



## CHAPTER 8

# Small Branch—Dual Hub/Dual DMVPN

---

This chapter describes the migration of a single Dynamic Multipoint Virtual Private Network (DMVPN) configuration, which is a router with a single DMVPN configuration connected to one DMVPN hub, with one configured generic routing encapsulation (GRE) tunnel, to a dual DMVPN configuration supporting VoIP.

**Note**

---

This is a hub-and-spoke deployment; spoke-to-spoke was not tested or recommended for VoIP.

---

The dual hub/dual DMVPN design provides head-end redundancy by configuring two DMVPN clouds on a remote router, with each cloud having a separate IPsec head-end router.

This chapter describes the changes that result from adding VoIP to configuration examples that initially support only data.

**Note**

---

IP telephony is supported only on a best effort basis, so the configurations that include VoIP are not complete.

---

This chapter includes the following sections:

- [Solution Characteristics](#)
- [Topology](#)
- [Failover/Recovery Time](#)
- [V3PN QoS Service Policy](#)
- [Performance Testing](#)
- [Test Topology](#)
- [Implementation and Configuration](#)
- [Cisco IOS Versions Tested](#)
- [Summary](#)

## Solution Characteristics

This design solution applies in situations where customers require VoIP, and IP multicast applications are supported. The final configuration represents a dual hub and dual DMVPN clouds supporting a VoIP deployment.

This deployment scenario is applicable to teleworkers or small branch offices that have the following connectivity characteristics:

- Low recurring costs for WAN access
- IP multicast requirements
- VoIP support
- Redundant IPSec/GRE termination at the campus head-end

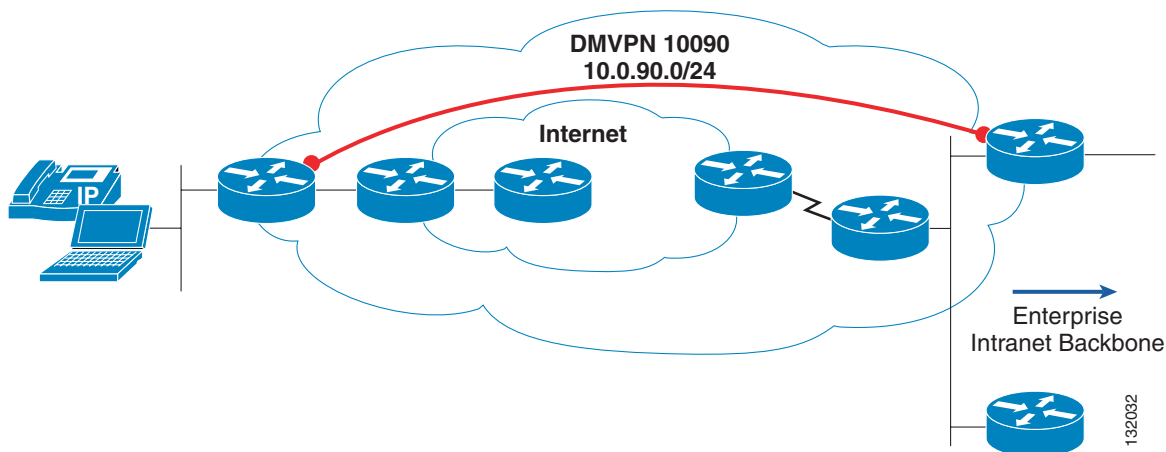
Test results are presented to describe voice quality with and without the recommended changes implemented to enhance the initial configuration of the customer.

This chapter also describes a case study in which the initial customer configuration is tested to validate support for VoIP.

## Topology

The initial customer configuration consists of a single DMVPN cloud with a single campus head-end router providing connectivity for the population of teleworkers. This topology is shown in [Figure 8-1](#).

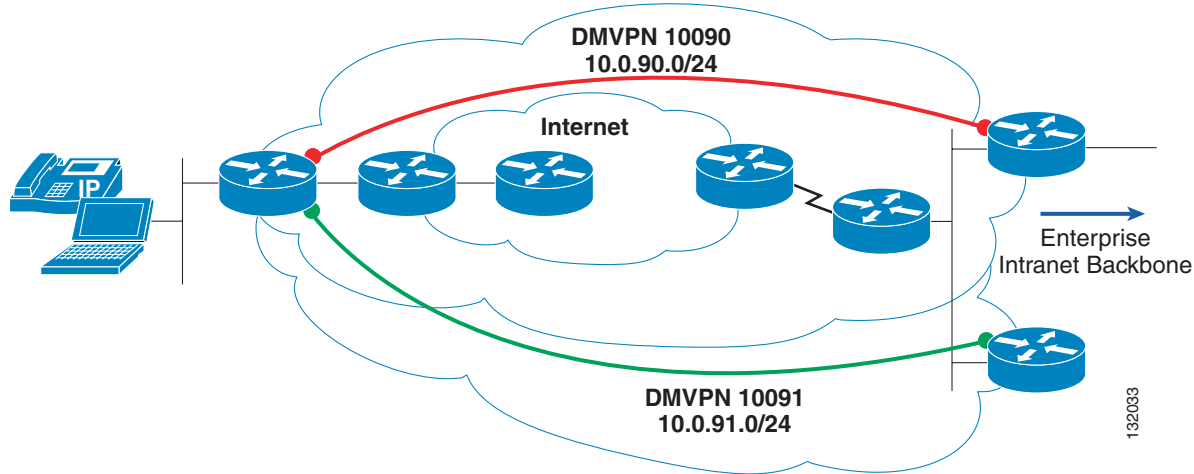
**Figure 8-1** *Single Hub—Single DMVPN*



Because the customer configuration must now support VoIP, a second DMVPN cloud is needed to increase availability for the remote locations. The dual hub/dual DMVPN cloud design is selected over a dual hub/single DMVPN cloud because the topology provides more control of the packet routing between the two head-end peers.

The recommended topology is shown in [Figure 8-2](#):

Figure 8-2 Dual Hub/Dual DMVPN



The dual hub/dual DMVPN topology has the advantage of providing two tunnel interfaces in the remote branch (teleworker) routers. Because the remote routers, or spokes, have a routing protocol neighbor relationship on two separate interfaces, the two paths can be influenced by interface specific values. Depending on the routing protocol in use, you can implement cost, bandwidth, delay, metric offset, or summary advertisements on the individual tunnel interfaces to influence which head-end router is the preferred path. From a manual load sharing perspective, half the population of spoke routers can use DMVPN cloud 10090 as their preferred path with cloud 10091 as the backup. The other half of the spokes can use cloud 10091 as the preferred path and cloud 10090 as backup.

With a distance vector routing protocol such as EIGRP, it is very easy to add a third DMVPN cloud, and to divide the population of spoke routers so that one third prefers the first cloud, one third prefers the second, and the final one third prefers the last cloud. The backup cloud for the spoke is spread across the other clouds and their respective head-end routers.

## Failover/Recovery Time

When EIGRP is the routing protocol on the mGRE tunnels, detection of a head-end or path failure by the remote router is based on the configured routing protocol dead interval (interface configuration command `ip hold-time eigrp ...`), which by default is 15 seconds. Other protocols, such as RIP, OSPF, and so on, have their own default values and can be configured by the network manager.

One currently-known issue with dual hub/dual DMVPN cloud configurations is that the second Internet Key Exchange (IKE) security association (SA) may be deleted. If the peer associated with the UP-NO-IKE status is reloaded, connectivity is not restored until the IPsec SAs age out, because there is no IKE SA to send keepalive/dead peer detection (DPD) messages.

As a result of this, the second IKE SA must re-key each time the IPsec SA expires. By default, the IKE lifetime is 24 hours and the IPsec lifetime is one hour. From a head-end performance standpoint (CPU consumption), that means 24 times more IKE processing than necessary. This defect is identified as CSCed18278-IKE SSA deleted in dual hub, dual DMVPN cloud configuration.

# V3PN QoS Service Policy

This section includes the following topics:

- [DMVPN \(GRE Transport Mode\) ESP 3DES/SHA](#)
- [DMVPN \(GRE Transport Mode\) ESP 3DES/SHA with NAT-T](#)
- [Sample V3PN Relevant QoS Configuration](#)

In various V3PN design guides, QoS service policies are defined to allocate bandwidth based on IPsec-protected GRE and direct IPsec encapsulation respectively.



## Note

For more information, see the V3PN design guide at the following URL:

[http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN\\_and\\_MAN/V3PN\\_SRND/V3PN\\_SRND.html](http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/V3PN_SRND/V3PN_SRND.html).

IPsec-protected GRE tunnels are commonly deployed for site-to-site communications, and direct IPsec encapsulation is well-suited for teleworkers.



## Note

IPsec encapsulation is also known as an IPsec-only deployment (no GRE). Teleworker deployments generally do not need multicast or multiprotocol support and thus do not reap any benefit from GRE encapsulation and its additional overhead.

DMVPN has been heavily marketed to customers, and it is one option for deployments that require IP multicast applications to the teleworker desktop (DMVPN does not support multiprotocol but only IP multicast). Examples of these deployments include video surveillance applications using IP multicast and financial brokerage house applications that are implemented using IP multicast.

In a small office small home (SOHO) deployment, it is common to see the VPN router deployed behind a personal firewall such as a Linksys BEFSR41 EtherFast® Cable/DSL Router. This architecture is deployed at the residence of the teleworker because it allows the teleworker to control the username and password of the PPP over Ethernet (PPPoE) session, simplifies configuration of the enterprise-managed VPN router, and provides a “spouse and child” network over the common broadband connection.

The deployment scenario assumes the following:

- The topology may include a Network Address Translation (NAT)/Port Network Address Translation (pNAT) personal firewall device.
- Both cable and DSL broadband are supported.
- PPPoE is typical on the DSL deployments, and Data Over Cable Service Interface Specifications (DOCSIS) 1.0 is typical for cable.
- The uplink data rates are at or below 768 kbps and as such, voice packets are subject to serialization delay.

Because of these factors, the configuration is optimized for the worst case scenario, which is DSL using PPPoE at an uplink data rate below 768 kbps. The **ip tcp adjust-mss** command is used to minimize the lack of Layer 2 link fragmentation and interleaving.

The goal is to select an optimum value for **ip tcp adjust-mss** that minimizes both the IPsec padding and ATM adaption layer (AAL) 5 padding. The diagrams in the following section show the individual field lengths and their relationship to the underlying ATM cells on a DSL deployment.

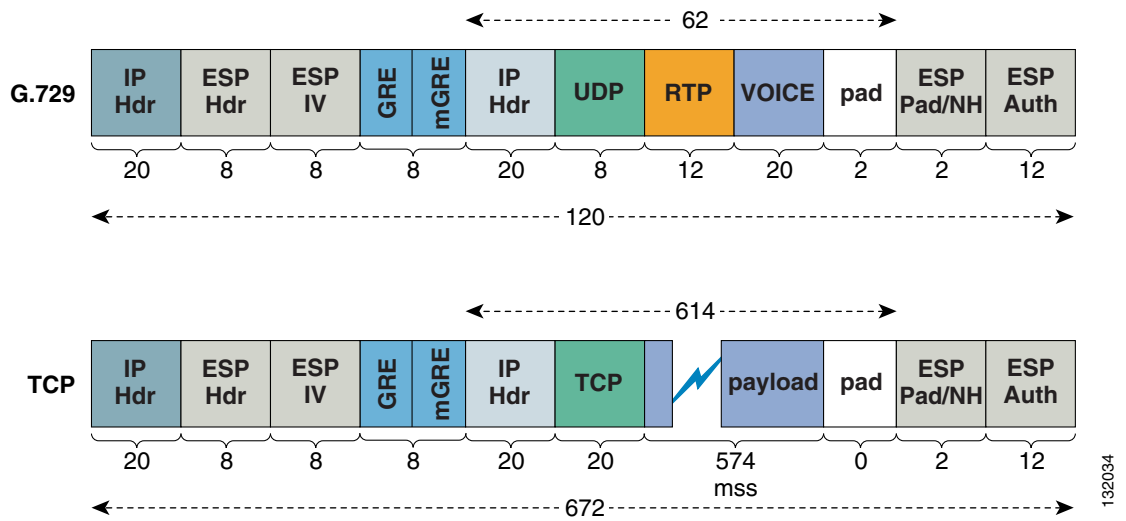
## DMVPN (GRE Transport Mode) ESP 3DES/SHA

The following configuration uses a transform set that includes Triple Data Encryption Standard (3DES), Secure Hash Algorithm (SHA), and transport mode for multipoint GRE (mGRE):

```
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
 mode transport
crypto ipsec profile ECT_PROFILE_1
...
 set transform-set TRANSPORT_3DES_SHA
!
interface Tunnel0
 description DMVPN
...
 tunnel mode gre multipoint
...
 tunnel protection ipsec profile ECT_PROFILE_1 shared
```

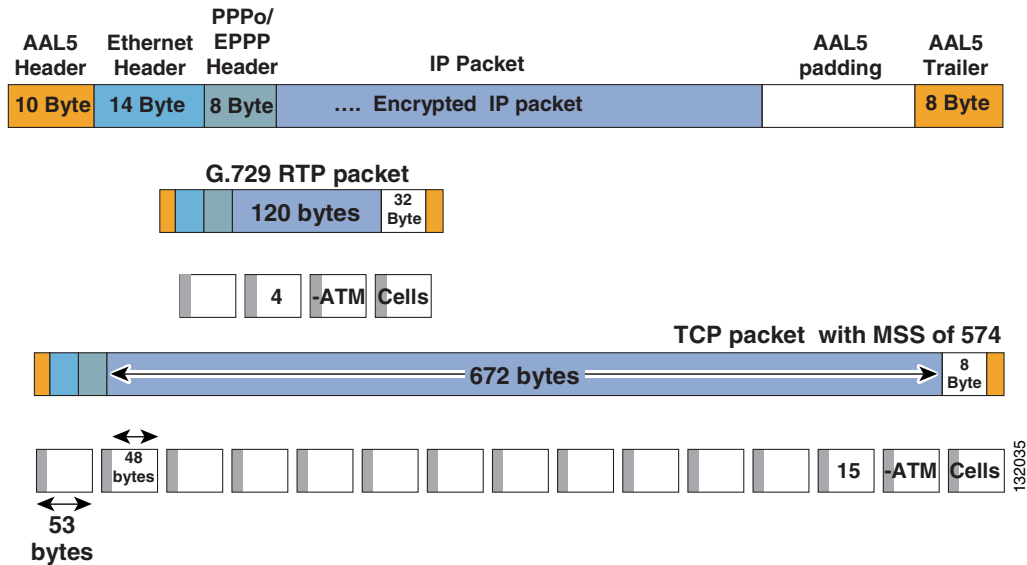
The encrypted mGRE encapsulated packets for both G.729 and a TCP packet are shown in Figure 8-3.

**Figure 8-3 Packet Decode—G.729 and TCP**



This encrypted IP packet, when encapsulated in PPPoE/AAL5/ATM cells for a DSL deployment, is shown in Figure 8-4.

Figure 8-4 DSL/PPPoE Encapsulation



The result is that a G.729 packet requires four ATM cells, and a TCP packet with a maximum segment size (MSS) of 574 requires 15 ATM cells. There are 8 bytes of AAL5 padding in the last cell. This configuration does not assume Network Address Translation Traversal (NAT-T), but rather the IP header is Extended Services Platform (ESP), protocol “50”. NAT-T is optimized so that when no NAT device is detected between the IPsec peers, UDP encapsulation is not used to avoid the additional overhead of the additional UDP header. This configuration shows IKE packets on UDP port 500 and ESP (protocol 50) for the IPsec tunnel.

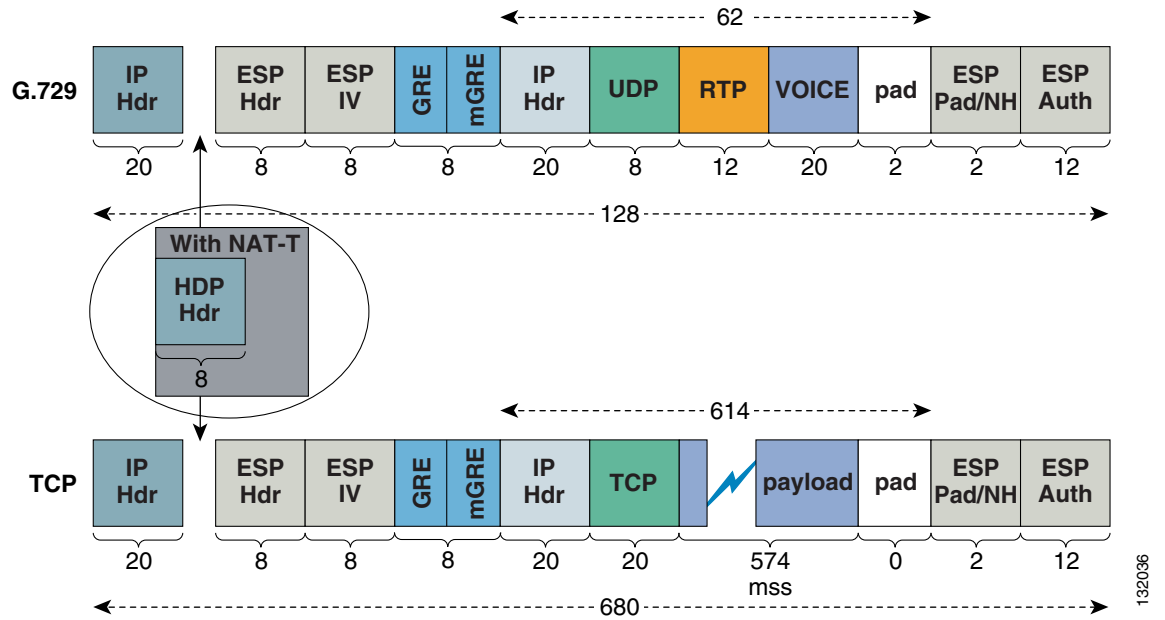
## DMVPN (GRE Transport Mode) ESP 3DES/SHA with NAT-T

Based on a configuration using a transform set that includes 3DES, SHA, and transport mode for mGRE using the same configuration from the previous section, assume that a NAT/pNAT device is in the path between the IPsec peers and NAT-T is enabled.

```
crypto ipsec nat-transparency udp-encapsulation
```

The above Cisco IOS configuration command is enabled by default. The encrypted mGRE encapsulated packets for both G.729 and a TCP packet are shown in [Figure 8-5](#).

Figure 8-5 Packet Decode—G.729 and TCP with NAT-T



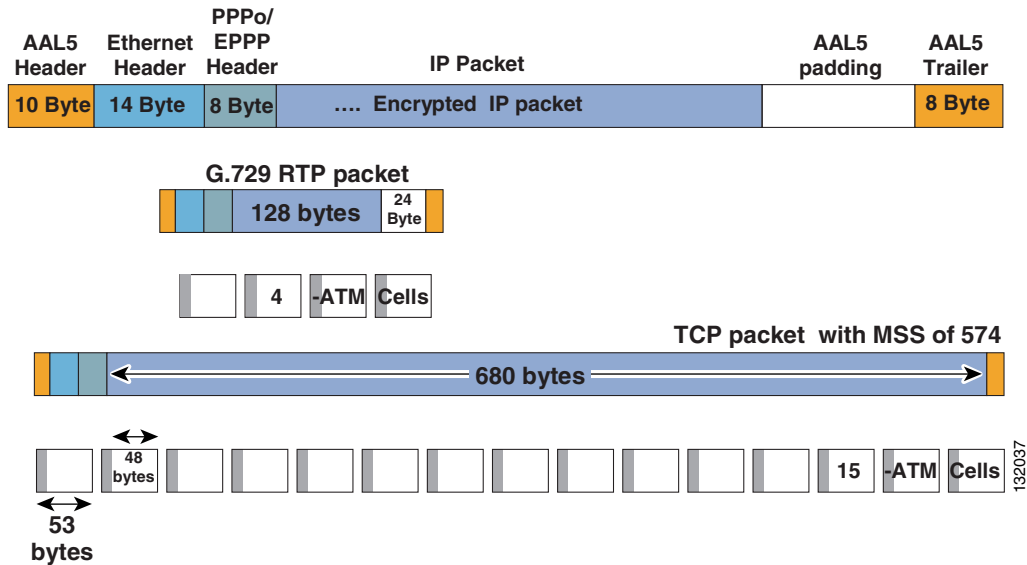
In this example, the TCP packets have a padding of 0 for IPsec. The IP header is UDP with source and destination port 4500. The NAT/pNAT device may change the IP address and port number. Using the **show crypto ipsec sa detail | inc peer** command on the head-end router shows the source port and IP address derived from NAT-T.

**Note**

Because both IKE and ESP packets share the same UDP port number (4500), IKE packets have a Non-ESP marker field consisting of 4 bytes zero filled that aligns with the Service Provider Interface (SPI) field of an ESP packet. Because the SPI cannot be all zeros, this enable the receiver to distinguish between an ESP and IKE packet. As such, the additional overhead of NAT-T is the 8 byte UDP header for ESP packets, and 12 bytes for IKE packets (8 bytes for the UDP header and an additional 4 bytes for the non-ESP Marker). There is also an additional packet, a NAT-keepalive packet, which is a UDP packet, port number 4500, with a single byte field with a value of 0xFF. The receiver ignores these packets; however, they serve to keep the NAT/pNAT device translation table fresh.

These encrypted IP packets, when encapsulated in PPPoE/AAL5/ATM cells for a DSL deployment, are shown in Figure 8-6.

Figure 8-6 DSL/PPPoE Encapsulation with NAT-T



The result is a G.729 packet that requires four ATM cells, and a TCP packet with an MSS of 574 that requires 15 ATM cells. There are zero bytes AAL5 padding in the last cell. The TCP MSS value of 574 is used so that with or without NAT-T negotiated, the TCP packets always require 15 ATM cells. This simplifies the task by generalizing the configuration of the remote router.

## Sample V3PN Relevant QoS Configuration

Based on the previous analysis of the customer configuration, this section shows recommended changes to optimize and enhance the configuration.

### TCP Maximum Segment Size

Given the previous analysis of the fields in the unencrypted payloads and resulting encryptions and encapsulations, using a TCP MSS size override of 574 on the inside Ethernet and GRE tunnel interface is used in the following configuration:

```
!
interface Ethernet0
 ip address 10.0.94.1 255.255.255.0
 ip route-cache flow
 ip tcp adjust-mss 574
!
interface Tunnel0
 description DMVPN
 ip address 10.0.90.12 255.255.255.0
 ...
 ip route-cache flow
 ip tcp adjust-mss 574
```



#### Note

Performance results with this change and the other recommended changes are shown in a subsequent section.

## IP MTU of Tunnel interfaces

The customer configuration includes a manually configured tunnel IP maximum transmission unit (MTU) with a value of 1408, as shown:

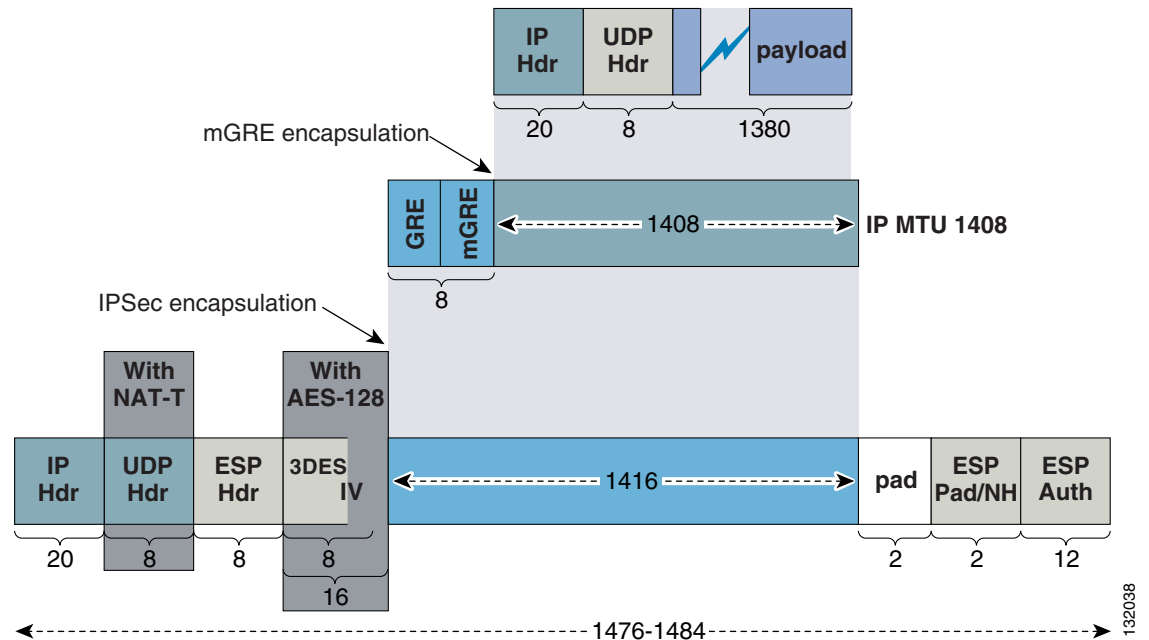
```
interface Tunnel0
...
 ip mtu 1408
```

1408 is an optimal IP MTU value for deployments, whether or not they include PPPoE, NAT-T, 3DES, or Advanced Encryption Standard (AES)-128. In the previous section, the remote router adjusts the MSS value for TCP sessions to and from the remote site. Although this eliminates any fragmentation issues for the majority of the data traffic, there still might be UDP applications that generate some MTU-sized packets. Ideally, these should be fragmented by the router before encryption.

Changing the IP MTU of the tunnel interface effectively forces fragmentation before encryption. Fragmenting after encryption means that the decrypting router must reassemble the fragments before they can be decrypted. This requirement means that the decrypting router must process switch the fragmented packets and allocate a huge buffer in memory to assemble the fragments, which negatively impacts performance, especially if the decrypting router is the head-end crypto aggregation point that decrypts for multiple remote or spoke routers. Fragmenting before encryption forces the receiving workstation to re-assemble the fragments instead.

Given a tunnel interface with an IP MTU of 1408, the largest UDP packet that can be encapsulated without fragmentation is 1380 bytes of payload plus 28 bytes for IP and UDP headers. This encapsulation process is shown in [Figure 8-7](#).

**Figure 8-7** mGRE and IPsec Encapsulation



With PPPoE (commonly used with residential DSL offerings), a maximum encrypted packet size of 1492 is preferred because PPPoE includes an 8-byte header.

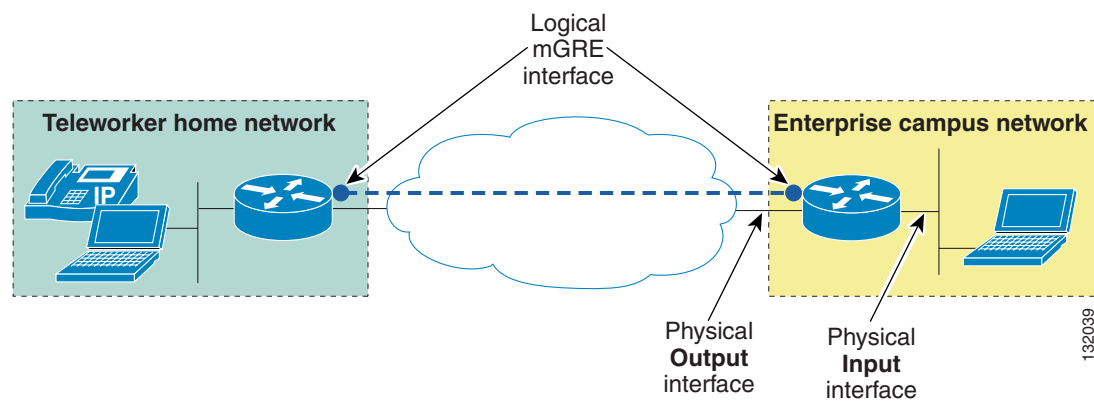
**Note**

Ethernet has a maximum payload size of 1500 octets. The PPPoE header is six octets and the PPP protocol ID is two octets, so the PPP MTU must not be greater than 1492. For more information, see RFC 2516 at the following URL: <http://www.rfc-archive.org/getrfc.php?rfc=2516>.

AES-128 has a 16-byte initialization vector (IV) as compared to 8 bytes for 3DES. If the remote router is behind a personal firewall, an additional UDP header is also present. The size of the ESP pad varies depending on the payload size being encrypted and whether the encryption algorithm is 3DES or AES.

There are some rules for identifying fragmentation and determining whether it is pre- or post-encryption. The topology in Figure 8-8 is shown as a reference:

**Figure 8-8** Fragmentation Illustration



Assume that the workstation in the enterprise campus network is generating packets to the remote teleworker home network at a constant rate with no other traffic present.

**Note**

A test tool or application that can be configured to generate a UDP packet at a configured size and at a constant rate in packets per second is useful for this illustration.

Fragmentation can be identified by observations on the head-end router.

- Pre-encryption fragmentation—Fragmentation because of the MTU of the mGRE tunnel interface
  - **show ip traffic | include fragmented** shows a steadily increasing counter.
  - **show interface tunnel[n] | include rate** shows an input rate twice the number of packets per second being sent by the workstation.
- Post-encryption fragmentation—Fragmentation because of the MTU of the output interface
  - **show interface tunnel[n] | include rate** shows an input rate equal to the sending rate of the workstation.
  - **show interface [output interface] | include rate** shows an output rate twice the number of packets per second as shown on the tunnel interface.

Thus, given the variety of topologies encountered in the typical teleworker deployment scenarios, the customer choice of IP MTU for the mGRE tunnel interfaces is a good choice.

## Class-map Configuration

In this case study, the customer has configured match statements in the class map that were not relevant and redundant. As a best practice, these extraneous entries should be removed.

For example, the initial customer configuration is as follows:

```
class-map match-any ISC_OUT_Cisco-IT_voice_call-setup
  match ip dscp af31
  match ip dscp af32
  match ip dscp cs3
  match ip precedence 3
class-map match-any ISC_OUT_Cisco-IT_voice_voice
  match ip dscp ef
  match ip dscp cs5
  match ip precedence 5
```

Matching on Differentiated Services Code Point (DSCP) value of CS5 and also on IP Precedence of “5” is redundant.



### Note

Section 4.2 of RFC 2474 describes the use of CS (Class Selector) codepoints to provide backward compatibility matching of IP Precedence values. See RFC 2474 at the following URL:  
<http://www.rfc-archive.org/getrfc.php?rfc=2474>

For example, see the following configuration, given this sample class map and an IP phone generating packets for call setup with DSCP value of CS3 or IP Precedence 3:

```
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
  match ip precedence 3

R1#show pol int e 0/0 output | beg CALL-SETUP
Class-map: CALL-SETUP (match-any)
  5 packets, 306 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp af31
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: ip dscp cs3
    5 packets, 306 bytes
    30 second rate 0 bps
  Match: ip precedence 3
    0 packets, 0 bytes
    30 second rate 0 bps
```

From the above display, observe that no packets are matching IP Precedence 3, but rather DSCP value of CS3. The following displays shows the order reversed in the class map:

```
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip precedence 3
  match ip dscp cs3

R1#show pol int e 0/0 output | beg CALL-SETUP
Class-map: CALL-SETUP (match-any)
  32 packets, 2068 bytes
```

```

30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp af31
    0 packets, 0 bytes
    30 second rate 0 bps
Match: ip precedence 3
    32 packets, 2068 bytes
    30 second rate 0 bps
Match: ip dscp cs3
    0 packets, 0 bytes
    30 second rate 0 bps

```

In the above configuration, there are no matches on the DSCP value of CS3, but rather the match for IP Precedence 3 selects the packets.

Additionally, the customer call-setup class contains a match for AF32. Because the target configuration is for a remote router supporting an IP phone, there is no expectation that AF32 packets will ever be seen at this point in the topology. The DSCP value of AF32 is generally seen only if the traffic is out of contract and was remarked from AF31 to AF32 by a router.

**Note**


---

According to RFC 2597 (“Assured Forwarding PHB Group”), AF31 has a lower drop probability than AF32 and the act of remarking from AF31 to AF32 is an indication of congestion within the per-hop behavior (PHB) group. See more information on RFC 2597 at the following URL:  
<http://www.rfc-archive.org/getrfc.php?rfc=2597>

---

Because this configuration is for the router that provides network access for the phone, and the phone either generates AF31 or CS3 for its call-setup traffic, no remarking is possible.

Assuming a Cisco IP phone, **match ip dscp cs5** can also be eliminated, because the firmware of the phone always generates DSCP values of EF for the voice media stream.

The proposed configuration can be reduced to the following:

```

class-map match-any ISC_OUT_Cisco-IT_voice_call-setup
  match ip dscp cs3
  match ip dscp af31

```

```

class-map match-all ISC_OUT_Cisco-IT_voice_voice
  match ip dscp ef

```

There now is only one entry for the voice class map, the **match-any** is changed to **match-all**, and the default value is for a one entry class-map.

## Weighted fair-queue Configured on Ethernet Interfaces

The customer configuration included **fair-queue** on the outside Ethernet interface, as shown in the following:

```

interface Ethernet1
  description Provisioned by ISC (public interface)
  ip address dhcp
  ip access-group ISC_FIREWALL_outside_inbound_1 in
  service-policy output ISC_OUT_Cisco-IT_voice_TOP
  ip route-cache flow
  duplex auto
  fair-queue

```

It is extremely unlikely that the Ethernet interfaces on these routers will ever experience congestion. Weighted fair queueing (WFQ) is only recommended for interfaces clocked below 2 Mbps. In fact, Cisco 83x and 17xx routers are gated by CPU consumption before 10 Mbps Ethernet interfaces can be congested. The default of FIFO queueing on the Ethernet interfaces is recommended. To remove WFQ from the interface, enter **no fair-queue** while in interface configuration mode.

## Service Assurance Agent (SAA) VoIP UDP Operation

The customer configuration includes an SAA VoIP UDP operation feature that was introduced in Cisco IOS Release 12.3(4) and includes Impairment/Calculated Impairment Planning Factor (ICPIF) and Mean Opinion Score (MOS) values. This feature is configured on the remote router configuration as follows:

```
rtr 10
type jitter dest-ipaddr 10.86.252.2 dest-port 16384 codec g729a
tag jitter-with-voice-scores
frequency 180
rtr schedule 10 life forever start-time now
```

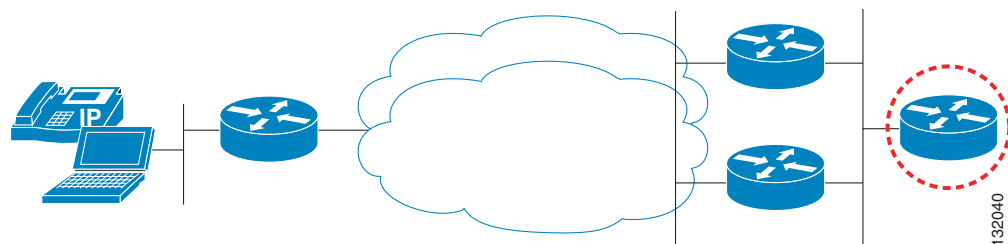
This is a very useful feature for diagnosing voice quality issues for a teleworker. However, some optimization is suggested to reduce the overhead and to optimize the data collection aspect.

## Configuring SAA VoIP UDP at the Campus Head-end

The first recommendation is to remove the SAA VoIP UDP operation from the remote router, and instead either deploy a dedicated router or use an existing campus head-end router to initiate the probes. The remote router must then be configured only with **rtr responder** and does not need to be running a Cisco IOS release at or later than 12.3(4)T; only the head-end router has the code dependency for the introduction of the feature.

The campus head-end router shown circled in [Figure 8-9](#) is assumed to have the recommended configuration described later in this section.

**Figure 8-9** Campus Head-end SAA VoIP UDP Router



## Reducing SAA Bandwidth Requirements

The default number of packets generated by the VoIP UDP operation (type jitter) is 1,000 with an interval of 20 ms between packets, or 50 packets per second. Thus, the default configuration generates 20 seconds worth of simulated voice traffic every 180 seconds or three minutes. Although the head-end router generates the packets initially, the remote router answers these packets on the return path. In the initial customer configuration, the type of service (ToS) byte of the packets of the probes was not set, and these simulated voice packets will be marked best effort, or ToS of 0. Because the goal is to measure the latency and jitter of the simulated voice stream assuming that it is representative of an actual voice call, it is preferred to mark the simulated packets with the same ToS value as an actual voice call.

For this reason, the number of packets are reduced to a more manageable value of 20 packets (**codec-numpackets 20**). The probe runs every 300 seconds or five minutes and marks the simulated voice stream with a ToS of decimal 184 (hex B8) or DSCP EF as would be the case with a real voice stream. The priority or Low Latency Queueing (LLQ) is adjusted to accommodate this additional traffic.

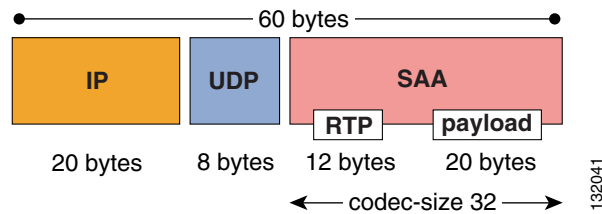
## Recommended Probe Configuration

The implemented configuration is as follows:

```
rtr 10
 type jitter dest-ipaddr 10.0.94.1 dest-port 16384 codec g729a codec-numpackets 20
 codec-size 32
 tos 184
 timeout 200
 tag JITTER_10.0.94.0
 frequency 300
!
```

The **codec-size** value of 32 is the default value and does not show in the running configuration. It is included here to illustrate that the codec size would be the sum of the RTP header plus the payload, or voice sample. [Figure 8-10](#) shows the fields of the SAA-generated packet:

**Figure 8-10 SAA VoIP Codec-size**



Assuming a DMVPN or mGRE encapsulation, look at the NetFlow display while the SAA probe is running to verify packet sizes:

```
R1#show ip cache verb flow
...
SrcIf          SrcIPAddress  DstIf          DstIPAddress  Pr TOS Flgs Pkts
Port Msk AS    Port Msk AS    NextHop        B/Pk Active
...
Et1            192.168.131.16 Local          192.168.128.207 2F B8 10    21
0000 /0 0      0000 /0 0      0.0.0.0        88    0.3
...
Tu0            10.0.90.16   Local          10.0.94.1     11 B8 10    1
DBA2 /0 0      07AF /0 0      0.0.0.0        80    0.0
...
Tu0            10.0.90.16   Local          10.0.94.1     11 B8 10    20
DBA2 /0 0      4000 /0 0      0.0.0.0        60    0.3
```

The first flow is Protocol (Pr) hex 2F or decimal 47, GRE. The ToS byte from the unencrypted packet is copied to the GRE header and as such, this GRE packet is marked DSCP EF or hex B8. There are 21 packets in this flow: one SAA control packet and the 20 packets simulating voice. The B/Pk shows the average number of bytes per packet, including the IP/GRE headers.

The second line of the display has a destination port address of hex 7AF or decimal 1967. Port 1967 is enabled when **rtr responder** is configured and the remote router is listening on this UDP port. By default, **control enable** is enabled, and it must be enabled for this SAA probe to function properly. This packet is the control plane for the SAA probe.

The third line in the display is the SAA-generated simulated voice packets. There are 20, as specified above. They have a destination UDP (hex 11 or decimal 17) port number of hex 4000 or decimal 16384, as specified in the SAA configuration above. Because all these packets are the same size, the average B/Pk is 60, which is the size of each packet from the packet decode in the previous figure.

## SAA Reaction Configuration

To aid in more quickly identifying teleworkers experiencing voice quality issues, reaction-configurations can be defined by using syslog/logging buffer entries to highlight probes that are experiencing jitter and latency that is exceeding or falling below a pre-determined threshold value.

For example, see the following:

```
rtr reaction-configuration 10 react jitterDSAvg threshold-value 8 7 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 10 react rtt threshold-value 150 149 threshold-type immediate
action-type trapOnly
rtr reaction-configuration 10 react jitterSDAvg threshold-value 6 5 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 10 react timeout threshold-type immediate action-type trapOnly
rtr schedule 10 life forever start-time now
!
```

In the above configuration, a log entry is generated if the average jitter from destination to source (teleworker to head-end) rises above 8 ms and again when it falls below 7 ms. The roundtrip time thresholds (RTTs) are 150 ms and 149 ms, and with the jitter from source to destination (head-end to teleworker), the reaction is triggered if the jitter rises above 6 ms and again if it falls below 5 ms.

The head-end to teleworker jitter values are lower than the teleworker to head-end path because most residential broadband services have greater bandwidth from the Internet, and the jitter typically is less in that direction. The values selected vary from deployment to deployment.

## Revising the Policy-map for VoIP UDP Operation

To accommodate including the SAA probes being marked DSCP EF, the priority or LLQ size is increased approximately 26 kbps. Assuming DMVPN (mGRE in transport mode) with NAT-T, ESP 3DES, and SHA, these SAA probe packets are 128 bytes in length after encryption. Now add 32 bytes per packet for the AAL5, Ethernet, and PPP/PPPoE header, resulting in 160 bytes per packet, at 8 bits per byte and 50 packets per second (160 \* 8 \* 50) or 64,000 kbps. The SAA probe is active in .4 seconds, because 20 packets at a 20 ms interval is 400 ms.

```
!
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
!
!
policy-map V3PN_DMVPN_Teleworker
description G.729=~64K G.711=~128K Plus 26K for IP SLA (SAA)
```

```

class CALL-SETUP
  bandwidth percent 2
class INTERNETWORK-CONTROL
  bandwidth percent 5
class VOICE
  priority 154
class class-default
  fair-queue
  random-detect
policy-map Shaper
  class class-default
    shape average 182400 1824
    service-policy V3PN_DMVPN_Teleworker
!
```

Comparison testing determined the impact of this SAA probe on latency, drops, and jitter of the real voice (RTP) stream. Branch to head-end jitter increases one millisecond, from 9.2 ms to 10.2 ms, and approximately 20 ms are added to the branch to head-end latency. The head-end to branch values were for all practical purposes unchanged. Voice drops are not an issue. However, the release under test was exposed to a packet classification issue identified as CSCeg34495. It is possible that the performance characteristics would actually be better than described using a Cisco IOS release not exposed to this issue.

## Routing

Before discussing access control for this implementation, it is necessary to describe the IP routing configuration. The enterprise security policy specifies that access to Internet services is via the head-end enterprise campus network. This is often referred to as split tunneling not being permitted.

That implies that the remote teleworker PC needs to follow a default route learned via the mGRE tunnel interface rather than from the DHCP server that supplied the outside IP addressing information to the VPN router.

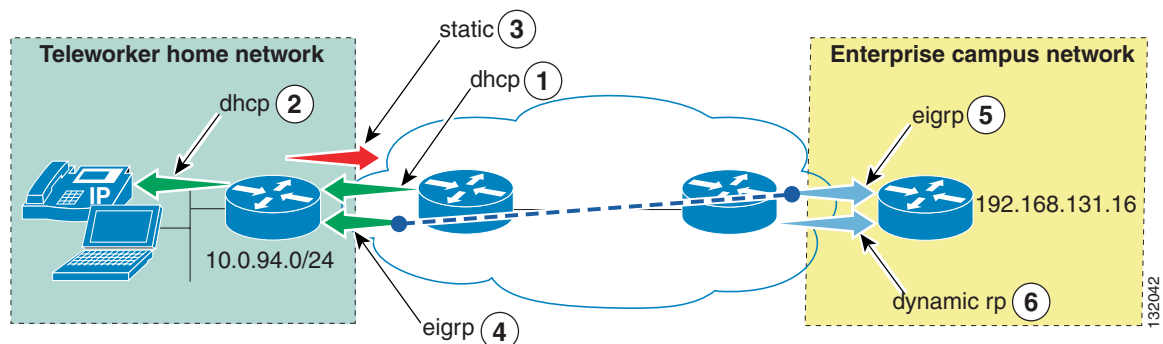
The routing information sources are described and shown in [Figure 8-11](#).



### Note

References to 192.168.x.x are a placeholder for an Internet-routable address.

**Figure 8-11** Routing Information Sources



The following sequence occurs:

1. The teleworker VPN router learns a default gateway from the DHCP server of the ISP.

```
vpn-831#show dhcp lease | inc default-gateway
Temp default-gateway addr: 192.168.128.1

vpn-831#show ip route | inc 192.168.128.1
Gateway of last resort is 192.168.128.1 to network 0.0.0.0
S    192.168.131.16 [1/0] via 192.168.128.1
S*   0.0.0.0/0 [254/0] via 192.168.128.1
```

2. The teleworker VPN router supplies a default gateway and serves IP addressing and other options to the IP phone and workstation using a local DHCP pool.

```
!
ip dhcp pool TELEWORKER
network 10.0.94.0 255.255.255.0
default-router 10.0.94.1
dns-server 10.2.120.253 10.2.120.252
domain-name ese.cisco.com
option 150 ip 10.2.120.254
!
```

3. The teleworker VPN router is configured with a static route to the head-end tunnel endpoint. In this example, 192.168.131.16 and 192.168.131.17 are placeholders for the head-end tunnel endpoint addresses. In an actual deployment, they would be Internet-routable addresses.

```
vpn-831#show run | inc ip route

ip route 192.168.131.16 255.255.255.254 dhcp
```

The above is required because there will be two sources of a default route, one from the Internet and one from the mGRE tunnel. The VPN router must have more specific routes to servers that must be reached outside the VPN tunnel, rather than using the default route learned inside the IP tunnel.

4. The teleworker VPN router learns a default route using the GRE tunnel from the head-end campus router. The default administrative distance for an EIGRP internal/external route is 90/170, and 254 for a DHCP learned route. The default route learned through the GRE tunnel is overridden because it has a lower administrative distance than the default route learned using DHCP.

```
vpn-jk3-2651xm-1#show ip route | inc 0.0.0.0/0
D*EX 0.0.0.0/0 [170/58770176] via 10.0.90.16, 00:00:14, Tunnel0
```

5. The head-end campus router learns an advertisement through the GRE tunnel for the subnet of the remote branch teleworker router.

```
vpn-jk3-2651xm-6#show ip route | inc 10.0.94.0
D    10.0.94.0/24 [90/1817600] via 10.0.90.12, 22:53:07, Tunnel0
```

6. The head-end campus router must learn either from a static default route or more likely from some dynamic routing protocol of the outside Internet routable address of the remote teleworker.

The difference between IPSec-protected GRE and direct IPSec encapsulation is related to determining whether a packet is encrypted. In the case of IPSec-protected GRE tunnels, all packets routed through the tunnel is encrypted, so it is the routing table of the remote router that determines if a packet is encrypted. In direct IPSec encapsulation, any packet that matches the access list specified in the crypto map is encrypted. So routing determines only whether the packet exits an interface with an applied

crypto map, not whether it is actually encrypted. This is a subtle but important difference, because it allows the network administrator to use the head-end routing protocol configuration to control the encryption selection process on the remote routers.

## Access Control

The initial customer configuration consists of inbound ACLs on the outside physical interface. There are no inbound access lists on the tunnel interface. Also, the configuration includes both Transport layer (TCP and UDP) inspection as well as Application layer inspection.

The initial configuration is as follows:

```
ip inspect name ISC_inside_1 tcp
ip inspect name ISC_inside_1 rtsp
ip inspect name ISC_inside_1 smtp
ip inspect name ISC_inside_1 h323
ip inspect name ISC_inside_1 realaudio
ip inspect name ISC_inside_1 tftp
ip inspect name ISC_inside_1 skinny
ip inspect name ISC_inside_1 ftp
ip inspect name ISC_inside_1 udp
ip inspect name ISC_inside_1 netshow
ip inspect name ISC_inside_1 sip
```

Typically, Transport layer inspection is sufficient for most deployments. With TCP and UDP inspection, the return path packets must match an existing session initiated from the protected (or inside) network. The source and destination IP addresses and port numbers must match in reverse of the session initiated by the inside client.



### Note

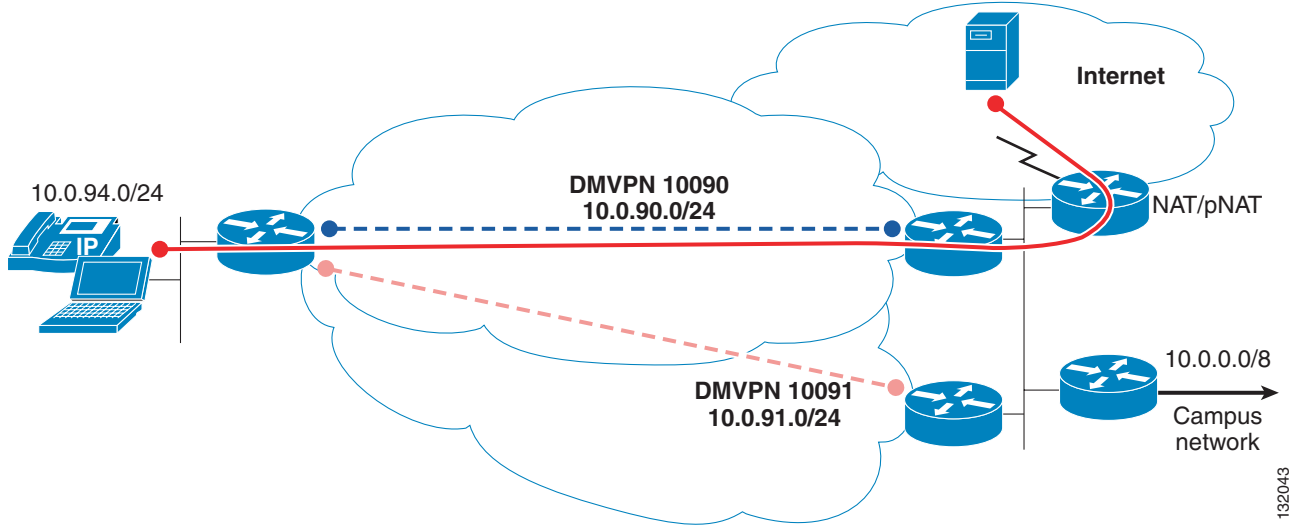
For more information, see the following URL (which requires a Cisco password):

[http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/products\\_white\\_paper09186a0080094658.shtml](http://www.cisco.com/en/US/partner/products/sw/secursw/ps1018/products_white_paper09186a0080094658.shtml)

Application layer inspection takes precedence over Network layer inspection, and is required if the specific application (such as FTP) uses different port numbers than specified by the session initiator in the return packets.

The customer security policy is such that split tunneling is not permitted. All Internet access for devices on the remote subnet must be through the corporation campus head-end. Because private addressing is in use, the campus head-end location must use NAT/pNAT to determine any Internet access required. The address of the return packets from the Internet server or application is the Internet routable address, and as such, Context-based Access Control (CBAC) must be configured to permit Internet access, but only for TCP, UDP, and FTP initially. Additional Application layer inspection can be added as required. An example of this topology is represented in [Figure 8-12](#).

Figure 8-12 Access Control Topology Example



The tunnel interfaces have inbound access lists, and CBAC is enabled on the inside Ethernet interface of the remote branch teleworker router. If the inbound access list entry does not specifically permit the packet, the CBAC configuration must have entered a dynamic entry into the access list to permit packets from the enterprise campus head-end to access the remote router subnet.

This layered security approach affords a more stringent posture than what is typically implemented in the enterprise campus network.

The recommended configuration is as follows:

```

!
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
!
interface Tunnel0
...
 ip address 10.0.90.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
!
interface Tunnel1
...
 ip address 10.0.91.12 255.255.255.0
 ip access-group TUNNEL_INBOUND_ACL in
!
interface Ethernet0
 ip address 10.0.94.1 255.255.255.0
 ip inspect CBAC in
 ip route-cache flow
 ip tcp adjust-mss 574
!
interface Ethernet1
 ip address dhcp
 ip access-group INBOUND_ACL in
 service-policy output Shaper
 ip route-cache flow
!
ip access-list extended INBOUND_ACL
 permit udp any eq isakmp any eq isakmp
 permit udp 192.168.131.0 0.0.0.31 eq non500-isakmp any eq non500-isakmp
 permit esp 192.168.131.0 0.0.0.31 any

```

```

permit gre 192.168.131.0 0.0.0.31 any
permit udp any any eq bootpc
remark NTP ACLs
permit udp any eq ntp any eq ntp
permit icmp any any
remark SSH
permit tcp 192.168.131.0 0.0.0.31 any eq 22
deny ip any any log
!
ip access-list extended TUNNEL_INBOUND_ACL
permit ip 10.0.0.0 0.0.0.255 10.0.94.0 0.0.0.255
permit icmp any any
permit eigrp any any
permit igmp any any
permit pim any any
deny ip any any log
!
line vty 0 4
login local
transport input ssh

```

**Note**

The log option is useful initially to identify any ports and protocols that are missing from the implementation but are needed for the deployment. After testing, it is recommended to remote this option to spare the overhead of process switching the matches on the entry and the resulting syslog chatter.

## Performance Testing

Performance tests were conducted using the customer initial configuration and the enhanced (revised) configuration described in this section. There are also test results using the revised configuration with and without a Linksys BEFSR41 personal firewall between the IPSec peers with NAT-T enabled. [Table 8-1](#) describes these tests.

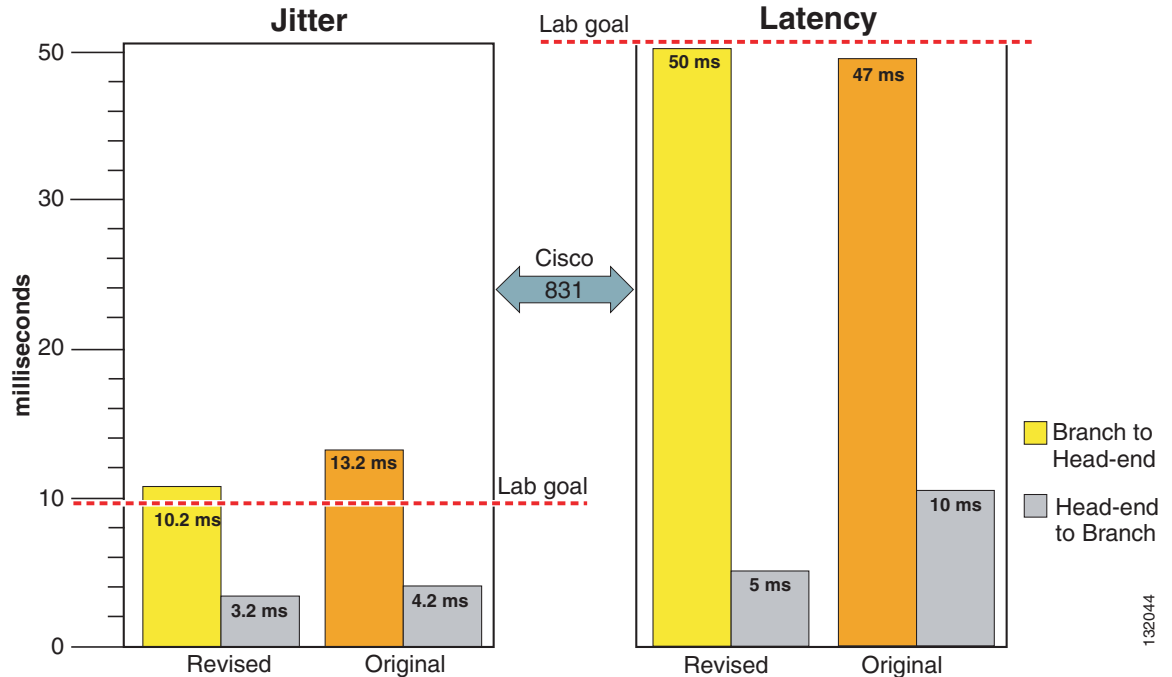
**Table 8-1 Performance Test Table**

Configuration	Customer Initial Configuration	Revised Configuration
Weighted fair-queue configured on Ethernet interfaces	WFQ enabled	FIFO
Class-map configuration	Extraneous entries	Optimized
TCP MSS	Not configured	574
SAA VoIP UDP Operation— Revised policy-map for VoIP UDP operation	On remote router without ToS marking and at customer configured frequency	Remote router as responder only, optimized, and head-end configured and initiated
Access control	All application layers enabled	UDP, TCP, and FTP only
NAT-T and Linksys Personal Firewall	N/A	With and without using the above configuration changes

## Original and Revised Configurations

Figure 8-13 shows the net impact of the revised configuration on VoIP latency and jitter. The difference in voice drops was of no consequence.

Figure 8-13 Original and Revised Configuration Test Results



The testbed uses a goal of 50 ms as the average Chariot reported latency and 8–10 ms as the average jitter for acceptable VoIP quality. In a customer deployment, acceptable VoIP quality can be obtained when both latency and jitter are observed at higher values. The lab is a controlled and optimal environment and these somewhat conservative goals are the standard.

In most teleworker environments, the data rates are asymmetrical; both branch router to head-end router and the reverse are reported. In this test, a simulated 256 kbps/1.4 Mbps data rate was assumed. The 831 output interface was shaped at 182,400 bps. Because of the higher downlink data rate, latency and jitter are generally not an issue for this half of the call leg. The downlink values are shown in the diagram but are subdued and behind the uplink or branch to head-end values.

In either configuration, the latency is similar, and near the 50 ms goal.

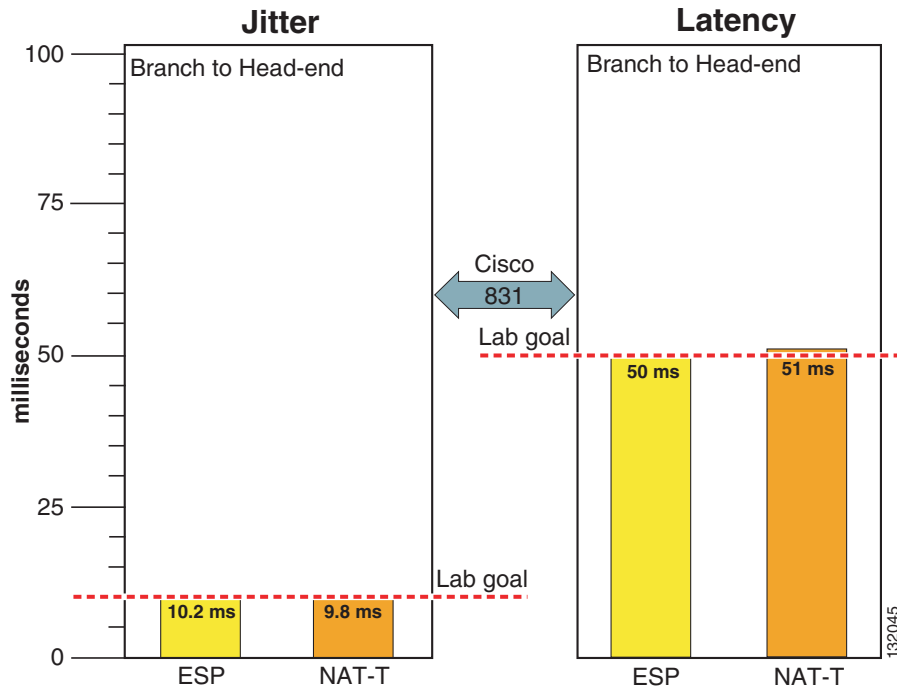
Average jitter for the revised configuration is 10.2 ms and 13.2 ms for the original configuration, or approximately a 22 percent improvement. At higher data rates, this difference would be less as the link speed approaches 768 kbps, and serialization or blocking delay becomes less of an issue.

## Impact of NAT-T

NAT-T mode is enabled by default in Cisco IOS routers, and if during the initial IKE exchange on UDP 500, a NAT/pNAT device is detected between the IPSec peers, these peers exchange both IKE and IPSec packets encapsulated in UDP on port 4500. If no NAT/pNAT device exists between the peers, the normal

behavior of IKE on UDP 500 and IPsec ESP in protocol “50” is used. A Linksys BEFSR41 EtherFast® Cable/DSL Router with 4-Port Switch is inserted between the IPsec peers and a performance test is run with the revised configuration. (See [Figure 8-14](#).)

**Figure 8-14** Impact of NAT-T

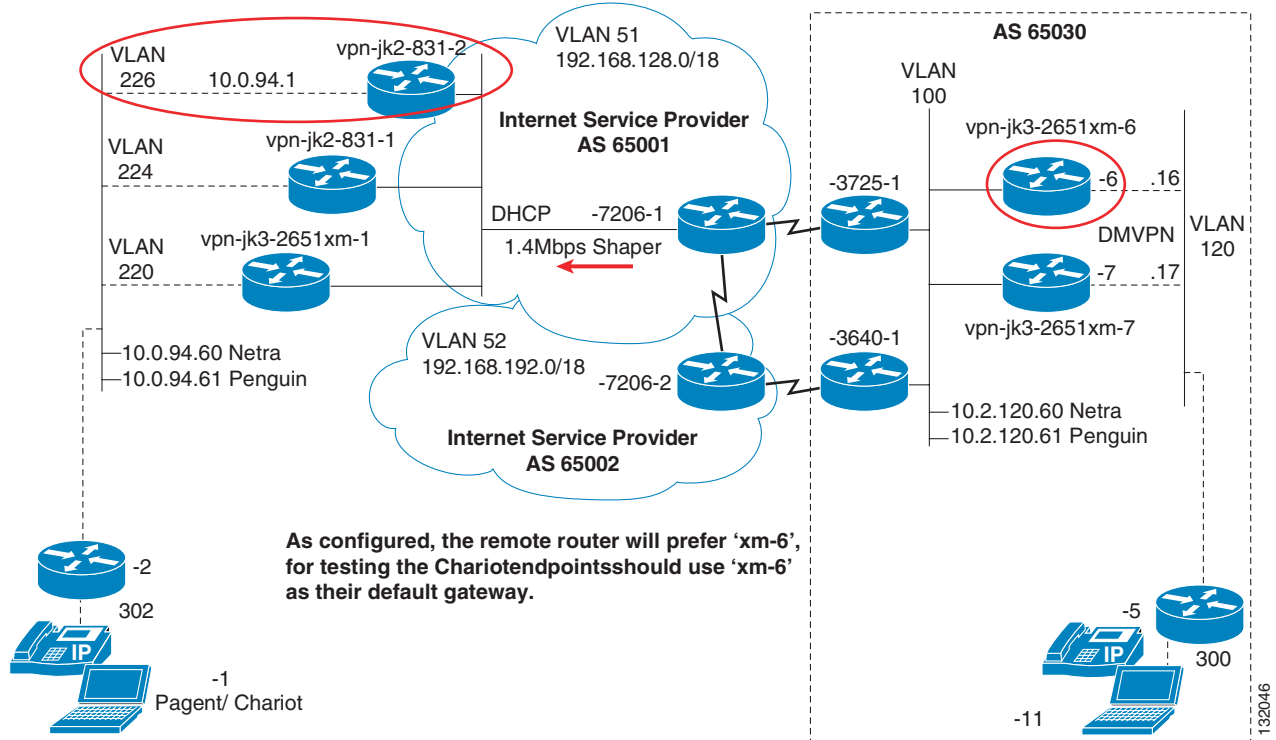


Simply stated, the results were similar enough to indicate that the additional router and the NAT/pNAT translation on the UDP 4500 packets did not impact latency and jitter of the VoIP stream to a measurable degree.

## Test Topology

[Figure 8-15](#) shows the topology under test:

Figure 8-15 Test Topology



## Implementation and Configuration

This section describes the configuration of the dual hub/dual DMVPN solution, and includes the following sections:

- [Remote Branch Router](#)
- [Primary Head-end Router](#)

### Remote Branch Router

This is the configuration of the remote branch router:

```

version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname vpn-jk2-831-2
!
clock timezone est -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!

```

```

!
!
no ip domain lookup
ip domain name ese.cisco.com
ip host JOEL_KING_LAB_ca_server 192.168.131.25
ip cef
ip inspect name CBAC tcp
ip inspect name CBAC udp
ip inspect name CBAC ftp
ip ips po max-events 100
no ftp-server write-enable
!
crypto pki trustpoint ESE_JK_RACK
  enrollment url http://JOEL_KING_LAB_ca_server:80
  revocation-check none
!
!
crypto pki certificate chain ESE_JK_RACK
  certificate 03
    [removed]
  quit
  certificate ca 01
    [removed]
  quit
!
!
class-map match-all VOICE
  match ip dscp ef
class-map match-any CALL-SETUP
  match ip dscp af31
  match ip dscp cs3
class-map match-any INTERNETWORK-CONTROL
  match ip dscp cs6
  match access-group name IKE
!
!
policy-map V3PN_DMVPN_Teleworker
  description G.729=~64K G.711=~128K Plus 26K for IP SLA (SAA)
  class CALL-SETUP
    bandwidth percent 2
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class VOICE
    priority 154
  class class-default
    fair-queue
    random-detect
policy-map Shaper
  class class-default
    shape average 182400 1824
    service-policy V3PN_DMVPN_Teleworker
!
!
!
crypto isakmp policy 10
  encr 3des
crypto isakmp keepalive 10
crypto isakmp nat keepalive 10
!
!
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
  mode transport
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!

```

```

crypto ipsec profile ECT_PROFILE_1
  set security-association lifetime kilobytes 530000000
  set security-association lifetime seconds 14400
  set transform-set TRANSPORT_3DES_SHA
!
!
crypto call admission limit ike sa 65536 # Included simply to show it is configurable
!                                     # An 831 has a 20 crypto peer (IKE peer limit)
!                                     but 5-10 peers is a practical limit.
!
interface Tunnel0
  description Tunnel0 - DMVPN
  bandwidth 2000
  ip address 10.0.90.12 255.255.255.0
  ip access-group TUNNEL_INBOUND_ACL in
  no ip redirects
  ip mtu 1408
  ip nhrp map 10.0.90.16 192.168.131.16
  ip nhrp map multicast 192.168.131.16
  ip nhrp network-id 10090
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.90.16
  ip route-cache flow
  ip tcp adjust-mss 574
  ip summary-address eigrp 100 10.0.94.0 255.255.255.0 5
  qos pre-classify
  tunnel source Ethernet1
  tunnel mode gre multipoint
  tunnel key 10090
  tunnel protection ipsec profile ECT_PROFILE_1 shared
!
interface Tunnel1
  description Tunnel1 - DMVPN
  bandwidth 2000
  ip address 10.0.91.12 255.255.255.0
  ip access-group TUNNEL_INBOUND_ACL in
  no ip redirects
  ip mtu 1408
  ip nhrp map 10.0.91.17 192.168.131.17
  ip nhrp map multicast 192.168.131.17
  ip nhrp network-id 10091
  ip nhrp holdtime 300
  ip nhrp nhs 10.0.91.17
  ip route-cache flow
  ip tcp adjust-mss 574
  ip summary-address eigrp 100 10.0.94.0 255.255.255.0 5
  load-interval 30
  qos pre-classify
  tunnel source Ethernet1
  tunnel mode gre multipoint
  tunnel key 10091
  tunnel protection ipsec profile ECT_PROFILE_1 shared
!
interface Ethernet0
  description Ethernet0 - inside
  ip address 10.0.94.1 255.255.255.0
  ip inspect CBAC in
  ip route-cache flow
  ip tcp adjust-mss 574
  load-interval 30
!
interface Ethernet1
  description Ethernet1 - outside
  ip address dhcp

```

```

ip access-group INBOUND_ACL in
service-policy output Shaper
ip route-cache flow
load-interval 30
duplex auto
!
interface FastEthernet1
no ip address
duplex auto
speed auto
!
interface FastEthernet2
no ip address
duplex auto
speed auto
!
interface FastEthernet3
no ip address
duplex auto
speed auto
!
interface FastEthernet4
no ip address
duplex auto
speed auto
!
router eigrp 100
network 10.0.0.0
no auto-summary          # Manual summarization on the interfaces
!
ip classless
ip route 172.26.0.0 255.255.0.0 10.0.94.2
ip route 192.168.131.16 255.255.255.254 dhcp
!
no ip http server
no ip http secure-server
!
!
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp
ip access-list extended INBOUND_ACL
permit udp 192.168.131.0 0.0.0.31 eq 500 isakmp any eq non500-isakmp
permit esp 192.168.131.0 0.0.0.31 any
permit gre 192.168.131.0 0.0.0.31 any
permit udp any any eq bootpc
remark NTP ACLs
permit udp any eq ntp any eq ntp
permit icmp any any
remark SSH
permit tcp 192.168.131.0 0.0.0.31 any eq 22
deny ip any any
ip access-list extended TUNNEL_INBOUND_ACL
permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
permit icmp any any
permit eigrp any any
permit igmp any any
permit pim any any
deny ip any any
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!

```

```

control-plane
!
call admission limit 99 # Included simply to show it is configurable
call admission load 1 10 # Included simply to show it is configurable
rtr responder
alias exec conact show cry eng conn act
alias exec shintb sh ip int brief
alias exec shacl show access-list
alias exec clacl clear access-list counters
alias exec shisa show crypto isa sa
alias exec stcon ping 10.2.120.16 source 10.0.94.1 repeat 15
!
line con 0
  exec-timeout 120 0
  no modem enable
  transport preferred all
  transport output all
line aux 0
  transport preferred all
  transport output all
line vty 0 4
  password [removed]
  login
  transport preferred all
  transport input all
  transport output all
!
scheduler max-task-time 5000
!
ntp server 192.168.130.1
end

```

## Primary Head-end Router

There are two head-end routers in this configuration, but only one is shown. The second head-end router terminates Tunnel 1 of the branch router.

```

version 12.3
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
hostname vpn-jk3-2651xm-6
!
!
logging buffered 8192 debugging
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate wic 0
no aaa new-model
ip subnet-zero
ip cef
!
!
ip ips po max-events 100
no ip domain lookup
ip domain name ese.cisco.com
ip host cisco123_LAB_ca_server 192.168.131.25
ip multicast-routing

```

```

no ftp-server write-enable
!
!
crypto pki trustpoint ESE_JK_RACK
  enrollment url http://cisco123_LAB_ca_server:80
  revocation-check crl
!
!
crypto pki certificate chain ESE_JK_RACK
  certificate 04
    [removed]
  quit
  certificate ca 01
    [removed]
  quit
!
crypto isakmp policy 1
  encr 3des
crypto isakmp keepalive 10
!
!
crypto ipsec transform-set TRANSPORT_3DES_SHA esp-3des esp-sha-hmac
  mode transport
crypto ipsec transform-set TUNNEL_3DES_SHA esp-3des esp-sha-hmac
!
crypto ipsec profile ECT_PROFILE_1
  set transform-set TRANSPORT_3DES_SHA TUNNEL_3DES_SHA
!
!
crypto call admission limit ike sa 65536 # Included simply to show it is configurable
!
!
interface Tunnel0
  description DMVPN
  bandwidth 2000
  ip address 10.0.90.16 255.255.255.0
  ip access-group TUNNEL_INBOUND_ACL in
  no ip redirects
  ip mtu 1408
  no ip next-hop-self eigrp 100
  ip pim nbma-mode
  ip pim sparse-dense-mode
  ip multicast rate-limit out 768
  ip nhrp map multicast dynamic
  ip nhrp network-id 10090
  ip nhrp holdtime 600
  ip nhrp server-only
  no ip split-horizon eigrp 100
  load-interval 30
  delay 2000
  tunnel source FastEthernet0/1.100
  tunnel mode gre multipoint
  tunnel key 10090
  tunnel protection ipsec profile ECT_PROFILE_1
!
interface FastEthernet0/0
  description FlashNet156
  ip address 172.26.157.36 255.255.254.0
  load-interval 30
  duplex auto
  speed auto
!
!
interface FastEthernet0/1.100

```

```

description Outside interface
encapsulation dot1Q 100
ip address 192.168.131.16 255.255.255.224 # Address referenced on remote peer
!
interface FastEthernet0/1.120
description Inside interface
encapsulation dot1Q 120
ip address 10.2.120.16 255.255.255.0
!
!
router eigrp 100
network 10.0.0.0
network 192.168.130.0 0.0.1.255
distribute-list TEN_and_SUBNETS out Tunnel0
no auto-summary
!
ip classless
ip http server
no ip http secure-server
!
ip access-list standard OFFSET
permit any
ip access-list standard TEN_ONLY
permit 10.0.0.0
remark --- only send 10.0.0.0
ip access-list standard TEN_and_SUBNETS
permit 10.0.0.0 0.0.255.255
!
ip access-list extended TUNNEL_INBOUND_ACL
permit ip 10.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255
permit icmp any any
permit eigrp any any
permit igmp any any
permit pim any any
deny ip any any
!
!
!
control-plane
!
call admission limit 99 # Included simply to show it is configurable
call admission load 1 10 # Included simply to show it is configurable
!
rtr responder
rtr 18
type jitter dest-ipaddr 10.0.94.1 dest-port 16384 codec g729a codec-numpackets 20
tos 184
timeout 200
tag JITTER_10.0.94.0
frequency 30
rtr reaction-configuration 18 react jitterDSAvg threshold-value 8 7 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 18 react rtt threshold-value 150 149 threshold-type immediate
action-type trapOnly
rtr reaction-configuration 18 react jitterSDAvg threshold-value 6 5 threshold-type
immediate action-type trapOnly
rtr reaction-configuration 18 react timeout threshold-type immediate action-type trapOnly
rtr schedule 18 life forever start-time now
alias exec conact show cry eng conn act
alias exec shintb sh ip int brief
alias exec shacl show access-list
alias exec clacl clear access-list counters
alias exec shisa show crypto isa sa
!

```

```
line con 0
  exec-timeout 120 0
line aux 0
line vty 0 4
  exec-timeout 0 0
  password [removed]
  login
!
ntp server 192.168.130.1
!
end
```

## Cisco IOS Versions Tested

The following Cisco IOS versions were used for testing:

- Branch routers—c831-k9o3sy6-mz.123-8.T5
- Head-end routers—c2600-advsecurityk9-mz.123-8.T5

## Summary

Although many customers often take the approach of implementing a pilot deployment without head-end redundancy, saying they will address redundancy later, all new installations should plan for and implement multiple head-ends from the beginning.

Extensive re-work of the deployed remote routers configuration may be necessary to accommodate VoIP in the future. With some minor revisions to the customer configuration, VoIP can be planned for and provisioned from the start, rather than later in a hurried manner.

These customer configurations were not dramatically wrong, but a few minor changes would have enhanced the performance of VoIP. As is often the case with networks, there is seldom only one problem and they tend not to cause a total failure of network connectivity. Generally, there are multiple issues that lead to a problem, and constant assessment of the network and its configuration serve to maintain reliability, availability, and good performance.