

Avaya Solution & Interoperability Test Lab

Configuring Cisco Dynamic Multipoint VPN (DMVPN) to Support Avaya IP Telephony with QoS – Issue 1.0

Abstract

These Application Notes provide a sample configuration using Cisco Dynamic Multipoint VPN (DMVPN) to support Avaya IP Telephony. DMVPN combines the existing capabilities of multipoint Generic Routing Encapsulation (mGRE) tunnels, Next Hop Resolution Protocol (NHRP), and IPSec encryption to provide a Hub and Spoke VPN infrastructure.

The sample configuration utilizes the QoS Pre-Classify feature of Cisco IOS to enable Quality of Service to VPN traffic prior to encryption and encapsulation. The Dynamic Spoke-to-Spoke capability of DMVPN to offload branch to branch traffic from the Hub router is also implemented.

Interoperability between DMVPN and the flexible QoS capabilities of Avaya Communication Manager is demonstrated.

©2006 Avaya Inc. All Rights Reserved.

TABLE OF CONTENTS

1. INTRODUCTION 3

2. NETWORK TOPOLOGY 4

3. TERMS AND ACRONYMS 5

4. EQUIPMENT AND SOFTWARE VALIDATED 5

5. CONFIGURATIONS 6

5.1. DMVPN HUB ROUTER CONFIGURATION – CISCO 2811 6
5.2. DMVPN SPOKE ROUTER CONFIGURATION – CISCO 2811 9
5.3. QOS 11
5.3.1. Classification and Policy 12
5.3.2. VPN Pre-Classification 14
5.4. AVAYA COMMUNICATION MANAGER CONFIGURATION 15
5.5. AVAYA MEDIA GATEWAY CONFIGURATION 16

6. VERIFICATION AND TROUBLESHOOTING 16

6.1. DMVPN TUNNEL VERIFICATION 16
6.2. QOS VERIFICATION 19

7. CONCLUSION 21

8. REFERENCES 22

APPENDIX A: DMVPN HUB CONFIGURATION – CISCO 2811 23

APPENDIX B: DMVPN SPOKE 1 CONFIGURATION – CISCO 2811 25

APPENDIX C: DMVPN SPOKE 2 CONFIGURATION – CISCO 2811 27

APPENDIX D: DMVPN SPOKE 3 CONFIGURATION – CISCO 2811 29

©2006 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes provide a sample configuration using Cisco Dynamic Multipoint VPN (DMVPN) to support Avaya IP Telephony. DMVPN combines the existing capabilities of multipoint Generic Routing Encapsulation (mGRE) tunnels, Next Hop Resolution Protocol (NHRP), and IPSec encryption to provide a Hub and Spoke VPN infrastructure.

The sample configuration implements the DMVPN dynamic Spoke-to-Spoke capability enabling a partial mesh VPN, offloading the DMVPN Hub router for branch to branch traffic. Unlike a traditional IPSec VPN, DMVPN supports the transporting of broadcast traffic from dynamic routing protocols such as Open Shortest Path First (OSPF) and Cisco Exterior Interior Gateway Routing Protocol (EIGRP). OSPF was used in the sample configuration.

Quality of Service is enabled for DMVPN tunnel ingress traffic by utilizing the QoS for VPN feature of Cisco IOS. QoS for VPN enables classification of packets entering a VPN tunnel prior to encryption and encapsulation, also known as pre-classification. QoS for VPN is applied to the DMVPN tunnel interface of all Hub and Spoke routers to enable QoS throughout the enterprise.

These Application Notes present the following steps for establishing a DMVPN with QoS:

1. Establish a DMVPN tunnel between a Hub and Spoke router.
2. Apply QoS to the DMVPN.
3. Configure Avaya Communication Manager QoS.
4. Verify the DMVPN tunnel is operational and connectivity across the tunnel is successful.
5. Verify QoS classification and policy enforcement is functioning properly.

Note: These Application Notes describe a DMVPN single Hub configuration. A redundant dual Hub DMVPN configuration is recommended for production networks carrying high priority traffic such as voice.

©2006 Avaya Inc. All Rights Reserved.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The Main Site contains the DMVPN Hub router connected to an ISP edge router for WAN/Internet connectivity. The IP Telephony infrastructure at the Main Site consists of Avaya Communication Manager, G650 Media Gateways and Avaya IP telephones. The Branch locations have DMVPN Spoke routers connected to the WAN over T1 links. The IP Telephony components at the B ranch Sites consists of Avaya Media Gateways and Avaya IP Telephones. The DMVPN configuration steps for the Main Site Hub router and Branch 1 Spoke router are presented in **Section 5**. See the Appendices for Spoke 2 and Spoke 3 configurations. All Hub and Spoke routers participating in the same DMVPN must use the same IP subnet for their tunnel interfaces. IP subnet **172.16.1.0/24** is used in the sample network.

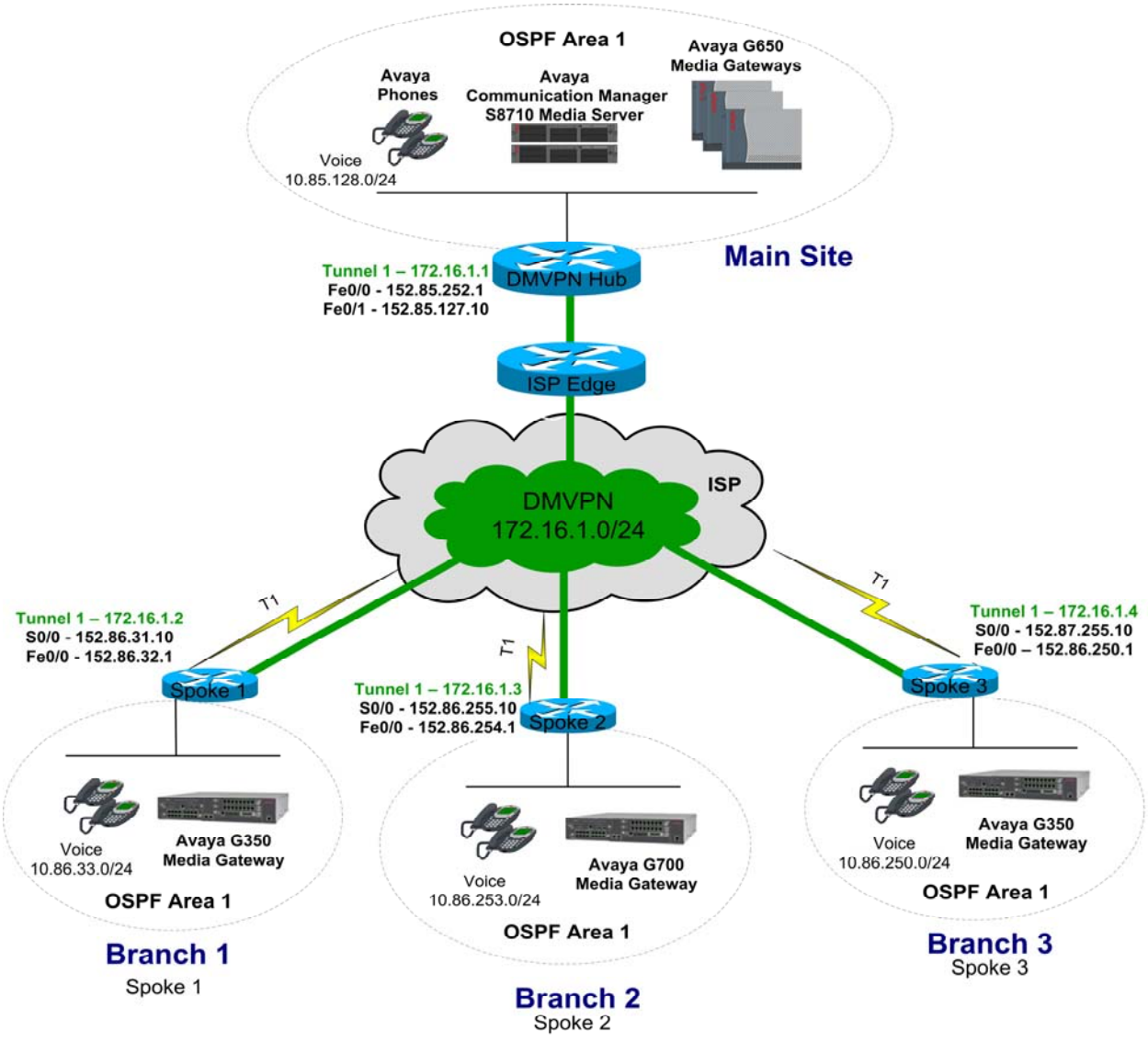


Figure 1: DMVPN Network Diagram

©2006 Avaya Inc. All Rights Reserved.

3. Terms and Acronyms

The following terms and acronyms are used throughout these Application Notes.

ACL	Access Control List
CLAN	Control LAN
DMVPN	Dynamic Multipoint Virtual Private Network
DSCP	Differentiated Services Code Point
GRE	Generic Route Encapsulation
IPSec	Internet Protocol Security
IPSI	IP Services Interface
ISAKMP	Internet Security Association and Key Management Protocol
MEDPRO	Media Processor
mGRE	Multipoint Generic Routing Encapsulation
NHRP	Next Hop Resolution Protocol
QoS	Quality of Service
RTP	Real-Time Transport Protocol
VPN	Virtual Private Network

4. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Component Description	Software/Hardware Version
Avaya S8710 Media Servers	Avaya Communication Manager R3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	 FW 022 (HW6) FW 016 (HW1) FW 108 (HW12)
Avaya G700 Media Gateway	23.17.0
Avaya G350 Media Gateway	25.28.0
Avaya IP Telephones	R2.3 (H.323)
Cisco 2811	IOS 12.4(9)T (C2800NM-ADVENTERPRISEK9-M)

Table 1 – Component Version Information

©2006 Avaya Inc. All Rights Reserved.

5. Configurations

5.1. DMVPN HUB Router Configuration – Cisco 2811

The following configuration steps will be presented in this section:

1. IPSec
2. Tunnel Interface
3. Outbound WAN Interface
4. Inbound LAN Interface
5. OSPF routing

See **Appendix A** for full Hub router configuration. Values specific to the sample network are highlighted in bold text. Other network environments may require different values.

1. IPSec

The sample configuration implements Pre-shared key authentication for hub-to-spoke tunnels as well as spoke-to-spoke tunnels. The following commands configure the IPSec encryption parameters of the mGRE tunnels.

Create an Internet Security Association and Key Management Protocol (ISAKMP) policy for Phase 1 negotiations using pre-shared key authentication.

```
crypto isakmp policy 5
 authentication pre-share
```

Add a dynamic pre-shared key.

```
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
```

Create a Phase 2 policy (transformer set) and specify the data encryption method to be used.

```
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode transport
```

Create an IPSec profile to be applied dynamically to the Hub-to-Spoke tunnels and specify which transform sets can be used with this IPSec profile.

```
crypto ipsec profile dmvpnprof
 set transform-set dmvpnset
```


©2006 Avaya Inc. All Rights Reserved.

2. Tunnel Interface

Create a tunnel interface and provide the appropriate options to match the network environment. **Table 2** provides a description of the tunnel interface options specific to the DMVPN configuration. See **Section 8** for Cisco documentation describing additional tunnel interface options.

```
interface Tunnel1
 description DMVPN Tunnel Interface to Branch Sites
 bandwidth 1000
 ip address 172.16.1.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip ospf network broadcast
 ip ospf priority 2
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpnprof
```

Tunnel Interface Command	Description
interface Tunnel1	Assigns a name and logical number to the tunnel interface.
bandwidth 1000	Logically defines the bandwidth value of the interface in kilobits per second to be used by higher-level protocols such as OSPF and EIGRP.
ip address 172.16.1.1 255.255.255.0	Set the IP address of the tunnel interface. **Note: All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.**
ip nhrp authentication dmvpn	Configures the authentication string for an interface using NHRP. **Note: The NHRP authentication string must be set to the same value on all hubs and spokes that are in the same DMVPN network.**
ip nhrp map multicast dynamic	Enables NHRP to automatically add spoke routers to the multicast NHRP mappings.
ip nhrp network-id 99	Enables NHRP on an interface and specifies a globally unique 32-bit network identifier. The range is from 1 to 4294967295. **Note: The NHRP network id must be set to the same value on all hubs and spokes that are in the same DMVPN network.**
ip nhrp holdtime 300	Sets the number of seconds that NHRP addresses are advertised as valid in authoritative NHRP responses. Valid values range from 300 seconds to 600 seconds.

©2006 Avaya Inc. All Rights Reserved.

Tunnel Interface Command	Description
ip ospf network broadcast	Enables the Spoke router's OSPF routing tables to contain routes to peer Spokes for Spoke-to-Spoke tunnels.
ip ospf priority 2	Sets the hub router as the OSPF Designated Router (DR) for the DMVPN network. Must be greater then 1 on the hub and 0 on the spokes.
tunnel source FastEthernet0/1	Sets the source interface the tunnel interface will use.
tunnel mode gre multipoint	Sets the encapsulation mode to multipoint GRE enabling dynamic spoke-to-spoke traffic.
tunnel protection ipsec profile dmvpnprof	Associates the tunnel interface with an IPSec profile. The IPSec profile name specified must match the *name* specified in the crypto ipsec profile from **Step 1** above.

Table 2 – DMVPN Tunnel Interface Commands

3. Outbound WAN Interface

The Hub router uses Fast Ethernet to interface with the ISP edge Router. The following commands configure the outbound physical interface.

```
interface FastEthernet0/1
 description To-WAN
 ip address 152.85.127.10 255.255.255.252
 duplex auto
 speed auto
```

4. Inbound LAN Interface

The Hub router uses Fast Ethernet to interface with the LAN. The following commands configure the inbound physical interface.

```
interface FastEthernet0/0
 description To-LAN
 ip address 152.85.252.1 255.255.255.252
 duplex auto
 speed auto
```


©2006 Avaya Inc. All Rights Reserved.

5. OSPF Routing

The DMVPN network, as well as any private network behind the hub router needing to be routable throughout the enterprise must be included in the OSPF configuration. The following commands configure the OSPF route entry.

```
router ospf 1
 log-adjacency-changes

!—- Specifies the Hub Site network to be routable across DMVPN
 network 152.85.252.0 0.0.0.3 area 0

!—- Specifies the DMVPN network to used across DMVPN Hubs and
!—- Spokes. See Step 2 above for Tunnel Interface IP address.
 network 172.16.1.0 0.0.0.255 area 0
```

5.2. DMVPN Spoke Router Configuration – Cisco 2811

The following configuration steps will be presented in this section:

1. IPSec
2. Tunnel Interface
3. Outbound WAN Interface
4. Inbound LAN Interface
5. OSPF routing

Values specific to the sample network are highlighted in bold text. Other network environments may require different values.

Because the DMVPN Spoke router configurations are very similar with only a few parameters differences per Spoke, only Spoke 1 parameters are shown in this section. **See Appendix B** for full Spoke 1 router configuration and **Appendix C and D** for Spoke 2 and Spoke 3 respectfully.

1. IPSec

The IPSec configuration on all Spoke routers is identical to the IPSec configuration of the Hub router shown in **Section 5.1 Step 1**. Copy the Hub router IPSec configuration and paste it into each Spoke router configuration.

©2006 Avaya Inc. All Rights Reserved.

2. Tunnel Interface

Create a tunnel interface and provide the appropriate options for the network environment. Only a few of the tunnel interface parameters on a Spoke configuration differ from the Hub configuration. These differences are highlighted below in bold text with descriptions of each. See **[1]** for Cisco documentation describing additional tunnel interface options.

```
interface Tunnel1
 description DMVPN Tunnel Interface to Branch Sites
 bandwidth 1000
!-- Sets the IP address of the tunnel interface. Note the network is the
same used by as the Hub tunnel interface.
 ip address 172.16.1.2 255.255.255.0
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
!-- Sets NHRP unicast and multicast mappings to the hub router.
 ip nhrp map 172.16.1.1 152.85.127.10
 ip nhrp map multicast 152.85.127.10
 ip nhrp network-id 99
 ip nhrp holdtime 300
!-- Sets the Hub as the Next Hop Server (NHS) for NHRP
 ip nhrp nhs 172.16.1.1
 ip ospf network broadcast
!-- Set OSPF priority to 0. Spoke routers cannot be allowed to become the
!-— Designated Router.
 ip ospf priority 0
!-- Sets the source interface the tunnel interface will use.
 tunnel source Serial0/0/0
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpnprof
```

3. Outbound WAN Interface

The sample configuration uses a Serial PPP interface for WAN connectivity. The following commands configure the outbound physical interface.

```
interface Serial0/0/0
 description To-WAN
 ip address 152.86.31.10 255.255.255.252
 encapsulation ppp
```

4. Inbound LAN Interface

The sample configuration uses Fast Ethernet to interface with the LAN. The following commands configure the inbound physical interface.

```
interface FastEthernet0/0
 description To-LAN
 ip address 152.86.32.1 255.255.255.252
 duplex auto
 speed auto
```


©2006 Avaya Inc. All Rights Reserved.

5. OSPF Routing

The DMVPN network, as well as any private network behind the Spoke 1 router needing to be routable throughout the enterprise must be included in the OSPF configuration. The following commands configure the OSPF route entry.

```
router ospf 1
 log-adjacency-changes

!—- Specifies the Spoke Site network to be routable across DMVPN
 network 152.86.32.0 0.0.0.3 area 0

!—- Specifies the DMVPN network to used across DMVPN Hubs and
!—- Spokes. See Step 2 above for Tunnel Interface IP address.
 network 172.16.1.0 0.0.0.255 area 0
```

5.3. QoS

The following configuration steps will be presented in this section:

1. QoS Classification
2. ACL Configuration
3. QoS Policy
4. Pre-Classification

©2006 Avaya Inc. All Rights Reserved.

5.3.1. Classification and Policy

With the DMVPN network operational and tunnel connectivity established between the Hub and at least one spoke router, QoS can be applied to DMVPN tunnel interfaces. The QoS classification implemented in the sample network of these Application Notes utilizes the Differentiated Services Code Point (DSCP) Layer 3 marking. As shown in **Table 3**, voice traffic is identified with a DSCP value of 46 and call signaling traffic (call control) with a DSCP value of 26. Avaya Communication Manager can set the DSCP values for Avaya IP Telephony components (e.g. Telephones, Media Gateways) to match the values defined in the network as described in **Section 5.4.**

In addition to matching on a DSCP value of 46, voice traffic must also match the classification rule for the sample configuration of being UDP traffic within the port range of 2048 to 3327 and coming from a network designated as a voice enabled network (Voice VLAN). This classification is enforced by an Access Control List (ACL) which is referenced by the Voice Class-map. The port range of 2048 to 3327 is defined in these Application Notes by Avaya Communication Manager as the port range to use for voice (RTP) traffic as described in **Section 5.4**

The QoS policy implemented in these Application Notes utilizes Class-Base Weighted Fair Queuing (CBWFQ) with strict priority queuing (low latency queue) for voice traffic as shown in **Table 4**.

Traffic Class	Class Name / Traffic Type	DSCP Value
1	Voice	46 (101110) Expedited Forwarding (EF)
2	Call Control	26 (011010) Assured Forwarding (af31)
3	Default (All other Data Traffic)	0

Table 3 – QoS Traffic Classes

Class Name	CBWFQ Policy
Voice	Strict Priority Queue 33% of available BW
Call Signaling	10% of available BW
Default (All other Data Traffic)	Fair Queue

Table 4 – QoS Policies

©2006 Avaya Inc. All Rights Reserved.

The following steps are to be applied to the Hub router and all Spoke routers.

1. **Classification Configuration – Hub and Spoke(s)**
   Create a QoS Class-map using the DSCP values defined in **Table 3**. In addition to the DSCP value, voice traffic is further characterized with an Access Control List (ACL).

```
class-map match-all call-control
 match ip dscp af31
class-map match-all voice
 match ip dscp ef
 match access-group 110
```

2. **ACL Configuration – Hub and Spoke(s)**
   Create an ACL referenced by the Class-map in **Step 1** above. Match the port range to be used by RTP voice packets as defined by Avaya Communication Manager in **Section 5.4**. Also specify any networks designated for carrying voice traffic.

```
access-list 110 remark Voice vlan RTP HUB -> any
access-list 110 permit udp 10.85.128.0 0.0.0.255 range 2048 3327 any
```

3. **Policy Configuration – Hub and Spokes(s)**
   Create a QoS Policy-map as defined in **Table 4.**

```
policy-map DMVPN
 class voice
  priority percent 33
 class call-control
  bandwidth percent 10
 class class-default
  fair-queue
```

   The policy-map must also be bound to an interface. The **`service-policy`** command can be applied to the outbound WAN interface used by the DMVPN tunnel. The **`service-policy`** command references the policy-map, the DMVPN policy-map in the example below, to be applied to the interface for outbound traffic. The Hub router interface is shown in the example below. The **`service-policy`** command should be applied to all spoke routers implementing QoS as well.

```
interface FastEthernet0/1
 description To-WAN
 ip address 152.85.127.10 255.255.255.252
 duplex auto
 speed auto
 service-policy output DMVPN
```


©2006 Avaya Inc. All Rights Reserved.

5.3.2. VPN Pre-Classification

The first step in a Quality of Service (QoS) process is to classify traffic. Based on this classification, the appropriate policy is applied. When packets are encapsulated by a VPN tunnel or encryption headers, the original packet headers are unable to be examined. This prevents packets from being properly classified and eliminating the ability to apply QoS. Packets traveling across the same tunnel have the same tunnel headers, so the packets are treated identically if the physical interface is congested.

By using the **`qos pre-classify`** IOS command, packets can be classified before tunneling and encryption occur. The process of classifying before tunneling and encryption allows routers to configure QoS features and tunneling on the same interface.

With the Class-map and Policy-map configured, the QoS pre-classification command can be applied to the DMVPN tunnel interface as shown below for the Hub router.

```
interface Tunnel1
 description DMVPN Tunnel Interface to Branch Sites
 bandwidth 1000
 ip address 172.16.1.1 255.255.255.0
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip ospf network broadcast
 ip ospf priority 2
 qos pre-classify
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel protection ipsec profile dmvpnprof
```


©2006 Avaya Inc. All Rights Reserved.

5.4. Avaya Communication Manager Configuration

A QoS policy must be established across the entire IP network, and the DSCP values used by Avaya Communication Manager and by the IP network infrastructure must be the same.

From the System Access Terminal (SAT) enter the **change ip-network-region** command with the appropriate region number specified to open an IP Network Region configuration screen. Set the QoS parameters and media port range to match the values used in **Section 5.3.1**. The Avaya IP telephony components will set these DSCP values and use these port ranges in IP packets sent to the network. The network elements will honor the DSCP values and apply the appropriate QoS policy. After completion of the configuration in this section, execute the **save translation** command to make the changes permanent.

- **UDP Port-Min** Specifies the lowest port number to be used for audio packets.
- **UDP Port-Max** Specifies the highest port number to be used for audio packets.
- **Call Control PHB Value** The Call Control Per-Hop Behavior DSCP decimal value.
- **Audio PHB Value** The VoIP Media Per-Hop Behavior DSCP decimal value.

```
change ip-network-region 1                                    Page   1 of
19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: sitl.com
    Name: DMVPN_HUB
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? n
   UDP Port Max: 3327
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 26      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2006 Avaya Inc. All Rights Reserved.

5.5. Avaya Media Gateway Configuration

The Avaya Media Gateways in theses Application Notes used the downloaded QoS parameters from the Avaya Communication Manager for local QoS treatment. The **show qos** media gateway command confirms the current media gateway QoS settings. All downloaded values should match the settings of the IP Network Region the media gateway is associated with on the Avaya Communication Manager.

```
G350-001(super)# show qos

PARAMETERS IN EFFECT: -- Downloaded --

QOS PARAMETERS          LOCALLY SET        DOWNLOADED
--------------------    ---------------    ---------------
Signal 802 Priority:    6                  6
Signal DSCP        :    26                 26
Bearer 802 Priority:    6                  6
Bearer BBE DSCP    :    46                 46
Bearer EF DSCP     :    46                 46
Minimum RTP Port   :    2048               2048
Maximum RTP Port   :    3327               3327
```

6. Verification

Use the steps in this section to confirm the DMVPN and QoS configurations are working properly.

6.1. DMVPN Tunnel Verification

The DMVPN tunnel between Hub and Spoke router(s) will be dynamically established.

The following verification steps will be presented in this section:

1. Hub - Spoke connectivity: Outside the tunnel
2. Hub - Spoke connectivity: Inside the tunnel
3. Hub Network – Spoke Network connectivity: Inside the tunnel (OSPF verification)
4. DMVPN status

1. Hub - Spoke connectivity: Outside the tunnel

While logged into the Hub router, ping the Spoke 1 router's physical WAN interface. This confirms WAN connectivity is good. If ping fails, DMVPN tunnels will not become established. Check the WAN configuration.

```
> ping 152.86.31.10
```


©2006 Avaya Inc. All Rights Reserved.

2. Hub - Spoke connectivity: Inside the tunnel

While logged into the Hub router, ping Spoke 1 router's tunnel interface. This confirms the DMVPN tunnel is up and connectivity between the Hub and Spoke tunnel interfaces are good. If ping fails, the DMVPN tunnel is not established. Check configuration settings at each site.

```
> ping 172.16.1.2
```

3. Hub Network – Spoke Network connectivity: Inside the tunnel (OSPF verification)

From a computer at the Main Site on the LAN behind the Hub router, ping an endpoint at Site 1 on the LAN behind the Spoke 1 router. An IP telephone endpoint was used for this test in the sample configuration. This confirms OSPF routing across the DMVPN is good. If ping fails, check OSPF routing tables at each site.

```
> ping 10.86.33.xxx
```

4. Show dmvpn

Execute the **show dmvpn** command from the IOS command line of any Hub or Spoke router. A status summary of all DMVPN links is displayed.

```
HUB-C2811#sh dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

Tunnel1, Type:Hub, NHRP Peers:3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1    152.86.31.10      172.16.1.2    UP    2d18h D
     1   152.86.255.10      172.16.1.3    UP    3d19h D
     1   152.87.255.10      172.16.1.4    UP    2d19h D
```


©2006 Avaya Inc. All Rights Reserved.

5. Show dmvpn detail

Execute the **show dmvpn detail** command from the IOS command line of any Hub or Spoke router. The detail of each DMVPN link is displayed.

```
HUB-C2811#sh dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer

 ------------- Interface Tunnel1 info: -------------
Intf. is up, Line Protocol is up, Addr. is 172.16.1.1
   Source addr: 152.85.127.10, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpnprof",
Tunnel VRF "", ip vrf forwarding ""

NHRP Details:
Type:Hub, NBMA Peers:3
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1    152.86.31.10      172.16.1.2    UP 00:00:31 D         172.16.1.2/32

  IKE SA: local 152.85.127.10/500 remote 152.86.31.10/500 Active
          Capabilities:(none) connid:1020 lifetime:23:54:34
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 152.85.127.10 host 152.86.31.10
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 73 drop 0 life (KB/Sec) 4553335/3568
        Outbound: #pkts enc'ed 64 drop 0 life (KB/Sec) 4553337/3568
   Outbound SPI : 0xFD914820, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1   152.86.255.10      172.16.1.3    UP    3d19h D         172.16.1.3/32

  IKE SA: local 152.85.127.10/500 remote 152.86.255.10/500 Active
          Capabilities:(none) connid:1017 lifetime:05:16:21
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 152.85.127.10 host 152.86.255.10
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 3353 drop 0 life (KB/Sec) 4447083/3397
        Outbound: #pkts enc'ed 3316 drop 7 life (KB/Sec) 4447069/3397
   Outbound SPI : 0x7D912657, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1   152.87.255.10      172.16.1.4    UP 00:04:11 D         172.16.1.4/32

  IKE SA: local 152.85.127.10/500 remote 152.87.255.10/500 Active
          Capabilities:(none) connid:1022 lifetime:23:56:06
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 152.85.127.10 host 152.87.255.10
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 205 drop 0 life (KB/Sec) 4531328/3366
        Outbound: #pkts enc'ed 207 drop 0 life (KB/Sec) 4531328/3366
   Outbound SPI : 0x1FC4A533, transform : esp-3des esp-sha-hmac
    Socket State: Open
```


©2006 Avaya Inc. All Rights Reserved.

6.2. QoS Verification

The following verification steps will be presented in this section:

1. QoS Preclassification
2. QoS Policy enforcement

1. To confirm the QoS pre-classification is being applied to the tunnel interface, execute the **show interfaces Tunnel 1** from the IOS command line of any DMVPN hub or spoke router. Note the Queuing strategy reported back should indicate QoS pre-classification is being applied as shown below.

```
HUB-C2811#sh interfaces Tunnel 1
Tunnel1 is up, line protocol is up
  Hardware is Tunnel
  Internet address is 172.16.1.1/24
  MTU 1514 bytes, BW 1544 Kbit, DLY 10000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 152.85.127.10 (GigabitEthernet1/0), destination UNKNOWN
  Tunnel protocol/transport multi-GRE/IP
    Key 0x186A0, sequencing disabled
    Checksumming of packets disabled

  Fast tunneling enabled
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Tunnel protection via IPSec (profile "dmvpnprof")
  Last input 00:00:02, output 00:00:02, output hang never
  Last clearing of "show interface" counters 2d18h
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 10
  Queueing strategy: fifo (QOS pre-classification)
  Output queue: 0/0 (size/max)
  5 minute input rate 11000 bits/sec, 16 packets/sec
  5 minute output rate 8000 bits/sec, 16 packets/sec
     4613783 packets input, 398299157 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     4596224 packets output, 325695099 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```


©2006 Avaya Inc. All Rights Reserved.

2. To confirm the QoS policies are being enforced, execute the **show policy-map interface** from the IOS command line of any DMVPN hub or spoke router. Note the Class map and Policy map settings from **Section 5.3**. In a properly tuned network, none of the Class map queues should report drops as shown below.

```
HUB-C2811#sh policy-map interface
 FastEthernet0/1

  Service-policy output: DMVPN

    Class-map: voice (match-all)
      108 packets, 29968 bytes
      5 minute offered rate 76000 bps, drop rate 0 bps
      Match: ip dscp ef (46)
      Match: access-group 110
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 33 (%)
        Bandwidth 3300 (kbps) Burst 82500 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0

    Class-map: call-control (match-all)
      72 packets, 9648 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: ip dscp af31 (26)
      Queueing
        Output Queue: Conversation 265
        Bandwidth 10 (%)
        Bandwidth 1000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      182 packets, 29416 bytes
      5 minute offered rate 5969000 bps, drop rate 31000 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 256
        (total queued/total drops/no-buffer drops) 0/0/0
```


©2006 Avaya Inc. All Rights Reserved.

3. The **show policy-map interface** output below shows voice and call-control class packets are being queued due to a high volume of competing data traffic on the Tunnel interface. The default queue is actively dropping data packets, while the voice and call-control queues maintain no drops. This output indicates the network is experiencing a problem. Although no voice packets are being dropped, the delay incurred by the increased queuing will eventually affect call quality.

```
HUB-C2811#sh policy-map interface
 FastEthernet0/1

  Service-policy output: DMVPN

    Class-map: voice (match-all)
      87734 packets, 24376356 bytes
      5 minute offered rate 55000 bps, drop rate 0 bps
      Match: ip dscp ef (46)
      Match: access-group 110
      Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 33 (%)
        Bandwidth 3300 (kbps) Burst 82500 (Bytes)
        (pkts matched/bytes matched) 6765/1879806
        (total drops/bytes drops) 0/0

    Class-map: call-control (match-all)
      65082 packets, 15602084 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: ip dscp af31 (26)
      Queueing
        Output Queue: Conversation 265
        Bandwidth 10 (%)
        Bandwidth 1000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 582/78644
        (depth/total drops/no-buffer drops) 0/0/0

    Class-map: class-default (match-any)
      204078 packets, 207700536 bytes
      5 minute offered rate 4128000 bps, drop rate 24000 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 256
        (total queued/total drops/no-buffer drops) 62/402/0
```

7. Conclusion

These Application Notes provide the steps to configure a Cisco Dynamic Multpoint VPN (DMVPN) with QoS pre-classification utilizing Layer 3 DiffServ markings. Interoperability between Avaya Communication Manager QoS capabilities and the DMVPN implementation was demonstrated.

©2006 Avaya Inc. All Rights Reserved.

8. References

[1] Cisco DMVPN site
http://www.cisco.com/go/dmvpn

[2] Avaya product documentation
http://avaya.support.com

[3] Additional Avaya Application Notes and Resources
http://avaya.com/gcm/master-usa/en-us/resource/

©2006 Avaya Inc. All Rights Reserved.

Appendix A: DMVPN Hub Configuration – Cisco 2811

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HUB-C2811
!
boot-start-marker
boot-end-marker
!
logging buffered 8192 debugging
!
no aaa new-model
!
resource policy
!
!
ip cef
!
!
no ip domain lookup
!
!
voice-card 0
 no dspfarm
!
!
class-map match-all call-control
 match ip dscp af31
class-map match-all voice
 match ip dscp ef
 match access-group 110
!
!
policy-map DMVPN
 class voice
  priority percent 33
 class call-control
  bandwidth percent 10
 class class-default
  fair-queue
!
!
crypto isakmp policy 5
 authentication pre-share
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile dmvpnprof
 set transform-set dmvpnset
```


©2006 Avaya Inc. All Rights Reserved.

```
!
!
interface Tunnel1
 bandwidth 1000
 ip address 172.16.1.1 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 ip ospf network broadcast
 ip ospf priority 2
 delay 1000
 qos pre-classify
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
interface FastEthernet0/0
 description To-LAN
 ip address 152.85.252.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description To-WAN
 ip address 152.85.127.10 255.255.255.252
 duplex auto
 speed auto
 service-policy output DMVPN
!
interface Serial0/0/0
 no ip address
!
interface GigabitEthernet1/0
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 network 152.85.252.0 0.0.0.3 area 0
 network 172.16.1.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 152.85.127.9
!
access-list 110 remark Voice vlan RTP HUB -> any
access-list 110 permit udp 10.85.128.0 0.0.0.255 range 2048 3327 any
!

control-plane
!
```


©2006 Avaya Inc. All Rights Reserved.

```
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
  login
!
!
end
```

Appendix B: DMVPN Spoke 1 Configuration – Cisco 2811

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke_01-C2811
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
resource policy
!
ip cef
!
no ip domain lookup
!
voice-card 0
 no dspfarm
!
class-map match-all call-control
 match ip dscp af31
class-map match-all voice
 match ip dscp ef
 match access-group 110
!
!
policy-map DMVPN
 class voice
  priority percent 33
 class call-control
  bandwidth percent 10
 class class-default
  fair-queue
!
!
!
```


©2006 Avaya Inc. All Rights Reserved.

```
crypto isakmp policy 5
 authentication pre-share
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile dmvpnprof
 set transform-set dmvpnset
!
!
!
interface Tunnel1
 bandwidth 1000
 ip address 172.16.1.2 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map 172.16.1.1 152.85.127.10
 ip nhrp map multicast 152.85.127.10
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 172.16.1.1
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 ip ospf network broadcast
 ip ospf priority 0
 delay 200
 qos pre-classify
 tunnel source Serial0/0/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
interface FastEthernet0/0
 description To LAN
 ip address 152.86.32.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 152.86.31.10 255.255.255.252
 encapsulation ppp
 service-policy output DMVPN
!
router ospf 1
 log-adjacency-changes
```


©2006 Avaya Inc. All Rights Reserved.

```
 network 152.86.32.0 0.0.0.3 area 0
 network 172.16.1.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 152.86.31.9
!
!
access-list 110 remark Voice vlan RTP Spoke1 -> any
access-list 110 permit udp 10.86.33.0 0.0.0.255 range 2048 3327 any
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
  login
!
!
end
```

Appendix C: DMVPN Spoke 2 Configuration – Cisco 2811

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke_02-C2811
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
resource policy
!
ip cef
!
no ip domain lookup
!
voice-card 0
 no dspfarm
!
class-map match-all call-control
 match ip dscp af31
class-map match-all voice
 match ip dscp ef
 match access-group 110
!
```


©2006 Avaya Inc. All Rights Reserved.

```
!
policy-map DMVPN
 class voice
  priority percent 33
 class call-control
  bandwidth percent 10
 class class-default
  fair-queue
!
!
!
crypto isakmp policy 5
 authentication pre-share
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile dmvpnprof
 set transform-set dmvpnset
!
!
!
interface Tunnel1
 bandwidth 1000
 ip address 172.16.1.3 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map 172.16.1.1 152.85.127.10
 ip nhrp map multicast 152.85.127.10
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 172.16.1.1
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 ip ospf network broadcast
 ip ospf priority 0
 delay 200
 qos pre-classify
 tunnel source Serial0/1/0
 tunnel mode gre multipoint
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
interface FastEthernet0/0
 description To LAN
 ip address 152.86.254.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
```


©2006 Avaya Inc. All Rights Reserved.

```
 shutdown
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 152.86.255.10 255.255.255.252
 encapsulation ppp
 service-module t1 timeslots 1-24
 service-policy output DMVPN
!
router ospf 1
 log-adjacency-changes
 network 152.86.254.0 0.0.0.3 area 0
 network 172.16.1.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 152.86.255.9
!
!
access-list 110 remark Voice vlan RTP Spoke2 -> any
access-list 110 permit udp 10.86.253.0 0.0.0.255 range 2048 3327 any
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
  login
!
!
end
```

Appendix D: DMVPN Spoke 3 Configuration – Cisco 2811

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Spoke_03-C2811
!
boot-start-marker
boot-end-marker
!
logging buffered 51200 warnings
!
no aaa new-model
!
resource policy
!
ip cef
!
```


©2006 Avaya Inc. All Rights Reserved.

```
no ip domain lookup
!
voice-card 0
 no dspfarm
!
class-map match-all call-control
 match ip dscp af31
class-map match-all voice
 match ip dscp ef
 match access-group 110
!
!
policy-map DMVPN
 class voice
  priority percent 33
 class call-control
  bandwidth percent 10
 class class-default
  fair-queue
!
!
!
crypto isakmp policy 5
 authentication pre-share
crypto isakmp key dmvpnkey address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set dmvpnset esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile dmvpnprof
 set transform-set dmvpnset
!
!
!
interface Tunnel1
 bandwidth 1000
 ip address 172.16.1.4 255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp authentication dmvpn
 ip nhrp map multicast dynamic
 ip nhrp map 172.16.1.1 152.85.127.10
 ip nhrp map multicast 152.85.127.10
 ip nhrp network-id 99
 ip nhrp holdtime 300
 ip nhrp nhs 172.16.1.1
 no ip route-cache cef
 no ip route-cache
 no ip mroute-cache
 ip ospf network broadcast
 ip ospf priority 0
 delay 200
 qos pre-classify
 tunnel source Serial0/0/0
 tunnel mode gre multipoint
```


©2006 Avaya Inc. All Rights Reserved.

```
 tunnel key 100000
 tunnel protection ipsec profile dmvpnprof
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0
 description To LAN
 ip address 152.86.250.1 255.255.255. 252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 152.87.255.10 255.255.255.252
 encapsulation ppp
 service-module t1 timeslots 1-24
 service-policy output DMVPN
!
router ospf 1
 log-adjacency-changes
 no auto-cost
 network 152.86.250.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
!
ip route 0.0.0.0 0.0.0.0 152.87.255.9
!
!
access-list 110 remark Voice vlan RTP Spoke3 -> any
access-list 110 permit udp 10.86.250.0 0.0.0.255 range 2048 3327 any
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
  login
!
!
end
```


©2006 Avaya Inc. All Rights Reserved.

©2006 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com

©2006 Avaya Inc. All Rights Reserved.