CHAPTER 6

Implementation and Configuration

This chapter provides step-by-step examples of how to configure the IP Video Surveillance environment tested by Cisco Enterprise Solutions Engineering (ESE) and contains the following main sections:

- Deploying Network Services for IP Video Surveillance, page 6-1
- Deploying a Cisco Video Surveillance IP Camera, page 6-13
- Deploying a Cisco Video Surveillance IP Camera, page 6-13
- Configuring Quality-of-Service (QoS) for IP Video Surveillance, page 6-21
- Local Storage for Video Archives Using iSCSI, page 6-41
- Performance Routing (PfR) Integration, page 6-50
- Wide Area Application Services (WAAS) Integration, page 6-61
- Wide Area Application Services (WAAS) for iSCSI, page 6-74
- Controlling Access to IP Video Surveillance, page 6-80
- Virtualization, Isolation and Encryption of IP Video Surveillance, page 6-87

Note that not every section in this chapter is necessary in all implementations. The recommendation is to read each section and then decide if the concepts in a particular section are relevant or important to the target implementation. For example, some implementations may not have the required topology to implement Performance Routing (PfR), however, this section contains a discussion and examples of how latency, jitter, and packet loss may impact the quality of video feeds on any topology. In this case, the background assumptions may be relevant general knowledge to the network manager, even if the technology approach is not implemented.

Many of the topics and concepts in this chapter are not specific to IP video surveillance deployments, while the discussion in this chapter focus on their relevance to video surveillance. Additional information is available in associated design guides or documentation at the following Cisco website http://www.cisco.com.

Deploying Network Services for IP Video Surveillance

This section discusses how various network services on the IP network can be integrated into an IP video surveillance deployment. The services include the following:

- Time Synchronization using Network Time Protocol, page 6-2
- Syslog, page 6-8
- Cisco IOS IP Service Level Agreements (SLAs), page 6-9

- Power-Over-Ethernet (PoE), page 6-11
- Cisco Discovery Protocol (CDP), page 6-12
- Simple Network Management Protocol, page 6-13

Time Synchronization using Network Time Protocol

The Network Time Protocol (NTP) is a protocol designed to synchronize the clocks of network nodes of an IP network with a reliable time source. NTP version 3 is defined in RFC-1305. The Cisco Video Surveillance Manager solution relies on NTP to synchronize the time of the servers, IP cameras and viewing stations. There are a number of third-party appliances which use GPS receivers as an accurate timing source.

The GPS receiver appliance requires line-of-sight to the sky for receiving the GPS signals. At least 4 satellites must be acquired for GPS time. To accomplish this the server is attached by a coax cable to a building exterior antenna. These servers are typically one rack unit high, have a RS-232 console port, Ethernet port and coax connection for the antenna. They are a stratum one time source and are capable of providing time synchronization accurate to within 1 to 5 milliseconds. The stratum levels refer to the distance (in number of servers) from the reference clock. Lower number is more preferred.

Also, CDMA signals, used by digital cellular telephones, can be used as a timing source. Code Division Multiple Access (CDMA)-based stations act as GPS repeaters. These signals are more readily received inside buildings. These may be an option due to the facility costs of connecting the NTP appliance to the exterior antenna.

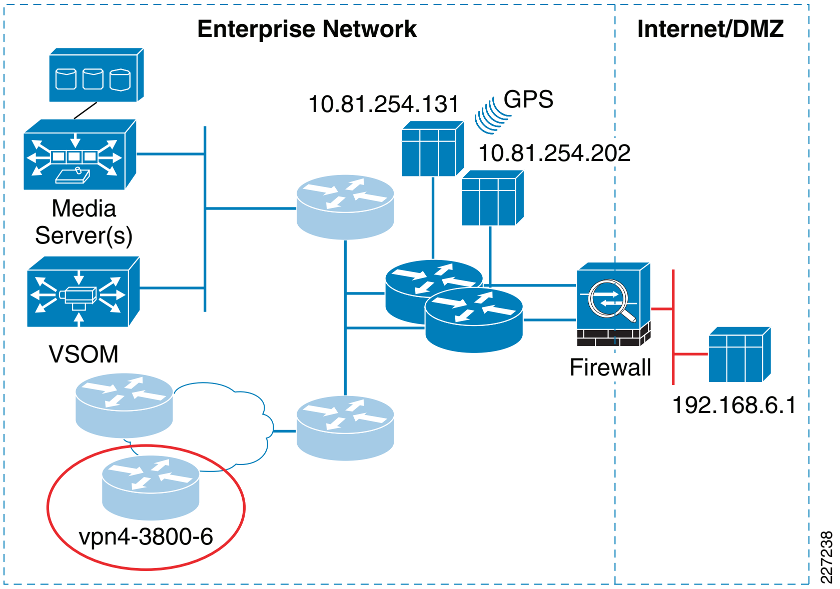
The advantage of using an enterprise owned GPS-based time server is reliability and availability. It is recommended that two of these servers be installed at diverse points in the network topology so one server remains accessible to the network in the event of a single data center disaster. Ideally, they would be located at multiple data centers or other core locations and provide the same degree of network redundancy as other network management and servers.

Topology

The topology (see Figure 1) in this chapter shows a sample configuration where the network manager has one or more time sources available in the internal network address space (10.81.254.0/24 in this example) and one or more time sources on public address space, represented by 192.168.0.0/16. The servers on the internal address space are stratum 1 sources. The server on the public address space (Internet DMZ) is a stratum 2 source referencing a clock source of the Naval Observatory (USNO) NTP servers.

The sample configuration is from a branch router configured as a stratum 12 NTP server, providing a time source to the IP cameras, Cisco Video Management and Storage System (VMSS), and the optional Analog Video Gateway Module. The branch router references lower stratum servers, the configured stratum 1 and 2 servers, and under normal operations will prefer these lower stratum source over its own internal clock.

Figure 1 Network Time Protocol Reference Topology



This design includes several advantages and best practices. By peering the routers in the network with the NTP servers rather than all devices in the network, it minimizes the polling to the servers. In a highly available network, the routers only generate a NTP poll request every 17 minutes. Because the routers have an accurate time source from the NTP servers, they are able to provide an accurate time source for hosts on their connected interfaces. This adds a level of hierarchy in the NTP deployment and can scale to very large enterprise networks.

Additionally, the design incorporates one or more internal GPS-based NTP appliances inside the enterprise firewall from the Internet. The NTP appliance (or router) located in the Internet/DMZ can be configured to peer to the internal NTP appliances (with the appropriate firewall rule allowing this inbound connection) as well as to NTP servers on the public Internet. The NTP appliance in the Internet/DMZ can also serve as a time source for remote access clients and broadband routers supporting enterprise teleworker or remote users.

By configuring the internal routers to also peer to the Internet/DMZ NTP appliance, a third-time source (although at a higher stratum) can be obtained from a publicly available server from the Naval Observatory (USNO).

Basic Router Configuration

The basic configuration of each router on the enterprise network is to specify in the configuration a **ntp master** statement with a stratum 12 value, and then reference one or more NTP appliances within the enterprise network and a router or NTP appliances on the Internet/DMZ.

```
ntp master 12
ntp server 192.168.6.1 source {source IP address}
ntp server 10.81.254.202 source {source IP address}
ntp server 10.81.254.131 source {source IP address}
```

The source IP address is optional but may be specified.

Note LAN switches in the network should also use the nearest router as their configured NTP server.

Tips and Additional Useful Information

NTP is transported by the UDP protocol and port 123. The size of the packets, including the IP header, is approximately 76 bytes. Cisco IOS sets the ToS byte in the IP header with an IP Precedence of '6' (DSCP CS6) for NTP packets.

NTP is VRF-aware and can configured to reference a VRF instance, using VRF IPVS as an example, **ntp server vrf IPVS** *{ip_address}* associates the NTP address with the appropriate VRF table.

NTP does not *converge* quickly to an alternate peer upon failure of the current master (synched) peer. This is by design and the expected behavior of NTP. It requires multiple comparisons over long periods for accurate clock synchronization.

The Cisco IOS implementation of the NTP client polls the configured servers between 64 seconds and up to 1024 seconds (over 17 minutes). When the peer is first configured, 16 polls are generated initially. After the first 64 second interval, if the poll is answered with a valid time source reply, the interval is incremented. The interval increases (or decreases) in powers of 2; for example, 64,128,256,512,1024 seconds. In a stable network, the poll interval is usually 1024 seconds.

However, not all network devices implement this backoff algorithm. For example, IP cameras may contact their configured NTP server on a polling interval based on the 64 second interval and never increase the polling interval.

Do not configure the **ntp clock-period** command when cutting and pasting from one router configuration to another. The system calculates the value on its own and includes it in the running configuration. The system may go out of synch if the user manually configures the **ntp clock-period** command. If it is manually configured, configure a **no ntp clock-period** command and reload the router so the value can be recalculated.

Output from **show ntp associations** command is shown and explained below.

```
vpn4-3800-6#show ntp associations

      address         ref clock     st  when  poll reach  delay  offset    disp
 ~127.127.7.1      127.127.7.1      11     1    64  377     0.0    0.00     0.0
+~192.168.6.1      .USNO.            2   444  1024  377     2.2   -2.83     0.9
*~10.81.254.202    .GPS.             1   350  1024  377     7.7    0.94     3.0
+~10.81.254.131    .GPS.             1   810  1024  377    18.6    6.49     2.1
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

- *st*—Stratum, number of levels from the time source
- *when*—Number of seconds since last ntp request was sent to this server
- *poll*—Number of seconds between ntp requests with this server
- *reach*—Bitmap represented in octal of last 8 ntp responses that were received from the NTP server for the last 8 ntp requests sent
- *delay*—Round trip delay to the reference clock in milliseconds
- *offset*—Amount to adjust our clock to correspond with the reference in milliseconds, can be negative
- *disp*—The maximum error between the local clock and the reference, in milliseconds

If the *reach* value is anything other than 377, NTP packets have been dropped by the network or server during the last 8 attempts.

NTP servers keep time in Universal Time (UTC), and each device on the network must be configured for the proper geographical time zone. The conversion to the proper local time is handled by the operating system of each device. Greenwich Mean Time (GMT), Greenwich Time and Zulu Time refer to UTC.

Sample ISR Router and VMSS Configuration

The branch router is configured to contact the internal servers, 10.81.254.202 and 10.81.254.101, sourced from the IP interface representing the inside VLAN of the branch. The external NTP server at 192.168.6.1 is sourced from the outside or WAN interface.

```
vpn4-3800-6#show run | inc ntp
ntp source Integrated-Service-Engine2/0
ntp master 12
ntp server 192.168.6.1 source GigabitEthernet0/0.150
ntp server 10.81.254.202 source Vlan1
ntp server 10.81.254.131 source Vlan1
```

The ISR router is configured as an NTP master with a stratum of 12. The NTP master stratum number identifies the relative position of this router in the NTP hierarchy. Higher numbers are less preferred sources. This router is configured to serve as a master and will provide an accurate time source to the VMSS and IP cameras and other hosts that request synchronization. Configuring the branch router as an NTP server provides a time source to the branch devices in the event WAN connectivity is disrupted and lower stratum devices are unreachable.

In this illustration, the NTP source address is Integrated-Service-Engine2/0 or IP address of 192.0.2.33, the address of the VMSS module. A loopback address of the router could also be used to source replies to client NTP packets. A loopback address would be preferred, this implementation did not provide for loopback addresses and the logical interface of the VMSS network module is used as an alternative.

Client workstations, IP cameras and other devices on the network may use any of the IP addresses associated with the router as a NTP peer IP address in their configuration, they need not only use the value specified by the **ntp source** configuration command.

The following configuration example shows the network administrator establishing a console session the VMSS network module in this ISR router, and showing that the configuration of Linux kernel on the VMSS module is using the host ISR router as a NTP peer.

```
vpn4-3800-6#sh run interface integrated-Service-Engine 2/0
Building configuration...
!
interface Integrated-Service-Engine2/0
 ip address 192.0.2.33 255.255.255.252
 ip route-cache flow
 service-module ip address 192.0.2.34 255.255.255.252
 service-module ip default-gateway 192.0.2.33
 no keepalive
end
```

The module is configured to use IP address 192.0.2.33, the IP address of the router hosting the VMSS module. These commands establish a console session to the network module operating system and displays the running configuration.

```
vpn4-3800-6#service-module integrated-Service-Engine 2/0 sess
Trying 192.0.2.33, 2130 ... Open
SITE150> en
Password:
SITE150#
SITE150# show run
Generating configuration:

clock timezone America/New_York
hostname SITE150
ip domain-name ese.cisco.com
system language preferred "en_US"
ntp server 192.0.2.33 prefer
```

Only one NTP server need be specified (192.0.2.33), because this is the IP address of the ISR router that is configured for more than one NTP server in the router configuration in addition to also being configured as an NTP master should connectivity to the lower stratum servers be lost. Note the time zone is also manually configured, as NTP exchanges time in UTC.

The NTP server associations from the VMSS network module may be displayed. The reference server (*refid*) is the time source from one of the enterprise network NTP sources, referenced in in the router configuration.

```
SITE150# show ntp servers
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.33      10.81.254.202    2 u  556 1024  377    1.687   -0.445   0.008
space reject,       x falsetick,       . excess,          - outlyer
+ candidate,        # selected,        * sys.peer,        o pps.peer
```

In the event network connectivity is disrupted, making the reference source unreachable, the branch router itself would be the reference clock. The NTP source at 10.81.254.202 is the current reference because the branch router has synched to that time source, indicated by the asterick ("*") next to the IP address.

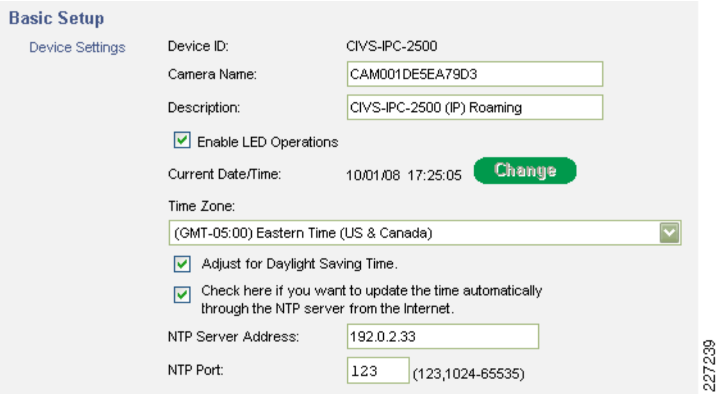
Sample IP Camera Configuration

This section illustrates the router and an IP camera configuration. The IP address of the default router in the IP configuration of the camera can also be used as the NTP server IP address if the router is configured per the recommended design. Assuming the default router is configured on the subnet of the IP camera is configured as follows:

```
router#sh run | inc ntp
ntp source Integrated-Service-Engine2/0
ntp master 12
ntp server 192.168.6.1 source GigabitEthernet0/0.150
ntp server 10.81.254.202 source Vlan1
ntp server 10.81.254.131 source Vlan1
!
interface GigabitEthernet0/1.210
 description IP Camera VLAN
 encapsulation dot1Q 210
 ip vrf forwarding IPVS
 ip address 192.0.2.97 255.255.255.224
end
```

The configuration of the IP camera can reference the NTP server as the same IP address as the default gateway for this camera, 192.0.2.97. The NTP port is not changed from the default port 123.

Figure 2 NTP Configuration for Cisco 2500 series IP Camera



Basic Setup

Device Settings

Device ID: CIVS-IPC-2500

Camera Name: CAM001DE5EA79D3

Description: CIVS-IPC-2500 (IP) Roaming

☑ Enable LED Operations

Current Date/Time: 10/01/08 17:25:05 Change

Time Zone:

(GMT-05:00) Eastern Time (US & Canada)

☑ Adjust for Daylight Saving Time.

☑ Check here if you want to update the time automatically through the NTP server from the Internet.

NTP Server Address: 192.0.2.33

NTP Port: 123 (123,1024-65535)

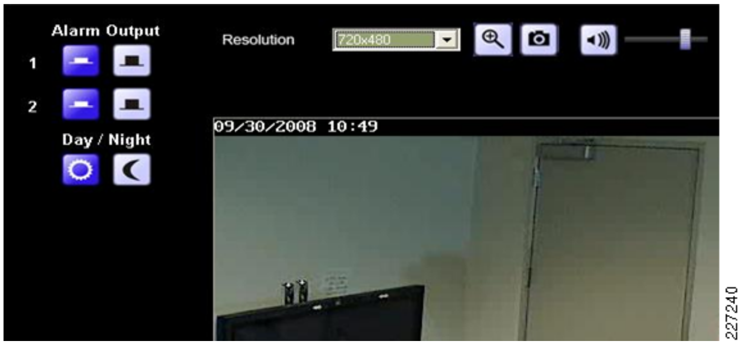
The IP camera is directed to adjust the local time for Daylight Savings Time when the offset is adjusted forward or back. The appropriate time zone is selected to specify the offset from UTC/GMT and the name of the time zone. Time is based off UTC, and each device on the network must be configured to adjust the clock by the offset for their locality.

Overlaying Video Image with a Timestamp

Most IP cameras can include the current time from the internal clock of the IP camera as an overlay to the video image. Because the NTP configuration discussed in this section provides an accurate time source to the IP cameras, this video overlay can serve as a reference to the time stamps associated with the video feed by the Media Server.

Figure 3 shows an example of a video image with a timestamp overlay with the date of *30 September 2008 at 10:49*. While there is no option to include the timezone in this display, there is also the ability to include a text overlay to the video image. The timezone can be entered as alphanumeric text along with the name or other location information of the camera.

Figure 3 Timestamp Overlay



Resolution 720x480

Server and Workstation Configuration

The Cisco Physical Security Multiservices platform or standalone servers running Cisco Video Surveillance Media Server (Media Servers), Video Surveillance Operations Manager (VSOM), Video Surveillance Virtual Matrix (VSVM) as well as client viewing stations, iSCSI appliances or other networked DVR servers would be similarly configured as the IP camera in this section. These devices all use the default router IP address as the NTP server IP address.

Summary

An accurate and consistent clock is important to provide for the synchronization of images archived from a variety of camera feeds. An accurate time source is vitally important for forensic uses of video surveillance data to equate a time with a point in time. By implementing NTP in an hierarchical design, accurate time service can be provided to a very large scale enterprise network and have excellent reliability and availability.

References

For additional information, refer to the *Network Time Protocol: Best Practices White Paper* at URL:

http://www.cisco.com/en/US/tech/tk869/tk769/technologies_white_paper09186a0080117070.shtml

Syslog

Syslog is a term for the standard logging facility on Unix/Linux systems. Most computer software programs and operating systems incorporate some logging file, but Syslog is a network-based protocol where the client system generates a log file entry to a syslog server. This syslog daemon (server) may run on the same host as the client, but the more useful implementation is realized by dedicating a machine on the network as a central syslog server and logging messages over the IP network from many hosts to this central repository.

Typically, these text messages are transmitted as UDP packets on port 514 in clear text. The RFC 5424 *The Syslog Protocol* provides more details.

Syslog messages are characterized by Facility and Severity. The severity is a numeric code of 0-7 which indicates the relative importance of the message. Emergency or severity 0 is more important than severity 7 for debug-level messages. Cisco routers send syslog messages to their logging server with a default facility of 'local7'. Cisco IP cameras use a facility of 'user'. Because of the differences in facility between a router and a IP camera, a syslog server which is logging Cisco router log messages must have the configuration file updated to include a directive for processing log files from cameras.

Assuming the goal is to include both router log files and IP camera log files into the same file (*/var/adm/logs/cisco.log*) on the syslog server for all logging levels (debug through emergency) the following example of a syslog configuration file is provided as an example.

```
/etc/syslog.conf
#
local7.debug                                    /var/adm/logs/cisco.log
user.debug                                      /var/adm/logs/cisco.log
```

Tip There are five tabs between the two text fields in the file. If the output file does not exist, it must be created with *touch /var/adm/logs/cisco.log* and the file permissions set with *chmod 755 /var/adm/logs/cisco.log.*

After editing the configuration file, the syslog daemon process must be reinitialized.

```
# kill -HUP `cat /etc/syslog.pid`
```

The following is a sample log message from a Cisco 2500 series IP camera.

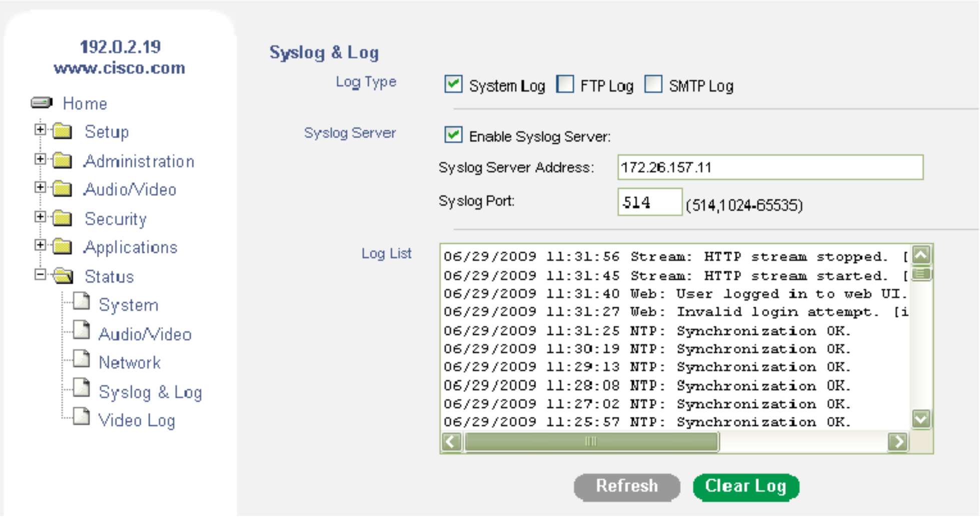
```
Sep 30 15:13:15 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:22:42 NTP:
Synchronization OK.^M
```

```
Sep 30 15:13:48 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:23:16 Web: User logged
in to web UI. [id: vsom, ip: 192.0.2.2]^M
Sep 30 15:13:49 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:23:17 Web: User logged
out from web UI. [id: vsom, ip: 192.0.2.2]^M
Sep 30 15:13:50 [192.168.16.30.4.2] 192.168.16.30 09/30/2008 15:23:17 Stream: RTSP
stream started. [ip: video, UDP: 192.168.16.30:5002 -> 192.0.2.2:6500, vsom]^
M
Sep 30 15:13:56 [192.0.2.19.4.1] 192.0.2.19 09/30/2008 15:23:23 NTP: Synchronization
OK.^M
```

Note that in the log file, the time stamp inserted by the syslog daemon differs by a few minutes from the time stamp placed in the log message from the end-node, the IP camera in this example. The IP camera is indicating from the log messages that it is synchronizing successfully with the configured NTP server; therefore, it can be assumed the clock on the Syslog server is not synched. This illustrates the importance of having all devices on the network peering with a NTP server, so that the time stamps are consistent across all devices on the network.

The screen snapshot in Figure 4 from a Cisco 2500 Series IP camera shows how the Syslog file can be viewed locally from the API of the camera and where the IP address of the central Syslog server can be entered.

Figure 4 IP Camera Syslog Configuration Screen



Log Type: ☑ System Log ☐ FTP Log ☐ SMTP Log

Syslog Server: ☑ Enable Syslog Server:

Syslog Server Address: 172.26.157.11

Syslog Port: 514 (514,1024-65535)

Log List

```
06/29/2009 11:31:56 Stream: HTTP stream stopped. [
06/29/2009 11:31:45 Stream: HTTP stream started. [
06/29/2009 11:31:40 Web: User logged in to web UI.
06/29/2009 11:31:27 Web: Invalid login attempt. [i
06/29/2009 11:31:25 NTP: Synchronization OK.
06/29/2009 11:30:19 NTP: Synchronization OK.
06/29/2009 11:29:13 NTP: Synchronization OK.
06/29/2009 11:28:08 NTP: Synchronization OK.
06/29/2009 11:27:02 NTP: Synchronization OK.
06/29/2009 11:25:57 NTP: Synchronization OK.
```

There are a number of programs available in the public domain, either commercially or are supported by user donations, that can be implemented to monitor log messages and take some action (running a command) based on these configured alerts. The web page http://www.syslog.org/ is a clearing house for syslog implementations available to the network manager.

Cisco IOS IP Service Level Agreements (SLAs)

IP Service Level Agreements (IP SLA) is a tool for the network manager to measure and report on network performance between a Cisco router and either a remote Cisco router or other IP device. One application of this technology is to configure the router that is providing network connectivity for IP cameras to verify the availability of these IP cameras. One type of probe that can be generated by the router is ICMP echo (Ping) which will be responded to by most IP stacks, including those of IP cameras. IP SLA incorporates other probe types that require a remote Cisco router with **ip sla responder-**enabled in the configuration as the IP SLA operation requires special processing.

One application of IP SLA in a camera deployment would be to use the router to generate ICMP echo requests on a periodic basis to all the local IP camera and then to maintain a history log of any connectivity failures or responses which exceed a specified time limit.

The following sample configuration shows a router configuration that sends an ICMP echo request every 60 seconds (the default value) to the camera at IP address 192.0.2.19 with a ToS value of CS6, in VRF IPVS with a threshold of 50 milliseconds. A history file is maintained for probes that receive no response or the response is over the configured treshold. The identifier of 219 is an arbitrary numeric identifier value.

```
!
ip sla 219
 icmp-echo 192.0.2.19
 tos 192
 threshold 50
 vrf IPVS
 owner networkmgr
 tag ipvs - design guide
 frequency 60
 history lives-kept 1
 history buckets-kept 60
 history filter failures
ip sla schedule 219 life forever start-time now
```

The history output can be displayed in tabular format or ‘full’ or verbose format. The history file is only updated for failure events, which provides more relevancy to the log file and prevents it from wrapping as frequently as it would if all entries are logged.

```
vpn1-2851-1#show ip sla hist 219
        Point by point History
Entry    = Entry number
LifeI    = Life index
BucketI  = Bucket index
SampleI  = Sample index
SampleT  = Sample start time
CompT    = RTT (milliseconds)
Sense    = Response return code

Entry LifeI      BucketI    SampleI    SampleT    CompT      Sense      TargetAddr
219   1          1          1          708986549  128        3          192.0.2.19
219   1          2          1          709250549  88         3          192.0.2.19
219   1          3          1          709280549  0          4          192.0.2.19
219   1          4          1          709286549  0          4          192.0.2.19
```

In the verbose output of the log file, the network manager can see at what time of the day the target camera failed to respond or responded over the threshold. The last two log file entries coincide with the author removing the Ethernet cable from the rear of the IP camera. Because the camera is using PoE, the network connectivity was lost and the device also lost power. The Over threshold values may have been a result of the operating system responding slowly to the ICMP echo response (on many systems, ICMP is a background process with low priority) or due to some network congestion.

```
vpn1-2851-1#show ip sla hist 219 full
Entry number: 219
Life index: 1
Bucket index: 1
Sample time: 11:55:23.207 edt Mon Jun 29 2009
RTT (milliseconds): 128
Response return code: Over threshold

Life index: 1
```

```
Bucket index: 2
Sample time: 12:39:23.207 edt Mon Jun 29 2009
RTT (milliseconds): 88
Response return code: Over threshold

Life index: 1
Bucket index: 3
Sample time: 12:44:23.207 edt Mon Jun 29 2009
RTT (milliseconds): 0
Response return code: Timeout

Life index: 1
Bucket index: 4
Sample time: 12:45:23.207 edt Mon Jun 29 2009
RTT (milliseconds): 0
Response return code: Timeout
```

IP SLA may be implemented on production routers; however, many network managers choose to dedicate a router for the sole purpose of generating and responding to IP SLA probes. Additionally, CiscoWorks Internetwork Performance Monitor uses the IP SLA software feature embedded within the Cisco IOS and can be part of an overall network management infrastructure for managing routers, switches, servers and end-nodes such as IP cameras.

Summary

IP SLA may be used by the network manager to aid in troubleshooting connectivity failures or as a part of an overall ongoing network management strategy implemented by software packages such as CiscoWorks IPM.

Power-Over-Ethernet (PoE)

Many analog camera deployments require an external power supply to provide the typical input voltage of 12VDC/24VAC, with 24VAC at 3.5 AMP being common. Many analog deployments may implement a smart BALUN to multiplex power, RS-485 (for PTZ control) and video signal over a CAT-5 cable at an attempt to provide a similar advantage to which an IP camera with Power over Ethernet enjoys.

PoE enables power for the camera using the same cable as that used for network connection. Switches must meet the IEEE 802.3af standard to be PoE-compliant. PoE is incorporated into many access-LAN switches to support IP telephony and wireless LAN controllers also using PoE. The maximum distance is the same as the Ethernet standard, 100 meters.

Providing backup power to each analog camera may be costly and time-consuming, while providing an uninterruptible power supply (UPS) for the access switch will not only provide for backup power to an IP camera, but also other devices on the LAN switch. IP cameras have a decided advantage over analog systems because of the PoE feature. One caveat, however, is that many IP cameras that incorporate a wireless LAN connection may not support PoE to the wired-port, because the assumption is made that the reason a wireless camera was purchased was to use the wireless features.

Additionally, PoE may decrease the time required to install an IP camera due to the elimination of the need for a licensed electrician to complete the installation or may permit installation in ceilings where PoE devices are permitted but other electrical inputs are not.

Note You must use the Cisco 12V power adapter (CIVS-PWRPAC-12V) when no IEEE 802.3af standard PoE switch is available.

The Cisco 2500 Series and the 4000 Series cameras are in Device Class 3 which specifies an power consumption range of 6.49 to 12.95 Watts. The following command output is from a Cisco 3750 LAN switch with both CIVS-IPC-2500 (Standard Definition) and CIVS-IPC-4300 (High Definition) IP cameras attached to the switch. The power consumption is 9.0 watts and 13.0 watts respectively.

```
3750-access#show power inline gigabitEthernet 1/0/2
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/2   auto   on         9.0     CIVS-IPC-2500       3     15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Gi1/0/2               15.4                 15.4
```

By omitting the interface option, all connected devices are shown as follows:

```
3750-access>show power  inline

Module   Available     Used     Remaining
          (Watts)     (Watts)    (Watts)
------   ---------   --------   ---------
1           370.0       35.0       335.0
Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/1   auto   off        0.0     n/a                 n/a   15.4
Gi1/0/2   auto   on         9.0     CIVS-IPC-2500       3     15.4
Gi1/0/3   auto   on         13.0    CIVS-IPC-4300       3     15.4
Gi1/0/4   auto   on         13.0    CIVS-IPC-4300       3     15.4
Gi1/0/5   auto   off        0.0     n/a                 n/a   15.4
```

Summary

PoE is a feature that provides a decided advantage of an IP-based video surveillance implementation over the analog counterpart. It is particularly useful in enterprise implementations that have existing IP telephony or wireless access points that also rely on PoE.

Cisco Discovery Protocol (CDP)

CDP is a Layer-2 network protocol that runs on most Cisco routers, switches and end-nodes like Cisco IP phones, access points, and also the Cisco IP surveillance cameras. CDP is primarily a troubleshooting tool, as it includes Layer-3 addressing (IP address) over a Layer-2 protocol and application information like the operating system version, capabilities, device name and type of device. It also has been enhanced to provide the value of the interface duplex setting and power requirements.

From a video surveillance perspective, it is most useful for the initial provisioning of IP cameras on the network. Cisco IP cameras have the hardware (MAC) address printed on the exterior of the IP camera. The CDP exchange also includes a reference to the MAC address through the *Device ID* field. The IP address of the camera and the firmware version are associated with the MAC address in the output of the **show cdp neighbors** command. Sample output is shown below:

```
3750-access#show cdp neighbors gigabitEthernet 1/0/2 detail
```

```
-------------------------
Device ID: 001DE5EA79D3
Entry address(es):
  IP address: 192.0.2.50
Platform: CIVS-IPC-2500,  Capabilities: Host
Interface: GigabitEthernet1/0/2,  Port ID (outgoing port): eth0
Holdtime : 153 sec

Version :
1.1.1

advertisement version: 2
Duplex: full
Power drawn: 9.000 Watts
Power request id: 57831, Power management id: 3
Power request levels are:9000 0 0 0 0
Management address(es):
  IP address: 192.0.2.50
```

If the Cisco IP camera is unable to obtain an IP address through DHCP, it will default to the address of 192.168.0.100. Either the DHCP assigned IP address or the static IP address is advertised via CDP, which provides useful information to the network manager as to the state of the camera installation.

As a best practice, IP cameras should be assigned a static IP address that is referenced in the enterprise DNS system. The initial DHCP address can be used by a remote network or physical security administrator to complete the initial configuration of the camera from the factory defaults. This includes changing the DHCP or default IP address to a static IP address registered with DNS. Once that change is made and saved, the remote administrator must reconnect to the camera and complete the initial configuration and definition within VSOM/Media Server.

Tip Some firmware versions of the Cisco IP cameras also support device discovery using the Bonjour protocol.

One additional use of CDP is device discovery. CiscoWorks Network Connectivity Monitor and other third-party software packages can autodiscover a network topology by using both CDP and SNMP access to routers and switches in the network. Because Cisco IP cameras support CDP and SNMP, these endpoints can also be discovered by these network management tools.

Simple Network Management Protocol

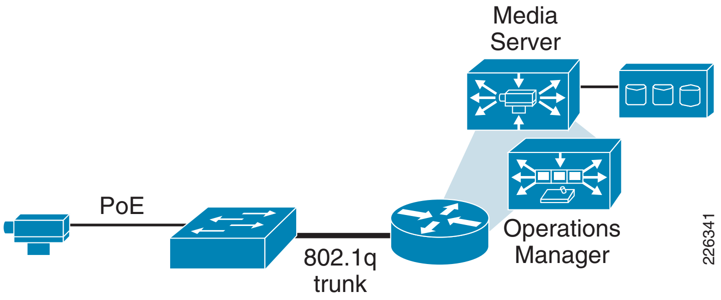
Cisco IP cameras also support the Simple Network Management Protocol (SNMP). This protocol is disabled by default, and once enabled the default read community string is *public*, which many organizations change to some site-specific value. Two SNMP trap receiver IP addresses may be entered in the dialog box on the configuration screen. There is no write SNMP option, it is a read-only implementation and must be configured from the API of the camera as there is no VSOM support for these values.

Deploying a Cisco Video Surveillance IP Camera

The Cisco Video Surveillance IP Camera User Guide provides information about installing, configuring, using, managing, and troubleshooting the Cisco Video Surveillance IP Camera model CIVS-IPC-2500. This section describes examples of one method of deploying the camera at a branch office location, facilitating and simplifying deployment.

This section assumes that the branch Cisco ISR router has an operational Cisco VMSS Network Module, a Layer-2 switch capable of providing Power-over-Ethernet (or an external power injector, or power supply is available) and a FastEthernet network connection on a VLAN dedicated to the cameras at the branch office. In this example, a Cisco 3825 ISR router and a Cisco Catalyst 3750 Series Switch is used. The router and the switch are connected by an 802.1q trunk. This toplogy is shown inFigure 5.

Figure 5 Cisco Video Surveillance IP Camera - Branch Office Deployment



Deployment Steps

Create (Verify) a DHCP Pool and Interface on the Router

This branch location is served by by less than 15 IP cameras. An IP network address with a mask of /28 (255.255.255.240) is shown in the following example. Create/verify a DHCP pool and sub-interface on the branch router.

```
!
ip dhcp pool cameras
   network 192.0.2.48 255.255.255.240
   default-router 192.0.2.49
   dns-server xx.xxx.6.247 xxx.xx.226.120
   domain-name cisco.com
!
interface GigabitEthernet0/0.208
 description inside interface for ip cameras
 encapsulation dot1Q 208
 ip address 192.0.2.49 255.255.255.240
!
end
```

The DHCP pool is used to allow the camera to initially obtain an IP address through DHCP. Once the camera has been powered and booted, the DHCP assigned IP address is made a static IP address. The VMSS network module refers to the static IP address when defining the camera.

Create a SmartPort Macro on the Switch

The Catalyst 3750 switch port for the camera can be configured using a Smartport macro. By defining the configuration commands in a macro, they can be easily applied to additional port which provide connectivity to other cameras at this location. Configure and apply the Smartports macros shown in global configuration mode.

```
macro name CIVS-IPC-2500
```

```
description Cisco Video Surveillance 2500 Series IP Camera
switchport mode access
switchport access vlan $VLAN
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdufilter enable
load-interval 60
no shutdown
@
```

These configuration commands enable the port as a Layer-2 access port and assigns the port to a separate VLAN for IP cameras. The VLAN must match the VLAN configured on the router from the previous step. Bridge Protocol Data Unit (BPDU) filters are enabled to prevent this control traffic from being sent out the port. This command has the same effect as disabling spanning tree on the interface and can result in spanning-tree loops. However, this port is intended to be used for the IP Camera and not for connecting to another switch. The portfast feature is commonly used for end-stations and decreases the time it takes for the port to begin forwarding traffic.

Port security is defined, allowing a single MAC address, the first MAC address seen on the port is automatically entered into the configuration. If the IP Camera is unplugged from the port and another device is attached, the port security feature marks the port as error-disabled and shutsdown the port immediately. An SNMP trap is sent and a syslog message is logged. To bring the port back on-line issue a shutdown and no shutdown interface configuration commands. As a best practice, the SNMP traps and syslog messages should be monitored and alerts sent to an appropriate contact(s) within the physical security organization to alert the operators when camera are being tampered with or removed from the network.

Because the DSCP values of IP packets are set by the camera firmware, the Layer-3 QoS values are trusted by the switch. The DSCP value of CS5 (40) is manually configured for both audio and video and is shown in a later step.

Finally, the *no shutdown command* is issued on the port, which brings up the port and through the CDP exchange, will negotiate and apply power to the camera.

Power Up Camera

In this example, it is assumed the camera is attached to interface gigabitEthernet 1/0/2 and is administratively shutdown.

```
3750-access#sh run int g 1/0/2
Building configuration...

Current configuration : 48 bytes
!
interface GigabitEthernet1/0/2
 shutdown
end
```

The macro is manually applied to the interface, specifying VLAN 208 as an argument to the macro. This parameter is substituted as the macro executes. When the macro finishes executing, the link is brought up and the camera powered from the switch.

```
3750-access(config)#interface gigabitEthernet 1/0/2
3750-access(config-if)#macro apply CIVS-IPC-2500 $VLAN 208
%Warning: portfast should only be enabled on ports connected to a single
```

```
 host. Connecting hubs, concentrators, switches, bridges, etc... to this
 interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION

%Portfast has been configured on GigabitEthernet1/0/2 but will only
 have effect when the interface is in a non-trunking mode.
3750-access(config-if)#
*Mar  2 17:34:29.774: %ILPOWER-7-DETECT: Interface Gi1/0/2: Power Device detecte
d: IEEE PD
*Mar  2 17:34:30.412: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed st
ate to down
*Mar  2 17:34:30.781: %ILPOWER-5-POWER_GRANTED: Interface Gi1/0/2: Power granted
*Mar  2 17:34:33.650: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed st
ate to up
*Mar  2 17:34:34.656: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/2, changed state to up
*Mar  2 17:34:55.343: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/2, changed state to down
*Mar  2 17:34:56.349: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed st
ate to down
*Mar  2 17:34:59.403: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed st
ate to up
*Mar  2 17:35:00.409: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEth
ernet1/0/2, changed state to up
3750-access(config-if)#
3750-access(config-if)#end
3750-access#
3750-access#
*Mar  2 17:35:19.368: %SYS-5-CONFIG_I: Configured from console by console
```

To verify the interface configuration, a *show run interface* command can be executed. The MAC address of the camera has been learned and is applied to the interface configuration.

```
3750-access#show run interface gigabitEthernet 1/0/2
Building configuration...

Current configuration : 409 bytes
!
interface GigabitEthernet1/0/2
 description Cisco Video Surveillance 2500 Series IP Camera
 switchport access vlan 208
 switchport mode access
 switchport port-security
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 001d.e5ea.79d3
 load-interval 60
 mls qos trust dscp
 macro description CIVS-IPC-2500
 spanning-tree portfast
 spanning-tree bpdufilter enable
end
```

Warning **The running configuration is not automatically saved following macro completion, enter write memory (copy running-config startup-config) to save the configuration changes.**

The following command output shows that the IP camera is a class 3 device and the switch is supplying 9 Watts to the IP Camera.

```
3750-access#show power  inline gigabitEthernet 1/0/2
Interface Admin  Oper       Power   Device              Class Max
```

```
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi1/0/2   auto   on         9.0     CIVS-IPC-2500       3     15.4

Interface  AdminPowerMax   AdminConsumption
             (Watts)           (Watts)
---------- --------------- --------------------

Gi1/0/2               15.4                 15.4
```

The IP camera, by default, will request a DHCP address. If the camera cannot obtain an IP address through DCHP within 90 seconds, it uses a default IP address of 192.168.0.100. To determine what IP address has been assigned to the IP Camera, a show *ip dhcp binding* can be issued from the branch router, and the MAC address printed on the adhesive label attached to the camera body, can be use to identify the IP address associated with the IP address of the Camera. The MAC address of the camera can also be learned from the *show mac address-table dynamic interface* command on the switch. Alternately, the IP address of the IP camera can be found from Cisco Discovery Protocol, as shown:

```
3750-access#show cdp neighbors gigabitEthernet 1/0/2 detail
-------------------------
Device ID: 001DE5EA79D3
Entry address(es):
  IP address: 192.0.2.52
Platform: CIVS-IPC-2500,  Capabilities: Host
Interface: GigabitEthernet1/0/2,  Port ID (outgoing port): eth0
Holdtime : 153 sec

Version :
1.1.1

advertisement version: 2
Duplex: full
Power drawn: 9.000 Watts
Power request id: 57831, Power management id: 3
Power request levels are:9000 0 0 0 0
Management address(es):
  IP address: 192.0.2.52

3750-access#
```

In this example, the camera has been assigned an IP address of 192.0.2.52. It can also be shown from the DHCP table of the branch router.

```
vpn4-3800-6#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address          Client-ID/              Lease expiration        Type
                    Hardware address/
                    User name

192.0.2.52          0100.1de5.ea79.d3       Feb 28 2009 02:17 PM    Automatic
```

The MAC address can be verified from the LAN switch as shown:

```
3750-access#show mac address-table interface gigabitEthernet 1/0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
```

```
----    -----------       --------    -----
 208    001d.e5ea.79d3    STATIC      Gi1/0/2
Total Mac Addresses for this criterion: 1
```

In this section it has been shown that the IP address and MAC address of the IP camera can be located in several ways by issuing **show** commands on the router and switch.

Document Switch, Router and DNS

In the next step, the camera configuration is changed to use a static IP address and the hostname of the camera is configured. The following checklist is helpful for ongoing documentation.

Configure the port name on the switch (for example, *set port name or description)*

- Exclude the IP address of the camera from the DHCP pool (for example, **ip dhcp excluded-address 192.0.2.52**)
- Update DNS to reference the deployed camera
  - ipc-2500-79d3.cisco.com. IN A 192.0.2.52
  - 52.2.0.192.in-addr.arpa. IN PTR ipc-2500-79d3.cisco.com

Configure the IP Camera

It is assumed the PC is connected to a network that has connectivity to the 192.0.2.48/28 network. Because the camera has obtained an IP address, mask, default gateway and DNS servers and domain-name from the DHCP pool on the router, the PC need not be connected to the same subnet as the camera. Using the DHCP method to deploy the camera initially enables the camera to be deployed at the remote location by a technician trained in physical cable termination, while the camera, switch, router and the VMSS configuration is done by the network and physical security personal at a central location.

Use the following URL to connect to the camera at IP address 192.0.2.50:

```
https://192.0.2.52
```

Note The protocol is Hypertext Transfer Protocol over Secure Socket Layer or **HTTPS**.

After successfully connecting to the web server of the Cisco IP Camera, several configuration options should be updated before defining the camera to the VMSS module. This checklist is provided to assist in completing these tasks.

Warning **Make sure the SAVE button is selected at the bottom of the screens when changing values.**

Table 7 Camera Configuration Checklist

Camera Configuration Checklist
Factory Default Initalization Screen • **Password**—Create an appropriate password for the ‘admin’ username. • **HTTP**—Enable HTTP as it is required by VSOM.
Administration -> Users —Create a userid specific for VSOM to configure, start and stop camera feeds. The web interface only allows one connection per userid. In testing a userid of ‘vsom’ with an appropriate password with ‘administrator’ privilege level is used.
Setup -> Basic Setup —Configure NTP as described previously in this design guide, if the branch router is configured as a NTP server, the default gateway IP address can be entered as the IP address of the NTP server.
Setup -> Basic Setup —Change the Configuration Type to Fixed IP address from DHCP, the values populated by the DHCP server configured previously in this section, will be maintained, eliminating the need to re-enter these values.
Setup -> Basic Setup - Under Camera Name and Description, Entering the IP address, Hostname or some unique identification value in this field may be useful in ongoing operation of the network.
Setup -> Advanced Setup -> QoS —Enable QoS and set both Audio and Video to DSCP value of ‘40’ which is CS5.
Security - > Complexity—It may be useful to only select password check option 4 - *Not used* , if the camera password checks conflict with corporate standards.
Audio/Video -> Video -> Options —Enable Time Stamp and Text to Display is useful in ongoing operations and management.
Status -> Syslog & Log—Enable Syslog server and enter the IP address of the server.
Setup -> IP Filter - This option is discussed in “Virtualization, Isolation and Encryption of IP Video Surveillance” section on page 6-87.

Complete Camera Installation Under VSOM

After saving changes, exit/logoff the camera web server and complete the camera configuration from the VSOM administration screens to complete the definition and configuration of the camera.

```
http://vsom-webserver
```

Then select the Admin icon to switch to Administration Mode.

In **Devices - > IP Network Cameras -> Add a New IP/Network Camera**, fill out the form to define the new network camera. Suggested values are shown below:

Camera Information

- *Camera Name: ipc-2500-79d3.cisco.com
- Description: CIVS-IPC-2500 LABRACK
- *Camera Type: - Cisco 2500 IP Camera
- *Host IP/Name: 192.0.2.52
- *Status: Enabled

Camera Feed

- *Server: -- VSMS_Site130
- *Media Type: MPEG-4
- *Format: NTSC
- *Resolution: D1 720 x 480
- *Transport: UDP
- Multicast Address:
- *Bitrate: -- Choose One -- 5000 4000 3000 2000 1500 1024 768 640 512 511 384 256 255 128 56
- *Quality: Defaults to 50^
- Camera requires authentication
- *Username:
- *Password:
- *Confirm Password:

Note The items above in asterisks (*) are required input.

Note

- Only MPEG-4 is supported in early firmware releases, MJPEG is supported in latest code.
- The format can be NTSC or PAL, when selected, changes the options available for selection under resolution
- Check the camera requires authentication and enter the userid and password from Table 7.
- The appropriate value for Bitrate is a function of desired image quality, available storage, and bandwidth. A value of 1,024K or 2,000K is a good starting value for a standard definition camera.

Summary

By using the Smartport macro capability of the Cisco Catalyst 3750 Series Switches, the DHCP server functions of the Cisco 3825 Integrated Services Router (ISR) and the Web server configuration utility of the Cisco Video Surveillance 2500 Series IP Cameras, IP Video Surveillance cameras can be quickly defined and deployed at a branch office or campus location. While the camera installation and wiring to the LAN switch must be accomplished by a technican at the physical location of the camera, the remainder of the configuration and installation can be completed from the network operations center over the IP network.

Configuring Quality-of-Service (QoS) for IP Video Surveillance

This chapter addresses implementing quality-of-service (QoS) for IP video surveillance deployments. The primary focus of this chapter is to understand the source and sinks of video surveillance feeds so that the network manager can mark packets with the appropriate QoS values to map into the enterprise QoS model. Equally important is to understand the bandwidth requirements of video surveillance feeds and take this into consideration when implementing QoS policies on LAN and WAN interfaces.

This chapter covers the following topics:

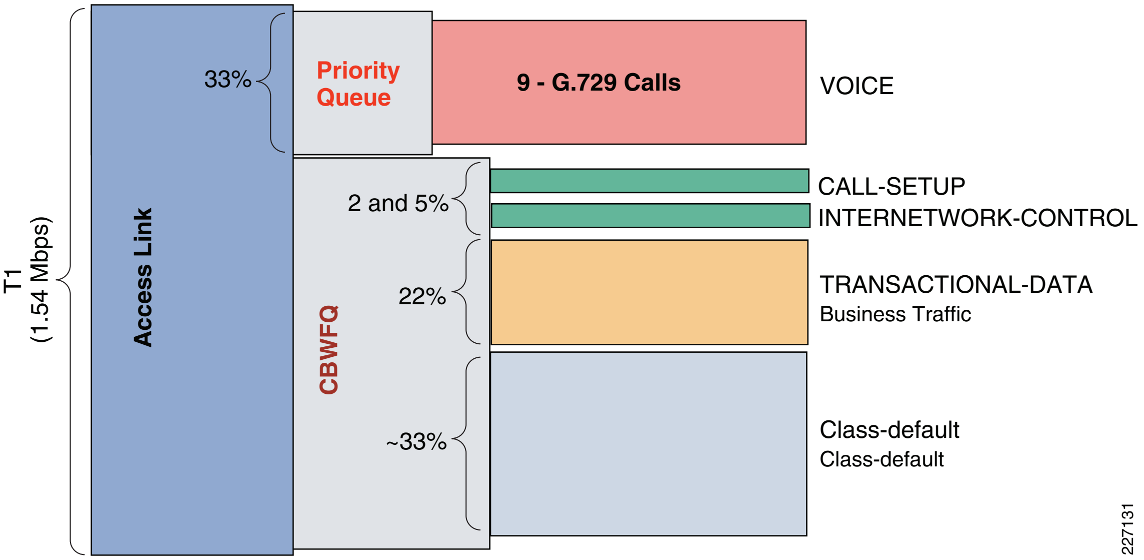
- WAN link bandwidth allocation changes for incorporating video into the network
- The QoS application classes and the DiffServ recommendations
- Examining the end-to-end traffic flows
- Ingress and end-node (IP cameras) marking of IP packets
- Examples of QoS techniques for routed MAN/WAN interfaces

WAN Link Bandwidth Allocation

The first network transition point was the introduction of VoIP to the traditional data network. In the 2004 time-frame, the Cisco Enterprise Solutions Engineering (ESE) labs extensively tested QoS-enabled encrypted VoIP and data. The traffic profile in those tests is characterized by a T1/E1 (1.5Mbps/2.0Mbps) or lower access circuit with nine G.729 VoIP calls and data traffic on the links. The data traffic is comprised of best effort traffic like file transfers and web browsing, as well as transactional data in the form of TN3270 and Telnet sessions.

The QoS service policy allocates 33 percent of the bandwidth for VoIP in a strict priority queue, 2 and 5 percent of the bandwidth for call control (CALL-SETUP) and routing protocol updates (INTERNETWORK-CONTROL). The remaining bandwidth classes were allocated for the TN3270/Telnet traffic in a TRANSACTIONAL-DATA class and the file transfers and web browsing fell to the default class (class-default). The bandwidth allocation from that testing is shown in Figure 6.

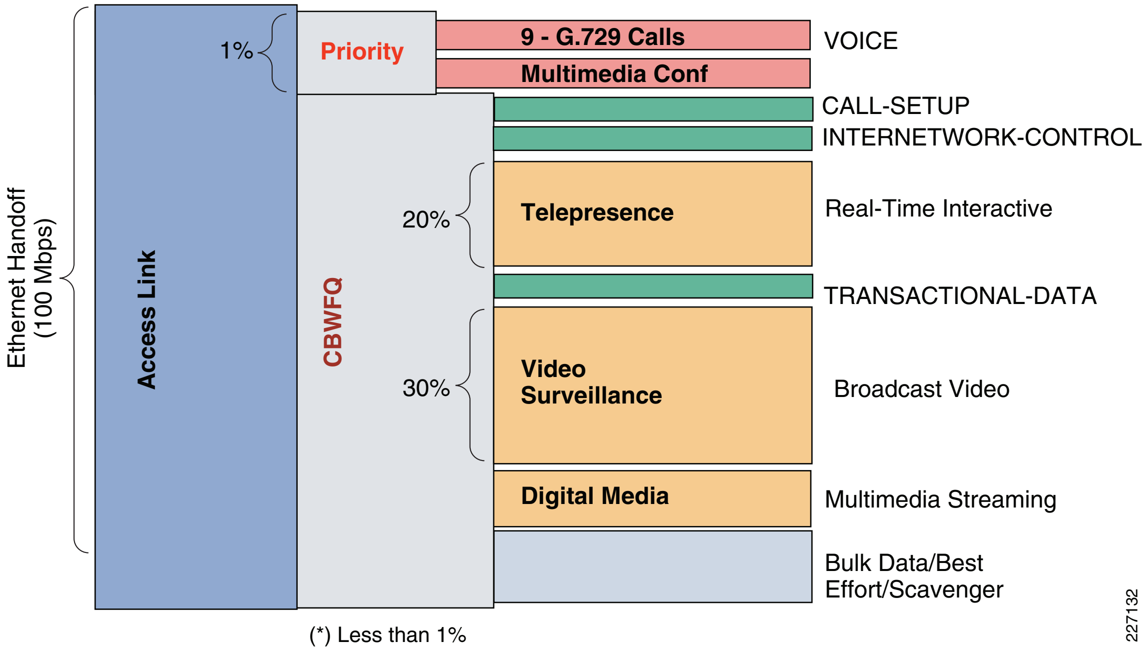
Figure 6 Bandwidth Allocation for Encrypted Voice and Data—2004



With the introduction of various video applications (Digital Media System (DMS), Telepresence, IP Video Surveillance, and Multimedia Conferencing to the VoIP and data network), the offered load to the network expands dramatically.

First, the total amount of bandwidth required for a branch location must be increased. Where VoIP and data can be transported on a T1/E1 link, 50 to 100 Mbps is required. The driver for this increase in bandwidth are the video applications provisioned on the links. Assuming similar branch requirements as is illustrated in Figure 6. Figure 7 includes additional bandwidth classes to accommodate video with an overall increase in the total amount of bandwidth.

Figure 7 Bandwidth Allocation to Provision Various Types of Video—009



While not all branches have a requirement for transporting Telepresence, Video Surveillance, or DMS over the WAN, there is a possibility that one or more of these video applications exist or will in the future and must be considered when provisioning WAN links.

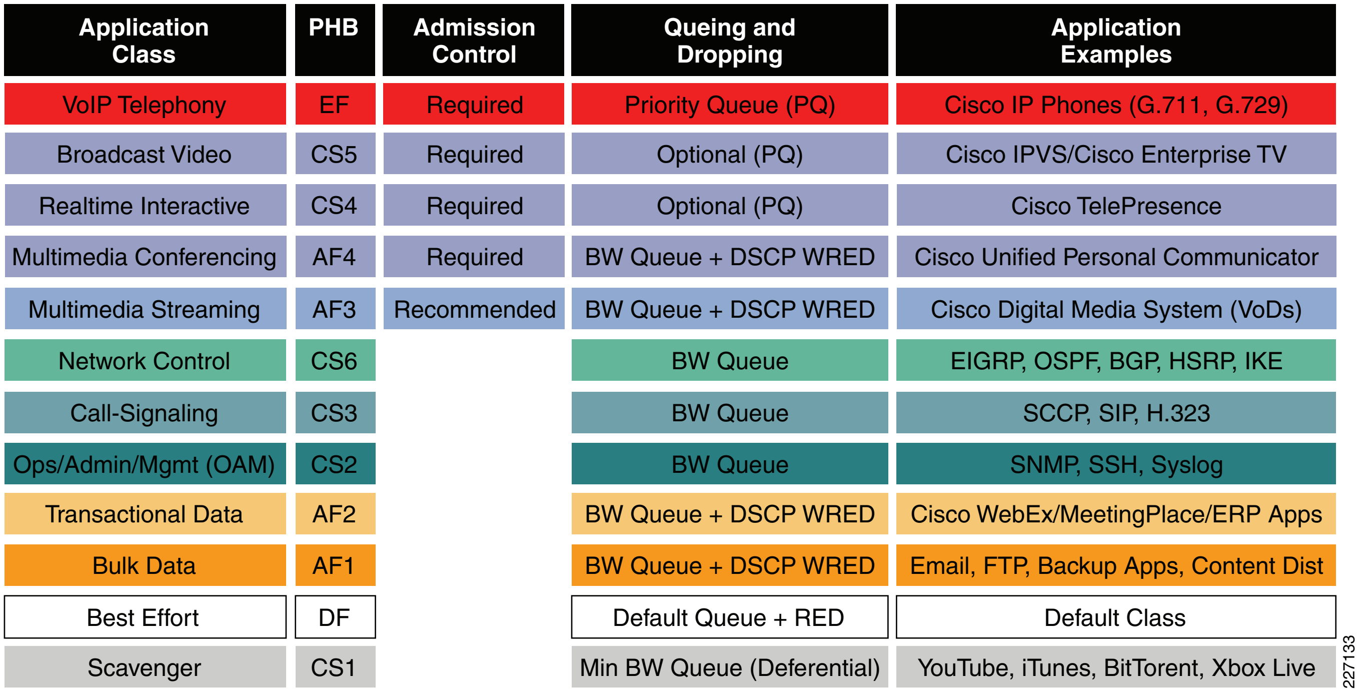
Given the same number of VoIP calls, nine, from the 2004 bandwidth allocation, note that in terms of the percentage of bandwidth for the priority queue for VoIP goes from 33 percent of the total bandwidth to a fraction of a percent when the WAN link is a 100Mbps Metro Ethernet link. A single Telepresence unit can consume 15 to 20Mbps of bandwidth and live viewing of 8 to 10 IP cameras at the branch from a central command center can easily consume 10Mbps of bandwidth for a single viewing station. Digital Media and Multimedia Conferencing also may be present at the branch and also consume bandwidth.

With these requirements, the next section provides a framework to map QoS DiffServ, the Diffserv Codepoint (DSCP) values for these application classes. For those not familiar with the term DiffServ or DSCP, these terms are for a revised definition of the IP type-of-service (ToS)-byte allocation in the IP header. In the past, 3 bits of this field was used as IP precedence, providing for distinguishing traffic into eight different categories. QoS DiffServ expands this quantification to 6 bits and adds new functionality to the ToS byte. In order to use this relative priority indicator consistently from end-to-end on the network, some consistent framework must be in place so that all routers and switches on the network derive the same meaning from the marking.

Cisco Medianet Application Classes

In Figure 8, the Cisco DiffServ QoS recommendations, based on the guideline from RFC 4594, is shown.

Figure 8 *DiffServ QoS Recommendations (RFC 4594-Based)*



Application Class	PHB	Admission Control	Queing and Dropping	Application Examples
VoIP Telephony	EF	Required	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
Broadcast Video	CS5	Required	Optional (PQ)	Cisco IPVS/Cisco Enterprise TV
Realtime Interactive	CS4	Required	Optional (PQ)	Cisco TelePresence
Multimedia Conferencing	AF4	Required	BW Queue + DSCP WRED	Cisco Unified Personal Communicator
Multimedia Streaming	AF3	Recommended	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
Network Control	CS6		BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
Call-Signaling	CS3		BW Queue	SCCP, SIP, H.323
Ops/Admin/Mgmt (OAM)	CS2		BW Queue	SNMP, SSH, Syslog
Transactional Data	AF2		BW Queue + DSCP WRED	Cisco WebEx/MeetingPlace/ERP Apps
Bulk Data	AF1		BW Queue + DSCP WRED	Email, FTP, Backup Apps, Content Dist
Best Effort	DF		Default Queue + RED	Default Class
Scavenger	CS1		Min BW Queue (Deferential)	YouTube, iTunes, BitTorent, Xbox Live

The applications listed under the *Application Class and Examples* column provides a description of the applications which comprise each class. For IP Video Surveillance, the media, whether it be TCP-based as is the case with Motion JPEG camera feeds, UDP/RTP-based for MPEG-4 and H.264 or TCP-based web delivery, the recommendation is to mark this traffic as DSCP decimal value **40** or **CS5**. The control plane traffic for video surveillance, such as RTSP, is recommended to be set at **CS3** or decimal value **24**. As a best practice, IP cameras are recommended to be configured for NTP, SNMP and Syslog, and these applications are suggested to be marked DSCP with decimal value **16** or **CS2**.

There is a very limited amount of network traffic in a video surveillance deployment for control plane and network management applications compared to media streams. Because of this, some network managers may find it both practical and expedient to mark media as **CS5** and all other traffic from cameras, clients and servers as either **CS3** or **CS2**. The examples shown in this section use **CS5** and **CS3** to illustrate how to identify and select traffic through access control lists and mark accordingly. The network managers can be as specific and detailed in marking as they desire.

The following configuration sample shows class-map names and the associated match statements that can be used in router and switch configurations:

```
!
class-map match-all VOICE
  match ip dscp ef
class-map match-all TELEPRESENCE
  match ip dscp cs4
class-map match-all NETWORK-CONTROL
  match ip dscp cs6
class-map match-any CALL-SIGNALING
  match ip dscp cs3
class-map match-all OAM
```

```
  match ip dscp cs2
class-map match-any MULTIMEDIA-CONFERENCING
  match ip dscp af41 af42 af43
class-map match-any MULTIMEDIA-STREAMING
  match ip dscp af31 af32 af33
class-map match-all BROADCAST-VIDEO
  match ip dscp cs5
class-map match-any LOW-LATENCY-DATA
  match ip dscp af21 af22 af23
class-map match-any HIGH-THROUGHPUT-DATA
  match ip dscp af11 af12 af13
class-map match-all SCAVENGER
  match ip dscp cs1
!
```

Tip Entering user-supplied values in upper case (for example, **SCAVENGER** versus **scavenger**) enhances readability of the configuration file.

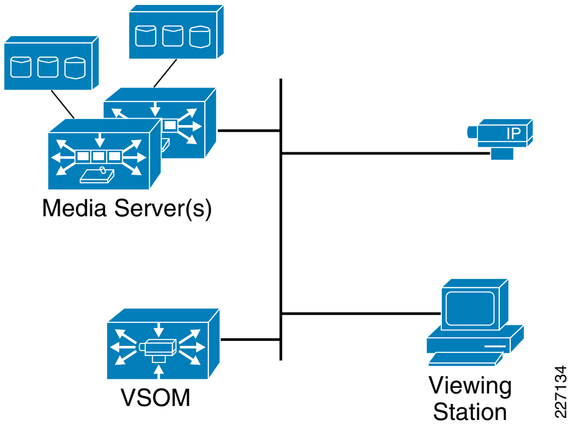
End-to-End QoS Marking

One fundamental best practice of implementing QoS on a network is to mark the ToS byte (DSCP) of the IP packets on the end nodes, or as close to the origination of the traffic as practical. In a Cisco IP Video Surveillance deployment, the primary components are as follows:

- IP Cameras—The original source of video feeds
- Viewing workstations—A destination of video feeds
- Management Software—Configure, manage, and view the video subsystem
- Storage Servers—Archives video feeds

These components are shown in Figure 9.

Figure 9 IP Video Surveillance End Nodes



In the sample deployment shown in Figure 9, there are one or more Media Servers being controlled by at least one Video Surveillance Operations Manager (VSOM) server. With a Cisco ISR router and the Video Management and Storage System (VMSS) Network Module, these two software components reside on the same logical interface. In a multiservice platform or standalone Unix implementation, they could reside on the same chassis or separate chassis. One VSOM server can control more than one Media Servers.

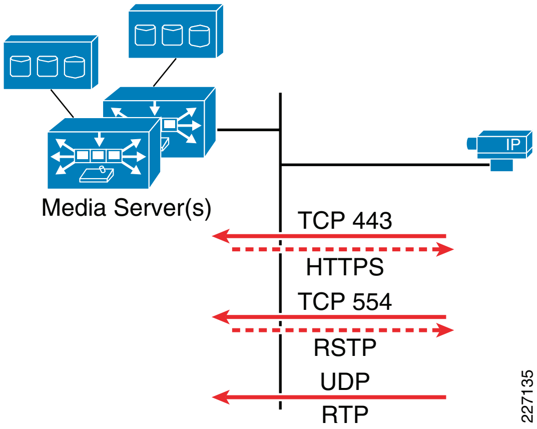
In this example, the assumption is that the IP camera is a Cisco IP camera or a camera from another vendor, which can be configured to mark the video media stream with a DSCP value. This is an example where the end-node is marking the IP packets with an appropriate DSCP value. For the viewing stations, Media Server and VSOM, it is assumed that a network device, either the first router or switch, will need to identify the traffic and mark it accordingly.

Traffic Flow Between IP Camera and Media Server

To understand how to implement QoS for IP video surveillance, we first must understand the data flows between camera, storage, and viewing station. While video from an IP camera can be viewed directly by a webserver client connecting to the camera application programming interface (API), it does not scale and introduces a security exposure and access control issues. Many IP cameras implement an access control-list feature that should be configured to deny IP access to the camera from all but authorized hosts. Typically, only the video management system servers and the address space where the configuration workstations and network management servers reside need be permitted.

Figure 10 illustrates the typical exchange between an IP camera and Media Server once the camera is installed on the network and defined through VSOM to the appropriate Media Server.

Figure 10 Traffic Flow—IP Camera and Media Server



In the implementation shown in Figure 10, the process flow is initiated by the Media Server. When a scheduled archive or live feed is needed from an IP camera, the Media Server initiates a connection to the IP camera to request the feed. Assuming the Cisco 2500 Series IP camera feed is MPEG-4, the Media Server performs the following:

- Initiates a HTTPS session with the IP camera for authentication and control plane.
- Initiates a RTSP session with the IP camera for description, initiation or termination of the media feed. Also control plane.
- The IP camera begins streaming the video feed as a UDP/RTP session on ports negotiated in the RTSP exchange. This is the media (data) plane.

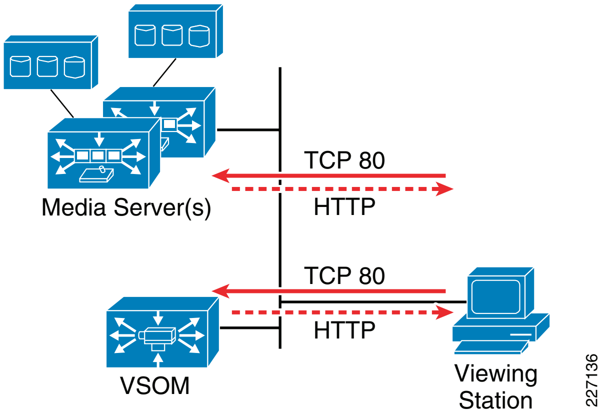
Of these exchanges, only the UDP/RTP session is marked by the Cisco 2500 Series camera with a DSCP value. The HTTPS and RTSP packets originating from the camera have a DSCP value of **0** or best effort (BE). Normally, the camera is configured for other network services such as NTP, syslog, SNMP, and this traffic is also marked BE.

However, the majority of the network traffic, certainly approaching 100 percent to and from the IP camera is the media stream. In this case, while the IP camera stack will set the DSCP value, there may still be certain types of traffic from the camera that the network manager would consider marking by the switch or router. One simple solution is to configure the switch to mark all IP packets from the camera as DSCP value **CS5**.

Traffic Flow Between Media Server and Viewing Station

The second leg of the traffic flow in the network is between the viewing station and the Media Server supporting the IP camera. Assuming that an operator has logged on the VSOM server with operator privileges, the TCP connections are initiated by the viewing station to the VSOM IP address for the control plane and the client also issues HTTP GETs to the appropriate Media Server IP address to initiate the video stream. This is shown in Figure 11.

Figure 11 Traffic Flow—Media Server and Viewing Station



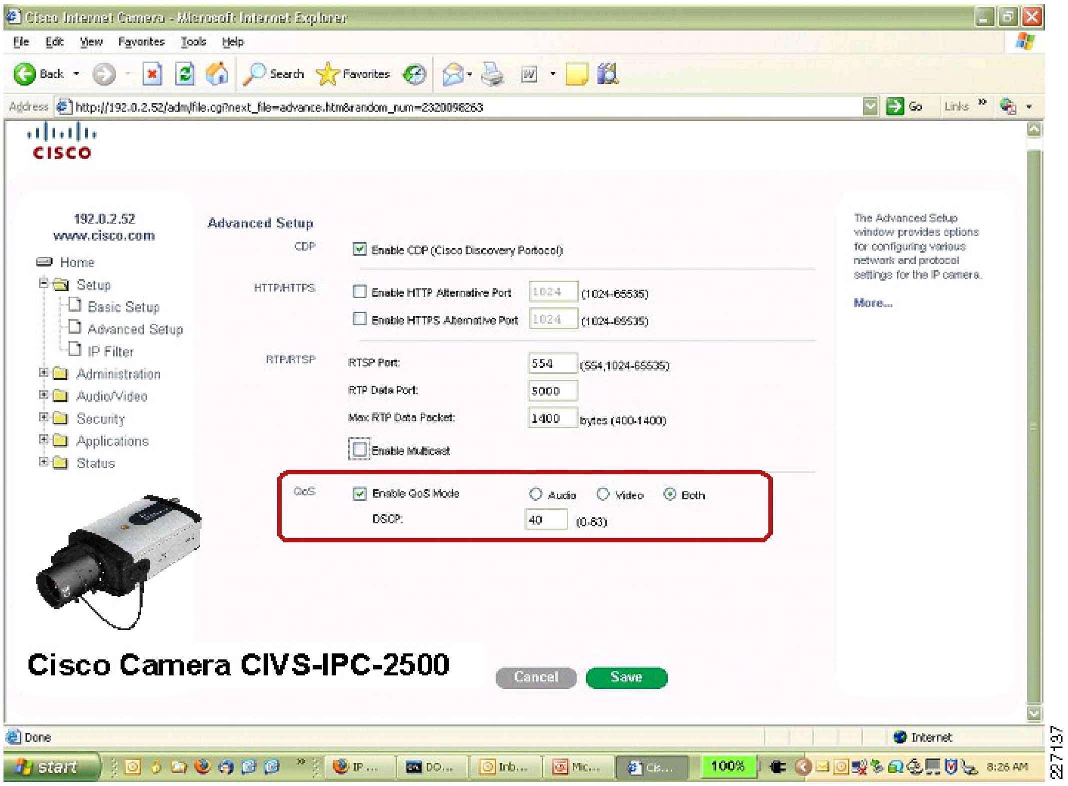
Given the initial premise that the viewing station and servers are not marking IP packets with DSCP values, the later sections of this chapter will provide some examples of how an access switch can be configured to mark traffic on the port servicing these devices. In the following section, an example is provided that shows using the ISR router to mark on ingress from the logical interface when the Media Server and VSOM resides on a VMSS network module. The example shows marking flows from the Media Server (HTTP web server) port as CS5 and the remaining flows as CS3. Recall from the previous section that the Media Server originates TCP sessions for HTTPS and RTSP to an IP camera to initiate video feeds. The model assumes, therefore, that any flows that are not sources from TCP port 80 are control plane traffic to an IP camera. These flows could be specifically identified by source port if the network manager desires.

Tip If a backup Media Server is defined for a video archive, the network manager may wish to mark these flows to the IP address of the backup Media Server as AF11 for inclusion in the HIGH-THROUGHPUT-DATA class.

Enabling QoS Marking by the IP Video Surveillance Camera

The Cisco IP Video Surveillance camera firmware, and that of other manufacturers, provides a dialog within the configuration section of the camera API to set QoS parameters for traffic originating from the camera. In some implementations, it is limited to the video and audio media streams; in others, more granularity is provided to various types of traffic. In many implementations, this is in the form of a Layer-3 QoS value such as a DSCP decimal value. Figure 12 shows a screen snapshot from a Cisco 2500 Series camera where the QoS parameters are entered.

Figure 12 Advanced Setup Menu—Cisco 2500 series Video Surveillance Camera



Address: http://192.0.2.52/adm/file.cgi?next_file=advance.htm&random_num=2320098263

Advanced Setup

CDP ☑ Enable CDP (Cisco Discovery Portocol)

HTTP/HTTPS
☐ Enable HTTP Alternative Port 1024 (1024-65535)
☐ Enable HTTPS Alternative Port 1024 (1024-65535)

RTP/RTSP
RTSP Port: 554 (554,1024-65535)
RTP Data Port: 5000
Max RTP Data Packet: 1400 bytes (400-1400)
☐ Enable Multicast

QoS ☑ Enable QoS Mode ○ Audio ○ Video ● Both
DSCP: 40 (0-63)

The Advanced Setup window provides options for configuring various network and protocol settings for the IP camera.

Table 8 is useful for selecting the correct decimal value to enter in the DSCP field.

Table 8 DSCP - IP Precedence - Reference Table

Code Point	IP Precedence	DSCP (binary)	DSCP (decimal)
Default	0	000000	0
CS1	1	001000	8
CS2	**2**	**010000**	**16**
CS3	**3**	**011000**	**24**
CS4	4	100000	32
CS5	**5**	**101000**	**40**
CS6	6	110000	48
CS7	7	111000	56

Note The values **CS2**, **CS3**, and **CS5** are highlighted in Table 8, because these values are recommended for network management, control and media streams from the IP cameras.

Medianet Switches

The Cisco Catalyst 2960, 2975, 3560G, 3750G, 3560-E, and 3750-E family of switches are access-layer switches that can be used for IP Video Surveillance deployments. These are considered medianet switches, meaning that they include Gigabit-Ethernet interfaces and implement in hardware a strict priority queue with at least three additional queues. The configuration examples are based on this family of switches unless otherwise noted.

Smartports Macros for IP Cameras

Smartports macros are a means of defining a collection of commands to quickly apply a common configuration for like devices. Because there may be hundreds or even thousands of IP cameras in the network, using a Smartport macro ensures that the port configuration are consistent.

The following sample Smartport macro is recommended for an IP camera. It defines the port as an access-port and the VLAN identifier is passed as a parameter to the macro. Port security may be enabled as shown, if the network manager chooses to implement this feature. Portfast is enabled to more quickly begin forwarding traffic on the port.

In this chapter the focus is on QoS, and the **mls qos trust dscp** command is included in the macro as shown:

```
macro name CIVS-IPC-2500
description Cisco Video Surveillance 2500 Series IP Camera
switchport mode access
switchport access vlan $VLAN
switchport port-security
switchport port-security mac-address sticky
switchport port-security maximum 1
switchport port-security violation shutdown
mls qos trust dscp
spanning-tree portfast
spanning-tree bpdufilter enable
load-interval 60
no shutdown
@
```

The macro is applied from interface configuration mode by specifying the name of the macro and any parameters. In this sample, the only variable substitution is the VLAN ID.

```
macro apply CIVS-IPC-2500 $VLAN 208
```

After modifying the configuration, be sure to save the running configuration using the following command:

```
write memory
```

The following output is an example of applying the macro to an interface:

```
3750-access(config)#interface gigabitEthernet 1/0/2
3750-access(config-if)#macro apply CIVS-IPC-2500 $VLAN 208
%Warning: portfast should only be enabled on ports connected to a single  host. Connecting
hubs, concentrators, switches, bridges, etc... to this  interface  when portfast is
enabled, can cause temporary bridging loops.  Use with CAUTION
%Portfast has been configured on GigabitEthernet1/0/2 but will only  have effect when the
interface is in a non-trunking mode.
3750-access(config-if)#
```

Ingress Queueing for IP Cameras

The Smartport macro previously illustrated contains the interface command **mls qos trust dscp** command, which directs the switch to honor the DSCP values set in the IP packets by the camera. IP camera is marking the media stream as DSCP value CS5. The default configuration puts CS5 traffic in the Ingress-PQ Threshold 1 (Q2T1). No additional explicit configuration commands are needed for ingress queuing.

There is no need to implement the Layer-2 CoS feature in the Cisco 4000 Series camera when the DSCP value is set by the camera and the switch trusts the DSCP value.

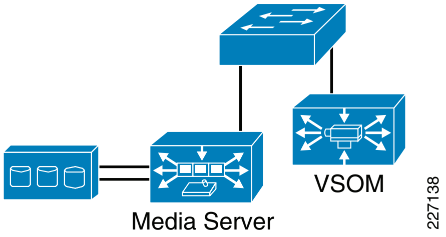
Tip CSCsz45893 Layer-2 CoS (802.1Q/p) for 4000 Series IP Camera provides additional information.

The recommendation is not to implement Layer-2 CoS for the 4000 Series IP camera.

Ingress Marking for Servers

In this section a sample access switch configuration for a port connecting to a standalone server or physical security multiservice platform is shown. The assumption is that the server is not setting the DSCP values or the values are not trusted by the network administrator.

Figure 13 Ingress Marking for Servers—Topology Diagram



The sample access switch configuration is shown below. An access-control list is configured to match on traffic originating from TCP port 80. Packets matching this access-control list are predominately live or archive video feeds from the Media Server to the client-viewing station. This is marked as DSCP value **CS5** and the remaining traffic is assumed to be primarily control plane and is marked **CS3**.

The service-policy is applied as an ingress policy.

```
hostname 3750-access
!
! System image file is "flash:c3750-advipservicesk9-mz.122-44.SE1.bin"
!
class-map match-all HTTP_acl
 match access-group name HTTP
!
policy-map VSMS
 class HTTP_acl
  set dscp cs5
 class class-default
  set dscp cs3
!
ip access-list extended HTTP
 permit tcp any eq www any
```

```
!
!
interface GigabitEthernet1/0/4
 description Physical Security Multiservices Pfm
 switchport access vlan 208
 switchport mode access
 priority-queue out
 spanning-tree portfast
 spanning-tree bpdufilter enable
 service-policy input VSMS
!
end
```

Tip The ***show policy-map interface*** command can be used to verify the service policy is matching and marking packets as intended.

The **priority-queue out** command is addressed in the "Egress Queueing for IP Cameras, Servers and Viewing Stations" section on page 6-32.

Ingress Marking for Video Management and Storage System Network Module

The Cisco Video Management and Storage System Network Module (VMSS) is a logical interface in the branch ISR router. This network module runs the Media Server and Video Surveillance Operation Manager (VSOM) software. In a deployment where this software runs on a Physical Security Multiservices Platform or stand-alone server, the QoS marking can be implemented on the LAN switch port connecting the server to the network. Because the network module implementation is a logical interface on the router, an ingress service policy is applied to the interface to mark media traffic and control plane traffic as it exists the logical interface. The relevant QoS commands are highlighted in blue in the following configuration sample.

```
!
interface Integrated-Service-Engine1/0
 ip vrf forwarding IPVS
 ip address 192.0.2.1 255.255.255.252
 ip flow ingress
 load-interval 30
 service-module external ip address 192.168.111.2 255.255.255.0
 service-module ip address 192.0.2.2 255.255.255.252
 service-module ip default-gateway 192.0.2.1
 no keepalive
 service-policy input INGRESS_VMSS
!
class-map match-any VMSS
 match access-group name HTTP
!
ip access-list extended HTTP
 permit tcp host 192.0.2.2 eq www any
!
policy-map INGRESS_VMSS
 class VMSS
  set ip dscp cs5
 class class-default
  set ip dscp cs3
!
end
```

There are two primary types of traffic leaving this logical interface and entering the IP network.

- Web traffic with a source port of 80; this is the video feeds from the Media Server to a client-viewing station.
- VSOM web traffic displaying the operator/administrator portal.

The Media Server also originates HTTP/HTTPS traffic to IP cameras for authentication and control of Motion JPEG feeds as well as RTSP command and control to IP cameras.

The basic QoS policy, therefore, is to mark TCP packets (port 80) from the logical interface with a DSCP value of **CS5** (BROADCAST-VIDEO) and mark all other traffic originated from the module **CS3** (CALL- SIGNALING).

The following **show policy-map** command was issued while a client-viewing station is watching the five video camera feeds on the ISR router.

```
vpn1-2851-1#show policy-map interface integrated-Service-Engine 1/0
 Integrated-Service-Engine1/0

  Service-policy input: INGRESS_VMSS

    Class-map: VMSS (match-any)
      760222 packets, 921342070 bytes
      30 second offered rate 7923000 bps, drop rate 0 bps
      Match: access-group name HTTP
        760222 packets, 921342070 bytes
        30 second rate 7923000 bps
      QoS Set
        dscp cs5
          Packets marked 760222

    Class-map: class-default (match-any)
      892 packets, 101243 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        dscp cs3
          Packets marked 892
vpn1-2851-1#
```

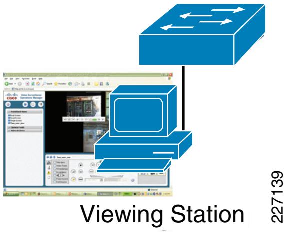
Note In this example, the video camera feed for one client-viewing station is generating approximately 8Mbps.

Ingress Marking for Viewing Stations

In the video surveillance system, there are client-viewing stations that are used to view live or archived camera feeds. The volume of packets going to the viewing station varies based on the number of cameras being displayed on the operator pane and the bit-rate and resolution of the video feeds.

The predominate type of IP packets originating from the viewing station are TCP acknowledgements, HTTP GETS and polling requests to the VSOM and Media Server web servers. This is all very low bandwidth flows from the viewing station. However, dropping of any of these packets in the network will impact the overall user experience. The viewing station is connected to an access port at the branch or campus location. See Figure 14.

Figure 14 Ingress Marking for Client Viewing Stations—Topology Diagram



This sample configuration below is very similar to that shown in "Ingress Marking for Servers" section on page 6-29. However, it specifically shows a sample of a matching on packets with a destination TCP port 80 rather than a source port 80.

```
hostname 3750-access
!
! System image file is "flash:c3750-advipservicesk9-mz.122-44.SE1.bin"
!
class-map match-all HTTP_acl_client
 match access-group name HTTP_client
!
policy-map Viewing_Station
 class HTTP_acl_client
  set dscp cs5
 class class-default
  set dscp cs3
!
ip access-list extended HTTP_client
 permit tcp any any eq www
!
!
interface GigabitEthernet1/0/5
 description Viewing Station
 switchport access vlan 208
 switchport mode access
 priority-queue out
 spanning-tree portfast
 spanning-tree bpdufilter enable
 service-policy input Viewing_Station
!
end
```

Tip The interface counters on this switch port will typically show the majority of the total bytes output to the viewing station with a relatively small number of bytes input from this viewing station. The video feeds are very unidirectional.

Egress Queueing for IP Cameras, Servers and Viewing Stations

The nature of the traffic flows between IP cameras, servers, and viewing stations are discussed in "End-to-End QoS Marking" section on page 6-24. There is minimal traffic flow from the LAN to the IP camera; as a result, there is little need to enable egress priority-queueing on a switch port connecting to a camera.

As a general best practice, it is recommended to enable egress priority-queueing on uplink ports and trunk ports between switches. The Layer-2 priority queue (1P3Q3T) is enabled with the **priority-queue out** interface command. Queue 1 is the priority queue, and it is serviced until empty before the other queues are serviced. By default, packets with a DSCP value of **CS5** (decimal **40**) are mapped to queue 1. Because the video media streams are marked DSCP **CS5**, the video traffic is serviced by the priority queue.

```
!
interface GigabitEthernet1/0/1
 description Uplink port
 switchport trunk encapsulation dot1q
 switchport mode trunk
 priority-queue out
 mls qos trust dscp
!
```

For most IPVS deployments, enabling egress priority-queueing is sufficient with all other options addressed by the default configuration values.

QoS on Routed WAN/MAN Interfaces

This section discusses QoS on MAN/WAN interfaces implementing egress shaping and queueing techniques. The branch router shown in the sample configuration has one interface configured to demonstrate Hierarchical Class-Based Weighted fair Queueing (HCBWFQ) and a second interface configuration applies a shaper for each class. These two techniques are shown because the bandwidth required to transport video from branch to campus will very likely require 50 to 100Mbps and a common deployment for these data rates is some form of Metro-Ethernet service.

The HCBWFQ configuration is characterized by shaping the Ethernet interface to an aggregate rate and then queueing the individual classes within that shaped rate. When using this shaper on the Ethernet interface, the congestion feedback mechanism is provided by the shaper function rather than the transmit (TX) ring of a serial interface. The child service policy referenced from the parent or shaper service policy could also be directly applied to a comparable speed physical interface.

The per-class shaper configuration may be used on a Metro-Ethernet service provider network where a service level agreement (SLA) is specified for each class of traffic based on some QoS marking and the data rate is capped or policed for each individual class.

Both egress QoS techniques shown optionally set the Layer-3 or Layer-2 QoS values (DSCP or CoS) accordingly.

For more detailed information on QoS for WAN/MAN handoff from a service provider, refer to the *Ethernet Access for Next Gen Metro and Wide Area Networks* at the following URL:

> http:www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_MAN_WAN_V3.1_external.html

For additional information and detailed QoS configuration examples for the whole range of LAN switches and line cards suitable for IP Video Surveillance deployments, refer to the *Medianet Campus QoS Design 4.0* at the following URL:

> http://www.cisco.com/go/designzone

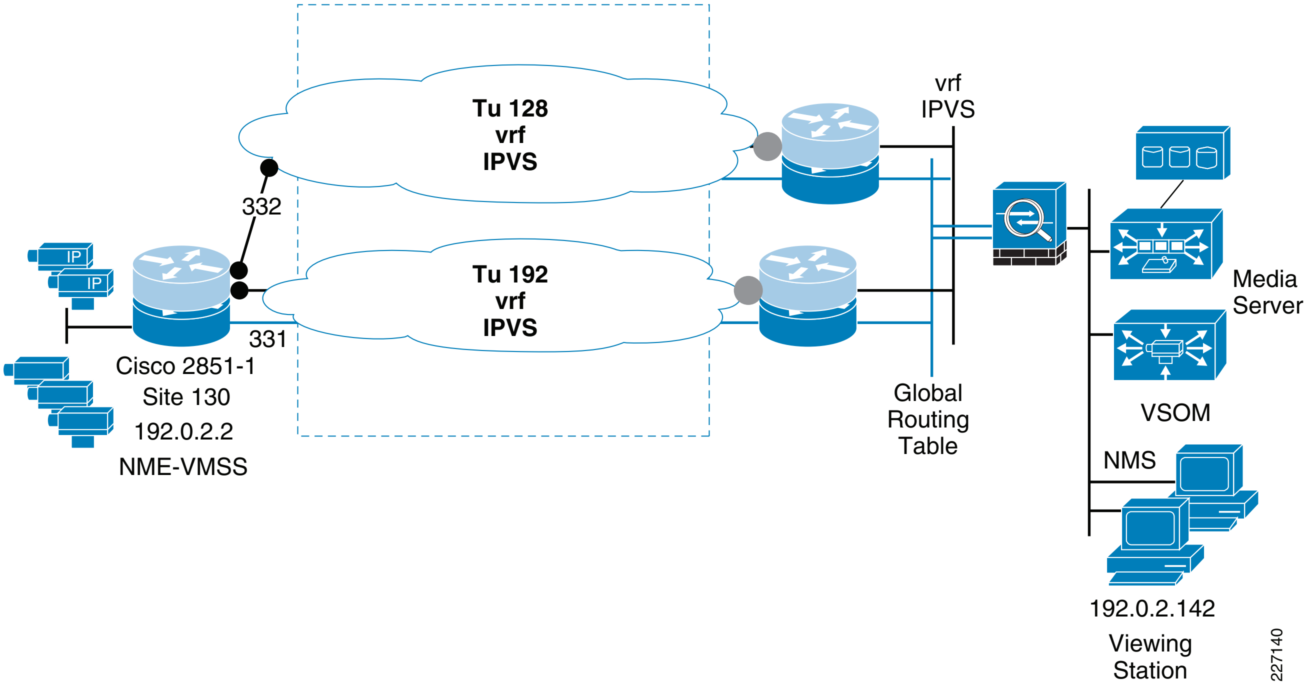
Topology

The configuration examples shown in this section are from the deployment topology from the "Virtualization, Isolation and Encryption of IP Video Surveillance" section on page 6-87. The network traffic is generated by a client-viewing station in the command center campus location. Labeled on the drawing as IP address 192.0.2.142 in Figure 15. This workstation is viewing a six-pane operator screen viewing five cameras at the branch location. Two cameras are IP cameras and three of the cameras are analog cameras attached to an Analog Video Gateway (AVG) at the branch location.

The branch router is an ISR 2851 with a NME-VMSS network module in addition to the AVG network module. The WAN interface is a Gigabit-Ethernet handoff into a service provider MAN network. There are two point-to-point virtual circuits (IEEE 802.1q) VLANs through the service provider network, one to each of the WAN aggregation routers at the central campus location.

There are two DMVPN tunnel interfaces, each sourced from one of the point-to-point links. Interface Tunnel 128 (in VRF IPVS) is transported over VLAN 332, interface tunnel 192 (in VRF IVPS) is transported over VLAN 331. The EIGRP configuration implements an *offset-list* in the EIGRP configuration. When both tunnels are up and active, the preferred path is over tunnel128. Traffic is forced over the backup path during testing by disabling ISAKMP (**no crypto isakmp enable** command) and clearing the IPSec security associations, effectively clearing and disabling the crypto tunnel from that WAN aggregation router. The topology is shown in Figure 15.

Figure 15 Topology for QoS on Routed WAN / MAN Interfaces



Ethernet Access—Per Class Shaping

Of the two WAN/MAN interfaces in this sample topology, one sub-interface is configured to transport the viewing of IP video surveillance feeds by a remote client-viewing station where the service provider offers a QoS-enabled WAN/MAN with four categories of traffic; real-time for VoIP and video, two distinct bandwidth classes and a default class. Each class is policed by the service provider to the contracted data rate within the SLA.

All classes are shaped with the exception of the real-time class. The per-class shaper for the classes GOLD, BRONZE and class-default provides a smoothing of the traffic flow into the service provider network with the goal of keeping these classes from being policed and dropped by the service provider.

The real-time class is not shaped, rather policed, but policed without a drop action. Shaping in the real-time class would introduce latency and jitter. The goal of this class is to identify if the real-time class is exceeding the configured data rate. The network manager must calculate how much bandwidth is required by the real-time class and use any techniques available to keep this class within the contracted data rate. Drops in the real-time class, either VoIP or video traffic, will degrade the quality of experience and must be avoided. In the case of VoIP, call admission control (CAC) techniques such as gatekeepers or locations in CallManager can be deployed. For the IP Video Surveillance traffic, it is more challenging as there is no global CAC technique in the application. Within VSOM, restricting what operator views are available to remote users can be used as well as defining bandwidth caps in the viewing panes. This, however, is not automatic and requires some coordination between the the network manager and the physical security manager to manage the real-time traffic in this class.

The following configuration implements per-class shaping:

```
!
interface GigabitEthernet0/1.332
 encapsulation dot1Q 332
 ip address 192.168.15.46 255.255.255.252
 service-policy output PER_CLASS_SHAPING
!
policy-map PER_CLASS_SHAPING
 class REAL_TIME
  set cos 5
    police 40000000 conform-action transmit  exceed-action transmit
 class GOLD
  shape average 2500000
  set cos 6
 class BRONZE
  shape average 2500000
  set cos 1
 class class-default
  set cos 0
  shape average 5000000
!
```

Because the DiffServ QoS recommendation is a twelve-class model and this service provider is offering four classes, the applications need be consolidated from twelve to four classes.

```
!
class-map match-any GOLD
 match ip dscp cs2  cs3  cs6  cs7
 match ip dscp af41  af42  af43
 match ip dscp af31  af32  af33
!
class-map match-any BRONZE
 match ip dscp af11  af12  af13
 match ip dscp cs1
!
class-map match-any REAL_TIME
 match ip dscp cs5
 match ip dscp cs4
 match ip dscp ef
!
end
```

The output interface (GigabitEthernet0/1.332) is in the global routing table, while the DMVPN tunnel interface sourced from the physical interface is transporting the packets.

```
vpn1-2851-1#show int tunnel 128 | include rate
  Queueing strategy: fifo
  5 minute input rate 371000 bits/sec, 679 packets/sec
  5 minute output rate 7784000 bits/sec, 815 packets/sec
```

The **show policy-map** command can be used to verify that packets are matching the appropriate class and also to report on the data rate of the applications in each class.

```
vpn1-2851-1#show policy-map interface gigabitEthernet 0/1.332
 GigabitEthernet0/1.332

  Service-policy output: PER_CLASS_SHAPING

    Class-map: REAL_TIME (match-any)
      638277 packets, 817396506 bytes
      30 second offered rate 8335000 bps, drop rate 0 bps
      Match: ip dscp cs5 (40)
        638277 packets, 817396506 bytes
        30 second rate 8335000 bps
      Match: ip dscp cs4 (32)
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: ip dscp ef (46)
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        cos 5
          Packets marked 638277
      police:
          cir 40000000 bps, bc 1250000 bytes
        conformed 638277 packets, 817396506 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          transmit
        conformed 8335000 bps, exceed 0 bps

    Class-map: GOLD (match-any)
      338 packets, 36594 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs2 (16) cs3 (24) cs6 (48) cs7 (56)
        338 packets, 36594 bytes
        30 second rate 0 bps
      Match: ip dscp af41 (34) af42 (36) af43 (38)
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: ip dscp af31 (26) af32 (28) af33 (30)
        0 packets, 0 bytes
        30 second rate 0 bps
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          2500000/2500000   15000  60000     60000     24        7500

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         338       36612     0         0         no
      QoS Set
        cos 6
          Packets marked 338

    Class-map: BRONZE (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp af11 (10) af12 (12) af13 (14)
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: ip dscp cs1 (8)
        0 packets, 0 bytes
        30 second rate 0 bps
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          2500000/2500000   15000  60000     60000     24        7500

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         0         0         0         0         no
      QoS Set
        cos 1
          Packets marked 0

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        cos 0
          Packets marked 0
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
          5000000/5000000   31250  125000    125000    25        15625

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         0         0         0         0         no
vpn1-2851-1#
```

Hierarchical Class-Based Weighted Fair Queueing

The second interface demonstrates applying a service policy on the Gigabit interface shaping the output traffic in aggregate to 50Mbps. Within that data rate, a child service policy (IPVS_BRANCH) is referenced to provide queueing within that shaped rate.

```
!
interface GigabitEthernet0/1.331
 encapsulation dot1Q 331
 ip address 192.168.15.22 255.255.255.252
 service-policy output UPLINK_50M
!
policy-map IPVS_BRANCH
 class BROADCAST-VIDEO
  bandwidth percent 40
 class VOICE
  priority percent 10
 class LOW-LATENCY-DATA
  bandwidth percent 4
 class HIGH-THROUGHPUT-DATA
```

```
  bandwidth percent 4
 class MULTIMEDIA-CONFERENCING
  bandwidth percent 4
 class SCAVENGER
  bandwidth percent 1
 class OAM
  bandwidth percent 1
 class NETWORK-CONTROL
  bandwidth percent 1
 class CALL-SIGNALING
  bandwidth percent 1
 class class-default
  fair-queue
policy-map UPLINK_50M
 class class-default
  shape average 50000000
  service-policy IPVS_BRANCH
```

Because the service provider is offering a SLA for the aggregate bandwidth of 50Mbps, the service policy can be more granular at the interface level than was the case in the per-class shaper example shown previously. In this example, the branch router is referencing nine of the twelve application classes in the DiffServ QoS Recommendations.

```
!
class-map match-any LOW-LATENCY-DATA
 match ip dscp af21  af22  af23
class-map match-any HIGH-THROUGHPUT-DATA
 match ip dscp af11  af12  af13
class-map match-all BROADCAST-VIDEO
 match ip dscp cs5
class-map match-all NETWORK-CONTROL
 match ip dscp cs6
class-map match-any MULTIMEDIA-CONFERENCING
 match ip dscp af41  af42  af43
class-map match-all OAM
 match ip dscp cs2
class-map match-all VOICE
 match ip dscp ef
class-map match-all SCAVENGER
 match ip dscp cs1
class-map match-any CALL-SIGNALING
 match ip dscp cs3
!
end
```

The **show policy-map** command can be used to verify packets are matching the correct class and provide insight into the data rate of application in each class.

```
vpn1-2851-1#show policy-map  interface gigabitEthernet 0/1.331
 GigabitEthernet0/1.331

  Service-policy output: UPLINK_50M

    Class-map: class-default (match-any)
      621338 packets, 792463266 bytes
      30 second offered rate 8339000 bps, drop rate 0 bps
      Match: any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
         50000000/50000000  312500 1250000   1250000   25        156250
        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        -      0         621338    792463284 0         0         no

      Service-policy : IPVS_BRANCH

        Class-map: BROADCAST-VIDEO (match-all)
          620942 packets, 792420308 bytes
          30 second offered rate 8339000 bps, drop rate 0 bps
          Match: ip dscp cs5 (40)
          Queueing
            Output Queue: Conversation 265
            Bandwidth 40 (%)
            Bandwidth 20000 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

        Class-map: VOICE (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp ef (46)
          Queueing
            Strict Priority
            Output Queue: Conversation 264
            Bandwidth 10 (%)
            Bandwidth 5000 (kbps) Burst 125000 (Bytes)
            (pkts matched/bytes matched) 0/0
            (total drops/bytes drops) 0/0

        Class-map: LOW-LATENCY-DATA (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af21 (18) af22 (20) af23 (22)
            0 packets, 0 bytes
            30 second rate 0 bps
          Queueing
            Output Queue: Conversation 267
            Bandwidth 4 (%)
            Bandwidth 2000 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

        Class-map: HIGH-THROUGHPUT-DATA (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af11 (10) af12 (12) af13 (14)
            0 packets, 0 bytes
            30 second rate 0 bps
          Queueing
            Output Queue: Conversation 268
            Bandwidth 4 (%)
            Bandwidth 2000 (kbps)Max Threshold 64 (packets)
            (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0

        Class-map: MULTIMEDIA-CONFERENCING (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af41 (34) af42 (36) af43 (38)
            0 packets, 0 bytes
            30 second rate 0 bps
          Queueing
            Output Queue: Conversation 269
            Bandwidth 4 (%)
```

```
        Bandwidth 2000 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

    Class-map: SCAVENGER (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs1 (8)
      Queueing
        Output Queue: Conversation 270
        Bandwidth 1 (%)
        Bandwidth 500 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

    Class-map: OAM (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs2 (16)
      Queueing
        Output Queue: Conversation 266
        Bandwidth 1 (%)
        Bandwidth 500 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

    Class-map: NETWORK-CONTROL (match-all)
      396 packets, 42958 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs6 (48)
      Queueing
        Output Queue: Conversation 271
        Bandwidth 1 (%)
        Bandwidth 500 (kbps)Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

    Class-map: CALL-SIGNALING (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: ip dscp cs3 (24)
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
        Output Queue: Conversation 272
        Bandwidth 1 (%)
        Bandwidth 500 (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)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
        Flow Based Fair Queueing
        Maximum Number of Hashed Queues 256
    (total queued/total drops/no-buffer drops) 0/0/0
vpn1-2851-1#
```

Caveats for Catalyst 4500 and 6500 Series

The Catalyst 4500 switch family only supports egress queuing models. On the classic supervisor, it can be configured as a 1P3Q1T mode, which is recommended for voice and video applications. On the supervisor 6-E it can be configured for a 1 priority queue add up to 7 bandwidth queues (1P7Q1T.)

The Catalyst 6500 Series switches support both ingress and egress queueing based on the supervisor model and policy feature card option installed. Additionally, there are line cards that support 10/100/1000 Ethernet and provide ingress queueing supporting a strict priority hardware queue with at least three additional hardware queues. For details, refer to the *Medianet Campus QoS Design 4.0* at the following URL:

http://www.cisco.com/go/designzone

Summary

All forms of video traffic on the enterprise network greatly increases the bandwidth requirements for both LAN and WAN. The existing QoS policies must include new application classes to support the various types of video traffic. For IP video surveillance, the recommended marking for the media streams is the DSCP value of **CS5**. This can be set by end nodes, such as IP cameras, or by a switch or router. While the majority of video traffic introduced by video surveillance are the media streams, the control plane and network management traffic should also be marked appropriately as well.

Local Storage for Video Archives Using iSCSI

The objections of this section is to understand the storage requirements for IP Video Surveillance at a branch location. Then, to support the iSCSI server, a branch topology is shown to provide network access to the iSCSI server for configuration and management as well as for the transport of the TCP session between the VMSS network module and the iSCSI server.

An example of how to configure the iSCSI server and format the volume for use and then select the volume for storing archives from the Video Surveillance Management Console (VMSC). There is also sample configurations and **show** commands relevant to the iSCSI file system.

Disk Space Requirements

There are many iSCSI servers in the market which provide data protection by using various RAID levels for data protection. RAID 5 is commonly used due to its low cost of redundancy. For example, a system advertised at 1 Terabyte has four individual disks, each with a raw capacity of 232 Gigabytes per disk, for a total capacity of (232 * 4) 928 Gigabytes of storage. With RAID mode 5, the usable capacity is 676 Gigabytes of usable space. With RADI mode 1 only half the total capacity is available for use. It is important to consider the usable capacity of the iSCSI server, as well as the initial cost of the chassis, the number of disk drives included in the entry level system, as well as the number of empty expansion bays available. Before selecting a system, make sure the usable capacity will meet the storage requirements of the site.

Typically the most cost effective solution on a per-Gigabyte basis is a fully populated chassis. This spreads the cost of the chassis over the maximum number of disks. On the market today, iSCSI storage can be obtained for for less than $2.00 per GB using SATA drives. Systems are available that range in scale from 2 to 96 Terabytes (TBs) of storage. Entry level systems that may support 1, 2, or 4 TB of raw storage may range in price less than $5000 USD, but for systems that support up to 96 TB of storage, the initial, minimal chassis investment may be $8,000 USD or more.

To provide some guidance on the amount of disk space required for a typical branch video surveillance deployment, Table 1 shows the amount of space required for a one-hour archive. Various media types, resolution, frame rate/target bit rates are shown for the Cisco 2500 Series IP camera as well as other cameras.

Table 1 Disk Space Required for One Hour Archive

	Media Type	Resolution	Rate (Frames or Bits Per Second	Reserved Mbytes	Actual Mbytes
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	512	241	243
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	768	347	357
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	1024	475	480
AutoDome - Analog GW	MPEG-4	704 x 480 (4CIF)	1024	477	462
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	2000	953	943
Cisco CIVS-IPC-2500	MPEG-4	720 x 480 (D1)	4000	1,860	1,800
Axis 223M	MJPEG	1600 x 1200	5	1,840	1,850
Axis 223M	MPEG-4	640 x 480 (VGA)	2000	931	68
Axis 207	MPEG-4	640 x 480 (VGA)	1024	477	405
Axis 207MW	MJPEG	1280 x 720	10	812	5,000

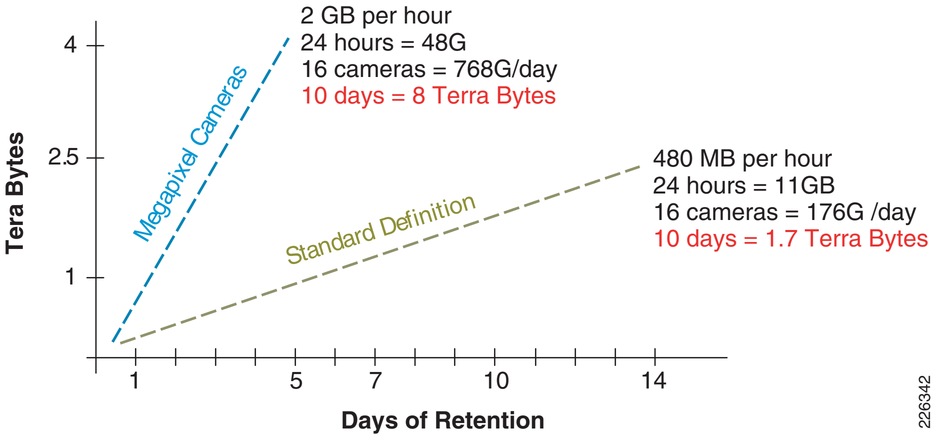
Now that a baseline is provided for an archive of one-hour duration, the next section shows an estimate of the total amount of storage required for multiple cameras based on a typical retention period.

Archive Retention and Storage Requirements

Given the enterprise may deploy standard definition cameras today and consider a megapixel (high) definition cameras in the future, or have a mixture of both, we look at both in this analysis. The Axis 223M is a megapixel camera with a resolution of 1600 x 1200 pixels. At 5 frames per-second, this camera requires almost 2GB per-hour of archived recording. The Cisco 2500 Series standard definition camera at 720x480 (D1) resolution with a target bit-rate of 1024Kbps requires 480MB of disk space per-hour of archive retained.

Assuming the enterprise has a retention period of 10 days per camera, a 16 camera deployment archiving 24 hours per day requires between 2 and 8TB of storage capacity. The megapixel camera has almost four times the storage requirements as the standard definition camera. This is illustrated in Figure 16.

Figure 16 Branch Office Video Surveillance Storage Requirements



Retention periods vary from organization to organization and some cameras may have a longer retention period than others. There may be multiple archives created from a single camera, with the longer retention period having a lower frame rate while a higher frame rate may have a retention of only a few days. Some archives are initiated only on triggered events. Additionally, the amount of storage for stored clips (local BWM/X clip repository) and backup (backup repository) must also be considered. Capacity for future camera installations as well as replacement of standard definition with high definition in the future must also be considered.

VMSS Network Module

This section provides a brief overview of the available hardware configurations of the VMSS network module. There are three models of VMSS network modules. Their characteristics are shown in Table 9.

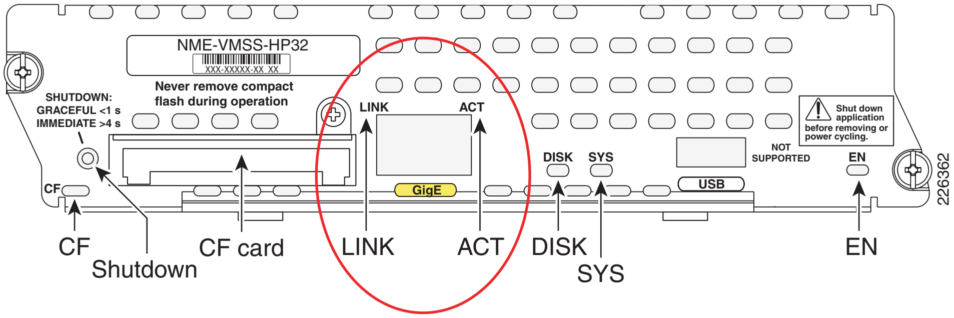
Table 9 VMSS Models

Model	Processor	Hard Disk	Memory
NME-VMSS-16	1.0 GHz	120 GB (SATA)	512 MB
NME-VMSS-HP16	1.4 GHz	160 GB (SATA)	2 GB
NME-VMSS-HP32	1.4 GHz	160 GB (SATA)	2 GB
NME-VMSS2-16	1.4 GHz	500 GB	2 GB
NME-VMSS2-HP32	1.4 GHz	500 GB	2 GB

Not all the listed hard disk space is available for archives, because the operating system files are contained on the disk as well. To meet the video archive storage requirements of the branch location that requires more storage is available on the network modules, attaching an Internet SCSI (iSCSI) appliance to the VMSS network module external interface is the preferred solution.

The VMSS faceplate has an external Gigabit Ethernet port for physically connecting to a switch to communicate with the iSCSI server. The location of the port is shown in Figure 17.

Figure 17 VMSS Faceplate Showing External GigabitEthernet

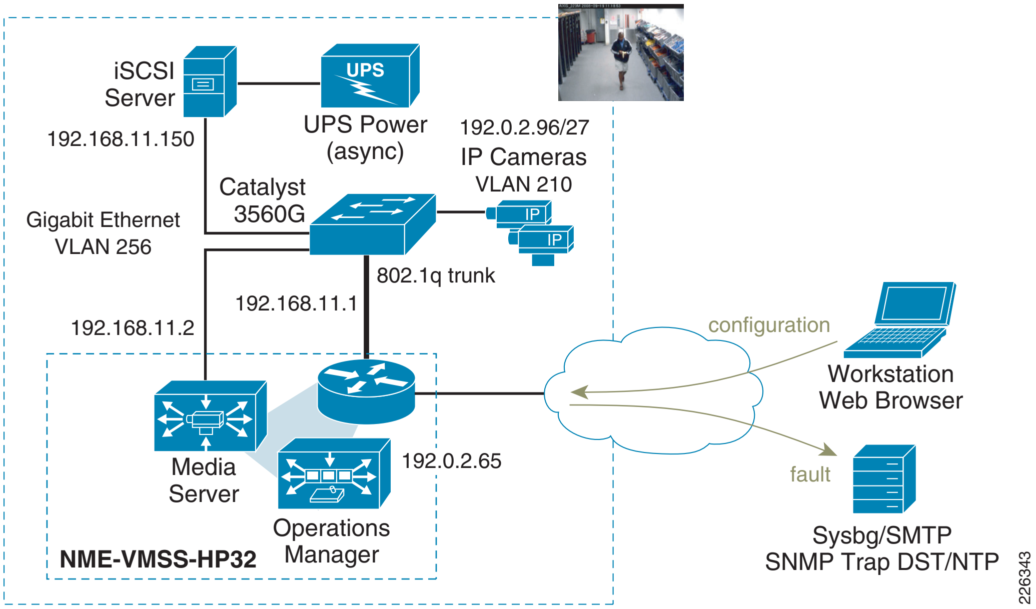


In testing three separate Buffalo TeraStation Pro II iSCSI Rackmount units are deployed on Cisco ISR 2851, 3825, and 3845 routers using the NME-VMSS-16, NME-VMSS-16HP and NME-VMSS-32 network modules. This brand of iSCSI server is used because of low initial cost, features, and availability. It is not a product recommendation. This server is available in 1,2, and 4TB configurations. In most customer deployments, servers with substantially higher storage capacity may be required.

Deployment Topology

A typical branch router deployment topology using iSCSI for local storage is shown in Figure 18.

Figure 18 Branch Router Deployment Topology using iSCSI



The LAN switch in this deployment is a Cisco Catalyst 3560G-48TS. This switch supports 48 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports in a 1RU form factor. The Cisco ISR router GigabitEthernet 0/1 interface is an 802.1q trunked interface. There is an isolated VLAN, 256, for the iSCSI network. The GigabitEthernet port on the face place of the VMSS network module is connected to a non-trunked switch port in VLAN 256. The Buffalo TeraStation Pro II iSCSI Rackmount TS-RI1.0TGL/R5 server is also attached to a non-trunked port on VLAN 256.

This iSCSI server has a facility for SMTP email alerts, NTP, syslog, and has an imbedded web server for configuration and management. To use these management functions and to access the server from the central campus location, the default gateway of the server is configured with the IP address of the branch router Gigabit Ethernet interface, 192.168.11.1. This network is advertised by the dynamic routing protocol (EIGRP) configured on the branch router.

The IP addressing of the router, external interface of the VMSS module and the iSCSI server are shown in Table 10.

Table 10 Devices and their IP Addresses

Device	IP Address
Branch router GigE VLAN 256	192.168.11.1
VMSS External Interface	192.168.11.2
iSCSI Server	192.168.11.150
VMSS-HP32 (VSOM/Media Server)	192.0.2.65

There are two interfaces connected to subnet 192.168.11.0/25 from the branch router; one through the GigabitEthernet interface on the ISR router chassis, the second through the external interface of the VMSS network module.

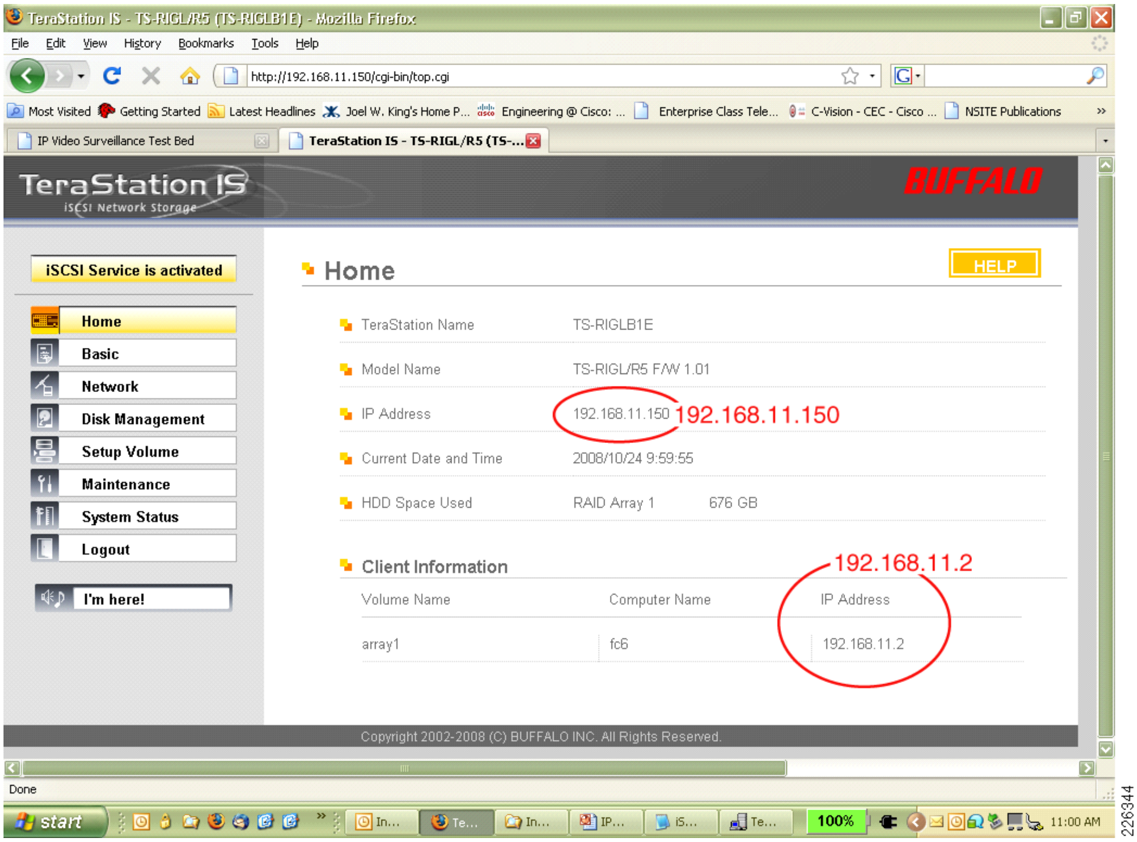
Installation and Configuration of iSCSI Server

This iSCSI server implementation uses DCHP to obtain an initial IP address, or if no DHCP server is accessible on the network, defaults to a documented static IP address. The recommended implementation approach is to configure a DHCP pool on the branch router, connect the iSCSI server to the network and and power up. After waiting a few minutes for the server to boot and obtain an IP address from this pool, use the **show ip dhcp binding** command to determine the IP address allocated to the server. Use a workstation and web browser to connect to the IP address of the server. The server used in testing also displays the IP address on the LCD status panel on the front of the unit.

From the web browser, change the default password, configure the NTP parameters, SNMP server, syslog server address, and any other parameters that may be relevant. Finally, change the IP address of the server to a static IP address and update this information in the corporate DNS services. Because the VMSS network module must be configured with a target IP address or hostname in the configuration, a static IP address is needed.

The following sample iSCSI configuration screen is shown in Figure 19.

Figure 19   Sample iSCSI configuration screen


TeraStation IS - TS-RIGL/R5 (TS-RIGLB1E) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.11.150/cgi-bin/top.cgi
Most Visited Getting Started Latest Headlines Joel W. King's Home P... Engineering @ Cisco: ... Enterprise Class Tele... C-Vision - CEC - Cisco ... NSITE Publications
IP Video Surveillance Test Bed
TeraStation IS - TS-RIGL/R5 (TS-...
TeraStation IS
iSCSI Network Storage
BUFFALO
iSCSI Service is activated
Home
Basic
Network
Disk Management
Setup Volume
Maintenance
System Status
Logout
I'm here!
HELP
192.168.11.150
192.168.11.2
Done
start
100%
11:00 AM
226344

Home

TeraStation Name	TS-RIGLB1E	
Model Name	TS-RIGL/R5 F/W 1.01	
IP Address	192.168.11.150	
Current Date and Time	2008/10/24 9:59:55	
HDD Space Used	RAID Array 1	676 GB

Client Information

Volume Name	Computer Name	IP Address
array1	fc6	192.168.11.2

Copyright 2002-2008 (C) BUFFALO INC. All Rights Reserved.

The screen shot in Figure 19 shows the VMSS network module's external address listed as a client connection at IP address 192.168.11.2. The IP address of the server is 192.168.11.150. The default gateway is the ISR router at address 192.168.11.1. Default network access through the router allows the iSCSI server to communicate with the corporate network devices through the ISR router while maintaining a direct, LAN-based connection to the iSCSI client, the VMSS network module.

Sample Branch Router iSCSI Configuration

The following configuration is the relevant portion of the branch router interfaces related to the iSCSI server deployment.

```
!
hostname vpn1-3845-1
!
interface GigabitEthernet0/1
 description Trunk
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1.150
 description Outside (WAN) Interface
 encapsulation dot1Q 150
 ip address dhcp
!
```

```
interface GigabitEthernet0/1.250
 description INSIDE VLAN
 encapsulation dot1Q 250
 ip address 10.81.7.1 255.255.255.248
!
interface GigabitEthernet0/1.256
 description iSCSI VLAN
 encapsulation dot1Q 256
```

This is the default gateway IP address for the iSCSI server.

```
 ip address 192.168.11.1 255.255.255.0

!
interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip address 192.0.2.64 255.255.255.254
 ip flow ingress
```

The VMSS operating system learns the external IP address from this configuration statement

```
 service-module external ip address 192.168.11.2 255.255.255.0
 service-module ip address 192.0.2.65 255.255.255.254
 service-module ip default-gateway 192.0.2.64
 no keepalive
!
router eigrp 64
 network 10.0.0.0
 network 192.0.2.64 0.0.0.63
```

A network statement for the iSCSI subnet is included to advertise this network to the intranet.

```
 network 192.168.11.0
 no auto-summary
 eigrp stub connected
!
end
```

Tip Following the configuration of the external IP address, the network module must be reloaded for the VMSS operating system to learn the configured address; for example, **service-module in2/0 reload**.

Verify IP Addressing on the VMSS Network Module

After completing the configuration of the external IP address and the module reload, use the **service-module** <*interface*> **session** command to access the console of the network module and verify the IP addresses are configured. Issue the **show interfaces** command as shown below.

```
VMSS-SITE140# show interfaces
GigabitEthernet 0 is up, line protocol is up
  Internet address is 192.0.2.65 mask 255.255.255.254 (configured on router)
     9101 packets input, 961197 bytes
     0 input errors, 0 dropped, 0 overrun, 0 frame errors
     9560 packets output, 2449037 bytes
     0 output errors, 0 dropped, 0 overrun, 0 collision errors
     0 output carrier detect errors

GigabitEthernet 1 is up, line protocol is up
  Internet address is 192.168.11.2 mask 255.255.255.0 (configured on router)
     382068 packets input, 31118652 bytes
     0 input errors, 0 dropped, 0 overrun, 0 frame errors
     8074102 packets output, 3415145010 bytes
     0 output errors, 0 dropped, 0 overrun, 0 collision errors
     0 output carrier detect errors

IDE hd0 is up, line protocol is up
     18699 reads, 2678064128 bytes
     0 read errors
     115791 write, 817836032 bytes
     0 write errors
```

If the GigabitEthernet 0 and 1 interfaces are not configured with an IP address from the router, verify the ISR router interface configuration and reload.

Formatting iSCSI Storage

The iSCSI storage must be formatted by the VMSS network module prior to use. While remaining on the console of the network module, enter configuration mode (**configure terminal**) and define the iSCSI tag (media 1 to 9) and target IP address of the iSCSI appliance. The IP address must be a static IP address defined in the corporate DNS, not the DHCP supplied IP address used in the initial configuration. The iSCSI server used in testing had an option to disable and enable the iSCSI service. Verify that the service is enabled, otherwise these steps will fail. The following examples assume the iSCSI tag is **media1**.

Configure the target IP address of ISCSI server as follows:

```
VMSS-SITE140(config)# storages iscsi media1
VMSS-SITE140(config-iscsi)# target-ip 192.168.11.150
VMSS-SITE140(config-iscsi)#exit
```

Verify/attach External Gig E port of the network module to the LAN switch as follows:

```
VMSS-SITE140(config)# storages iscsi media1
Modifying existing iscsi
VMSS-SITE140(config-iscsi)# state enable
iSCSI volume not formatted or unsupported file system:
VMSS-SITE140(config-iscsi)#exit
```

Format the storage as follows:

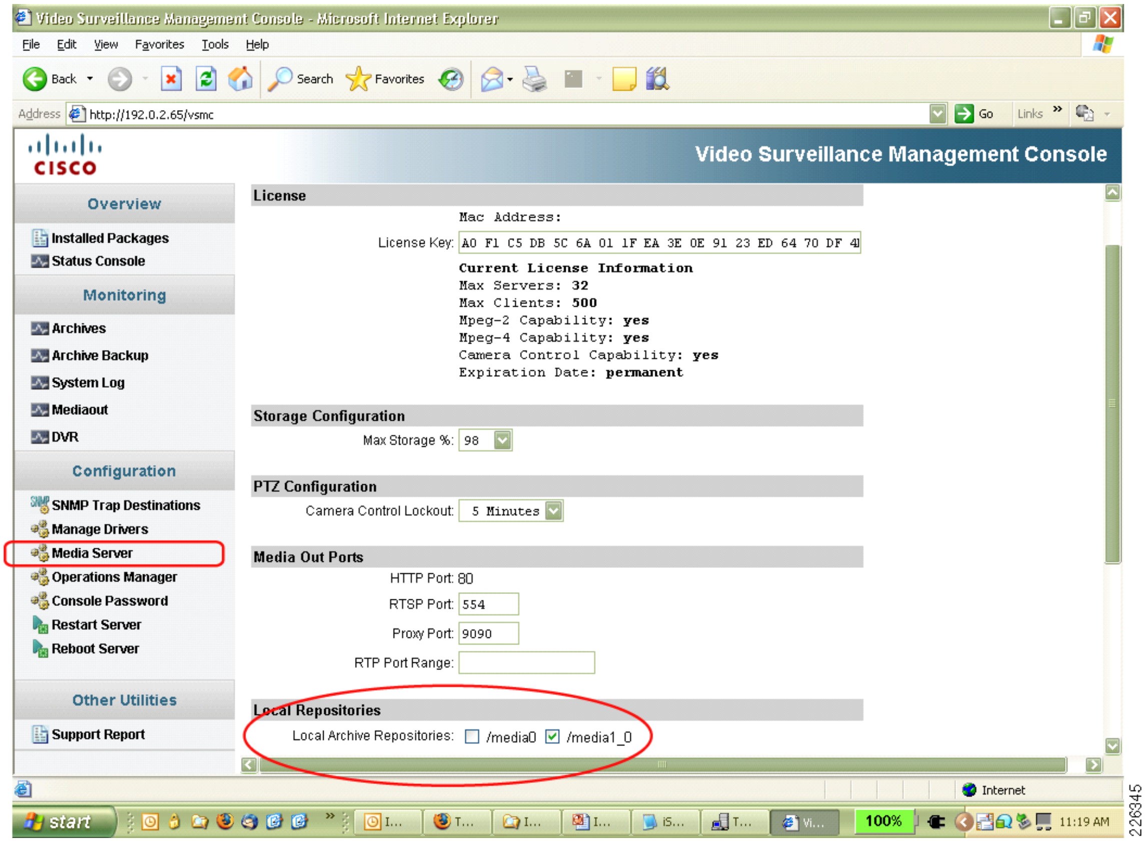
```
VMSS-SITE140# format storages iscsi media1
The storage device you are about to format has the following parameters:

Target name: iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D73262B1E:array1 LUN: 0

[output deleted for brevity]

Writing inode tables: done
Creating journal (8192 blocks): done
Writing superblocks and filesystem accounting information: done

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
    Done.
To use the storage, please issue "state disable" then "state enable"
 on media1

VMSS-SITE140(config)# storages iscsi media1
Modifying existing iscsi
VMSS-SITE140(config-iscsi)# state disable
VMSS-SITE140(config-iscsi)# state enable
Media successfully enabled!
```

At this point the volume is formatted and available for use.

Select iSCSI Volume for Use

Now that the volume is mounted and ready, connect to the Video Surveillance Management Console (http://192.0.2.65/vsmc) and select Media Server and at Local Repositories, deselect the on-board disk at **/media0** and select iSCSI disk **/media1_0** as shown in Figure 20.

Figure 20 Video Surveillance Management Console



License

Mac Address:

License Key: A0 F1 C5 DB 5C 6A 01 1F EA 3E 0E 91 23 ED 64 70 DF 4I

Current License Information
Max Servers: **32**
Max Clients: **500**
Mpeg-2 Capability: **yes**
Mpeg-4 Capability: **yes**
Camera Control Capability: **yes**
Expiration Date: **permanent**

Storage Configuration

Max Storage %: 98

PTZ Configuration

Camera Control Lockout: 5 Minutes

Media Out Ports

HTTP Port: 80
RTSP Port: 554
Proxy Port: 9090
RTP Port Range:

Local Repositories

Local Archive Repositories: □ /media0 ☑ /media1_0

Clipping and backup can also be directed to the iSCSI device.

VMSS Network Module Configuration

After formatting is complete, the configuration of the VMSS network module appears as follows.

The **target-ip** line with the volume name and the iSCSI Qualified Name (IQN) is entered automatically, only the **target-ip** address need be manually configured.

```
storages iSCSI media1
 target-ip 192.168.11.150
  target-ip 192.168.11.150 volumeName iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D7326
2B1E:array1 LUN 0
```

```
 end storages-iscsi
end
```

To verify the detailed status of the volume, the **show storages iscsi** command can be entered.

```
VMSS-SITE140# show storages iscsi status  detail
       Fou Log                                                           Portal
  Tag  nd  in   Device    Mounts    LUN  FS Types      iSCSI Portal      Reachab
le IO Target Name
====== === === ======== =========== ===  ======== ===================== =======
== == =============
media1 yes yes /dev/sdb /media1_0     0   ext3      192.168.11.150:3260,1    Yes
   rw iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D73262B1E:array1
```

Tip The status of ‘rw’read-write should be verified. If the status is ‘ro’, read-only, the volume cannot be written to and archives will fail.

Summary

In practically all branch office video surveillance deployments, an external iSCSI device is needed to provide sufficient disk space for storage of local video archives. The branch topology must be configured to provide network connectivity for fault and configuration management of the iSCSI server. The enterprise network management system must monitor the iSCSI server, router and VMSS network modules to insure the operational health of the surveillance system at the branch location.

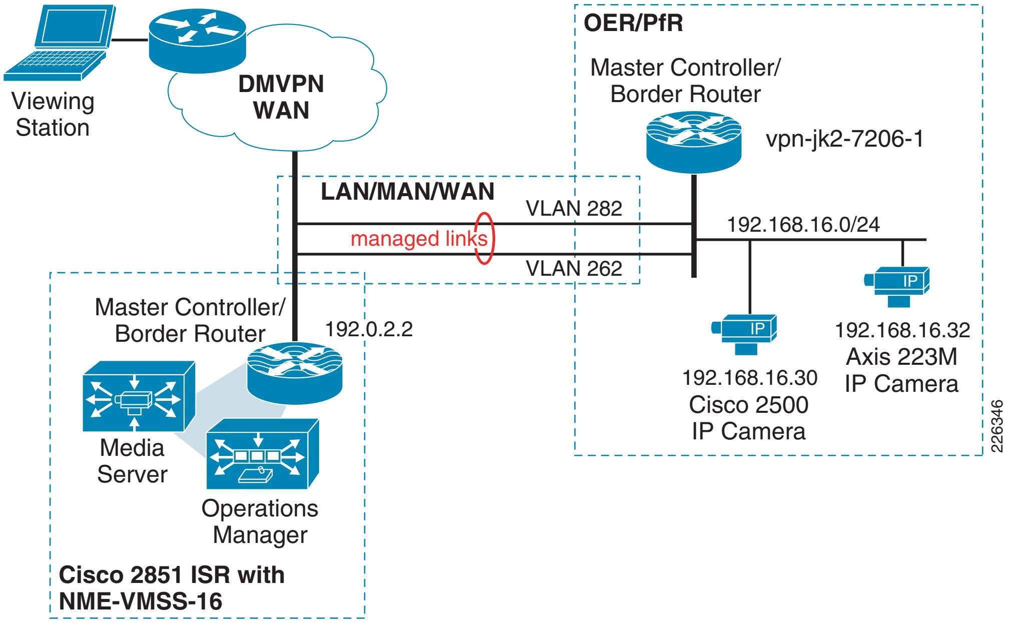
Performance Routing (PfR) Integration

This section shows that the video traffic flows from a video surveillance camera to the Media Server and then live or archived feed can be viewed through the Video Surveillance Operations Manager (VSOM) using a client viewing station. Viewing stations are workstations running Microsoft Internet Explorer (IE). Examples showing the impact of loss, latency, and jitter on the video feed are presented. Given an understanding of the requirements of the video surveillance traffic, a demonstration of how Performance Routing (PfR) is implemented on multiple WAN links to enhance the video quality. PfR intelligently selects the best WAN link, or a link that meets the configured criteria, from the available paths. Because video surveillance images often have a forensic use for identifying or criminally prosecuting subjects, optimal video quality is imperative for IP Video Surveillance deployments.

Topology

To illustrate how latency, loss, and jitter effect video feeds, we have set up a topology where the originating video feeds are not directly attached to the LAN of the Media Server recording the video. This allows test tools to introduce impairments in the network. The IP cameras are attached to a VLAN on a separate router from the branch location where the Video Management and Storage System (VMSS) network module resides. A WAN is simulated by injecting latency, loss, and jitter by a test appliance connected to two VLANs separating these locations. The branch router is a Cisco 2851 ISR with a NME-VMSS-16 network module. This topology is shown in Figure 21.

Figure 21 Performance Routing Test Topology



The PfR Master Controller and Border Router function are configured on the Cisco 2851 (IOS Release 12.4(15)T5) as well as the Cisco 7200 Series router at the campus location. The Cisco IP camera is Firmware Version is 1.1.1.

Video (MPEG-4) Characteristics

Before configuring PfR to select the best link, or a link that meets the minimum service level, we must first examine how the video in this example is encoded and transported between the camera and the Media Server. Most IP Video Surveillance cameras support Motion JPEG and MPEG-4. MPEG-4 usually refers to MPEG-4 part 2 encoding. Some cameras also support H.264, which is the nomenclature for MPEG-4 Part 10 or the Advanced Video Coding (AVC). The biggest difference between MPEG-4 part 2 and MPEG-4 Part 10 is the efficiency of the video compression.

MPEG-4 encoding is object-oriented compression, meaning it detects "objects" in the frame and sends out information when there is a change. A complete frame is sent to resynchronize periodically. This is called a key frame (slice) referred to as an I-frame. Predicted frames (P or B) build upon a reference slice. Usually, the key frame requires more than one IP packet for transport. In testing up to 30 IP packets have been observed to transport a single I-frame. Predicted frames may fit in a single IP packet but usually require more than one. MPEG-4 is typically encapsulated in UDP/RTP and is connectionless. The RTP header includes a packet sequence number so that the receiver can identify if packets are lost, but due to the connectionless nature of UDP, there is no retransmission of lost packets. When viewing the video feed with 1 percent or more loss, most people find the image noticeably degraded for standard definition images.

The Cisco 2500 Series IP camera uses UDP/RTP transport for video feeds to the Media Server. For IP cameras which MJPEG is supported, as is the case with the Axis 223M, the video feed between camera and Media Server is TCP-based. When viewing a live or archived video feed from a viewing station logged on VSOM, both MPEG-4 and MJPEG images are encapsulated in TCP/HTTP.

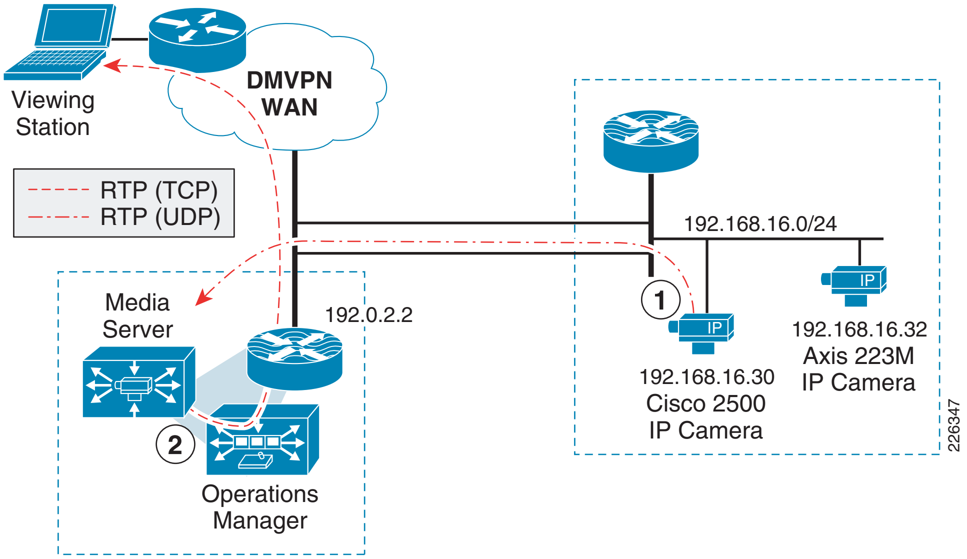
In this section PfR is used to optimize the UDP/RTP packets between camera and media server. In a later section, Wide Area Application Services (WAAS) is incorporated into the topology and both PfR and WAAS is used to optimize video feeds transported in TCP.

Media Server as a De-Jitter Buffer

In a Video Surveillance Manager (VSM) implementation, video from a surveillance camera is not viewed directly by a viewing station off the IP camera. Rather, the viewing station, a PC, connects to the web server of the Video Surveillance Operations Manager (VSOM). VSOM communicates with the Media Server and displays a video feed from the selected camera. If there is no active feed from the camera, the Media Server contacts the camera and initiates a live feed. The viewing station can display both live and archived feeds from one or more cameras defined to the Media Server.

Because camera feeds are not viewed directly from the camera, the Media Server acts as a de-jitter buffer for MPEG4-based video. This process is shown in Figure 22.

Figure 22 Video Path from Camera to Viewing Station



In general, packet loss presents more of an impairment to video quality than latency and jitter in this RTP/UDP deployment topology.

In VoIP deployments, latency impacts usability. As latency increases, the likelihood that two people would talk at the same time increases. This is referred to as the Walkie-talkie effect. Latency does not impact audio fidelity, it impacts usability. In VoIP, excessive jitter may be addressed by the de-jitter buffer in the IP telephone, but in some instances packets with excessive jitter are dropped if they arrive too late and must be dropped. Single packet loss for VoIP may not be noticed by the listener if packet loss concealment is implemented.

Video requirements differ from VoIP deployments in that surveillance applications have no two-way, real-time exchange of data. If the surveillance camera is a fixed camera, no Pan-Tilt-Zoom functions, the only two-way communication is the authentication step and RTSP step to initiate a camera feed. While latency in the network will slow down these packet flows, once the camera is initiating the RTP stream, no two-way communication is necessary. This packet flow between Media Server and IP Camera is described in more detail in the next section.

Loss for MPEG-4, however, cannot be recovered. There is no retransmission of lost packets. If the packet loss occurs in a 'key slice', and this slice required 30 IP packets for transmission, this single packet loss causes the 'key slice' to be incomplete. Packet loss degrades the MPEG-4 video quality.

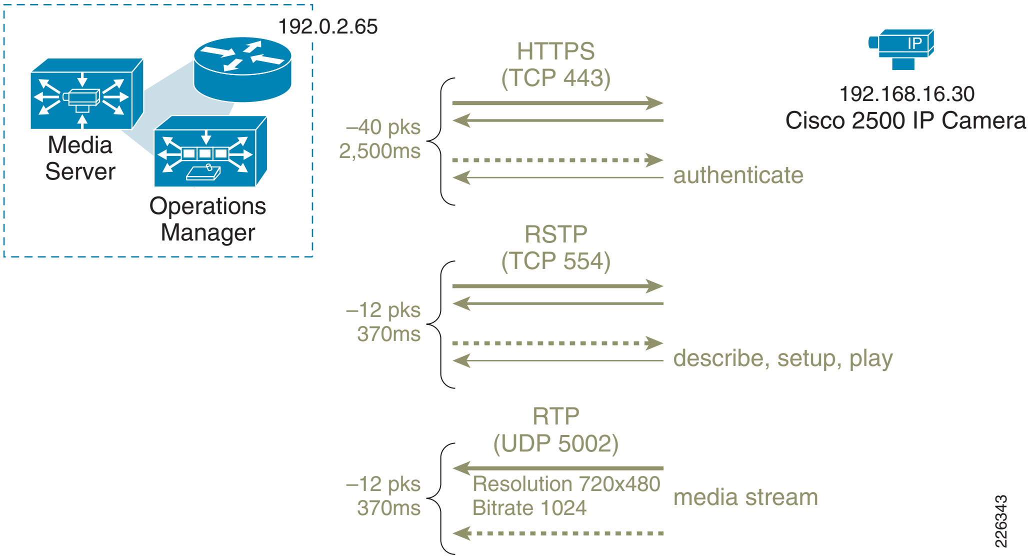
The network characteristics to provide good video quality is different and, in some cases, more stringent than for VoIP. In general, VoIP is more tolerant to packet loss than video, while video is more forgiving to latency and jitter than VoIP.

Packet Flow Between Camera and Media Server

To better the network requirements for IP Video Surveillance, it is helpful to understand the process flow between a Cisco 2500 Series IP camera configured for MPEG-4 and the Media Server. In the authentication phase, the Media Server contacts the Cisco IP Camera with Hypertext Transfer Protocol over Secure Socket Layer (HTTPS - TCP port 443). This process takes approximately 2.5 seconds with 40 IP packets between the camera and Media Server. Next, the Media Server contacts the camera over the Real Time Streaming Protocol (RTSP - TCP port 554) to issue instructions to describe, setup, and play the video media stream. This requires approximately 12 packets over the period of 370ms. The IP camera then, begins to unicast the media stream (video feed) as Real-Time Transport Protocol (RTP - UDP port varies) packets. The RTP data is to be carried on an even UDP port number and the corresponding Real-time Transport Control Protocol (RTCP) packets are to be carried on the next higher (odd) port number. RTCP is not implemented on the Cisco IP Camera at this time.

The video feed continues until the Media Server instructs the camera to stop the media stream again through RTSP commands. This exchange is shown in Figure 23.

Figure 23 Packet Flow Between Camera and Media Server



In this test, the camera has a resolution of 720x480 (D1) with a target bit-rate of 1024Kbps. The resulting RTP stream is observed at approximately 115 packets per second with an average of 1,054 bytes per packet.

Warning **The Cisco IP camera can be configured to set the DSCP value of the RTP stream. However, the HTTPS or RTSP stream is not configurable and, unless set by a router or switch, is DSCP best effort.**

Reference Tests—Illustrate Loss versus Latency

Before configuring PfR to demonstrate how this feature can select and use one WAN link over another, we must first understand what impairment has the biggest impact on video quality. Once the application requirements are understood, PfR can be configured to manage the WAN links to optimize the application performance.

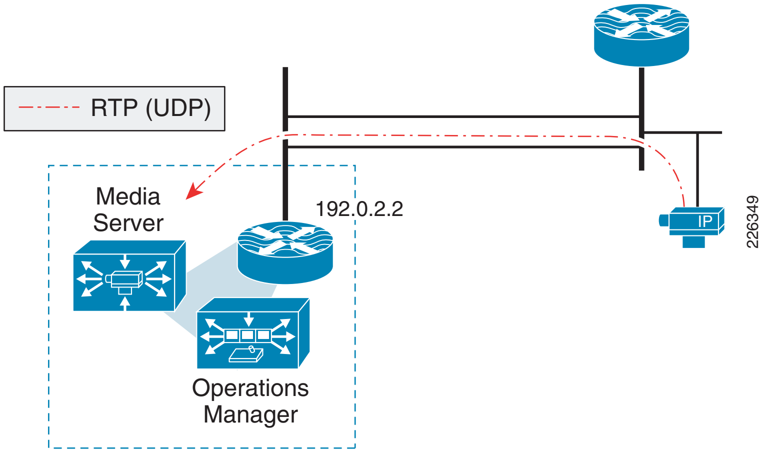
In the previous section, it was asserted that the quality of the video feed is degraded by packet loss more than latency. To illustrate this point, three tests were run and the video images are subjectively analyzed.

The Cisco IP Video Surveillance camera used in testing was configured with the following parameters:

```
Camera Name: CIVS-IPC-2500 ESELAB
Description: 001DE5EA7999
Camera Type: Cisco 2500 IP Camera
Server: VSMS_Site130
Host IP/Name: 192.168.16.30
Resolution: 720 x 480
Format: NTSC
Media Type: MPEG-4
UDP: On (UDP)
Bitrate: 1024
Quality: 50
```

Between the camera and Media Server there are two WAN links. Before PfR is enabled on the routers, the link that is used by the camera feed is subject to latency (jitter is influenced by the randomness of latency applied) and loss. The topology of the test is shown in Figure 24.

Figure 24 Reference Tests - Loss versus Latency



For each test, an archive is scheduled and retained for later viewing, with the WAN network simulator configured for the following criteria.

Typical Latency—Low Loss

- Drop on-in 1,000 (1/10th 1%)
- Delay 30 to 40ms

High Latency—No Loss

- Drop off (no configured packet loss)
- Delay 120 to 150ms

LAN Latency—High Loss

- Delay off (typical minimal LAN switching delay)
- Drop one-in 100 (1%)

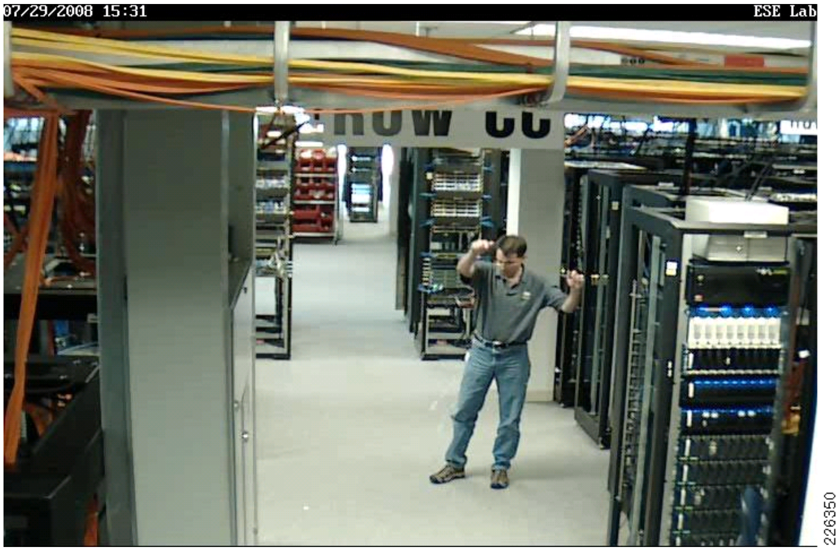
The results of the three tests are described in the following sections.

Typical Latency—Low Loss

In this first test, latency was measured by an IP SLA probe traversing the same WAN link as the camera feed. The probe reported an average latency of approximately 35 milliseconds with jitter at 3ms. The MOS score is 4.06. Latency was applied in both directions, with a result of a round trip time (RTT) of approximately 71ms on average. Latency values in this range are not uncommon, for example, between two locations in North America serviced by Internet T1 links.

A snapshot from the video archive is shown in Figure 25.

Figure 25 Snapshot of Typical Latency—Low Loss Archive



The motion in the view of the camera is generally smooth. The subject is dropping packing peanuts in a lab environment with racks of network equipment, allowing the fan exhaust to blow the peanuts across the floor. Several peanuts are on the floor and to the left of the right knee of the subject, you can see several peanuts falling.

There are some artifacts with quick motion, but they are not excessive. This is used as a baseline to determine the difference in quality for the remaining tests.

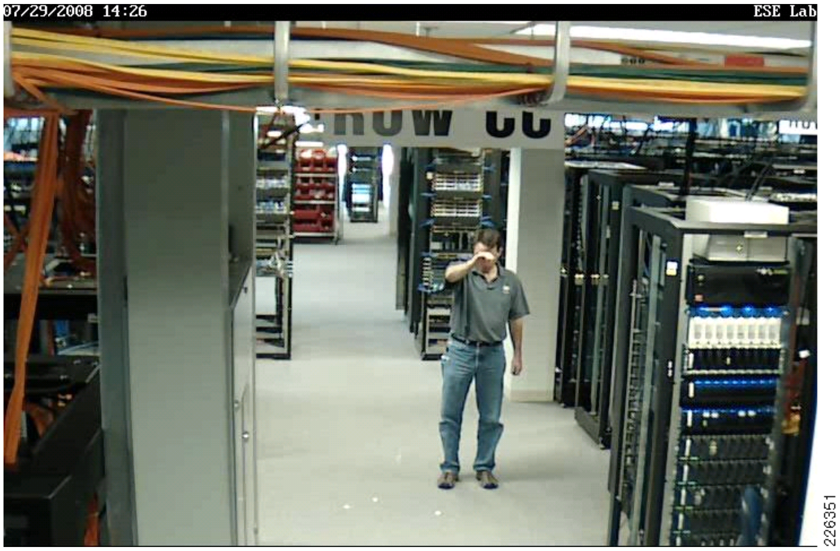
A copy of this archive can be viewed at http://tools.cisco.com/cmn/jsp/index.jsp?id=84464

High Latency—No Loss

In this test, latency and jitter were increased. The IP SLA measured latency averaged 274ms RTT with one-way latency in the 135ms to 139ms range. Jitter averaged between 9 to 10ms with a maximum value of 25ms. The MOS score reported as 3.88. This latency is typical of links with high serialization delay such as dialup Internet connections, or with high propagation delay such as intercontinental Frame-Relay communications.

A snapshot from the archive is shown in Figure 26.

Figure 26 Snapshot of High Latency - No Loss Archive



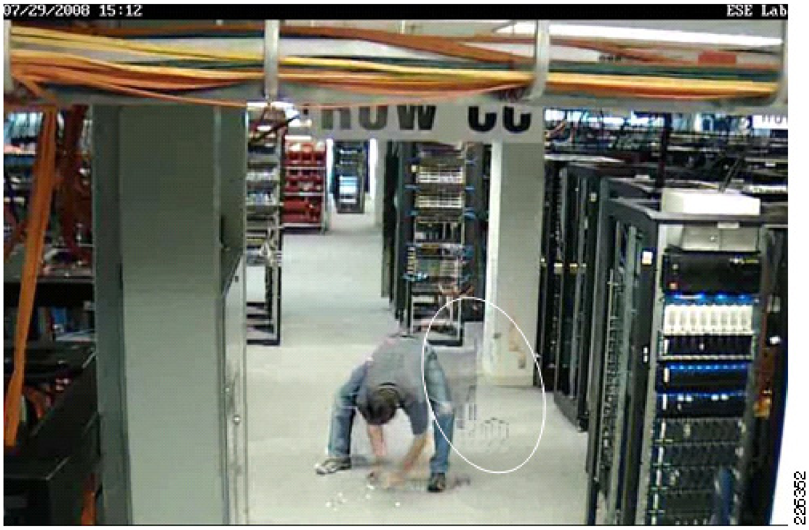
The image quality is very similar to the baseline test. Motion is smooth. There is the same degree of video artifacts as the baseline test; artifacts are apparent when quick motion changes a large number of pixels. However, latency in the 150ms range (one-way) does not produce substantially different video quality than the baseline test.

A copy of this archive can be viewed at http://tools.cisco.com/cmn/jsp/index.jsp?id=84463

LAN Latency—High Loss

In this test, the artificially introduced delay was eliminated, but packet loss is 1 dropped packet in 100 packets, or 1 percent. The average RTT is only 2ms, or LAN like latency performance, but because of the packet loss, the IP SLA MOS score is 3.76. The network characteristics are the opposite of the previous test, but the packet loss introduced its own set of challenges for video. A snapshot from the archive is shown in Figure 27 with a white circle indicating the area of particular interest.

Figure 27 Snapshot of LAN Latency - High Loss Archive



MPEG-4 has a high inter-frame dependency and artifacts become pronounced around 1 percent packet loss. In this archive, the artifacts are more pronounced than both the baseline and the previous test. They linger substantially longer. In many cases, the disruption of video quality is to such a degree that the subject is not identifiable.

The white circle overlay on the snapshot calls out an area of the image from which the subject has recently moved. His movement is from the right to left in the frame. What occurred in the video image is commonly called microblocking, tiling , mosaicking, or pixelating. These are terms used to describe a condition when the contents of a macroblock is missing or in error. Macroblocks are noticeable in an image as square-areas in the picture do not have complete information. The macroblock could be seen as a single color or a low-resolution block with noticeable edges.

Tip A macroblock represents a block of 16 by 16 pixels. The contents of the macroblock contains both luminance (brightness) and chroma (color) definitions.

From this example, it is apparent that packet loss greatly impacts the video quality of this surveillance image. To address this, PfR is configured to select the path with packet loss as the primary differentiator between multiple links.

A copy of this video archive can be viewed at http://tools.cisco.com/cmn/jsp/index.jsp?id=84462

Implement Performance Routing to Address Packet Loss

There are two existing design guides that provide information on implementing performance routing in an enterprise network. These documents are available at the following URLs:

- *Transport Diversity: Performance Routing (PfR) Design Guide*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Transport_diversity/Transport_Diversity_PfR.html

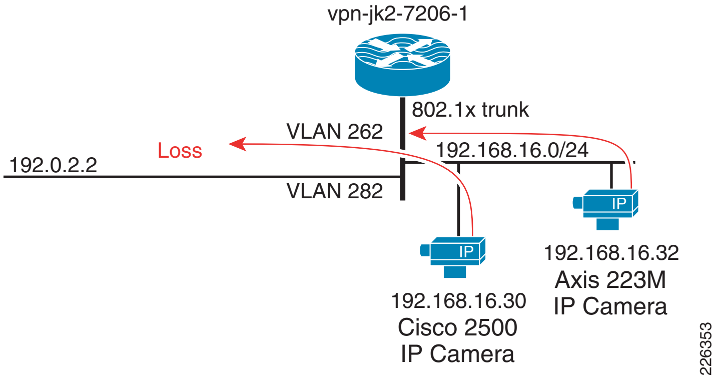
- *Performance Routing (PfR) Master Controller Redundancy Configuration*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Transport_diversity/PfR_Master_Controller_Redundancy.html

Topology

In the test topology, two links exist between the cameras and Media Server. These are FastEthernet links with a delay and loss generation tool configured to introduce 5 percent packet loss on the VLAN 262 (upper) link with a RTT of approximately 71ms. The second link, the lower link shown, has no loss but has the same 71ms round-trip delay. The MOS score of the link with the packet loss was 2.95 while the other link was 4.06. The topology is shown in Figure 28.

Figure 28 PfR Test Topology



Without PfR enabled, both links are in the IP routing table and Cisco Express Forwarding (CEF) load shares over the two links, based on source and destination IP address. In this example, both IP cameras are routed over the link with loss. This can be seen with the **show ip cef exact-route** command.

```
vpn-jk2-7206-1#show ip cef exact-route 192.168.16.30 192.0.2.2
192.168.16.30   -> 192.0.2.2       : FastEthernet0/1.262 (next hop 192.168.12.2)
vpn-jk2-7206-1#show ip cef exact-route 192.168.16.32 192.0.2.2
192.168.16.32   -> 192.0.2.2       : FastEthernet0/1.262 (next hop 192.168.12.2)
```

CEF does not take into consideration link characteristics. It uses a hash to determine which link is used for any one source and destination IP address pair. Based on the IP address of the source addresses, both cameras happen to use the same link. CEF can provide a degree of load sharing as the number of source/destination pairs increase, because statistically traffic will routed across both links. CEF can provide a degree of load sharing, but not load balancing. It has no mechanism to select an alternate path if the WAN performance is degraded due to latency or packet loss. At this point in the test, the OER master controller was administratively shutdown.

PfR Configuration

In this configuration, both master controller and the border router exist on the same router: the Cisco 7200 Series at the campus location. A similar configuration is implemented on the branch router. PfR has a requirement for at leas two external links (exit points) and one internal interface. These are shown configured under the border router section of the configuration.

Also a requirement of PfR, two equal cost routes, or parent routes, are included in the routing table. They are in the routing table from the two static routes defined in the configuration. In this example, they are default routes (0.0.0.0 / 0.0.0.0), but any equal cost route to the destination subnet is sufficient.

The destination network is explicitly identified by a prefix-list definition, as referenced in the oer-map named **LOSS**, which is invoked by the **policy-rules** command under the master controller definition. Learn mode is configured, but these statements apply to traffic observed in the NetFlow cache, traffic that is also on the network but not explicitly identified by the **oer-map** command.

The relevant configuration on the Cisco 7200 series router for PfR is shown below:

```
!
hostname vpn-jk2-7206-1
!
key chain PURPLE
 key 10
   key-string 7 xxxxxx
!
oer master
 policy-rules LOSS
 logging
 !
 border 192.168.16.1 key-chain PURPLE
  interface FastEthernet0/1.282 external
  interface FastEthernet0/1.262 external
  interface FastEthernet0/1.216 internal
 !
 learn
  throughput
  delay
  periodic-interval 0
  monitor-period 1
  expire after time 30
  aggregation-type prefix-length 27
 no max range receive
 mode route control
 mode select-exit best
!
!
oer border
 local FastEthernet0/1.216
 master 192.168.16.1 key-chain PURPLE
!
!
ip route 0.0.0.0 0.0.0.0 192.168.13.2 name OER_Parent
ip route 0.0.0.0 0.0.0.0 192.168.12.2 name OER_Parent
!
ip prefix-list SITE_130 seq 5 permit 192.0.2.0/27
!
oer-map LOSS 10
 match traffic-class prefix-list SITE_130
 set mode select-exit best
 set mode route control
 set mode monitor fast
 set resolve loss priority 1 variance 10
 set loss relative 100
 set active-probe jitter 192.0.2.1 target-port 32000 codec g729a
 set probe frequency 10
!
end
```

The **oer-map** command specifies that the ‘best’ exit is used, and the **monitor mode fast** command is configured to provide for continuous probing of all exits at 10 seconds frequency. An explicitly configured active jitter probe is enabled using the G729a codec. The IP address target of the probe is the branch router VMSS network module logical interface IP address. On the branch router, the **ip sla responder** command must be configured so that the probes are replied to by the branch router.

Enabling PfR

In this test, the video feeds are active and being archived. PfR is enabled by entering configuration mode on the Cisco 7206 router at the campus location and initiating operation by issuing the **no shutdown** command to the master controller. This function is shown as follows:

```
vpn-jk2-7206-1(config-oer-mc)#no shut
vpn-jk2-7206-1(config-oer-mc)#
Aug 12 11:04:48.110 edt: %OER_MC-5-NOTICE: System enabled
Aug 12 11:04:51.870 edt: %OER_MC-5-NOTICE: BR 192.168.16.1 UP
...
Aug 12 11:04:52.062 edt: %OER_MC-5-NOTICE: Uncontrol Prefix 192.0.2.0/27, Traffi
c Class in Fast Mode
Aug 12 11:05:18.306 edt: %OER_MC-5-NOTICE: Route changed Prefix 192.0.2.0/27, BR
 192.168.16.1, i/f Fa0/1.282, Reason None, OOP Reason Timer Expired
```

From the timestamps in the syslog messages, the elapsed time from the startup of operations to a point where PfR is managing the explicitly configured prefix is approximately 30 seconds. The exit chosen is the path with the least amount of packet loss. To view the current state of the network prefix, issue the **show oer master prefix** command. Sample output is shown below:

```
vpn-jk2-7206-1#show oer master prefix
OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

Prefix                  State     Time Curr BR         CurrI/F         Protocol
                      PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos
                      ActSDly  ActLDly   ActSUn   ActLUn      EBw      IBw
                      ActSJit  ActPMOS  ActSLos  ActLLos
--------------------------------------------------------------------------------
192.0.2.0/27            HOLDDOWN     @106 192.168.16.1    Fa0/1.282       STATIC

                               U        U        0        0        0        0
                              72       72        0        0      723        1
                               3        0        0        0
```

In the output above, there are several items of interest. First, the prefix is in HOLDDOWN state. This is because the route for the prefix has recently changed. A prefix is placed in HOLDDOWN state to avoid link flapping and resulting destabilization of the network-wide routing tables. The exit bandwidth (EBw) and the input bandwidth (IBw) are shown. There is a great disparity between the two, although not unexpected. The traffic flow is from cameras to Media Server and very little traffic is destined for these cameras in this topology. Only control plane traffic would be sent to the cameras. The current exit interface (Fa0/1.282) is shown and this can also be verified by viewing the routing table. The short-term active delay and jitter is 72ms and 3ms, respectively.

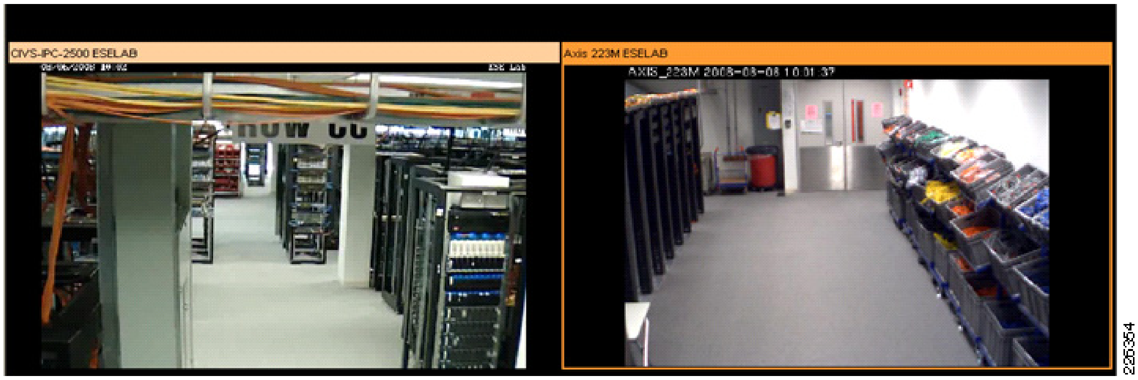
Tip The **show oer master prefix 192.0.2.0/27 detail** command can be used to provide more verbose information on this prefix.

Effect on Video Quality

Previously, it was discussed how 1-percent packet loss can lead to noticeable degradation of the video image. In the test topology, the link that is the path of the video feeds when CEF is loadsharing over the two WAN link, has 5 percent loss. In the video archive, with this amount of loss, the faces of the people in the image are not recognizable, motion is very choppy, and artifacts clutter the video image and linger for long periods of time. The video does not clear up until a clean key slice is received to refresh the image. This amount of packet loss dramatically degrades the video quality.

When PfR is enabled and begins sending the video traffic over the link with no loss, immediately the video quality improves to what is normal for the camera. The snapshot in Figure 29 is the video images from both cameras after PfR has routed the traffic over the best link.

Figure 29 Video Images with Performance Routing Active



In a production network with two links between camera and Media Server, 5 percent packet loss is obviously an excessive amount of loss that should be identified by the enterprise network management system (NMS) function. The link with this excessive amount of loss must be taken out-of-service and corrected before being brought back online; however, PfR can circumvent the problem and take almost immediate action to preserve the quality of the video. PfR therefore is an important tool to address problems that may be a temporary disruption or need a short-term solution until a log-term fix can be implemented.

Summary

Packet loss dramatically degrades video quality. Constant or sustained packet loss at levels of 1 percent or more will decrease the usefulness of video images. Because of the forensic nature of IPVS, minimizing packet loss is critical to this video application. Loss can be attributed to hardware or soft failures that may not be identified by Layer-2 keepalives, static routes, or a Layer-3 Routing Protocol. When multiple links exist between the source of the video image and the storage system, PfR is an effective tool to select the best among several links between the video endpoints.

Wide Area Application Services (WAAS) Integration

Because of the benefits customers have realized by implementing the Cisco Wide Area Application Services (WAAS) between branch offices and central locations, the question of how WAAS might also provide bandwidth savings and TCP optimization for IP Video Surveillance traffic is frequently asked. The objective of this section is to understand the impact of WAAS on IP Video Surveillance traffic. Two types of video transport are discussed in this section:

- Camera Feeds to Media Server (TCP transport of Motion JPG)
- Video Surveillance Operations Manager (VSOM) to client viewing station (HTTP)

In the "Wide Area Application Services (WAAS) for iSCSI" section on page 6-74, a discussion on WAN transport of iSCSI video archives is also addressed.

The topology for these scenarios is a branch router, a Cisco ISR 3845, with a VMSS network module (NME-VMSS-HP-32), and a WAAS network module (NME-WAE-522-K9). The campus location hosts a core Cisco Wide Area Application Engines (WAEs) and WAAS Central Manager. This topology builds upon the PfR integration topology where multiple WAN links exist between branch and campus location. The WAAS optimization of IPVS traffic across multiple WAN links managed by PfR was verified in this test phase. Included in this section are various Cisco IOS show commands and reports and exported data from the WAAS Central Manager, as well as verification from NetFlow exports from the routers in the tested topology.

Feature Overview

WAAS implements both data compression and optimization of the TCP session across the WAN between the branch (or edge) WAE and the core WAE. Two compression techniques are implemented: Persistent Lempel-Ziv (LZ) compression and Data Redundancy Elimination (DRE). LZ compression can achieve compression ratios in the order of 2:1, 5:1 or 100:1 if the data contains common strings or phrases. This form of compression is helpful for data that has not been previously seen or suppressed by DRE. DRE operates by maintaining a database of data that has been seen previously traversing the network. One advantage of DRE is that it is application-independent, meaning the redundant data may be part of a HTTP session or iSCSI archive and if commonalities exist, DRE can eliminate the redundant traffic. DRE can eliminate up to 99 percent of redundant network traffic and provide up to 100:1 compression.

However, both Motion JPEG and MPEG4 / H.264 camera feeds are compressed by the encoding function of the IP camera. Given this fact, the prospects of dramatic compression ratios by either LZ or DRE compression is unlikely. The data in this section supports that assumption.

WAAS uses the transport flow optimization (TFO) features to optimize TCP traffic. The specific techniques are as follows:

- Windows scaling (RFC 1323)
- TCP Initial Window Size Maximization RFC 3390
- Increased Buffering
- Selective Acknowledgement (SACK) (RFC 2018)

Note that a WAN transport with sufficient bandwidth to transport the video surveillance feeds are likely based on some form of Metro Ethernet service or DS3. DS3 bandwidth is capable of speeds up to 45 Mbps and Metro Ethernet may range in one to 10Mbps increments, using a 10/100/1000 Mbps interface handoff. Metro Ethernet services are usually policed by class or in aggregate by the service provider according to the contracted service. In the lab testing environment, between 10 to 20Mbps of WAN bandwidth was needed to transport the camera feeds for 1 to 4 cameras in the deployment. Given a viewing station observing 4 feeds simultaneously, with each feed at a target bit rate of 1Mbps, would therefore require approximately 4Mbps per viewing station. With these data rates as an example, it is obvious that viewing or archiving the video surveillance data across the WAN requires more bandwidth than a single T1 to the branch location.

Windows scaling and the enhanced buffering algorithm increase link utilization and take advantage of the available bandwidth. While these techniques may be optimal in a T1 WAN environment, the sheer amount of WAN bandwidth required for this deployment may render the advantages of these techniques less effective. Selective Acknowledgement provides efficient packet loss recovery and retransmission. If the WAN also transports UDP/RTP-based video, such as is the case with Telepresence and H.264/MPEG-4-based IP Video Surveillance, the loss needs to be closely monitored and addressed to preserve the video quality of these connectionless video feeds. Ideally, the WAN will exhibit very low loss and minimalize the need for selective acknowledgement.

Key Concepts

Some basic concepts must be understood to better understand the nature of the traffic and applications tested in this section. WAAS does not optimize traffic that is non-TCP (i.e., UDP or ICMP) traffic. Because H.264/MPEG-4 is typically RTP/UDP encapsulated, there is no optimization if this traffic is traversing the WAAS optimized WAN. Currently, all traffic between client viewing station and Media Server is TCP-based. Both MPEG-4 and Motion JPEG camera feeds, live, or archived are encapsulated in TCP. Motion JPEG camera feeds are typically TCP encapsulated. The Video Surveillance Media Server (VSMS) version tested is 6.0.0 and the Video Surveillance Operations Manager (VSOM) is 4.0.0. This version supports a Motion JPEG feed from the Axis 223M camera, TCP-based, and this camera was installed in the campus location to provide a TCP-based feed across the WAN. Currently, the Cisco Video Surveillance IP Camera (CIVS-IPC-2500) is not supported for MJPEG from VSMS 4.0.

Warning **Future releases of the client viewing station code are slated to incorporate RTSP support that may implement MPEG-4 streams between the media server and viewing station to UDP.**

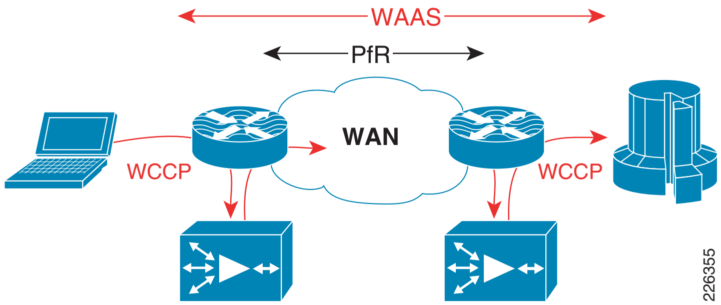
The WAAS tested version is 4.1.1c for the branch WAE, core WAE, and WAAS Central Manager. The video component in this version relates to Windows Media live video broadcasts that use RTSP over TCP. The video accelerator implemented by this feature eliminates duplicate video streams on the WAN and creates multiple streams to serve multiple clients on the LAN. This video acceleration is not applicable to IP Video Surveillance.

Traffic Optimization Overview

In the test topology, WAAS is added to the existing topology which is also performance Routing (PfR)-enabled. This overview and illustration is helpful to better understand how WAAS and PfR co-exist over the WAN. PfR manages two or more WAN links between the branch and campus router. PfR selects a path which meets the criteria, or the best path of so configured. In this video surveillance testing, sample configurations are shown which select the best path based on loss, or a combination of loss and delay. PfR is highly configurable and very granular; down to specific applications, if desired.

AS shown in Figure 30, PfR manages the WAN links between two routers, while WAAS intercepts traffic on the LAN interface of each router, routing the optimized traffic across the WAN interface in the IP routing table. PfR injects routes into the IP routing table or by policy-based routing (PBR).

Figure 30 Traffic Optimization Overview

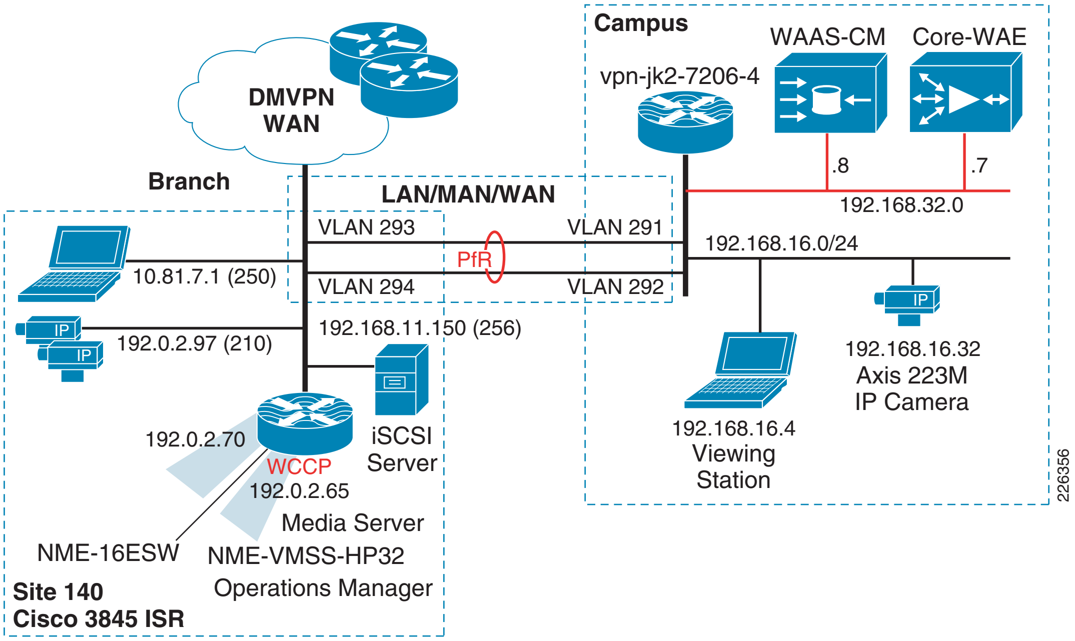


In these tests, traffic is intercepted with Web Cache Communication Protocol version 2 (WCCP v2) and redirected to the WAE. WCCP v2 supports any IP protocol (including any TCP or UDP). Intercepted TCP traffic is optionally a candidate for optimization. The WAE adds information to the TCP header to flag the next WAE that this traffic is being optimized. In the test lab, NetFlow is used to analyze the extent of WAN bandwidth savings. From the analysis of that data, it is noted that the WAAS sets the Explicit Congestion Notification (ECN) flag in the ToS byte. Because NetFlow v5 reports flows based on source/destination IP address, port, protocol, and ToS byte, a flow with the ECN bits set and one without is reported, even though they are actually part of the same flow if the ECN bits are ignored.

Topology

The tested topology is shown in Figure 31 discussed below.

Figure 31 WAAS Integration Topology



Some highlights of the topology are as follows:

- The branch Cisco ISR 3845 houses both NME-WAE-522 and NME-VMSS-HP32
- A branch VLAN for MPEG-4 and Motion JPEG cameras

- The campus 7200 Series router has a VLANs for WAAS-CM and core WAE appliance
- A campus VLAN for viewing station and a Motion JPEG (Axis 223M) camera.
- The WAN is dual FastEthernet links with two delay generation devices to introduce loss, latency, and jitter

PfR is implemented similarly on both the campus and branch router. WCCP is configured on the logical interface of the NME-VMSS-HP32 and on the VLAN of the viewing station/IP camera at the campus. Note that there is a Motion JPEG (Axis 223M) configured camera at the campus and transporting the video to the branch. Typically, a video surveillance deployment would not transport a video feed from the campus to a branch location for management and storage. It is not a recommended configuration, but it was inserted into the topology to demonstrate that WAAS could intercept TCP-based camera feeds across a WAN environment. Several customer deployments have been planned that require a single remote IP camera at an isolated location with the Media Server role at a larger branch deployment or campus location. This camera is included in the topology as a demonstration of that topology.

Role of WAAS Central Manager

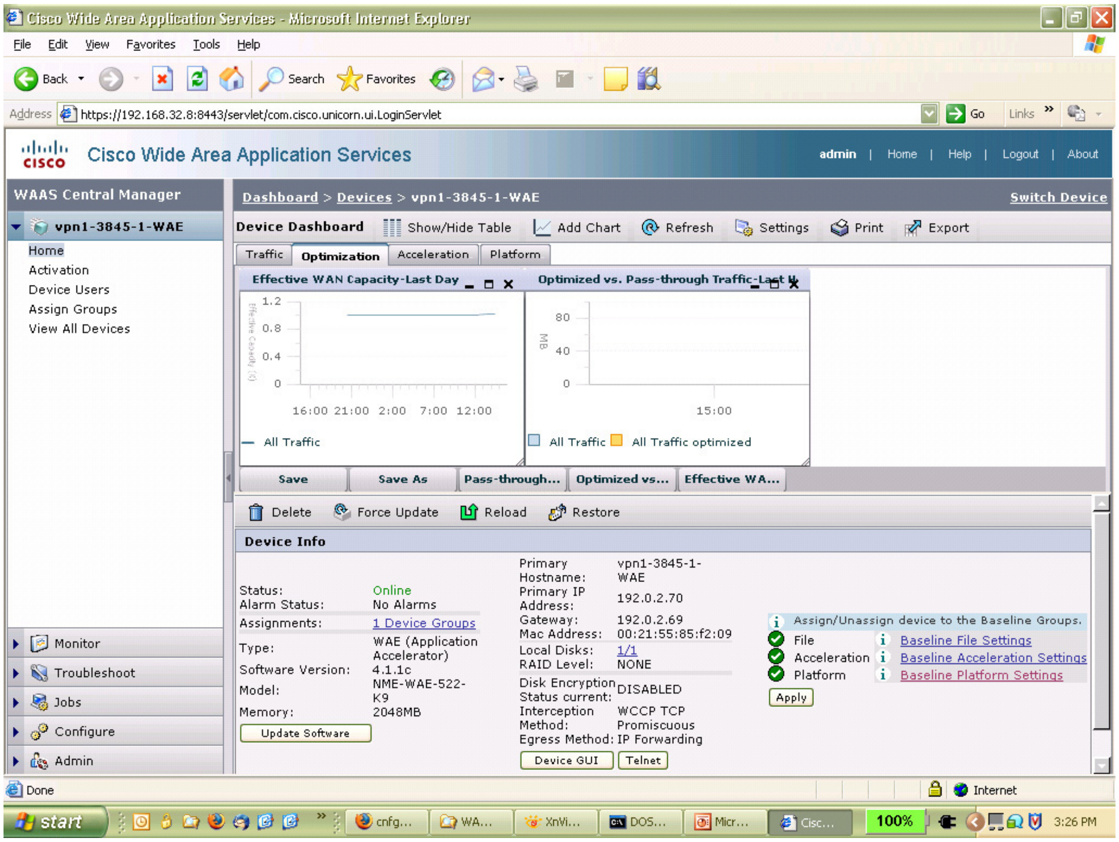
The role of the WAAS Central Manager (CM) is to provide the network administrator with a graphical user interface for fault, configuration, performance of WAE(s). For detailed information on the WAAS CM , refer to the appropriate *Cisco Wide Area Application Services Configuration Guide* on www.cisco.com.

To illustrate the role of the WAAS CM, a screen snapshot is included showing the view of a remote WAE. To connect to the WAAS CM, the testbed campus PC accesses the WAAS CM by connecting to the IP address of the CM at port 8443 using the HTTP/SSL. For example:

```
https://192.168.32.8:8443/
```

Once validated, the branch WAE device can be selected. The screen snapshot in Figure 32 provides an idea of the GUI interface available to the network manager.

Figure 32 WAAS Central Manager Device Dashboard



Device Info

Status: Online
Alarm Status: No Alarms
Assignments: 1 Device Groups
Type: WAE (Application Accelerator)
Software Version: 4.1.1c
Model: NME-WAE-522-K9
Memory: 2048MB

Primary Hostname: vpn1-3845-1-WAE
Primary IP Address: 192.0.2.70
Gateway: 192.0.2.69
Mac Address: 00:21:55:85:f2:09
Local Disks: 1/1
RAID Level: NONE
Disk Encryption Status current: DISABLED
Interception Method: WCCP TCP Promiscuous
Egress Method: IP Forwarding

Assign/Unassign device to the Baseline Groups.
✓ File — Baseline File Settings
✓ Acceleration — Baseline Acceleration Settings
✓ Platform — Baseline Platform Settings

From the device dashboard screen shown above, the reports for the WAE can be viewed, the device can be managed by Telnet or a WEB browser, and other pertinent information like software version, alarms, IP address, and the MAC address can be displayed.

For the branch and core WAE to identify themselves to the CM, the configuration on the WAE must include the address of the CM; in the following example, 192.168.32.8.

```
vpn1-3845-1-WAE#sh run
! WAAS version 4.1.1c
! (build b16 Nov  5 2008)
!
device mode application-accelerator
!
hostname vpn1-3845-1-WAE
!
… [lines removed]
!
central-manager address 192.168.32.8
cms enable
!
! End of WAAS configuration
```

Once that is configured and the WAE contacts the CM, the remote WAE devices can be managed from the CM GUI interface.

Test Goals

The goal of this testing was to demonstrate PfR routing traffic over the WAN link that exhibits the best path between branch and campus. Once PfR is operational in the WAN, WAAS is implemented to optimize the TCP/HTTP traffic to and from the Video Management and Storage System (VMSS) logical interface in the branch Cisco 3845 ISR.

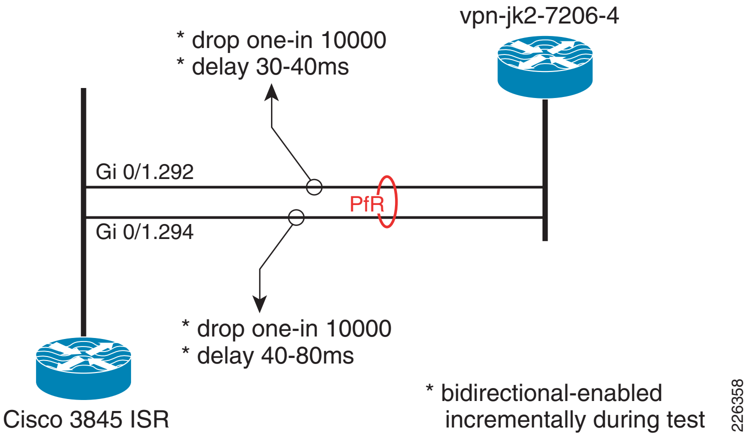
The Cisco IOS Release tested at the branch is **c3845-adventerprisek9-mz.124-15.T5** using the NME-VMSS-HP-32 (version 4.0/6.0) network module and the NME-WAE-522-K9 network module using WAAS version 4.1.1.c. To verify the bandwidth savings, both NetFlow and the WAAS CM Report Effective WAN Capacity (bandwidth savings) data are used.

The approach is therefore to first describe the WAN characteristics, examine the PfR configuration, and then enable WAAS on the topology. The PfR configuration in this section builds upon the configuration in the previous section. In this testing, PfR is now managing both on packet loss and delay. Loss is the first priority and delay is the second priority. In testing, path changes are triggered by both loss and delay.

WAN Characteristics

On the two WAN links, a latency and packet loss tool is used to introduce loss, latency, and jitter. The values shown are applied in each direction. Both links have packet loss of one packet in every 10,000 packets, or 1/100th of 1 percent loss. Delay is in the range of 30 to 40 milliseconds on one link and 40 to 80 milliseconds on the other link. The variation in delay introduces jitter into the traffic. These values are shown in Figure 33.

Figure 33 WAN Characteristics - Latency, Jitter and Loss



At the beginning of the test, neither WAN link had any appreciable loss or delay, the tool is enabled during the test to simulate WAN links that are changing characteristics over a period of time.

PfR Configuration

The PfR configuration deployed in this testing uses the Fast Reroute feature. The Fast Reroute feature probes all exits continuously. This allows PfR to have the current state of all managed links reflected in its database. An explicitly configured active jitter probe (UDP jitter) is configured to characterize the delay, loss, and jitter of all exits. This probe also provides voice statistics such as Mean Opinion Score

(MOS) although MOS is not, in this testing, used to make path selection determinations. PfR is selecting the best path, rather than a path that simply meets the criteria. Loss is the first priority, then delay as the second priority. The probe frequency is every 10 seconds.

The **oer-map** command that implements this configuration is shown as follows:

```
oer-map LOSS 10
  sequence no. 8444249301975040, …
  match ip prefix-lists: CAMPUS
  backoff 300 3000 300
  delay threshold 80
  holddown 300
  periodic 0
 *probe frequency 10
 *mode route control
 *mode monitor fast
 *mode select-exit best
 *loss relative 100
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
 *resolve loss priority 1 variance 10
 *resolve delay priority 2 variance 10
 *resolve utilization priority 12 variance 20

  Forced Assigned Target List:
   active-probe jitter 192.168.16.1 target-port 32014 codec g729a

* Overrides Default Policy Setting
```

This **oer-map** command is referenced in the configuration sample by the policy-rules statement shown later in this document.

Path Selection Based on Loss and Delay

PfR can select the best exit based on the loss and delay criteria. When PfR selects a new route, the change can be seen in the logging buffer of the master controller. During testing, this output was captured and is included here for review. Note that the route is changed for reason of delay in the first instance and for reason of packet loss in the second instance.

```
Dec 19 10:14:19.855 est: %OER_MC-5-NOTICE: Route changed Prefix 192.168.16.0/20,
 BR 192.168.0.1, i/f Gi0/1.294, Reason Delay, OOP Reason None

Dec 19 10:19:56.862 est: %OER_MC-5-NOTICE: Route changed Prefix 192.168.16.0/20,
 BR 192.168.0.1, i/f Gi0/1.293, Reason Loss, OOP Reason Loss
```

Given the low amount of loss in the test environment (1/100th of 1 percent) and that delay is incurred for all traffic, it is not unexpected to occasionally observe route changes alternate between loss and delay. In the Performance Routing (PfR) Integration chapter it was shown that PfR can manage links based on loss, and there was a high amount of loss on one link verses the other. In this test, loss is very minimal and the same on both links during the test, while the links have different delay characteristics.

Branch Router Configuration Details

Relevant portions of the branch router configuration is shown below with imbedded annotations:

```
hostname vpn1-3845-1
!
```

WCCP Version 2 is enabled by default and WCCP services 61 and 62 (TCP promiscuous mode)

```
ip wccp 61
ip wccp 62
```

Cisco Express Forwarding (CEF) is required for PfR to function.

```
ip cef
!
oer master
 policy-rules LOSS
 logging
 !
```

At least one internal interface and two or more external interfaces are required. The In3/0 interface is the NME-VMSS-HP32 logical interface.

```
 border 192.168.0.1 key-chain PURPLE
  interface Integrated-Service-Engine3/0 internal
  interface GigabitEthernet0/1.293 external
  interface GigabitEthernet0/1.294 external
  interface GigabitEthernet0/1.210 internal
  interface GigabitEthernet0/1.250 internal
 !
```

For traffic not selected by the oer-map, learn mode is enabled to allow PfR to control routes for traffic exiting from VLANS 210 and 250 identified as internal interfaces above.

```
 learn
  throughput
  delay
  periodic-interval 0
  monitor-period 1
  expire after time 30
  aggregation-type prefix-length 29
 no max range receive
 delay threshold 80
 mode route control
 mode select-exit best
!
```

The border router and master controller are both configured on this branch router, the key-chain of PURPLE is not shown, but is a requirement of PfR.

```
oer border
 local Loopback0
 master 192.168.0.1 key-chain PURPLE
!
```

The WAN interfaces are VLAN 293 and 294, these VLANs attach to the delay and loss appliance.

```
interface GigabitEthernet0/1.293
 description To vpn-jk2-7206-1 for PfR
 encapsulation dot1Q 293
 ip address 192.168.15.6 255.255.255.252
!
interface GigabitEthernet0/1.294
 description To vpn-jk2-7206-1 for PfR
 encapsulation dot1Q 294
 ip address 192.168.15.2 255.255.255.252
!
```

```
!
interface Integrated-Service-Engine2/0
 description NME-WAE-522-K9
 ...
  ip wccp redirect exclude in
!
```

This interface is an internal interface for PfR and is configured for WCCP redirection; therefore, traffic entering and leaving this interface are candidates for WAAS optimization.

```
interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip address 192.0.2.64 255.255.255.254
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ...
```

PfR requires parent routes in the routing table. These routes identify the campus subnet of the viewing station and IP camera. The corresponding prefix-list selects traffic for the oer-map.

```
!
ip route 192.168.16.0 255.255.240.0 192.168.15.1 name OER_Parent
ip route 192.168.16.0 255.255.240.0 192.168.15.5 name OER_Parent

ip prefix-list CAMPUS seq 5 permit 192.168.16.0/20
!
```

The oer-map shown was also shown previously in this section.

```
oer-map LOSS 10
 match traffic-class prefix-list CAMPUS
 set mode select-exit best
 set mode route control
 set mode monitor fast
 set resolve loss priority 1 variance 10
 set resolve delay priority 2 variance 10
 set loss relative 100
 set active-probe jitter 192.168.16.1 target-port 32014 codec g729a
 set probe frequency 10
!
end
```

Note The target of the active-probe defined above is the campus router with an IP address of 192.168.16.1. This router is also contains a similar PfR configuration. The UDP jitter probe requires the **ip sla responder** command in the configuration.

PfR Verification

To verify PfR is managing the path to the campus network prefix where the viewing station and IP camera resides, the output of the **show oer master prefix detail** command is shown.

```
vpn1-3845-1#show oer masert prefix detail
Prefix: 192.168.16.0/20
   State: INPOLICY    Time Remaining: @0
   Policy: 10

   Most recent data per exit
   Border          Interface         PasSDly  PasLDly  ActSDly  ActLDly
  *192.168.0.1     Gi0/1.294               0        0       75       75
   192.168.0.1     Gi0/1.293               0        0      128      128
```

```
 Most recent voice data per exit
 Border          Interface         ActSJit  ActPMOS  ActSLos  ActLLos
*192.168.0.1     Gi0/1.294               4        0        0        0
 192.168.0.1     Gi0/1.293              11        0        0        0

 Latest Active Stats on Current Exit:
 Type     Target          TPort Attem Comps    DSum     Min     Max     Dly
 jitter   192.168.16.1    32014     1   100    7510       1     106      75
 jitter   192.168.16.1    32014     1   100    7490       1     106      74
 jitter   192.168.16.1    32014     1   100    7458       1     106      74
 jitter   192.168.16.1    32014     1   100    7564       1     106      75
 jitter   192.168.16.1    32014     1   100    7527       1     106      75


 Latest Active Voice Stats on Current Exit:
 Type     Target          TPort     Codec Attem Comps  JitSum      MOS
 jitter   192.168.16.1    32014     g729a     1   100     413     4.06
 jitter   192.168.16.1    32014     g729a     1   100     443     4.06
 jitter   192.168.16.1    32014     g729a     1   100     451     4.06
 jitter   192.168.16.1    32014     g729a     1   100     425     4.06
 jitter   192.168.16.1    32014     g729a     1   100     392     4.06
```

…

In the above output, under *Most recent data per exit,* the active short and long-term delay values are 75 and 128 milliseconds. This is consistent with the WAN characteristics described previously. Also, the active short-term jitter is 4 and 11 milliseconds, which is a result of the range of latency values introduced by the test tool on each link.

WAAS Implementation

WAAS is also tested and documented in the V3PN large scale IPSec aggregation testbed and included in the following document:

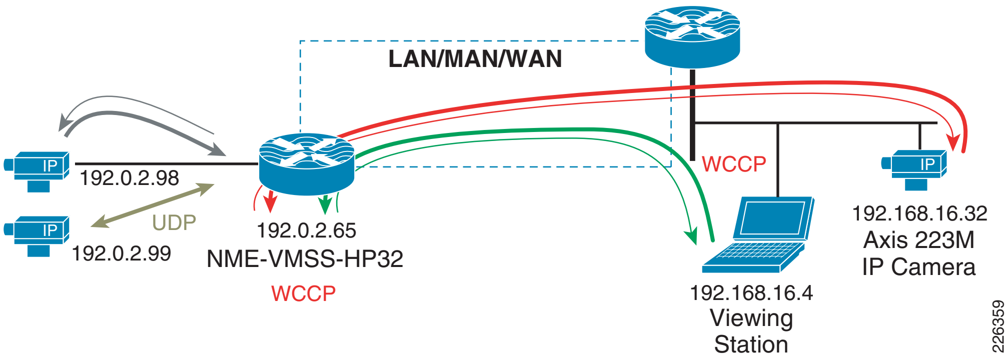
- *Transport Diversity: Performance Routing (PfR) Design Guide*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Transport_diversity/Transport_Diversity_PfR.html.html

The traffic profile used in the PfR and WAAS testing consisted of VoIP and data. The testing referenced here, WCCP enabled on the VMSS logical interface and therefore the target traffic for optimization is the HTTP requests the Client Viewing Station (Internet Explorer) makes to the VSOM web server. The nature of this traffic is video feeds displayed on the PC as well as the underlying web interface. Because in this phase of testing the Axis 223M camera is also located on the campus subnet, the TCP session for the Motion JPEG is also traversing the WAN to the Media Server IP address under the VMSS logical interface. This traffic is therefore also a candidate for optimization.

Figure 34 illustrates these flows to and from the VMSS logical interface.

Figure 34 Traffic Flows Optimized by WAAS



The flow from the IP camera to the Media Server is Motion JPEG (MJPEG) is at 5 video frames per second. The flows between VSOM and the Viewing Station are MJPEG/MPEG-4 (three cameras) along with the the HTTP control traffic. To verify these flows are candidates for optimization, the accelerated flows can be displayed on the branch WAE network module as shown in the following example:

```
vpn1-3845-1-WAE#show statistics connection  all

D:DRE,L:LZ,T:TCP Optimization,
C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,V:VIDEO

ConnID  Source IP:Port        Dest IP:Port          PeerID             Accel
20334   192.0.2.65:36908      192.168.16.32:80      0:14:5e:85:54:7b   THDL
20467   192.168.16.4:65488    192.0.2.65:80         0:14:5e:85:54:7b   THDL
20468   192.168.16.4:65485    192.0.2.65:80         0:14:5e:85:54:7b   THDL
20469   192.168.16.4:65482    192.0.2.65:80         0:14:5e:85:54:7b   THDL
20489   192.168.16.4:65508    192.0.2.65:80         0:14:5e:85:54:7b   THDL

Local IP:Port       Remote IP:Port      Peer ID             ConnType
192.0.2.98:80       192.0.2.65:41233    N/A                 PT No Peer
192.0.2.65:41233    192.0.2.98:80       N/A                 PT No Peer
```

There are a total of five TCP/HTTP flows being optimized by TFO and targeted for DRE and LZ compression. This is signified by the THDL designation at the right of each connection detail line. The two flows that are listed as ‘No Peer’ are the camera feeds on the branch LAN to the Media Server. These are not optimized because there is no WAN transport of these feeds, the camera feeds are local to the router.

Table of Effective Capacity

In the test results reported here, data is collected for over a hour and the results from the WAAS CM are shown Table 2. These results are summarized from an export of the device dashboard to a CSV file and analyzed. The following table represents the Effective WAN Capacity report for the remote (vpn1-3845-1-WAE) WAE.

Table 2 Effective WAN Capacity

	Bandwidth Savings Bytes	Reduction % (include pass-through)	Reduction % (Exclude Pass-through)	Pass-through Traffic (Bytes)	Application Traffic (Bytes)
	769,179,772	6	10	5,128,480,196	12,473,380,864

The WAN bandwidth savings is shown at less than 10 percent. As a point of reference, the test results in the *Transport Diversity: Performance Routing (PfR) Design Guide* demonstrated compression ratios in the range of 3:1 to over 40:1 for Web and File Transfer sessions generated by Chariot/IXIA. From this, it can be concluded that data traffic is more compressible than the video traffic used in this test.

WCCP Configuration

This section includes the WCCP configurations on the campus and branch router.

Campus Router

The relevant WCCP configuration for the campus router is as follows:

```
hostname vpn-jk2-7206-1
!
ip wccp 61
ip wccp 62
ip cef
!
interface FastEthernet0/1.216
 description CAMPUS with IP Cameras and PC
 encapsulation dot1Q 216
 ip address 192.168.16.1 255.255.240.0
 ip wccp 61 redirect in
 ip wccp 62 redirect out
!
interface FastEthernet0/1.232
 description CAMPUS with WAAS CM and Core WAE
 encapsulation dot1Q 232
 ip address 192.168.32.1 255.255.240.0
 ip wccp redirect exclude in
!
end
```

Branch Router

The relevant WCCP configuration for the branch routers is as follows:

```
hostname vpn1-3845-1
!
ip wccp 61
ip wccp 62
ip cef
!
interface Integrated-Service-Engine2/0
 description NME-WAE-522-K9
 ip address 192.0.2.69 255.255.255.252
 ip wccp redirect exclude in
 service-module ip address 192.0.2.70 255.255.255.252
 service-module ip default-gateway 192.0.2.69
 no keepalive

interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip address 192.0.2.64 255.255.255.254
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip flow ingress
 ip route-cache flow
 service-module external ip address 192.168.11.2 255.255.255.0
 service-module ip address 192.0.2.65 255.255.255.254
 service-module ip default-gateway 192.0.2.64
 no keepalive
!
```

Summary

Video feeds from IP Video Surveillance cameras to the Media Server are TCP-based when the camera is configured for Motion JPEG. Additionally, viewing live or archived feeds through VSOM by a client viewing stations is also TCP/HTTP based for feeds which are either MJPEG or MPEG-4. While TCP-based traffic can be optimized and compressed by WAAS, for this video traffic the compression is on the order of less than 10 percent. Video feeds are compressed by the encoder of the IP camera before being transported over the IP network. Additional compression by WAAS does not provide as dramatic savings as is the case with typical user data traffic.

However, both WAAS and PfR can be implemented effectively together and PfR is shown to manage multiple WAN links and select the path with the least loss and lowest delay.

Wide Area Application Services (WAAS) for iSCSI

The Cisco ISR router Video Management and Storage System (VMSS) network module houses an external Gigabit Ethernet interface on the module faceplate to provide connectivity to a locally attached Internet Small Computer System Interface (iSCSI) storage server. This iSCSI filesystem supplements the on-board disk drive for storing video archives. Cisco Video Management And Storage System (NME-VMSS-HP16/32 NME-VMSS-16) include GigE port for local iSCSI attachment. This is the preferred method and is described in "Local Storage for Video Archives Using iSCSI" section on page 6-41.

While the recommended design is to archive locally, it is possible to route the iSCSI traffic through the ISR router backplane and the WAN interface(s) to reach a target IP address in the enterprise campus. Locating an iSCSI server in the campus and transporting archives across the WAN is of interest to customers for management and support efficiencies. Many customers, knowing the amount of bandwidth required to transport video feeds from surveillance cameras, have requested design guidance on what, if any, benefit implementing WAAS has on iSCSI transport of video archives over a WAN.

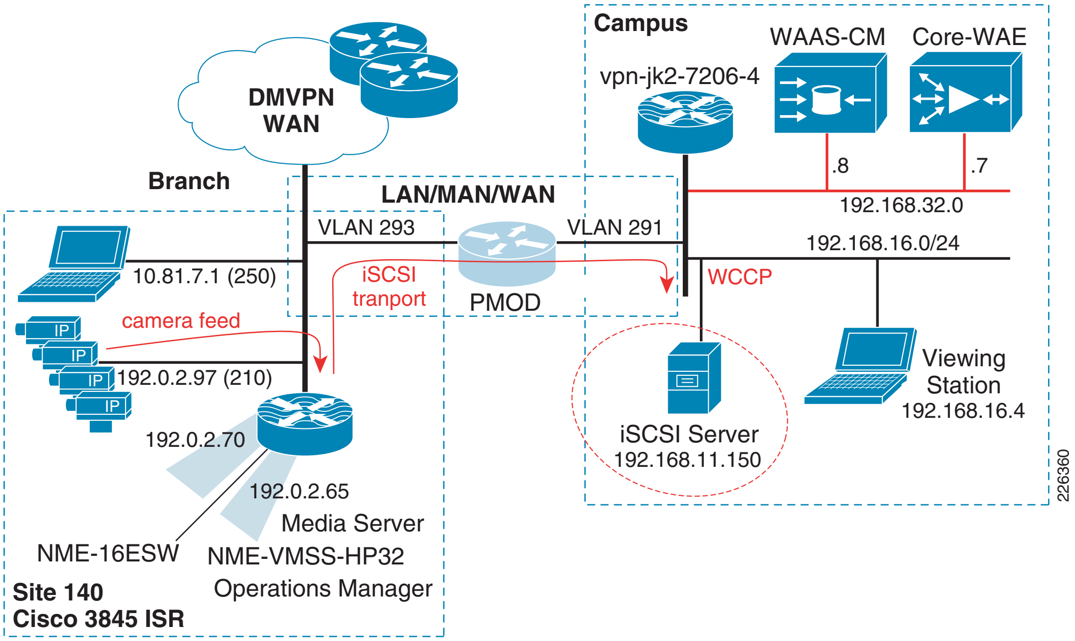
iSCSI Overview

The iSCSI operates over TCP port 3260 in this implementation. It does not require any dedicated cabling, it uses existing LAN switches and the IP network. iSCSI operates as a clear text protocol, there is no encryption inherent in the protcol. If it is transported over a public WAN or the nature of the video feeds require the need for data privacy, IPSec encryption must be deployed to meet that requirement. The TCP session between the NME-VMSS and iSCSI appliance is persistent, or long-lived. It is only terminated or initiated to recover from a timeout or manual shutdown.

Topology

The test topology is very similar to the topology used to test WAAS and PfR between branch and campus. The notable difference is the placement of the iSCSI appliance. Previously, it was attached to a LAN Gigabit Ethernet switch in the branch location. Now, it is connected to the LAN switch in the campus location. The IP address of the server has changed accordingly. There are four IP Video Surveillance cameras in the topology; an Axis 223M (MJPEG), Axis 207 (MPEG-4), Axis 207MW (MJPEG), and a Cisco 2500 series (MPEG4). Results are consistent across all cameras. The iSCSI server is a Buffalo (www.buffalotech.com) TeraStation Pro™ II iSCSI Rackmount Storage System. Figure 35 illustrates the topology.

Figure 35 WAAS and iSCSI Deployment Topology



The path of the camera video feeds, iSCSI transport and location of the iSCSI server in the topology are shown for reference.

Configuration

The relevant portion of the branch router configuration is shown in this section. The WCCP configuration on the router is not changed from what was documented in the previous chapter. Because the iSCSI TCP session originates from the NME-VMSS-HP32 logical interface (Integrated-Service_Engine 3/0) the iSCSI TCP session is intercepted by WCCP configured on that interface.

```
!
hostname vpn1-3845-1
```

```
!
boot-start-marker
boot system flash
   flash:c3845-adventerprisek9-mz.124-15.T5
!
!
interface GigabitEthernet0/1.210
 description IP Camera VLAN
 encapsulation dot1Q 210
 ip address 192.0.2.97 255.255.255.224
!
!
interface Integrated-Service-Engine2/0
 description NME-WAE-522-K9
 ip address 192.0.2.69 255.255.255.252
 ip wccp redirect exclude in
 service-module ip address 192.0.2.70 255.255.255.252
 service-module ip default-gateway 192.0.2.69
 no keepalive

interface Integrated-Service-Engine3/0
 description NME-VMSS-HP32
 ip address 192.0.2.64 255.255.255.254
 ip wccp 61 redirect in
 ip wccp 62 redirect out
 ip flow ingress
 ip route-cache flow
 ! service-module external ip address 192.168.11.2 255.255.255.0
 service-module ip address 192.0.2.65 255.255.255.254
 service-module ip default-gateway 192.0.2.64
 no keepalive
!
```

The external IP address which was in use as the iSCSI local subnet, 192.168.11.0/24, is commented out of the configuration.

The steps to move the iSCSI server from the branch to the campus is to:

Step 1 Deselect Media1_0 as disk from the Media Server.

Step 2 Enter configuration mode of the VMSS network module and issue a ‘state disable’ for Media1 to gracefully shutdown the service.

Step 3 Shutdown the iSCSI service on the iSCSI server, change the IP address and physically move the connection to the correct VLAN at the campus and again enable the iSCSI service.

Step 4 Change the target IP address on the VMSS network module. Because the volume is already formatted, it will become available for use.

Step 5 Select Media1_0 as a disk to be used by the Media Server.

Following the above changes, the relevant portion of the VMSS network module configuration is shown as follows:

```
hostname VMSS-SITE140
storages iSCSI media1

 target-ip 192.168.16.150
  target-ip 192.168.16.150 volumeName iqn.2004-08.jp.buffalo:TS-RIGLB1E-001D7326
2B1E:array1 LUN 0
```

```
 end storages-iscsi

end
```

Verification

To verify WAAS has selected the iSCSI TCP session for optimization, connection statistics for the remote WAE can be displayed with the **show statistics connection** command. Detailed output from the connection specific to the iSCSI TCP session is shown below:

```
vpn1-3845-1-WAE#show statistics connection conn-id 29275


Connection Id:            29275
    Peer Id:                  00:14:5e:85:54:7b
    Connection Type:          EXTERNAL CLIENT
    Start Time:               Fri Jan  9 10:23:56 2009
    Source IP Address:        192.0.2.65
    Source Port Number:       57326
    Destination IP Address:   192.168.16.150
    Destination Port Number:  3260
    Application Name:         Storage
    Classifier Name:          iSCSI
    Map Name:                 basic
    Directed Mode:            FALSE
    Configured Policy:        TCP_OPTIMIZE + DRE + LZ
    Derived Policy:           TCP_OPTIMIZE + DRE + LZ
    Peer Policy:              TCP_OPTIMIZE + DRE + LZ
    Negotiated Policy:        TCP_OPTIMIZE + DRE + LZ
    Accelerators:             None
```

Note The above command was issued on Wed Jan 14 14:06:04 edt 2009 and the start time of the WAAS optimization is 9 January, demonstrating the persistence of the iSCSI TCP session.

WAN Characteristics

In this test, the WAN link in use has a random delay averaging 60 milliseconds in each direction with packet loss of 1 packet per 10,000 packets.

Optimization Validation

In the previous section, the WAAS Effective WAN capacity report is used to demonstrate the bandwidth savings. In this section, NetFlow is used as a demonstration of another method of validating the WAN bandwidth savings. Understanding how NetFlow reports the flows prior to de-compression by the WAE as well as from WAE to the application server also provides a means of understanding how WAAS interception functions. In this test, a NetFlow export is configured on the campus router to a unix server. These Version 5 flows are captured and summarized.

The complete record layout for NetFlow Version 5 Flow Record Format is available on www.cisco.com. The SNMP index of the input and output interface is part of the flow record. In order to associate these Ifindex values with the interface name, the **show snmp mib ifmib ifindex** command is issued on the campus router and portions of the output are as follows:

```
vpn-jk2-7206-1# show snmp mib ifmib ifindex
FastEthernet0/0: Ifindex = 1
Null0: Ifindex = 6
…
FastEthernet0/1.232: Ifindex = 26
…
FastEthernet0/1.216: Ifindex = 25

FastEthernet0/1.291: Ifindex = 31
```

Both the WAAS compressed and optimized and the original flows are reported by NetFlow in the exported records. Because the source and destination IP address and port numbers are unchanged by WAAS, the Ifindex values are needed to identify the flows seen input from the WAN interface, and then the flow as it is observed following WCCP redirection.

NetFlow summarizes and reports the flow based on the source and destination IP address, port number, protocol, and ToS byte. The ECN bits are part of the ToS byte. The ECN field is bits 6 and 7 in the IPv4 ToS octet.

The layout of the ToS byte from RFC 3168 is as follows:

```
   0     1     2     3     4     5     6     7
   +-----+-----+-----+-----+-----+-----+----+-----+
   |            DS FIELD, DSCP         | ECN FIELD |
   +-----+-----+-----+-----+-----+-----+----+-----+
        DSCP: differentiated services codepoint
         ECN: Explicit Congestion Notification
```

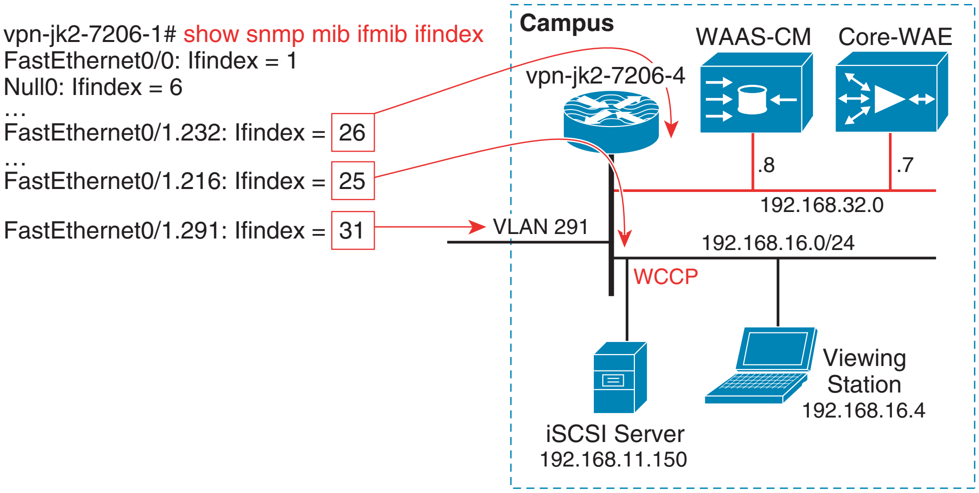
WAAS sets the ECN bits and because NetFlow v5 reports all eight bites of the ToS byte, the flow observed from the WAN interface is reported as two flows; with and without the ECN bits set.

The Ifindex numbers displayed by the **show snmp mib ifmib ifindex** command are referenced on the topology as follows:

- Ifindex 26 is VLAN 232—Core-WAE
- Ifindex 25 is VLAN 216—iSCSI Server
- Ifindex 31 is VLAN 291—WAN
- Ifindex 0 is the router chassis itself

These are shown in Figure 36.

Figure 36 Ifindex to Interface Mapping



```
vpn-jk2-7206-1# show snmp mib ifmib ifindex
FastEthernet0/0: Ifindex = 1
Null0: Ifindex = 6
...
FastEthernet0/1.232: Ifindex = 26
...
FastEthernet0/1.216: Ifindex = 25

FastEthernet0/1.291: Ifindex = 31
```

In testing, NetFlow v5 export is configured on the campus 7206 and summarized. The iSCSI traffic flows are extracted from the summarized data and presented in Table 11. A single archive of one camera, an Axis 207MW, is active during the data capture.

Table 11 NetFlow Export Summarized Data for Axis 207MW

Src IP / port	SrcIfIndex	Dst IP/ port	DstIfindex	PPS	Bytes per Packet	Protocol/ToS Byte	Total Bytes
Core WAE	to	iSCSI	Server				
192.0.2.65 57326	26	192.168.16.150 3260 [iSCSI]	25	363	1430	TCP / 0	245,092,552
WAN	to	Core WAE					
192.0.2.65 57326	31	192.168.16.150 3260 [iSCSI]	0	8	250	TCP / 0	839,682
192.0.2.65 57326	31	192.168.16.150 3260 [iSCSI]	0	352	1451	TCP / 2	240,762,778

There is a single flow reported from the core WAE to the iSCSI server. This is the flow post WAE processing. From the WAN to the core WAE, there are two flows reported: one flow with a ToS byte of 0 another with a ToS byte value of 2. The ToS byte value of 2 flow are packets in the WAN traffic with the ECN field populated.

To compare the flows from the WAN to the core WAE and from the core WAE to the iSCSI server, we must add the total bytes from WAN to core WAE (839,682 + 240762778) for a combined value of 242,602,460 bytes. The number of bytes for the core WAE to the iSCSI server is 245,092,552. By comparing these two sets of values, the optimized verses the unoptimized traffic, the impact of WAAS compression on the flows is less than two percent.

As a point of comparison and verification, the Media Server provides the details of that same data when stored as an archive on the iSCSI disk. This output is shown as follows:

```
Archive History Details: 5MIN_207MW_only

Archive Name   : a_p_Axis_207MW__192_0_2_98_-_a_5MIN_207MW_only
Storage Path   : /media1_0/1000
Archive Type   : regular
Video Width    : 1280
Video Height   : 720
Archive Status   : SHELVED
Archive Media   : jpeg
Recording Rate   : 10.581754 Mbps
Video Quality   : 50
Video Framerate : 30.000000 fps
Video Bitrate   : 640
Archive Expiry   : 5 days
Archive Size   : 224512 Kbytes
Archive Start Time: Fri Jan  9 16:00:02 2009
Archive End Time   : Fri Jan  9 16:04:46 2009
Max Fps  : 13.482701
Max Frame Size   : 103171 bytes
Archive Duration : 300 seconds
Current Duration : 284 seconds
Current Retention: 94.67%
```

This is a five-minute archive of a 1280 x 720 resolution Motion JPEG that on disk is 224,512 Kbytes. The NetFlow export includes IP Layer-3 overhead which accounts for the higher number of bytes reported by NetFlow.

Summary

Both Motion JPEG and MPEG4 or H.264 camera feeds are compressed by the encoding function of the IP Camera. Persistent Lempel-Ziv (LZ) compression can achieve compression ratios in the order of 2:1, 5:1 or even up to 100:1 if the data contains common strings of characters. LZ compression can be beneficial for data which has not been previously traversed the network and categorized by Data Redundancy Elimination (DRE). DRE maintains a database of data that has been observed on the network. DRE is application independent. DRE can eliminate up to 99 percent of redundant network traffic and provide up to 100:1 compression.

Because the files being transported and archived to the iSCSI server are solely video feeds, and this data has been compressed by the encoding function of the IP cameras, the iSCSI transport shows little bandwidth savings. However, WAAS can be very instrumental in compressing application data to free bandwidth for other uses, including network video traffic.

Controlling Access to IP Video Surveillance

This section provides a high-level overview of how to control access using policy-based access-control lists on Cisco IOS routers to limit access to IP video surveillance resources. Included is an example on how to block traffic to video surveillance resources when these services exist in the enterprise global routing table along with other end-user devices. There are two subsections:

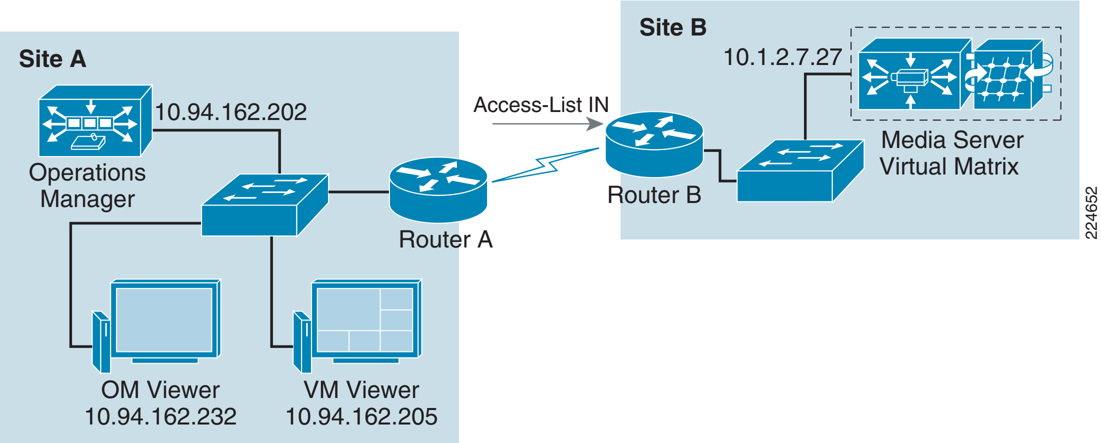
- Securing IP Video Surveillance Traffic, page 6-81
- Securing Access to ISR VMSS Network Modules, page 6-83

In the Virtualization, Isolation and Encryption of IP Video Surveillance chapter, a more detailed discussion on implementing both policy-based and control plane access control is provided. Each enterprise deployment must balance the need for access control to resources against the cost and complexity. The next two chapters provide the network manager with a review of the techniques to deploy very basic or very advanced access control techniques.

Securing IP Video Surveillance Traffic

Figure 37 shows an example where the viewers and the Operations Manager are separated from the Media Server and Virtual Matrix through Cisco IOS routers. The Media Server and Virtual Matrix applications are installed on the same server. In this example IOS access lists are used but other security devices, such as the Cisco ASA 5500 Adaptive Security Appliance may be used.

Figure 37 Traffic Filtering



The following access lists shows simple ways to block traffic to these resources and control what devices can receive video streams. The same examples can be used if a firewall is in place to protect video streams.

The syntax may vary when using different IOS or firewall devices.

The following access list may be applied to Router B to allow traffic destined for the servers on Site B.

```
interface Multilink1
 ip address 10.1.20.2 255.255.255.252
 ip access-group ALLOW_VMS in
 ppp multilink
 ppp multilink group 1
!
!
ip access-list extended ALLOW_VSM_TRAFFIC
 permit tcp any host 10.1.27.27 eq www
 permit tcp any host 10.1.27.27 eq 1066
 permit tcp any host 10.1.27.27 eq 8086
 deny   ip any any
```

The access-list is applied to the Multilink1 interface on the incoming direction and specifies what traffic can reach the server Site B. This access list allows any hosts to reach the 10.1.27.27 server and blocks all other types of traffic. Access lists have an implicit deny statement at the end of the list in order to block traffic types that were not explicitly permitted with the access list.

The access-list only allows the following traffic types to reach the server with IP address 10.1.27.27:

- HTTP traffic. This traffic is required for all viewers to reach the Media Server and receive video streams
- TCP port 1066, required by the VM monitor client to reach the Virtual Matrix server
- TCP port 8086, required by the Operations Manager to reach the Virtual Matrix server

The following example shows an access-list with more granular statements to allow traffic only from specific hosts and block any other hosts from access video streams.

```
interface Multilink1
 ip address 10.1.20.2 255.255.255.252
 ip access-group ALLOW_VSM_HOSTS in
 ppp multilink
 ppp multilink group 1
!
!
ip access-list extended ALLOW_VSM_HOSTS
 permit tcp host 10.94.162.202 host 10.1.27.27 eq 8086
 permit tcp host 10.94.162.205 host 10.1.27.27 eq 1066
 permit tcp host 10.94.162.232 host 10.1.27.27 eq www
 permit tcp host 10.94.162.205 host 10.1.27.27 eq www
 deny   ip any any
```

This access list is also applied to the incoming traffic of Router B and only allows traffic from the hosts on Site A to reach the server resources at 10.1.27.27. This example allows the network administrator to ensure that video streams reach only the intended recipients.

The diagram in Figure 37 does not show IP Cameras or encoders but the traffic from those devices can also be blocked or configured to reach only the intended Media Server acting as the direct proxy.

For MJPEG transmission, Media Servers communicate with edge devices using TCP port 80 (HTTP) but in some cases a different transmission and protocol may be selected.

When using MPEG-4 video transmission, the Media Server communicates with cameras using unique UDP port numbers. The ports listed in Table 12 show the UDP ports used by different manufacturers.

Table 12 UDP Ports Used for MPEG-4

Edge Device Model	UDP Ports
Axis	16400
Bosch	6001–60001
Cisco	65000
Cornet	16400
Mango	2000
Panasonic	1024
Smartsigth	19000
Sony	1024
Teleste	
MPEG2	16400
MPEG4	16100–65534
Vbrick	18000

The network path must allow for the appropriate TCP and UDP ports to travel freely between edge devices, application servers, and viewing stations. If access control lists (ACL) or firewalls are deployed between the devices, they should be configuration to allow traffic between all video surveillance devices.

Securing Access to ISR VMSS Network Modules

The Video Management and Storage Software implementation on the ISR network modules must establish a connection, usually through the web server of the IP cameras, to direct the camera to initiate video feeds to the media server for live viewing and archiving, If the IP camera requires authentication, as does the Cisco IP Cameras, a username and password is entered on the ‘Add a new IP/Network Camera’ and the ‘Camera requires authentication’ dialog box is selected on the form.

Passwords in a Cisco IOS router can be entered in the configuration as clear text (type 0), a type 7 encryption (hashing) or type 5, which uses the MD5 algorithm. Type 5 passwords are the most secure of the three. There is currently no known method for decrypting a type 5 password, but can compromised by a initiating a brute-force or dictionary attack. The password strings in the IOS configuration file can be viewed if someone has physical access to the router, can log into the router either through the console or over the network (Telnet, SSH, HTTP, etc.) and can access the router in enable mode (privilege level 15) which allows the configuration file to be viewed. Additionally, router configuration files are often stored on a TFTP or FTP server for backup and recovery purposes. Access to these files must also be safeguarded to prevent unauthorized access.

Type 0 Passwords

In Cisco IOS, type 0, or clear text passwords are stored without the benefit of any hash or encryption algorithm. Here is an example of the configuration file with a clear text password.

```
no service password-encryption
username test password 0 w3nd0v3r
```

Passwords for the IP cameras defined to the VMSS network module are stored as **.xml** files with the password, username, camera IP address, and other configuration information in clear text.

Type 7 Passwords

Type 7 passwords are obfuscated, not encrypted. These passwords can be displayed in clear text by several publicly available scripts, as does the Cisco IOS show command ‘show key chain’. An example username with the type 7 password is entered and then displayed.

```
service password-encryption
username test password 7 044C58080B715A1D1B
!
key chain decrypt
 key 1
   key-string 7 044C58080B715A1D1B
!

vpn4-3800-6#show key chain decrypt
Key-chain decrypt:
    key 1 -- text "w3nd0v3r"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
```

The Type 7 passwords are used for PAP configurations, as with PAP, passwords are sent over the circuit "in the clear". Cisco IOS must have some means of recovering the original clear text from hashed value of the type 7 password for PAP and other protocols.

Type 5 Passwords

Type 5 passwords are the most secure of the three. There is currently no known method for decrypting a type 5 password, but can compromised by a initiating a brute-force or dictionary attack. An example of a type 5 password from a Cisco IOS configuration file is as follows:

```
username wendover privilege 15 secret 5 $1$02OG$.fgh.mKdXD8hiVOUi6kb6/
```

IP Camera Passwords

These usernames and passwords are stored in the individual camera configuration files clear text and by default, require no user authentication on the VMSS network module to view the files. This has been identified by defect

```
CSCsu36435 ISR VMSS IP Camera passwords displayed in clear text without authenticat
```

While type 7 passwords obfuscation could be used for the camera username and password, which would provide some degree of protection, the more pressing issue with the CSCsu36453 defect is the fact that no authentication is required to see the .XML configuration files by default. The next section describes one method of addressing this issue.

Control Access to the VMSS Network Module

To limit exposure of this vulnerability, several configuration options must be implemented on the ISR router to require authorization and a secure network channel between network devices and the VMSS network module. Access to the VMSS network module is through telnet to a port on the host router which corresponds to the console of the Integrated Service Engine (VMSS) network module. The ‘service-module’ command in Cisco IOS is essentially a reverse-telnet command to the appropriate port number assigned to the network module. To determine which port is used for the module, issue the *service-module* command. The port number assigned is the TTY line plus 2000. In this example, the port number for interface In2/0 is 2130.

```
vpn4-3800-6#service-module integrated-Service-Engine 2/0 status
Service Module is Cisco Integrated-Service-Engine2/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Foundation 1.1.1
FNDN Running on NME
```

To prevent unauthorized remote access to the network module, and to the camera configuration files, several Cisco IOS hardening concepts should be implemented to limit exposure.

- **Enable SSH on the Router**—Enabling SSH first requires generating an RSA key for the router.

```
vpn-jk3-2651xm-1(config)#cry key generate rsa
The name for the keys will be: vpn-jk3-2651xm-1.ese.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

vpn-jk3-2651xm-1(config)#
Sep 12 15:15:57.562 edt: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

- **Disable Telnet access, enable SSH access** —The router and VMSS network module should not be network accessible through an insecure channel. Only allow SSH connections to the VTY ports of the router.

```
line vty 0 4

 transport input ssh
```

- **Permit access to the VMSS module from the host router**— deny all other access. The forces the use of SSH over the WAN. This example assumes the interface addressing as shown, with a TTY line of 130 (TCP port 2130). The log option on the deny statement is optional, however is useful for troubleshooting.

```
!
interface Integrated-Service-Engine2/0
 ip address 192.0.2.33 255.255.255.252
 service-module ip address 192.0.2.34 255.255.255.252
 service-module ip default-gateway 192.0.2.33
!
!
ip access-list extended LOCAL_LOGIN
 permit tcp host 192.0.2.33 any eq 2130
 deny   ip any any log
!
```

The access-list is applied to the TTY line in the following example.

- **Require authentication for reverse Telnet to the network module**—A local username with a type 5 password can be configured on the host router, or radius can be used for authentication.

```
username wendover privilege 15 secret 5 $1$02OG$.fgh.mKdXD8hiVOUi6kb6/


line 130
 access-class LOCAL_LOGIN in vrf-also
 login local
 no activation-character
 no exec
 transport preferred none
 transport input telnet
 transport output none
!
!
line vty 0 4
 transport input ssh
 login local
!
```

In the above configuration example, remote access is SSH only, Telnet has been disabled, and the login is locally authenticated. Access to the network module is only permitted from the IP address of the logical interface and is also re-authenticated.

Test the Configuration

To test this configuration, attempt a session to the service module after successfully logging into the host router. The output is shown below:

```
vpn4-3800-6#service-module in2/0 session
Trying 192.0.2.33, 2130 ... Open

   C i s c o S y s t e m s
     ||                ||
     ||                ||       Cisco Systems, Inc.
    ||||             ||||       IT-Transport
 .:|||||||:.......:|||||||:..
  US, Asia & Americas support:    + 1 408 526 8888
 EMEA support:                   + 31 020 342 3888
  UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
 You must have explicit permission to access or configure this
 device. All activities performed on this device are logged and
 violations of this policy may result in disciplinary action.


User Access Verification

Username: wendover
Password:
Password OK
SITE150>
SITE150>


SITE150> show video-surveillance configs
...
```

To verify that access to the VMSS network module is blocked without first logging on the host router, initiate a telnet to port 2130 of the host router. The connection must fail and the logging option on the access-list has identified the source IP address of the PC nictitating the Telnet session.

```
C:>telnet 192.0.2.33 2130
Connecting To 192.0.2.33...Could not open connection to the host, on port 2130:
Connect failed
```

```
vpn4-3800-6#
Sep 12 15:12:44.150 edt: %SEC-6-IPACCESSLOGP: list LOCAL_LOGIN denied tcp
10.81.7.78(4223) -> 0.0.0.0(2130), 1 packet
```

This demonstrates that access to the configuration files of the VMSS network module can be secured over the WAN by requiring SSH to access the host router, and to require multiple userid and password checks before an administrator can access the network module.

References

Additional tools and techniques to protect and secure Cisco routers can be found in the *Cisco Guide to Harden Cisco IOS Devices* - Document ID: 13608 at the following URL:

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml

Additional security related documentation is available at www.cisco.com.

Virtualization, Isolation and Encryption of IP Video Surveillance

This section demonstrates how to secure and logically separate an enterprise network to support IP Video Surveillance. The design described in this section implements the concepts of virtualization, path isolation, and encryption at both branch and campus LAN/WAN. If remote users have a business requirement to view live and archived video feeds, an option to provide an authenticated and secure VPN connection is also shown.

Definitions and Goals

The term *network virtualization* is the creation of logical isolated network partitions over a common network infrastructure. The concept of virtualization of computing resources is not new, IBM released the operating system Virtual Machine Facility/370 in 1972. This software implemented a virtual hardware architecture on IBM 370 hardware. The primary advantage of virtualization for network or computing resources is to share a common hardware within the bounds of isolating the address space of one user from another.

In networking terms, *path isolation* is an important component of virtualization and it describes the creation of independent logical traffic paths over a shared physical network infrastructure. Path isolation is implemented in LAN switches by means of virtual LANs (VLANs). In WAN environments, path isolation is typically implemented through the use of virtual circuits. Both Frame-Relay and ATM include the concept of virtual circuits. Physically separate circuits can be associated with a Virtual Routing and Forwarding Lite (VRF-Lite) instance, a virtual router, and isolated from other VRF instances or the global routing table. Generic Routing Encapsulation (GRE) or IPSec encrypted tunnels can also be configured to provide path isolation. Examples of this are shown in "Configuring DMVPN Tunnel Interface" section on page 6-97, a Cisco IPsec/GRE solution.

By implementing VLANs, VRF-Lite and optionally IPSec/GRE, the network manager can provide access to a common network infrastructure while maintaining a separate address space, broadcast domain, and separation of one user group from another. *Segmentation* is the term often used to describe this technique and is synonymous with the term *isolation*. In layman's terms, network virtualization is a general concept, while path isolation is specific to maintaining a separation of the isolated network partitions between two points in the topology.

Historically, the physical security manager and the network manager had little interaction between their respective responsibilities. The physical security manager relied on a network infrastructure of coaxial cable (COAX) between camera, matrix switch, CCTV monitor, and networked digital video recorder (NDVR). Twisted pair (RS-485) is deployed for Pan Tilt Zoom control of analog cameras. The key requirement of any video surveillance implementation is the three Rs: *resolution, retention, and reliability.* Resolution in analog deployments is typically '4CIF/30', meaning 704x576 pixels at 30 frames per second. Retention is based on the number of days and is either regulated by a government agency, such as the State of Nevada Gaming Control board, a corporate policy, or the necessities of costs and the available disk space. Reliability is accomplished through a combination of the separate physical cable plant and human controls verifying the usefulness of the video images.

In many cases the physical security manager is going to be more confident in his ability to address the surveillance needs of the enterprise with a reliable, physically separate, cable plant for which he has total control.

Historically neither the physical security manager of value added resellers (VARs) are experts in IP networking. Therefore, the idea of transporting video over the enterprise IP network, with cameras sharing the same network with end-user workstations, servers, voice over IP (VoIP), and Internet traffic is an unknown, a cause for concern for the physical security manager. The physical security manager now must rely on the network manager for some degree of success and this is a barrier to acceptance.

Techniques to Achieve Virtualization

There are two primary techniques used to achieve network virtualization: policy-based and control plane-based. In this section, both techniques are implemented in a synergistic fashion to logically separate the video surveillance traffic from the other network traffic.

Policy-Based

Policy-based network virtualization restricts the forwarding of traffic to a specific destination based on some rule or administrative policy. These policies are independent of the control plane, meaning the destination is reachable and it may be listed in the routing table, but it is administratively prohibited. The most common implementation example is an access control list (ACL) on a router or firewall.

To implement policy-based controls, the router or firewall examines IP packets entering an interface and either forwards or drops packets based on matching fields in the IP header, transport header, or in more advanced implementations, some character string or fields in the payload of the packet. Firewalls also implement general policy-based matches on the security level of the source and destination interface of the packets. By default, firewalls permit packets to flow from a higher (more trusted) interface to a lower (less trusted) interface and the return path of that session is dynamically permitted. Packets that must be permitted from the less to more trusted interface must be explicitly defined and permitted.

Control Plane-Based

Control plane-based network virtualization is implemented by restricting the propagation of routing information. In other words, the routing tables are virtualized. The IP networks are segregated by their respective virtual routing table, or VPN routing and forwarding (VRF) table. VRF-Lite is one method of segmenting the routing tables, by creating virtual routing domains. These domains may reuse the same IP network addresses, they need not be globally unique. The can use separate address spaces from the remainder of the enterprise network or private address spaces based on RFC 1918 addressing. However, to aid in troubleshooting, it may be easier for the enterprise network manager to allocate unique IP addressing to each VRF domain. Allocating address space that facilitates summarization is as applicable to a VRF as is the case with routes in the global routing table.

Both policy-based and control plane-based techniques can be implemented in a synergistic approach to segment the network. The topology implemented in this sample deployment demonstrates both techniques. A firewall is implemented to connect the global routing table and the IP video surveillance domain (IPVS VRF) to allow a controlled and restricted access between the two domains.

IPSec Encryption

IPSec encryption provides privacy of the data, voice, and video on an IP network. Digital signatures is an important component of any IPSec implementation, providing authenticity (verifying the identity of the peer) and hashing techniques provide integrity (verifying packets have not been manipulated in transit).

In many encryption implementations, a logical tunnel interface joins two or more crypto peers, which in itself facilitates path isolation. Dynamic Multipoint VPN (DMVPN), generic routing encapsulation (GRE) over IP Security (IPSec) , IPSec/GRE, and Static Virtual Tunnel Interfaces (SVTI) are all examples of logical tunnel implementations. Group Encrypted Transport VPN (GET VPN) and Secure Sockets Layer virtual private network (SSL/VPN) are examples of payload encryption that have no logical tunnel interface. An IPSec implementation based on logical tunnels is more applicable to path isolation than payload encryption, because the logical tunnel endpoints can be in the global routing table with the tunnel itself residing in a VRF.

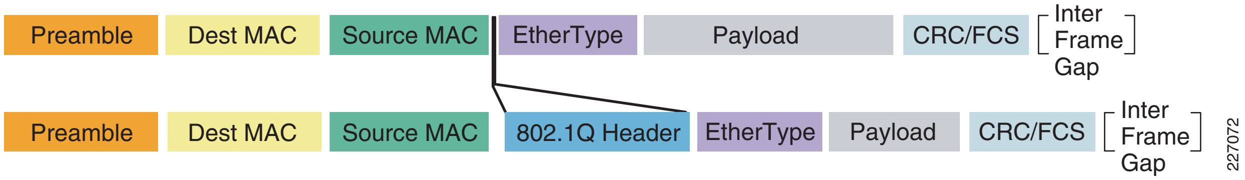
Multiple logical tunnels may be transported over a single physical path, providing an effective means of path isolation without the additional costs of a separate physical circuit. Alternately Layer-2 virtual circuit such as is implemented by ATM, 802.1Q trunking or Frame Relay could also be used, but there is no inherent privacy, authentication, or integrity component as with IPSec.

Path Isolation for LANs

In a campus LAN environment, IEEE 802.1Q (also known as VLAN tagging) is a means of associating a VLAN identifier with a Ethernet frame. This facility allows multiplexing several VLANs over the same physical switch and links between other switches, routers, and hosts. This allows for path isolation in a Layer-2 LAN in a campus or Metro-Ethernet service provider.

The Ethernet frame is not encapsulated, as is the case with IPSec or GRE tunnels; rather, a header is inserted between the source MAC address and the EtherType field in the frame. This concept is shown in Figure 38.

Figure 38 Ethernet Frame with VLAN Tagging



The 802.1Q header contains two fields of interest to the network manager: the VLAN identifier and the priority code point, or IEEE 802.1p class-of-service (CoS). The CoS field may be used to mark packets for the purpose of Layer-2 prioritization. The Cisco 4000 Series IP cameras can mark both CoS (Layer-2

QoS) and DSCP (Layer-3 QoS). Many LAN switches can prioritize frames based on the Layer-3 DSCP value so the use of Layer-2 QoS marking may be of less importance than the VLAN identifier associated with a tagged frame.

Note *CSCsz45893 Layer-2 CoS (802.1Q/p) for 4000 Series IP Camera* provides more information on the switch port configuration to support this feature.

In the topology demonstrated in this section, IP cameras are attached to switch ports that are configured as access ports associated with the appropriate VLAN, and the branch ISR routers are connected to the switch over an IEEE 802.1Q trunk link. This configuration allows both corporate end-users to share the same switch chassis as the IP video surveillance cameras, while maintaining isolation through unique VLANS and IP addressing.

Path Isolation for WANs

The ability to provide access from a central command center to video surveillance systems located at remote or branch offices is a key business driver for deploying IP-based systems. Many retail organizations currently create a physical CD-ROM / DVD of video feeds needed by the command center and use an overnight courier service to transport the media. Alternately, the investigation team may travel to the store location and view the video archive in-person at the store. Both of these methods of exchanging the video archive are costly and introduce delay of one or more days. Given the business requirement to demonstrate segmentation for IP video surveillance and the need to view video from a branch by the central command center, the WAN must therefore extend the segmentation between VLANs at the branch and command center.

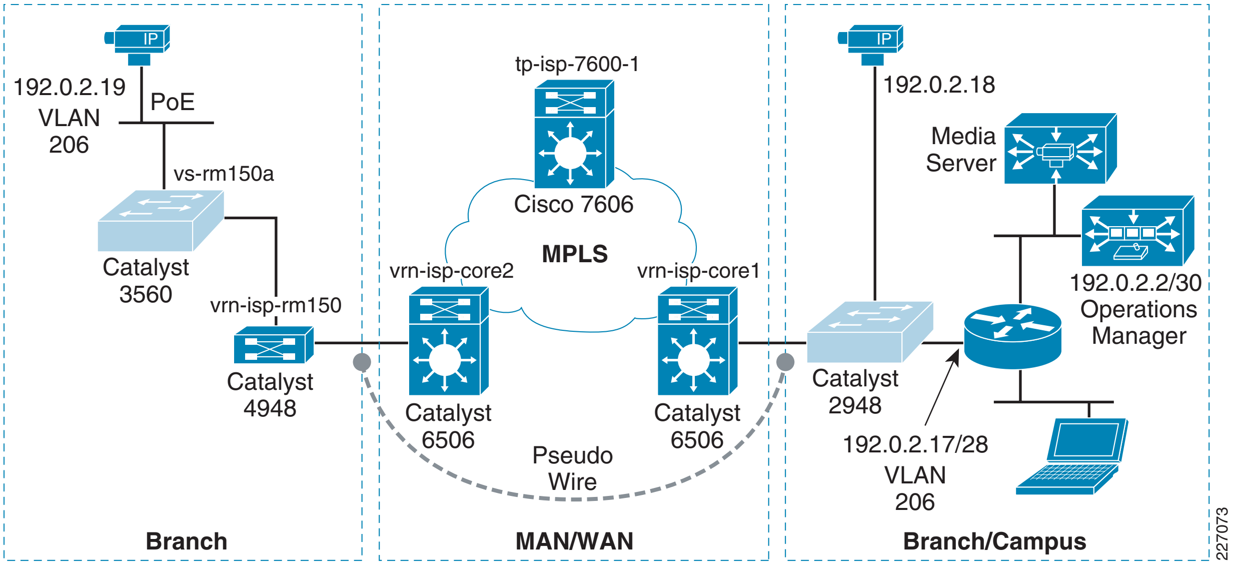
While segmentation with VLANs on a single switch incurs no costs, provisioning physically separate WAN circuits to connect these VLANs may be cost prohibitive. While Layer-2 virtual circuits based on Frame Relay and/or Frame Relay/ATM service interworking could be used to extend these LANs and provide path isolation, the exiting branch access circuit will likely have insufficient bandwidth. Many legacy branch access circuit data rates are typically at T1/E1 (1.5/2.0 Mbps) or less. As a rule of thumb, a standard definition IP camera requires approximately 1 Mbps and a high definition IP camera requires 3 to 4Mbps per feed.

Branches with access-circuits of dedicated leased lines (T1/E1 or DS3) that have no concept of a virtual circuit at the data link layer can be logically segmented by the use of multiple IPSec or GRE tunnels traversing the physical circuit. The test topology in this section demonstrates how to implement path isolation with IPSec tunnels (specifically DMVPN) as well as with Layer-2 path isolation using VLANs simulating a Metro-Ethernet type deployment.

As a best practice, video feeds from the cameras are stored to the local disk subsystem of the Media Server. The WAN connectivity between branch and campus location is segmented by VRF-Lite. Video is stored locally and only transported over the WAN occasionally for investigative purposes. As a point of reference, it is possible to implement a MPLS pseudowire deployment such that a camera at a remote location appears to be attached to the same LAN segment local to the Media Server and Operations Manager, and viewing stations.

This topology is illustrated in Figure 39.

Figure 39 MPLS Pseudowire Deployment



One practical application of this topology is a deployment where no corporate user-access is required and a single camera is sufficient for the business needs at the remote location. However, because the video feed is transmitted across the MPLS pseudowire WAN before being archived on the Media Server, packet loss must be managed by the service provider SLA and QoS marking, shaping, and queueing by both the enterprise and service provider. Costs in this deployment must also be considered, because the access circuit will likely be a dedicated T1/E1 that could be cost prohibitive. Single camera deployments may be better served by a teleworker class router, such as a Cisco 880 Series and a business class broadband access circuit.

While this topology may be implemented, the recommended solution is to store video locally, as close to the camera generating the feed as practical, and only transport across the WAN for occasional viewing or off-hours backup.

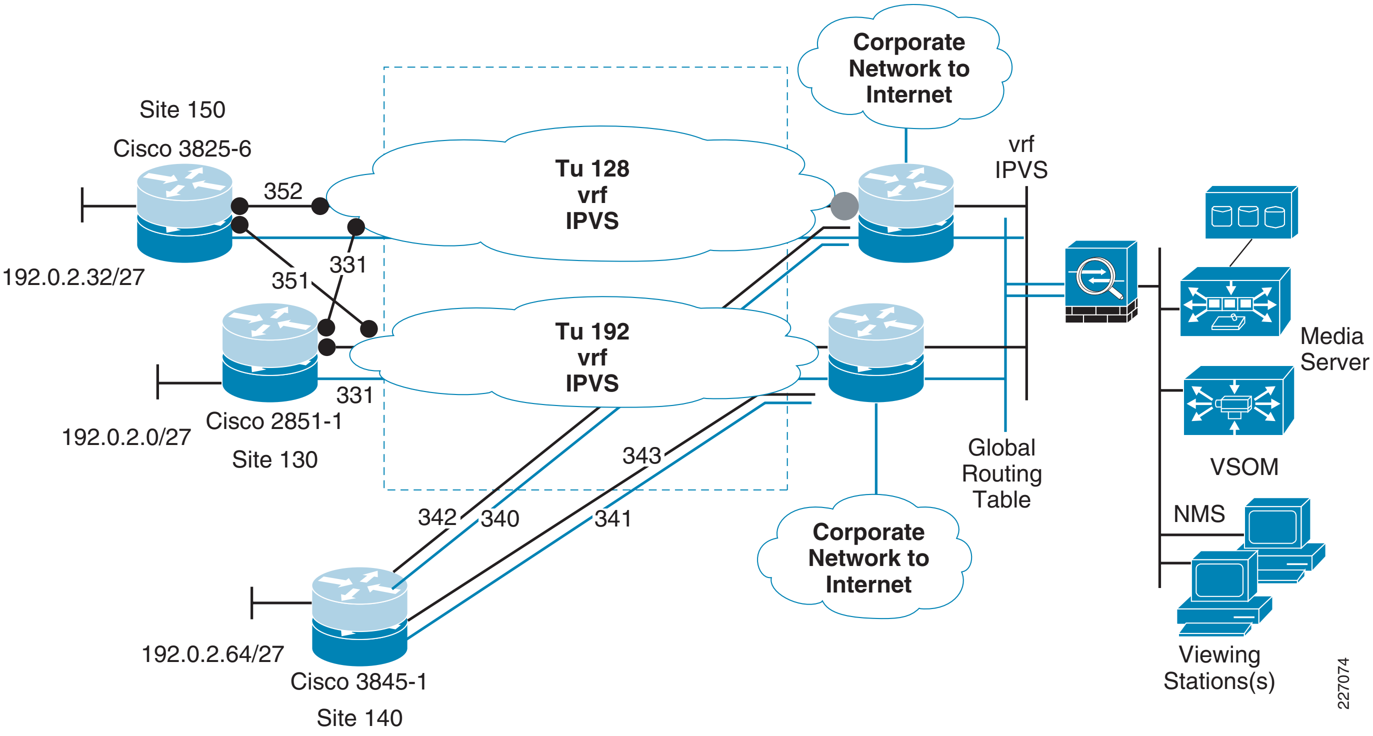
Implementing Virtualization

In this section the configuration of the switches, routers, and firewalls are discussed and the relevant configuration commands are shown to implement network virtualization and path isolation to segment the IP video surveillance devices and end-points from the global routing table. This segmentation of the network is accomplished by isolation of the control plane and network address space at the branch locations and campus command center by the use of VRF-Lite to create virtual routing tables. IP networks are comprised of both Layer-3 (routed) and Layer-2 (switched) domains. VRF-lite (VRFs without MPLS) is used in this enterprise network example to implement a virtual routing protocol instance. To provide end-to-end segmentation, both Layer-2 and Layer-3 are virtualized and mapped to each other accordingly.

Topology Diagram

The testing topology used is shown in Figure 40.

Figure 40 Virtualization Topology



In Figure 40, there are three branch locations each with a single Cisco ISR router. Both blue and grey router icons are shown to represent virtualization of the routing table. The blue icons represent the global routing table and the grey router icons represent the IPVS virtual routing table. The WAN aggregation routers shown in the center of the diagram terminate the branch locations and connect to the corporate network and Internet through separate DMVPN tunnels. These aggregation routers therefore are tunnel aggregation routers for the branches in the topology, and are spoke routers for connectivity to the corporate network. The aggregation routers are configured with HSRP on both the global routing table interface to the firewall as well as the IPVS interface.

Topology Description

In Figure 40, the Video Management and Storage System (VMSS) and Analog Video Gateway (AVG) network modules are logical interfaces. They, along with the DMVPN tunnel interfaces, are mapped to a Layer-3 domain: the VRF. The tunnel source and destination IP address are in the global routing table while the logical tunnel interface itself is in the video surveillance VRF. This separate VRF is named IPVS (for IP Video Surveillance). The iSCSI appliances, IP cameras, and viewing stations reside on a VLAN separate from the underlying corporate IP network and is in the IPVS VRF.

There are three branches shown in this topology example. Two branches demonstrate the deployment of DMVPN and one branch uses multiple virtual circuits (simulating MetroE MAN/WAN) for path isolation. At the branch locations, the iSCSI servers and IP cameras are in their own unique VLANs, which are dedicated to their respective function. Separate VLANS exist for the normal end-user traffic at the branch location and access to these devices are accomplished through the existing global routing table.

To demonstrate policy-based access control, a Cisco ASA5510 firewall is deployed at the command center location. This firewall includes two external interfaces, one in the global routing table and a second in the IPVS VRF. The inside, or most secure interface, is connected to a LAN switch and a VLAN to support the command center Media Server, VSOM, cameras, storage servers and viewing stations are deployed. This inside interface uses a subnet of the IP network address space allocated to the IPVS VRF. Access to the command center VLAN is controlled by firewall policy and static IP routes on the core routers and firewall. The NAT/pNAT configuration on firewall as well as the security levels and access-list permits communication from the IPVS VRF to the global routing table, provided that the session is initiated from the command center VLAN. There is no inbound global routing table access permitted to the IPVS VRF; only the return path to established sessions are permitted. Next, controlled inbound access is implemented by deploying a VPN concentrator.

The VPN concentrator (Cisco VPN 3000 Series) is added to the topology to allow access for selected users in the global routing table to the command center VLAN. The Cisco VPN client on the workstations connects to the VPN concentrator to authenticate the end-user and create a private and secured access to view live or archived video feeds. Adding the concentrator demonstrates a technique by which an external agency, such as a law enforcement department, can be provided with secured and authenticated access over the Internet/extranet.

Because the VPN concentrator allocates an IP address from the IPVS VRF address space, no NAT/pNAT exists inside the crypto tunnel. There are issues with access to a VSOM/Media Server web addresses and ports when these devices are behind a NAT/pNAT device. This is discussed in a separate section.

Address Table

Details of the IP addressing scheme in use for the following topology examples is shown in Table 3.

Table 3 Virtualization IP Addressing Scheme

Routing Table/VLAN	IP Address	Comments
WAN/MAN Global	192.168.15.0/26	MAN/WAN Interfaces (w/ crypto)
vpn4-3800-6 351	192.168.15.28/30	GigabitEthernet0/0.351
vpn4-3800-6 351	192.168.15.28/30	GigabitEthernet0/0.351
vpn4-3800-6 352	192.168.15.48/30	GigabitEthernet0/0.352
Global	10.81.7.0/24	Enterprise end-user
vpn4-3800-6 203	10.81.7.88/29	GigabitEthernet0/0.203
WAN IPVS vrf	192.168.15.64 /26	MAN/WAN Interfaces (w/o crypto)
DMVPN Tu128 IPVS vrf	192.168.15.128/26	vpn-jk2-7206-1 Headend
DMVPN TU192 IPVS vrf	192.168.15.192/26	vpn-jk2-7206-2 Headend
IP VS Net IPVS vrf	192.0.2.0/24	Branch / Command Center Cameras, VSOM, AVG, Media Svr
vpn4-3800-6 IPVS vrf	192.0.2.32/27	Null0 - summary
vpn4-3800-6 IPVS vrf	192.0.2.32/30	Integrated-Service-Engine2/0 (VMSS)
vpn4-3800-6 IPVS vrf	192.0.2.36/30	Video-Service-Engine1/0 (AVG)
vpn4-3800-6 208	192.0.2.48/28	GigabitEthernet0/0.208 (Cameras)
iSCSI IPVS vrf	192.168.nnn.0/24	iSCSI Mgmt networks
vpn1-3845-1 256	192.168.11.0/24	
vpn1-2851-1 254	192.168.111.0/24	
vpn4-3800-6 258	192.168.211.0/24	

Implementation Overview

In the following sections, sample configuration files are shown to demonstrate the techniques used in creating a virtualized network for IP Video Surveillance. These steps include:

- Defining the VRF and Mapping Logical Interfaces
- Mapping Layer-2 (VLAN) to Layer-3 (VRF)
- Configuring VRF-Aware Routing Protocol
- Configuring DMVPN Tunnel Interface
- Configuring WAN Aggregation Router
- Configuring Firewall Interface
- Configuring Firewall Management Interface and Software Version
- Configuring Firewall Routes, Access-lists and NAT/pNAT
- Configuring Policy-based Features of Cisco IP Surveillance Cameras

Defining the VRF and Mapping Logical Interfaces

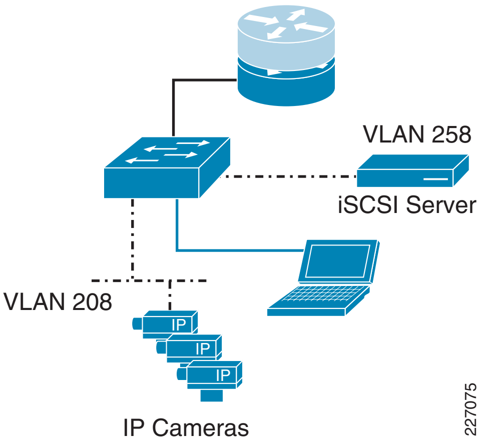
On the branch router, the VRF is defined and the logical interfaces of the AVG and the VMSS network module are associated with the VRF by the **ip vrf forwarding** interface command. The following is an example from one branch router, vpn4-3800-6:

```
hostname vpn4-3800-6
!
ip vrf IPVS
 rd 100:10
 route-target export 100:10
 route-target import 100:10
!
!
interface Video-Service-Engine1/0
 description EVM-IPVS-16A
 ip vrf forwarding IPVS
 ip address 192.0.2.37 255.255.255.252
 ip route-cache flow
 service-module ip address 192.0.2.38 255.255.255.252
 service-module ip default-gateway 192.0.2.37
 no keepalive
!
interface Integrated-Service-Engine2/0
 description NME-VMSS-HP16
 ip vrf forwarding IPVS
 ip address 192.0.2.33 255.255.255.252
 ip route-cache flow
 service-module external ip address 192.168.211.2 255.255.255.0
 service-module ip address 192.0.2.34 255.255.255.252
 service-module ip default-gateway 192.0.2.33
 no keepalive
!
```

Mapping Layer-2 (VLAN) to Layer-3 (VRF)

IP networks are comprised of both Layer-2 (switches) and Layer-3 (routers) devices. To provide for end-to-end segmentation, the VLANs and the VRF must be mapped together. An association between Layer-2 and Layer-3 must be established. Using the branch topology as an example, the IP cameras are attached to access ports in VLAN 208 with an IEEE 802.1Q trunk port connecting the switch and the ISR router. The IPVS iSCSI server is on VLAN 258. The end-user workstations are in the global routing table. The topology is shown in Figure 41.

Figure 41 *Mapping VLAN to VRF*



The following sample configuration shows the router sub-interface for VLAN 208 and 258. They are associated with the IPVS VRF.

```
vpn4-3800-6#
!
interface GigabitEthernet0/0.208
 description inside interface for ip cameras
 encapsulation dot1Q 208
 ip vrf forwarding IPVS
 ip address 192.0.2.49 255.255.255.240
!
interface GigabitEthernet0/0.258
 description iSCSI Management Subnet
 encapsulation dot1Q 258
 ip vrf forwarding IPVS
 ip address 192.168.211.1 255.255.255.0
!
```

From the switch configuration, the uplink port to the ISR router and the access port for the IP camera is shown. The port for the iSCSI server would be similarly configured as the camera, but in VLAN 258. The following is a sample configuration:

```
!
interface GigabitEthernet1/0/1
 description trunk to vpn4-3800-6
 switchport trunk encapsulation dot1q
 switchport mode trunk
 load-interval 60
 priority-queue out
 mls qos trust dscp
!
interface GigabitEthernet1/0/2
 description CIVS-IPC-2500
 switchport access vlan 208
 switchport mode access
end
```

The mapping of the VLAN to VRF is the responsibility of the supporting router, as the VLAN ID and the VRF name are associated with each other, because both references share the router sub-interface configuration.

Configuring VRF-Aware Routing Protocol

The branch router has interfaces in both the global routing table as well as the IPVS VRF and both network address spaces must be defined to the routing protocol. In the following example, EIGRP is the routing protocol used to illustrate the configuration.

```
!
router eigrp 65
 network 10.81.7.88 0.0.0.7
 network 192.168.15.0 0.0.0.63
 no auto-summary
 !
 address-family ipv4 vrf IPVS
  network 192.0.2.32 0.0.0.31
  network 192.168.15.128 0.0.0.127
  network 192.168.211.0
  no auto-summary
  autonomous-system 65
 exit-address-family
!
```

In the above sample configuration:

- Subnet 192.0.2.32/27 is for the AVG and VMSS network modules and IP cameras.
- Network 192.168.15.128/25 is for the DMVPN tunnels.
- Network 192.168.211.0/24 is for the iSCSI server at this branch.
- In the global routing table, 10.81.7.88/29 is for the end-user workstations and network 192.168.15.0/26 is for the WAN interfaces connecting this branch to the hub routers.

To display an instance of the virtual routing table associated with IPVS, the target VRF must be specified as shown in the following example:

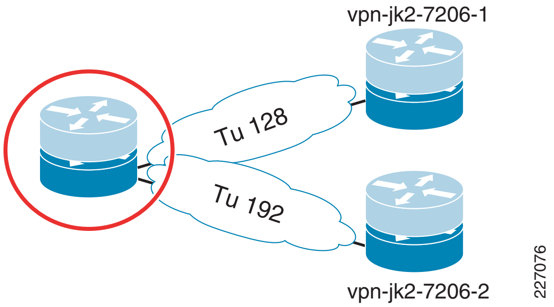
```
vpn4-3800-6#show ip eigrp vrf IPVS neighbors
IP-EIGRP neighbors for process 65
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
1   192.168.15.129          Tu128             14 01:17:47  134  5000  0  182
0   192.168.15.193          Tu192             10 01:17:47  132  5000  0  167
```

In the following section, the DMVPN tunnel interface configuration is shown for Tunnel 128. Tunnel 192 is configured similarly but not shown.

Configuring DMVPN Tunnel Interface

In this section, the configuration from one of the two tunnels of the branch router is shown (see Figure 42). The crypto topology deployed is a DMVPN dual-hub, dual-cloud implementation.

Figure 42 DMVPN Tunnel Interface Configuration



This branch router has a point-to-point Metro-Ethernet MAN link to the primary headend router, vpn-jk2-7206-1. This interface is in the global routing table and is VLAN 332 through the service provider network.

```
!
interface GigabitEthernet0/1.332
 encapsulation dot1Q 332
 ip address 192.168.15.46 255.255.255.252
!
```

The logical tunnel interface is in the IPVS VRF, the tunnel source is the above interface in the global routing table and the destination is Loopback 0 interface on vpn-jk2-7206-1, which is also in the global routing table.

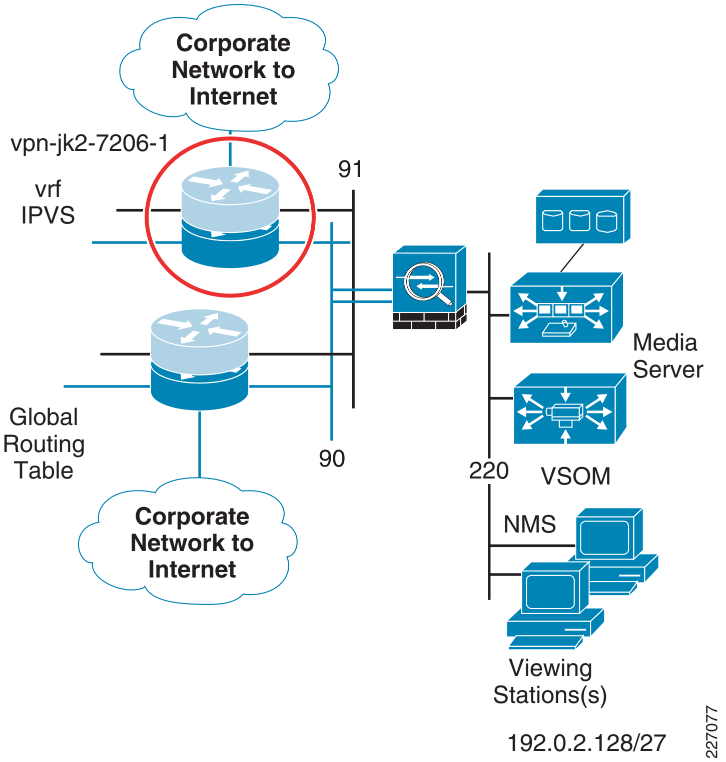
```
!
interface Tunnel128
 ip vrf forwarding IPVS
 ip address 192.168.15.130 255.255.255.192
 ip mtu 1400
 ip nhrp authentication FOO
 ip nhrp map 192.168.15.129 192.168.15.40
 ip nhrp map multicast 192.168.15.40
 ip nhrp network-id 128
 ip nhrp nhs 192.168.15.129
 ip summary-address eigrp 65 192.0.2.0 255.255.255.224 5
 tunnel source GigabitEthernet0/1.332
 tunnel destination 192.168.15.40
 tunnel key 128
 tunnel protection ipsec profile IPVS_Branches_ipsec_profile
!
ip route 192.168.15.40 255.255.255.255 192.168.15.45 name vpn-jk2-7206-1_Loopback_0
!
end
```

A static route to the tunnel destination is included so that this tunnel interface has an affinity to the physical interface; Tunnel 128 traffic is always transported over VLAN 332.

Configuring WAN Aggregation Router

This section examines the interfaces and topology of the WAN aggregation routers (see Figure 43). There are two WAN aggregation routers for high availability to the branch locations. Only one of these two similarly configured WAN aggregation router configuration is shown for the sake of brevity.

Figure 43 WAN Aggregation Router Configuration



The WAN aggregation router vpn-jk2-7206-1 has interfaces in both the global routing table and in the IPVS VRF. For clarity, the interfaces in the global routing table are shown in blue in the following sample configuration. The IPVS interfaces are shown in black text. The tunnel's logical interface is in the IPVS VRF while the tunnel source/destination IP addresses are in the global routing table.

```
vpn-jk2-7206-1#sh run b | beg interface Loopback0
interface Loopback0
 description Loopback for Global RT
 ip address 192.168.15.40 255.255.255.255
!
interface Tunnel128
 description DMVPN tunnel/cloud to Branches
 ip vrf forwarding IPVS
 ip address 192.168.15.129 255.255.255.192
 no ip redirects
 ip mtu 1400
 ip nhrp authentication FOO
 ip nhrp map multicast dynamic
 ip nhrp map multicast 192.168.15.40
 ip nhrp network-id 128
 ip nhrp nhs 192.168.15.129
 ip nhrp server-only
 ip route-cache flow
 no ip split-horizon eigrp 65
 ip summary-address eigrp 65 192.0.2.0 255.255.255.0 5
 tunnel source Loopback0
 tunnel mode gre multipoint
 tunnel key 128
 tunnel protection ipsec profile IPVS_Branches_ipsec_profile
!
interface Tunnel300
 description DMVPN Tunnel to Enterprise/Internet
 ip address 10.81.7.254 255.255.255.240
 ip mtu 1400
 ip pim sparse-mode
 ip nhrp authentication BAR
 ip nhrp map multicast dynamic
 ip nhrp map 10.81.7.241 64.102.223.24
 ip nhrp map multicast 64.102.223.24
 ip nhrp network-id 22341
 ip nhrp nhs 10.81.7.241
 ip route-cache flow
 load-interval 30
 tunnel source FastEthernet0/0
 tunnel destination 64.102.223.24
 tunnel key 300
 tunnel protection ipsec profile DMVPN_IPSEC_PROFILE
!
interface FastEthernet0/1.90
 description ASA DMZ Global
 encapsulation dot1Q 90
 ip address 10.81.7.161 255.255.255.248
 ip flow ingress
 standby 0 ip 10.81.7.166
 standby 0 preempt delay minimum 60
!
interface FastEthernet0/1.91
 description ASA DMZ vrf IPVS
 encapsulation dot1Q 91
 ip vrf forwarding IPVS
 ip address 192.168.15.97 255.255.255.248
 ip flow ingress
 standby 0 ip 192.168.15.102
 standby 0 preempt delay minimum 60
!
!
interface FastEthernet0/1.332
 description MAN/WAN to Site 130 (vpn1-2851-1)
 encapsulation dot1Q 332
 ip address 192.168.15.45 255.255.255.252
 ip flow ingress
!
interface FastEthernet0/1.340
 description MAN/WAN to Site 140 (vpn1-3845-1)
 encapsulation dot1Q 340
 ip address 192.168.15.13 255.255.255.252
 ip flow ingress
!
interface FastEthernet0/1.342
 description MAN/WAN to Site 140 (vpn1-3845-1)
 encapsulation dot1Q 342
 ip vrf forwarding IPVS
 ip address 192.168.15.77 255.255.255.252
 ip flow ingress
 ip summary-address eigrp 65 192.0.2.0 255.255.255.0 5
!
interface FastEthernet0/1.352
 description MAN/WAN to Site 150 (vpn4-3800-6)
 encapsulation dot1Q 352
 ip address 192.168.15.49 255.255.255.252
 ip flow ingress
!
end
```

The Cisco ASA 5510 firewall is connected to the two WAN aggregation routers and there are FastEthernet interfaces in both the global and IPVS VRF to the firewall. Two of the three branch routers in this topology are cryptography-enabled and have a single MAN link between the branch and each aggregation router. One branch, vpn1-3845-1 (Site 140), router demonstrates a branch without crypto on the MAN, and to implement path isolation, there are two physical links, one in the global routing table and one in the IPVS VRF.

Connectivity from this central command center location to the remainder of the corporate network and to the Internet is provided by way of Tunnel300 in the global routing table.

Configuring Firewall Interface

Referring to the topology in Figure 43 on page 6-98, the firewall interface configuration is shown below. The blue text highlights the interface description in the global routing table while the interfaces in black text are associated with the VRF IPVS.

```
!
interface Ethernet0/0
 description Campus_IPVS VLAN 220
 nameif Campus_IPVS
 security-level 70
 ip address 192.0.2.129 255.255.255.224
!
interface Ethernet0/1
 description DMZ_IPVS VLAN 91
 nameif DMZ_IPVS
 security-level 50
 ip address 192.168.15.99 255.255.255.248
!
interface Ethernet0/2
 description DMZ_Global VLAN 90
 nameif DMZ_Global
 security-level 10
 ip address 10.81.7.163 255.255.255.248
!
```

In this topology, the firewall is functioning as a policy-based network virtual device and there are no interface configuration commands that make the ASA 5510 VRF-aware. The interface named *Campus_IPVS* is attached to VLAN 220 on the campus switch. Access to this address space from the global routing table and branch locations in the IPVS VRF is policy-based. The firewall configuration controls the access between the three interfaces.

Configuring Firewall Management Interface and Software Version

A management interface is connected to the lab FlashNet network to facilitate software upgrades and out-of-band (OOB) management of the firewall. The management interface-related commands are shown below and will not be referenced in any subsequent sections of this chapter.

```
!
interface Management0/0
 description FlashNET
 speed 100
 duplex full
 nameif FlashNET
 security-level 0
 ip address 172.26.156.3 255.255.254.0
!
route FlashNET 172.26.0.0 255.255.254.0 172.26.156.1 1
!
```

```
access-group MANAGEMENT in interface FlashNET control-plane
access-list MANAGEMENT extended permit tcp 172.26.0.0 255.255.254.0 interface FlashNET

http server enable
http 172.26.156.0 255.255.254.0 FlashNET
snmp-server location ESE Lab
snmp-server contact foo.bar@cisco.com
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
telnet 172.26.156.0 255.255.254.0 FlashNET
telnet timeout 60
!
ssh 172.26.156.0 255.255.254.0 FlashNET
ssh timeout 60
console timeout 0
```

The software version used in testing is: as follows

```
vpn-jk2-asa5510-1# sh ver

Cisco Adaptive Security Appliance Software Version 8.0(4)
Device Manager Version 6.1(5)51

Compiled on Thu 07-Aug-08 20:53 by builders
System image file is "disk0:/asa804-k8.bin"
```

Configuring Firewall Routes, Access-lists and NAT/pNAT

The global routing table has the lowest security-level (ignoring the security-level 0 management interface, FlashNet) and this configuration is intended to deny access to the IPVS VRF from the outside. No access-lists are configured to permit inbound access. The branch locations are in the IPVS VRF which is at security-level of 50, lower than the security level of the command center at 70. For initiating access from a lower value security level to a higher value requires the definition of access-list.

The access-lists are configured on the firewall to permit the branch routers, switches, cameras and the iSCSI servers to send traffic to the network management server(s) located in the command center.

The following sample configuration assumes that syslog, snmptraps, NetFlow export (UDP port 7777) and any viewing stations at the branch (TCP to port 80 or WWWW) are permitted from the branch IPVS VRF to the command center.

```
!
access-list IPVS-CC extended permit udp any 192.0.2.128 255.255.255.224 eq syslog
access-list IPVS-CC extended permit udp any host 192.0.2.139 eq snmptrap
access-list IPVS-CC extended permit udp any host 192.0.2.139 eq 7777
access-list IPVS-CC extended permit tcp 192.0.2.0 255.255.255.0 any eq www
access-group IPVS-CC in interface DMZ_IPVS
!
```

For troubleshooting purposes, ICMP is also permitted. This can be disabled if specified by the security policy of the enterprise network.

```
icmp unreachable rate-limit 1 burst-size 1
icmp permit any Campus_IPVS
icmp permit any DMZ_IPVS
icmp permit any DMZ_Global
!
```

The two next-hop IP addresses in the following route statements are HSRP addresses configured on the WAN aggregation routers: 10.81.7.166 and 192.168.15.102. A default route is configured for the global routing table and routes to the IP addresses present in the IPVS VRF are shown.

```
route DMZ_Global 0.0.0.0 0.0.0.0 10.81.7.166 1
route DMZ_IPVS 192.0.2.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.11.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.111.0 255.255.255.0 192.168.15.102 1
route DMZ_IPVS 192.168.211.0 255.255.255.0 192.168.15.102 1
!
```

Tip In this example, the IP subnets for the iSCSI management networks are not allocated from contiguous address space. Had that been done, these three routes could have been consolidated into a single route, as is the case with the 192.0.2.0 network. Address allocation that allows summarization is an aid to reducing the size and complexity of configurations.

Lastly, the NAT/pNAT configuration implements the policy that the command center address space is port address translated (PAT) to the global interface IP address. No address or port translation takes place between the IPVS VRF address space at the branch locations and the command center.

```
global (DMZ_Global) 1 interface
nat (Campus_IPVS) 1 192.0.2.128 255.255.255.224
static (Campus_IPVS,DMZ_IPVS) 192.0.2.128 192.0.2.128 netmask 255.255.255.224
```

Configuring Policy-based Features of Cisco IP Surveillance Cameras

The Cisco 2500 Series IP cameras have several policy-based features that protect the camera resource from unauthorized access. There are three steps in initiating a video feed between the camera and the media server.

1. First, the authentication step, is initiated via HTTPS and as such the payload of this session is encrypted. The control plane negotiation, RTSP, and the video feed, RTP, are not secured by any payload encryption. The topology described in this section demonstrates how IPSec encryption can be implemented on the WAN to provide encryption and the resulting privacy of video feeds that leave the campus for live or archive viewing, or for archive backup.
2. The camera software includes access control, through userid and password, which is configured on both the camera configuration and the corresponding VSOM definition of the camera. Because the Cisco camera software allows only a single concurrent login, a unique account (userid) for the media server, when the camera is defined through VSOM, is recommended. This allows an administrator to be logged on the camera while the media server is starting or stopping video feeds. This aids in troubleshooting. The log files can be viewed in real-time without disrupting the command and control function of the media server.
3. The Cisco 2500 Series IP camera software, as many other vendor camera software does, provides an access control-list to permit or deny what IP addresses are authorized to attempt to access the camera. While implementations differ, one advantage of the Cisco implementation is the ability to define a range of IP address and either permit or deny access from that range. The addressing scheme deployed in this test topology uses 192.0.2.0/24 for branch and command center IPVS VRFs. The WAN interfaces and the iSCSI network address is in the 192.168.0.0/16 address space. Given this addressing scheme, a workstation in the command center in the 192.0.2.128/27 address space or the branch VMSS network modules at 192.0.2.2/32, 192.0.2.34/32 and 192.0.2.65/32, can access their respective cameras when all cameras are configured to:

   permit ip 192.0.2.0 255.255.255.0

   deny ip any

The advantage of selecting an address scheme that can be consolidated in this manner provides a simple configuration on all IP cameras in the network, yet provides a reasonable level of access control that does not require frequent updates.

Tip Both 192.0.2.0/24 and 192.168.0.0/16 are RFC3330 special use IPv4 addresses. 192.0.2.0/24 is assigned as *TEST-NET* and used in documentation and example code. 192.168.0.0/16 is used in private networks and is documented in RFC1918. Neither address block should appear, or be routed, on the public Internet.

Summary

This section addressed the need for implementing a logically separate IP network infrastructure to support an IP based video surveillance deployment in an existing enterprise network. Both control plane virtualization as well as policy-based techniques are deployed. IPSec encryption is also implemented to leverage the inherent path isolation of a logical tunnel as well as to make private the video feeds as they traverse the MAN/WAN. Access to resources outside the IPVS VRF must be initiated from hosts on the command center in order for the firewall to permit inbound packets. Because the IP addressing in use is based on addresses that are not routed on the public Internet, the firewall implements NAT/pNAT of these sessions from the IPVS VRF to the Internet or other enterprise address space.

In this next section, the configuration is enhanced to permit workstations external to the IPVS address space to view video feeds.

External Access to IPVS VRF

The goal of this section is to demonstrate a method of providing access to video feeds for viewing stations (PCs) that are in the global routing table, extranet, or even the Internet.

Topology Description

To accomplish this, a VPN concentrator, a Cisco VPN 3080, is deployed on the remaining unused interface on the Cisco ASA 5510 firewall. Client PCs connect to the VPN concentrator by installing the VPN 3000 client software from *www.cisco.com*. Access to the VPN concentrator is authenticated on a group name and key, as well as a userid and password. In these examples, the group/key and userid/password are stored locally on the VPN concentrator and can be administered by the command center security operations manager, or based on enterprise security policies, can be in an external database. The external authentication server database option improves scalability and manageability.

Because the VPN concentrator uses IPSec encryption, the video feeds that are leaving IPVS VRF through the command center VLAN are encrypted and hashed. In testing 3DES/HMAC-MD5 is used. To limit outside access to the VPN concentrator, the firewall is configured to permit inbound access to the outside interface of the VPN concentrator to only.

- UPD 500 (IKE)
- UDP 4500 (IKE/IPSEC with NAT-T)
- Protocol ESP (Protocol ‘50’)
- ICMP (for troubleshooting and verification of connectivity)

This firewall configuration, therefore, rejects all other packets that are not required for transporting the IKE/IPSec tunnels and ICMP (ping). This, in addition to deploying a group/key and userid/password to authenticate the end-users, is a commonly deployed best practice.

Alternatives to the VPN Concentrator

Cisco announced the end-of-sale and end-of-life dates for the Cisco® VPN 3000 Series Concentrators. The product becomes obsolete August 4, 2012. See the *EOL/EOS for the VPN 3000 Series Concentrators* document on www.cisco.com.

An alternative to the VPN concentrator is a remote access solution based on Secure Sockets Layer Virtual Private Network (SSL VPN). SSL VPN clients can be terminated on a Cisco ASA 5500 Series device or on a Cisco modular ISR routers (1800, 2800, 3800) with the appropriate SSL VPN hardware acceleration.

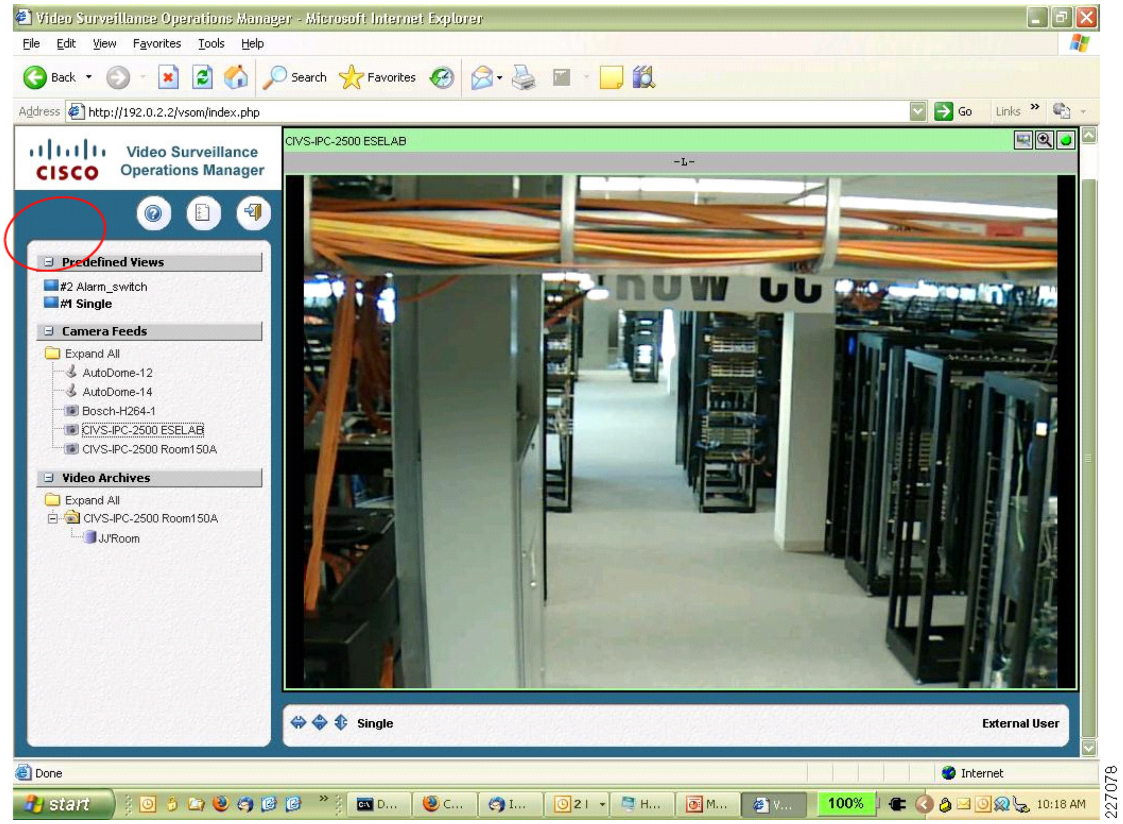
As a best practice, terminate the VPN concentration function on a device separate from the firewall. In other words, an ISR router or ASA device could be substituted for the VPN 3000 Series concentrator shown.

Limiting Authority in VSOM

Once the remote PC has connected and authenticated to the VPN Concentrator, the user has access to devices in the IPVS VRF. In the previous section, the policy-based features of the IP surveillance cameras are implemented to limit access to a configured address space within the IPVS VRF. The VPN concentrator is configured with an address pool that is not included in the IP camera access-list, which means users connecting through the VPN concentrator are not permitted direct access to the web server on the camera.

For remote users to view the live or archive video feeds, they must connect to the appropriate Video Surveillance Operations Manager (VSOM)/Media Server Web Server using a supported browser. To gain access to the video feeds, a userid and password must be entered. It is recommended that users are provided only the privileges necessary for their job function. In this case, the remote user only requires operator privileges, and as such a user account is configured accordingly. When a user with only operator privileges is logged on VSOM, no admin icon exists on the screen; the user may view live or archived video, but no configuration changes are permitted. A sample operator screen is shown in Figure 44.

Figure 44 Sample VSOM Operator Screen



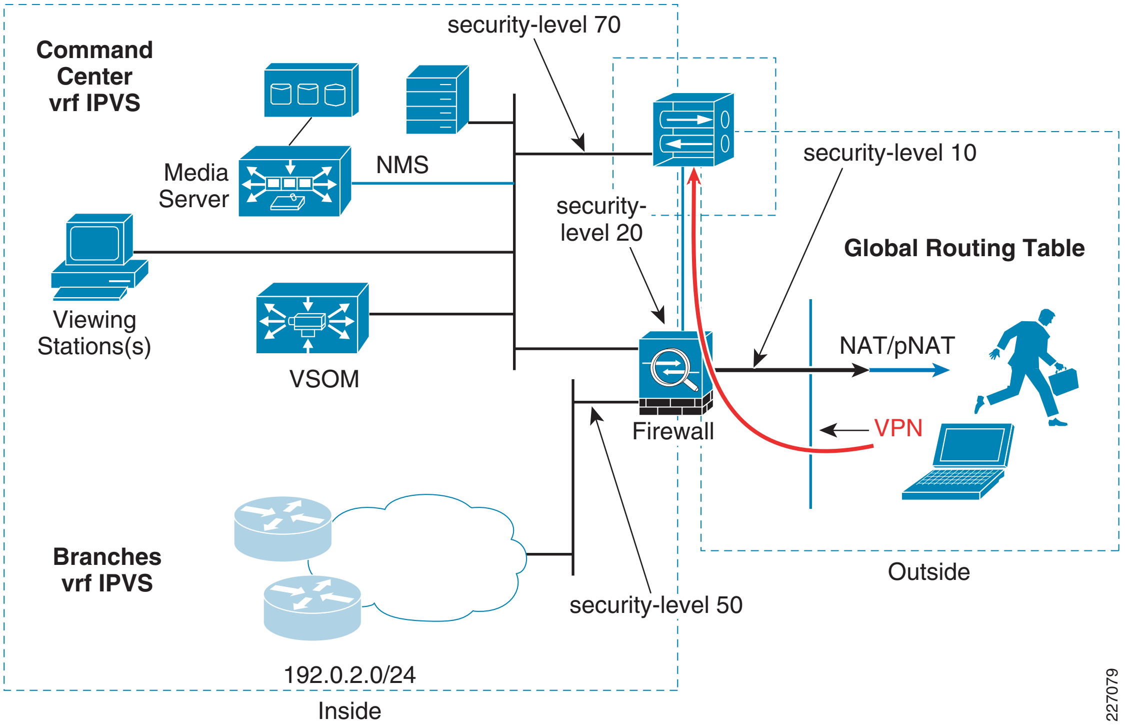
Other than the obvious differences associated with available bandwidth to the remote user, there is no difference in the presentation of the video feed for a remote user connected through the VPN concentrator versus a PC attached to the LAN in the command center.

Topology Diagram

The VPN concentrator consists of a public and private interface configuration. The public, or outside, interface is attached to the remaining unused interface on the ASA5510. The private (or inside) interface is attached to the LAN switch on VLAN 220, the command center VLAN. The security level of the ASA interface connecting to the VPN concentrator is 20. Because this value is numerically higher than the firewall outside interface with security-level 10, access-control lists are created on the firewall to allow the port numbers and protocols permitted to reach the VPN concentrator.

Figure 45 illustrates where in the topology the VPN concentrator is located.

Figure 45 Virtualization Topology with VPN Concentrator



The revised interface configuration of the ASA 5510 and the IP addressing for the VPN concentrator is shown in the following subsections.

Implementation Overview

To show how the VPN concentrator is deployed in the topology, the following configuration steps are implemented or updated from the previous sections.

- Configuring VPN Concentrator Interface and Address
- Configuring Firewall Interface
- Configuring WAN Aggregation Routing
- Configuring Firewall NAT/pNAT and Routing
- Configuring Firewall Access-lists
- Configuring VPN Concentrator User/Group/Proposals

Configuring VPN Concentrator Interface and Address

The public VPN concentrator interface is on a point-to-point network to the firewall. The VPN concentrator is at 10.81.7.57 and the firewall is at 10.81.7.58. The public interface in the global routing table is highlighted in blue. The management interface on FlashNET is shown, but is optional.

```
vpn2-3080-1: Config -> 1

This table shows current IP addresses.

  Intf         Status       IP Address/Subnet Mask          MAC Address
-------------------------------------------------------------------------------
```

```
Ether1-Pri|      UP      |    192.0.2.136/255.255.255.224| 00.03.A0.88.3F.58
Ether2-Pub|      UP      |     10.81.7.57/255.255.255.252| 00.03.A0.88.3F.59
Ether3-Ext|      UP      |  172.26.157.15/255.255.254.0  | 00.03.A0.88.3F.5A
```

The remote clients are allocated an IP address from the configured pool. This assigned address is used to identify the remote PC inside the IPSec tunnel interface. The address pool list used in this configuration is five IP addresses from the 192.168.15.64/29 subnet. If more concurrent remote sessions are required, a larger IP address pool must be allocated. Allocate as a large a pool as required, but not more than necessary.

```
vpn2-3080-1: Address -> 2

  This is the Address Pool List

   Start Addr         End Addr         Subnet Mask
------------------------------------------------------
 192.168. 15. 65 | 192.168. 15. 70 | 255.255.255.248 |
------------------------------------------------------
```

The IP routing configuration on the VPN concentrator is straight forward. A default route is configured to the firewall IP address and a network route is configured to 192.0.2.0/24. As discussed in the previous sections, note the iSCSI devices and the WAN interfaces in the IPVS VRF are allocated from the 192.168.0.0/16 address space; therefore, with this configuration, the remote users can only reach IP hosts on the 192.0.2.0/24 subnet: the VSOM and Media Servers. The IP cameras are on the 192.0.2.0/24 subnet, but access-control lists prevent any connectivity from source IP address in the address pool 192.168.15.64/29.

```
vpn2-3080-1: Routing -> 1

Static Routes
-------------
Destination     Mask            Metric Destination
------------------------------------------------------------
0.0.0.0         0.0.0.0              8 10.81.7.58
172.26.0.0      255.255.0.0          1 172.26.156.1
192.0.2.0       255.255.255.0        8 192.0.2.129
```

Note The 172.26.0.0 network is lab FlashNet for management of the device.

Configuring Firewall Interface

The previously unused interface Ethernet 0/3 is now deployed as the point-to-point interface to the VPN concentrator. All other interfaces are the same as discussed in the previous sections. The interfaces in the global routing table are highlighted in blue.

```
vpn-jk2-asa5510-1# show run
: Saved
:
ASA Version 8.0(4)
!
hostname vpn-jk2-asa5510-1
domain-name ese.cisco.com
enable password [removed] encrypted
passwd [removed] encrypted
names
dns-guard
!
interface Ethernet0/0
 description Campus_IPVS VLAN 220
 nameif Campus_IPVS
 security-level 70
 ip address 192.0.2.129 255.255.255.224
!
interface Ethernet0/1
 description DMZ_IPVS VLAN 91
 nameif DMZ_IPVS
 security-level 50
 ip address 192.168.15.99 255.255.255.248
!
interface Ethernet0/2
 description DMZ_Global VLAN 90
 nameif DMZ_Global
 security-level 10
 ip address 10.81.7.163 255.255.255.248
!
interface Ethernet0/3
 description DMZ for VPN3080
 nameif DMZ_VPN3080
 security-level 20
 ip address 10.81.7.58 255.255.255.252
!
```

There is no NAT/pNAT address translation between Ethernet 0/2 and Ethernet 0/3. The WAN aggregation routers must have a route to the VPN concentrator IP address, 10.81.7.57.

Configuring WAN Aggregation Routing

The WAN aggregation routers needs to be configured to include the two additional IP networks which are required to support the VPN concentrator. These networks are the public interface and the IP address pool for the remote client workstations. In this sample topology, these networks are

- 10.81.7.56/30 —Public subnet
- 192.168.15.64/29—IP address pool

Because the WAN routers are not exchanging routing updates from the firewall and VPN concentrator, a static route for the public subnet must be added to the global routing table and redistributed to the dynamic routing protocol to update the global routing tables.

```
ip route 10.81.7.56 255.255.255.252 10.81.7.163 name ASA5510
```

The second route is included in the IPVS VRF, and is also redistributed to the dynamic routing protocol to inform the branch routers of this route.

```
ip route vrf IPVS 192.168.15.64 255.255.255.248 192.168.15.99 name VPN3080_pool
!
```

The remainder of the WAN aggregation routers configuration addresses defining these two networks in the appropriate prefix-list and route-map and then redistributing these networks under the appropriate autonomous system (AS) number and VRF.

```
ip prefix-list ASA5510_VPN3080 seq 5 permit 10.81.7.56/30
!
route-map ASA5510_VPN3080 permit 10
 match ip address prefix-list ASA5510_VPN3080
!
ip prefix-list COMMAND_CENTER seq 100 permit 192.0.2.128/25
ip prefix-list COMMAND_CENTER seq 101 permit 10.81.7.0/24
ip prefix-list COMMAND_CENTER seq 102 permit 192.168.15.64/29
!
route-map COMMAND_CENTER permit 10
 match ip address prefix-list COMMAND_CENTER
 set tag 2128
!
router eigrp 64
 redistribute static metric 1000 100 255 1 1500 route-map ASA5510_VPN3080
 redistribute eigrp 65 metric 1000 100 255 1 1500 route-map Branch_Networks
 passive-interface FastEthernet0/1.90
 network 10.0.0.0
 no auto-summary
 eigrp stub connected redistributed
!
router eigrp 65
 redistribute eigrp 64 metric 1000 100 255 1 1500 route-map DEFAULT
 network 192.168.15.0 0.0.0.63
 no auto-summary
 !
 address-family ipv4 vrf IPVS
  redistribute static metric 1000 10 255 1 1500 route-map COMMAND_CENTER
  network 192.168.15.64 0.0.0.63
  network 192.168.15.128 0.0.0.63
  distribute-list route-map Branch_Net_vrf_IPVS_RT in
  no auto-summary
  autonomous-system 65
 exit-address-family
!
```

Note EIGRP AS 64 is used to connect to the enterprise address space. EIGRP AS 65 is used to connect to the branch networks for both the global routing table and the IPVS VRF.

Configuring Firewall NAT/pNAT and Routing

The NAT/pNAT configuration on the firewall is changed by adding two static entries to the configuration deployed in the previous section. The first static entry for 192.168.15.56/30 defines that no address translation occurs between the outside global routing table and the point-to-point network address between the firewall and the concentrator.

The second static entry, for 192.168.15.64, defines that no address translation occurs for the IP address pool defined in the VPN concentrator for remote users and the IPVS VRF.

```
global (DMZ_Global) 1 interface
nat (Campus_IPVS) 1 192.0.2.128 255.255.255.224
!
static (DMZ_VPN3080,DMZ_Global) 192.168.15.56 192.168.15.56 netmask 255.255.255.252
static (Campus_IPVS,DMZ_IPVS) 192.0.2.128 192.0.2.128 netmask 255.255.255.224
static (Campus_IPVS,DMZ_IPVS) 192.168.15.64 192.168.15.64 netmask 255.255.255.248
!
```

A route in the firewall for the concentrator address pools is required. All other routes are the same as from the previous section.

```
route Campus_IPVS 192.168.15.64 255.255.255.248 192.0.2.136 1
!
```

Configuring Firewall Access-lists

In addition to the access-list and group IPVS-CC, documented in the previous section, with the addition of the VPN concentrator, access-lists permitting the protocols and ports needed for the encryption protocols are added to the firewall configuration. Protocol ESP, UDP 500 and 4500, and ICMP are permitted. This allows the remote VPN client to contact the concentrator.

```
access-group INBOUND in interface DMZ_Global
access-list INBOUND extended permit esp any host 10.81.7.57
access-list INBOUND extended permit udp any host 10.81.7.57 eq isakmp
access-list INBOUND extended permit udp any host 10.81.7.57 eq 4500
access-list INBOUND extended permit icmp any host 10.81.7.57

icmp permit any DMZ_VPN3080
!
```

The VPN concentrator is at IP address 10.81.7.57.

Configuring VPN Concentrator User/Group/Proposals

It is recommended to use an external database server for authentication in large deployments. A complete VPN concentrator configuration is outside the scope of this document, however, configuration notes for the miscellaneous configuration for the user, group, and IKE proposals are shown below.

```
vpn2-3080-1: User Management -> 2

                              Current User Groups
-------------------------------------------------------------------------------
| 1. foo (Internal)                    |                                      |
-------------------------------------------------------------------------------

vpn2-3080-1: User Management -> 3

Internal groups are configured on the VPN 3000 Concentrator's Internal Database.
ESP-3DES-MD5 with IKE Keepalive - Tunnel Type is Remote Access - Authentication Internal
IPSec UDP (allow NAT-T)

                                   Current Users
-------------------------------------------------------------------------------
| 1. aprilmay                          |                                      |
-------------------------------------------------------------------------------

User(s) arein group 'foo', IPSEC and WebVPN are selected as the tunneling protocol with a
30 minute idle timeout, Simultaneous Logins (5000)  ESP-3DES-MD5 and store password
on client is permitted (when using the software client, authenticating user is prompted by
the VPN software client on the PC)

vpn2-3080-1: IKE Proposals -> 1

                           The Active IKE Proposals
-------------------------------------------------------------------------------
| 1. IKE-3DES-MD5                      | 2. IKE-3DES-SHA                      |
-------------------------------------------------------------------------------
```

In testing the userid of **aprilmay**, the configured password is entered when prompted for this information by the Cisco VPN client. The group name **foo** and group key are configured in the client software along with the destination IP address of the concentrator, 10.81.7.57 and IPSec/UDP is defined as the transport.

Summary

This section addresses the need to provide secure, authenticated, network access from the enterprise network and the public Internet to the video surveillance VRF for real-time viewing of surveillance feeds. One method of accomplishing this is through the use of a VPN concentrator that can be accessed by appropriately configured workstations. This technique extends access to the segemented and logically isolated video surveillance deployment from any location with sufficient bandwidth to view the video feed.

References

The concepts in this chapter are intended to be focused on a targeted deployment for implementing IP video surveillance at the branch and central command center campus with controlled access from the enterprise network. For additional deployment information and a more thorough discussion of these concepts, refer to the following documents:

- *Network Virtualization—Path Isolation Design Guide Network Virtualization 3.0 - CVD*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/Network_Virtualization/PathIsol.html

- *Ethernet Access for Next Gen Metro and Wide Area Networks*

  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/Ethernet_Access_for_NG_MAN_WAN_V3.1_external.html

- Other relevant Cisco Validated Design (CVD) design guides, refer to the following URL:

  www.cisco.com/go/designzone