



Cisco Unified Wireless Network Solution: VideoStream Deployment Guide

[Cisco Unified Wireless Network Solution: VideoStream Deployment Guide](#) 2

[Introduction](#) 2

[Theory of Operation](#) 3

[Concepts](#) 9

[Cell Planning](#) 11

[Configuration](#) 15

[Conclusion](#) 39

[Related Documents](#) 40

Revised: July 22, 2015,

Cisco Unified Wireless Network Solution: VideoStream Deployment Guide

Introduction

Cisco Unified Wireless Network (CUWN) introduces a new feature, VideoStream, for enterprise wide deployments. This feature enables the wireless architecture to deploy multicast video streaming across the enterprise to wireless clients. This feature recompenses the drawbacks that degrade the video delivery as the streams and clients scale in an enterprise network. VideoStream makes video multicast to wireless clients more reliable and uses the bandwidth/spectrum more efficiently. In a multi-streaming enterprise network, the feature assigns priority to the stream and provides more weightage to preferred streams. This feature also guarantees delivery of video to wireless clients and denies video to new client subscription under heavy channel utilization.

Requirements

Knowledge of Cisco Unified Wireless LAN Solution.

Components Used

VideoStream feature is available in Cisco Unified Wireless Network software version 8.1 with enhancements in Cisco Unified Wireless Network software version 8.1. This feature is supported on all wireless LAN controllers (WLANs) and newer generation indoor access points (APs). This feature is not available on autonomous access points and outdoor access points.

Related Products

Supported Wireless Hardware and Software

VideoStream is supported on all wireless LAN controllers. This includes the Cisco 5500 controller (Cisco 5508 and 5520 wireless controllers), Cisco 8500 series wireless controllers (8510 and 8540 wireless controllers), Cisco Flex 7500 series wireless controllers, Cisco 4400 controller, Cisco 2100 controller and WiSMs. VideoStream is also supported on the Cisco 2504 standalone and Cisco WiSM-2 controller. IGMPv2 is the supported version on all of the controllers.

VideoStream is supported on all access points. This includes all 802.11n and 802.11ac models of access points consisting of Cisco Aironet 3700 series access point, Cisco Aironet 3600 series access point, Cisco Aironet 3500 series access point, Cisco Aironet 2700 series access point, Cisco Aironet 2600 series access point, Cisco Aironet 1700 series access point, Cisco Aironet 1260 series access point, Cisco Aironet 1250 series access points, Cisco Aironet 1140 series access points, and Cisco Aironet 1040 series access points. VideoStream is also supported on Cisco Aironet 1240AG* series access points and Cisco Aironet 1130AG* series access points.

The VideoStream feature was introduced in the CUWN 7.0 version of controller code and continued its support on later versions of controller software with enhancements.

Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

Theory of Operation

Before going into details about the VideoStream feature, some of the shortfalls in Wi-Fi multicast needs to be understood. 802.11n and 802.11ac are prominently discussed wireless technologies for indoor wireless deployments. Equally prominent requirement is seen in multimedia service on an enterprise wireless network, in particular, video. Multicast video streaming is a cost effective solution in a huge enterprise network as unicast of video services does not scale in an enterprise wide streaming. Multicast does not provide any MAC layer recovery on multicast/broadcast frames. Multicast and broadcast packets do not have an Acknowledgment (ACK), and all packet delivery is best effort. Multicast over wireless with 802.11a/b/g/n does not provide any mechanism for reliable transmission.

Enterprise wireless deployments are prone to interference, high channel utilization, incompatible client, and low SNR at the edge of the cell. Video delivery to wireless clients is at the highest mandatory data rates on the respective channel. Also, many clients share the same channel but have different channel conditions, power limitations, and client processing capabilities. Therefore, multicast is not a reliable transmission protocol to all the clients in the same channel as each client has different channel conditions.

Wireless multicast does not prioritize the video traffic even though it is a Differentiated Service Code Point (DSCP) marked by the video server. The application has loss of packets with no ACK, and the retries to the delivery is bad. To provide reliable transmissions of multicast packet, it is necessary that the network classifies queues and provisions by means of Quality of Service (QoS). This virtually removes the issue of unreliability by eliminating drop packets and delay of the packets to the host by marking the packets and sorting them to the appropriate queue.

Even though the 802.11n and 802.11ac adaptation has gained momentum both with the network and clients, wireless multicast has not been able to use the 802.11n data rates. This has also been one of the factors for an alternate mechanism for wireless multicast propagation.

Legacy Multicast

The implementation of multicast has evolved over releases on CUWN. Prior to CUWN 7.0 code, the multicast performance was optimized and an efficient way to deliver multicast traffic from the controller to the access point was introduced.

In this process, a multicast group is configured on the controller to register the access points and deliver multicast packet. This implementation dropped the process of the controller using unicast to deliver multicast packets to each access point over a Lightweight Access Point Protocol (LWAPP) tunnel. In this configuration, the underlying network components are used by the controller to replicate and deliver multicast packet to the access point. The controller becomes the multicast source for the configured LWAPP/CAPWAP group and the access points are the multicast receivers. The access point accepts Internet Group Management Protocol (IGMP) queries from the upstream router and multicast packets with a source IP address of the associated controller. This enhances the multicast performance considerably. The IGMP query is sent to its members and clients, thus keeping the database updated.

IGMP snooping configuration introduced a better multicast delivery of packets. The queries from an upstream multicast router/neighbor are replied with a IGMP report based on the group configuration on the controller. A unique multicast group ID (MGIDs) is created by the controller from the IGMP reports after checking the L3 multicast addresses and the VLAN number, and updates an IGMP report to the upstream L3 switch or neighbor. The controller sends the reports with the source address as the interface address on which the reports are received from the clients. A MGID table is created or updated on the access point with the client MAC addresses.

When the controller receives a multicast join reply for a particular group, it forwards to all the access points in the group. However, only those access points that have active clients subscribed to that multicast group send multicast traffic. The multicast traffic flows to the client at the highest mandatory data rate as seen in the capture. The client is associated to the access point at 802.11n rate on a 5 GHz radio.

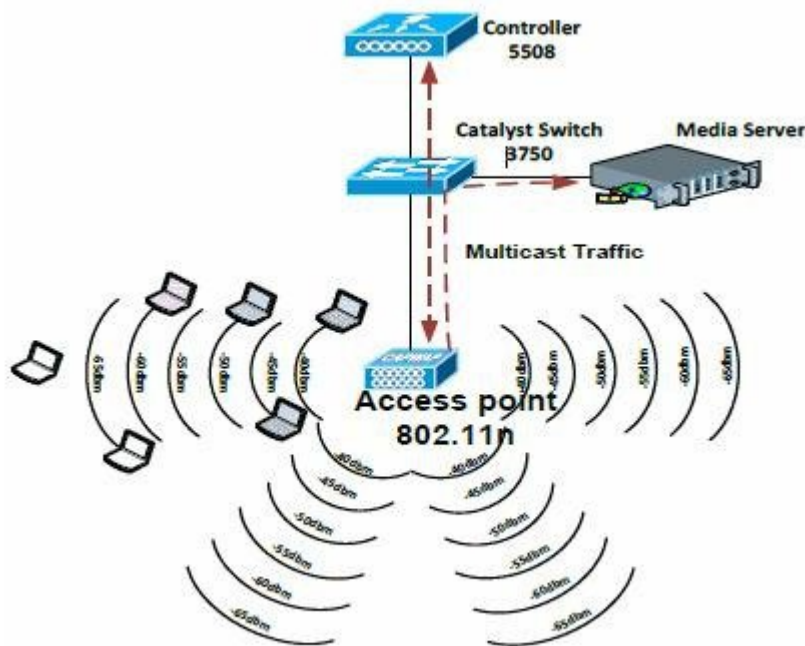
Packet Number:	4066
Flags:	0x0000000
Status:	0x0000005 Encrypted
Packet Length:	1396
Timestamp:	11:17:11.079789000 06/21/2010
Data Rate:	48 24.0 Mbps
Channel:	140 5745MHz 702.11a 20MHz
802.11a Flags:	40000000000000000000000000000000
Signal Level:	100%
Signal dBm:	-44
Noise level:	20%
Noise dBm:	-76
802.11 MAC Header	
Version:	0 [0 Mask 0x03]
Type:	410 Data [0 Mask 0x0C]
Subtype:	40000 Data Only [0 Mask 0xF0]
Frame Control Flags:	401100010 [1]
	0... Non-strict order
	..1.. Protected Frame
	...1.. More Data
	...0... Power Management - active mode
0... This is not a Re-Transmission
0... Last or Unfragmented Frame
0... Exit from the Distribution System
0... Not to the Distribution System
Duration:	0 Microseconds [2-3]
Destination:	01:00:58:40:01:96 Mcast IP IANA702:40:01:96 [4-5]
SSID:	00:22:BD:D1:71:3E Cisco-D1:71:3E [10-13]

VideoStream

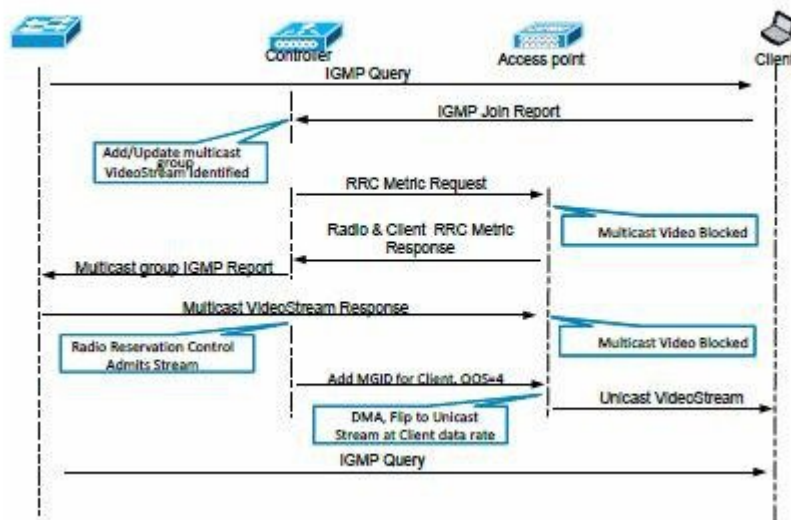
VideoStream provides efficient bandwidth utilization by removing the need to broadcast multicast packets to all WLANs on the AP regardless of a client connected to a multicast group. To address this limitation, the AP must be able to send multicast traffic to the host via Unicast forwarding, only on the WLAN that the client has joined and do so at the data rate the client has joined. Before VideoStream is configured, you must understand how it differs from the normal Multicast deployment (Multicast / Broadcast).

VideoStream, for the first time in a wireless system, provides a seamless approach for engineers to design and implement a multicast solution without destroying the bandwidth between the controller and the upstream switch or router.

Cisco VideoStream technology is a new system with a wide set of features of the Cisco Unified Wireless Network that incorporates some of the key enhancements to deliver superior video quality. Cisco VideoStream showcases Cisco's RF and video expertise for delivering a reliable, consistent platform for different types of video. This takes the physical, MAC, and application layers of the wireless LAN into consideration. The following sections highlight some of the VideoStream features and how the features uniquely enhance the delivery of video over Wi-Fi and the quality of the end user experience. A simple network diagram for VideoStream is shown below to explain the concepts that are introduced.



The following process flow for VideoStream helps you in understanding the next few sections of the feature description. The process flow also introduces the modules such as Stream Admission, Stream Prioritization, Radio Reservation Control, Multicast-to-unicast, and AutoQoS.



VideoStream can be enabled globally on the controller. The feature can be enabled at the radio level (2.4 GHz and 5 GHz) and at the WLAN or SSID level, and provides more control to the administrator to identify specific video streams for preferential quality-of-service treatment.

Stream Admission and Prioritization

As previously mentioned, while video is an efficient, high-impact means of communication, it is also a very bandwidth intensive. However, not all video content is prioritized the same. From earlier discussion, it is clear that organizations investing in video cannot afford to have network bandwidth consumed without any prioritization of business-critical media.

Stream admission will empower the network administrator to have control over all the multicast video streaming in the network. Stream admission will facilitate network administrator to use pre-defined templates for input multicast streams. There are few predefined templates for stream bandwidths of 300 Kbps, 500 Kbps, 1 Mbps, 3 Mbps, and 5 Mbps. Network administrators with less experience of video can use the pre-defined templates.

```
<Cisco_Controller> >show media-stream group detail Stream-Less300Kbps
```

```
Media Stream Name.....Stream-Less300Kbps
Start IP Address.....239.1.2.3
End IP Address.....239.1.2.3
  RRC Parameters
  Avg Packet Size(Bytes).....1200
  Expected Bandwidth(Kbps).....300
  Policy.....Admit
  RRC re-evaluation.....periodic
  QoS.....Video
  Status.....Multicast-direct
  Usage Priority.....1
  Violation.....drop
```

```
<Cisco_Controller> >show media-stream group detail Stream-Less300Kbps
```

```
Media Stream Name.....Stream-Less300Kbps
Start IP Address.....239.1.2.3
End IP Address.....239.1.2.3
  RRC Parameters
  Avg Packet Size(Bytes).....1200
  Expected Bandwidth(Kbps).....300
  Policy.....Admit
  RRC re-evaluation.....periodic
  QoS.....Video
  Status.....Multicast-direct
  Usage Priority.....5
  Violation.....drop
```

```
<Cisco_Controller> >
```

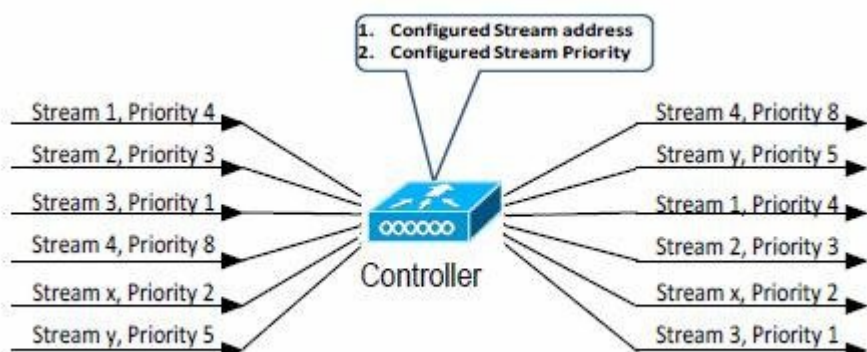
```
<Cisco_Controller> >show media-stream group detail Stream-Less5Mbps
```

```
Media Stream Name.....Stream-Less5Mbps
Start IP Address.....239.1.2.8
End IP Address.....239.1.2.8
  RRC Parameters
  Avg Packet Size(Bytes).....1200
  Expected Bandwidth(Kbps).....5000
  Policy.....Admit
  RRC re-evaluation.....periodic
  QoS.....Video
  Status.....Multicast-direct
  Usage Priority.....3
  Violation.....drop
```

```
<Cisco_Controller> >
```

You must have a basic understanding of streaming video characteristic before configuring. For example, consider the above two configurations. If the video bit rate is around 4 Mbps, you need to manually add the configurations instead of using any of the above two templates. If Stream-Less3Mbps is used, the quality of video will be bad due to missing video frames. It is observed that there is pixelation of video and constant freeze of video on a wireless client. If Stream-Less5Mbps is used, the number of video clients will be less as every wireless client is guaranteed of 5 Mbps while the video bit rate is only 4 M bits. If you had ten wireless clients, the aggregate client bandwidth should be around 40 Mbps. Using the Stream-Less5Mbps, the controller will be using 50 Mbps, hence depriving three wireless clients of video.

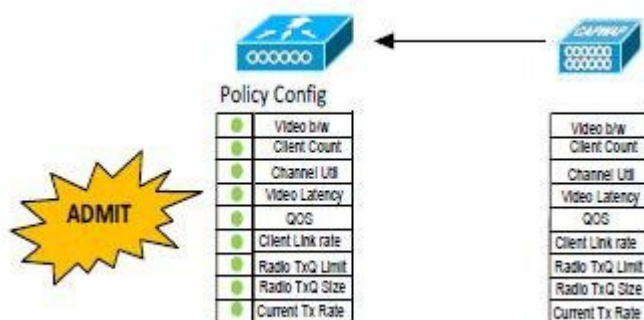
Stream Priority can configure the media stream with different priority based on importance within the enterprise network. RRC Priority takes effect only when there is a congestion or contention in the wireless access point.



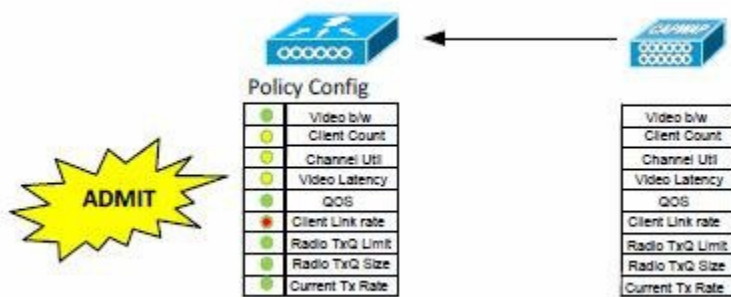
When there is a congestion and there are too many video multicast streams and clients, stream 4 takes precedence over the rest of the configured streams. The configured video stream will have lower priority than voice, and higher priority than best effort traffic. All the other multicast traffic will be admitted as best effort traffic even though they are marked for QoS for Video priority.

Resource Reservation Control

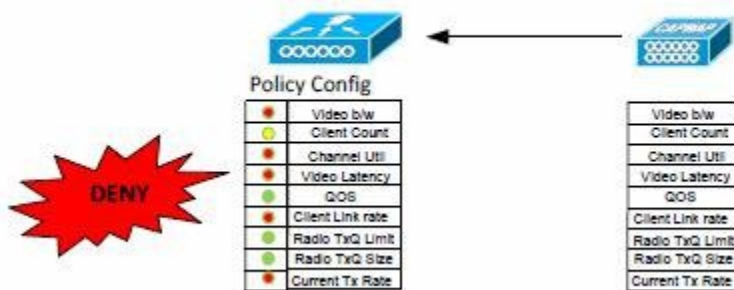
As more and more users begin to use video in the workplace on Wi-Fi endpoints, the ability to manage and scale a continuous, and high-quality experience for fluctuating groups of users at any given time or location is critical. The controller and access points have a crucial decision making algorithm, that is Resource Reservation Control (RRC), which provides enhanced capabilities to manage admission and policy controls. Admission and policy decisions are made based on the radio resource measurements, statistics measurement of the traffic, and system configurations. The controller initiates RRC requests to the access points for the IGMP join. The access point processes the request for all the parameters listed in the following diagram.



In the above response, all the parameters passed the policy configuration on the controller. The IGMP join request from the client on that access point will be admitted. If the RRC request has a response as shown in the following diagram, the join request will be investigated and the RRC algorithm will be checked for the policy configuration again. The client will be admitted, but as a best effort client. However, on several attempts of RRC check, it will be admitted with a better QoS priority.



RRC is initiated on a client at IGMP join to a stream and can be configured for periodic check. Due to any changes in the wireless characteristic, if the RRC metric reply varies considerably, the client will be denied to the stream.



RRC provides bandwidth protection for the video client by denying requests that would cause over-subscription. Channel utilization is used as a metric to determine the capacity and perform admission control. Integration with Voice CAC guarantees video quality and voice priority.

Multicast to Unicast

By enabling 802.11n data rates and providing packet error correction, multicast-to-unicast capabilities of Cisco VideoStream enhance the reliability of delivering streaming video over Wi-Fi beyond best-effort features of traditional wireless networks.

A wireless client application subscribes to an IP multicast stream by sending an IGMP join message. With reliable multicast, this request is snooped by the infrastructure, which collects data from the IGMP messages. The system checks the stream subscription and configuration, and then collects metrics and traffic policies for the requested stream. If the requested stream is allowed by the policies, a response is sent to the wireless client attached to the access point to initiate reliable multicast once the stream arrives. The system also looks for available bandwidth and configured stream metrics to determine if there is enough airtime to support the new subscription. In addition, the system considers the prevailing load on the radio and the health of the media before making the admission decision. After all the above criteria are met, a join response is sent to the access point. This is when the access point replicates the multicast frame and converts it to 802.11 unicast frames. Finally, a reliable multicast service delivers the video stream as unicast directly to the client.

Higher Video Scaling on Clients

Increase in the number of clients accessing video over Wi-Fi will place an increased pressure and demand on the network. This impacts both performance and quality. Higher video scaling is a measure of the number of clients supported per controller while optimizing the traffic flow from the wired to wireless network. With Cisco VideoStream technology, all of the replication is done at the edge (on the access point), thus utilizing the overall network efficiently.

At any point in time, there is only the configured media stream traversing the network, because the video stream is converted to unicast at the access points based on the IGMP requests initiated by the clients. Some other vendor implementations do a similar conversion of multicast to unicast, but does it inefficiently as evidenced by the load put on the wired network to support the stream.

Theoretically, in a non-802.11n network with both 2.4 GHz and 5 GHz clients associated, there can be as many as three or four clients watching a 5M bit video stream. With any additional video clients, the channel utilization will be maxed out and the possibility of the clients dropping or losing connectivity is higher.

With 802.11n network, the scalability of clients increases significantly due to the availability of bandwidth. The client scalability of clients with or without channel bonding also varies in the 802.11n network. This is non-existent in a legacy/non 802.11n network.

Concepts

At this time, you should have an understanding on the infrastructure functionality when VideoStream is configured. It is also important to understand how the video applications, client devices, and so on contribute for a better synergy for the system to work. It is observed in all wireless installation applications that clients have an equal role to play for a end-to-end delivery.

Applications

There are various video applications available today for streaming video over IP network. The video streaming source is common across wired and wireless networks. The controller is in the core or the distribution of the wired network in the path as the last reporter for multicast network. Some of the video applications that have been tested with VideoStream are discussed in the following sections.

- Cisco Media Experience Engine
- Cisco Content Delivery Application
- Windows Media Server/services
- VBrick – H.264 Appliance
- Video Furnace
- Video Furnace
- VLC Player

Cisco Media Experience Engine

The Cisco Media Experience Engine (MXE) 3500 is an easily deployed appliance that integrates transparently into the network to deliver a rich set of media-processing capabilities. Designed as a core component of the Cisco Media-Ready Network, the Cisco MXE 3500 provides:

- Comprehensive live and video on demand (VoD)-based transcoding services that allows you to share video content across your network to virtually any type of endpoint.
- Innovative post production features that transform ordinary video content into stunning studio-quality output.
- Cutting-edge speech-to-text transcription services.
- Innovative collaboration with other applications delivered by the Cisco suite of media products.

The result is a powerful media-processing platform that allows IT administrators to significantly streamline operating costs associated with live media streaming, media production, and distribution.

Cisco Content Delivery Application

Cisco Content Delivery Applications are the software elements of the CDS and implement content processes on top of Cisco Content Delivery Engines, which provides functions such as ingest, storage, caching, personalization, and streaming. TV streaming delivery applications include:

- Cisco Vault Application
- Cisco TV Streamer Application
- Cisco TV Playout Application
- Cisco Integrated Streamer-Vault Application
- Cisco Content Delivery System Manager

Internet streaming content delivery applications include:

- Cisco Internet Streamer Application
- Cisco Content Acquirer Application
- Cisco Service Router Application
- Cisco Content Delivery System Manager

The Cisco content delivery system comprises one or more networked Cisco content delivery engines, each optimized for one or more tasks such as content ingest, storage, caching, or streaming.

Windows Media Server

Windows Media Server streams digital audio and video content to clients over the Internet or an intranet. These clients can be either computers or devices that play back the content using a player, such as Windows Media Player. The clients can also be other computers that are running Windows Media services (called Windows Media servers) that proxy, cache, or redistribute the content.

The content that your Windows Media server streams to clients can be a live stream or a pre-recorded digital media file. Wireless companies that deliver wireless broadband entertainment services by using scalable and reliable Windows Media servers use media servers:

- Internet broadcasters that deliver content for radio, television, cable, or satellite.
- Film and music distributors that distribute audio and video content in a secure manner without excessive buffering or network congestion.
- IPTV professionals that deliver a high-quality IPTV experience on local area networks (LANs).

VideoFurnace

Haivision's Furnace provides a secure, easy to use, simple to deploy end-to-end system for encoding and distributing live video to computers and set top boxes, for creating scheduled playback channels for enterprise TV and signage, and also for recording content and delivering video on demand.

The Furnace provides a complete IP video solution. The viewing experience to access live and recorded channels as well as on demand content is provided for the desktop through the "zero footprint" InStream player and to fixed monitors and displays through the Stingray set top box. With fine grain control of all viewers and displays, the Furnace is the ideal system for managing and distributing

enterprise video securely, for establishing HD signage throughout a facility, for providing on-demand material, and for capturing, organizing, and reviewing events.

End-to-End H.264, the Furnace provides seamless end-to-end capabilities. The Furnace Portal Server controls the direct and secure distribution of SD and HD H.264 video and MPEG-1, MPEG-2, MPEG-4 SD video to both the InStream player and the Stingray set top box. The Furnace Playback Manager supports scheduled channels for both live and prerecorded IP video broadcasts and digital signage. The Furnace Media Server enables video-on-demand. Leveraging the efficiencies of H.264 video compression, high definition media is available to all users. Also, the Furnace incorporates direct support for Haivision's revolutionary Barracuda and Makito H.264 encoders delivering live SD and HD content at bit rates from 150 kbps to 15 Mbps.

Cell Planning

Cell planning is a key aspect that needs to be considered for a video or voice deployment. Cell planning is not as simple as mounting an access point in an appropriate location and providing wireless connectivity. This has changed over the last few years as pervasive wireless coverage has become a requirement. There are several tools available today to perform a proper cell planning. Cisco Wireless Control System has a Planner tool that is very effective.

Besides normal wireless planning criteria, there are a few more parameters that need to be considered in the cell planning for video. These are the latency, jitter, and packet loss. These parameters are highlighted in the following table and also categorized with field realistic values. From the table, you can see that cell planning is very effective.

	Latency	Jitter	Throughput	Packet Loss
Video Teleconferencing	High	High	Low	Medium
HD Video Teleconferencing	High	High	High	High
Video on Demand	Low	Low	Medium	Low
Live Streaming Video	Medium	Medium	Medium	High

To quantify the video application in terms of values, the following table is widely acknowledged for video applications.

Metric	Video Collaboration	Digital Signage	TelePresence	Video Surveillance
Latency (secs)	150	200	150	300
Jitter	30	10	10	10
Packet Loss (%)	1%	.05%	.05%	.05%

Consider a Cisco CAPWAP access point installed with the latest version of code in a clean test environment with no interference in an office environment. When the client association rate, signal strength, and noise are measured at various points, the data looks as in the following tables. The measurements in the tables are captured with channel bonding and without channel bonding. Observe the signal strength and the noise in all test scenarios. This will give you a basic understanding of the variation of signal and noise. The planning guidelines are not based on the two considered values, but also take into consideration the co-channel interference, client data rates, client transmit power, and total channel capacity. These will be planning considerations when the access point density and client count increase.

Table 1: 5 GHz with Channel Bonding

Distance from Access Point (ft)	Client Association Rate (Mbps)	Signal Strength (-dbm)	Noise (-dbm)
5	276	42	72
20	250	44	75
40	243	47	77
80	216	59	89
100	198	64	90

Table 2: 5 GHz without Channel Bonding

Distance from Access Point (ft)	Client Association Rate (Mbps)	Signal Strength (-dbm)	Noise (-dbm)
5	144	41	71
20	144	51	79
40	130	55	81
80	108	60	90
100	87	77	93

Table 3: 2.4 GHz Radio without Channel Bonding

Distance from Access Point (ft)	Client Association Rate (Mbps)	Signal Strength (-dbm)	Noise (-dbm)
5	144	30	61
20	144	32	62
40	121	49	77
80	108	53	80
100	84	56	88

The Call Admission Control (CAC) configuration stops the over-subscription of the channel and guarantees configured media bandwidth. The CAC configuration will also stop new media users, hence safe-guards the current users from being affected when oversubscribed.

The CAC configurations for VideoStream is a key tuning point that balances the voice, video and data users on a wireless media using Cisco Unified Wireless Network 8.1. This configuration is radio specific and can be enabled on both 2.4 GHz and 5 GHz radios. The CAC configuration can be enabled by clicking **WIRELESS > 802.11a/n or 802.11b/g/n > Media**.

MONITOR WLANs CONTROLLER WIRELESS SECURITY

802.11a(5 GHz) > Media

Voice Video **Media**

General

Unicast Video Redirect ☒

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%)) 85

Client Minimum Phy Rate 6000

Maximum Retry Percent (0-100%) 80

Media Stream - Multicast Direct Parameters

Multicast Direct Enable ☒

Multicast Direct Max Number of Streams auto

Best Effort QoS Admission ☐ Enabled

By default, both the Voice and Video CAC settings are disabled. Any configurations that are made here will directly apply to the voice and video configurations. In short, Media = Voice + Video. This is by default configured to a maximum of 85% of the total radio bandwidth. The remaining 15% of the radio bandwidth is best effort traffic (data). Depending on the usage of data, voice, and video, it is recommended to change these values. The media settings can be changed by clicking the **Media** tab. It is recommended to maintain default values until there is an absolute necessity to change these values.

The voice and video settings can be tuned based on the type of network services provided. If voice is the prime application in the network, then the CAC values can range from 5% to 85%. There is also a reserved roaming bandwidth that is included in the voice and video configuration. With a maximum CAC setting of 85% on a 5 GHz radio, the wireless system can accommodate about 21 voice calls. Similarly, on a 2.4 GHz radio with a maximum CAC setting of 85%, the system can accommodate about 13 voice calls.

Similarly, if you switch to a video CAC, with a max of 85%, the wireless system can accommodate about 22 clients on a 5 GHz radio. With a maximum CAC setting of 85% on a 2.4 GHz radio, the wireless system can accommodate 10 clients. The following table gives an idea on how the systems behaves under different configurations. These values are with channel bonding on the 5 GHz radio and a video bit rate configuration of 3M bits.

Video CAC Value	Video Clients	Voice Call	Voice CAC Value
85	22	0	0
65	15	6	20
45	10	11	40
25	5	16	60
5	2	20	80



Note These test results are documented for CUWN 7.2 after the improvement of aggregation, buffering, and smart scheduling of video packets to client.

Video CAC Value	Voice CAC Value	Video Bit Rate	Clients
85	0	1.5 ~2M	51
85	0	5M	30
85	0	10M	20



Note All the clients in test are similar in configuration with a 3X3 802.11a/b/g/n wireless adapter. The test environment is clear from all wireless interferences and also non-Wi-Fi interferers.

The radios are capable of handling 255 associations. Because the wireless media is shared in half-duplex media, there will be contention by the clients. As clients move further away from the radio, the throughput decreases. Further down the edge of the cell, the client data rates drops to the lowest, and hence introduced too many retries. Even though the radio can allow a higher number of associations, it is recommended to limit the clients to less than 60 per access point for normal data applications. However, when you have voice and video services on the access point, it is recommended to plan the access point layout such that client adapter signal strength does not fall below -60db or equivalent client association rate. Also, consider providing a 15 ~ 20% cell overlapping to ensure there is a smooth handoff of the video application from one access point to another when the clients are roaming.

Quality of Service

Normally, all video hosting sources ensure that the DSCP marking is appropriately marked on the wired side. If the video server is located locally and does not have to traverse to any router boundaries, DSCP marked packets are guaranteed to be the same. Sometimes, when the video packets are traversing routed boundaries, the DSCP markings tend to be reset. CUWN ensures that video packets

have the correct DSCP marking on the wireless side. This can be observed on the access point as the video queue counters will be incrementing. If there is no video traffic and only best-effort traffic exists, the respective counters will increment. All of the discussed operation will be effective only if the video profile on the controller is mapped to 802.1p protocol with a tagged value of 5.

[MONITOR](#)
[WLANs](#)
[CONTROLLER](#)
[WIRELESS](#)
[SECURITY](#)

Edit QoS Profile

QoS Profile Name

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Wired QoS Protocol

Protocol Type

802.1p Tag

Foot Notes

*1. Override Bandwidth Contracts parameters are specific to per Radio of AP.
The value zero (0) indicates the feature is disabled*

Configuration

VideoStream can be deployed on an existing enterprise wide wired and wireless network. The overall implementation and maintenance costs of a video over wireless network are greatly reduced. The assumption is that the wired network is multicast enabled. To verify that a distribution or access switch is part of the layer 3 network, connect a client machine to the switch port and verify if the client machine is able to join a multicast feed.

Show run | include multicast will display if multicast is enabled on the layer 3 switch. If not enabled for multicast, you can enable multicast by adding the following command on the switch.

```
Switch14-1#
Switch14-1#sh run : include multicast
```

```
ip multicast-routing distributed
Switch4-1#
Switch4-1(config)#
Switch4-1(config)#ip multicast-routing distributed
Switch4-1(config)#
Switch4-1(config)#
```

Depending on the type of Protocol Independent Routing (PIM) configuration on the wired network, the layer 3 switch is configured for either PIM Sparse mode or PIM dense mode. There is also a hybrid mode, however, PIM sparse-dense mode is widely used.

```
interface Vlan111
 ip address 172.20.227.97 255.255.255.254
 ip pim sparse-dense-mode
end
```

Show ip igmp interfaces displays the SVI interfaces that are participating in the IGMP membership. This command also shows the version of IGMP configured on the switch or the router. The IGMP activity on the interface can also be verified in the form of joins and leaves by the clients.

```
Switch4-1#
Switch4-1#sh ip igmp interface vlan111
Vlan111 is up, line protocol is up
 Internet address is 172.20.227.97/27
 IGMP is enabled on interface
 Current IGMP host version is 2
 Current IGMP router version is 2
 IGMP query interval is 60 seconds
 IGMP configured query interval is 60 seconds
 IGMP querier timeout is 120 seconds
 IGMP configured querier timeout is 120 seconds
 IGMP max query response time is 10 seconds
 Last member query count is 2
 Last member query response interval is 1000 ms
 Inbound IGMP access group is not set
 IGMP activity: 3 joins, 0 leaves
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 172.20.227.97 (this system)
 IGMP querying router is 172.20.227.97 (this system)
 Multicast groups joined by this system (number of users):
   224.0.1.40(1)
Switch4-1#
```

The above configuration can be verified by running the **show ip mroute** command on the layer 3 switch.

```
Switch4-1#sh ip mroute
IP Multicast Routing Table
Flags: D — Dense, S — Sparse, B — Bidir Group, s — SSM Group, C — Connected,
       L — Local, P — Pruned, R — RP-bit set, F — Register flag,
       T — SPT-bit set, J — Join SPT, M — MSDP created entry, E — Extranet,
       X — Proxy Join Timer Running, A — Candidate for MSDP Advertisement,
       U — URD, I — Received Source Specific Host Report,
       Z — Multicast Tunnel, z — MDT-data group sender,
       Y — Joined MDT-data group, y — Sending to MDT-data group,
       V — RD & Vector, v — Vector
Outgoing interface flags: H — Hardware switched, A — Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode
(*, 239.100.1.2), 00:22:48/stopped, RP 0.0.0.0, flags: DC
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan10, Forward/Sparse—Dense, 00:21:56/stopped
(172.20.227.112, 239.100.1.2), 00:22:48/00:02:39, flags: T
 Incoming interface: Vlan111, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan10, Forward/Sparse—Dense, 00:21:56/stopped
(*, 224.0.1.40), 00:22:54/00:02:11, RP 0.0.0.0, flags: DCL
 Incoming interface: Null, RPF nbr 0.0.0.0
 Outgoing interface list:
   Vlan111, Forward/Sparse—Dense, 00:22:54/stopped
```

The above data has certain entries that need to be looked in to. The special notation is Source (S) and Group (G), where "S" is the source IP address of the multicast server and "G" is the Multicast Group Address that a client has requested to join. If the network has many sources, you will see in your routers (S, G) for each of the source IP addresses and Multicast Group addresses. This data also has information of the outgoing and incoming interfaces.

Supported Wireless Hardware and Software

VideoStream is supported on all wireless LAN controllers. This includes the Cisco 8500 controller, Cisco 5500 controller, Cisco 4400 controller, Cisco 2100 controller and WiSMs. VideoStream is also supported on the Cisco 2504 standalone and Cisco WiSM-2 controller. IGMPv2 is the supported version on all of the controllers.

VideoStream is supported on all newer access points. This includes models of Cisco Aironet 3700 series access point, Cisco Aironet 3600 series access point, Cisco Aironet 3500 series access point, Cisco Aironet 2700 series access point, Cisco Aironet 2600 series access point, Cisco Aironet 1700 series access point, Cisco Aironet 1260 series access point, Cisco Aironet 1250 series access points, Cisco Aironet 1240AG series access points, Cisco Aironet 1140 series access points, Cisco Aironet 1130AG series access points, and Cisco Aironet 1040 series access points.

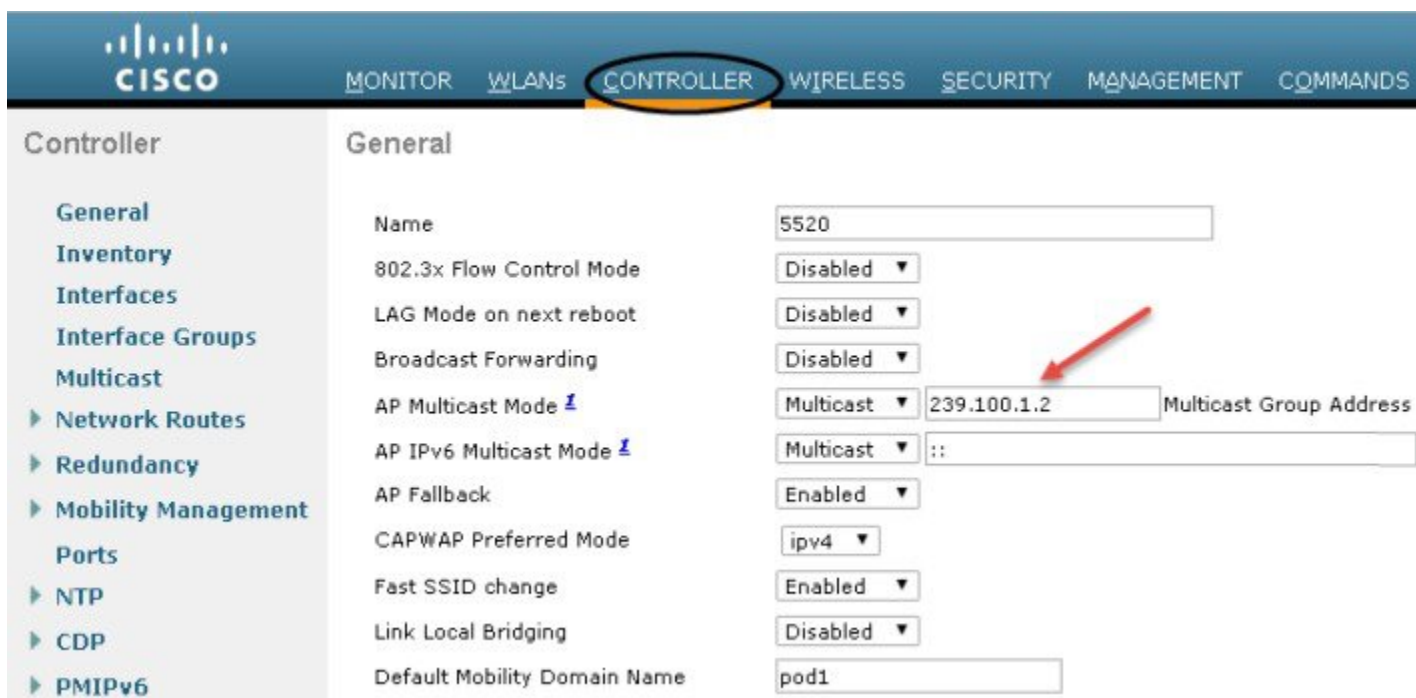
The VideoStream feature is introduced in the CUWN 7.0 version of controller code and is supported on later versions of controller software.

Controller Configuration

VideoStream feature requires multicast enabled on the controller. Multicast on the controller can be enabled in two modes: multicast-unicast and multicast-multicast. When IP multicast is enabled, the controller delivers multicast packets to wireless LAN clients by making copies of the multicast packets, then forwarding the packets through a unicast Lightweight Access Point Protocol tunnel to each access point connected to the controller. Unicast delivery places a heavy burden on the AP, as well as the controller's network processing unit, due to the deluge of packets that need to be replicated down to the access points.

Cisco Multicast-Unicast delivery method is commonly used by customers who only want to provide multicast over their wireless network, or the network does not support multicast. It is recommended for customers to avoid using the Multicast-Unicast method of delivery. This method is processor intensive depending on the number of multicast streams to be supported. In this mode, every multicast packet must be replicated to all access points that have joined the controller regardless of a client requesting the multicast group address.

The multicast performance has been optimized with the introduction of Multicast-Multicast mode. Instead of using unicast to deliver each multicast packet over the CAPWAP tunnel to each access point, a CAPWAP multicast group is configured to deliver the multicast packet. This allows the routers in the network to use standard multicast techniques to replicate and deliver multicast packets to the access points. For the CAPWAP multicast group, the controller becomes the multicast source and the access points become the multicast receivers. The multicast performance is enhanced as the access points accept IGMP queries only from the router and multicast packets with a source IP address of the controller with which they are currently associated.



The screenshot shows the Cisco Controller configuration page. The 'CONTROLLER' tab is selected and highlighted with a yellow circle. In the left sidebar, the 'Multicast' option is selected. The 'General' configuration section is displayed, showing various settings. A red arrow points to the 'Multicast Group Address' field, which contains the value '239.100.1.2'.

Configuration Item	Value
Name	5520
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast
AP IPv6 Multicast Mode	Multicast
AP Failback	Enabled
CAPWAP Preferred Mode	ipv4
Fast SSID change	Enabled
Link Local Bridging	Disabled
Default Mobility Domain Name	pod1
Multicast Group Address	239.100.1.2



Note IP multicast uses the Class D range of IP addresses 224.0.0.0 through 239.255.255.255. The reserved ranges of address, Link Local Multicast address (224.0.0.0 through 224.0.0.255) are for use by protocols and cannot be used. The rest of the Class D address, Administratively Scoped multicast address (239.0.0.0 through 239.255.255.255) can be used for configuring the IP networks for multicast.

The above configuration can also be configured using command lines in a couple of steps.

```
<Cisco_Controller> >
<Cisco_Controller> >config network multicast global enable
<Cisco_Controller> >config network multicast mode multicast 239.100.1.2
<Cisco_Controller> >
```



Note It is recommended to use one unique multicast address/controller.

One more important configuration on the controller is to enable IGMP snooping. Enabling of IGMP snooping on the controller helps to collect IGMP reports from the hosts and sends each AP a list of hosts that are listening to any multicast group. The AP then forwards multicast packets only to those hosts.

IGMP timeout and IGMP Query interval help the IGMP snooping to be more effective. When the IGMP timeout expires, the controller sends a query on all SSIDs causing the clients that are listening to the multicast group to send a packet back to the controller. IGMP query interval is based on how often the controller sends a query to all SSIDs. If the IGMP timeout is set to 60 seconds and the IGMP query interval is configured to 20, there will be three queries.

Controller

- General
- Inventory
- Interfaces
- Interface Groups
- Multicast
- Network Routes
- Redundancy
- Mobility Management
- Ports
- NTP
- CDP
- PMIPv6
- Tunneling
- IPv6
- mDNS
- Advanced

Multicast

Enable Global Multicast Mode	<input checked="" type="checkbox"/>
Enable IGMP Snooping	<input checked="" type="checkbox"/>
IGMP Timeout (30-7200 seconds)	60
IGMP Query Interval (15-2400 seconds)	20
Enable MLD Snooping	<input type="checkbox"/>
MLD Timeout (30-7200 seconds)	60
MLD Query Interval (15-2400 seconds)	20

```

<Cisco_Controller> >
<Cisco_Controller> >config network multicast igmp snooping enable
Cisco_Controller> >config network multicast igmp timeout 60
<Cisco_Controller> >config network multicast igmp query interval 20
<Cisco_Controller> >

```

Enabling VideoStream – Global

The VideoStream feature can be enabled in three different places depending on the implementation of the feature. This helps network administrators to control enabling VideoStream feature on the controller.

The feature must be enabled globally on the controller by checking the **Multicast Direct feature** check box under **Wireless > Media Stream > General**. Enabling this feature will populate some of the configuration parameters on the controller for VideoStream. The VideoStream feature can also be enabled under the PHY type. The customer has the flexibility to enable VideoStream only on 5 GHz radio or 2.4 GHz radio or both.

The **Multicast Direct** button under **WLAN > QoS** appears on if the feature is enabled globally. This gives the flexibility to enable VideoStream feature per SSID.

Wireless

- Access Points
 - All APs
 - Radios
 - 802.11a/n/ac
 - 802.11b/g/n
 - Dual-Band Radios
 - Global Configuration
- Advanced
 - Mesh
 - ATF
 - RF Profiles
 - FlexConnect Groups
 - FlexConnect ACLs
 - FlexConnect VLAN
 - Templates
 - OEAP ACLs
 - Network Lists
 - 802.11a/n/ac
 - 802.11b/g/n
 - Media Stream
 - General**
 - Streams

Media Stream > General

Multicast Direct feature ☒ Enabled

Session Message Config

Session announcement State ☐ Enabled

Session announcement URL

Session announcement Email

Session announcement Phone

Session announcement Note

```
<Cisco_Controller> >
<Cisco_Controller> >config media-stream multicast-direct enable
```

WARNING: Media Stream Multicast-direct requires Load based CAC to run,
Voice deployment employing Static CAC needs to convert to Load Based CAC.

```
<Cisco_Controller> >
```

Adding Multicast Stream Configuration

The multicast feeds can be enabled to take part in RRC only if the multicast feed is configured on the controller. To add a multicast stream to the controller, click **Streams** under **MediaStream**.

As mentioned, the administrator must be aware of the video characteristic streaming through a controller. A true balance must be drawn when the stream configurations are added. For example, if the stream bit rate varies between 1200 kbps and 1500 kbps, then the stream must be configured for a bandwidth of 1500 kbps. If the stream is configured for 3000 kbps, you will have lesser video client serviced by the access point. Similarly, configuring for 1000 kbps will cause pixelization, bad audio, and bad user experience.

There are a few pre-configured templates on the stream configuration that can be used. It is necessary to apply the similar judgment when selecting them. Some of the configurations are already captured in the [Stream Admission and Prioritization](#) section. If you are not using the templates, there are a few more configurations that can be used to enhance the user experience. The average packet size

can be changed to match the streaming video. Resource reservation control can be enabled for periodic update so that the systems can check for health periodically. This can also be disabled to enable RRC to run only at admission. The priority of the stream can be also set to a high value for prioritization of the stream. A configured value of 8 will allow the stream to be prioritized and not bumping down to best effort.

On any violation of the previous policies, the stream can be downgraded to best-effort or can be dropped. It is recommended to downgrade to best-effort.

The screenshot shows the Cisco Wireless configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS (highlighted), and SECURITY. The left sidebar shows the configuration tree with 'Media Stream' selected under the 'Streams' category. The main content area is titled 'Media Stream > Edit' and displays the following configuration details:

Stream Name	test1.5K
Multicast Destination Start IP Address	239.4.5.6
Multicast Destination End IP Address	239.4.5.6
Maximum Expected Bandwidth (1 to 35000 Kbps)	1500 (Kbps)

Below the configuration details is the 'Resource Reservation Control(RRC) Parameters' section:

Average Packet Size (100-1500 bytes)	1200 (bytes)
RRC Periodic update	<input checked="" type="checkbox"/>
RRC Priority	1
Violation	best-effort ▼
Policy	admit ▼

```
<Cisco_Controller> >
Cisco_Controller> >config media-stream add multicast-direct test1.5K 239.4.5.6 detail 1500 1200
periodic video 1 fallback
```

```
<Cisco_Controller> >
```

The multicast destination start IP address and end IP address can be the same address. One can also configure a range of multicast address on the controller. There is no limitation on the number of multicast addresses entries or the number of stream entries. The start IP address can be 239.4.5.1 and the end IP address can be 239.4.5.254.

VideoStream configurations can be enabled on both the radios on the access points. The configurations on the radio can be configured or modified only with the radios disabled. Some configurations will also require the WLANs / SSID to be disabled.



Note It is recommended to make all configuration required on the radios when disabled.

Enabling VideoStream – 802.11 a/n Radio

To enable VideoStream, perform these steps:

Procedure

- Step 1** Click **WIRELESS > 802.11 a/n > Media > Media** to enable the VideoStream and add CAC/QOS configurations. Similar configurations might be required on the 802.11 b/g/n radio, depending on the type of service provided on the radio.
- Step 2** Check the **Multicast Direct Enable** check box to enable VideoStream (By default, VideoStream is disabled on the radios).
- Step 3** Configure the maximum number of streams allowed per radio and maximum number of streams allowed per client from the **Max Streams per Radio** and **Max Streams per Client** drop-down list respectively. These values can range from 1 to 20. If you choose **No-limit**, there is no limit set for the number of client subscriptions.

802.11a Global Parameters	
General	
802.11a Network Status	<input checked="" type="checkbox"/> Enabled
Beacon Period (millisecs)	100
Fragmentation Threshold (bytes)	2346
DTPC Support	<input checked="" type="checkbox"/> Enabled
Maximum Allowed Clients	200
RSSI Low Check	<input checked="" type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	-80
802.11a Band Status	
Low Band	Enabled
Mid Band	Enabled
High Band	Enabled



The **Unicast Video Redirect** is enabled by default. This will allow unicast video traffic flow to wireless clients.

RRC will admit clients to join a stream after pass criteria is achieved. The admitted clients will have a QoS priority of 4. The clients who do not pass the RRC criteria will be dropped and will not be allowed to join the stream. However, this can be overruled by enabling the **Best Effort QoS Admission**. Now, all wireless clients requested to join a stream will be admitted to the multicast stream, but some of them will have a QoS priority of 0. The media bandwidth is currently set to 85% by default.

Media bandwidth is the sum of Voice and Video traffic on a radio interface. The lowest that a client can drop on the radio is 6000 kbps to join a streaming video. If there are clients that need to be restricted from joining a stream below a certain PHY rate, this value can be changed. The value is 6000 by default. The maximum retry percent is, by default, set to 80%. The system keeps track of the retries on the radio. If the retries are greater than the configured value the client will not be allowed to join the stream.

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY

FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates

OEAP ACLs

Network Lists

▼ **802.11a/n/ac**
Network
▼ RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n/ac)
CleanAir

▼ **802.11b/g/n**
Network
▼ RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
High Throughput (802.11n)
CleanAir

▼ **Media Stream**
General
Streams

► **Application Visibility And Control**

Lync Server

802.11b(2.4 GHz) > Media

Voice Video Media

General

Unicast Video Redirect ☒

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))

Client Minimum Phy Rate [i](#)

Maximum Retry Percent (0-100%)

Media Stream - Multicast Direct Parameters

Multicast Direct Enable ☒

Max Streams per Radio

Max Streams per Client

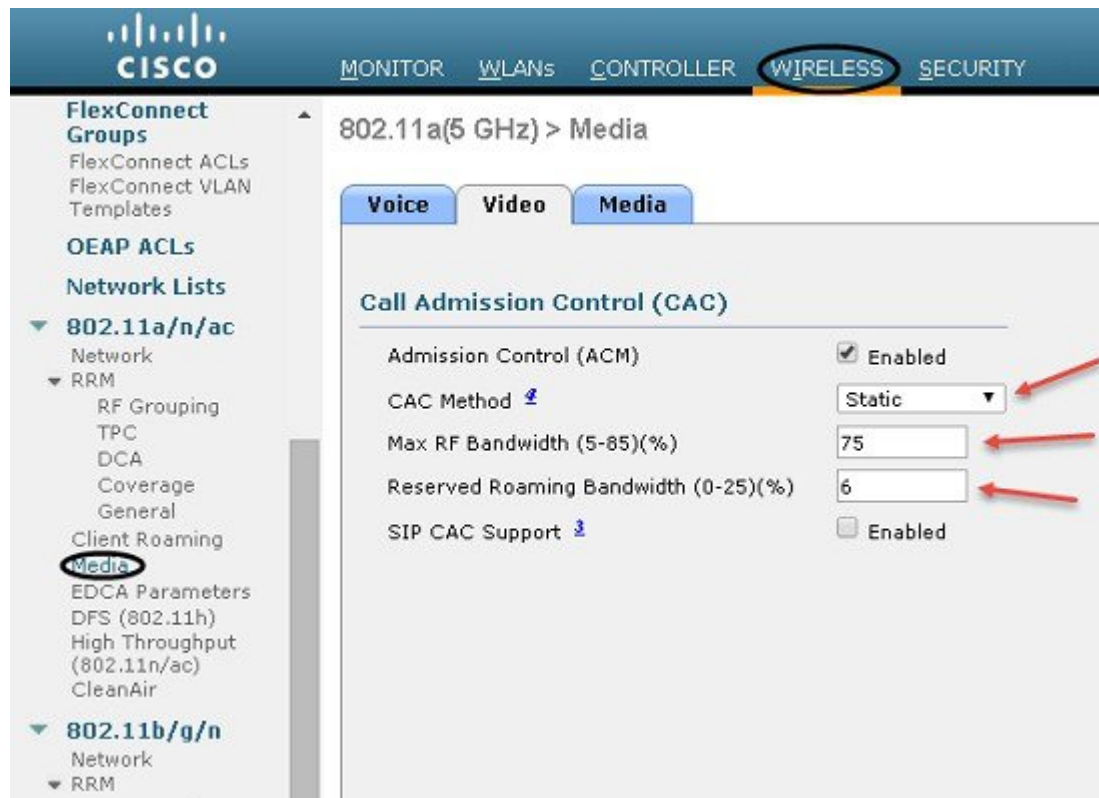
Best Effort QoS Admission ☒

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19

Note It is recommended to keep the default values.

Step 4 Click **WIRELESS > 802.11 a/n > Media > Video** to enable CAC/Admission control. Enable Admission control for Video.

Depending on the type of service that needs to be enabled on the radio, configure a value for **Max RF Bandwidth**. This value will decide the number of video clients to be allowed to join a configured multicast stream on the radio. For example, a maximum value of 80% will allow twenty wireless clients stream with a bit rate of 5M bits.



Step 5 Click **WIRELESS > 802.11 a/n > Media > Voice** to enable Voice CAC/Admission control. Enable Admission control for Voice.

This value will decide the number of voice calls that will be allowed on the radio.

The screenshot displays the Cisco Wireless Configuration Manager interface. The left sidebar shows the navigation tree with '802.11a/n/ac' expanded and 'Media' selected. The main panel shows the configuration for the 802.11a(5 GHz) radio. The 'Media' tab is active, showing the 'Call Admission Control (CAC)' and 'Per-Call SIP Bandwidth' sections. A red arrow points to the 'Max RF Bandwidth (5-85)(%)' field, which is set to 10.

The radio was disabled to add the VideoStream configurations. Enable the 802.11a radio.

Enabling VideoStream – 802.11b/g/n radio



Note The above configuration can be repeated on the 802.11b/g/n radio.

Procedure

Step 1 Disable the 802.11b/g/n radio before any changes are made.

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY

FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates

OEAP ACLs

Network Lists

▼ **802.11a/n/ac**
Network
▼ RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n/ac)
CleanAir

▼ **802.11b/g/n**
Network
▼ RRM

802.11b/g Global Parameters

General

802.11b/g Network Status	<input type="checkbox"/> Enabled
802.11g Support	<input type="checkbox"/> Enabled
Beacon Period (milliseconds)	100
Short Preamble	<input checked="" type="checkbox"/> Enabled
Fragmentation Threshold (bytes)	2346
DTPC Support.	<input checked="" type="checkbox"/> Enabled
Maximum Allowed Clients	200
RSSI Low Check	<input type="checkbox"/> Enabled
RSSI Threshold (-60 to -90 dBm)	-80

CCX Location Measurement

Mode	<input type="checkbox"/> Enabled
------	----------------------------------

Enabling the VideoStream feature on 802.11b/g/n needs closer attention as there will be a higher client density. It is necessary to allocate a sufficient amount of bandwidth for wireless clients to join the multicast stream. Balancing the data, voice, and video clients on the 802.11b/g/n radio should be planned well in advance so the configurations, once applied, will not cause major issues.

Note BandSelect and ClientLink are the two features that will service the wireless clients and reduce some of the clients on the 2.4 GHz radio.

Step 2 Click **WIRELESS > 802.11 b/g/n > Media > Media**.
By default, the VideoStream feature is disabled on the radios.

Step 3 Enable the **Multicast Direct Enable** feature.

Step 4 Configure the maximum number of streams with a value ranging from 1 to 20, or leave it as default.
The **Unicast Video Redirect** is enabled by default. This will allow unicast video traffic flow to wireless clients.

CISCO MONITOR WLANs CONTROLLER **WIRELESS** SECURITY

FlexConnect Groups
 FlexConnect ACLs
 FlexConnect VLAN Templates

OEAP ACLs

Network Lists

▼ **802.11a/n/ac**
 Network
 ▼ RRM
 RF Grouping
 TPC
 DCA
 Coverage
 General
 Client Roaming
 Media
 EDCA Parameters
 DFS (802.11h)
 High Throughput (802.11n/ac)
 CleanAir

▼ **802.11b/g/n**
 Network
 ▼ RRM
 RF Grouping
 TPC
 DCA
 Coverage
 General
 Client Roaming
Media
 EDCA Parameters

802.11b(2.4 GHz) > Media

Voice Video Media

General

Unicast Video Redirect ☒

Multicast Direct Admission Control

Maximum Media Bandwidth (0-85(%))

Client Minimum Phy Rate

Maximum Retry Percent (0-100%)

Media Stream - Multicast Direct Parameters

Multicast Direct Enable ☒

Max Streams per Radio

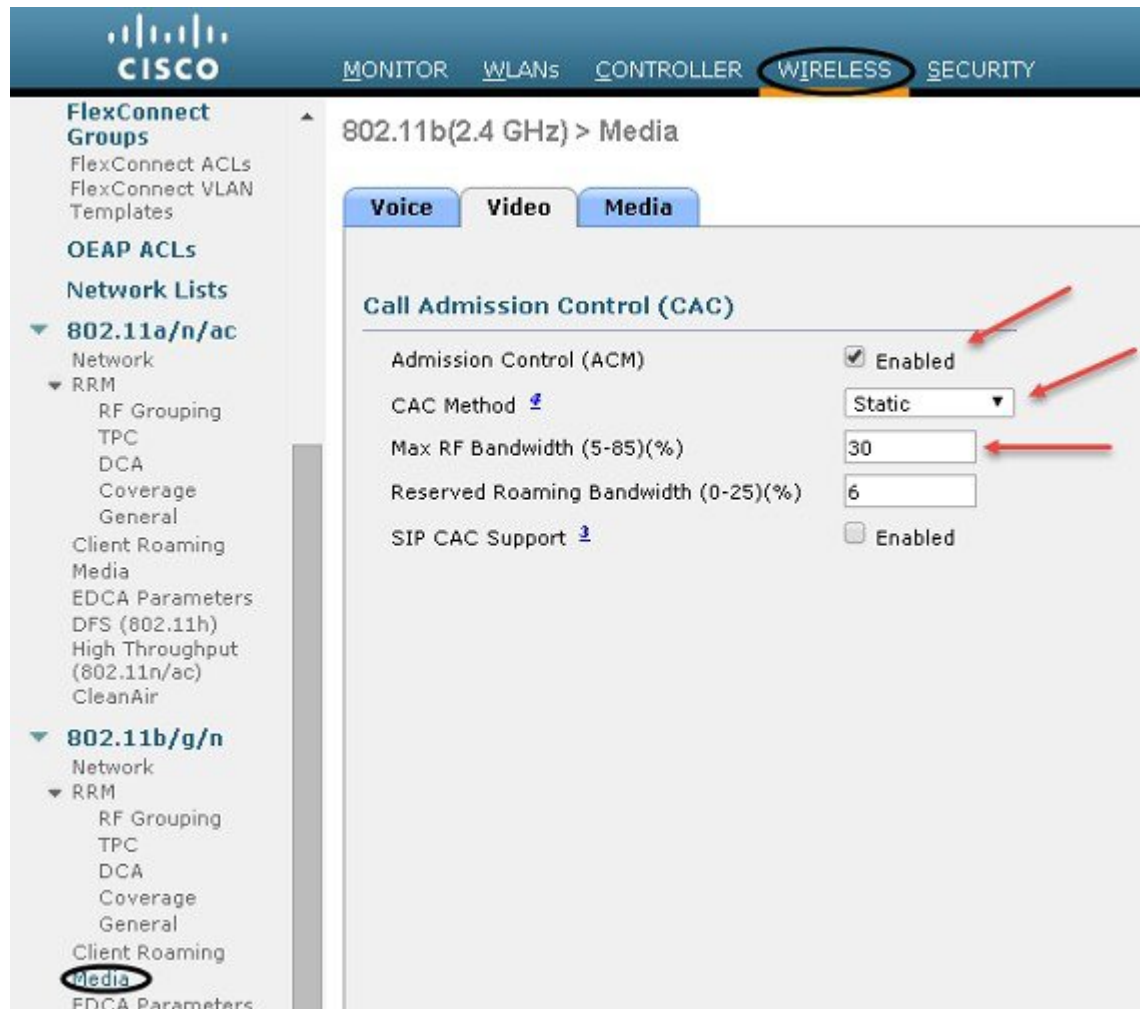
Max Streams per Client

Best Effort QoS Admission ☐ Enabled

RRC will admit clients to join a stream after pass criteria is achieved. The admitted clients will have a QoS priority of 4. The clients who do not pass the RRC criteria will be dropped and will not be allowed to join the stream. However, this can be overruled by enabling **Best Effort QoS Admission**. Now all wireless clients requested to join a stream will be admitted to the multicast stream, but some of them will have a QoS priority of 0.

The media bandwidth is currently set to 85% by default. Media bandwidth is the sum of Voice and Video traffic on a radio interface. The lowest that a client can drop on the radio is 6000 kbps to join a streaming video. If there are clients that need to be restricted from joining a stream below a certain PHY rate, then this value can be changed. The value is 6000 by default. The maximum retry percent is by default set to 80%. The system keeps track of the retries on the radio and if the retries is greater than configured value the client will not be allowed to join the stream.

- Step 5** Click **WIRELESS > 802.11 b/g/n > Media > Video** to enable CAC/Admission control.
- Step 6** Check the **Admission control (ACM)** check box to enable admission control for video.
- Step 7** Depending on the type of service that needs to be enabled on the radio, configure a value for **Max RF Bandwidth**. The value added here will decide the number of video client that will be allowed to join a configured multicast stream on the radio.



- Step 8** Click **WIRELESS > 802.11 b/g/n > Media > Voice** to enable Voice CAC/Admission control.
- Step 9** Check the **Admission Control (ACM)** check box to enable admission control for voice.
- Step 10** Configure a value for **Max RF Bandwidth**. The value added here will decide the number of voice calls to be allowed on the radio.

FlexConnect Groups
FlexConnect ACLs
FlexConnect VLAN Templates

OEAP ACLs

Network Lists

▼ **802.11a/n/ac**
Network
▼ RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
DFS (802.11h)
High Throughput (802.11n/ac)
CleanAir

▼ **802.11b/g/n**
Network
▼ RRM
RF Grouping
TPC
DCA
Coverage
General
Client Roaming
Media
EDCA Parameters
High Throughput

802.11b(2.4 GHz) > Media

Voice **Video** **Media**

Call Admission Control (CAC)

Admission Control (ACM) ☒ Enabled

CAC Method [?](#) Load Based ▼

Max RF Bandwidth (5-85)(%) 55

Reserved Roaming Bandwidth (0-25)(%) 6

Expedited bandwidth ☐

SIP CAC Support [?](#) ☐ Enabled

Per-Call SIP Bandwidth [?](#)

SIP Codec G.711 ▼

SIP Bandwidth (kbps) 64

SIP Voice Sample Interval (msecs) 20 ▼

Traffic Stream Metrics

Metrics Collection ☐

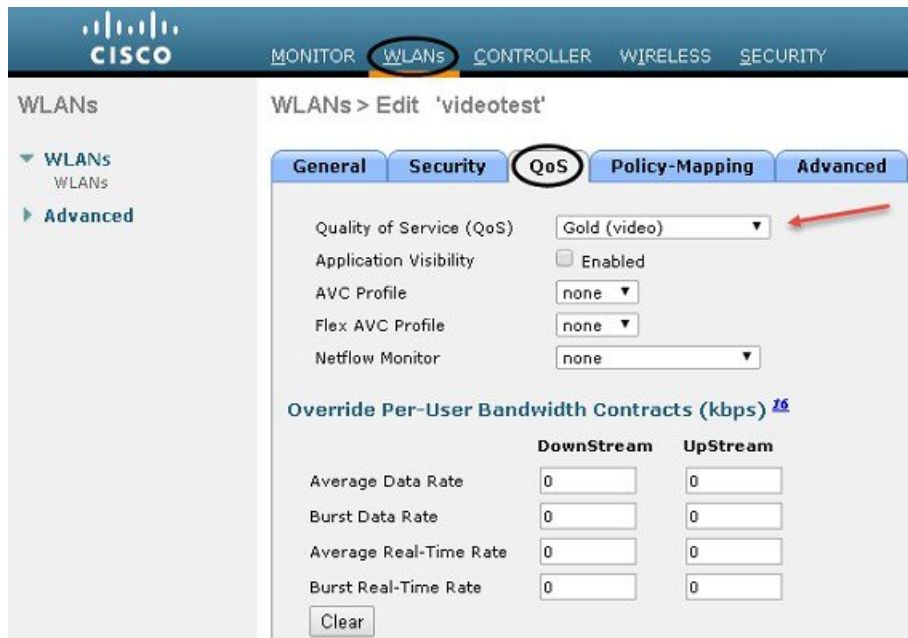
Step 11 Enable the radio(s) to allow clients to associate.

Enabling VideoStream - WLAN

One or all the WLANs / SSIDs configured can be enabled for streaming video with VideoStream. Enabling or disabling of the VideoStream feature is non-disruptive.

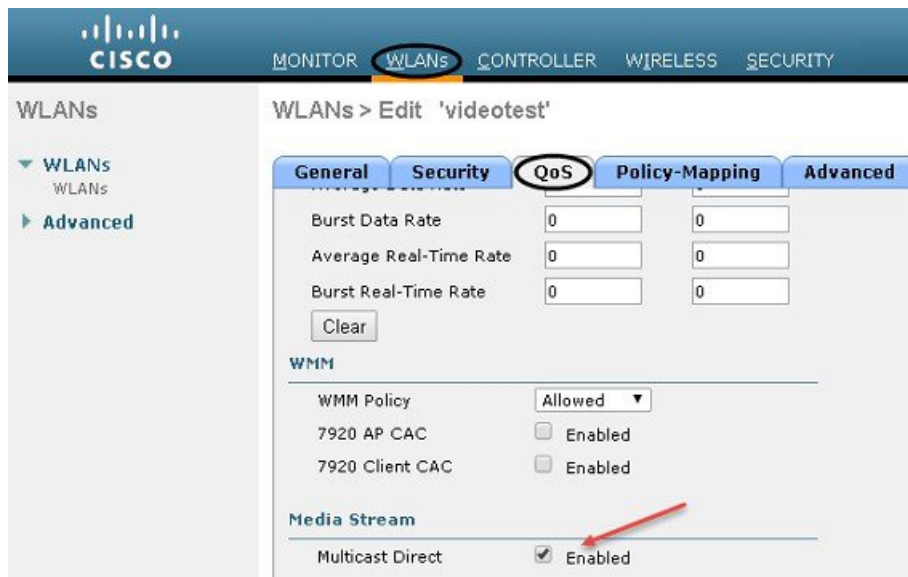
Procedure

Step 1 Click WLAN > <WLAN ID> > QoS.



Step 2 Configure the **Quality of Service (QoS)** to **Gold (video)** to stream video to wireless client at a QoS value of gold (4). This will only enable the video quality of service to wireless clients joined to a configured stream on the controller. The rest of the clients will be enabled for appropriate QoS.

Step 3 Enable **Multicast Direct** on the WLAN. This will enable the WLAN to service wireless clients with the VideoStream feature.



All wireless clients requesting to join a stream will be assigned video QoS priority on admission. Wireless client streaming video prior to enabling the feature on the WLAN will be streaming using normal multicast. Enabling of the feature will switch the clients to multicast-direct automatically on the next IGMP snooping interval.

Legacy multicast can be enabled on the WLAN by not checking the Multicast Direct feature. This will show that wireless clients streaming video are in Normal Multicast mode.

Verifying VideoStream Functionality

Make sure the wireless clients are associated to the access point(s), and are configured for a correct interface. As seen in the following screen shot, there are three clients associated to one access point. All three clients have an IP address from VLAN111 (management).

The screenshot shows the Cisco WLC Monitor page. The 'MONITOR' tab is selected in the top navigation bar. In the left sidebar, the 'Clients' link is circled. The main content area displays a table of associated clients. The table has columns for Client MAC Addr, IP Address (Ipv4/Ipv6), AP Name, WLAN Profile, and WLAN SSID. Three clients are listed, all with IP addresses in the 172.20.227.0/24 range. The WLAN SSID for all clients is 'videotest'.

Client MAC Addr	IP Address (Ipv4/Ipv6)	AP Name	WLAN Profile	WLAN SSID
18:f6:43:45:57:18	172.20.227.126	CAP2702I-1	videotest	videotest
3c:a9:f4:17:5c:80	172.20.227.120	CAP3702I	videotest	videotest
b8:f6:b1:11:7f:23	172.20.227.121	CAP1702I	videotest	videotest

The associated clients have an IP address and good uplink connectivity to the access point.

Client Properties		AP Properties	
MAC Address	0c:8b:fd:74:57:5c	AP Address	f0:7f:06:65:8d:a0
IPv4 Address	172.20.227.121	AP Name	CAP1702I
IPv6 Address	fe80::dc5a:18d6:b4b9:dd70,	AP Type	802.11ac
		AP radio slot Id	1
		WLAN Profile	videotest
		WLAN SSID	videotest
		Status	Associated
		Association ID	1
		802.11 Authentication	Open System
		Reason Code	1
		Status Code	0
Client Type	Simple IP		
User Name			
Port Number	1		
Interface	management		
VLAN ID	111		
Quarantine VLAN ID	0		
CCX Version	CCXv4		

Client Statistics	
Bytes Received	148877
Bytes Sent	14727
Packets Received	1676
Packets Sent	210
Policy Errors	0
RSSI	-68
SNR	28

There are no clients that have joined the multicast stream. There is only the controller entry with the configured multicast group address registered on the switch.

```
Switch14-1#
Switch14-1#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.100.1.2), 00:11:59/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 00:11:16/stopped

(172.20.227.112, 239.100.1.2), 00:11:59/00:02:50, flags: T
  Incoming interface: Vlan111, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 00:11:16/stopped

(*, 239.255.255.250), 00:05:47/00:02:57, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan111, Forward/Sparse-Dense, 00:05:47/stopped
```

There is no video streaming on the wired network, hence no entries for the (S, G) source, group addresses. Enable streaming on the wired side by connecting a video server with a configured multicast address 239.4.5.6. The capture on the switch will be more than what was observed earlier.

```
Switch14-1#
Switch14-1#sh ip mroute
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 239.100.1.2), 00:11:59/stopped, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 00:11:16/stopped

(172.20.227.112, 239.100.1.2), 00:11:59/00:02:50, flags: T
  Incoming interface: Vlan111, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan10, Forward/Sparse-Dense, 00:11:16/stopped

(*, 239.4.5.6), 00:10:07/00:02:53, RP 0.0.0.0, flags: DC
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Vlan111, Forward/Sparse-Dense, 00:10:07/stopped

(172.20.227.125, 239.4.5.6), 00:08:26/00:02:58, flags: T
  Incoming interface: Vlan111, RPF nbr 0.0.0.0
  Outgoing interface list: Null
Switch14-1#
```

Debug - Switch

Join a wireless client to the multicast streaming video. Also, capture the debug bcast all enable from the controller. The debug capture has information on the client request, group address, status of the request, and the update.

```
*bcastReceiveTask: Jul 06 21:13:23.414: bcastProcessNPUMsg: received packet (rxTunType 1, dataLen 126)
*bcastReceiveTask: Jul 06 21:13:23.414: bcastLwappRx: Rcvd lwapp pkt from STA : 0C:8B:FD:74:57:5C .
*bcastReceiveTask: Jul 06 21:13:23.414: IGMP Pkt Rcvd over vlan = 111 from client 0C:8B:FD:74:57:5C .
*bcastReceiveTask: Jul 06 21:13:23.414: Recieved Igmp v2 report packet from client 0C:8B:FD:74:57:5C..
*bcastReceiveTask: Jul 06 21:13:23.414: 239.4.5.6 is not a link-local mcast addr
*bcastReceiveTask: Jul 06 21:13:23.414: Received JOIN for IGMP group = 239.4.5.6
*bcastReceiveTask: Jul 06 21:13:23.422: Received status Update for client: 0C:8B:FD:74:57:5C
  status = 2 qos = 4
*bcastReceiveTask: Jul 06 21:13:23.422: 0C:8B:FD:74:57:5C client is already in ALLOWED state.
*bcastReceiveTask: Jul 06 21:13:23.486: IGMPv2 REPORT for GROUP= 239.4.5.6 send SUCCESS.
```

The wireless client with MAC address 0C:8B:FD:74:57:5C sent an IGMP v2 joins in the form of a report to a stream address of 239.4.5.6. The client joined the group with a qos=4 and was changed to an ALLOWED state.

Click **MONITOR > Multicast > MGID** for the streaming address 239.4.5.6. It is observed that the MAC address of the wireless client is in a **Multicast-Direct Allowed State**. The QoS User priority is 4. This shows the client processing the video packets in the video queue.

Monitor

Multicast Group Detail

Current Filter : 12362 [Change Filter] [Show All]

Client MAC Addr	AP Name	Expire Time (mm:ss)	Multicast Status	QOS User Priority
0c:8b:fd:74:57:5c	CAP3702I	00:53	Multicast-direct Allowed	4
3c:a9:f4:17:5c:80	CAP2702I-1	00:57	Multicast-direct Allowed	4

```
(Cisco_Controller) >
(Cisco_Controller) >show network multicast mgid detail 12362

mgid.....12362
MulticastGroup Address.....239.4.5.6
Vlan.....111
No of clients.....2
Client List.....
Client MAC      AP Name      Expire Time (mm:ss)  Multicast-Status      Qos User Priority
.....
3c:a9f4:17:5c:80  CAP2702I-2    0:55                Mcast-direct Allowed   4
0c:8b:fd:74:57:5c  CAP3702I      0:59                Mcast-direct Allowed   4
```

Debug - Controller

The processing of a wireless client's request on a controller can be clearly understood by enabling the debugs on the controller. The enabled debugs are also captured on the controller. A request 3694 is created for client with MAC address 0c8b.fd74.575c. All of the data flow is with respect to the client with the MAC address 0c8b.fd74.575c as shown in the debug below. The RRC validates the resources for the associated radio. The validation is successful and the client is admitted based on the values validated. The stream will be in blocked state until the stream is admitted and the client will not receive any video during this time period . The client will start streaming video once it receives a join response.

Any further requests from the same client will be validated. As the client is already streaming, the RRC engine will respond with an "Already admitted "message. This will not hinder the performance of the wireless client.

```
(Cisco_Controller) >
(Cisco_Controller) >show debug

MAC debugging ..... disabled
Debug Flags Enabled:
  Media-Stream Admission debug enabled.
  Media-Stream Config debug enabled.
  Media-Stream Errors debug enabled.
  Media-Stream Event debug enabled.
  Media-Stream Client History debug enabled.
  Media-Stream Rrc debug enabled.

Flex-AP Client Debugging ..... disabled
Flex-Group Client Debugging ..... disabled
```

```

(Cisco Controller) >*bcastReceiveTask: Jul 06 22:17:01.826: mc2uc update client 0c8b.fd74.575c radio
f07f.0665.8da0 destIp 239.4.5.6 srcIp 0.0.0.0 mgid 12362 slot 1 vapId 3 vlan 111
*bcastReceiveTask: Jul 06 22:17:01.826: Already admitted, mc2uc Update the last IGMP timestamp
*rrcEngineTask: Jul 06 22:17:20.026: rrcEngineProcessPurgeTimer: table expired
*rrcEngineTask: Jul 06 22:17:20.026: SR expire dest 239.4.5.6 client 0c8b.fd74.575c now
Mon Jul 6 22:17:20 2015

last Mon Jul 6 22:17:01 2015
*bcastReceiveTask: Jul 06 22:18:02.234: mc2uc update client 0c8b.fd74.575c radio f07f.0665.8da0
destIp 239.4.5.6 srcIp 0.0.0.0 mgid 12362 slot 1 vapId 3 vlan 111
*bcastReceiveTask: Jul 06 22:18:02.234: msPolicyGetStreamParameters 1500 1200
*bcastReceiveTask: Jul 06 22:18:02.234: mc2uc update: Add history record with cause 9
*bcastReceiveTask: Jul 06 22:18:02.234: Sending delist trap
*bcastReceiveTask: Jul 06 22:18:02.235: leave client 0c8b.fd74.575c radio f07f.0665.8da0
destIp 239.4.5.6 mgid 12362
*bcastReceiveTask: Jul 06 22:18:02.235: mc2uc Leave, remove stream
*rrcEngineTask: Jul 06 22:18:02.235: start FindRequestByClient
*rrcEngineTask: Jul 06 22:18:02.235: FindRequestByClient not found dest 239.4.5.6
client 0c8b.fd74.575c radio f07f.0665.8da0 source 0.0.0.0 slot 1
*rrcEngineTask: Jul 06 22:18:02.235: rrcEngineHandleStreamLeave no record for client
0c8b.fd74.575c radio f07f.0665.8da0 dest 239.4.5.6
*rrcEngineTask: Jul 06 22:18:02.235: rrcSrExpireStreamRecord dest 239.4.5.6 client 0c8b.fd74.575c
*rrcEngineTask: Jul 06 22:18:02.235: RRC clientRecord remove clientMac 0c8b.fd74.575c #of streams 0
*rrcEngineTask: Jul 06 22:18:02.235: RadioRemoveStreamRecord # of streams is 0 on radio f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.235: rrcSrDeleteStreamRecord dest 239.4.5.6 client 0c8b.fd74.575
*rrcEngineTask: Jul 06 22:18:02.235: Creating request 3694
*rrcEngineTask: Jul 06 22:18:02.235: for radio f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.235: rrcEngineInsertAdmitRequest dest 0.0.0.0 mgid 0 request 3694
*rrcEngineTask: Jul 06 22:18:02.235: rrcEngineInsertReRrcRequest request 3694
*rrcEngineTask: Jul 06 22:18:02.235: rrcEngineSendReRrcMetricsRequest sent request 3694 to radio
f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.235: rrcEngineInitiateStatsUpdate request 3694 to radio f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.238: rrcEngineHandleStreamCleanup radio f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.246: rrcEngineProcessRadioMetrics start radio f07f.0665.8da0
request 3694
*rrcEngineTask: Jul 06 22:18:02.246: rrcEngineFindRequest look for request 3694
*rrcEngineTask: Jul 06 22:18:02.246: rrcEngineFindRequest found request 3694
*rrcEngineTask: Jul 06 22:18:02.246: rrcEngineRemoveAdmitRequest request 3694
*rrcEngineTask: Jul 06 22:18:02.246: statistics video: client number 0 request 3694 radio
f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:02.246: rrcEngineProcessRadioMetrics statistics update radio
f07f.0665.8da0 request 3694
*bcastReceiveTask: Jul 06 22:18:21.814: msPolicyPlatform test AP 1100 type
*bcastReceiveTask: Jul 06 22:18:21.814: msPolicyPlatform not AP 1100
*bcastReceiveTask: Jul 06 22:18:21.814: mStreamWlanMc2ucAllowed allow
*bcastReceiveTask: Jul 06 22:18:21.814: mStreamBand 1 allow mc2uc
*bcastReceiveTask: Jul 06 22:18:21.814: stream policy allow mc2uc
*bcastReceiveTask: Jul 06 22:18:21.822: mc2uc update client 0c8b.fd74.575c radio
f07f.0665.8da0 destIp 239.4.5.6 srcIp 0.0.0.0 mgid 12362 slot 1 vapId 3 vlan 111
*bcastReceiveTask: Jul 06 22:18:21.822: msPolicyGetRrcQosSupport 1 4 1
*bcastReceiveTask: Jul 06 22:18:21.822: mc2uc begin check policy
*bcastReceiveTask: Jul 06 22:18:21.822: msPolicyPlatform test AP 1100 type
*bcastReceiveTask: Jul 06 22:18:21.822: msPolicyPlatform not AP 1100
*bcastReceiveTask: Jul 06 22:18:21.822: mc2uc qos admit 1 qos 4 pri 1
*bcastReceiveTask: Jul 06 22:18:21.822: mc2uc submit client client 0c8b.fd74.575c radio
f07f.0665.8da0 destIp 239.4.5.6 mgid 12324 vapId 3 vlan 111
*bcastReceiveTask: Jul 06 22:18:21.822: start FindRequestByClient
*bcastReceiveTask: Jul 06 22:18:21.822: FindRequestByClient not found dest 239.4.5.6 client
0c8b.fd74.575c radio f07f.0665.8da0 source 0.0.0.0 slot 1
*bcastReceiveTask: Jul 06 22:18:21.822: Creating request 3695
*bcastReceiveTask: Jul 06 22:18:21.822: for radio f07f.0665.8da0
*bcastReceiveTask: Jul 06 22:18:21.822: for client 0c8b.fd74.575c
*bcastReceiveTask: Jul 06 22:18:21.822: rrcEngineInsertAdmitRequest dest 239.4.5.6 mgid 12362
request 3695
*bcastReceiveTask: Jul 06 22:18:21.822: rrcEngineSendMeasureMetricsRequest sent request 3695
to radio f07f.0665.8da0, minRate = 6000, maxRetryPercent = 80
*rrcEngineTask: Jul 06 22:18:21.824: rrcEngineProcessRadioMetrics start radio f07f.0665.8da0
request 3695
*rrcEngineTask: Jul 06 22:18:21.824: rrcEngineFindRequest look for request 3695
*rrcEngineTask: Jul 06 22:18:21.824: rrcEngineFindRequest found request 3695
*rrcEngineTask: Jul 06 22:18:21.824: done rrcEngineProcessRadioMetrics radio f07f.0665.8da0
request 3695
*rrcEngineTask: Jul 06 22:18:21.830: rrcEngineProcessClientMetrics radio f07f.0665.8da0 request 3695

```

```

*rrcEngineTask: Jul 06 22:18:21.830: rrcEngineFindRequest look for request 3695
*rrcEngineTask: Jul 06 22:18:21.830: rrcEngineFindRequest found request 3695
*rrcEngineTask: Jul 06 22:18:21.830: rrcEngineRemoveAdmitRequest request 3695
*rrcEngineTask: Jul 06 22:18:21.830: p_video = 0, p_voice = 0, pb = 25, video_qo = 0,
video_l_r_ratio = 0, video_no = 0, video_delay_hist_severe = 0, video_pkt_loss_discard = 0,
video_pkt_loss_fail = 0,
*rrcEngineTask: Jul 06 22:18:21.830: radio_tx_q_max_size = 2, radio_tx_q_limit = 27839,
vi_tx_q_max_size = 0, current_rate = 720
*rrcEngineTask: Jul 06 22:18:21.830: msPolicyGetStreamParameters 1500 1200
*rrcEngineTask: Jul 06 22:18:21.830: Admit video: number of streams on radio is 0,
number of streams on client is 0
*rrcEngineTask: Jul 06 22:18:21.830: Mapping wme code 1 to history code 0
*rrcEngineTask: Jul 06 22:18:21.830: Admit video: request 3695 radio f07f.0665.8da0,
decision 1 admission 2
*rrcEngineTask: Jul 06 22:18:21.830: mStreamBandMc2ucAdmit besteffort 0
*rrcEngineTask: Jul 06 22:18:21.830: Approve Admission on radio f07f.0665.8da0 request 3695
vlan 111 destIp 239.4.5.6 decision 1 qos 4 admitBest 0
*rrcEngineTask: Jul 06 22:18:21.830: RRC Admission: Add history record with cause code 0
destIp 239.4.5.6
*rrcEngineTask: Jul 06 22:18:21.830: Sending admit trap
*rrcEngineTask: Jul 06 22:18:21.830: RRC clientRecord add clientMac 0c8b.fd74.575c #of streams 1
*rrcEngineTask: Jul 06 22:18:21.831: RadioInsertStreamRecord # of streams is 1 on radio
f07f.0665.8da0
*rrcEngineTask: Jul 06 22:18:21.831: Recording request 3695 destIp 239.4.5.6 qos 4 vlan 111
violation-drop 0 priority 1 sourceIp 0.0.0.0 client 0c8b.fd74.575c radio f07f.0665.8da0 slotId 1
*rrcEngineTask: Jul 06 22:18:21.831: done rrcEngineProcessClientMetrics client 0c8b.fd74.575c
radio f07f.0665.8da0 request 3695
*bcstReceiveTask: Jul 06 22:18:23.322: msPolicyPlatform test AP 1100 type
*bcstReceiveTask: Jul 06 22:18:23.322: msPolicyPlatform not AP 1100
*bcstReceiveTask: Jul 06 22:18:23.322: stream policy default MC
*bcstReceiveTask: Jul 06 22:19:01.322: mc2uc update client 0c8b.fd74.575c radio f07f.0665.8da0
destIp 239.4.5.6 srcIp 0.0.0.0 mgid 12362 slot 1 vapId 3 vlan 111
*bcstReceiveTask: Jul 06 22:19:01.322: Already admitted, mc2uc Update the last IGMP timestamp
(Cisco_Controller) >

```

Show commands—Controller

Some of the **show** commands were captured earlier in this document. This section of the capture is only for reference. For more details on the commands, see the CUWN Release 8.1 Commands Reference Guide.

```

Cisco_Controller) >
(Cisco_Controller) >show ap summary

```

```

Number of APs..... 2

Global AP User Name..... Not Configured
Global AP Dot1x User Name..... Not Configured

```

AP Name IP Address	Slots Clients	AP Model DSE Location	Ethernet MAC	Location	Country
CAP3702I 10.1.1.75	2 1	AIR-CAP3702I-A-K9 [0 ,0 ,0]	d4:6d:50:91:fb:d8	default location	US
CAP2702I-2 10.1.1.74	2 1	AIR-CAP2702I-A-K9 [0 ,0 ,0]	f4:0f:1b:72:fd:1c	default location	US

```

(Cisco_Controller) >
(Cisco_Controller) >show client summary

```

```

Number of Clients..... 2

Number of PMIPv6 Clients..... 0

Number of EoGRE Clients..... 0

```

MAC Address	AP Name	Slot Status	WLAN	RLAN/ Auth Protocol	Port Wired Tunnel	Role
-------------	---------	-------------	------	------------------------	-------------------	------

```

0c:8b:fd:74:57:5c CAP3702I      1   Associated      3   Yes   802.11ac(5 GHz)  1   N/A   No   Local
3c:a9:f4:17:5c:80 CAP2702I-2    1   Associated      3   Yes   802.11n(5 GHz)   1   N/A   No   Local
(Cisco_Controller) >
(Cisco_Controller) >show media-stream multicast-direct state

```

```

Multicast-direct State..... enable
Allowed WLANs..... 3
(Cisco_Controller) >
(Cisco_Controller) >show media-stream group summary

```

Stream Name	Start IP	End IP	Operation Status
test1.5K	239.4.5.6	239.4.5.6	Multicast-direct

```

(Cisco_Controller) >
(Cisco_Controller) >show media-stream group detail test1.5K

```

```

Media Stream Name..... test1.5K
Start IP Address..... 239.4.5.6
End IP Address..... 239.4.5.6
RRC Parmmeters
Avg Packet Size(Bytes)..... 1200
Expected Bandwidth(Kbps)..... 1500
Policy..... Admit
RRC re-evaluation..... periodic
QoS..... Video
Status..... Multicast-direct
Usage Priority..... 1
Violation..... fallback
(Cisco_Controller) >
(Cisco_Controller) >show network multicast mgid summary

```

Layer2 MGID Mapping:

InterfaceName	vlanId	MGID
management	111	0

```

Layer2 mDNS MGID Mapping:
Start mDNS Mgid..... 16447
End mDNS Mgid..... 20545

```

Layer3 MGID Mapping:

```

Number of Layer3 MGIDs..... 2

```

Group address	VLAN	MGID	IGMP/MLD
239.4.5.6	111	12362	IGMP
239.255.255.250	111	12364	IGMP

```

(Cisco_Controller) >
(Cisco_Controller) >show network multicast mgid detail 12362

```

```

Mgid..... 12362
Multicast Group Address..... 239.4.5.6
Vlan..... 111
No of clients..... 2
Client List.....
Client MAC      AP Name      Expire Time (mm:ss)  Multicast-Status  Qos User Priority
-----
3c:a9:f4:17:5c:80 CAP2702I-2    0:55                Mcast-direct Allowed    4
0c:8b:fd:74:57:5c CAP3702I      0:59                Mcast-direct Allowed    4
(Cisco_Controller) >
(Cisco_Controller) >show 802.11a media-stream rrc

```

```

Multicast-direct..... Enabled
Best Effort..... Disabled
Video Re-Direct..... Enabled
Max Allowed Streams Per Radio..... Auto
Max Allowed Streams Per Client..... Auto

```

```

Max Video Bandwidth..... 75
Max Voice Bandwidth..... 10
Max Media Bandwidth..... 85
Min PHY Rate..... 6000
Max Retry Percentage..... 80

```

```
(Cisco_Controller) >
```

Conclusion

CUWN 8.1 software supports VideoStream feature on the newer controller hardware. This includes:

- Cisco 2500 series controllers
- Cisco 5500 series controllers (Cisco 5508 and 5520 wireless controllers)
- Cisco Flex 7500 series wireless controllers
- Cisco 8500 series wireless controllers (8510 and 8540 wireless controllers)
- Cisco virtual wireless controllers on the Cisco Services-Ready Engine (Cisco SRE) or the Cisco wireless LAN controller module for Cisco integrated services routers G2 (UCS-E) Kernel-based virtual machine (KVM) is supported in Cisco wireless release 8.1.102.0 and later.
- Cisco WiSM2 for Catalyst 6500 Series Switches

CUWN 7.4 and 7.6 software supports VideoStream feature on the following controllers. This includes:

- Cisco 5500 series controllers
- Wireless Service Module - 2
- Cisco 2500 series controllers*
- Cisco ISR-G2 with SRE module*



Note *—The performance numbers differ on the non-802.11n access points.

CUWN 7.0 software supports VideoStream feature on the following controller hardware. This includes:

- Cisco 5500 series controllers
- Cisco 4400 series controllers
- Cisco 2100 series controllers
- Wireless Service Module

VideoStream is also supported on the Cisco 2504 standalone and Cisco WiSM-2 controller.

CUWN 8.1 software supports VideoStream feature on all newer 802.11ac access points and a few legacy access points. This includes:

- Cisco Aironet 3700 series access points
- Cisco Aironet 3600 series access points
- Cisco Aironet 3500 series access points
- Cisco Aironet 2700 series access points

- Cisco Aironet 2600 series access points
- Cisco Aironet 1700 series access points
- Cisco Aironet 1260 series access points
- Cisco Aironet 1250 series access points
- Cisco Aironet 1240AG series access points*
- Cisco Aironet 1140 series access points
- Cisco Aironet 1130AG series access points*
- Cisco Aironet 1040 series access points



Note *Client capacity varies on the low end controllers.



Note The Cisco 1040 series, 1140 series, and 1260 series access points have feature parity with Cisco wireless release 8.0. Features introduced in Cisco wireless release 8.1 and later are not supported on these access points.

The VideoStream feature can stream video over Cisco Unified Wireless hardware and provide a superior quality. Static CAC configuration will provide wireless client control on the radios. The feature enables multicast streaming over wireless on par with multicast streaming on wired clients. Multicast streaming to wireless clients with IGMP join request and replication are done only at the access points thus conserving bandwidth on the uplink ports of the distribution and access switches.

Related Documents

- Cisco Wireless LAN Controller Configuration Guide, Release 7.0
- Technical Support & Documentation - Cisco Systems

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2015 Cisco Systems, Inc. All rights reserved.

**Americas Headquarters**

Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.