Cisco MeetingPlace Express

Networking Provisioning and Configuration

Table of Contents

1 Introduction

This white paper describes information that may be useful when installing Cisco MeetingPlace Express.

This white paper is designed to be used in conjunction with the *Administrator's Installation, Upgrade, and Troubleshooting Guide for Cisco MeetingPlace Express Release 1.1*. It is not intended to be used in place of that guide.

2 Network Provisioning Considerations

Cisco MeetingPlace Express sends and receives a mix of traffic including web conferencing and audio streams. The web conferencing is high bandwidth and the audio streams have severe latency and packet loss requirements. The network needs to be provisioned appropriately to avoid either saturating links, affecting both Cisco MeetingPlace Express and other applications, or damaging the voice quality.

Best practices for provisioning the network for Cisco MeetingPlace Express include the following:

- Make sure that the network is provisioned to expedite voice traffic. This can be done by using Differentiated Services Code Point (DSCP) packet marking or by isolating the voice traffic onto a separate physical network. If using DSCP, make sure that the local switch honors the DSCP marking supplied by Cisco MeetingPlace Express.
- Make sure that your voice gateways properly handle Dual Tone Multifrequency (DTMF) digits and echo cancellation, as described below.
- Assume that Cisco MeetingPlace Express is capable of demanding in excess of 1Mbs for each concurrent web conferencing user, although the average is much less. If your system is licensed for more than about 40 concurrent users, it will probably benefit from a gigabit Ethernet link and network backbone.
- Look for "pinch points" in the network, where multiple users share a relatively slow line. Wide Area Network (WAN) links often act as pinch points. Make sure that those links have adequate bandwidth available for this application as you intend to use it.
- Explicitly configure the Ethernet links rather than relying on auto-negotiation.

2.1 Voice over IP (VoIP) Voice

For good voice quality, Cisco MeetingPlace Express needs to be set up on a network that can provide the following:

- Adequate bandwidth to and from the server for all the voice connections.
- Quality of Service (QOS) or traffic isolation so that other types of traffic will not interfere with the voice streams.
- Low latency between the phone and the server.

2.1.1 Bandwidth Settings

Cisco MeetingPlace Express supports only G.711 (mu-law or a-law). Within the core network, Cisco recommends allowing the end points to use G.711 when communicating with Cisco MeetingPlace Express, without employing a transcoder.

Assuming the default packet size of 20ms, each voice endpoint can send and receive approximately 84Kbs of constant bandwidth traffic, including packet overhead. On a 120 port system, that is an aggregate of approximately 10Mbs each direction at the server. For acceptable voice quality, it is important that this bandwidth always be available, with negligible packet loss or delay, even when sharing links with high bandwidth applications such as web conferencing.

Using Voice Activity Detection (VAD) can reduce the average bandwidth consumed by the voice links. Cisco MeetingPlace Express is compatible with VAD on incoming streams. It can also be configured to use VAD on outgoing streams. Note, however, that outgoing streams from conferences are much less frequently silent than they are in two-way conversations, so the benefit to enabling VAD in Cisco MeetingPlace Express is not substantial – and enabling it will slightly reduce voice quality.

2.1.2 Quality of Service (QOS)

Cisco MeetingPlace Express supports DSCP marking of voice packets. Assuming that the server and the network are properly configured to support DSCP QOS, this has the effect of prioritizing voice packets higher than most other classes of traffic, so that they can get though even when network links are otherwise overloaded.

Some QOS considerations:

- You can configure the server DSCP setting in the Cisco MeetingPlace Express Administration Center under the Call Configuration / Voice Parameters section. The default is Expedited Forwarding (EF), which is the Cisco standard for voice.
- It is common for switches to remark packets from untrusted endpoints to disable DSCP settings. Be sure that packets from your phones and Cisco MeetingPlace Express are not remarked. This may require special configuration of the switch port connected to Cisco MeetingPlace Express.
- Cisco MeetingPlace Express only marks voice data packets (Routing Table Protocol [RTP] and RTP Control Protocol [RTCP]) for DSCP. Signaling packets (SIP or H.323) are not marked and consequently have ordinary priority. Signaling over congested links can result in call setup failures or delays even if the voice connections work fine once established.

2.1.3 Latency

To support high quality conversations, end-to-end latency ("mouth to ear") should not exceed 150ms. A conference call involves two network links and a conference bridge, as opposed to just a single network link for an ordinary phone call, so latency will normally be higher.

In a lecture-style meeting, latency generally does not matter. However, in an interactive discussion, high latency breaks the normal conversation model, causing serious frustration as people attempt to break into a conversation and discover they can't without colliding with someone else. If you are finding that the conversation flow seems unnaturally difficult, it may be because of high latency on one or more of the connections.

Recommendations for limiting latency:

- Provision the network to give priority to voice traffic.
- Do not cascade conferences using multiple bridges.
- Try to minimize the use of VoIP over slow lines.
- Do not route traffic through transcoders or Media Termination Points (MTPs).

2.1.4 Using Voice Gateways

Calls coming in from the Public Switched Telephony Network (PSTN) will need to come through a VoIP gateway to connect to Cisco MeetingPlace Express. Requirements for gateways are more stringent than for two-way voice conversations, assuming high voice quality is desired. In particular:

- Cisco MeetingPlace Express depends on gateways to detect and remove the DTMF tones used for signaling in traditional telephony networks. If the tones are not accurately detected, even in the presence of speech, users will have difficulty entering or controlling meetings. If tones are not fully removed from the incoming stream, users employing in-meeting controls may give other the other meeting participants an earful of noise.
- Cisco MeetingPlace Express works best if DTMF tones are converted into in-band RTP/RFC2833 packets, rather than out-of-band H.245 packets. When using SIP signaling, Cisco MeetingPlace Express only works with RFC2833.
- Cisco MeetingPlace Express depends on the gateway for echo cancellation. Failure to properly cancel echo will result in echo bleeding into the meeting through traditional telephones, yielding unsatisfactory voice quality. Cisco recommends that gateways associated with Cisco MeetingPlace Express provide echo cancellation with a tail of at least 128ms. International calls may benefit from even longer tails.
- If you want to use the Cisco MeetingPlace Express pager notification features or if you wish to navigate through Interactive Voice Response (IVR) systems on outgoing calls through a gateway, the gateway should be configured to convert outgoing RFC2833 digits into real DTMF tones. Cisco MeetingPlace Express will not generate H.245 signals for this purpose.

2.2 Web Conferencing

Cisco MeetingPlace Express web conferencing employs the Macromedia Real-Time Messaging Protocol (RTMP) between the server and Macromedia Flash clients on the desktop. Traffic consists of:

- Screen updates sent by the presenter to the server.
- Screen updates sent by the server to each client.
- Roster updates and meeting control messages.

The aggregate quantity varies considerably due to several factors. In a steady state with no presenters or no screen updates, traffic will average well under 1Kbs per client. In the worst case, with complex, rapidly presented materials, it is possible for Cisco MeetingPlace Express to sustain output in excess of 1Mbs per client, or well over 100Mbs on aggregate in a 120 port system. Since this can severely overload many networks, this traffic needs to be carefully managed.

Factors contributing to traffic characteristics include the following:

- The meeting room bandwidth and resolution settings, which affects how much data is generated by the presenter.
- Individual client bandwidth settings, which affects how much data is sent to the client.
- Per-client bandwidth availability. Back pressure on client links causes data to be discarded.
- Complexity of presentation materials. Complex, high resolution, high color images generate considerably more bandwidth than simple images.
- Number of presenters. Each presenter adds to the traffic for the meeting.
- Rapidity of presenter screen changes. The faster the presenter flips the slides, the more traffic that is generated. You can sustain the maximum traffic by flipping slides at the same rate that the system is capable of transmitting them.
- Size of meeting. If all clients are in the same meeting, output is synchronized for all of them, which yields big traffic bursts. Conversely, if you have lots of small meetings, the traffic is statistically distributed, with smaller peaks and valleys.

2.2.1 Bandwidth Settings

The maximum amount of data generated by Cisco MeetingPlace Express web conferencing can be controlled by the meeting room and client connection settings. As a moderator, you can control the meeting room settings and clients control their own bandwidth settings. These are set by pulling down the Meeting menu while attending a web meeting. *Note that these are manual settings and the system does not attempt to automatically determine optimum values.*

Bandwidth setting options are LAN, DSL, or Modem. For each client, the system uses the lesser of the client’s connection setting or the meeting room setting. Settings are:

Setting	To Server	From Server
LAN	Unlimited	Unlimited
DSL[1]	250Kbs	600Kbs
Modem	28Kbs	40Kbs

Each presenter limits the amount they send to the server to approximately the lesser of that presenter’s client connection setting or the meeting room setting. Likewise, the

[1] The system default setting is “DSL”.

server limits the output to each client according to the lesser of that client's connection setting and the meeting room setting.

For example, say the meeting room is set to DSL, the presenter is set to LAN, one client is set to DSL, and one client is set to Modem.

The meeting room setting of DSL overrides the presenter's LAN setting, so the presenter transmits to the server at a maximum of 250Kbs. The server then retransmits that back to the presenter and to the DSL client as is, and to the Modem client at 40Kbs. To achieve 40Kbs, the system may have to drop some content, depending on the activity level of the presenter.

The resolution setting also controls the traffic by limiting the bits per image. A meeting room set at 640x480 will typically generate less than one third of the traffic at 1280x1024.

2.2.2 Behavior on Slow and Congested Links

Cisco MeetingPlace Express limits client output to a client in two circumstances:

- The client's connection bandwidth setting
- When the server gets an output buffer full condition, typically due to slow or congested links

In both cases, Cisco MeetingPlace Express responds by dropping content. It attempts to do this in a smart fashion, meaning that the client's display is usually still coherent, just not updating as rapidly or dynamically as a faster client.

If the connection is sufficiently congested, which typically only happens on links shared between multiple users or applications, the client eventually gives up and drops its connection. It will attempt to reconnect, but if the conditions have not improved this may not work.

While the difference between output limited by the bandwidth setting versus output limited by congestion is not always obvious, there are several reasons to prefer that the output be limited by the bandwidth. The bandwidth setting should be set appropriately if possible. Advantages of using the bandwidth setting include:

- Generally better responsiveness. When buffers are always full, the latency for client updates is significantly increased.
- Reduced network congestion. The server will be more likely to limit traffic before links are congested.
- Better server performance. Backed-up connections increase memory usage and put a greater load on the processor

Note that congestion does not cause the server to change the bandwidth setting for client.

2.2.3 Roster-Only Meetings

Roster-only meetings, which are meetings with no application sharing, use the same rules as above, but the server does not generate more than about 1Kbs per client.

2.3 End-User Interface and Administration Center

On the whole, Cisco MeetingPlace Express HTTP traffic is neither high bandwidth nor real-time in nature and is relatively insignificant compared to other traffic types. However, during the period when meetings are starting, particularly in the few minutes right after the hour, you should assume many users will hit the server for the purpose of attending a meeting.

The total traffic involved in a client entering a web conference is approximately 400KB downstream and 70KB upstream. This assumes that the client has accessed the server before, so some items are in cache. Included are accessing the main server web page, selecting a meeting, and entering the meeting room, but not any screen sharing. Assuming 120 users, that is an aggregate of about 50MB of output over approximately 5 minutes, or somewhat less than 1Mbs.

In addition to meeting attendance, web pages are used for scheduling and system management. Typical transactions involve a few hundred kilobytes, but some, such as downloading reports, can be arbitrarily large. Compared with attendance, these are low in frequency.

Note that there is no enforced limit on the number of simultaneous web sessions. Access limits are imposed only on voice connections and on web conferencing sessions.

2.4 Downloading and Playing Voice Recordings

Meeting recordings are published in MP3 format and occupy approximately 6MB of disk space per hour. Playback involves downloading the file and it is possible for a substantial number of downloads to be running simultaneously. The speed of the download is limited only by the capacity of the HTTP server and the available bandwidth. The system is designed with the assumption that downloading of recordings is not a frequent activity.

2.5 Wide Area Network (WAN) Considerations

The previous sections in this chapter mostly assume the following:

- Voice connections are across a high capacity core network.
- Web conferencing connections are either across a high capacity core network or on a single-user, single-application link.

Other scenarios that deserve special consideration include:

- Users employing IP voice from outside the core network.
- Users sharing a slow to moderate speed link, perhaps in a satellite office.

2.5.1 Voice over a WAN

Assuming the raw bandwidth is available, external VoIP voice connections should work adequately provided the DSCP packet marking can be honored and preserved by all the equipment, end-to-end. However, it is typical for public Internet connections and virtual private networks to not honor DSCP marking. As a result, it may be necessary to use traditional (PSTN) links and voice gateways to achieve high voice quality for external callers.

Voice end points can reduce their bandwidth usage by employing low-bit-rate coders or compressed headers. Note, however, that Cisco MeetingPlace Express does not natively support any CODEC except G.711; nor does it support compressed RTP. If you wish to use a low-bit-rate coder, you will need to introduce a transcoder. Phone systems like Cisco Call Manager will introduce a transcoding device (part of a media termination point) automatically if one is necessary and available. However, transcoding will reduce voice quality and increase latency.

2.5.2 Web Conferencing over a WAN

The web conferencing engine does a reasonably good job of handling end points that are either on a high performance core network, and thus not sensitive to bandwidth issues, or at the end of a pipe where the available bandwidth is limited primarily by the client end point's local connection (modem or personal DSL link). Situations where multiple clients share a slow or medium speed link are more problematical. An example is where you have several people sharing a T1 line in a branch office.

In the shared line scenario, it is vital for the affected end users or the moderator to set the connection speeds so that Cisco MeetingPlace Express will limit its output without flooding the shared line. Failure to do this can have several negative effects, including:

- Affected clients are likely to behave sluggishly.
- Traffic between Cisco MeetingPlace Express and one client may flood the link sufficiently to cause traffic to another client to fail, resulting in disconnections.
- Other network-based applications may be prevented from performing normally.

2.6 Ethernet Link Configuration

The minimum recommended network link is 100Base-TX, full duplex. Systems with more than about 40 web conferencing licenses will benefit from gigabit Ethernet.

By default, the Cisco MeetingPlace Express Ethernet adapters will auto-negotiate the speed and duplex settings with the switch. However, experience shows this negotiation can result in suboptimal settings and, in some cases, transient link failures and voice dropouts. Consequently, we recommend using hardcoded settings for the link. Make sure that the Cisco MeetingPlace Express and switch settings match.

Ethernet link settings can be configured using the **net** command (described in *Configuration Methods*).

3 Binding of Services and Traffic

This chapter deals with how services are assigned to IP addresses and host names, DNS configuration requirements, and controlling which traffic flows on which port.

The following are some best practices:

- You will need at least two IP addresses and two host names, configured both in Cisco MeetingPlace Express and in Domain Name System (DNS).
- Choose one of the three supported port configuration models.
- If audio is divided onto a separate network, use static route settings to assure traffic will go to the right network.

3.1 Services, IP Addresses, and Hostnames

Some of the services running on Cisco MeetingPlace Express bind to specific IP addresses, as follows:

Services	Binding
End-User Interface and Administration Center (HTTP/S)	HTTP IP address
Web conferencing (RTMP/S)	RTMP IP address
Voice signaling (SIP and H.323)	Any IP address
Audio data (RTP/RTCP)	IP address bound to port 1 (eth0)
Other services[2]	Any IP address

Due to the need to distinguish the HTTP and RTMP traffic and the desire to allow them both to connect using a single firewall-friendly port (80 or 443), it is necessary to assign different IP addresses to these services.

It is further necessary for the HTTP and RTMP IP addresses to have a distinct hostname configured in the DNS. To be sure that service binding works correctly, it is vital that the HTTP and RTMP hostnames, corresponding IP addresses, and domain name are configured the same way in the DNS tables as in the Cisco MeetingPlace Express configuration. Hostnames must match exactly, except for capitalization, or the URLs generated by Cisco MeetingPlace Express will be incorrect.

The only hostname that needs to be exposed to end users is the one for HTTP. Names and addresses associated with the other services are normally transparent.

[2] SSH, SNMP, and NTP

3.2 Configuration Models

Consistent with the above rules, the following configurations can be supported: (Only the voice, HTTP, and RTMP services are listed because the other services can be accessed using any of the IP addresses assigned to the server.)

1. One Ethernet port, two IP addresses:
   a. Primary: HTTP and voice
   b. Secondary: RTMP

2. Two Ethernet ports, two IP addresses:
   a. Port 1 (eth0): HTTP and voice
   b. Port 2 (eth1): RTMP

3. Two Ethernet ports, three IP addresses:
   a. Port 1 (eth0): Voice
   b. Port 2 (eth1), primary: HTTP
   c. Port 2 (eth1), secondary: RTMP

The standard configuration is model 2 and that is the only model supported by the installation software. You can switch to a different model using the **net** command after installation is complete. *Model 2 assumes that both ports have connectivity to all clients.*

With models 2 and 3, if you connect both ports to the same LAN segment you get a redundancy effect where failure of one port will, after a timeout, cause traffic to divert to the other. Note that this mechanism is only supported at the layer 1 network level, so it will not work if you divide the links between different LAN segments.

Choose model 1 only if you have a gigabit Ethernet port or you are sure all the traffic can comfortably coexist on a single 100Mb link. Systems with more than six web conferencing licenses should normally not choose this configuration unless gigabit Ethernet is employed.

Choose model 3 if it is necessary to isolate the audio onto its own link. This choice is offered to support dual-network installations, where the audio is isolated onto its own network. Note the requirement for <u>three</u> distinct IP addresses in this model.

The current configuration options for Cisco MeetingPlace Express do <u>not</u> support the following:

- Separation of user and administrative traffic onto different ports.
- Connecting the two ports onto disjoint networks for security purposes (for example, one port internal and one on a DMZ).

3.3 Binding of Traffic to Ports

With two Ethernet ports, it can be useful to control the type of traffic that flows on each port. For instance, it can be desirable to run the voice on one port and the web conferencing on another, thus separating the high bandwidth traffic from the time critical traffic. The assignment of services to IP addresses and IP addresses to Ethernet ports, described above, can provide good control of incoming traffic. However, this only partially controls how Linux divides outbound traffic.

Cisco MeetingPlace Express only supports traditional Linux (UNIX) packet routing. The simple rule is Linux always sends traffic on the "cheapest" port for the destination. Only the destination IP address is used in this calculation, not the source IP address, TCP, or UDP port. As a result, Cisco MeetingPlace Express does not divide output traffic by type, only by destination IP address.

In cases where the destination IP address is related to the traffic type, it is possible to influence routing using the Linux routing tables. This would be the case, for instance, where voice traffic is separated onto a distinct network, with its own range of IP addresses. In that case, configure the system as follows:

1. Connect Ethernet port 1 (eth0) to the voice network.
2. Connect Ethernet port 2 (eth1) to the "all other traffic" network.
3. Set up the ports and IP addresses using model #3, above.
4. Set a default gateway on Ethernet port 2 to send most traffic to a router connected to Ethernet port 2.
5. Set up a static route, covering the range of audio IP addresses, to send audio traffic to a router connected through Ethernet port 1. Do not assign a default gateway to port 1.

The **net** command can be used to set static routes (described in *Configuration Methods*).

4 Configuration Methods

4.1 During Installation

The Cisco MeetingPlace Express installation program prompts you for the values for the basic configuration parameters for the two Ethernet ports. This sets the system up using method 2 (described in *Configuration Models*).

4.2 Using the *net* Command

After installation, you can use the **net** command to modify the initial configuration settings. To access the **net** command, use SSH to log in to the CLI as the user called *mpxadmin* and then enter **net**.

Notes:

- You do not need to be logged in as root to use the **net** command.
- Shut down the application before changing network settings by entering the following:

  sudo mpx_sys stop
- Most changes take effect after you reboot the system.

The **net** command is menu driven. First, choose option 4, **Configure service bindings**. This lets you select the port model (described in *Configuration Models)*. After selecting the port model, go to the main menu and choose option 1, **List current configuration**. You can change configuration parameters here.

When you quit, the **net** command verifies some of the settings to ensure that they are consistent. If they are not consistent, you can correct them. After that, the **net** command asks if you want to save the configuration before it exits.

Notes when using the **net** command:

- You can safely hit Ctrl-C to get out of the **net** command at any time except briefly at the end while it is saving the configuration.
- If you exit without saving, no changes will be permanent.
- If you set the domain name, the **net** command will strip that name from the end of the hostnames. Do not worry; it will re-append the domain when setting variables that need a fully qualified name.