APPENDIX B

# Configuration Supplement—Voice Module, EIGRP Stub, DSCP, HDLC

This appendix contains supplemental configurations used during a V$^3$PN performance and scalability evaluation. Specific configurations address the following devices and supporting networking functions:



## Voice Module Configuration

The full-scale solution test was designed to validate a site-to-site VoIP over IPSec solution where the voice bearer traffic would be received on the LAN interface rather than generated locally by the router from a voice network module.

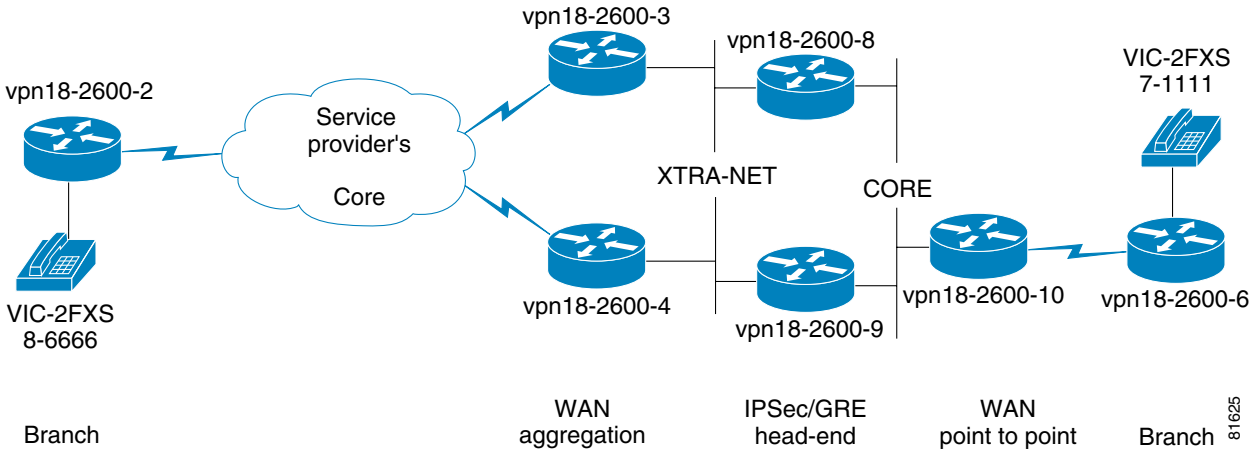
The purpose of this appendix is to create a single rack (small scale) configuration to supplement the main design guide to include the follow capabilities:

- IPSec *transport* mode configuration example
- EIGRP stub configuration
- Redundant configuration for dual WAN aggregation routers in addition to dual IPSec/GRE head-end routers
- Implement DSCP based *class-map*

HDLC sample configuration for a point-to-point WAN link

Figure B-1 illustrates an example network configuration.

*Figure B-1 Topology Diagram*




These configuration examples do not include *class-map*, *policy-map* or *ISAKMP policy* configurations unless they differ from the configurations illustrated previously in this design guide.

To simplify the topology drawing, the interface descriptions in the following router configurations include the keywords *XTRA-NET* and *CORE* or in the case of serial links, the router on the opposite end of the link is listed. The addressing scheme is configured such that the 192.168.x.0 subnets would represent routable addresses (Non-RFC 1918) and the 10.0.0.0 address space would be representative of where an enterprise might deploy that address space.

The third octet of the loopback 0 interface on the devices shown is the same as the last digit of the host name. For example, router *vpn18-2600-8* has the loopback address of 192.168.8.1.

It should be noted, that while IPSec transport mode decreases the WAN interface bandwidth requirements, it does not decrease the number of packets per second, which in most cases, is the limiting factor of a router's performance. The **priority** keyword of the voice class in the policy-map was not decreased from the value used in the design guide—bandwidth not used by the priority, or low-latency queue, is not wasted; it is available to the bandwidth classes.

In IPSec transport mode, a G.729 voice call uses 48,000 bps (Layer 3 – 120 bytes * 50 pps * 8 = 48,000) verses 54,400 bps (Layer 3 – 136 bytes * 50 pps * 8 = 54,400). With one voice call active between the two handsets and VAD disabled, the following is an example **show interface** display output:

```
vpn18-2600-6#show interface se 0/1 | include rate
  Queueing strategy: weighted fair
  30 second input rate 50000 bits/sec, 50 packets/sec
  30 second output rate 50000 bits/sec, 50 packets/sec
```

In these configuration examples, the alternate or backup path is not used unless the primary path is unavailable. Both the logical path (the GRE tunnel) and the physical path are similar. Router *vpn18-2600-3* and *vpn18-2600-8* are the primary logical and physical path and *vpn18-2600-4* and *vpn18-2600-9* are the backup logical and physical path.

With this addressing scheme, recursive routing is addressed by more specific static routes targeted to the interface, while a supernet, 192.168.0.0/16 is advertised via EIGRP through the tunnel interface. Also note the core routers do not have a route to 192.168.6.1, the IPSec/GRE address for *vpn18-2600-6*, this is not an oversight, rather an illustration data traffic can be encrypted from network end to end without reachability to IPSec/GRE endpoints.

In the case of routers *vpn18-2600-8* and *vpn18-2600-9*, no QoS is enabled on these IPSec/GRE endpoints, QoS is addressed by the WAN aggregation routers *vpn18-2600-3* and *vpn18-2600-4*, as well as the remote branch router *vpn18-2600-2*. However, in the case of *vpn18-2600-10* and *vpn18-2600-6*, IPSec/GRE and QoS are configured on the same router. Either configuration is valid, however, from a design standpoint, separating QoS from IPSec/GRE head-end routers should be considered a more scalable and manageable approach.

# Router Configuration—vpn18-2600-2

```
!
hostname vpn18-2600-2
!
boot system flash c2600-ik9s-mz.122-8.T
!
crypto isakmp key bigsecret address 192.168.8.1
crypto isakmp key bigsecret address 192.168.9.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
!
crypto map static-map local-address Loopback0
crypto map static-map 10 ipsec-isakmp
 set peer 192.168.8.1
 set transform-set vpn-test
 match address vpn-static1
crypto map static-map 20 ipsec-isakmp
 set peer 192.168.9.1
 set transform-set vpn-test
 match address vpn-static2
!
interface Loopback0
 ip address 192.168.2.1 255.255.255.252
!
interface Loopback1
 description Target address  for dial peer
 ip address 10.0.3.1 255.255.255.0
!
interface Tunnel0
 ip address 10.0.100.1 255.255.255.0
 ip summary-address eigrp 44 10.0.0.0 255.255.252.0 5
 qos pre-classify
 tunnel source Loopback0
 tunnel destination 192.168.8.1   # Primary IPSec/GRE peer vpn18-2600-8
 crypto map static-map
!
interface Tunnel1
 ip address 10.0.101.1 255.255.255.0
 ip summary-address eigrp 44 10.0.0.0 255.255.252.0 5
 delay 60000                     # Increasing the delay makes this the
!                                # backup peer
 qos pre-classify
 tunnel source Loopback0
 tunnel destination 192.168.9.1  # Backup IPSec/GRE peer vpn18-2600-9
 crypto map static-map
!
interface Serial0/0
 bandwidth 512
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
```

```
!
interface Serial0/0.100 point-to-point
 description Link to vpn18-2600-3
 bandwidth 512
 ip address 192.168.100.1 255.255.255.0
 frame-relay interface-dlci 100
  class ts-branch
 crypto map static-map
!
interface Serial0/0.101 point-to-point
 description Link to vpn18-2600-4
 bandwidth 512
 ip address 192.168.101.1 255.255.255.0
 frame-relay interface-dlci 101
  class ts-branch
 crypto map static-map
!
router eigrp 44
 network 10.0.0.0
 no auto-summary
 eigrp stub summary           # EIGRP stub configured
 eigrp log-neighbor-changes
!
! Two static routes to the head-end IPSec peers, 192.168.8.1 and
! 192.168.9.1 covered by the netmask of 255.255.254.0, the primary
! path to vpn18-2600-3 if available, otherwise use the second route
! with its higher administrative distance.
!
ip route 192.168.8.0 255.255.254.0 Serial0/0.100
ip route 192.168.8.0 255.255.254.0 Serial0/0.101 2
!
ip access-list extended vpn-static1
 permit gre host 192.168.2.1 host 192.168.8.1
ip access-list extended vpn-static2
 permit gre host 192.168.2.1 host 192.168.9.1
!
voice-port 1/0/0
 description 8-6666
!
dial-peer voice 10 voip
 destination-pattern 155467.....
 session target ipv4:10.251.0.1       # vpn18-2600-6
 ip qos dscp ef media
 ip qos dscp af31 signaling
 no vad
!
dial-peer voice 1 pots
 destination-pattern 15556786666
 port 1/0/0
!
end
```

# Router Configuration—vpn18-2600-3

```
!
hostname vpn18-2600-3
!
boot system flash c2600-ik9s-mz.122-8.T
!
interface Serial0/0
 description link to vpn18-2600-4
```

```
 bandwidth 2000
 ip address 192.168.99.3 255.255.255.0
 clockrate 2000000
!
interface FastEthernet0/1
 description XTRA-NET
 ip address 10.254.1.42 255.255.255.0
!
interface Serial0/1
 bandwidth 512
 no ip address
 encapsulation frame-relay
 frame-relay traffic-shaping
!
interface Serial0/1.100 point-to-point
 description Link to vpn18-2600-2
 bandwidth 512
 ip address 192.168.100.2 255.255.255.0
 frame-relay interface-dlci 100
  class ts-headend
!
router eigrp 44
 redistribute static
 passive-interface Serial0/1.100
 network 10.0.0.0
 network 192.168.99.0
 network 192.168.100.0
 default-metric 64000 20000 255 1 1500
 no auto-summary
 eigrp log-neighbor-changes
!
! Create a /16 route to be advertised to vpn18-2600-6
!
ip route 192.168.0.0 255.255.0.0 Null0
!
! Redistribute the primary path into EIGRP, so vpn18-2600-4 will learn
! an EIGRP external dynamically.
!
ip route 192.168.2.0 255.255.255.0 Serial0/1.100
!
end
```

# Router Configuration—vpn18-2600-4

```
!
hostname vpn18-2600-4
!
boot system flash c2600-ik9s-mz.122-8.T
!
interface Serial0/0
 description link to vpn18-2600-3
 bandwidth 2000
 ip address 192.168.99.4 255.255.255.0
!
interface FastEthernet0/1
 description XTRA-NET
 ip address 10.254.1.46 255.255.255.0
!
interface Serial0/1
 bandwidth 512
 no ip address
```

```
 encapsulation frame-relay
 frame-relay traffic-shaping
!
interface Serial0/1.101 point-to-point
 description link to vpn18-2600-2
 bandwidth 512
 ip address 192.168.101.2 255.255.255.0
 frame-relay interface-dlci 101
  class ts-headend
!
router eigrp 44
 redistribute static
 passive-interface Serial0/1.101
 network 10.0.0.0
 network 192.168.99.0
 network 192.168.101.0
 default-metric 64000 20000 255 1 1500
 no auto-summary
 eigrp log-neighbor-changes
!
!
! Create a /16 route to be advertised to vpn18-2600-6
!
ip route 192.168.0.0 255.255.0.0 Null0
!
! Due to admin distance of 240, this route will only be placed
! in the routing table if the EIGRP external (admin distance 170)
! from vpn18-2600-3 is withdrawn.
!
ip route 192.168.2.0 255.255.255.0 Serial0/1.101 240
!
end
```

# Router Configuration—vpn18-2600-8

```
!
hostname vpn18-2600-8
!
boot system flash c2600-ik9s-mz.122-8.T
crypto isakmp key bigsecret address 192.168.2.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
!
crypto map static-map local-address Loopback0
crypto map static-map 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set vpn-test
 match address vpn-static1
!
interface Loopback0
 ip address 192.168.8.1 255.255.255.0
!
interface Tunnel0
 ip address 10.0.100.2 255.255.255.0
 tunnel source Loopback0
 tunnel destination 192.168.2.1   # vpn18-2600-2
 crypto map static-map
!
interface FastEthernet0/1
 description CORE
```

```
 ip address 10.254.0.48 255.255.255.0
!
interface Ethernet1/0
 description XTRA-NET
 ip address 10.254.1.48 255.255.255.0
 crypto map static-map
!
router eigrp 44
 redistribute static
 network 10.0.0.0
 network 192.168.8.0
 default-metric 64000 20000 255 1 1500
 distribute-list 44 out Tunnel0
 no auto-summary
 eigrp log-neighbor-changes
!
! Create a /8 route to be advertised to the remote sites
!
ip route 10.0.0.0 255.0.0.0 Null0
!
ip access-list extended vpn-static1
 permit gre host 192.168.8.1 host 192.168.2.1
!
! Only need to send a /8 and /16 across the tunnel interface
!
access-list 44 permit 10.0.0.0
access-list 44 permit 192.168.0.0
access-list 44 deny any
!
end
```

# Router Configuration—vpn18-2600-9

```
!
hostname vpn18-2600-9
!
boot system flash c2600-ik9s-mz.122-8.T
!
crypto isakmp key bigsecret address 192.168.2.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
!
crypto map static-map local-address Loopback0
crypto map static-map 10 ipsec-isakmp
 set peer 192.168.2.1
 set transform-set vpn-test
 match address vpn-static1
!
interface Loopback0
 ip address 192.168.9.1 255.255.255.0
!
interface Tunnel1
 ip address 10.0.101.2 255.255.255.0
 delay 60000
 tunnel source Loopback0
 tunnel destination 192.168.2.1   # vpn18-2600-2
 crypto map static-map
!
interface FastEthernet0/1
 description CORE
```

```
 ip address 10.254.0.49 255.255.255.0
!
interface Ethernet1/0
 description XTRA-NET
 ip address 10.254.1.49 255.255.255.0
 crypto map static-map
!
router eigrp 44
 redistribute static
 network 10.0.0.0
 network 192.168.9.0
 default-metric 64000 20000 255 1 1500
 distribute-list 44 out Tunnel1
 no auto-summary
 eigrp log-neighbor-changes
!
! Create a /8 route to be advertised to the remote sites
!
ip route 10.0.0.0 255.0.0.0 Null0
!
ip access-list extended vpn-static1
 permit gre host 192.168.9.1 host 192.168.2.1
!
! Only need to send a /8 and /16 across the tunnel interface
!
access-list 44 permit 10.0.0.0
access-list 44 permit 192.168.0.0
access-list 44 deny any
!
end
```

# Router Configuration—vpn18-2600-10

```
!
hostname vpn18-2600-10
!
boot system flash c2600-ik9s-mz.122-8.T
!
! Example of matching on DSCP rather than IP Precedence
!
class-map match-all call-setup
  description AF31
  match ip dscp 26
class-map match-any mission-critical
  description cs2 and cs6
  match ip dscp 16
  match ip dscp 48
class-map match-all voice
  description EF
  match ip dscp 46
!
policy-map hdlc
  class voice
    priority 672
  class call-setup
   bandwidth percent 5
  class mission-critical
   bandwidth percent 22
  class class-default
   fair-queue
!
```

```
crypto isakmp key bigsecret address 192.168.6.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
!
crypto map HDLC local-address Loopback0
crypto map HDLC 10 ipsec-isakmp
 set peer 192.168.6.1
 set transform-set vpn-test
 match address hdlc-GRE
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
interface Tunnel1
 ip address 10.249.0.2 255.255.255.0
 tunnel source Loopback0
 tunnel destination 192.168.6.1    # vpn18-2600-6
 crypto map HDLC
!
interface Serial0/0
 description to vpn-2600-6 se0/1
 bandwidth 2000
 ip address 192.168.65.2 255.255.255.0
 service-policy output hdlc
 clockrate 2000000
 crypto map HDLC
!
interface FastEthernet0/1
 description CORE
 ip address 10.254.0.50 255.255.255.0
!
router eigrp 44
 passive-interface Serial0/0
 network 10.0.0.0
 network 192.168.10.0
 distribute-list 44 out Tunnel1
 no auto-summary
 eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
! Need to know how to reach the crypto peer vpn18-2600-6
!
ip route 192.168.6.0 255.255.255.0 Serial0/0
!
ip access-list extended hdlc-GRE
 permit gre host 192.168.10.1 host 192.168.6.1
!
! Only need to send a /8 and /16 across the tunnel interface
!
access-list 44 permit 10.0.0.0
access-list 44 permit 192.168.0.0
access-list 44 deny any
!
end
```

# Router Configuration—vpn18-2600-6

```
!
hostname vpn18-2600-6
!
boot system flash c2600-ik9s-mz.122-8.T
!
policy-map hdlc
  class voice
    priority 672
  class call-setup
   bandwidth percent 5
  class mission-critical
   bandwidth percent 22
  class class-default
   fair-queue
!
crypto isakmp key bigsecret address 192.168.10.1
!
crypto ipsec transform-set vpn-test esp-3des esp-sha-hmac
 mode transport
!
crypto map HDLC local-address Loopback0
crypto map HDLC 10 ipsec-isakmp
 set peer 192.168.10.1
 set transform-set vpn-test
 match address hdlc-GRE
!
interface Loopback0
 description target for IPSec
 ip address 192.168.6.1 255.255.255.0
!
interface Loopback1
 description target for VoIP dial-peers
 ip address 10.251.0.1 255.255.255.0
!
interface Tunnel1
 ip address 10.249.0.1 255.255.255.0
!
! Summarize up to the network core
!
 ip summary-address eigrp 44 10.248.0.0 255.248.0.0 5
 qos pre-classify
 tunnel source Loopback0
 tunnel destination 192.168.10.1    # vpn18-2600-10
 crypto map HDLC
!
interface Serial0/1
 description to vpn-2600-10 se0/0
 bandwidth 2000
 ip address 192.168.65.1 255.255.255.0
 service-policy output hdlc
 crypto map HDLC
!
router eigrp 44
 passive-interface Serial0/1
 network 10.0.0.0
 no auto-summary
 eigrp stub summary
 eigrp log-neighbor-changes
 no eigrp log-neighbor-warnings
!
! Need to know how to reach crypto peer vpn18-2600-10
```

```
!
ip route 192.168.10.0 255.255.255.0 Serial0/1
!
ip access-list extended hdlc-GRE
 permit gre host 192.168.6.1 host 192.168.10.1
voice-port 1/0/0
 description 7-1111
!
dial-peer voice 10 voip
 destination-pattern 155567.....
 session target ipv4:10.0.3.1
 ip qos dscp ef media
 ip qos dscp af31 signaling
 no vad
!
dial-peer voice 1 pots
 destination-pattern 15546771111
 port 1/0/0
!
end
```