



# CHAPTER 10

## Large Branch—Multilink PPP

---

Large branch offices that require encrypted voice and data are generally limited to nine G.729 calls for a single T1 because 33 percent of the link is targeted for voice and the remainder of the bandwidth is targeted for data. For the enterprise customer who needs more than nine concurrent calls, or must also support video conferencing, using Multilink PPP (MLPPP) and including an additional T1 line rather than upgrading to either a full or fractional DS3 may be desirable from a cost standpoint.

Multilink PPP over leased lines to a head-end location may be the most cost effective option for the medium-to-large branch. The disadvantage with MLPPP is the lack of service provider support. Test results are included in this chapter for 8–15 concurrent voice calls, given a 4:1 to 10:1 Erlang ratio that translates to a WAN topology that can support an office staffed from 32 to 150 people.



### Note

---

An *Erlang* is a unit of telecommunications traffic measurement. An Erlang represents the continuous use of one voice path. Erlang traffic measurements (or estimates) can be used to determine how many concurrent voice calls should be provisioned between multiple network locations.

---

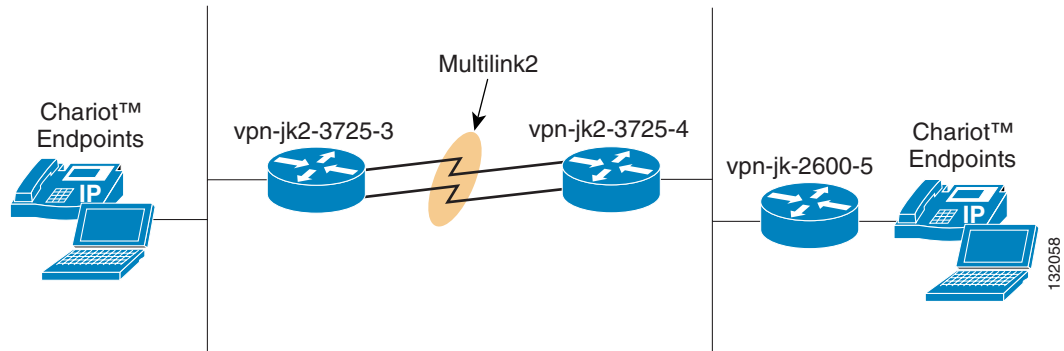
This chapter includes the following sections:

- [Topology](#)
- [Traffic Profile](#)
- [V3PN QoS Service Policy](#)
- [Implementation and Configuration](#)
- [Show Commands](#)
- [Cisco IOS Versions Tested](#)
- [Caveats](#)
- [Summary](#)

## Topology

The topology under test, as shown in [Figure 10-1](#), contains two Cisco 3725 routers with two serial interfaces (WIC-2T) clocked internally.

Figure 10-1 Large Branch—Multilink PPP



The **clockrate 1300000** command is used on one router serial interface to provide clocking for the lab testing. A rate of 1.536 M or 1.544 M is not supported by Cisco IOS for this interface type when clocked internally.

In testing, it is assumed that a branch of this size requires a separate router to increase the availability of the site. In other words, it was not assumed the second T1 was for availability, but rather as a capacity requirement.

## Traffic Profile

The traffic profile in these tests include G.729 voice calls, transactional data (TN3270 and HTTP), and best effort including HTTP, SMTP, DNS, and FTP.

Simulated Video Conferencing is also included. As part of the standard Chariot tests, an H.261 NetMeeting video conference stream is included and was modified for these tests. The H.261 video coding standard was designed for data rates that are multiples of 64 kbps, and is sometimes called “p x 64 kbps” (p is in the range 1–30). This video codec was designed for ISDN lines, which add capacity in increments of 64 kbps.

The default Chariot test has a buffer size of 522 bytes. The Layer 3 size of these UDP packets as reported by NetFlow is approximately 559 bytes, the difference being the IP, UDP, and Chariot headers included in the Layer 3 size of the packet. Note that this 559-byte packet does not include GRE, crypto, or PPP encapsulation headers. When using IPsec transport mode, the packet is 626 bytes or 650 bytes per packet using IPsec tunnel mode.

The Chariot target data rate is configured at 256 kbps, which equates to a video data stream of approximately 58 pps. The Chariot file size for this video stream is 2,088,000 bytes. In the caveats section, the testing ramifications of this file size are explored in more detail.

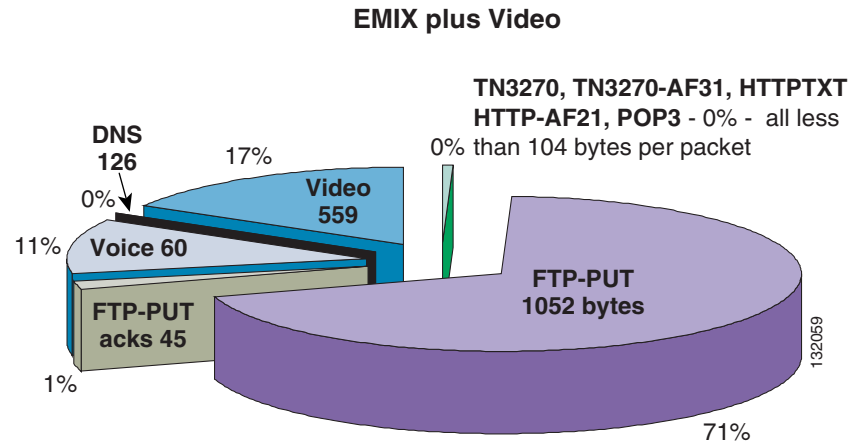
Shown in Figure 10-2 is a representation of the traffic flow used in these tests. The branch to head-end flows are shown. The head-end to branch flows are similar in percentages. The average packet size is shown for the respective categories.



### Note

The Cisco 6729 IP Phone was used for voice and NetMeeting for video only (no audio).

Figure 10-2 Traffic Profile—Branch to Head-end



Note that in this traffic profile, the QoS service policy is provisioned for voice and video in percentages of link bandwidth:

```
class VOICE
  priority percent 18

class VIDEO-CONFERENCING
  priority percent 15
```

The Call Admission Control parameters for this test limit the number of concurrent voice calls to less than 18 percent of the available bandwidth, and the data rate of the video stream is sufficient for the allocated bandwidth. In the test results documented in this chapter, the number of concurrent G.729 voice calls is eight. At approximately 56 kbps per call, the priority queue should have at least 448 kbps ( $56 * 8$ ).

```
vpn-jk2-3725-4#show policy-map interface multilink 2 out class VOICE
Multilink2
Service-policy output: V3PN_Branch

Class-map: VOICE (match-all)
 96040 packets, 8450920 bytes
 30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp ef
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 18 (%)
  Bandwidth 468 (kbps) Burst 11700 (Bytes)
  (pkts matched/bytes matched) 96041/13445040
  (total drops/bytes drops) 0/0
```

Calculating an adequate size of the priority (LLQ) queue for encrypted video is not as straightforward as for voice. Where voice packets are a fixed size, video packets can vary in size. As such, the crypto overhead as a percentage of the unencrypted video packet varies based on the size of the packet. Smaller packets have a higher percentage of crypto overhead than do large packets.

The rule of thumb for provisioning the video LLQ requirements is to add 20 percent to the configured video data rate. Table 10-1 illustrates the crypto overhead associated with the packet size distribution of a typical video stream.

**Table 10-1 V3PN—Video Provisioning**

Packet size distribution (bytes) <sup>1</sup>	% of Packets <sup>2</sup>	Assuming video packet of N bytes	IPSec tunnel mode and GRE byte increase	Percent increase
1025–1518	37%	1025	1104	8%
513–1024	20%	513	592	15% <sup>3</sup>
257–512	8%	257	336	31%
129–256	34%	129	208	61%

1. Rule of Thumb: Video LLQ provisioned at rate plus 20%
2. Rule of Thumb: Video LLQ provisioned at rate plus 20%
3. Assuming an average packet size between 500–600 bytes

The Chariot video stream simulated a 256 kbps video stream. Given that the average packet size in that stream falls between 500 to 600 bytes, the crypto overhead can be assumed to be approximately 15 percent. Adding 15 percent crypto overhead to the video stream and then adding 20 percent to accommodate video bursts, you should allocate at least 353 kbps. In testing, the recommended 15 percent bandwidth allocation for the 2.6 M link is 390 kbps, which is sufficient for the 256 kbps video stream.

```
vpn-jk2-3725-4# show policy-map interface multilink 2 out class VIDEO-CONFERENCING
Multilink2
```

```
Service-policy output: V3PN_Branch
```

```
Class-map: VIDEO-CONFERENCING (match-all)
 0 packets, 0 bytes
 30 second offered rate 0 bps, drop rate 0 bps
Match: ip dscp af41
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 15 (%)
  Bandwidth 390 (kbps) Burst 9750 (Bytes)
  (pkts matched/bytes matched) 0/0
  (total drops/bytes drops) 0/0
```

In testing, this proved to be an acceptable allocation for the video stream. Note that both the VOICE and VIDEO-CONFERENCING display show the same Output Queue Conversation number of 264. There is only one Strict Priority queue. Although voice and video are provisioned separately, they share the same queue. For this reason, interactive video conferencing is not recommended on link speeds that have serialization (blocking) delay issues; namely, links below 768 kbps.

## V3PN QoS Service Policy

The configuration was coded with an absolute **bandwidth 2600** and **ppp multilink links minimum 2**, assuming that a backup router and pair of T1s would be deployed.

Be advised, however, that the bandwidth of the multilink interface is derived from the sum of the bandwidth of the active member links, and the QoS service policy calculates the actual bandwidth by multiplying the configured percentages by the derived multilink interface bandwidth. The given voice is shown as 33 percent of 2,600,000, or 858 kbps.

```
vpn-jk2-3725-4#show policy int multilink 2 | inc Class-map|Bandwidth
  Class-map: CALL-SETUP (match-any)
    Bandwidth 2 (%)
    Bandwidth 52 (kbps) Max Threshold 64 (packets)
  Class-map: INTERNETWORK-CONTROL (match-any)
    Bandwidth 5 (%)
    Bandwidth 130 (kbps) Max Threshold 64 (packets)
  Class-map: VOICE (match-all)
    Bandwidth 33 (%)
    Bandwidth 858 (kbps) Burst 21450 (Bytes)
  Class-map: TRANSACTIONAL-DATA (match-all)
    Bandwidth 22 (%)
    Bandwidth 572 (kbps) Max Threshold 64 (packets)
  Class-map: class-default (match-any)
```

The bandwidth values above are calculated from the derived multilink bandwidth:

```
vpn-jk2-3725-4#show int multilink 2 | inc BW
  MTU 1500 bytes, BW 2600 Kbit, DLY 100000 usec,
```

The multilink bandwidth is derived from the member links, which in this case are two serial interfaces:

```
vpn-jk2-3725-4#show interface serial 1/0 | inc BW
  MTU 1500 bytes, BW 1300 Kbit, DLY 20000 usec,
vpn-jk2-3725-4#show interface serial 1/1 | inc BW
  MTU 1500 bytes, BW 1300 Kbit, DLY 20000 usec,
```

If the second T1 is installed for availability rather than capacity, it is better to specify the voice and video bandwidth of the LLQ in absolute kbps values rather than a percentage.

For testing, three QoS service polices were tested. The legend on the chart lists them as default WRED, Tuned WRED, and Voice + Video Tuned WRED. These test iterations and their policy map configurations are shown in [Table 10-2](#):

**Table 10-2** QoS Service Policy Testing

Test Iteration	Policy Map
Default WRED	<pre> policy-map V3PN_Branch   class CALL-SETUP     bandwidth percent 2   class INTERNETWORK-CONTROL     bandwidth percent 5   class VOICE     priority percent 33   class TRANSACTIONAL-DATA     bandwidth percent 22   class class-default     fair-queue     random-detect </pre>
Tuned WRED	<pre> policy-map V3PN_Branch   class CALL-SETUP     bandwidth percent 2   class INTERNETWORK-CONTROL     bandwidth percent 5   class VOICE     priority percent 33   class TRANSACTIONAL-DATA     bandwidth percent 22   class class-default     fair-queue     random-detect dscp-based     random-detect dscp 0 4 10 10 </pre>
Voice + Video Tuned WRED	<pre> policy-map V3PN_Branch   class CALL-SETUP     bandwidth percent 2   class INTERNETWORK-CONTROL     bandwidth percent 5   class VOICE     priority percent 18   class TRANSACTIONAL-DATA     bandwidth percent 22   class VIDEO-CONFERENCING     priority percent 15   class class-default     fair-queue     random-detect dscp-based     random-detect dscp 0 4 10 10 </pre>

The rationale for testing the tuned Weighted Random Early Detection (WRED) was to apply the concept originally tested in the *Voice and Video Enabled IPsec VPN (V3PN) Design Guide*, where IPsec anti-replay drops were reduced by decreasing the queue-limit in the individual bandwidth classes from a default of 64 packets to much lower values.

**Note**

See the *Voice and Video Enabled IPsec VPN (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).

Because the **queue-limit** command is not germane with WRED enabled, the minimum and maximum thresholds for the best effort traffic in class default. The command format is the following:

```
random-detect dscp dscpvalue min-threshold max-threshold [mark-probability-denominator]
```

As can be seen in [Table 10-2](#), the min-threshold was set at 4 packets, max-threshold was set at 10 packets, and the default of .1 or 10 percent was not changed.

With WRED enabled but using default values, no drops were encountered on the output service policy, with the min-threshold at 4 and max-threshold at 10. In general, the anti-replay drops decreased slightly and output interface queue drops were registered.

However, it is important to note that anti-replay drops on all tests, using Multilink PPP or Inverse Multiplexing over ATM (IMA) were always less than 1 percent of packets decrypted given these link speeds of 2.6–3 M. In these tests, the priority or LLQ does not exceed 33 percent of the link.

[Table 10-3](#) shows the relevant performance metrics:

**Table 10-3 Performance Metrics**

Cisco 3725 Multilink PPP 2 links 2.6 Mbps total	Voice milliseconds <sup>1</sup>		Number data		CPU
	Jitter (goal <8)	Latency (goal < 50)	G.729 Calls	Mbps in/out	
Default WRED	2.4	7.9	15	2.4 M	28%
Tuned WRED	2.5	6.3	15	2.5 M	28%
Voice + Video Tuned WRED	2.3	6.7	8	3.4 M <sup>2</sup>	21%

1. Branch to Head and Head to Branch values are averaged
2. Video included in data Mbps values

In all three tests, voice jitter and latency was well below the testing goal of 8 ms and 50 ms respectively. Voice lost is not shown, but was approaching 0 percent in all tests.

The hardware encryption acceleration module was an AIM-VPN/EPII VPN Hardware Module. The router had 248832K/13312K bytes of memory.

## Implementation and Configuration

This section describes the configuration for the components of the Multilink PPP solution, and includes the following sections:

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

### Remote Router

Following is the remote router configuration:

```
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
```

```

hostname vpn-jk2-3725-3
!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-6
boot-end-marker
!
enable secret 5 [removed]
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
ip host ect-msca 172.26.179.237
ip host harry 172.26.176.10
!
ip audit po max-events 100
no ftp-server write-enable
!
!
class-map match-all VOICE
  match ip dscp ef
class-map match-all VIDEO-CONFERENCING
  match ip dscp af41
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
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
!
policy-map V3PN_Branch
  class CALL-SETUP
    bandwidth percent 2
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class VOICE
    priority percent 18          # See previous section for changes between test iterations
  class TRANSACTIONAL-DATA
    bandwidth percent 22
  class VIDEO-CONFERENCING
    priority percent 15
  class class-default
    fair-queue
    random-detect dscp-based
    random-detect dscp 0 4 10 10
!
!
!
crypto isakmp policy 20
  encr 3des

```



```

authentication pre-share
group 2
crypto isakmp keepalive 10
!
crypto isakmp peer address 192.168.255.3
set aggressive-mode password 77-80-69_24.1_WW-748
set aggressive-mode client-endpoint fqdn Store_223.eso.cisco.com
crypto isakmp profile AGGRESSIVE
description _
self-identity fqdn
match identity host domain eso.cisco.com
initiate mode aggressive
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto map PRIMARY_LINK 1 ipsec-isakmp
description Crypto Map for Primary Path
set peer 192.168.255.3
set transform-set 3DES_SHA_TUNNEL
match address GRE_MAP_ACL
qos pre-classify
!
interface Loopback0
description lo0
ip address 10.0.80.254 255.255.255.255
!
interface Multilink2
description Multilink2
bandwidth 2600 # See V3PN Service Policy Section
ip address 192.168.193.18 255.255.255.252
service-policy output V3PN_Branch
ip route-cache flow
load-interval 30
ppp multilink
ppp multilink slippage msec 26
ppp multilink links minimum 2
ppp multilink group 2
crypto map PRIMARY_LINK
!
interface Tunnel0
description Tunnel0 # Note no crypto map on Tunnel interface
ip address 10.0.80.250 255.255.255.252
qos pre-classify
keepalive 10 3 # No routing protocol configured,
# rather GRE keepalive
!
tunnel source Loopback0
tunnel destination 192.168.255.3
!
interface FastEthernet0/1
description FastEthernet0/1
no ip address
ip route-cache flow
load-interval 30
duplex auto
speed auto
!
interface FastEthernet0/1.212
description FastEthernet0/1.212
encapsulation dot1Q 212
ip address 10.0.80.1 255.255.255.128
!
interface Serial1/0

```

```

description Serial1/0
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 2
!
interface Serial1/1
description Serial1/1
no ip address
encapsulation ppp
ppp multilink
ppp multilink group 2
!
ip http server
no ip http secure-server
ip classless
!      No routing protocol configured on this router.
ip route 0.0.0.0 0.0.0.0 Multilink2 249
ip route 10.3.0.0 255.255.255.128 Tunnel0 237
!
ip access-list extended CRYPTO_MAP_ACL
permit ip 10.0.80.0 0.0.0.127 any
ip access-list extended GRE_MAP_ACL
permit gre host 10.0.80.254 host 192.168.255.3
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp
!
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!
!
line con 0
exec-timeout 120 0
transport preferred all
transport output all
line aux 0
transport preferred all
transport output all
line vty 0 4
password 7 [removed]
login
transport preferred all
transport input all
transport output all
!
ntp source FastEthernet0/1.212
!
end

```

## Head-end Router

Following is the head-end router configuration:

```

version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname vpn-jk2-3725-4

```

```

!
boot-start-marker
boot system flash:c3725-ik9o3s-mz.123-6
boot-end-marker
!
enable secret 5 [removed]
!
clock timezone est -5
clock summer-time edt recurring
no network-clock-participate slot 1
no network-clock-participate slot 2
no network-clock-participate wic 0
no network-clock-participate wic 1
no network-clock-participate wic 2
no network-clock-participate aim 0
no network-clock-participate aim 1
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
ip domain name ese.cisco.com
ip host ect-msca 172.26.179.237
ip host harry 172.26.176.10
!
ip audit po max-events 100
no ftp-server write-enable
!
!
class-map match-all VOICE
  match ip dscp ef
class-map match-all VIDEO-CONFERENCING
  match ip dscp af41
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
class-map match-all TRANSACTIONAL-DATA
  match ip dscp af21
!
!
policy-map V3PN_Branch          # See comments in remote router's policy-map configuration
  class CALL-SETUP
    bandwidth percent 2
  class INTERNETWORK-CONTROL
    bandwidth percent 5
  class VOICE
    priority percent 18
  class TRANSACTIONAL-DATA
    bandwidth percent 22
  class VIDEO-CONFERENCING
    priority percent 15
  class class-default
    fair-queue
    random-detect dscp-based
    random-detect dscp 0 4 10 10
!
!
crypto keyring Purple_Stores
pre-shared-key hostname Store_223.ese.cisco.com key 77-80-69_24.1_WW-748
!
crypto isakmp policy 20

```

```

encr 3des
authentication pre-share
group 2
crypto isakmp keepalive 10
crypto isakmp profile AGGRESSIVE
    description _
    keyring Purple_Stores
    self-identity fqdn
    match identity host domain ese.cisco.com
!
!
crypto ipsec transform-set 3DES_SHA_TUNNEL esp-3des esp-sha-hmac
no crypto ipsec nat-transparency udp-encaps
!
crypto dynamic-map DYNO-TEMPLATE 10    # Dynamic Crypto Maps with GRE and IKE Aggressive
description dynamic crypto map        # mode in this configuration
set transform-set 3DES_SHA_TUNNEL
qos pre-classify
!
!
crypto map DYNO-MAP local-address Loopback0
crypto map DYNO-MAP 10 ipsec-isakmp dynamic DYNO-TEMPLATE
!
!
!
interface Loopback0
description lo0
ip address 192.168.255.3 255.255.255.255
!
interface Multilink2
description Multilink2
bandwidth 2600
ip address 192.168.193.17 255.255.255.252
service-policy output V3PN_Branch
ip route-cache flow
load-interval 30
ppp multilink
ppp multilink slippage msec 26
ppp multilink links minimum 2
ppp multilink group 2
crypto map DYNO-MAP
!
interface Tunnel0
description Tunnel0
ip address 10.0.80.249 255.255.255.252
qos pre-classify
keepalive 10 3
tunnel source Loopback0
tunnel destination 10.0.80.254
!
interface FastEthernet1/0
description dot1q
no ip address
ip route-cache flow
load-interval 30
duplex auto
speed auto
!
interface FastEthernet1/0.128
encapsulation dot1Q 128
ip address 10.2.128.3 255.255.255.0
!
interface Serial1/0
description Serial1/0

```

```

no ip address
encapsulation ppp
clockrate 1300000
ppp multilink
ppp multilink group 2
!
interface Serial1/1
description Serial1/1
no ip address
encapsulation ppp
clockrate 1300000
ppp multilink
ppp multilink group 2
!
router eigrp 100
redistribute static metric 2600 1000 255 1 1500 route-map PERMIT_80
network 10.0.0.0
!
# We should have included a passive interface command
# because we are not expecting to form a neighbor relationship
!
# across the GRE tunnel
distribute-list 10 in FastEthernet1/0.128
no auto-summary
no eigrp log-neighbor-warnings
!
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 Multilink2 249
ip route 10.0.80.0 255.255.255.128 Tunnel0 237
!
!
!
ip access-list extended IKE
permit udp any eq isakmp any eq isakmp
access-list 10 permit 10.3.0.0
access-list 10 deny any
access-list 80 permit 10.0.80.0
!
route-map PERMIT_80 permit 10
description To only allow 10.0.80.0/24
match ip address 80
!
snmp-server community private RW
snmp-server community public RO
snmp-server system-shutdown
snmp-server enable traps tty
!
!
line con 0
exec-timeout 120 0
transport preferred all
transport output all
line aux 0
transport preferred all
transport output all
line vty 0 4
password 7 [removed]
login
transport preferred all
transport input all
transport output all
!
ntp server 192.168.130.1
!

```

```
end
```

## Show Commands

According to the interface counters, the interface is running in the 80–84 percent utilization range with a load interval of 30 seconds.

```
Multilink2 is up, line protocol is up
Hardware is multilink group interface
Description: Multilink2
Internet address is 192.168.193.18/30
MTU 1500 bytes, BW 2600 Kbit, DLY 100000 usec,
    reliability 255/255, txload 207/255, rxload 214/255
Encapsulation PPP, LCP Open, multilink Open
Open: CDPCP, IPCP, loopback not set
DTR is pulsed for 2 seconds on reset
Last input 00:00:07, output never, output hang never
Last clearing of "show interface" counters 00:02:25
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1570
Queueing strategy: weighted fair
Output queue: 6/1000/64/1570 (size/max total/threshold/drops)
  Conversations 1/4/256 (active/max active/max total)
  Reserved Conversations 3/3 (allocated/max allocated)
  Available Bandwidth 338 kilobits/sec
30 second input rate 2185000 bits/sec, 683 packets/sec
30 second output rate 2111000 bits/sec, 682 packets/sec
99861 packets input, 39534594 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
100101 packets output, 39145904 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
0 carrier transitions
```

```
show policy int
Multilink2
```

```
Service-policy output: V3PN_Branch

Class-map: CALL-SETUP (match-any)
  0 packets, 0 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
    0 packets, 0 bytes
    30 second rate 0 bps
  Queueing
    Output Queue: Conversation 265
    Bandwidth 2 (%)
    Bandwidth 52 (kbps) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

Class-map: INTERNETWORK-CONTROL (match-any)
  76 packets, 7664 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: ip dscp cs6
```

```

    76 packets, 7664 bytes
    30 second rate 0 bps
Match: access-group name IKE
    0 packets, 0 bytes
    30 second rate 0 bps
Queueing
  Output Queue: Conversation 266
  Bandwidth 5 (%)
  Bandwidth 130 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 15/1256
  (depth/total drops/no-buffer drops) 0/0/0

Class-map: VOICE (match-all)
  58160 packets, 5118080 bytes
  30 second offered rate 282000 bps, drop rate 0 bps
Match: ip dscp ef
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 18 (%)
  Bandwidth 468 (kbps) Burst 11700 (Bytes)
  (pkts matched/bytes matched) 58152/8141280
  (total drops/bytes drops) 0/0

Class-map: TRANSACTIONAL-DATA (match-all)
  278 packets, 162904 bytes
  30 second offered rate 10000 bps, drop rate 0 bps
Match: ip dscp af21
Queueing
  Output Queue: Conversation 267
  Bandwidth 22 (%)
  Bandwidth 572 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 278/178472
  (depth/total drops/no-buffer drops) 0/0/0

Class-map: VIDEO-CONFERENCING (match-all) # See Caveats in this section!
  8746 packets, 5133902 bytes
  30 second offered rate 252000 bps, drop rate 9000 bps
Match: ip dscp af41
Queueing
  Strict Priority
  Output Queue: Conversation 264
  Bandwidth 15 (%)
  Bandwidth 390 (kbps) Burst 9750 (Bytes)
  (pkts matched/bytes matched) 8746/5632424
  (total drops/bytes drops) 630/405720

Class-map: class-default (match-any)
  34005 packets, 24847658 bytes
  30 second offered rate 1404000 bps, drop rate 51000 bps
Match: any
Queueing
  Flow Based Fair Queueing
  Maximum Number of Hashed Queues 256
  (total queued/total drops/no-buffer drops) 2/962/0
  exponential weight: 9

dscp      Transmitted      Random drop      Tail drop      Minimum Maximum Mark
          pkts/bytes        pkts/bytes        pkts/bytes      thresh  thresh prob
af11      0/0                0/0                0/0              32     40  1/10
af12      0/0                0/0                0/0              28     40  1/10
af13      0/0                0/0                0/0              24     40  1/10
af21      0/0                0/0                0/0              32     40  1/10
af22      0/0                0/0                0/0              28     40  1/10

```

af23	0/0	0/0	0/0	24	40	1/10
af31	0/0	0/0	0/0	32	40	1/10
af32	0/0	0/0	0/0	28	40	1/10
af33	0/0	0/0	0/0	24	40	1/10
af41	0/0	0/0	0/0	32	40	1/10
af42	0/0	0/0	0/0	28	40	1/10
af43	0/0	0/0	0/0	24	40	1/10
cs1	0/0	0/0	0/0	22	40	1/10
cs2	0/0	0/0	0/0	24	40	1/10
cs3	0/0	0/0	0/0	26	40	1/10
cs4	0/0	0/0	0/0	28	40	1/10
cs5	0/0	0/0	0/0	30	40	1/10
<b>cs6</b>	<b>23/2912</b>	0/0	0/0	32	40	1/10
cs7	0/0	0/0	0/0	34	40	1/10
ef	0/0	0/0	0/0	36	40	1/10
rsvp	0/0	0/0	0/0	36	40	1/10
<b>default</b>	<b>33049/25916882</b>	<b>963/825988</b>	0/0	4	10	1/10

See caveats following this section.

## Cisco IOS Versions Tested

The following Cisco IOS version was tested: Cisco 3725—c3725-ik9o3s-mz.123-6

## Caveats

This section describes the caveats to the Multilink PPP solution, and includes the following topics:

- [Drops In Class VIDEO-CONFERENCEING](#)
- [Incorrect Packet Classification](#)

## Drops In Class VIDEO-CONFERENCEING

In [Show Commands, page 10-14](#), packet loss in the video class was observed during performance testing. Upon further analysis and testing, it was determined that the drops resulted from a testing anomaly and not a Cisco IOS or configuration issue. Recall from the previous discussion on the Chariot video test stream that the size of the stream was configured at 2,088,000 bytes. At the 256 kbps data rate, this simulates a video conference that has a duration of approximately one minute. Chariot then restarts the simulated video stream and then again the second stream lasts approximately one minute. This sequence of events continues for the duration of the test. For a ten minute test, there might be 9–10 individual video streams during the test.

The packet loss experienced occurred at the end of the Chariot stream. In most cases, for the duration of the test, the video packet loss ranged from 3–7 percent. After this behavior was determined, the size of the Chariot video stream was increased to simulate a video conference that would last the duration of the test. In this mode, the video packet loss was negligible. The packet loss goal for an interactive video conference is less than 1 percent.

```
vpn-jk2-3725-4#sh pol int mu 2 output class VIDEO-CONFERENCEING
Multilink2
```

```
Service-policy output: V3PN_Branch
```



```
Class-map: VIDEO-CONFERENCING (match-all)
  19163 packets, 11245772 bytes
  30 second offered rate 252000 bps, drop rate 1000 bps
  Match: ip dscp af41
  Queueing
    Strict Priority
    Output Queue: Conversation 264
    Bandwidth 15 (%)
    Bandwidth 390 (kbps) Burst 9750 (Bytes)
    (pkts matched/bytes matched) 19168/12338456
    (total drops/bytes drops) 16/10304
```

The 16 packets dropped in this test all occurred in the last few seconds of the video stream when the session was closing, so this loss behavior is thus marked against the test tool and is not an issue with Cisco IOS or configuration.

## Incorrect Packet Classification

In [Show Commands, page 10-14](#), the QoS service policy includes a class for INTERNETWORK-CONTROL that includes a match for a Differentiated Services Code Point (DSCP) value of CS6. Note that in the same display under class class-default, the WRED display indicates there are matches for CS6. This is a classification issue because these packets are in class default and not in the bandwidth class INTERNETWORK-CONTROL.

## Summary

This chapter includes performance results and configuration examples for features that have not been tested to date. These include interactive video conferencing in the traffic profile and the use of Multilink PPP for data rates above E1 but less than T3. WRED has also been included in class default, where the initial V3PN site-to-site testing used a fair queue configuration. Tuning the WRED parameters was also tested. Although various router hardware platforms were not exhaustively tested (only the Cisco 3725 was tested), the viability of encrypted voice and video was demonstrated. Also, note that the incidence of anti-replay drops in a higher data rate multilink configuration exhibits similar characteristics to the sub-E1/T1 rates previously tested.

