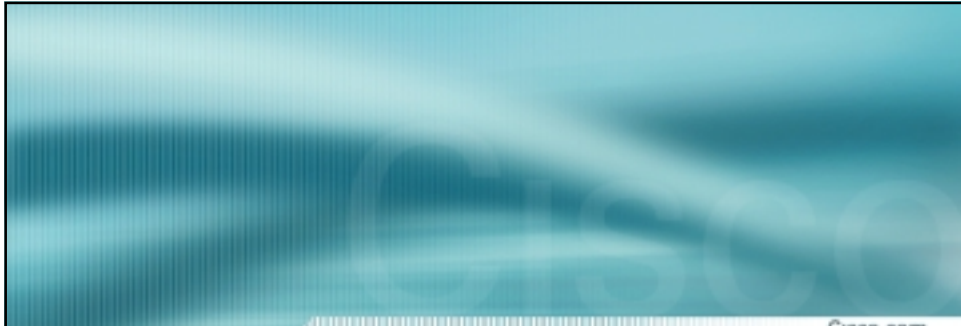
Session VVT-216

Cisco.com

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

74



Cisco.com

# Please Complete Your Evaluation Form

Session VVT-216

WT-216  
5172\_05\_2002\_c1

© 2002, Cisco Systems, Inc. All rights reserved.

75

# CISCO SYSTEMS



EMPOWERING THE  
INTERNET GENERATION

WT-216  
5172\_05\_2002\_c1

© 2001, Cisco Systems, Inc. All rights reserved.

76