What Is New on Cisco Networking Capabilities for Medianet

Enterprise Medianet Overview

Medianet is an end-to-end architecture for a media-optimized network comprising advanced, intelligent technologies and devices in a platform optimized for the delivery of rich-media experiences. A medianet has the following characteristics:

- Media-aware: Capable of detecting and optimizing different media and application types (telepresence, video surveillance, desktop collaboration, and streaming media) to deliver the best experience
- Endpoint-aware: Detects and configures media endpoints automatically
- Network-aware: Can detect and respond to changes in device, connection, and service availability

Enterprise medianet is unique because it extends the boundary of networks to include the endpoints to scale, optimize, and enhance the performance of video. As a result, medianet provides a tight integration between intelligent network services and the rich-media applications delivered over a variety of endpoints.

Cisco® Networking Capabilities 2.1 for Medianet focuses on reducing IT costs and complexity of deploying video as well as improving the video experience.

Cisco Networking Capabilities 2.1 for Medianet

Cisco Networking Capabilities 2.1 for Medianet introduces features that aid in configuration and provisioning of video endpoints:

- Cisco Auto Smartports on switches
- Location information exchange
- Cisco AutoQoS for video endpoints
- Media Services Interface
- CiscoWorks LAN Management Solution (LMS) medianet plug-in

In addition to those features, the Cisco Unified Wireless VideoStream can enhance video performance over wireless networks.

Autoconfiguration and Location Information

Autoconfiguration capabilities help address some of the challenges involved in mass deployments of rich-media endpoints such as digital media players and physical security cameras. Before the availability of autoconfiguration features, switch ports that are used to connect media endpoints such as digital media players and physical security cameras need to be configured with the appropriate settings. These endpoints are often installed in distributed locations and mounted in hard-to-reach places such as walls, ceilings, or poles, and they are usually preconfigured before mounting and installation, requiring preparation and planning.

Personnel who install these endpoints do not typically possess IP networking skills or are not granted access to the network configuration consoles. When an endpoint is installed in the field, it can inadvertently be plugged into the wrong network port.If the port lacks the correct configuration, the device may not get assigned to the proper VLAN.If that happens, the device cannot connect to its management server, so it cannot become operational. The operator needs to physically go to the switch and troubleshoot.These situations increase operating cost and are inefficient.

If the device is connected to the wrong port, the location information may be incorrect. Because the location information is statically configured at the application manager such as Digital Media Manager or Video Surveillance Operations Manager, applications that rely on this information will receive incorrect data. For example, a streaming server could send incorrect content to a specific digital media player. Or a security officer may think he is watching streaming video from one IP surveillance camera location when he is actually viewing video from another location.

Autoconfiguration capabilities overcome those deployment challenges. With the autoconfiguration capability, when endpoint devices are connected to an access switch, the access switch can recognize the device and automatically configure the port for VLAN, quality of service (QoS) or AutoQoS, security features, and location information. This autoconfiguration reduces configuration costs and minimizes the effect of an incorrectly deployed device.

To recognize and configure a device, the access switch must have the Auto Smartports feature enabled. Access switches with Auto Smartports can recognize endpoint devices based on the Cisco Discovery Protocol or the MAC address range of the endpoint device.

Autoconfiguration has three components.

The first component allows an endpoint device to announce and identify itself to the network. Typical endpoint devices use, Cisco Discovery Protocol, or MAC address range to announce themselves.

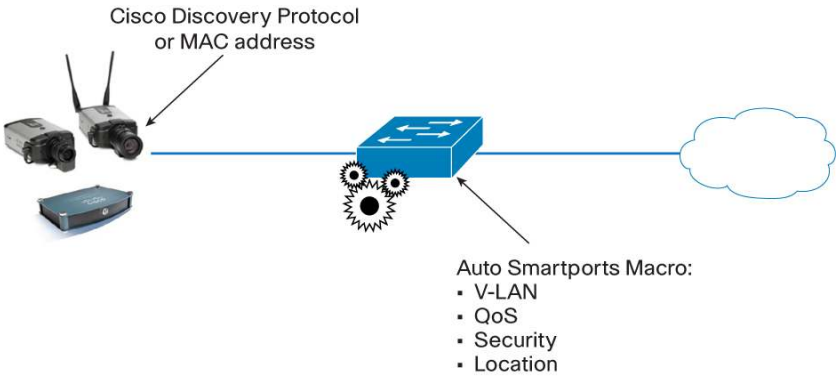
The second component is the Auto Smartport feature implemented in the access switch images of Cisco IOS® Software. This component applies device-specific configuration and AutoQoS macros to switch ports upon detection of a media endpoint. The switch software comes with a set of built-in best-practice configuration macros for a variety of media endpoints.

The third component is setting up and sending out location information. Cisco IOS Software allows network operators to configure device-specific location information on the switches. This location information is then propagated to the endpoint devices.

These components help in simplifying deployment, QoS configuration, and asset tracking and help reduce operating costs of rich-media applications and endpoints.

Figure 1 shows the autoconfiguration solution and its components. Endpoint devices announce themselves through Cisco Discovery Protocol or MAC address. The Auto Smartport feature in the access switch applies device specific configuration and AutoQoS macros.

Figure 1. Autoconfiguration solution and its components.



Media Services Interface

One of the critical aspects of a medianet is the need to provide tighter integration between the network infrastructure services and the rich-media endpoints and applications. These medianet services could be used to either enhance

quality of experience with the application or reduce the operating costs of managing and deploying the applications. However, in most enterprise networks today, the crucial linkage between the application and these services is often either missing or incomplete, meaning that enterprises are unable to take full advantage of the value of the network infrastructure and the total cost of ownership (TCO) for the rich-media applications increases.

The Media Services Interface was developed to address the challenge of tightly integrating applications and network infrastructure services to deliver an optimized high-quality rich-media experience while minimizing the TCO. The interface provides Cisco rich-media endpoints and applications with a series of application programming interfaces (APIs) to enable them to take advantage of the medianet services in the network infrastructure. Embedding the Media Services Interface into a wide range of rich-media endpoints enables the network to provide a standardized set of services, which can be accessed in a consistent and controlled manner. This scenario reduces interoperability problems, complexity, and costs of operations, enabling the network administrator to extract greater value from the network infrastructure deployed.

The Media Services Interface APIs are designed to provide these services in an abstract manner, enabling applications to take full advantage of the services without needing to integrate with - or be aware of - the network layer protocols needed to communicate with the network. This scenario simplifies and accelerates application adoption of medianet services, in turn enabling the applications to improve the user experience. The APIs also provide the means by which to exchange information from the network to the application, and conversely.

Enabling the flow of information between the two entities gives the application greater visibility into what level of service the network can provide, in turn allowing the application to adapt better to the prevailing network conditions. Likewise, the network benefits from a better understanding of the applications that are running over it and the network can intelligently apply services based on the specific needs of the applications.

The Media Services Interface provides the essential glue between the intelligent network services and the increasingly sophisticated rich-media applications. Bridging the gap between the network services and the applications exponentially increases the value to both.

Simplifying the Configuration and Management of Medianet Endpoints with CiscoWorks LAN Management Solution (LMS)

CiscoWorks LMS is an integrated suite of management functions that simplify the configuration, administration, monitoring, and troubleshooting of Borderless Networks. The medianet “plug-in” for CiscoWorks LMS provides workflows for setting up autoconfiguration and location settings to aid the provisioing and tracking of medianet endpoints such as digital media players and IP video surveillance cameras. The medianet workflows enable the network operator to select the type of medianet to provision, and automatically prepare the network for deplyment and check to ensure the appropriate location attibutes are configured for tracking and monitoring purposes, reducing the chance for errors and time required to set up an end-to-end video infrastructure.

CiscoWorks LMS 4.1 can help customers configure autoconfiguration and location settings to aid in provisioning and tracking medianet endpoints such as the Cisco Digital Media Player (DMP) and the Cisco IP Video Surveillance Camera (IPVSC).

Cisco Works LMS can provide workflows to help users select the type of medianet provisioning they want in their network by providing high-level details such as how to prepare the network for DMP and IPSVC provisioning and how to enable availability monitoring of DMP and IPVSC, etc.

Depending on what you select, CiscoWorks LMS internally builds a workflow for configuring the features associated with your selection. For example, if you select “Prepare network for DMP and IPVSC provisioning”, then CiscoWorks LMS runs a readiness check for Auto Smartports and location configuration and builds workflows for configuring Auto Smartports and location attributes in your network.

Readiness Report for Auto Smartports

This check involves validation of proper hardware and software platforms that can support Auto Smartports. Readiness criteria for Auto Smartports remain the same as that for CiscoWorks LMS 4.0.

Readiness Report for Location

This check involves validation of proper hardware and software platforms that can support location attribute configuration at the device and port level.

For more information about CiscoWorks LMS and the medianet plug-in, please visit: http://www.cisco.com/go/lms.

Cisco VideoStream

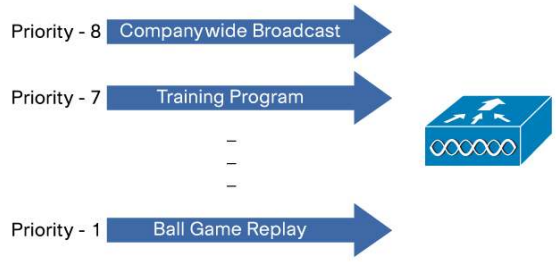
Cisco VideoStream is a new set of features for the Cisco Unified Wireless Network that optimizes the performance of multimedia over the wireless and wired network. Cisco VideoStream provides the features needed to support the rich-media requirements of medianets. It removes the challenges associated with streaming video over the wireless network by enforcing video priority levels, controlling resource reservation, and delivering reliable multicast. These features help ensure that the quality of existing wireless media sessions is maintained as additional wireless video streams are added to the network.

This section highlights the features of Cisco VideoStream features and explains how they uniquely enhance the delivery of video over Wi-Fi and the quality of the end-user experience.

Stream Admission and Prioritization

Although video is an efficient, highly effective means of communication, it is also very bandwidth-intensive. Not all video content is prioritized the same. Organizations investing in video cannot afford to have network bandwidth consumed without prioritization of business-critical media. With stream admission, network administrators can configure media streams with different priorities based on importance within the organization. The feature can be enabled at the radio level (2.4 and 5 GHz) and at the wireless LAN (WLAN) or Service Set Identifier (SSID) level. It also gives administrators more control to identify specific video streams for preferential QoS treatment. For example, a companywide address from the CEO takes precedence over a replay of a sporting event from the previous night (Figure 2).

Figure 2. Stream Prioritization: Streams Marked for Preferential QoS



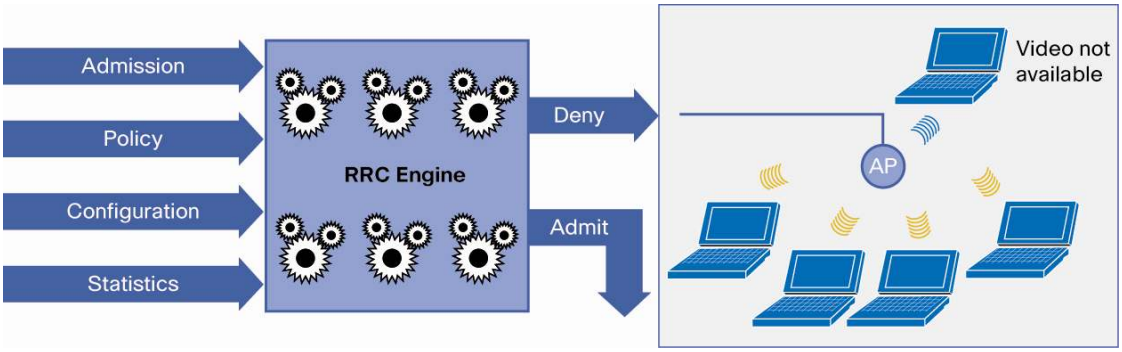
The configured video stream will have lower priority than voice and higher priority than best-effort traffic. All other multicast traffic will be admitted as best-effort traffic, even though it is marked for QoS for video priority.

Resource Reservation Control

As more and more users begin to use video on Wi-Fi endpoints, the ability to gracefully manage and scale a continuous, high-quality experience for fluctuating groups of users at any given time or location is critical. Resource reservation control (RRC) provides enhanced capabilities to manage admission and policy controls. Admission and policy decisions are performed based upon the radio frequency measurements, traffic statistics measurements, and

system configurations. Because the availability of bandwidth is limited in the wireless medium, admission control becomes very important to control access and for the efficient use of the available bandwidth. The resource for which the client needs admission is the medium time, which is the air time packets consume in traveling over the air. RRC provides bandwidth protection for the video client by denying requests that would cause oversubscription. Channel usage is used as a metric to determine the capacity and perform admission control. Figure 3 illustrates how RRC works.

Figure 3. RRC Engine



Multicast to Unicast

Native Wi-Fi multicast is not a reliable service. With unicast, acknowledgements (ACKs) help ensure reliability. If no acknowledgement is received, the packet is resent. For multicast there are no ACKs, so the Wi-Fi packet loss rate can be 1 to 2 percent or higher. This unreliability is a problem for streaming video. With multicast-to-unicast conversion, the frames are sent as unicast, allowing the access point to receive ACKs from the clients and to determine when frames need to be retransmitted (in the case of lost or corrupted frames).

By enabling IEEE 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 the best-effort features of traditional wireless networks.

A wireless client application subscribes to an IP Multicast stream by sending an Internet Group Management Protocol (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 collects metrics and traffic policies for the requested stream. If the policies allow the requested stream, a response is sent to the wireless client attached to the access point in order to initiate reliable multicast when 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 these criteria are met, a join response is sent to the access point. At this point 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.

Summary

Cisco Networking Capabilities 2.1 for Medianet further enhances the interaction between media endpoints and the network to improve users' quality of experience while at the same time reducing operating costs by simplifying the deployment and operation of medianets.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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.**

Printed in USA C22-623827-00 10/10