AudioCodes CPE & Access Gateway Products

MP-20x Series | MediaPack™ Series Telephone Adapters with Integrated Router

Application Note

MP-20x Remote Management Options

Version 2.6.x

AudioCodes
Connecting Networks

Table of Contents

List of Figures

List of Tables

Notice

This document describes the remote management options for AudioCodes MP-20x Telephone Adapter.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: March-08-2009

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the ALT and ◄ keys.

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI², CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are the property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and service are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For Customer support for products purchased directly from AudioCodes, contact support@audiocodes.com.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used, and only Industry standard terms are used throughout this manual.

Related Documentation

Document #	Manual Name
LTRT-505xx	MP-20x Telephone Adapter Release Notes
LTRT-506xx	MP-20x Telephone Adapter User's Manual
LTRT-504xx	MP-20x Telephone Adapter Quick Installation Guide

Revision History

Revision	Date	MP-20x Version	Comments
1	14 August 2008	2.6.x	First edition
2	4 September 2008	2.6.x	TR-069 was added
3	8 March 2009	2.6.x	Descriptions for TR-069/TR-104

Application Note   1. Introduction

1   Introduction

The MP-20x was designed to be mass-deployed by carriers and service providers. One of the keys to guarantee end-user satisfaction and true toll-quality service in mass field deployment is comprehensive remote configuration and management capabilities:

■   "Out-of-the-box" installation at user's site without any manual configuration

■   Automatic and remote configuration updates

■   Automatic and remote firmware updates

■   Remote diagnosis of problems reported by the user

■   Remote collection of statistical information regarding the quality of the service

■   Remote notifications of service problems

This Application Note provides a high-level overview of all the remote management and configuration options offered by the MP-20x series product line. The document is divided into two parts:

■   The first part (Section 2) describes the configuration and management tasks, i.e., what must be configured and managed in the MP-20x (the "what").

■   The second part (Section 3) describes the available configuration and management interfaces and methods (the "how").

Version 2.6.x/2.8.0   7   March 2009

Reader's Notes

2   Configuration and Management

2.1   Configuration

By default, the MP-20x is provided by AudioCodes with factory default settings, which are common to all MP-20x devices (except for the MAC address). The factory settings allows the user to connect to the MP-20x's embedded Web server from the LAN interface.

By default, the WAN interface is configured for DHCP (i.e., automatically obtains its IP address from a DHCP server). In the case of PPPoE or other Internet dialers, this default configuration will not allow the MP-20x to connect to the Internet. The default configuration does not include any VoIP service provider settings (such as a SIP proxy).

In some cases, AudioCodes can ship MP-20x devices that are pre-configured with some customer-specific parameters. This set of parameters is usually defined as the new "factory settings" for this specific customer.

The MP-20x's factory default settings and the current configuration running on the MP-20x are stored on the MP-20x's non-volatile flash memory. The current configuration can be remotely updated using several configuration interfaces (as shown in Figure 2-1):

■   HTTP-based Web server

■   SNMP

■   TR-069

■   Configuration file upload/download

Figure 2-1: Remote Management Interfaces
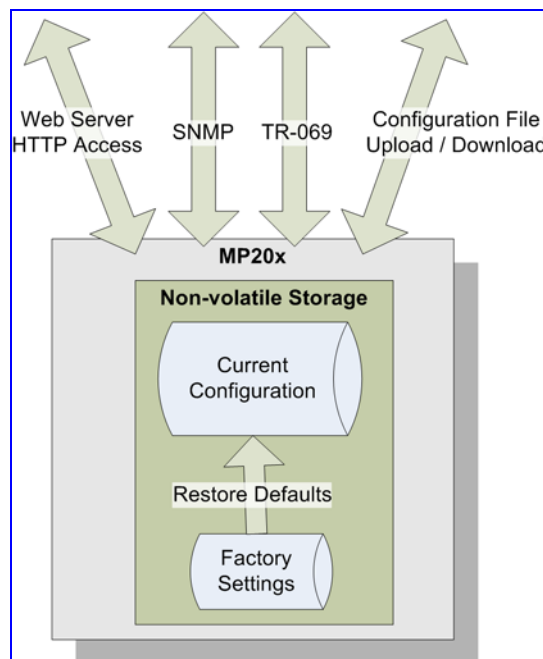
All configuration interfaces access the same internal configuration repository. The configuration file represents the complete set of MP-20x configuration parameters. Specific configuration interfaces (e.g. SNMP and TR-069) might support access only to a sub-set of these configuration parameters.

At any time, the factory settings can be restored using the Web interface or by pressing on the Restore Defaults push-button while the MP-20x is being powered up.

The table below lists the main MP-20x configuration parameter groups:

Table 2-1: Main MP-20x Configuration Parameter Groups

Group	Description
VoIP	Parameters relating to the VoIP functionality of the MP-20x (e.g. analog interface, SIP or MGCP signaling, voice and fax, media streaming)
WAN Interface	The main WAN Internet connection (this group is also referred to as the "Quick Setup").
Network Connections	Configuration of all network connections (LAN and WAN), including advanced connections such as VLANs.
Security	Parameters relating to the MP-20x internal firewall.
QoS	Configuration of Quality of Service parameters such as priorities and traffic shaping.
System / Advanced	Configuration of system parameters such as Remote Update and Remote Access and advanced parameters such as Dynamic DNS, UPnP.

The following list represents a typical set of parameters that a service provider may want to configure:

■ Remote access and/or automatic firmware and configuration update parameters

■ VoIP configuration: SIP proxy, line settings (User IP, Password)

■ QoS parameters (e.g. traffic shaping)

2.2 Remote Management

2.2.1 Firmware Upgrade

Service providers require the ability to update the MP-20x's firmware in the field (e.g. in case of maintenance releases or releases that support new required features). The process is required to be:

■ Automatic, allowing mass update

■ Robust and fail-safe

The MP-20x's firmware is stored in the non-volatile flash memory. The MP-20x's flash memory is capable of storing a recovery firmware that ensures a fail-safe operation (even if the user unplugs the power during the firmware burning process).

The MP-20x's firmware can be upgraded using one of the following mechanisms (refer to Figure 2-2):

■ The new firmware can be "pushed" (uploaded) to the MP-20x, using the embedded Web server

■ The new firmware can be "pulled" (downloaded) by the MP-20x from a remote HTTP, FTP, or TFTP server

Figure 2-2: Firmware Upgrade Mechanisms
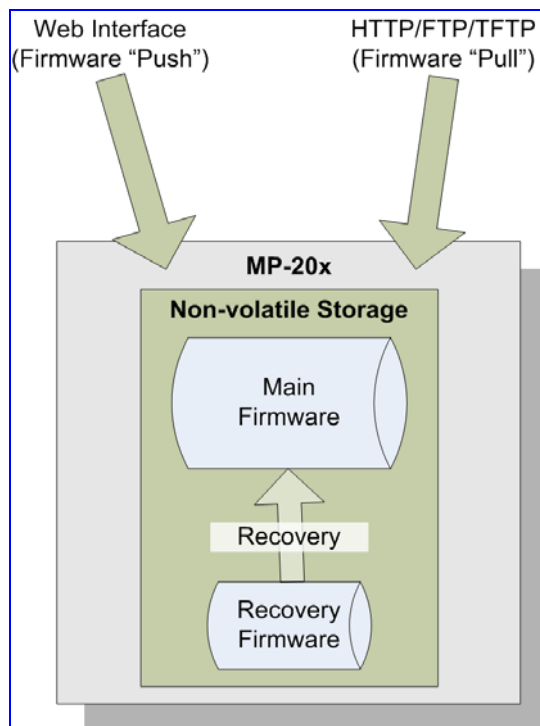
The remote firmware download process can be triggered by one of the following:

■ MP-20x checks for a new firmware upon MP-20x restart

■ MP-20x periodically checks for a new firmware

■ Manual trigger using CLI, TR-069, SNMP, or Web

Note: Unless forced, the MP-20x downloads and upgrades to the new firmware only if its version number is higher than the current firmware version. The version number is not taken from the image file name, but from the header of the image file.

2.2.2 Status and Performance Monitoring

The ability to remotely monitor the status of the MP-20x is critical to the service provider, who wants to support users without having to send a technician on site (avoiding the "truck roll"). The service provider may want to know the current status of the MP-20x (e.g. is it registered to the SIP proxy, is the phone off-hook) or some statistical information (e.g. average packet loss during a call).

The MP-20x maintains a set of status and performance information internally. This information (or parts of it) can be retrieved via the different management interfaces (e.g. Web, SNMP, or TR-069).

The table below describes the status and performance monitoring (statistical) information available in the MP-20x, divided to the main groups.

Table 2-2: Status and Performance Monitoring Parameters

Group	Status and Performance Monitoring Parameters
VoIP	▪ **Current status information per line:** ✔ Phone state ✔ Registration status ✔ Source, codec and type of current call ✔ Packet loss, jitter and delay of current call ▪ **Statistical (min, max, average) information[1]:** ✔ Packet loss, jitter and delay ✔ Out-of-service (e.g. no registration) time ✔ Call establishment time (INVITE to OK)
Network Connections	▪ **Current status information per interface:** ✔ Connection status ✔ Allocated IP address ✔ Received and transmitted packets ▪ **Statistical (min, max, average) information*:** ✔ Out-of-service (e.g. link down) time ✔ Traffic statistics (sent / received bytes, errors)
System	▪ Software version information ▪ Hardware version information ▪ System Up time

---

[1] Supported in the next applicable release.

2.2.3   Alarms, Notifications and Logging

Instead of periodically polling the MP-20x to obtain its current status, the service provider may want the MP-20x to notify abnormal events or to send regular reports to a logging server. Both options are supported by the MP-20x from Version 2.8.0. Table 2-4 shows the relevant interfaces for alarms and notifications.

Note that the terms Alarm and Notification represent the same thing. The difference between alarm/notification and logging is that an alarm is normally used to represent an abnormal event (e.g. registration error), while logged events can represent either regular events (e.g. end of call) or abnormal events. The table below shows the event severity levels defined in the MP-20x. Typically, events with severity of Error or Emergency are notified in addition to being logged.

Table 2-3: Severity of Logged Events

Severity	Description
Debug	Debug-level messages.
Notice	Normal but significant condition. Notices requiring attention at a later time. Non-error conditions that might require special handling.
Error	Recoverable / temporary error condition.
Emergency	System is unusable. The most severe messages that prevent continuation of operation, such as immediate system shutdown.

The table below shows the available notifications and logged events.

Table 2-4: Notifications and Logged Events

Group	Notifications and Logged Events
VoIP	▪ **Notifications:** ✔ Registration error or timeout ▪ **Logged Events:** ✔ End of call (Call Detail Record logging) ✔ SIP messages logging (optional – for debugging)
Network Connections	▪ **Notifications:** ✔ Connection up / down
Security	▪ **Logged Events:** ✔ Security log (configurable)
System	▪ **Notifications:** ✔ System restart ✔ Firmware / configuration update ▪ **Logged Events:** ✔ Debug-level logging (optional)

Reader's Notes

3 Remote Configuration and Management Interfaces

The following interfaces are available on the MP-20x for remote configuration and management:

■ Web server (GUI) over http / https (refer to Section 3.1 on page 16)

■ TR-069 and TR-104 refer to Section 3.2 on page 17)

■ SNMP (refer to Section 3.3 on page 29)

■ Syslog (refer to Section 3.4 on page 32)

■ Firmware or configuration file download via HTTP/ HTTPS / FTP / TFTP (refer to Section 3.5 on page 33)

■ CLI over Telnet / SSH (refer to Section 3.6 on page 35)

The table below lists the possible operations over these different interfaces:

Table 3-1: Operations per Configuration/Management Interface

Operation	Web GUI	TR-069	SNMP	Syslog	File D/L	CLI
Configuration Update	Yes	Yes	Yes[2]	No	Yes	Yes
Firmware Upgrade	Yes	Yes	Yes[3]	No	Yes	Yes
Status Monitoring	Yes	Yes*	Yes[4]	No	No	Yes
Performance Monitoring	Yes[5]	Yes*	Yes[6]	Yes*	No	Yes[7]
Alarms and Notifications	No	Yes*	Yes[8]	Yes	No	No
Debugging and Diagnostics	Yes	No	No	Yes	No	Yes

Service providers can choose to combine several management interfaces, for example, Automatic file download for configuration and firmware updates plus SNMP for alarms.

---

[2] Supported in the next applicable release.
[3] Supported in the next applicable release.
[4] Supported in the next applicable release.
[5] Supported in the next applicable release.
[6] Supported in the next applicable release.
[7] Supported in the next applicable release.
[8] Supported in the next applicable release.

3.1 Embedded Web Server / Web GUI

The MP-20x provides an embedded Web server with a rich Graphical User Interface (GUI). The Web server can be accessed from the local LAN interface (e.g. by the home user) or from the WAN interface (e.g. by the service provider support personnel). The Web GUI provides easy and intuitive configuration of all MP-20x parameters (i.e., VoIP, network interfaces, security, QoS and advanced system settings). In addition, the Web GUI provides status monitoring pages, diagnostic pages and enabled firmware upgrade.

Typically, service providers do not want to configure each MP-20x manually and therefore, they do not use the Web server in live deployments. However, the Web server is still useful for:

■ Trying different configurations in the lab during the integration phases

■ Creating mass-configuration template files

■ Debugging special customer problems (by accessing the Web server from the WAN interface)

3.1.1 Security Concerns and Measures

Since the Web server allows all configuration and management operations, it is important to protect it. The following security measures are available:

■ The Web server is user and password protected. Several users can be defined. A special user with limited-access (only to the Quick Setup) can be defined.

■ The access to the Web server can be blocked from the WAN and/or LAN interfaces.

■ Access to the Web server can be limited to specific IP addresses.

■ Secured HTTP (HTTPS) is supported. It is possible to enable HTTPS-only, if required.

■ The HTTP and/or HTTPS port can be modified (from the default 80 and 8080).

3.2   TR-069 and TR-104 CPE WAN Management Protocol

TR-069 is a relatively new protocol for managing CPE devices over the WAN interface. The standard is published by the DSL Forum. TR-069 runs over SOAP/HTTP and enables device configuration, management (including firmware upgrade), and status monitoring.

TR-104 is an extension of TR-069 for VoIP configuration and monitoring.

TR-069 requires a special server on the service provider's side, called an Auto Configuration Servers (ACS).

The TR standards are published by the DSL forum:

■   TR-069: http://www.broadband-forum.org/technical/download/TR-069.pdf

■   TR-104: http://www.broadband-forum.org/technical/download/TR-104.pdf

Figure 3-1: TR-069 CPE WAN Management Protocol
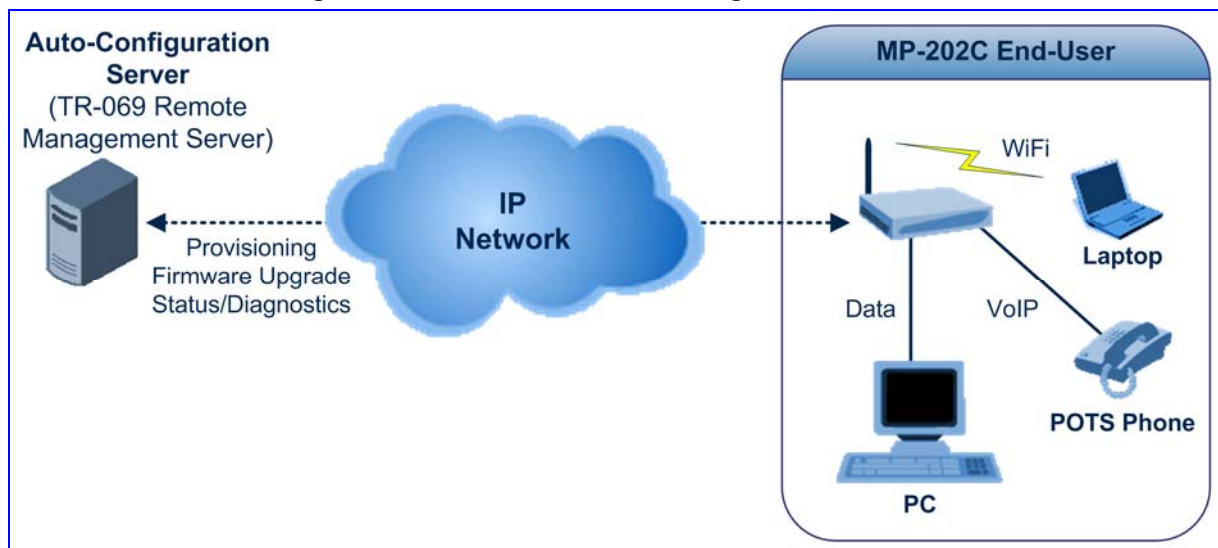
Notes:

- The MP-20x was tested for interoperability with two ACS vendors – Motive and FriendlyTR69. Working with other ACS types may require specific interoperability effort.

- Additional TR-069 and TR-104 parameters will be implemented by MP-20x in Version 3.0.0.

- The parameter values in the subsequent tables are sample values only taken from an ACS.

3.2.1 Configuring MP-20x via TR-069 and TR-104

TR-069 allows basic configuration of the MP-20x. The configuration is defined in a hierarchical tree-like structure according to the TR-069 standard.

3.2.1.1 Configuring the WAN Interface

Table 3-2: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i.WANIPConnection.i

Parameter	Description
AddressingType	The method used to assign an address to the WAN side interface of the CPE for this connection: ▪ "DHCP" ▪ "Static" **Note:** This will be supported in the next applicable release.
ConnectionStatus	Current status of the connection: ▪ "Unconfigured" ▪ "Connecting" ▪ "Connected" ▪ "PendingDisconnect" ▪ "Disconneting" ▪ "Disconnected"
ConnectionType	Specifies the connection type of the connection instance: ▪ "Unconfigured" ▪ "IP_Routed" ▪ "DHCP_Spoofed" ▪ "PPPoE_Bridged" ▪ "PPPoE_Relay" ▪ "PPTP_Relay" ▪ "L2TP_Relay"
DefaultGateway	The IP address of the default gateway for this connection. This parameter is configurable only if the AddressingType is Static. **Note:** This will be supported in the next applicable release.
DNSEnabled	Whether or not the device should attempt to query a DNS server across this connection. **Note:** This will be supported in the next applicable release.
DNSOverrideAllowed	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN. **Note:** This will be supported in the next applicable release.
DNSServers	Comma-separated list of DNS server IP addresses for this connection. Support for more than three DNS Servers is optional. **Note:** This will be supported in the next applicable release.
Enable	Enables or disables the connection instance. On creation of a WANIPConnection instance, it is initially disabled.

Parameter	Description
ExternalIPAddress	The external IP address used by NAT for this connection. This parameter is configurable only if the AddressingType is Static.
MaxMTUSize	The maximum allowed size of an Ethernet frame from LAN-side devices. **Note:** This will be supported in the next applicable release.
Name	User-readable name of this connection.
NATEnabled	Indicates if NAT is enabled for this connection. **Note:** This will be supported in the next applicable release.
PortMappingNumberOfEntries	Total number of port mapping entries.
PossibleConnectionTypes	A comma-separated list indicating the types of connections possible for this connection instance. Each element of the list is an enumeration of: ▪ "Unconfigured" ▪ "IP_Routed" ▪ "IP_Bridged"
RouteProtocolRx	Defines the Rx protocol to be used: ▪ "Off" ▪ "RIPv1" (Optional) ▪ "RIPv2" (Optional) ▪ "OSPF" (Optional)
RSIPAvailable	Indicates if Realm-specific IP (RSIP) is available as a feature on the MP-20x. **Note:** This will be supported in the next applicable release.
ShapingRate	Rate to shape this connection's egress traffic to. If less than or equal to 100, in percentages of the rate of the highest rate-constrained layer over which the packet travels on egress. The rate is limited over the window period specified by ShapeWindow. If greater than 100, in bits per second. A value of -1 indicates no shaping.
SubnetMask	Subnet mask of the WAN interface. This parameter is configurable only if the AddressingType is Static. **Note:** This will be supported in the next applicable release.
SpecVersion	Currently, 1.0 is the only available version.
Uptime	The time in seconds that this connection has been up.

3.2.1.2   Configuring the LAN Interface

Table 3-3: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig

Parameter	Description
Enable	Enables or disables this interface.
MACAddress	The physical address of the interface.
MaxBitRate	The maximum upstream and downstream bit rate available for this connection: ▪ "10" ▪ "100" ▪ "1000" ▪ "Auto"
Status	The status of the interface: ▪ "Up" ▪ "NoLink" ▪ "Error" ▪ "Disabled"

Table 3-4: InternetGatewayDevice.LANDevice.i.LANHostConfigManagement

Parameter	Description
AllowedMACAddresses	Represents a comma-separated list of hardware addresses that are allowed to connect to this connection if MACAddressControlEnabled is 1 for a given interface.
DHCPLeaseTime	Specifies the lease time in seconds of client assigned addresses. A value of -1 indicates an infinite lease. **Note:** Will be supported in the next applicable release.
DHCPRelay	Determines if the DHCP server performs the role of a server (0) or a relay (1) on the LAN interface. **Note:** Will be supported in the next applicable release.
DHCPServerEnable	Enables or disables the DHCP server on the LAN interface.
DNSServers	Comma-separated list of DNS servers offered to DHCP clients. Support for more than three DNS Servers is optional.
DomainName	Sets the domain name for clients on the LAN interface. **Note:** Will be supported in the next applicable release.
IPRouters	Comma-separated list of IP addresses of routers on this subnet. Also known as default gateway. Support for more than one Router address is optional. **Note:** Will be supported in the next applicable release.
MaxAddress	Specifies the last address in the pool to be assigned by the DHCP server on the LAN interface.

Parameter	Description
MinAddress	Specifies the first address in the pool to be assigned by the DHCP server on the LAN interface.
SubnetMask	Specifies the client's network subnet mask.

3.2.1.3   Configuring VoIP via TR-104

Table 3-5: InternetGatewayDevice.Services.VoiceService.i.Capabilities

Parameter	Description
ButtonMap	Support for a configurable button map. A true value indicates support for a configurable button map via the VoiceService.{i}.VoiceProfile.{i}.ButtonMap object.
DSCPCoupled	A true value indicates that the CPE is constrained such that transmitted call control packets use the same DSCP marking as transmitted RTP packets. If the value is true, the CPE must not support the DSCPMark parameter for call control.
EthernetTaggingCoupled	A true value indicates that the CPE is constrained such that transmitted call control packets use the same Ethernet tagging (VLAN ID Ethernet Priority) as transmitted RTP packets. If the value is true, the CPE must not support the VLANIDMark or EthernetPriorityMark parameters within a call control object (e.g., SIP, MGCP, or H323).
FaxPassThrough	Support for fax pass-through. A true value indicates support for the parameter VoiceService.{i}.VoiceProfile.{i}.FaxPassThrough.
FaxT38	Support for T.38 fax. A true value indicates support for the object VoiceService.{i}.VoiceProfile.{i}.FaxT38.
MaxLineCount	Maximum number of lines supported across all profiles.
MaxProfileCount	Maximum number of distinct voice profiles supported.
MaxSessionCount	Maximum number of voice sessions supported across all lines and profiles. (This might differ from MaxLineCount if each line can support more than one session for CPE provided conference calling. This value can be less than the product of MaxLineCount and MaxSessionsPerLine.)
MaxSessionsPerLine	Maximum number of voice sessions supported for any given line across all profiles. A value greater than one indicates support for CPE provided conference calling.
ModemPassThrough	Support for modem pass-through. A true value indicates support for the parameter VoiceService.{i}.VoiceProfile.{i}.ModemPassThrough.
NumberingPlan	Support for a configurable numbering plan. A true value indicates support for a configurable numbering plan via the VoiceService.{i}.VoiceProfile.{i}.NumberingPlan object.

Parameter	Description
PSTNSoftSwitchOver	A true value indicates the MP-20x is capable of supporting the PSO_Activate Facility Action, which allows a call to be switched to a PSTN FXO. **Note:** Currently, FXO is not supported.
Regions	Comma-separated list of geographic regions supported by the MP-20x. Each item in the list must be an alpha-2 (two-character alphabetic) country code as specified by ISO 3166. An empty list indicates that the MP-20x does not support region-based customization. **Note:** This format is currently not supported.
RingGeneration	Support for ring generation. A true value indicates support for control of ring generation via the VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Ringer object. A true value also indicates that the RingDescriptionsEditable, PatternBasedRingGeneration and FileBasedRingGeneration parameters in this object are present.
RTCP	Support for RTCP.
RTPRedundancy	Support for RTP payload redundancy as defined in RFC 2198. A true value indicates support for VoiceService.{i}.VoiceProfile.{i}.RTP.Redundancy.
SignalingProtocols	Signal protocol: ▪ "SIP" ▪ "MGCP" Each entry can be appended with a version indicator in the form "/X.Y". For example: "SIP/2.0". **Note:** Only one protocol is supported at a time.
SRTP	Support for SRTP. **Note:** Currently, SRTP is not supported.
ToneGeneration	Support for tone generation. A true value indicates support for the object VoiceService.{i}.VoiceProfile.{i}.Tone. A true value also indicates that the ToneDescriptionsEditable, PatternBasedToneGeneration and FileBasedToneGeneration parameters in this object are present.
VoicePortTests	Support for remotely accessible voice-port tests. A true value indicates support for the VoiceService.{i}.PhyInterface.{i}.Tests object.

Table 3-6: InternetGatewayDevice.Services.VoiceService.i.Capabilities.Codecs

Parameter	Description
Codec	Identifier of the type of codec.
EntryID	Unique identifier for each entry in the table.
PacketizationPeriod	Comma-separated list of supported packetization periods (in milliseconds), or continuous ranges of packetization periods. Ranges are indicated as a hyphen-separated pair of unsigned integers.
	For example:
	▪ "20" indicates a single discrete value.
	▪ "10, 20, 30" indicates a set of discrete values.
	▪ "5-40" indicates a continuous inclusive range.
	▪ "5-10, 20, 30" indicates a continuous range in addition to a set of discrete values.
	A range must only be indicated if all values within the range are supported.
	Note: Currently, only a single ptime per codec is supported.

Table 3-7: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile

Parameter	Description
DTMFMethod	Method by which DTMF digits must be passed:
	▪ "InBand"
	▪ "RFC2833"
	▪ "SIPInfo
Enable	Enables or disables all lines in this profile, or places it into a quiescent state:
	▪ "Disabled"
	▪ "Quiescent"
	▪ "Enabled"
	On creation, a profile must be in the Disabled state.
	In the Quiescent state, in-progress sessions remain intact, but no new sessions are allowed. Support for the Quiescent state in a MP-20x is optional. If this parameter is set to "Quiescent" in a MP-20x that does not support the Quiescent state, it must treat it the same as the Disabled state.
Name	String to easily identify the profile instance.
	Note: Currently, this is not supported.
NumberOfLines	Number of instances of Line within this VoiceProfile.

Table 3-8: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.SIP

Parameter	Description
OutboundProxy	Host name or IP address of the outbound proxy. If a non-empty value is specified, the SIP endpoint must send all SIP traffic (requests and responses) to the host indicated by this parameter and the port indicated by the OutboundProxyPort parameter. This must be done regardless of the routes discovered using normal SIP operations, including use of Route headers initialized from Service-Route and Record-Route headers previously received. The OutboundProxy value is not used to generate the URI placed into the Route header of any requests.
OutboundProxyPort	Destination port for connecting to the outbound proxy. This parameter must be ignored unless the value of the OutboundProxy parameter in this object is non-empty.
ProxyServer	Host name or IP address of the SIP proxy server.
ProxyServerPort	Destination port for connecting to the SIP server.
ProxyServerTransport	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
RegisterExpires	Register request Expires header value (in seconds).
RegistrarServerTransport	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
UserAgentPort	Port for incoming call control signaling.
UserAgentTransport	Transport protocol for incoming call control signaling.

3.2.1.4 Upgrading Firmware via TR-069

TR-069 contains a built-in mechanism for MP-20x device firmware upgrade.

3.2.2 Monitoring the MP-20x Status via TR-069 and TR-104

The service provider can monitor the status of the MP-20x via TR-069 and TR-104.

3.2.2.1 Device Information

Table 3-9: InternetGatewayDevice.DeviceInfo

Parameter	Description
Description	A full description of the MP-20x device (string).
DeviceLog	Vendor-specific log(s).
HardwareVersion	A string identifying the particular MP-20x model and version.
Manufacturer	A string identifying the manufacturer of the MP-20x, i.e., AudioCodes.
ManufacturerOUI	Organizationally unique identifier of the device manufacturer. Represented as a six hexadecimal-digit value using all upper-case letters and including any leading zeros.
ModelName	A string identifying the model name of the MP-20x.
ProductClass	Identifier of the class of product for which the serial number applies. That is, for a given manufacturer, this parameter is used to identify the product or class of product over which the SerialNumber parameter is unique.
ProvisioningCode	Identifier of the primary service provider and other provisioning information, which may be used by the Server to determine service provider-specific customization and provisioning parameters.
	If non-empty, this argument must be in the form of a hierarchical descriptor with one or more nodes specified. Each node in the hierarchy is represented as a 4-character sub-string, containing only numerals or upper-case letters. If there is more than one node indicated, each node is separated by a "." (dot). For example, "TLCO" and "TLCO.GRP2".
SerialNumber	Serial number of the MP-20x.
SoftwareVersion	A string identifying the software version currently installed in the MP-20x.
	To allow version comparisons, this element must be in the form of dot-delimited integers, where each successive integer represents a more minor category of variation. For example, 3.0.21 where the components mean Major.Minor.Build.
UpTime	Time in seconds since the MP-20x was last reset.

3.2.2.2   WAN Status

Table 3-10: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i. WANIPConnection.i.Stats

Parameter	Description
EthernetBytesReceived	Total number of bytes received over all connections within the same WANConnectionDevice that share a common MAC address since the MP-20x was last reset.
EthernetBytesSent	Total number of bytes sent over all connections within the same WANConnectionDevice that share a common MAC address since the MP-20x was last reset.
EthernetPacketsReceived	Total number of Ethernet packets received over all connections within the same WANConnectionDevice that share a common MAC address since the MP-20x was last reset.
EthernetPacketsSent	Total number of Ethernet packets sent over all connections within the same WANConnectionDevice that share a common MAC address since the MP-20x was last reset.

3.2.2.3   LAN Status

Table 3-11: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig.i.Stats

Parameter	Description
BytesReceived	Total number of bytes received over the interface since the MP-20x was last reset.
BytesSent	Total number of bytes sent over the interface since the MP-20x was last reset.
PacketsReceived	Total number of packets received over the interface since the MP-20x was last reset.
PacketsSent	Total number of packets sent over the interface since the MP-20x was last reset.

3.2.2.4   VoIP Status via TR-104

Table 3-12: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.Line.i.Stats

Parameter	Description
ResetStatistics	When set to one, it resets the statistics for this voice line. Always False when read.
PacketsSent	Total number of RTP packets sent for this line.
PacketsReceived	Total number of RTP packets received for this line.
BytesSent	Total number of RTP payload bytes sent for this line.
BytesReceived	Total number of RTP payload bytes received for this line.
PacketsLost	Total number of RTP packets that have been lost for this line.
Overruns	Total number of times the receive jitter buffer has overrun for this line.
Underruns	Total number of times the receive jitter buffer has underrun for this line.
IncomingCallsReceived	Total incoming calls received.
IncomingCallsAnswered	Total incoming calls answered by the local user.
IncomingCallsConnected	Total incoming calls that successfully completed call setup signaling.
IncomingCallsFailed	Total incoming calls that failed to successfully complete call setup signaling.
OutgoingCallsAttempted	Total outgoing calls attempted.
OutgoingCallsAnswered	Total outgoing calls answered by the called party.
OutgoingCallsConnected	Total outgoing calls that successfully completed call setup signaling.
OutgoingCallsFailed	Total outgoing calls that failed to successfully complete call setup signaling.
CallsDropped	Total calls that were successfully connected (incoming or outgoing), but dropped unexpectedly while in progress without explicit user termination.
TotalCallTime	Cumulative call duration (in seconds).
ServerDownTime	The number of seconds the MP-20x is unable to maintain a connection to the server. Applies only to SIP.
ReceivePacketLossRate	Current receive packet loss rate (in percentage).
FarEndPacketLossRate	Current far-end receive packet lost rate (in percentage).
ReceiveInterarrivalJitter	Current receive interarrival jitter (in microseconds).
FarEndInterarrivalJitter	Current Interarrival jitter (in microseconds) as reported from the far-end device via RTCP.
RoundTripDelay	Current round-trip delay (in microseconds).
AverageReceiveInterarrivalJitter	Average receive interarrival jitter (in microseconds) since the beginning of the current call.

Parameter	Description
AverageFarEndInterarrivalJitter	Average far-end interarrival jitter (in microseconds) since the beginning of the current call.
AverageRoundTripDelay	Average round-trip delay (in microseconds) since the beginning of the current call. This is the average of the RoundTripDelay statistics accumulated each time the delay is calculated.

3.2.3   Security Concerns and Measures

The CPE WAN Management Protocol is designed to allow a high degree of security in the interactions that use it. The CPE WAN Management Protocol is designed to prevent tampering with the transactions that take place between a CPE and ACS, provide confidentiality for these transactions, and allow various levels of authentication.

The following security mechanisms are incorporated in this protocol:

■ The protocol supports the use of SSL/TLS for communications transport between CPE and ACS. This provides transaction confidentiality, data integrity, and allows certificate-based authentication between the CPE and ACS.

■ The HTTP layer provides an alternative means of CPE authentication based on shared secrets.

3.3   SNMP

Simple Network Management Protocol (SNMP) is used in network management systems to configure and monitor network-attached devices. SNMP is an IETF standard defined by RFC 1157, 1441 and additional RFCs for specific Management Information Base (MIBs).

The MP-20x contains an embedded SNMP agent and supports SNMPv1, SNMPv2 and partially supports SNMPv3. For monitoring of the network interfaces, the standard SNMP MIB-II (RFC 1213) is supported. For more options, a proprietary MIB will be defined (for SW version 2.8.0) by AudioCodes for the MP-20x product line – the acMP20x MIB. The MIB is divided to the following sections:

■   **acMP20xConfig:** for changing the MP-20x's configuration

■   **acMP20xStatus:** for monitoring the MP-20x's status

■   **acMP20xAlarms:** for receiving notifications (alarms) from the MP-20x

The figure below shows the SNMP network architecture:

Figure 3-2: SNMP Network Architecture
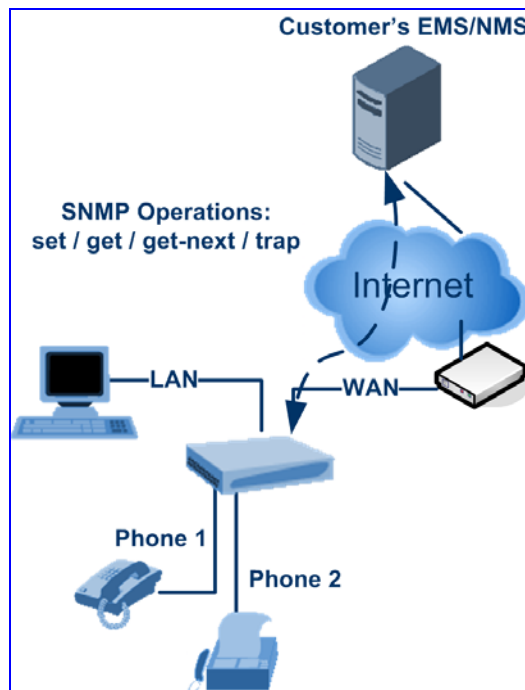
3.3.1 Configuring the MP-20x via SNMP

The acMP20xConfig MIB section is structured in a similar hierarchy as the MP-20x's Web GUI. Each parameter in the MIB has a matching parameter in the Web GUI and a matching parameter in the gateway's configuration file. The MIB file defines the valid range and the default value for each parameter. Typically, the customer will integrate the MP20x MIB into the customer's Network Management System (NMS) to automate the configuration process.

> **Notes:**
>
> - For SW version 2.8.0, only the VoIP parameters and the Quick Setup parameters are defined. Other parameters (e.g. Security, QoS) must be configured in other methods or using a special generic set object in the MP20x MIB (acMP20xConfigParamPath/ acMP20xConfigParamValue).
>
> - A special MIB object is defined to allow MP-20x firmware upgrade triggered by SNMP. The object acMP20xRemoteUpdate triggers a remote upgrade from the SNMP-configured URL.

3.3.2 Monitoring the MP-20x via SNMP

SMNP can be used to monitor the status of the MP-20x. VoIP-related monitoring is performed via the proprietary MIB acMP20x. Other parameters are available in the standard MIB-II.

3.3.2.1 VoIP Monitoring

The acMp20xStatus section allows the service provider to get the current MP-20x status. The list below shows the available objects.

```
acMP20xStatus
    acMP20xStatusVoIP
        acMP20xStatusVoIPLinesTable
            acMP20xLinePhoneState – on-hook / off-hook / ringing
            acMP20xLineRegistrationState – not registered /
            registered / registration error
            acMP20xLineCallsTable
                acMP20xCallOrigine – Incoming / outgoing
                acMP20xCallRemoteNumber – Remote phone number
                acMP20xCallRemoteID – Remote SIP ID
                acMP20xCallDuration – Call duration in ms
                acMP20xCallType – Voice/Fax/Modem
                acMP20xCallEncoder – Tx codec type
                acMP20xCallDecoder – Rx codec type
                acMP20xCallPacketsSent – Number of RTP
                packets sent
                acMP20xCallPacketsReceived – Number of RTP
                packets sent
                acMP20xCallBytesSent – Number of payload
                bytes sent
                acMP20xCallBytesReceived – Number of payload
                bytes received
                acMP20xCallPacketsLost – Number of packets lost
```

<pre>
                              acMP20xCallLostPercentage – Packet loss
                              percentage
                              acMP20xCallJitter – Average call jitter in ms
                              acMP20xCallRoundTripDelay – Average call
                              round-trip delay in ms
</pre>

3.3.2.2   Network Interfaces and System Monitoring

Status monitoring of the system and network interfaces can be done via the standard MIB-II (iso(1).org(3).dod(6).internet(1).mgmt(2).mib-2(1)). The following table shows some of the information elements available via MIB-II:

Table 3-13: Information Elements Available via MIB-II

Section	Available Information
system	▪ Description ▪ Version Information ▪ Up-time
interfaces	**Information per network interface:** ▪ Description ▪ Type ▪ Speed ▪ MAC address ▪ Traffic statistics ▪ Errors
ip	Assigned IP addresses and IP-related parameters
icmp, udp, tcp	Transport-protocol specific statistical information
ifMIB	Information about network interfaces per RFC 2233

3.3.3   Security Concerns and Measures

Since SNMP allows write-access to configuration parameters, it is important to protect this interface. The following security measures are available:

■   A community string (password) can be defined for read-only access and for read/write access.

■   It is possible to limit access to SNMP to a trusted peer (single IP address or a range of addresses).

■   SNMPv3 provides an significant security improvement over SNMPv1/2. Version 2.8.0 will support SNMPv3 and will allow the service provider to configure SNMPv3 security parameters.

■   SNMP traffic can be allowed over an IPSec secured connection – check availability with AudioCodes.

3.4   Syslog

Syslog is a standard protocol for reporting and logging of messages over IP network and is defined by RFC 3164. The MP-20x enables the service provider to configure a Syslog server and a severity level above which errors are sent to the server. Typically, only error-level messages should be sent to the Syslog server (in order not to flood it with irrelevant debug-level information). For debugging, it is possible to temporarily allow logging for debug-level messages (e.g. for SIP messages).

Many free Syslog servers exist, including Kiwi Syslog Daemon' (http://www.kiwisyslog.co'm http://www.kiwisyslog.com).

Refer to Section 2.2.3 on page 12 for information about the existing severity levels and logged events in the MP-20x.

> **Note:**   The logged events are being re-defined in Version 3.0.0

3.4.1   Security Concerns and Measures

Since Syslog is only used to output messages from the MP-20x, it does not contain any security concerns.

3.5   Automatic File Download

A practical, straight-forward and easy to implement method for mass configuration and firmware update is automatic file download from a remote file server (via HTTP, FTP, or TFTP). This method is used by many service providers.

3.5.1   Firmware File Download

The MP-20x's firmware files contain information about the target product type and the firmware version information. See Section 2.2.1 on page 10 for information about the basic mechanism and the type of management interfaces that can be used to trigger firmware file download.

3.5.2   Configuration File Download

The MP-20x supports two configuration file formats – a .conf file and an .ini file. Both files define the same parameters, but in a different format; the .conf file has a hierarchical tree-like structure and the .ini file is flat (defining the full path for each parameter).

As with the firmware file, the configuration file can be "pushed" to the MP-20x via the Web server or "pulled" by the MP-20x from a remote server. This section refers only to the second option.

When the MP-20x downloads a file from a remote server, it performs the following actions:

■   Decrypts the file if it is encrypted.

■   Checks that the file version is later than the current configuration file version (if it is not later, the new configuration is not used).

■   Checks the software version with which the configuration file was created (if the file was created with a later software version, it is not used).

■   Merges the configuration file with the current configuration:

   •   Parameters that appear in the new file are modified or added

   •   Parameters that do not appear in the new file remain in their existing value

---

Notes:

   •   It is recommended that the configuration file (that is downloaded from the network), contains only the small subset of parameters that the service provider needs to update remotely.

   •   To create the configuration file, it is recommended to use a MP-20x that is restored to the factory settings, modify the required parameters using the Web GUI and then upload the configuration file from the MP-20x with the option to get only the modified configuration fields enabled.

3.5.3   Security Concerns and Measures

The main security hazard in automatic file download is that a hacker can force the MP-20x to download a file from the hacker's server instead of the service provider's legitimate server. Another concern is exposing information such as the SIP proxy IP address and user and password information in the configuration file (if the hacker is sniffing the network).

The following security measures are available to prevent this:

■   The configuration file can be encrypted using 3DES with pre-configured key. This prevents the user from learning the format of the file and obtaining information from it.

■   HTTPS can be used to further encrypt the transport.

■   HTTPS certificates can be used to allow the MP-20x to authenticate the server and also to prevent the user from acquiring the file from the server.

3.6   Telnet CLI

The MP-20x features a Command Line Interface (CLI) over Telnet. The CLI enables the service provider to manage the MP-20x (e.g. reboot, force a firmware upgrade), to obtain information about the status of the device (e.g. VoIP calls, network interfaces, version information), to change the configuration and to perform different debugging tasks (e.g. enable debug logging, enable packet recording).

Typically, the CLI interface is only used for debugging and diagnostics since it does not allow mass configuration and monitoring.

For additional information about debugging and diagnostic tools, refer to *LTRT-58201 MP-20x Debugging and Diagnostic Tools Application Note Ver 2.6.1*.

3.6.1   Security Concerns and Measures

Since the CLI allows all configuration and management operations, it is important to protect it. The following security measures are available:

■   The CLI is user and password protected (same as the Web).

■   Telnet access can be blocked from the WAN and/or LAN interfaces.

■   It is possible to limit Telnet access to specific IP addresses.

■   Future versions will support SSH.

Application Note

MP-20x Remote Management Options

Version 2.6.x/2.8.0