



## CHAPTER 8

# High Latency and Low Bandwidth Interconnection

---

Cisco IPICS provides support for environments that include high latency and low or variable bandwidth links, such as satellite links. In these types of environments, connectivity may become unstable because of the geographical location of the user, weather elements, and other interferences. Cisco IPICS compensates for these dynamically variable bandwidth scenarios and enhances its support for mobile operations.

Cisco IPICS supports the following deployment scenarios:

- Central site server solution—Supports a Cisco IPICS server that is installed at a central site and a distributed router media service (RMS) and end-user client components that are installed at a remote site.
- Remote locations solution—Supports deployment of the Cisco IPICS server, RMS, and end-user clients at two remote sites that are connected by M1:U12:M2 tunnels.
- Remote PMC solution—Supports a Cisco IPICS server and a distributed RMS at a central site and end-user PMC clients at a remote site.



**Note** With this deployment scenario, remote PMC clients must be configured to use the “Optimize for low bandwidth” setting in the PMC **Settings > Channels** menu. For information about how to configure the PMC for use in this deployment scenario, refer to the “Configuring the PMC Application” chapter in *Cisco IPICS PMC Installation and User Guide, Release 2.1(1)*.

---

The M1:U12:M2 tunneling technology enables these deployment scenarios. For more information about these deployment scenarios, see the “[Supported Deployment Solutions](#)” section on page 8-2.

This chapter includes these topics:

- [Supported Deployment Solutions, page 8-2](#)
- [Requirements and Support Information, page 8-4](#)
- [Performing Additional Configurations on the Cisco IPICS Server, page 8-5](#)
- [Performance Guidelines, page 8-8](#)

# Supported Deployment Solutions

Cisco IPICS enhancements include support for the deployment solutions that are described in the following topics:

- [Central Site Server Solution, page 8-2](#)
- [Remote Locations Solution, page 8-3](#)
- [M1:U12:M2 Configuration Examples, page 8-3](#)

## Central Site Server Solution

In the central site server solution, the Cisco IPICS server is located in a central site and an RMS is distributed with the PMC and other end-user clients in a remote site that is connected via a high latency, low bandwidth connection. In this situation, the Cisco IPICS server must control the distributed RMS, and the dispatcher at the central site needs to be able to communicate with remote PMC clients in the field.

This deployment solution provides the ability to remotely control the RMS over the high latency, low bandwidth links. Communications are enabled by the support of an M1:U12:M2 connection trunk between the RMS in the central site and a remotely-located RMS.

The M1:U12:M2 connection trunk also provides the capability for IP phone XML services and PMC clients to communicate between sites.



### Note

M1:U12:M2 (Multicast1:Unicast1-Unicast2:Multicast2) provides a unicast connection path between two multicast islands. An M1:U12:M2 connection trunk maps multicast to unicast on one side of the network, provides transport over the unicast wide area network (WAN) as a unicast Voice over IP (VoIP) call, and then converts it back to multicast on the other side of the connection, such that multicast 1 is connected to multicast 2 via a unicast connection between 1 and 2. M1:U12:M2 transports only the multicast traffic that is configured on the trunk as contrasted to Generic Routing Encapsulation (GRE) tunnels, which transports all multicast traffic.

See the [“Performing Additional Configurations on the Cisco IPICS Server”](#) section on page 8-5 for additional configurations that apply to this deployment.

### Caveats

Be aware of the following caveats when you use the central site server deployment solution:

- Because all RMS commands flow over the high latency, low bandwidth link, this solution results in reduced throughput and slower response time.
- Some RMS-related operations may take over 3 minutes. Throughput considerations are based on factors such as the number of active channels that are included in the VTGs, the number of DS0s that are being used on the RMS, and the number of PMC users who are communicating between the sites. This limitation is due to inherent Transmission Control Protocol/Internet Protocol (TCP/IP) limitations over high latency, low bandwidth links. For information about RMS configuration updates when you use this deployment solution, see the [“Updating the RMS Configuration”](#) section on page 8-5.
- If you do not have a local router installed at the central site, you may need to configure Address Resolution Protocol (ARP) commands to increase the ARP timer so that the RMS remains reachable. For more information, see the [“Adjusting ARP Commands”](#) section on page 8-6.

- The RMS and the Cisco IPICS server automatic synchronization mechanism must be disabled in this scenario. Therefore, you must manually synchronize these components. For more information about the manual configurations that you must perform, see the [“Disabling the RMS Comparator” section on page 8-6](#) and the [“Merging the Configuration” section on page 8-6](#).
- To conserve bandwidth, you must disable the PMC upload log frequency. For more information, see the [“Disabling the PMC Upload Activity Log Frequency” section on page 8-7](#).
- Although the M1:U12:M2 connection trunk consumes dedicated bandwidth between the central site and the remote site, it does provide for bandwidth optimization by allowing transcoding to the G.729 codec.
- This deployment solution does not support the use of IP phone XML services at the remote locations. IP phone XML services are available only at the central site.
- There is no support for direct PMC access to the remote locations. The PMC clients can be at the remote site or the central site but they cannot remotely connect across sites.

## Remote Locations Solution

In the remote locations solution, a Cisco IPICS server, RMS, PMC, and other end-user clients are located at two remote sites. High latency, low bandwidth links that connect these remote sites enable communications flow.

This deployment enables communications by the use of fixed M1:U12:M2 tunnels that are configured between the channels that are hosted on each RMS at each remote site, such that each channel is mirrored on the other sites.

The M1:U12:M2 connection trunk also provides the capability for IP phone XML services and PMC clients to communicate between sites.

See the [“Performing Additional Configurations on the Cisco IPICS Server” section on page 8-5](#) for additional configurations that apply to this deployment.

### Caveats

Be aware of the following caveats when you use the remote locations deployment solution:

- The M1:U12:M2 connection trunks consume dedicated bandwidth between the remote sites, however bandwidth optimization is enabled by allowing transcoding to the G.729 codec.
- If you use several Cisco IPICS servers that each control their own RMS, care must be taken not to duplicate VTGs when defining channels. Because each channel is mirrored on the other remote site, audio loops can occur between the sites when you use the same VTGs at each site.
- This deployment provides support for IP phone XML services at either the central site or the remote sites. The IP phone XML services must be local to the site where they are deployed.
- There is no support for direct PMC access to the remote locations. The PMC clients can be at the remote site(s) or the central site, but they cannot remotely connect across the sites (they must be local to the site where they are deployed).

## M1:U12:M2 Configuration Examples

The following tables provide configuration examples for the multicast portion of the M1:U12:M2 connection trunks.

For detailed examples that show how to configure the unicast portion of the M1:U12:M2 connection trunk, see [Chapter 7, “Cisco IPICS Deployment Models.”](#)

The two multicast addresses that are being tunneled in the following configuration examples are 239.192.21.3:21000 and 239.192.21.5:21000.

[Table 8-1](#) illustrates the manual commands that are required to configure the voice port and dial peer entries in RMS location #1 to enable the M1 portion of the M1:U12:M2 connection trunk.

**Table 8-1** RMS Location #1 Configuration

RMS Location #1 Voice Port Configuration	RMS Location #1 Multicast Dial Peer M1 Configuration
<pre>voice-port 0/0:1  auto-cut-through  lmr m-lead audio-gate-in  lmr e-lead voice  no echo-cancel enable  playout-delay mode adaptive  playout-delay maximum 250  playout-delay minimum high  playout-delay nominal 100  no comfort-noise  timeouts call-disconnect 3  timing hookflash-in 0  timing hangover 40  connection trunk 2001</pre>	<pre>dial-peer voice 3 voip  destination-pattern 2001  session protocol multicast  session target  ipv4:239.192.21.3:21000                                (RMS M1)  codec g711ulaw vad aggressive</pre>

[Table 8-2](#) illustrates the manual commands that are required to configure the voice port and dial peer entries in RMS location #2 to enable the M2 portion of the M1:U12:M2 connection trunk.

**Table 8-2** RMS Location #2 Configuration

RMS Location #2 Voice Port Configuration	RMS Location #2 Multicast Dial Peer M1 Configuration
<pre>voice-port 0/0:2  auto-cut-through  lmr m-lead audio-gate-in  lmr e-lead voice  no echo-cancel enable  playout-delay mode adaptive  playout-delay maximum 250  playout-delay minimum high  playout-delay nominal 100  no comfort-noise  timeouts call-disconnect 3  timing hookflash-in 0  timing hangover 40  connection trunk 1001</pre>	<pre>dial-peer voice 3 voip  destination-pattern 1001  session protocol multicast  session target  ipv4:239.192.21.5:21000                                (RMS M2)  codec g711ulaw vad aggressive</pre>

## Requirements and Support Information

Cisco IPICS provides the following levels of support:

- Delay—Provides support for up to three seconds end-to-end latency.
- Packet Loss—Supports up to 10% packet loss over the network.

- Jitter buffer—Enables support for up to 250 ms of maximum jitter on the network (to support burst latency).
- Link outages—Provides support for temporary link outages so that if the connection from the PMC is interrupted, the connection automatically continues when it becomes available again. (The PMC user is not informed of the outage.)
- Bandwidth—Supports 64 kbps bandwidth per channel configured over an M1:U12:M2 connection trunk.

#### Caveat

The first time that the PMC logs in to the server, an error message displays to inform the user that the channels are being disabled. This error occurs because of the time delay to connect. To recover from this error, click **OK**. After the server completes its tasks, the channels will display on the PMC (this timing will vary based on latency).

## Performing Additional Configurations on the Cisco IPICS Server

The following additional configurations are required when you use the central site server or the remote locations deployment solution:

- [Updating the RMS Configuration, page 8-5](#)
- [Adjusting ARP Commands, page 8-6](#)
- [Disabling the RMS Comparator, page 8-6](#)
- [Merging the Configuration, page 8-6](#)
- [Disabling the PMC Upload Activity Log Frequency, page 8-7](#)

### Updating the RMS Configuration

When you use the central site or the remote locations deployment solution, you must update every RMS that is configured with Cisco IPICS and that is used over a high latency, low bandwidth connection. This configuration update modifies the maximum TCP outgoing queue on a per-connection basis.

To modify the maximum TCP outgoing queue, perform the following procedure on each RMS:

#### Procedure

- 
- Step 1** Enter global configuration mode by entering the following command:
- ```
Router# configure terminal
```
- Step 2** To set the maximum TCP outgoing queue to 100000 packets, enter the following command:
- ```
Router(config)# ip tcp queuemax 100000
```
- Step 3** To save your configuration, enter the following command:
- ```
Router(config)# write mem
```
- Step 4** To exit the router configuration mode, enter the following command:
- ```
Router# exit
```
-

## Adjusting ARP Commands

If you use the central site server solution and you do not have a local router installed at the central site, you may need to increase the ARP timer in the server. This adjustment helps to prevent timeouts and to ensure reachability between the server and the RMS when these components are connected via Ethernet and separated by a high latency link.

If you encounter issues with ARP timeouts and ping response times, contact the Cisco Technical Assistance Center.

## Disabling the RMS Comparator

The RMS comparator is the mechanism that checks the responsiveness of the RMS and checks whether there have been changes made to the configuration. If there have been changes to the RMS configuration and these changes are not reflected in the Cisco IPICS server, the RMS comparator automatically updates the configuration so that the two components are synchronized.

Because this synchronization mechanism can interject delay, the RMS comparator needs to be manually disabled. To disable the RMS comparator, perform the following procedure.



### Note

---

This change is a global change and affects all RMS components that are configured in the server.

---

### Procedure

- 
- Step 1** Log in to Cisco IPICS the server as a system administrator.
  - Step 2** From the Administration Console, choose **Administration > Options**.
  - Step 3** From the General tab, check the **Disable RMS Comparator** check box that is located in the RMS pane. This change disables the RMS comparator so that it does not run.
  - Step 4** Click **Save** to save your change.
  - Step 5** In the RMS pane, verify that the Disable RMS Comparator check box is checked and that the RMS Polling Frequency field is dimmed.
- 

## Merging the Configuration

After you have disabled the RMS comparator, you must merge the configuration to make sure that the router is synchronized with the server.



### Note

---

As a best practice, make sure that you merge the RMS configuration whenever manual changes have been made to the RMS. This process ensures that the components are synchronized. Perform this procedure before you perform any configuration changes, such as activating a VTG.

---

To merge the configuration, perform the following procedure:

---

**Procedure**

- Step 1** From the Cisco IPICS Administration Console, choose **Configuration > RMS**.
- Step 2** Check the check box that corresponds to the RMS that you need to manage.
- Step 3** From the Configuration drop-down list, choose **Merge** to merge the RMS configuration.  
Wait while this process completes. Cisco IPICS displays the changes in the Edit Router Details area.
- 

## Disabling the PMC Upload Activity Log Frequency

To conserve bandwidth, you must disable the PMC upload log frequency. To disable the PMC upload log frequency, perform the following procedure.



**Note** Be aware that this change is a global change and affects all PMC clients that connect to the server.

---

**Procedure**

- Step 1** Log in to the Cisco IPICS server as a system administrator.
- Step 2** From the Cisco IPICS Administration Console, choose **Administration > Options**.
- Step 3** Click the **PMC** tab to access the PMC configuration options.  
In the Configuration pane, check the **Disable PMC Activity Log Upload** check box.  
This change disables the PMC log upload mechanism so that the PMC clients that are connect to this server never upload their logs to the server.
- Step 4** Click **Save** to save your change.
- Step 5** In the Configuration pane, verify that the Disable PMC Activity Log Upload check box is checked and that the PMC Send Logs on Rollover, PMC Activity Log Update, and PMC Log Upload Frequency fields display as dimmed.
- 

## Adjusting Internet Explorer Browser Settings

When you use a high latency, low bandwidth connection, you may encounter browser timeout errors when you try to update the RMS configuration for any RMS that is configured with 12 or more loopback interfaces.

To resolve this issue, you must modify the Internet Explorer settings on your PC to adjust the timeout duration. This configuration modifies the ReceiveTimeout data value to allow for the additional delay.

**Caution**

Use extreme caution when you modify the registry. If you are not familiar with editing the registry, you should seek technical support assistance before you perform this procedure. If you modify the registry incorrectly, you may need to reinstall the operating system. Therefore, make sure that you back up the registry before you modify it and are aware of how to restore the registry, if a problem occurs.

---

**Tip**

For more information about how to back up, restore, and modify the registry, access the Microsoft Support site and search the Microsoft Knowledge Base for a description of the Microsoft Windows registry.

To modify the ReceiveTimeout data value, perform the following procedure on the PC that you use to access the Cisco IPICS Administration Console:

**Procedure**

- 
- Step 1** On the PC that you use to access the Administration Console, choose **Start > Run**.
- Step 2** In the Open dialog box, enter **regedit**.  
The Registry Editor displays.
- Step 3** Click the + sign that displays next to the **HKEY\_CURRENT\_USER** entry.  
The folders that contain root configuration information for the user who is currently logged in displays.
- Step 4** Click the + signs that display next to each of the folder names to navigate to the **Software\Microsoft\Windows\CurrentVersion\** folder.
- Step 5** Click the + sign that displays next to the **Internet Settings** folder.  
At this point, you have navigated to this folder:  
**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings**.
- Step 6** In the Internet Settings folder, look for the **ReceiveTimeout** name.
- Step 7** To modify this setting, right-click the **ReceiveTimeout** name, then click **Modify**.  
The Edit DWORD Value dialog box displays. The current DWORD value displays in hexadecimal format.  
Alternatively, you can choose to delete the ReceiveTimeout name by clicking **Delete**. If you take this action, be aware that you could wait indefinitely for the server to respond.
- Step 8** Click the **Decimal** radio button to display this value in decimal format.
- Step 9** To configure this value to the recommended setting to accommodate high latency, low bandwidth links, enter **480000** in the Value data field.  
This modification configures the timeout value to 8 minutes.
- Step 10** Click **OK** to save your change.
- Step 11** To exit the Registry Editor, choose **Registry > Exit**.
- Step 12** Restart your PC for the change to become effective.
- 

## Performance Guidelines

Be aware of the following guidelines:

- Each RMS can support a predefined number of commands, such as VTG activation, VTG deactivation, and PMC SIP (remote) connections. If the number of commands that the RMS receives exceeds this threshold, the excess commands fail and must be resubmitted.

- For high latency, low bandwidth deployments, allow 1.5 minutes for every three channel/VTG activations.
- If five dispatchers submit commands, or if the same dispatcher submits several commands, a wait time of 1.5 minutes should be allotted before resubmitting new command requests.
- For constant load conditions, a frequency of about 18 seconds per simple VTG command should be allotted on 2811 routers (RMS components), on average. Additional RMS components must be installed to support above average load conditions.

