Application Note: Tactical Communications Using Cisco IPICS 2.0 Across High-Latency Networks

Introduction

An emergency by definition is a chaotic event. Whether it is a motor vehicle accident, a crime in progress, or a natural disaster that strikes a wide area, those who are responsible for responding to an emergency require real-time, accurate information in order to effectively manage that situation. This paper discusses the need for effective tactical communications, and how the Cisco® IP Interoperability and Collaboration System (IPICS) meets these challenges. It then presents sample Cisco IPICS architectures over high-latency satellite-based IP networks.

Large-scale emergencies are particularly challenging. Ensuring that proper communications is established among thousands of responders would be difficult enough under normal circumstances, but in such an emergency, the response may be further complicated by the fact that the preexisting communications infrastructure may have been damaged or destroyed by the event, compounding the response challenge.

For those who prepare for and respond to these crises, the emergence of modern technology in tactical operations holds the promise of greater operational effectiveness—but also presents its own set of unique challenges.

Interagency interoperability is critical to the success of the operation. Responding agencies, whether they are traditional first responders (police, fire, and emergency medical services [EMS]), allied agencies (such as power utilities), or nongovernmental organizations (NGOs) such as the Red Cross/Red Crescent, are expected to work efficiently together across wide geographic areas.

In an environment where existing cellular phones, radio repeaters, and other critical infrastructure is unavailable, often the only communications medium that can enable this level of interoperability is satellite.

The Cisco IPICS provides a systems approach to communications interoperability, operations, and emergency management that delivers the right information to the right person in the right format at the right time. Based upon proven IP standards and technology, Cisco IPICS transparently integrates disparate push-to-talk (PTT) networks, providing advanced features without requiring a change in existing operating procedures. It offers a flexible, dynamic, and secure platform that facilitates immediate sharing of information, improves daily enterprise operations, and provides a robust framework for real-time event management while protecting investments in traditional PTT and Land Mobile Radio (LMR) systems.

Cisco IPICS allows these agencies to interoperate and establish an effective span of control in emergency environments. Regardless of whether the user is using a PTT radio, an IP telephone, or a PC-based client, Cisco IPICS allows an unprecedented level of collaboration. Recent enhancements included in Cisco IPICS 2.0 have now brought these advantages to satellite-based IP networks.

Background: Adapting to Lessons Learned from Previous Disasters and Emergencies

Recent emergencies such as the September 11, 2001, attacks and Hurricane Katrina in the United States, the 2005 Pakistan earthquake, and the 2004 Indian Ocean tsunami emphasize the human suffering and economic damage that strike without warning and typify a modern disaster.

Management of a large-scale emergency requires cooperation and collaboration across many different groups: fire departments, police departments, EMS, private organizations, and NGOs. The communications challenges among these groups, however, are daunting. For example, according to COMCARE in United States alone, “today there are more than 100,000 emergency response agencies and the vast majority of them are not able to rapidly, accurately and easily communicate data with each other, much less the public .” Indeed, many emergency response communications systems are not funded if the interoperability of that solution is unaddressed.

Further, although many first responders and NGOs have well-established procedures to deal with day-to-day operations and incidents, often these processes cannot scale to the level required by a major disaster. In such situations, the use of technology in the field helps to scale the response effort. Response organizations of all sizes and functions are in the process of reevaluating their use of technology in the first hours and days of a major emergency.

Lastly, those who fund and provide oversight for disaster response are requiring an increasing amount of accountability for those organizations’ actions. Politicians, donors, and others expect that the resources applied to a disaster response meet the needs of the disaster in the most efficient manner possible.

These lessons from previous emergencies all point toward an increasing reliance upon technology in the field of emergency response. Technology such as that found on computer desktops and modern networking is no longer considered optional for emergency response. In an increasing number of cases, technology is vital to the situational awareness, scalability, and efficiency of a disaster relief operation.

Satellite-Based IP Networks and Tactical Communications

Because of the mobile and unpredictable nature of emergency communications, responders have traditionally relied upon technologies such as LMR and cellular telephones to communicate. Both of these systems have several disadvantages:

- Reliance upon local infrastructure—Radio repeaters and cellular phone towers may not be available to responders after an emergency occurs. The resources may be oversubscribed, destroyed, or even nonexistent.
- Limited communications modes—In many cases, users must use multiple devices for voice, video, and data communications. Those individual devices may be based on proprietary networks that do not interoperate.

Because of these difficulties, many organizations are choosing to deploy satellite-based IP networks for emergency communications. The advantages of having an always-available solution for voice, video, and data communalizations without any reliance on the on-the-ground environment are compelling.

Cisco IPICS Satellite Implementation Scenarios

Several tactical and standard configurations are available for deployment in the field, each having its own challenges. Links from the tactical field unit(s) to users or servers may be over satellite links (geosynchronous or low earth orbit); wireless mesh technology for WiMax; 802.11 or 802.x; Evolution Data Optimized (EVDO) or XR1TT, or similar cellular technology; or an IP-enabled ultra high-frequency (UHF) , very-high-frequency (VHF), or high-frequency (HF) link. In these environments, links can be dynamically degraded based upon the geolocation of the user, weather, RF, or urban canyon interferences. The intricacies of propagation can significantly affect traffic flow.

With half-duplex PTT, the voice network requirements are adjusted to include high latency, very low bandwidth, and highly dynamically variable bandwidth that cannot be accomplished with a standard full-duplex voice network. As long as the network design supports the proper quality of service (QoS) and minimum bandwidth requirements for half-duplex PTT voice (and its control and management overhead), Cisco IPICS 2.0 can function in these networks using a multicast-unicast-multicast (M1:U12:M2, frequently referred to as MUM) configuration. The MUM concept is discussed later in this document.

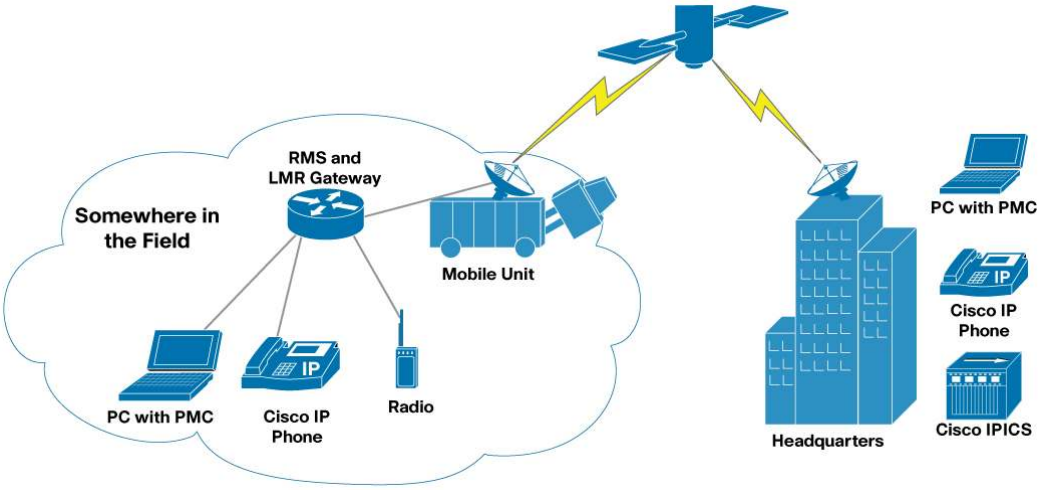
The “Home Server” M1:U12:M2 Configuration

The home-server configuration currently is the most requested field deployment scenario. This configuration maps directly to the built-in Cisco IPICS concept of “locations” or “multicast domains”. “Locations” has the following basic assumptions:

- Most traffic is kept within a location.
- Traffic between locations should be coordinated with knowledge of the underlying network to assure latency and bandwidth.
- Locations are disconnected from other locations, including the core.
- Locations must function in a standalone mode when the core is not available.

In this configuration, the Cisco IPICS server is located in the core at the “back end” of the reach-back. The Cisco Router Media Service (RMS) and Cisco IPICS Media Gateways are deployed forward. This scenario is one of the most common tactical scenarios. The Cisco RMS and the radios are “deployed” and the reach-back is used for the Cisco RMS and client (IP phones and PTT media client PMC) interactions with the Cisco IPICS server. With the Cisco RMS and LMR Gateway in the field, site-based communications can be multicast, and Session Initiation Protocol (SIP) resources are used only by IP phones or PMC clients on “the other side” of the reach-back (refer to Figure 1).

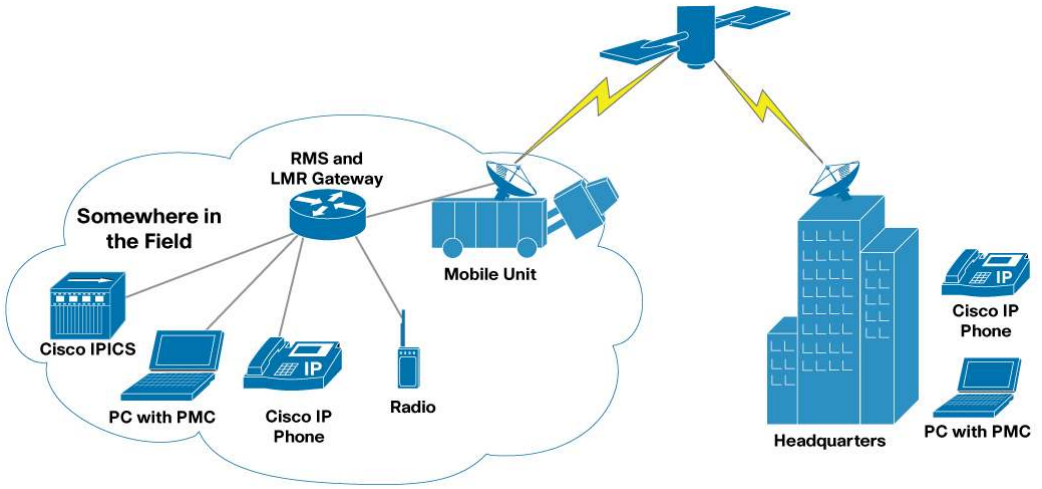
Figure 1. Simplistic “Home Server” Configuration



“All-in-One” M1:U12:M2 Configuration

In this configuration, the Cisco IPICS servers, the Cisco RMS and Cisco IPICS Media Gateways, and clients are on site with the forward-deployed unit. This scenario is generally not affected by the lack of reach-back. However, if the onsite Cisco IPICS server fails, it is important for the PMC or IP phone users to be able to connect through the satellite reach-back to a back-end Cisco IPICS server. In today’s implementation this feature requires manual user intervention on the PMC, and the IP phones have to fail over to the “back-end” Cisco CallManager (refer to Figure 2).

Figure 2. “All-in-One” Configuration



Unique Challenges to Satellite Communications

Satellite-based IP networks present their own challenges that must be accommodated and mitigated in order to establish effective communications:

- For geosynchronous satellite systems, a significant delay is inherent to the satellite link. The round-trip time over a satellite link is more than 540 ms—in addition to any packetization and packet-handling delays.
- The bandwidth over a satellite link is limited, especially when a large number of remote sites are active.

WAN QoS

Like any other voice or video service, there must be an assured QoS on the network. The network must be able to handle certain timing, delay, and bandwidth requirements. This challenge is even greater in an inherently high-latency environment such as geosynchronous satellite communications.

The radio traffic is converted into voice-over-IP (VoIP) traffic by the Cisco IPICS system. Before placing VoIP traffic on a network, it is important to ensure that there is adequate bandwidth for all required applications. When this bandwidth is provisioned, QoS mechanisms (such as differentiated services code point [DSCP] remarking and priority queuing) must be performed on all network device interfaces. The goal of these QoS mechanisms is to ensure reliable, high-quality voice by reducing delay, packet loss, and jitter if a burst of traffic oversubscribes a buffer. A network that is outside of “voice-quality” parameters is not supported for Cisco IPICS. For example, a network that has an overall jitter of more than 250 ms is not supported because voice quality on such a network would be seriously degraded.

Bandwidth Calculation

Properly provisioning the network bandwidth is a major component of designing a successful IP network. Customers can calculate the required bandwidth by adding the bandwidth requirements for each major application (for example, voice, video, and data). This sum then represents the minimum bandwidth requirement for any given link, and it should not exceed approximately 75 percent of the total available bandwidth for the link. This 75-percent rule assumes that some bandwidth is required for overhead traffic, such as routing and Layer 2 keepalive messages.

In addition to using no more than 75 percent of the total available bandwidth for data, voice, and video, the total bandwidth configured for all Low-Latency Queuing (LLQ) priority queues should typically not exceed 33 percent of the total link bandwidth. Provisioning more than 33 percent of the available bandwidth for the priority queue can be problematic for many reasons. First, provisioning more than 33 percent of the bandwidth for voice can result in increased CPU usage. Because each voice call sends 50 packets per second (with 20-ms samples), provisioning for large numbers of calls in the priority queue can lead to high CPU levels due to high packet rates. In addition, a larger percentage of reserved priority bandwidth effectively dampens the QoS effects by making more of the link bandwidth FIFO.

Obviously, for very slow links (for example, less than 192 kbps), the recommendation to provision no more than 33 percent of the link bandwidth for the priority queue(s) might be unrealistic because a single call could require more than 33 percent of the link bandwidth. In these situations, and in situations where specific business needs cannot be met while holding to this

recommendation, it may be necessary to exceed the 33-percent rule. Cisco recommends a minimum of 64 kbps per M1:U12:M2 tunnel, which conservatively allows for a successful transcode of G.711 encoded streams.

In the Cisco IPICS solution, no VoIP call-control signaling is involved except for the remote PMC scenario, which is not recommended because of the large delay over the high-latency satellite link. Thus, when the VoIP bandwidth for Cisco IPICS is calculated, only the bandwidth requirements of the VoIP bearer traffic—Real-Time Transport Protocol (RTP) packets—need to be considered.

As illustrated in Figure 3, a VoIP packet consists of the payload, IP header, User Datagram Protocol (UDP) header, RTP header, and Layer 2 link header.

Figure 3. Typical VoIP Packet

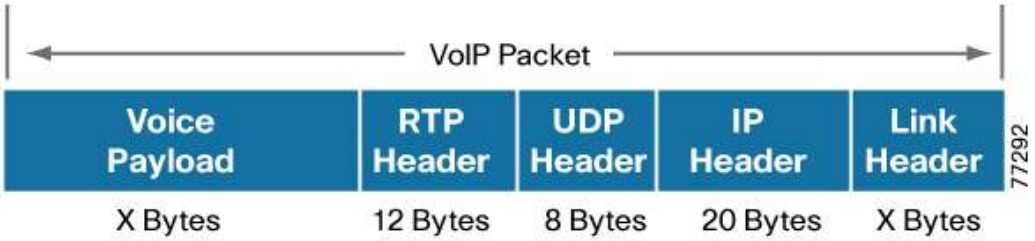


Table 1 lists the bandwidth consumed by the VoIP packets for codecs G.711 and G.729A, respectively, at a default packet rate of 50 packets per second (pps) or 20-ms voice payload.

Table 1. Bandwidth Calculation for Different VoIP Codecs

Codec	Sampling Rate	Voice Payload in Bytes	PPS	IP Bandwidth	Ethernet Bandwidth (14 bytes)	Point-to-Point Protocol (PPP) Bandwidth (6 bytes)
G.711	20 ms	160	50.0	80.0 kbps	85.6 kbps	82.4 kbps
G.729A	20 ms	20	50.0	24.0 kbps	29.6 kbps	26.4 kbps

As sampling size increases, the number of packets per second decreases, resulting in a smaller bandwidth requirement. However, as sample size increases, so does packetization delay, resulting in increased overall end-to-end delay for voice traffic. The trade-off between packetization delay and packets per second must be considered when configuring sample size.

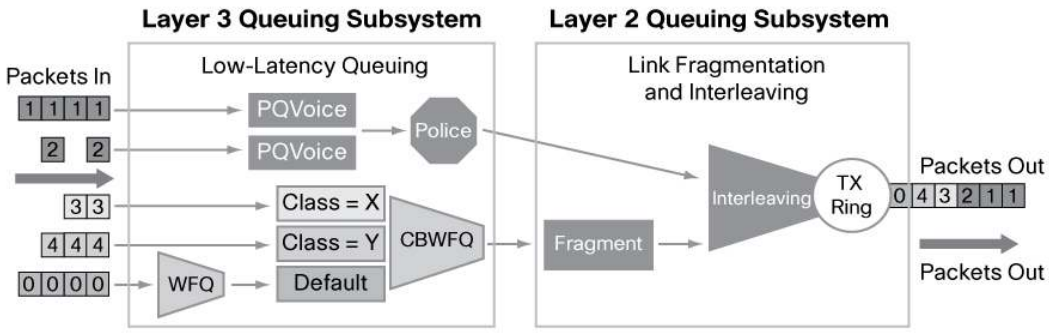
DSCP Remarking and Traffic Prioritization

Cisco recommends the Differentiated Services (DiffServ)-based QoS model for Cisco IPICS high-latency, low-bandwidth applications. In the DiffServ model, IP packets are classified and remarked with appropriate traffic classes before being forwarded to the router output queue. Additionally, Cisco recommends that VoIP traffic use Expedited Forwarding class with an IP Precedence value of 5. By default, the PMC client remarks all VoIP packets with IP Precedence 5. Traffic from ear-and-mouth (E&M) ports can be remarked with IP Precedence 5 by including the following command in the dial-peer configuration statement:

```
ip qos dscp cs5 media
```

In choosing from among the many available prioritization schemes, the major factors to consider include the type of traffic involved and the type of media on the WAN. For multiservice traffic over an IP WAN, Cisco recommends LLQ for VoIP traffic and Class-Based Weighted Fair Queuing (CBWFQ) for different types of data traffic. Figure 4 shows an example prioritization scheme.

Figure 4. LLQ + CBWFQ for Multiservice Traffic over WAN Link



Security

It is important that the IP transport network used to transport voice traffic implements appropriate security that ensures confidentiality, integrity, availability, and accountability of the network while not disrupting protected data transiting the network.

These security elements, delivered by Cisco today in a variety of forms, include the following:

- Extended perimeter security—This element provides the means to control access to critical IP communications applications, such as Cisco IPICS, so that only legitimate IP devices and applications can access the network. Routers and switches with access control lists and stateful firewalls, as well as dedicated firewall appliances, provide the control necessary for extended perimeter security.
- Voice privacy and secure connectivity—To ensure communications privacy and integrity, voice media streams must be protected from eavesdropping and tampering. Data networking technologies such as Layer 2 and Layer 3 access control, stateful firewalls, and VLANs can segment voice traffic from data traffic, preventing access to the voice network (voice VLAN) from the data network (data VLAN). Stateful firewalls broker the connections between the voice and data VLANs, restricting access to only legitimate devices. VPN solutions encrypt voice traffic as it traverses the WAN.
- Intrusion protection—Network-based and host-based intrusion detection systems reside in the voice network to monitor and reactively respond to security events in real time. Using intrusion protection systems, network managers can obtain unprecedented visibility into the network current data stream and security posture.
- Security management—As networks grow in size and complexity, so, too, does the requirement for using centralized tools to manage device, configuration, and security events. Sophisticated tools for managing security policies also enhance the usability and effectiveness of network security solutions. Policy management tools enable users to define, distribute, enforce, and audit the state of security policies through a browser interface.

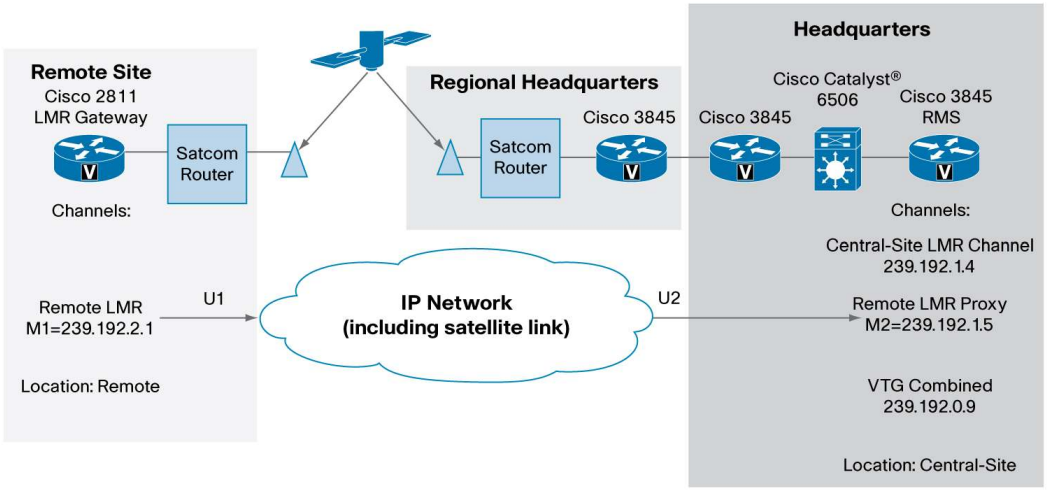
In addition to the appropriate technical tools and architectures referenced previously, an organization must have the appropriate security program in place to develop appropriate security policies, user education, and incident-response procedures. There must also be a process for ensuring that the components of the Cisco IPICS network receive security patches or enhancements in a timely manner.

End-to-end security must also be considered. In a radio-based PTT environment, the “last mile” is often over an unencrypted radio channel that could easily be monitored, and it often is in a place where a hostile user with the right radio could spoof a legitimate user on the radio network. Likewise, although highly available IP networks with redundant paths can be constructed, radio networks usually have significant single points of failure, such as the repeater.

Example: M1:U12:M2 Connection Trunk Concept

Supported Cisco IPICS 2.0 satellite-based configurations require Multicast:Unicast:Multicast (M1:U12:M2) connection trunks to transport real-time multicast voice traffic between Cisco IPICS “islands,” such as that between a central site and a remote location over satellite. This example explains the concept of MUM trunking and how it might apply to a real-world customer (refer to Figure 5).

Figure 5. M1:U12:M2 Connection Trunk for Remote Site



In this example, the remote site has a remote LMR port configured as a channel and the central site has a LMR port configured as a channel. Both locations are configured to be separate multicast domains. The locations that are configured on the Cisco IPICS server represent the two multicast domains, remote and central site.

The LMR channel in the remote site must be configured with location “remote”, and the central-site LMR channel and the RMS in the central site must be configured with location “central site”.

Users in the remote site can communicate with each other using the remote LMR channel. Users at the central site can communicate with each other using the central-site LMR channel.

Interoperating the remote LMR channel with the central-site LMR channel using the RMS in the central site requires the use of a M1:U12:M2 connection trunk, as shown in Figure 5, because interdomain virtual talk group (VTG) is not permitted.

The M1:U12:M2 connection trunk maps the multicast traffic from the remote LMR channel (M1) to a unicast address (U1) to transport this traffic across the IP network. The unicast traffic that is received by the central-site RMS is mapped to the multicast address M2. The M2 multicast address assigned to the remote LMR proxy channel in the central site is placed in a VTG with the central-site channel.M2 should be assigned a valid multicast address in the central-site multicast domain. To avoid conflicts, it should not be an address that is part of the multicast pool or one that is used by any other channel.

- Assume the following IP Multicast ranges:
- 239.192.0.1–60: Channel addresses
- 239.192.1.0–15: VTG addresses Also assume that the following addresses have been allocated:
- 239.192.1.3: Remote LMR channel (M1)
- 239.192.1.4: Central-site LMR channel
- 239.192.1.5: Remote LMR proxy channel (M2)

The remote LMR proxy channel is needed to represent the remote LMR channel in the central-site location. When the VTG called “Combined” is created on the Cisco IPICS server, the VTG contains two channels: central-site LMR and remote LMR proxy. The Cisco IPICS server configures the RMS in the central site (both channels have central-site locations) to mix the two channels to the VTG. Assume that Cisco IPICS uses the multicast address 239.192.0.9 for the VTG. Two pairs of DS-0s are required on the central-site RMS to mix the channels to the VTG and the VTG to the channels.

One limitation of this configuration is that to implement the M1:U12:M2 connection trunk, you must manually configure the central-site RMS and the remote LMR gateway with a pair of loopback T1 controllers. This configuration is needed to transport traffic from the remote LMR channel into the VTG and conversely.

The traffic flow from the remote LMR channel to the VTG and the central-site LMR channel is shown in Figure 6. In this example, a remote user is talking on the remote LMR channel using a radio. The destination address is the multicast address (M1) assigned to the channel when the channel was configured on the Cisco IPICS server. When this traffic reaches the remote LMR gateway with a pair of loopback T1 controllers, it is sent as unicast traffic across the connection trunk to the central-site RMS. The central-site RMS maps the unicast traffic from the remote site to the remote LMR proxy channel, which is mapped to the VTG, which is mapped to the central-site LMR channel. Any users listening on the central-site channel receives the traffic.

Figure 6. Traffic Flow: Remote LMR Channel to VTG and Central-Site LMR Channel

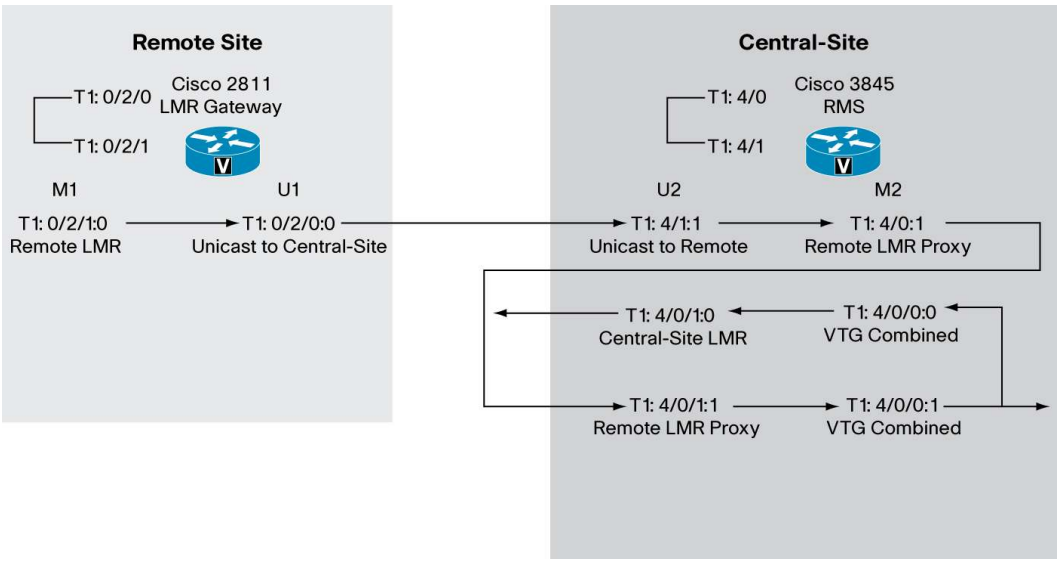
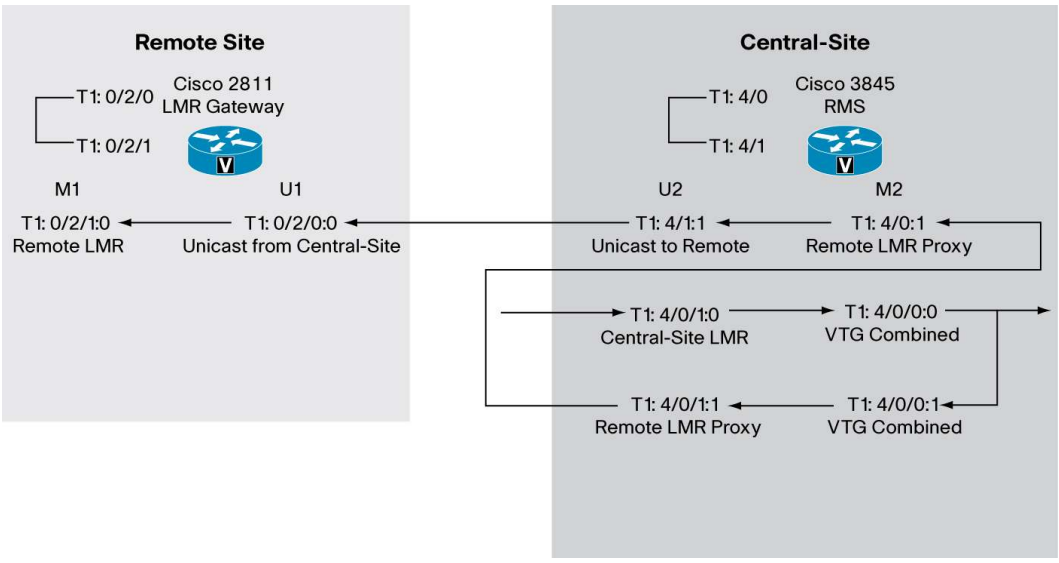


Figure 7 shows the traffic flow from the central-site LMR channel to the remote LMR channel.

Figure 7. Traffic Flow: Central-Site LMR to VTG and Remote LMR



Customers should consider numerous caveats as part of the M1:U12:M2 design before implementing. First, customers should understand that the unicast “trunk” created between the locations over the satellite link have to be replicated between each pair of endpoints. These trunks preclude the dynamic use of the satellite bandwidth and could result in satellite oversubscription, especially if the organization is running multiple sites simultaneously. Additionally, within the M1:U12:M2 architecture it is possible to inadvertently create VTG-to-VTG loops, because there is no assurance of a loop-free topology.

Conclusion

Many enhancements have been made to Cisco IPICS 2.0 to better support satellite-based networks that are commonly found in tactical communications environments. Cisco IPICS now provides enhanced flexibility to customers who are planning high-latency, low-bandwidth implementations.

Careful planning is still required for these implementations, and customers should consider quality, bandwidth, and security variables when planning a Cisco IPICS deployment.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C11-393460-00 03/07

