

Figure 13-5: Create Self Signed X509 Certificate Screen

- c. Enter the fields as required, and then click **Generate**; a message appears notifying you that MP252 is generating the certificate.
- d. After a few moments, click **Refresh**; the 'New Self Signed X509 Certificate' screen appears.

Figure 13-6: New Self Signed X509 Certificate Screen

- e. Click **OK**; the new certificate appears listed in the 'Certificates' screen.

Figure 13-7: Newly Created Self-Signed Certificate

Name	Issuer	Action
AudioCodes	CN=MP202, O=AudioCodes, C=US, CN=AudioCodes	
gateway	CN=mp252, O=company, ST=OR, C=US, CN=gateway	
Upload Certificate		


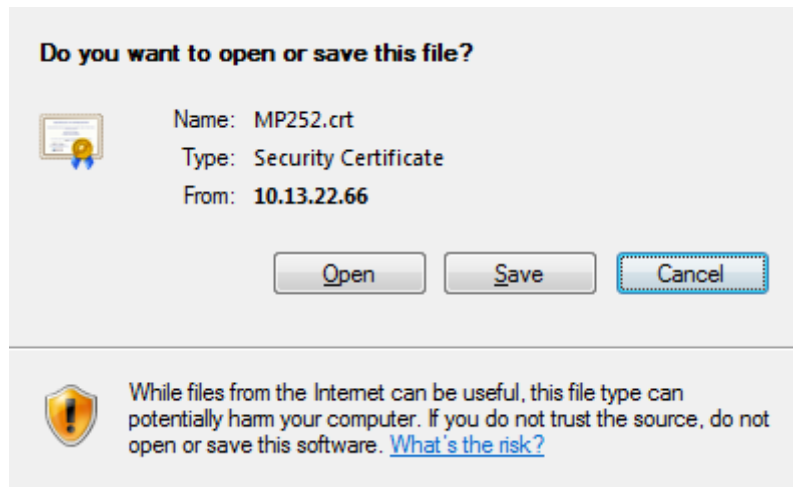
- f. In the 'Certificates' screen, click the **Download**  icon corresponding to the new self-signed certificate that you created; the 'File Download' window appears.

Figure 13-8: File Download Window




- g. Click **Save**, and then browse to the folder to where you want to save the file; the file is saved as a *.crt file.
- 3. Configure the Apache server, by configuring the SSLCACertificateFile parameter to point to the location where the certificate file is located. Since this is a self-signed certificate, you are also considered the CA.
- 4. Load the self-signed certificate to MP252:
 - a. In the 'Certificates' screen, click the **Upload Certificate** link; the 'Load MP252's Local Certificate' screen appears.

Figure 13-9: Load MP252's Local Certificate




- b. Click **Browse**, locate the certification file that you created, and then click **Upload** to load the file.
- 5. Load the CA's certificate to MP252:
 - a. Select the **CA's** tab; the 'CA's' screen appears.

Figure 13-10: CA's Certificates Page

 **Certificates**

MP252's Local **CA's**

Name	Issuer	Action
Upload Certificate		

- b. Click the **New**  icon; the 'Load CA's Certificate' screen appears.

Figure 13-11: Load CA's Certificate Page



Load CA's Certificate

Browse to locate either PEM-encoded signed certificate or Personal Information Exchange PKCS#12 file (.PFX,.P12), then press **Upload**.

Certificate File:

Personal Information Exchange PKCS#12 File Password (leave empty if no password is required):

- c. Click **Browse**, locate the CA certification file that you created, and then click **Upload** to load the file.
6. Configure the Apache server, using the following parameters:
- **SSLCACertificateFile**: Set the path to the CA's certificate.
 - **SSLCertificateFile**: Set the path to your signed certificate.
 - **SSLCertificateKeyFile**: Set the path to your private key.

13.4 Remote Configuration and Management Interfaces

MP252 supports the following remote configuration and management interfaces:

- Web server (GUI) over HTTP/HTTPS
- TR-069 and TR-104
- SNMP
- Syslog
- Firmware or configuration file download through HTTP/HTTPS and FTP/TFTP
- CLI over Telnet/SSH

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

Table 13-5: Operations per Configuration/Management Interface

Operation	Web GUI	TR-069	SNMP	Syslog	File D/L	CLI
Configuration Update	Yes	Yes	Yes	No	Yes	Yes
Firmware Upgrade	Yes	Yes	Yes	No	Yes	Yes
Status Monitoring	Yes	Yes	Yes	No	No	Yes
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.

13.4.1 Embedded Web Server

MP252 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 MP252 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 MP252 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)

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' screen) 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).

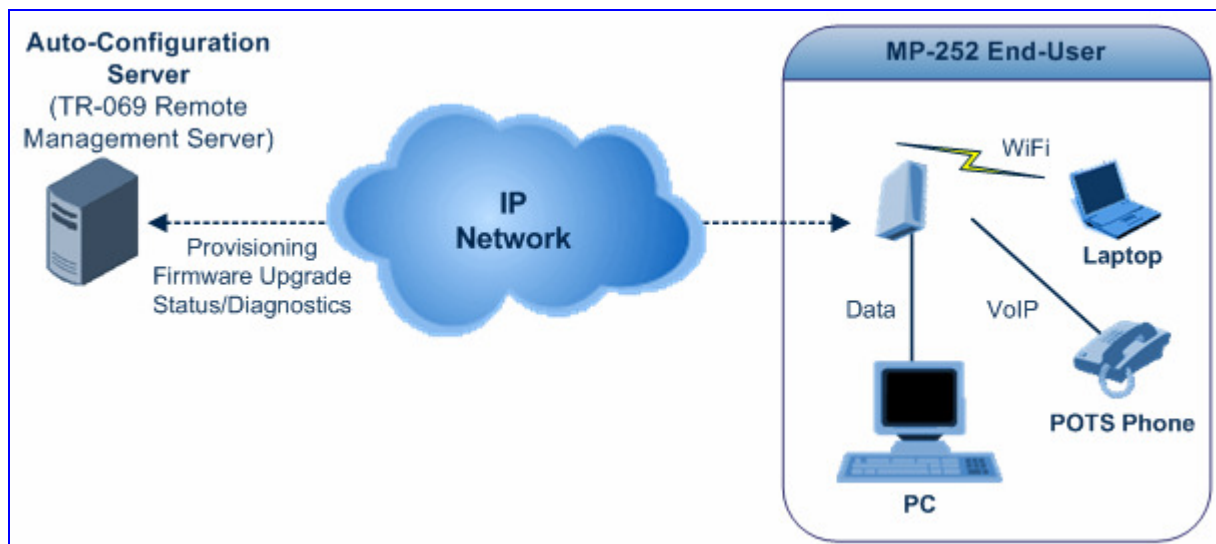
13.4.2 TR-069 and TR-104 CPE WAN Management Protocol

TR-069 is a WAN management protocol intended for communication between Customer Premise Equipment (CPE) or residential devices (such as MP252), and an Auto-Configuration Server (ACS), residing on the service provider's side. It defines a mechanism that encompasses secure auto configuration of CPE, and also incorporates other CPE management functions into a common framework. In simpler terms, TR-069 is a protocol that enables remote server management of the MP252. Such a protocol is useful, for example, for remotely and securely controlling MP252 by the CPE provider. 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.

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 13-12: TR-069 CPE WAN Management Protocol



The TR-069 protocol allows an ACS to provision a CPE or collection of CPE based on a variety of criteria. The provisioning mechanism includes specific provisioning parameters and a general mechanism for adding vendor-specific provisioning capabilities as needed. The provisioning mechanism allows CPE provisioning at the time of initial connection to the broadband access network, and the ability to re-provision at any subsequent time. This includes support for asynchronous ACS-initiated re-provisioning of CPE. TR-069 defines several Remote Procedure Call (RPC) methods, as well as a large number of parameters, which may be set or read. Some of these methods and parameters are defined as mandatory.



Notes:

- MP252 was tested for interoperability with two ACS vendors – Motive and FriendlyTR69. Working with other ACS types may require specific interoperability effort.
- The parameter values in the subsequent tables are sample values only taken from an ACS.

13.4.2.1 Configuring MP252 via TR-069 and TR-104

TR-069 allows basic configuration of MP252. The configuration is defined in a hierarchical tree-like structure according to the TR-069 standard.

13.4.2.1.1 Configuring the WAN Interface

Table 13-6: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i.WANIPConnection.i

TR-069/TR-104 Parameter	Configuration File Parameter	Description
AddressingType	<code>mt_cwmp_param_wan_connection_ip_addressing_type_get/set</code>	The method used to assign an address to the WAN side interface of the CPE for this connection: <ul style="list-style-type: none"> “DHCP” “Static”
ConnectionStatus	<code>mt_cwmp_param_wan_connection_ip_status_get</code>	Current status of the connection: <ul style="list-style-type: none"> “Unconfigured” “Connecting” “Connected” “PendingDisconnect” “Disconnecting” “Disconnected”
ConnectionType	<code>mt_cwmp_param_wan_connection_ppp_type_get</code>	Specifies the connection type of the connection instance: <ul style="list-style-type: none"> “Unconfigured” “IP_Routed” “DHCP_Spoofed” “PPPoE_Bridged” “PPPoE_Relay” “PPTP_Relay” “L2TP_Relay”
DefaultGateway	<code>mt_cwmp_param_wan_connection_ip_default_gateway_get/set</code>	The IP address of the default gateway for this connection. This parameter is configurable only if the AddressingType is Static.
DNSEnabled	<code>mt_cwmp_param_wan_connection_ip_dns_enabled_get/set</code>	Whether or not the device should attempt to query a DNS server across this connection.
DNSOverrideAllowed	<code>mt_cwmp_param_wan_connection_ip_dnsoverrideallowed_get/set</code>	Whether or not a manually set, non-empty DNS address can be overridden by a DNS entry received from the WAN.
DNSServers	<code>mt_cwmp_param_wan_connection_ip_dns_servers_get/set(i)</code>	Comma-separated list of DNS server IP addresses for this connection. Support for more than three DNS Servers is optional.
Enable	<code>mt_cwmp_param_wan_connection_ip_enable_get/set(1)</code>	Enables or disables the connection instance. On creation of a WANIPConnection instance, it is initially disabled.
ExternalIPAddress	<code>mt_cwmp_param_wan_connection_ip_externalip_get(i)</code>	The external IP address used by NAT for this connection. This parameter is configurable only if the AddressingType is Static.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
MaxMTUSize	mt_cwmp_param_wan_con n_ip_max_mtu_size_get/set(i)	The maximum allowed size of an Ethernet frame from LAN-side devices.
Name	mt_cwmp_param_wan_con n_XXX_name_get/set(i)	User-readable name of this connection.
NATEnabled	mt_cwmp_param_wan_con n_XXX_nat_enabled_get/set(i)	Indicates if NAT is enabled for this connection.
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: <ul style="list-style-type: none"> ▪ "Unconfigured" ▪ "IP_Routed" ▪ "IP_Bridged"
RouteProtocolRx	mt_cwmp_param_wan_con n_XXX_route_protocol_rx_get/set	Defines the Rx protocol to be used: <ul style="list-style-type: none"> ▪ "Off" ▪ "RIPv1" (Optional) ▪ "RIPv2" (Optional) ▪ "OSPF" (Optional)
RSIPAvailable	mt_cwmp_param_wan_con n_XXX_rsip_available_get(i)	Indicates if Realm-specific IP (RSIP) is available as a feature on MP252.
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	lan_host_config_management_get/set rg_conf dhcps/ netmask	Subnet mask of the WAN interface. This parameter is configurable only if the AddressingType is Static.
SpecVersion	""	Currently, 1.0 is the only available version.
Uptime	-	The time in seconds that this connection has been up.

13.4.2.1.2 Configuring the LAN Interface

Table 13-7: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Enable	device_eic_enable_get/set	Enables or disables this interface.
MACAddress	device_mac_address_get	The physical address of the interface.
MaxBitRate	device_max_bit_rate_get	The maximum upstream and downstream bit rate available for this connection: <ul style="list-style-type: none">▪ "10"▪ "100"▪ "1000"▪ "Auto"
Status	device_status_get	The status of the interface: <ul style="list-style-type: none">▪ "Up"▪ "NoLink"▪ "Error"▪ "Disabled"

Table 13-8: InternetGatewayDevice.LANDevice.i.LANHostConfigManagement

TR-069/TR-104 Parameter	Configuration File Parameter	Description
AllowedMACAddresses	allowed_mac_addresses_get/set	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	dhcp_lease_time_get/set	Specifies the lease time in seconds of client assigned addresses. A value of -1 indicates an infinite lease.
DHCPRelay	dhcp_relay_get/set	Determines if the DHCP server performs the role of a server (0) or a relay (1) on the LAN interface.
DHCPServerEnable	lan_host_config_management_get/set rg_conf dhcps/enable	Enables or disables the DHCP server on the LAN interface.
DNSServers	dhcps_dns_servers_get/set	Comma-separated list of DNS servers offered to DHCP clients. Support for more than three DNS Servers is optional.
DomainName	domain_name_get/set	Sets the domain name for clients on the LAN interface.
IPRouters	ip_routers_get/set	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.
MaxAddress	lan_host_config_management_get/set rg_conf dhcps/end_ip	Specifies the last address in the pool to be assigned by the DHCP server on the LAN interface.
MinAddress	lan_host_config_management_get/set rg_conf dhcps/start_ip	Specifies the first address in the pool to be assigned by the DHCP server on the LAN interface.
SubnetMask	lan_host_config_management_get/set rg_conf dhcps/netmask	Specifies the client's network subnet mask.

13.4.2.1.3 Configuring VoIP via TR-104

Table 13-9: InternetGatewayDevice.Services.VoiceService.i.Capabilities

TR-069/TR-104 Parameter	Configuration File 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. (True if voip/audio/fax/fax_transport_mode equals Bypass)
FaxT38	-	Support for T.38 fax. A true value indicates support for the object VoiceService.{i}.VoiceProfile.{i}.FaxT38.
MaxLineCount	voip/num_of_fxs_lines	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.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ModemPassThrough	-	Support for modem pass-through. A true value indicates support for the parameter <code>VoiceService.{i}.VoiceProfile.{i}.ModemPassThrough</code> .
NumberingPlan	-	Support for a configurable numbering plan. A true value indicates support for a configurable numbering plan via the <code>VoiceService.{i}.VoiceProfile.{i}.NumberingPlan</code> object.
PSTNSoftSwitchOver	-	A true value indicates MP252 is capable of supporting the <code>PSO_Activate Facility Action</code> , which allows a call to be switched to a PSTN FXO. Note: Currently, this parameter is not supported.
Regions	<code>pkg\mgt\lib\mgt_regional_settings.c</code> <code>slic_dsp_general_and_regional_settings_params_array</code>	Comma-separated list of geographic regions supported by MP252. 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 MP252 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 <code>VoiceService.{i}.VoiceProfile.{i}.Line.{i}.Ringer</code> object. A true value also indicates that the <code>RingDescriptionsEditable</code> , <code>PatternBasedRingGeneration</code> and <code>FileBasedRingGeneration</code> 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 <code>VoiceService.{i}.VoiceProfile.{i}.RTP.Redundancy</code> .
SignalingProtocols	<code>voip/signalling/protocol</code>	Signal protocol: <ul style="list-style-type: none"> ▪ "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.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ToneGeneration	-	Support for tone generation. A true value indicates support for the object <code>VoiceService.{i}.VoiceProfile.{i}.Tone</code> . A true value also indicates that the <code>ToneDescriptionsEditable</code> , <code>PatternBasedToneGeneration</code> and <code>FileBasedToneGeneration</code> parameters in this object are present.
VoicePortTests	-	Support for remotely accessible voice-port tests. A true value indicates support for the <code>VoiceService.{i}.PhyInterface.{i}.Tests</code> object.

Table 13-10: `InternetGatewayDevice.Services.VoiceService.i.Capabilities.Codecs`

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Codec	<code>voip/codec/i/name</code>	Identifier of the type of codec.
EntryID	<code>voip/codec/i/</code>	Unique identifier for each entry in the table.
PacketizationPeriod	<code>voip/codec/i/ptime</code>	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: <ul style="list-style-type: none"> ▪ “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 13-11: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile

TR-069/TR-104 Parameter	Configuration File Parameter	Description
DTMFMethod	voip/out_of_band_dtmf	Method by which DTMF digits must be passed: <ul style="list-style-type: none"> ▪ “InBand” ▪ “RFC2833” ▪ “SIPInfo”
Enable	-	Enables or disables all lines in this profile, or places it into a quiescent state: <ul style="list-style-type: none"> ▪ “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 MP252 is optional. If this parameter is set to “Quiescent” in a MP252 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	voip/num_of_fxs_lines	Number of instances of Line within this VoiceProfile.

Table 13-12: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.SIP

TR-069/TR-104 Parameter	Configuration File Parameter	Description
OutboundProxy	voip/signalling/sip/sip_outbound_proxy/addr	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.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
OutboundProxyPort	voip/signalling/sip/sip_outbound_proxy/proxy	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	voip/signalling/sip/proxy_address or voip/signalling/sip/sip_registrar/addr	Host name or IP address of the SIP proxy server.
ProxyServerPort	voip/signalling/sip/proxy_port or voip/signalling/sip/sip_registrar/port	Destination port for connecting to the SIP server.
ProxyServerTransport	voip/signalling/sip/transport_protocol	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
RegisterExpires	voip/signalling/sip/proxy_timeout	Register request Expires header value (in seconds).
RegistrarServerTransport	voip/signalling/sip/transport_protocol	Transport protocol for connecting to the SIP server. Must be chosen from among the transports supported.
UserAgentPort	voip/signalling/sip/port	Port for incoming call control signaling.
UserAgentTransport	voip/signalling/sip/transport_protocol	Transport protocol for incoming call control signaling.

13.4.2.1.4 Upgrading Firmware via TR-069

TR-069 contains a built-in mechanism for MP252 firmware upgrade.

13.4.2.2 Monitoring MP252 Status via TR-069 and TR-104

The service provider can monitor the status of MP252 via TR-069 and TR-104.

13.4.2.2.1 Device Information

Table 13-13: InternetGatewayDevice.DeviceInfo

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Description	manufacturer/description	A full description of MP252 (string).
DeviceLog	“”	Vendor-specific log(s).
HardwareVersion	Manufacturer/hardware/version	A string identifying the particular MP252 model and version.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
Manufacturer	manufacturer/vendor_name	A string identifying the manufacturer of MP252, i.e., AudioCodes.
ManufacturerOUI	manufacturer/vendor_oui	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	manufacturer/model_number	A string identifying the model name of MP252.
ProductClass	manufacturer/product_class	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	cwmp/provisioning_code	<p>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.</p> <p>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".</p>
SerialNumber	Manufacturer/hardware/serial_num	Serial number of MP252.
SoftwareVersion	system/external_version	<p>A string identifying the software version currently installed in MP252.</p> <p>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.</p>
UpTime	-	Time in seconds since MP252 was last reset.

13.4.2.2.2 WAN Status

Table 13-14: InternetGatewayDevice.WANDevice.i.WANConnectionDevice.i.WANIPConnection.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
EthernetBytesReceived	mt_cwmp_param_wan_connection_ip_stats_get (STAT_RX_BYTES)	Total number of bytes received over all connections within the same WANConnectionDevice that share a common MAC address since MP252 was last reset.
EthernetBytesSent	mt_cwmp_param_wan_connection_ppp_stats_get (STAT_TX_BYTES)	Total number of bytes sent over all connections within the same WANConnectionDevice that share a common MAC address since MP252 was last reset.
EthernetPacketsReceived	mt_cwmp_param_wan_connection_ppp_stats_get (STAT_RX_PACKETS)	Total number of Ethernet packets received over all connections within the same WANConnectionDevice that share a common MAC address since MP252 was last reset.
EthernetPacketsSent	mt_cwmp_param_wan_connection_ppp_stats_get	Total number of Ethernet packets sent over all connections within the same WANConnectionDevice that share a common MAC address since MP252 was last reset.

13.4.2.2.3 LAN Status

Table 13-15: InternetGatewayDevice.LANDevice.i.LANEthernetInterfaceConfig.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
BytesReceived	mt_voip_get_state (line, state)	Total number of bytes received over the interface since MP252 was last reset.
BytesSent	mt_voip_get_state (line, state)	Total number of bytes sent over the interface since MP252 was last reset.
PacketsReceived	mt_voip_get_state (line, state)	Total number of packets received over the interface since MP252 was last reset.
PacketsSent	mt_voip_get_state (line, state)	Total number of packets sent over the interface since MP252 was last reset.

13.4.2.2.4 VoIP Status via TR-104

Table 13-16: InternetGatewayDevice.Services.VoiceService.i.VoiceProfile.i.Line.i.Stats

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ResetStatistics	-	When set to one, it resets the statistics for this voice line. Always False when read.
PacketsSent	mt_voip_get_state(line, state)	Total number of RTP packets sent for this line.
PacketsReceived	mt_voip_get_state(line, state)	Total number of RTP packets received for this line.
BytesSent	mt_voip_get_state(line, state)	Total number of RTP payload bytes sent for this line.
BytesReceived	mt_voip_get_state(line, state)	Total number of RTP payload bytes received for this line.
PacketsLost	mt_voip_get_state(line, state)	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 MP252 is unable to maintain a connection to the server. Applies only to SIP.

TR-069/TR-104 Parameter	Configuration File Parameter	Description
ReceivePacketLossRate	mt_voip_get_state(line, state)	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	mt_voip_get_state	Current round-trip delay (in microseconds).
AverageReceiveInterarrivalJitter	-	Average receive interarrival jitter (in microseconds) since the beginning of the current call.
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.

13.4.2.3 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.

13.4.3 SNMP

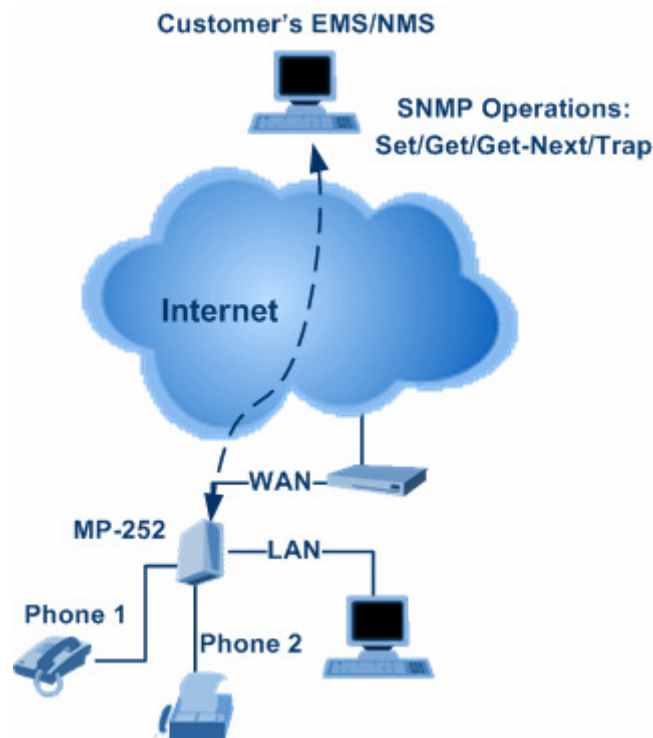
Simple Network Management Protocol (SNMP) is used in network management systems to configure and monitor network-attached devices. SNMP is an IETF standard defined by RFC 1157, 1441 and additional RFCs for specific Management Information Base (MIBs).

MP252 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, AC-MP20X-MIB includes the following sections:

- **acMP20xConfig:** for changing MP252's configuration
- **acMP20xStatus:** for monitoring MP252's status

The figure below shows the SNMP network architecture:

Figure 13-13: SNMP Network Architecture



13.4.3.1 Enabling SNMP in the Web Interface

Simple Network Management Protocol (SNMP) enables Network Management Systems (NMSs) to remotely configure and monitor your MP252. Your ISP may use SNMP to identify and resolve technical problems. Technical information regarding the properties of MP252's SNMP agent should be provided by your ISP.

The procedure below describes how to configure the SNMP agent embedded on the MP252.

➤ **To configure MP252's SNMP agent:**

1. In the 'Advanced' screen, click the **Simple Network Management Protocol (SNMP)**



icon; the 'Simple Network Management Protocol (SNMP)' screen appears.

Figure 13-14: Simple Network Management Protocol (SNMP) Screen

2. Select the 'Enabled' check box to enable SNMP.
3. Select the 'Allow Incoming WAN Access to SNMP' check box to allow access to MP252's SNMP agent over the Internet.
4. In the 'Read-Only Community Names' and 'Read-Write Community Names' fields, enter the SNMP community strings. These strings are passwords used in SNMP messages between the management system and MP252. A read-only community allows the manager to monitor MP252. A read-write community allows the manager to monitor and configure MP252.
5. From the 'Trusted Pair' drop-down list, enter the IP address, or subnet of addresses that identify which remote management stations are allowed to perform SNMP operations on MP252.
6. Under the **SNMP Traps** group, select the 'Enabled' check box to allow MP252 to send messages (traps) to a remote management station to notify the manager about the occurrence of important events or serious conditions.
 - **Version:** SNMP version - SNMP v1 or SNMP v2c traps.
 - **Destination:** remote management station's IP address.
 - **Community:** community name that is associated with the trap messages.
7. Click **OK** to save your settings.

13.4.3.2 Configuring MP252 via SNMP

The acMP20xConfig MIB section is structured in a similar hierarchy as MP252'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 integrates the MP20x MIB into the customer's Network Management System (NMS) to automate the configuration process.



Note: A special MIB object is defined to allow MP252 firmware upgrade triggered by SNMP. The object acMP20xRemoteUpdate triggers a remote upgrade from the SNMP-configured URL.

13.4.3.3 Status Monitoring of System and Network Interfaces via SNMP

SNMP can be used to monitor the status of MP252. 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 13-17: Table 3-13: Information Elements Available via MIB-II

Section	Available Information
system	<ul style="list-style-type: none"> ▪ Description ▪ Version Information ▪ Up-time
interfaces	Information per network interface: <ul style="list-style-type: none"> ▪ 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

13.4.3.4 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 a 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.

13.4.4 Syslog

Syslog is a standard protocol for reporting and logging of messages over IP network and is defined by RFC 3164. MP252 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>).



Note: Since Syslog is used only to output messages from MP252, it does not contain any security concerns.

13.4.5 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.

13.4.5.1 Firmware File Download

MP252's firmware files contain information about the target product type and the firmware version information.

13.4.5.2 Configuration File Download

MP252 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 MP252 via the Web server or "pulled" by MP252 from a remote server. This section refers only to the second option.

When MP252 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 MP252 that is restored to factory settings, modify the required parameters using the Web GUI, and then upload the configuration file from MP252 with the option to get only the modified configuration fields enabled.

13.4.5.3 Security Concerns and Measures

The main security hazard in automatic file download is that a hacker can force MP252 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 MP252 to authenticate the server and also to prevent the user from acquiring the file from the server.

13.4.6 Telnet CLI

MP252 features a Command Line Interface (CLI) over Telnet. The CLI enables the service provider to manage MP252 (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.

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

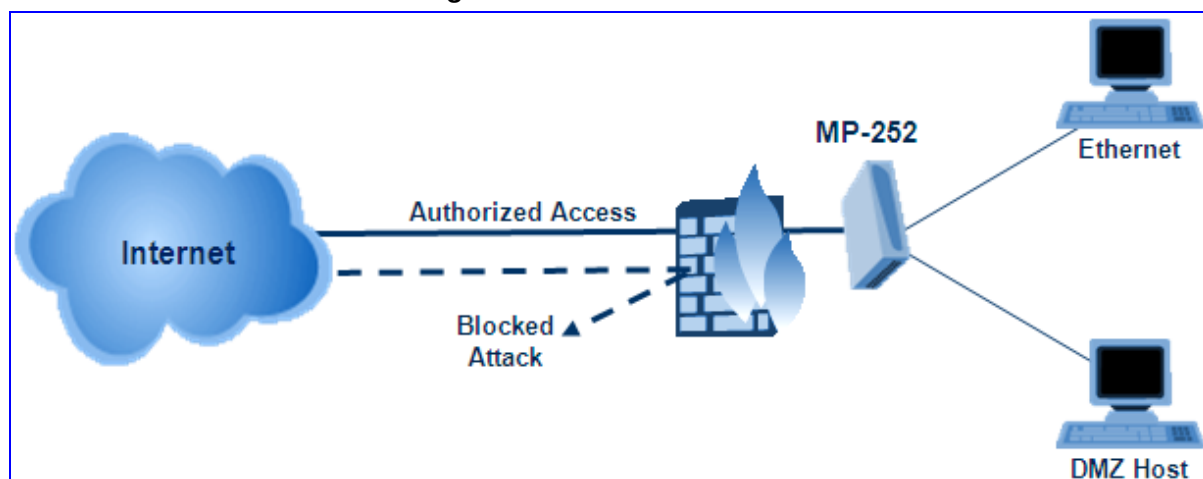
- The CLI is user and password protected (same as the Web).
- Telnet access can be blocked from the WAN and/or LAN interfaces.
- It is possible to limit Telnet access to specific IP addresses.
- Future versions will support SSH.

14 Security

MP252's security suite includes comprehensive and robust security services: Stateful Packet Inspection Firewall, user authentication protocols and password protection mechanisms. These features together allow users to connect their computers to the Internet and simultaneously be protected from the security threats of the Internet.

The firewall, which is the cornerstone of your MP252's security suite, has been exclusively tailored to the needs of the residential/office user and has been pre-configured to provide optimum security.

Figure 14-1: Firewall in Action



MP252 firewall provides both the security and flexibility that home and office users seek. It provides a managed, professional level of network security while enabling the safe use of interactive applications, such as Internet gaming and video-conferencing.

Additional features, including surfing restrictions and access control, can also be easily configured locally by the user through a user-friendly Web-based interface, or remotely by a service provider.

MP252 firewall supports advanced filtering, designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN network devices.

The Web-based management screens in the Security section feature the following:

- The 'General' screen allows you to choose the security level for the firewall (see 'General Security Level Settings' on page 226).
- The 'Access Control' screen can be used to restrict access from the home network to the Internet (see 'Local Servers (Port Forwarding)' on page 229).
- The 'Port Forwarding' screen can be used to enable access from the Internet to specified services provided by computers in the home network and special Internet applications (see 'Port Forwarding' on page 229).
- The 'DMZ Host' screen allows you to configure a LAN host to receive all traffic arriving at your MP252, which does not belong to a known session (see 'Port Triggering' on page 235).
- The 'Port Triggering' screen allows you to define port triggering entries, to dynamically open the firewall for some protocols or ports. (see 'Remote Administration' on page 261).
- The 'Website Restrictions' allows you to block LAN access to a certain host or web site on the Internet (see 'Website Restrictions' on page 237).
- 'Advanced Filtering' allows you to implicitly control the firewall setting and rules (see 'Advanced Filtering' on page 244).

- 'Security Log' allows you to view and configure the firewall Log (see Security Log).

14.1 General Security Level Settings

Use the 'Security Settings' screen to configure the MP252's basic security settings.

Figure 14-2: General Security Level Settings



The firewall regulates the flow of data between the home network and the Internet. Both incoming and outgoing data are inspected and then either accepted (allowed to pass through MP252) or rejected (barred from passing through MP252) according to a flexible and configurable set of rules. These rules are designed to prevent unwanted intrusions from the outside, while allowing home users access to the Internet services that they require.

The firewall rules specify what types of services available on the Internet may be accessed from the home network and what types of services available in the home network may be accessed from the Internet. Each request for a service that the firewall receives, whether originating in the Internet or from a computer in the home network, is checked against the set of firewall rules to determine whether the request should be allowed to pass through the firewall. If the request is permitted to pass, then all subsequent data associated with this request (a "session") are also allowed to pass, regardless of its direction.

For example, when you point your Web browser to a Web page on the Internet, a request is sent out to the Internet for this page. When the request reaches MP252, the firewall identifies the request type and origin--HTTP and a specific PC in your home network, in this case. Unless you have configured access control to block requests of this type from this computer, the firewall allows this request to pass out onto the Internet (see 'WAN PPPoE' on page 181 for more on setting access controls). When the Web page is returned from the Web server the firewall associates it with this session and allows it to pass, regardless of whether HTTP access from the Internet to the home network is blocked or permitted.

Note that it is the *origin of the request*, not subsequent responses to this request, that determines whether a session can be established or not.

You can choose from among three pre-defined security levels for MP252: Minimum, Typical, and Maximum (the default setting). The table below summarizes the behavior of MP252 for each of the three security levels.

Table 14-1: Behavior for the Three Security Levels

Security Level	Requests Originating in the WAN (Incoming Traffic)	Requests Originating in the LAN (Outgoing Traffic)
Maximum Security (Default)	Blocked: No access to home network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens	Limited: Only commonly- used services, such as Web- browsing and e-mail, are permitted
Typical Security	Blocked: No access to home network from Internet, except as configured in the Local Servers, DMZ host and Remote Access screens	Unrestricted: All services are permitted, except as configured in the Access Control screen
Minimum Security	Unrestricted: Permits full access from Internet to home network; all connection attempts permitted.	Unrestricted: All services are permitted, except as configured in the Access Control screen

These services include Telnet, FTP, HTTP, HTTPS, DNS, IMAP, POP3 and SMTP.

The list of allowed services at 'Maximum Security' mode can be edited in the screen 'Access Control' on page [228](#).

Some applications (such as some Internet messengers and Peer-To-Peer client applications) tend to use these ports if they cannot connect with their own default ports. When applying this behaviour, these applications are not blocked outbound, even at Maximum Security Level.

➤ **To configure MP252's security settings:**

(See the figure 'General Security Level Settings')

1. Choose from among the three predefined security levels described in the table above. 'Maximum Security' is the default setting.

Using the Minimum Security setting may expose the home network to significant security risks, and thus should only be used, when necessary, for short periods of time.

2. Check the 'Block IP Fragments' check box to protect your home network from a common type of hacker attack that could make use of fragmented data packets to sabotage your home network. Note that some UDP-based services make legitimate use of IP fragments. You need to allow IP fragments to pass into the home network to make use of these select services.
3. In the 'TCP Session timeout' field, enter the time-to-live (TTL) in units of seconds for TCP sessions. The valid range is 1 to 3600 hours (default is an hour).
4. Click **OK** to save the changes.

14.2 Access Control

You may want to block specific computers within the home network (or even the whole network) from accessing certain services on the Internet. For example, you may want to prohibit one computer from surfing the Web, another computer from transferring files using FTP, and the whole network from receiving incoming e-mail.

Access Control defines restrictions on the types of requests that may pass from the home network out to the Internet, and thus may block traffic flowing in both directions. In the e-mail example given above, you may prevent computers in the home network from receiving e-mail by blocking their *outgoing* requests to POP3 servers on the Internet.

There are services you should consider blocking, such as popular game and file sharing servers. For example, to ensure that your employees do not put your business at risk from illegally traded copyright files, you may want to block several popular P2P and file sharing applications.

➤ **To view and allow/restrict these services:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Access Control** tab; the screen 'Access Control' opens.


Figure 14-3: Access Control




2. Click the **New** + icon; the screen 'Add Access Control Rule' opens (see the figure below).

Figure 14-4: Add Access Control Rule



3. The parameter 'Address' enables you to specify the computer or group of computers for which you would like to apply the access control rule. You can select between any or a specific computer address in your LAN. If you choose the 'Specify Address' option, the screen refreshes, and an 'Add' link appears. Click it to specify a computer address. Specify an address by creating a 'Network Object'.
4. The parameter 'Protocol' lets you select or specify the type of protocol to be used. In addition to the list of popular protocols it provides, you may also choose any or a specific protocol. If you choose option 'Specify Protocol', the screen refreshes and an 'Add' link appears. Click it to specify a protocol address.
5. The parameter 'Schedule' allows you to define the time period during which this rule takes effect. You can select between 'Always' or a specific schedule. If you choose the option 'Specify Schedule', the screen refreshes and an 'Add' link appears. Click it to specify a schedule.
6. Click **OK** to save your settings; the 'Access Control' screen displays a summary of the rule that you just added. Click the **Edit**  icon to edit the access control rule for the service; the screen 'Edit Service' opens.
7. Select the network group to which you would like to apply the rule and the schedule during which the rule takes effect.
8. Click **OK** to save your changes and return to the 'Access Control' screen.

You can disable an access control rule and make the service available without having to remove the service from 'Access Control'. This can be useful when making the service only temporarily available and when expecting to reinstate the restriction in the future.

- To temporarily disable rule, clear the check box adjacent to the service name.
- To reinstate the restriction at a later time, recheck it.
- To remove a rule, click the **Remove**  icon for the service; the service is removed from 'Access Control'.



Note: When Web Filtering is enabled, HTTP services cannot be blocked by Access Control.

14.3 Port Forwarding

By default, MP252 blocks all external users from connecting to or communicating with your network. Therefore, the system is safe from hackers who may try to intrude on the network and damage it. However, you may want to expose your network to the Internet in certain limited and controlled ways to enable some applications to work from the LAN (game, voice and chat applications, for example) and to enable Internet access to servers in the home network. The Port Forwarding feature supports both of these functionalities.

The 'Port Forwarding' screen lets you define the applications that require special handling by MP252. You must select the application's protocol and the local IP address of the computer using or providing the service. If required, you can add new protocols in addition to the most common ones provided by MP252.

For example, to use an FTP application on one of your PCs, select 'FTP' from the list and enter the local IP address or host name of the designated computer; all FTP-related data arriving at MP252 from the Internet is then forwarded to the specified computer.

Similarly, to grant Internet users access to servers inside your home network, you must identify each service that you want to provide and the PC that provides it. For example, to host a Web server inside the home network you must select 'HTTP' from the list of protocols and enter the local IP address or host name of the computer that hosts the Web server. When an Internet user points her browser to the external IP address of MP252, it forwards the incoming HTTP request to the computer that is hosting the Web server.

Additionally, port forwarding enables you to redirect traffic to a different port instead of the one to which it was designated. If for example you have a Web server running on your PC on port 8080 and you want to grant access to this server to anyone who accesses MP252 via HTTP, do the following:

- Define a port forwarding rule for the HTTP service, with the PC's IP or host name.
- Specify 8080 in the field 'Forward to Port'.

All incoming HTTP traffic is now forwarded to the PC running the Web server on port 8080.

When setting a port forwarding service, you must ensure that the port is not already in use by another application, which may stop functioning. A common example is when using SIP signaling in Voice over IP - the port used by MP252's VoIP application (5060) is the same port on which port forwarding is set for LAN SIP agents.



Note: Some applications, such as FTP, TFTP, PPTP and H323, require the support of special specific Application Level Gateway (ALG) modules in order to work inside the home network. Data packets associated with these applications contain information that allows them to be routed correctly. An ALG is needed to handle these packets and ensure that they reach their intended destinations. MP252 is equipped with a robust list of ALG modules in order to enable maximum functionality in the home network. The ALG is automatically assigned based on the destination port.

➤ **To add a new port forwarding service :**

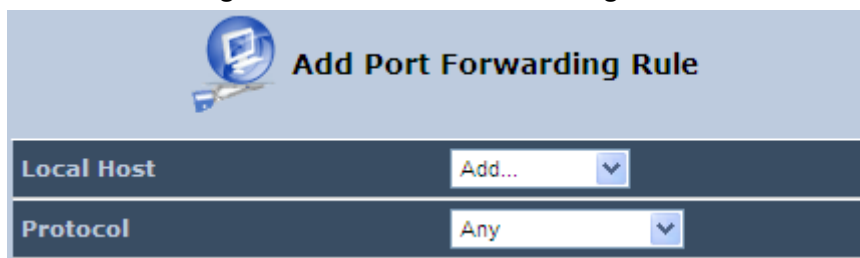
1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Port Forwarding** tab; the screen 'Port Forwarding' opens.

Figure 14-5: Port Forwarding Screen



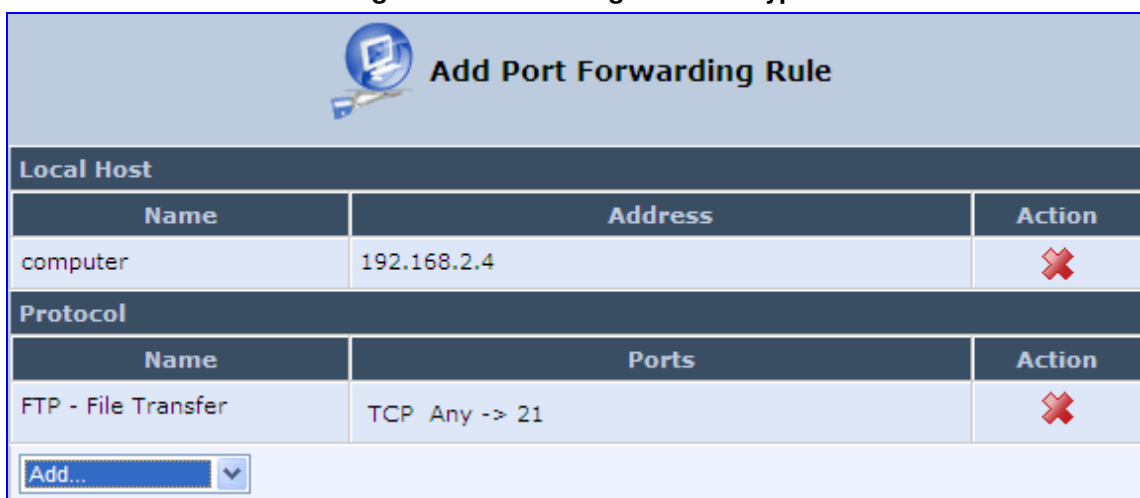
2. Click the **New**  icon; the screen 'Add Port Forwarding Rule' opens.

Figure 14-6: Add Port Forwarding Rule



3. From the 'Local Host' drop-down list, select the network object (defined in Section 4.5.2 on page 50) or define one now by selecting the 'User Defined' option. This is the IP address or host name of the computer that provides the service (the 'server'). **Note:** Only one LAN computer can be assigned to provide a specific service or application.
4. From the 'Protocol' drop-down list, select the type of protocol (defined in Section 4.5.3 on page 51) or select 'User Defined' to define one now. You can select multiple protocols for this rule.

Figure 14-7: Selecting Protocol Type



5. Click the **Advanced** button to configure advanced settings:
 - a. Select the 'Specify Public IP Address' check box if you want to apply this rule on MP252's non-default IP address defined in the 'NAT' screen (see Section 14.7 on page 240). Enter the additional external IP address in the 'Public IP Address' field.

Figure 14-8: Specifying Public IP Address

Add Port Forwarding Rule

Local Host		
Name	Address	Action
DHCP	miked	✖

Protocol		
Name	Ports	Action
FTP - File Transfer	TCP Any -> 21	✖

Add... ▾

Specify Public IP Address

Public IP Address: 0 . 0 . 0 . 0

Forward to Port: Same as Incoming Port ▾

Schedule: Always ▾

- b. By default, MP252 forwards traffic to the same port as the incoming port. If you wish to redirect traffic to a different port, then from the 'Forward to Port' drop-down list, select the 'Specify', and then enter the port number in the field provided.
 - c. By default, the rule is always active. However, you can select a schedule rule that defines the time during which the rule may be active. From the 'Schedule' drop-down list, select a defined Schedule rule (defined in Section 4.5.1 on page 47) or define a new one quickly by selecting 'User Defined'.
6. Click **OK** to save changes.

You can disable a port forwarding rule to make a service unavailable without having to remove the rule from the screen 'Port Forwarding'. This can be useful when making the service temporarily unavailable and when expecting to reinstate it in the future.

Figure 14-9: Select Check Box of Port Forwarding Rule (Active)

Port Forwarding

Expose services on the LAN to external Internet users.

Local Host	Local Address	Protocols	Status	Action
<input checked="" type="checkbox"/> 10.13.0.1	10.13.0.1	FTP - TCP Any -> 21	Active	✎ ✖
New Entry				+

- To temporarily disable a rule, clear the check box next to the service name.
- To reinstate it at a later time, select the check box.

- To remove a rule, click the **Remove**  icon for the service; the service is permanently removed.

14.4 DMZ Host

The DMZ (Demilitarized) Host feature allows one local computer to be exposed to the Internet. Designate a DMZ host to:

- Use a special-purpose Internet service, such as an on-line game or video-conferencing program, that is not present in the Local Servers list and for which no port range information is available.
- To expose one computer to all services, without restriction, irrespective of security.

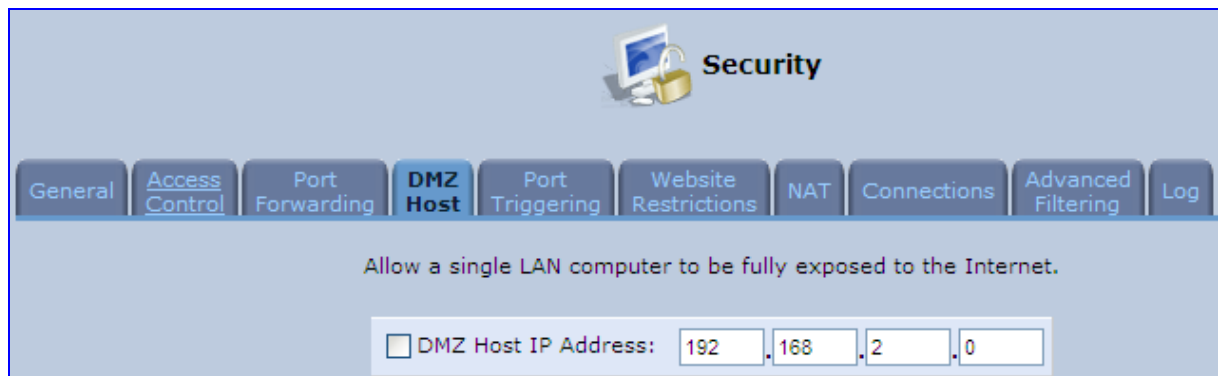
Warning: A DMZ host is not protected by the firewall and may be vulnerable to attack. Designating a DMZ host may also put other computers in the home network at risk. When designating a DMZ host, you must consider the security implications and protect it if necessary.

An incoming request for access to a service in the home network, such as a Web-server, is fielded by MP252. MP252 forwards this request to the DMZ host (if one is designated) unless the service is being provided by another PC in the home network (assigned in Local Servers), in which case that PC receives the request instead.

➤ **To designate a local computer as a DMZ Host:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **DMZ Host** tab; the screen 'DMZ Host' opens.

Figure 14-10: DMZ Host



2. Enter the local IP address of the computer to be designated as a DMZ host. Note that only one LAN computer can be a DMZ host at any time.
3. Click **OK** to save your changes and return to the screen 'DMZ Host'.

You can disable the DMZ host so that it does not fully exposed to the Internet, but keep its IP address recorded on the 'DMZ Host' screen. This may be useful if you wish to disable the DMZ host but expect that you may want to enable it again in the future.

- To disable the DMZ host so that it is not fully exposed to the Internet, clear the check-box next to the DMZ IP designation and click **OK**.
- To re-enable the DMZ host later, recheck the check-box.

14.5 Port Triggering

Port triggering can be used for dynamic port forwarding configuration. By setting port triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

For example, consider a gaming server that is accessed using UDP protocol on port 222. The gaming server responds by connecting the user using UDP on port 333 when starting gaming sessions. In such a case you must use port triggering, since this scenario conflicts with the following default firewall settings:

- The firewall blocks inbound traffic, by default.
- The server replies to MP252's IP, and the connection is not sent back to your host, since it is not part of a session.

To solve this, you need to define a Port Triggering entry, which allows inbound traffic on UDP port 333, only after a LAN host generated traffic to UDP port 222. This results in accepting the inbound traffic from the gaming server and sending it back to the LAN Host which originated the outgoing traffic to UDP port 222.

➤ **To view port triggering settings:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Port Triggering** tab; the screen 'Port Triggering' opens. The screen lists all port triggering entries.

Figure 14-11: Port Triggering

Trigger opening of ports for incoming data.

Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
<input checked="" type="checkbox"/> L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✘
<input checked="" type="checkbox"/> TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✘

Add...

➤ **To add an entry for the gaming example above:**

1. From the drop-down list, select 'User Defined' to add an entry; the screen 'Edit Service' opens.

Figure 14-12: Adding Port Triggering Rules

Edit Port Triggering Rule

Service Name:

Outgoing Trigger Ports

Protocol	Server Ports	Action
New Trigger Ports		+

Incoming Ports to Open

Protocol	Opened Ports	Action
New Opened Ports		+

2. Enter a name for the service (e.g., 'game_server'), and then click the link **New Trigger Ports**; the screen 'Edit Service Server Ports' opens.

Figure 14-13: Edit Service Server Ports

Edit Service Server Ports

Protocol: Other

Protocol Number:

3. In the 'Protocol' drop-down list, select 'UDP'; the screen refreshes, providing source and destination port options.
4. Leave the 'Source Ports' drop-down list at its default 'Any'. In the 'Destination Ports' drop-down list, select 'Single'; the screen refreshes again, providing an additional field in which you should enter '222' as the destination port.

Figure 14-14: Edit Service Server Ports

Edit Service Server Ports

Protocol: UDP

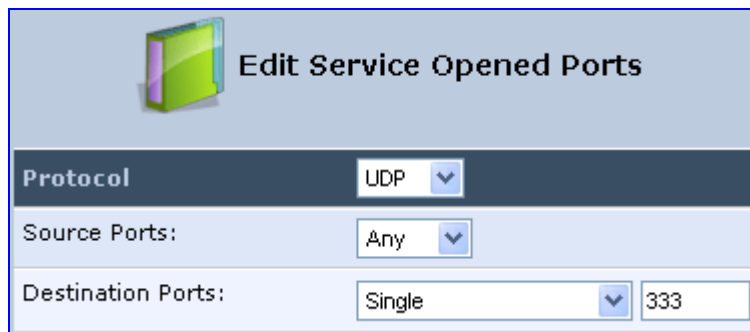
Source Ports: Any

Destination Ports: Single

5. Click **OK** to save the settings.
6. In the screen 'Edit Service', click the link **New Opened Ports**; the screen 'Edit Service Opened Ports' opens.

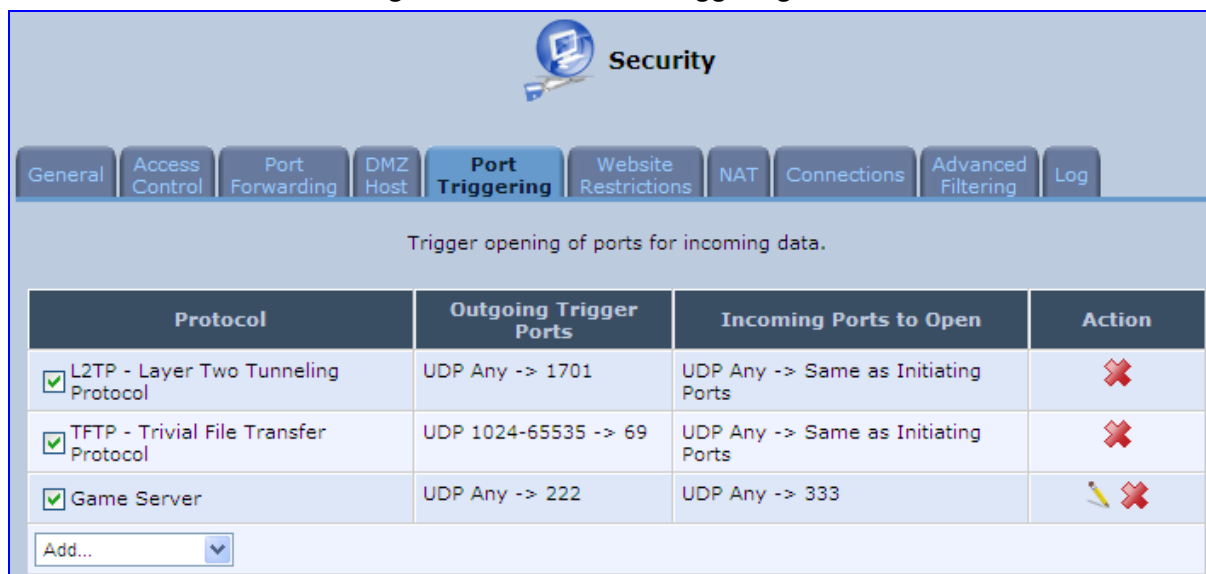
- Similar to the trigger ports screen, select UDP as the protocol, leave the source port at 'Any', and enter a 333 as the single destination port.

Figure 14-15: Edit Service Opened Ports



- Click **OK** to save the settings; the screen 'Edit Service' presents your entered information. Click **OK** again to save the port triggering rule; the screen 'Port Triggering' now includes the new port triggering entry.

Figure 14-16: New Port Triggering Rule



Protocol	Outgoing Trigger Ports	Incoming Ports to Open	Action
<input checked="" type="checkbox"/> L2TP - Layer Two Tunneling Protocol	UDP Any -> 1701	UDP Any -> Same as Initiating Ports	✘
<input checked="" type="checkbox"/> TFTP - Trivial File Transfer Protocol	UDP 1024-65535 -> 69	UDP Any -> Same as Initiating Ports	✘
<input checked="" type="checkbox"/> Game Server	UDP Any -> 222	UDP Any -> 333	✎ ✘

Add...

You can disable a port triggering rule without having to remove it from the screen 'Port Triggering':

- To temporarily disable a rule, clear the check box corresponding to the service name.
- To reinstate it later, simply reselect the check box.
- To remove a rule, click the **Remove** ✘ icon for the service; the service is permanently removed.

There may be a few default port triggering rules listed when you first access the port triggering screen. Note that disabling these rules may result in impaired MP252 functionality.

14.6 Website Restrictions

You can configure MP252 to block specific Internet websites so that they cannot be accessed from computers in the home network. Moreover, restrictions can be applied to a comprehensive and automatically-updated table of sites to which access is not recommended.

- **To block access to a website:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Website Restrictions** tab; the screen 'Website Restrictions' opens.

Figure 14-17: Website Restrictions




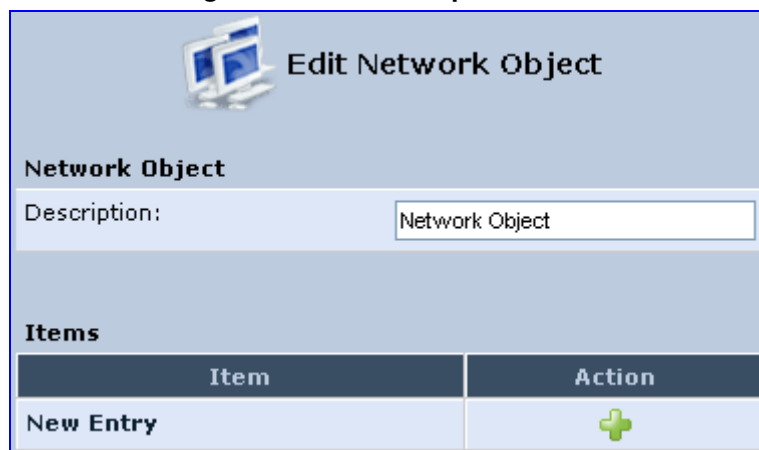
2. Click the **New**  icon; the 'Restricted Website' screen appears.

Figure 14-18: Restricted Website



3. Enter the website address (IP address or URL) that you would like to make inaccessible from your home network (all Web pages within the site are also blocked). If the website address has multiple IP addresses, MP252 resolves all additional addresses and automatically adds them to the restrictions table.
4. The 'Local Host' drop-down list provides you the ability to specify the computer or group of computers for which you would like to apply the website restriction. You can select between any or a specific computer address in your LAN. If you choose the option 'User Defined', the screen refreshes and the 'Edit Network Object' appears:

Figure 14-19: Add a Specific Host




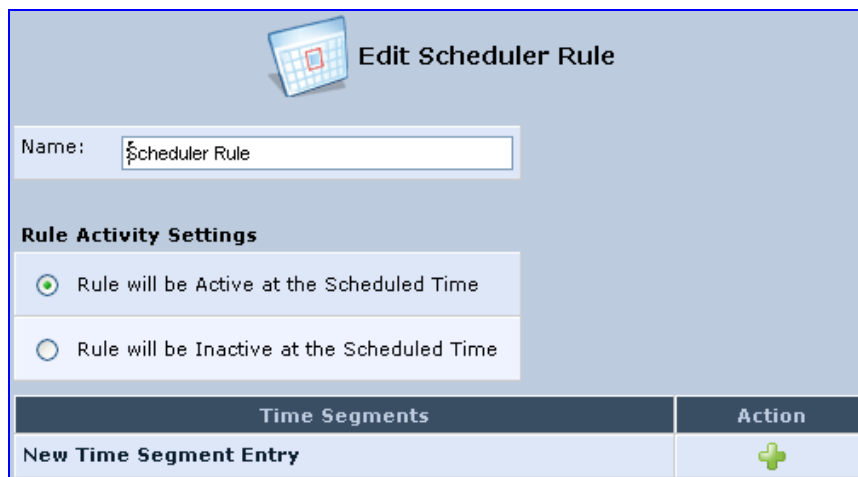


5. Click the **New**  icon to specify a computer address. Specify an address creating a 'Network Object'.
6. The parameter Schedule allows you to define the time period during which this rule takes effect. You can select between 'Always' or a specific schedule. If you choose the option 'User Defined', the screen 'Edit Scheduler Rule' appears:

Figure 14-20: Add a Specific Schedule



Time Segments	Action
New Time Segment Entry	

7. Click the **New**  icon to specify the time segment, and then click **OK**.
8. Click **OK** to save the settings; MP252 attempts to find the site. 'Resolving...' appears in the Status column while the site is being located (the URL is 'resolved' into one or more IP addresses).
9. Click the **Refresh** button to update the status if necessary. If the site is successfully located, 'Resolved' appears in the status bar; if not, 'Hostname Resolution Failed' appears.

➤ **If MP252 fails to locate the website:**

1. Use a Web browser to verify that the website is available. If it is, then you probably entered the website address incorrectly.
2. If the website is unavailable, return to the screen 'Website Restrictions' later and click the button **Resolve Now** to verify that the website can be found and blocked by MP252.
3. You can edit the website restriction by modifying its entry under the column 'Local Host' in the screen 'Website Restrictions'.

➤ **To modify an entry:**

1. Click the icon **Edit** for the restriction; the screen 'Restricted Website' opens. Modify the website address, group or schedule as required.
2. Click **OK** to save your changes and return to the screen 'Website Restrictions'.

➤ **To ensure that all current IP addresses corresponding to the restricted websites are blocked:**

1. Click the button **Resolve Now**; MP252 checks each of the restricted website addresses and ensures that all IP addresses at which this website can be found are included in the IP addresses column.

You can disable a restriction to make a website available again without having to remove it from the screen 'Website Restrictions'. This can be useful when making the website temporarily available and when expecting to block it again in the future.

- To temporarily disable a rule, clear the check box adjacent to the service name.
- To reinstate it at a later time, recheck the check box.

- To remove a rule, click the **Remove**  icon for the service; the service is permanently removed.

14.7 NAT

MP252 features a configurable Network Address Translation (NAT) and Network Address Port Translation (NAPT) mechanism, allowing you to control the network addresses and ports of packets routed through your gateway. When enabling multiple computers on your network to access the Internet using a fixed number of public IP addresses, you can statically define which LAN IP address will be translated to which NAT IP address and/or ports.

By default, MP252 operates in NAPT routing mode. However, you can control your network translation by defining static NAT/NAPT rules. Such rules map LAN computers to NAT IP addresses. The NAT/NAPT mechanism is useful for managing Internet usage in your LAN, or complying with various application demands. For example, you can assign your primary LAN computer with a single NAT IP address, in order to assure its permanent connection to the Internet. Another example is when an application server with which you wish to connect, such as a security server, requires that packets have a specific IP address – you can define a NAT rule for that address.

➤ **To define NAT:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **NAT** tab; the screen 'NAT' opens.

Figure 14-21: NAT Screen

Security

General Access Control Port Forwarding DMZ Host Port Triggering Website Restrictions **NAT** Connections Advanced Filtering Log

NAT IP Addresses Pool

IP Address	Action
New IP Address	+

NAT/NAPT Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
WAN Ethernet Rules						New Entry


2. Before configuring NAT/NAPT rules, you must first enter the additional public IP addresses obtained from your ISP as your NAT IP addresses, in the 'NAT IP Addresses Pool' section. The primary IP address used by the WAN device for dynamic NAPT should not be added to this table.
 - a. To add a NAT IP address, click the **New**  icon; the 'Edit Item' screen appears.

Figure 14-22: Adding a NAT IP Address

Edit Item

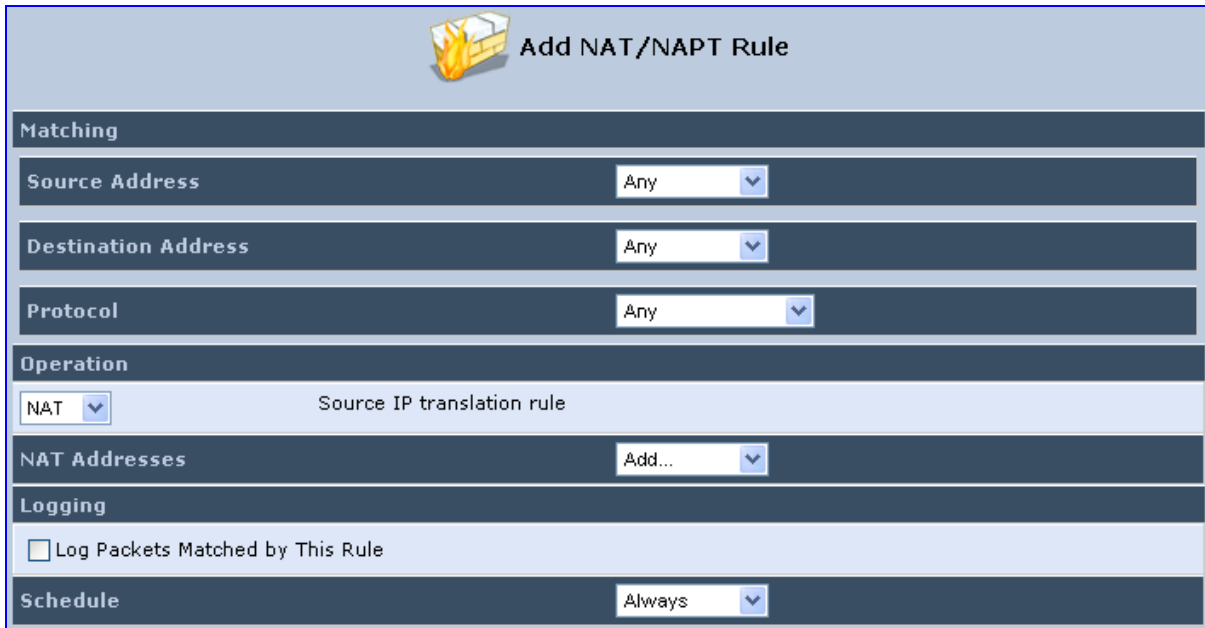
Network Object Type: IP Address


IP Address: 0 . 0 . 0 . 0

- b. From the 'Network Object Type' drop-down list, select between IP address, subnet or range, and then enter the information respectively, and click **OK** to save the settings.

3. To add a new NAT/NAPT rule:
 - a. In the 'NAT/NAPT Rule Sets' section, click the **New Entry** link; the 'Add NAT/NAPT Rule' screen appears.

Figure 14-23: Adding NAT/NAPT Rule



 Add NAT/NAPT Rule

Matching	
Source Address	Any
Destination Address	Any
Protocol	Any
Operation	
NAT	Source IP translation rule
NAT Addresses	Add...
<input type="checkbox"/> Log Packets Matched by This Rule	
Schedule	Always

This screen is divided into two main sections: 'Matching' and 'Operation'. The 'Matching' section defines the LAN addresses to be translated to the external addresses, which are defined in the 'Operation' section.

4. 'Matching' section (define characteristics of the packets matching the rule):
 - a. **Source Address:** source address of packets sent or received by MP252. You can select the computer or group of computers on which you would like to apply the rule. To apply the rule on all the LAN hosts, select 'Any' . If you would like to add a new address, select the 'User Defined'. This commences a sequence to add a new Network Object, representing the new host.
 - b. **Destination Address:** destination address of packets sent or received by MP252. This address can be configured in the same manner as the source address. This entry enables further filtration of the packets.
 - c. **Protocol:** specifies a traffic protocol. Selecting the 'Show All Services' option expands the list of available protocols. Select a protocol or add a new one using the 'User Defined' option. This commences a sequence that adds a new Service, representing the protocol. Using a protocol requires observing the relationship between a client and a server to distinguish between the source and destination ports.

5. Operation section (define the operation to apply on the IP addresses, matching the criteria defined above): NAT or NAPT.
 - **NAT Addresses:** NAT address into which the original IP address is translated. The drop-down list displays all of your available NAT addresses/ranges from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option. This commences a sequence that adds a new Network Object, representing the new host.
 - **NAPT Address:** NAPT address into which the original IP address is translated. The drop-down list displays all of your available NAPT addresses/ranges from which you can select an entry. If you would like to add a single address or a sub-range from the given pool/range, select the 'User Defined' option. This commences a sequence that adds a new Network Object, representing the new host. . Note, that in this case the network object may only be an IP address, as NAPT is port-specific.
 - ◆ **NAPT Ports:** specify the port(s) of the IP address into which the original IP address is translated. Enter a single port or select 'Range' (the screen refreshes, enabling you to enter a range of ports).
6. Select the 'Log Packets Matched by This Rule' check box to log the first packet from a connection that was matched by this rule.
7. By default, the 'Schedule' rule is always active. However, you can configure scheduler rules to define time segments during which the rule may be active.
8. Click **OK** to save the settings.

14.8 Connections

The connection list displays all the connections that are currently open, as well as various details and statistics. You can use this list to close an undesired connection by clicking its corresponding action icon. The basic display includes the name of the protocol, the different ports it uses, and the direction in which the connection was initiated.

➤ **To view currently open connections:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Connections** tab; the screen 'Connections' opens.
2. From the Connections Per Page drop-down list, select the number of connections that you want displayed per page. To browse to the next page, click the ➡ icon or the page number located at the bottom left of the page.

Figure 14-24: Connections Screen

The screenshot shows the 'Security' configuration page with the 'Connections' tab selected. It displays a summary of active connections and a detailed list below.

Number	Protocol	LAN IP:Port	MP252 IP:Port	WAN IP:Port	Direction	Action
1	TCP	10.13.22.32:80	10.13.22.32:80	10.13.22.25:1915	Incoming	✘
2	TCP	10.13.22.32:80	10.13.22.32:80	10.13.22.25:1914	Incoming	✘
3	UDP	239.255.255.250:1900	239.255.255.250:1900	10.13.22.13:63882	Incoming	✘
4	UDP	10.13.22.32:123	10.13.22.32:123	213.28.138.38:123	Outgoing	✘
5	UDP	239.255.255.250:1900	239.255.255.250:1900	10.13.2.17:53546	Incoming	✘
6	TCP	192.168.2.2:57061	10.13.22.32:57061	80.179.55.90:110	Outgoing	✘
7	TCP	192.168.2.2:57060	10.13.22.32:57060	80.179.55.90:110	Outgoing	✘
8	TCP	192.168.2.2:57059	10.13.22.32:57059	80.179.55.90:110	Outgoing	✘
9	TCP	192.168.2.2:57057	10.13.22.32:57057	17.149.34.67:5223	Outgoing	✘
10	TCP	192.168.2.2:57056	10.13.22.32:57056	17.149.36.195:5223	Outgoing	✘

To display additional details in the Connection list, click the **Advanced** button.

The 'Approximate Max. Connections' value displays the amount of additional concurrent connections possible.

14.9 Advanced Filtering

Advanced filtering is designed to allow comprehensive control over the firewall's behavior. You can define specific input and output rules, control the order of logically similar sets of rules and make a distinction between rules that apply to WAN and LAN devices.

- **To view MP252's advanced filtering options:**
 - From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Advanced Filtering** tab; the 'Advanced Filtering' opens.

Figure 14-25: Advanced Filtering

 **Security**

General
Access Control
Port Forwarding
DMZ Host
Port Triggering
Website Restrictions
NAT
Connections
Advanced Filtering
Log

Input Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
Final Rules						New Entry

Output Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Initial Rules						New Entry
LAN Bridge Rules						New Entry
LAN Hardware Ethernet Switch Rules						New Entry
LAN Wireless 802.11n Access Point Rules						New Entry
WAN ETHoA Rules						New Entry
WAN PPPoE Rules						New Entry
Final Rules						New Entry

ALG Rule Sets

Rule ID	Source Address	Destination Address	Match	Operation	Status	Action
Input						
<input checked="" type="checkbox"/> 0	Any	Any	FTP - TCP Any -> 21	ALG FTP	Active	✎ ✖ ↓
<input checked="" type="checkbox"/> 1	Any	Any	SIP - UDP Any -> 5060	ALG SIP	Active	✎ ✖ ↑ ↓

This screen is divided into two identical sections, one for 'Input Rule Sets' and the other for 'Output Rule Sets', which are for configuring inbound and outbound traffic, respectively. Each section is comprised of subsets, which can be grouped into three main subjects:

1. Initial rules - rules defined here are applied first, on all MP252 devices.
2. Network devices rules - rules can be defined per MP252.
3. Final rules - rules defined here are applied last, on all MP252 devices.

Numerous rules are automatically inserted by the firewall to provide improved security and block harmful attacks.



Note: The order of appearance of the firewall rules determines the sequence by which they are applied.

➤ **To configure an advanced filtering rule:**

1. After choosing the traffic direction and the device on which to set the rule, click the corresponding link **New Entry**; the screen 'Add Advanced Filter' opens.


Figure 14-26: Add Advanced Filter

Add Advanced Filter

Matching	
Source Address	Any ▼
Destination Address	Any ▼
Protocol	Any ▼
<input type="checkbox"/> DSCP	
<input type="checkbox"/> Priority	
<input type="checkbox"/> Length	
Operation	
Drop ▼	Drop packets
Logging	
<input type="checkbox"/> Log Packets Matched by This Rule	
Schedule	
Always ▼	

2. In the section 'Matching', define a match between IP addresses and a traffic protocol:
 - a. Configure the source address of the packets sent to or received from the network object. To add an address, select the option 'User Defined' from the drop-down list; the screen 'Edit Network Object' appears.

Figure 14-27: Add a Specific Host

Click the **New**  icon; this commences a sequence that adds a new network object.

- b. Configure the destination address of the packets sent to or received from the network object. This address can be configured in the same manner as the source address.
 - c. From the 'Protocol' drop-down list, select a specific traffic protocol or add a new one (by selecting 'User Defined'); the 'Edit Services' screen appears. Click the link **New Server Ports**; this commences a sequence that adds a new protocol.
3. Select the check box 'DSCP' to mark a DSCP value on packets matching this rule; the screen refreshes, allowing you to enter the hexadecimal value of the DSCP.
4. Select the check box 'Priority' to add a priority to the rule; the screen refreshes, allowing you to select between one of eight priority levels, zero being the lowest and seven the highest (each priority level is mapped to low/medium/high priority). This sets the priority of a packet on the connection matching the rule, while routing the packet.

Figure 14-28: Set Priority Rule

5. Select the check box 'Length' to specify the length of packets or the length of their data portion.
6. In the section 'Operation', define the action of the rule:
 - **Drop:** Deny access to packets that match the source and destination IP addresses and service ports defined in 'Matching'.
 - **Reject:** Deny access to packets that match the source and destination IP addresses and service ports defined in 'Matching' and sends and sends an ICMP error or a TCP reset to the origination peer.
 - **Accept Connection:** Allow access to packets that match the source and destination IP addresses and service ports defined in 'Matching'. The data transfer session is handled using Stateful Packet Inspection (SPI).

- **Accept Packet:** Allow access to packets that match the source and destination IP addresses and service ports defined in 'Matching'. The data transfer session is not handled using Stateful Packet Inspection (SPI), meaning that other packets that match this rule are not automatically allowed access. For example, this can be useful when creating rules that allow broadcasting.
7. Under the section 'Logging', select the parameter 'Log Packets Matched By This Rule' to log the first packet from a connection that was matched by this rule.
 8. By default, the 'Schedule' rule is always active. However, you can configure scheduler rules to define time segments during which the rule may be active.
 9. Click **OK** to save the settings.

14.10 Security Log

The Security log displays a list of firewall-related events, including attempts to establish inbound and outbound connections, attempts to authenticate at an administrative interface (Web-based management or Telnet terminal), firewall configuration and system start-up.

➤ **To view the Security Log:**

1. From the menu bar, click the **Security** menu, and in the screen 'Security', click the **Log** tab; the screen 'Log' opens.

Figure 14-29: Security Log

The screenshot shows the 'Security' configuration screen with the 'Log' tab selected. Below the navigation tabs, there are buttons for 'Close', 'Clear Log', 'Download Log', 'Settings', and 'Refresh'. A message states: 'Press the **Refresh** button to update the data.'

Time	Event	Event-Type	Details
Jan 1 03:03:47 2003	WBM Login	User authentication success	Username: admin [repeated 5 times, last time on Jan 1 04:18:09 2003]
Jan 1 02:56:33 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded
Jan 1 02:56:32 2003	Firewall Setup	Firewall internal	Starting firewall configuration
Jan 1 02:56:23 2003	WBM Login	User authentication success	Username: admin
Jan 1 02:43:42 2003	Firewall Setup	Firewall internal	Firewall configuration succeeded

2. The log table displays the following:
 - **Time:** to determine the time the event occurred.
 - **Event:** type of event. There are five types of events:

- ◆ **Inbound Traffic:** The event is a result of an incoming packet.
- ◆ **Outbound Traffic:** The event is a result of outgoing packet.
- ◆ **Firewall Setup:** Configuration message.
- ◆ **WBM Login:** Indicates that a user has logged in to WBM.
- ◆ **CLI Login:** Indicates that a user has logged in to CLI (via Telnet).
- **Event-Type:** textual description of the event:
 - ◆ **Blocked:** The packet was blocked. The message is color-coded red.
 - ◆ **Accepted:** The packet was accepted. The message is color-coded green.
- **Details:** details of the packet or the event, such as protocol, IP addresses, ports, etc.

➤ **To change the security log settings:**

1. In the 'Log' screen, click **Settings**; the screen 'Log Settings' opens.

Figure 14-30: Security Log Settings



Log Settings

Accepted Events

Accepted Incoming Connections

Accepted Outgoing Connections

Blocked Events

<input type="checkbox"/> All Blocked Connection Attempts		
<input type="checkbox"/> Winnuke	<input type="checkbox"/> Multicast/Broadcast	<input type="checkbox"/> ICMP Replay
<input type="checkbox"/> Defragmentation Error	<input type="checkbox"/> Spoofed Connection	<input type="checkbox"/> ICMP Redirect
<input type="checkbox"/> Blocked Fragments	<input type="checkbox"/> Packet Illegal Options	<input type="checkbox"/> ICMP Multicast
<input type="checkbox"/> Syn Flood	<input type="checkbox"/> UDP Flood	<input type="checkbox"/> ICMP Flood
<input type="checkbox"/> Echo Chargen		

Other Events

Remote Administration Attempts

Connection States

Log Buffer

Prevent Log Overrun

2. Select the types of activities for which you would like to have a log message generated.
 - **Accepted Events:**
 - ◆ **Accepted Incoming Connections:** Write a log message for each successful attempt to establish an inbound connection to the home network.
 - ◆ **Accepted Outgoing Connections:** Write a log message for each successful attempt to establish an outgoing connection to the public network.
 - **Blocked Events:**

- ◆ **All Blocked Connection Attempts:** Write a log message for each blocked attempt to establish an inbound connection to the home network or vice versa. You can enable logging of blocked packets of specific types by disabling this option, and enabling some of the more specific options below it.
 - ◆ **Specific Events:** Specify the blocked events that should be monitored. Use this to monitor specific event such as SynFlood. A log message is generated if either the corresponding check-box is checked, or the check-box 'All Blocked Connection Attempts' is checked.
 - **Other Events:**
 - ◆ **Remote Administration Attempts:** Write a log message for each remote-administration connection attempt, whether successful or not.
 - ◆ **Connection States:** Provide extra information about every change in a connection opened by the firewall. Use this option to track connection handling by the firewall and Application Level Gateways (ALGs).
 - **Log Buffer:**
 - ◆ **Prevent Log Overrun:** Select this check box in order to stop logging firewall activities when the memory allocated for the log fills up.
3. Click **OK** to save the settings.

15 Advanced Networking Features

This chapter describes various advanced networking features such as DHCP.

15.1 IP Address Distribution

The MP252's Dynamic Host Configuration Protocol (DHCP) server makes it possible to easily add computers that are configured as DHCP clients to the home network. It provides a mechanism for allocating IP addresses and delivering network configuration parameters to such hosts. MP252's default DHCP server is the LAN bridge.

A client (host) sends out a broadcast message on the LAN requesting an IP address for itself. The DHCP server then checks its list of available addresses and leases a local IP address to the host for a specific period of time and simultaneously designates this IP address as 'taken'. At this point, the host is configured with an IP address for the duration of the lease.

The host can choose to renew an expiring lease or let it expire. If it chooses to renew a lease then it also receives current information about network services, as it did with the original lease, allowing it to update its network configurations to reject any changes that may have occurred since it first connected to the network. If the host wishes to terminate a lease before its expiration it can send a release message to the DHCP server, which then makes the IP address available for use by others.

The MP252 embedded DHCP server provides the following features:

- Displays a list of all DHCP host devices connected to MP252
- Defines the range of IP addresses that can be allocated to the LAN
- Defines the length of time for which dynamic IP addresses are allocated
- Provides the above configurations for each LAN device and can be configured and enabled / disabled separately for each LAN device
- Can assign a static lease to a LAN PC so that it receives the same IP address each time it connects to the network even if this IP address is within the range of addresses that the DHCP server may assign to other computers
- Provides the DNS server with the host name and IP address of each PC that is connected to the LAN




In addition, MP252 can act as a DHCP relay, escalating DHCP responsibilities to a WAN DHCP server. In this case, MP252 acts merely as a router, while its LAN hosts receive their IP addresses from an external DHCP server on the WAN.

With MP252's optional Zero Configuration Technology feature, the IP Auto Detection method detects statically-defined IP addresses in addition to MP252's DHCP clients. It learns all the IP addresses on the LAN and integrates the collected information with the database of the DHCP server. This allows the DHCP server to issue valid leases, thus avoiding conflicting IP addresses used by other computers in the network.

➤ **To view services currently provided by the DHCP server:**

- In the 'Advanced' screen, click the **IP Address Distribution**  icon; the 'IP Address Distribution' screen appears.

Figure 15-1: DHCP Server Summary

 IP Address Distribution				
Name	Service	Subnet Mask	Dynamic IP Range	Action
LAN Bridge	DHCP Server	255.255.255.0	192.168.2.1 - 192.168.2.254	
WAN Ethernet	Disabled			



Note: If the 'Service' column displays “Disabled”, then DHCP services are not being provided to hosts connected to the network through that MP252 interface. This means that MP252 does not assign IP addresses to these computers, which is useful if you wish to work with static IP addresses only.

15.1.1 DHCP Server Parameters

The procedure below describes how to edit a service provided by the DHCP server.

➤ **To edit the DHCP server settings for a device:**


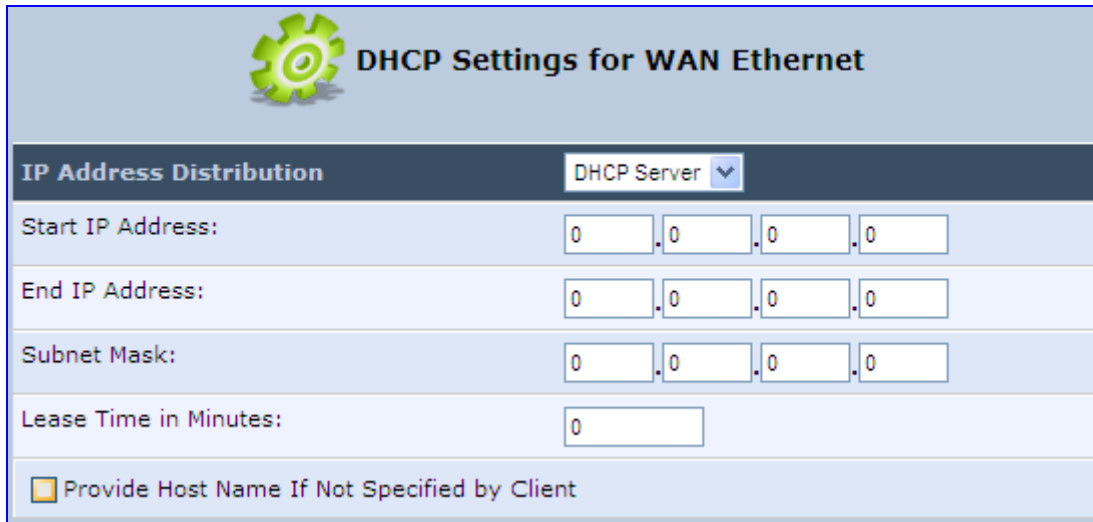
1. In the 'IP Address Distribution' screen, click the **Edit**  icon corresponding to the entry that you want to edit; the DHCP Server settings for this device are displayed.

Figure 15-2: DHCP Settings Screen



DHCP Settings for WAN Ethernet	
IP Address Distribution	DHCP Server
Start IP Address:	0 . 0 . 0 . 0
End IP Address:	0 . 0 . 0 . 0
Subnet Mask:	0 . 0 . 0 . 0
Lease Time in Minutes:	0
<input type="checkbox"/> Provide Host Name If Not Specified by Client	

2. From the 'IP Address Distribution' drop-down list, select whether to disable the MP252 DHCP server, or enable DHCP (MP252 serves as a DHCP server or DHCP relay).
3. In the 'Start IP Address' and 'End IP Address' fields, define the IP address range. This determines the number of hosts that may be connected to the network in this subnet. The 'Start IP Address' field specifies the first IP address that may be assigned in this subnet; the 'End IP Address' field specifies the last IP address in the range.
4. In the 'Subnet Mask' field, define the subnet to which an IP address belongs (e.g., 255.255.0.0).
5. In the 'Lease Time in Minutes' field, define the time for which each device is assigned an IP address by the DHCP server when it connects to the network. When the lease expires, the server determines if the computer has disconnected from the network. If it has, then the server may reassign this IP address to a newly-connected computer. This feature ensures that IP addresses that are not in use become available for other computers on the network.
6. Select the 'Provide Host Name If Not Specified by Client' check box to enable the MP252 to assign clients a default name if they do not have a host name.
7. Click **OK**.

15.1.2 DHCP Relay Parameters

The MP252 can act as a DHCP relay if you want to dynamically assign IP addresses from a DHCP server other than the MP252's DHCP server. .



Note: When implementing DHCP relay, you must configure the WAN of the MP252 to operate in routing mode.

➤ **To configure a device as a DHCP relay:**


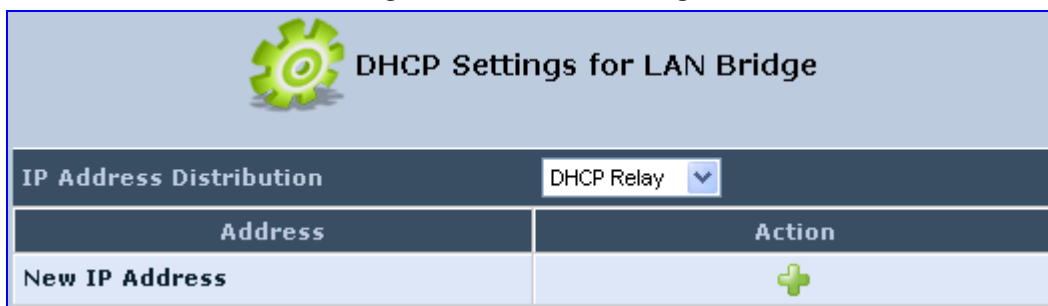
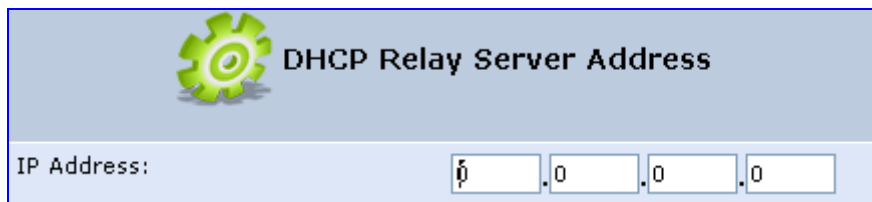
1. In the 'IP Address Distribution' screen, click the **Edit**  icon corresponding to the entry that you want to edit; the DHCP Server settings for this device are displayed.
2. From the 'IP Address Distribution' drop-down list, select the 'DHCP Relay' option; the 'DHCP Settings' screen appears.


Figure 15-3: DHCP Settings



3. Click the **New**  icon; the 'DHCP Relay Server Address' screen appears.

Figure 15-4: DHCP Relay Server Address Screen



4. In the 'IP Address' field, enter the IP address of the DHCP server.
5. Click **OK** to save your changes.
6. Click **OK** once more in the 'DHCP Settings' screen.
7. Change MP252's WAN to operate in routing mode:
 - a. On the menu bar, click the **Network Connections** menu; the 'Network Connections' screen appears.
 - b. Click the **Edit**  icon corresponding to the WAN Ethernet connection; the 'WAN Ethernet Properties' screen appears.
 - c. Click the **Routing** tab.
 - d. From the 'Routing Mode' drop-down list, select 'Route'.
 - e. Click **OK** to save the settings.









15.1.3 Viewing DHCP Clients

The procedure below describes how to view a list of hosts (computers) that are allocated IP addresses by the DHCP server.

➤ **To view a list of computers currently recognized by the DHCP server:**

1. In the 'IP Address Distribution' screen, click the **Connection List** button; the 'DHCP Connections' screen appears.

Figure 15-5: DHCP Connection Screen

 DHCP Connections							
Host Name	IP Address	Physical Address	Lease Type	Connection Name	Status	Expires In	Action
itaico-laptop	192.168.2.3	00:13:02:39:88:00	Dynamic	LAN Bridge	Active	36 Minutes	  
TW-Laptop	192.168.2.4	00:14:c2:e4:3d:f0	Dynamic	LAN Bridge	Active	49 Minutes	  
New Static Connection							

15.1.4 Defining Static DHCP Clients

The procedure below describes how to define a static (fixed) IP address for a DHCP client.

➤ **To define a DHCP client with a fixed IP address:**



1. In the 'IP Address Distribution' screen, click the **Connection List** button; the 'DHCP Connections' screen appears.
2. Click the **New**  icon; the 'DHCP Connection Settings' screen appears.

Figure 15-6: DHCP Connection Settings Screen

 DHCP Connection Settings	
Host Name:	<input type="text" value="new-host"/>
IP Address:	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
MAC Address:	<input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/> <input type="text" value="00"/>


3. In the 'Host Name' field, enter a host name for this connection.
4. In the 'IP Address' field, enter the fixed IP address to be assigned to the computer.
5. In the 'MAC Address' field, enter the MAC address of the computer's network card.



Note: A device's fixed IP address is actually assigned to the specific network card's (NIC) MAC address installed on the LAN computer. If you replace this network card then you must update the device's entry in the DHCP Connections list with the new network card's MAC address.

6. Click **OK** to save the settings; the 'DHCP Connections' screen reappears displaying the defined static connection. This connection can be edited or deleted.

15.2 DNS Server

The **DNS Server**  icon allows you to manage the MP252 Domain Name System (DNS) server. The DNS server does not require configuration. However, you can view the list of computers known by the DNS, edit the host names or IP addresses of computers in the list, or manually add a new computer to the list.

DNS provides a service that translates domain names into IP addresses and vice versa. MP252's DNS server is an auto-learning DNS, which means that when a new computer is connected to the network, the DNS server learns its name and automatically adds it to the DNS table. Other network users may immediately communicate with this computer using either its name or its IP address.

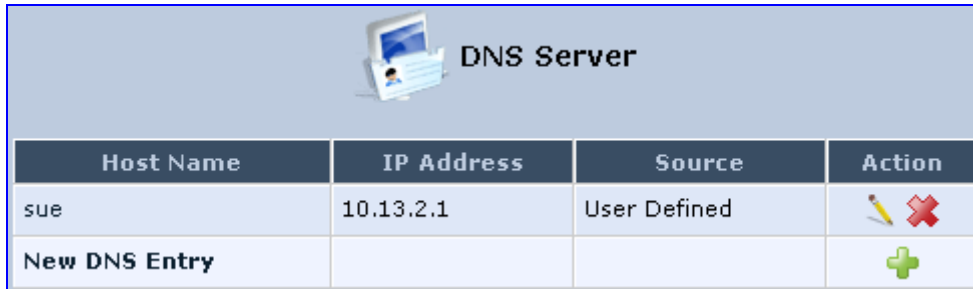
The MP252 DNS server also provides the following functionalities:




- Shares a common database of domain names and IP addresses with the DHCP server.
- Supports multiple subnets within the LAN simultaneously.
- Automatically appends a domain name to unqualified names.
- Allows new domain names to be added to the database using MP252's Web interface.
- Permits a computer to have multiple host names.
- Permits a host name to have multiple IPs (needed if a host has multiple network cards).

➤ **To add a new host computer to the DNS table:**

1. In the 'Advanced' screen, click the  icon; the DNS table is displayed.

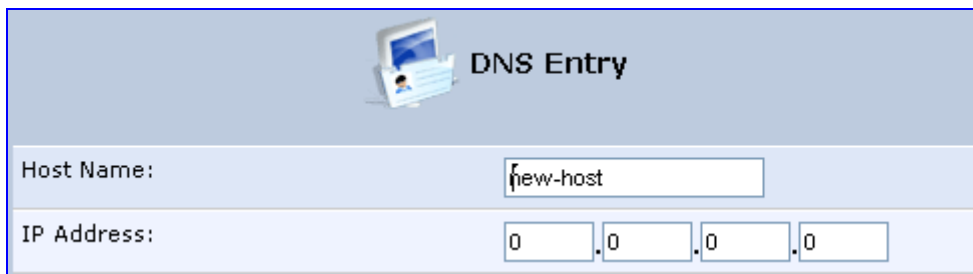
Figure 15-7: DNS Server



Host Name	IP Address	Source	Action
sue	10.13.2.1	User Defined	 
New DNS Entry			

2. Click the **New**  icon; the 'DNS Entry' screen appears.

Figure 15-8: DNS Entry




Host Name:


IP Address: . . .

3. Enter the computer's host name and IP address.
4. Click **OK** to save your changes.

➤ **To edit the host name or IP address of an entry:**

1. Click the **Edit**  icon corresponding to the host that you want to edit; the 'DNS Entry' screen appears.
2. If the host was manually added to the DNS Table, you can modify its host name and/or IP address. If it wasn't, you can only modify its host name.
3. Click **OK** to save your changes.

➤ **To remove a host from the DNS table:**

- Click the **Remove**  icon corresponding to the host that you want to delete; the entry is removed from the table.

15.3 Dynamic DNS

The Dynamic DNS (DDNS) feature allows you to alias a dynamic IP address to a static hostname, allowing your computer to be more easily accessible from various locations on the Internet. Typically, when you connect to the Internet, your ITSP assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of a specific connection. Dynamically assigning addresses extends the usable pool of available IP addresses, whilst maintaining a constant domain name.

When using the DDNS service, each time the IP address provided by your ITSP changes, the DNS database changes accordingly to reflect the change. In this way, even though your IP address changes often, your domain name remains constant and accessible.

To be able to use the Dynamic DNS (DDNS) feature, you must first open a free DDNS account at <http://www.dyndns.org/account/create.html>. When applying for an account, you need to specify a user name and password. Have them readily available when customizing MP252's DDNS support. For detailed information on DDNS, see <http://www.dyndns.org>.

➤ **To open a dynamic DNS account:**


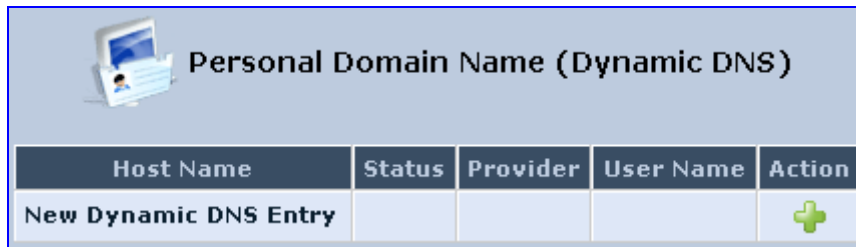

1. In the 'Advanced' screen, click the **Personal Domain Name (Dynamic DNS)**  icon; the 'Personal Domain Name (Dynamic DNS)' screen appears.

Figure 15-9: Personal Domain Name (Dynamic DNS) Screen



Host Name	Status	Provider	User Name	Action
New Dynamic DNS Entry				


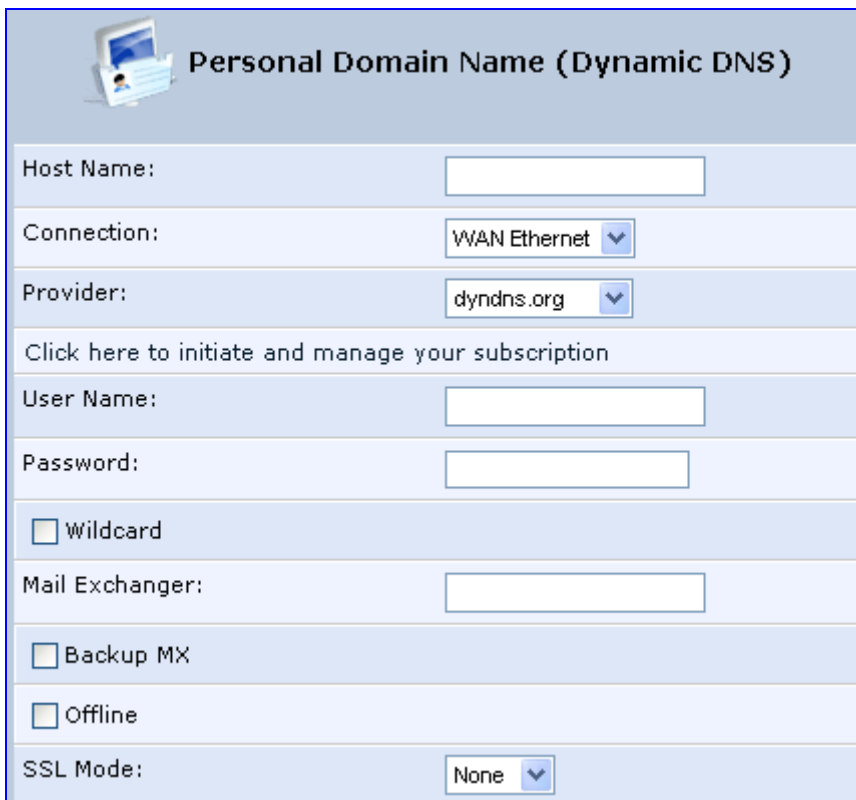
2. Click the **New**  icon to add a new connection; the 'Personal Domain Name (Dynamic DNS)' screen appears.

Figure 15-10: Personal Domain Name (Dynamic DNS) - Adding



Personal Domain Name (Dynamic DNS)

Host Name:

Connection:

Provider:

[Click here to initiate and manage your subscription](#)

User Name:

Password:

Wildcard

Mail Exchanger:

Backup MX

Offline

SSL Mode:

3. In the 'Host Name' field, enter your full DDNS domain name.
4. From the 'Connection' drop-down list, select the connection to which you want to couple the DDNS service. The DDNS service uses only the selected device, unless failover is enabled. In this case, the failed-to device is used instead (assuming its route rules consent), until the chosen device is up again. In a single WAN scenario, this field appears as static text (non-configurable). This is applicable if you have multiple WAN devices.

5. From the 'Provider' drop-down list, select your DDNS service provider and then click the link **Click here to initiate and manage your subscription** to open the selected provider's account creation Web page. For example, if you select 'dyndns.org', the following page opens: <http://www.dyndns.com/account>.
6. In the 'User Name' and 'Password' fields, enter your DDNS user name and password, respectively.
7. To enable use of special links (such as such as www.<your host>.dyndns.org), select the 'Wildcard' check box.
8. In the 'Mail Exchanger' field, enter your mail exchange server address to redirect all e-mails arriving at your DDNS address to your mail server.
9. To designate the mail exchange server as a backup server, select the 'Backup MX' check box.
10. To temporarily take your site offline (i.e., prevent traffic from reaching your DDNS domain name), select the 'Offline' check box. This redirects DNS requests to an alternative, predefined URL. The availability of this feature depends on your DDNS account's level of service. The redirection URL must be configured through the account as well.
11. From the 'SSL Mode' drop-down list, select the certificate validation method used by MP252 to validate the DDNS server's certificate upon secured connection to DDNS using HTTPS:
 - **None:** The server's certificate is not validated.
 - **Chain:** Validates the entire certificate chain. When selecting this option, the screen refreshes, displaying the 'Validate Time' drop-down list for selecting whether or not to validate the certificate's expiration time ('Ignore' or 'Check' respectively). If the certificate has expired, the connection terminates immediately.
 - **Direct:** Ensures that the server's certificate is directly signed by the root certificate. This option also provides the 'Validate Time' drop-down list for validation of the certificate's expiration time, as described above.
12. Click **OK**.

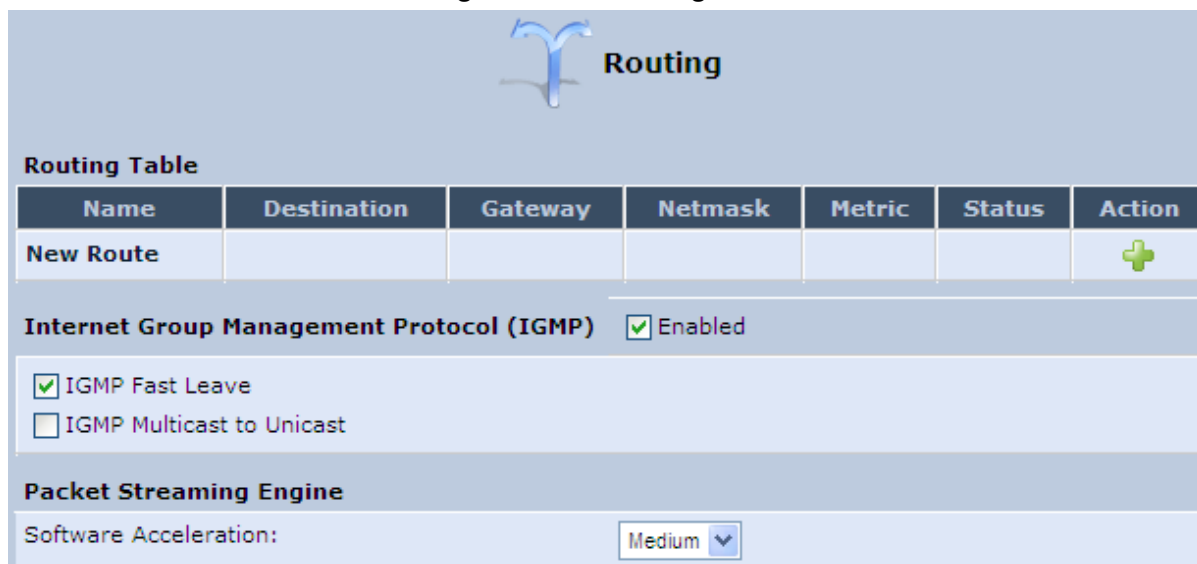
15.4 Routing


This section describes how to configure routing rules and enable routing protocols. These are configured in the 'Routing' screen, as described below.

➤ **To access the Routing screen:**

- In the 'Advanced' screen, click the **Routing**  icon; the 'Routing' screen appears.

Figure 15-11: Routing Rules



Name	Destination	Gateway	Netmask	Metric	Status	Action
New Route						

Internet Group Management Protocol (IGMP) Enabled

IGMP Fast Leave
 IGMP Multicast to Unicast

Packet Streaming Engine

Software Acceleration: Medium ▾

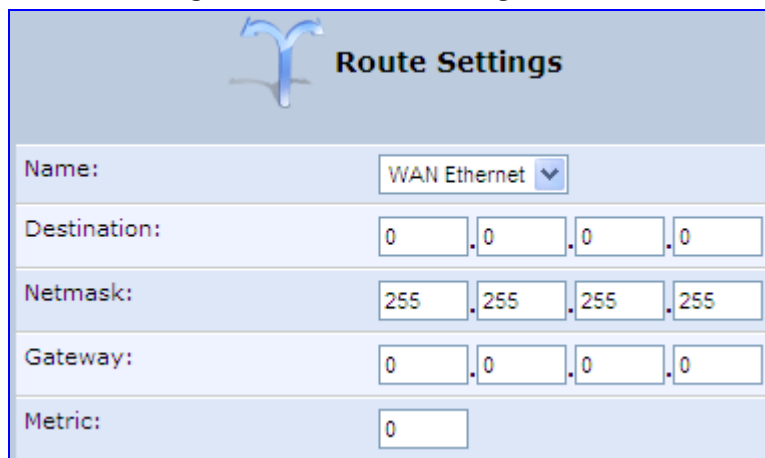
15.4.1 Managing Routing Table Rules

The procedure below describes how to add routing rules.

➤ **To add routing tables:**

1. In the 'Advanced' screen, click the **New**  icon in the **Routing Table**; the 'Route Settings' screen appears.

Figure 15-12: Route Settings Screen



Route Settings

Name: WAN Ethernet ▾

Destination: . . .

Netmask: . . .

Gateway: . . .

Metric:

2. From the 'Name' drop-down list, select the network device for which you want to add a routing rule.

3. In the 'Destination' field, enter the destination host, subnet address, network address, or default route. The destination for a default route is "0.0.0.0".
4. In the 'Netmask' field, enter the network mask that used in conjunction with the destination to determine when a route is used.
5. In the 'Gateway' field, enter the MP252's IP address.
6. In the 'Metric' field, enter the measurement of the preference of a route. Typically, the lowest metric is the most preferred route. If multiple routes exist to a given destination network, the route with the lowest metric is used.
7. Click **OK** to save your settings.

15.4.2 Routing Protocols

MP252 supports IGMP multicasting, which allows hosts connected to a network to be updated whenever an important change occurs in the network. A multicast is simply a message that is sent simultaneously to a pre-defined group of recipients. When you join a multicast group you receive all messages addressed to the group, similar to an e-mail message sent to a mailing list.

IGMP multicasting enables UPnP capabilities over wireless networks and may also be useful when connected to the Internet through a router. When an application running on a computer in the home network sends out a request to join a multicast group, MP252 intercepts and processes the request. If MP252 is set to 'Minimum Security', no further action is required. However, if MP252 is set to 'Typical Security' or 'Maximum Security', you must add the group's IP address to MP252's 'Multicast Groups' screen. This allows incoming messages addressed to the group to pass through the MP252 firewall and on to the correct LAN computer.

➤ To configure routing protocols:

1. In the 'Advanced' screen, under the **Internet Group Management Protocol (IGMP)** group, do the following:
 - a. Select the 'Enabled' check box to enable IGMP multicasting.
 - b. Select the 'IGMP Fast Leave' check box if you want MP252 to stop forwarding traffic to a host that is the only subscriber, immediately upon request (without query delay).
 - c. Select the 'IGMP Multicast to Unicast' check box to enable MP252 to convert the incoming multicast data stream into unicast format to route it to the specific LAN host that requested the data. In this way, MP252 prevents flooding the rest of the LAN hosts with irrelevant multicast traffic.
2. Under the **Packet Streaming Engine** group, from the 'Software Acceleration' drop-down list, select the packet flow speed:
 - **None:** Packet Streaming Engine (PSE) is disabled
 - **Medium:** PSE is active (recommended)
 - **High:** PSE traffic is prioritized over other traffic
3. Click **OK**.

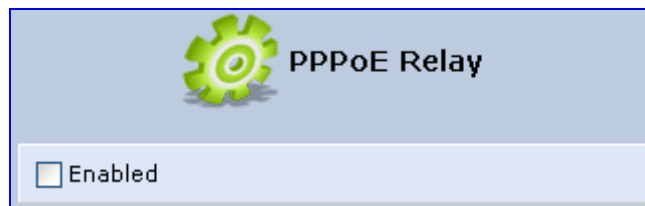
15.5 PPPoE Relay

PPPoE relay enables MP252 to relay packets on PPPoE connections while keeping its designated functionality for any additional connections.

➤ To enable PPPoE relay:

1. In the 'Advanced' screen, click the **PPPoE Relay**  icon; the 'PPPoE Relay' screen appears.

Figure 15-13: PPPoE Relay Screen



2. Select the 'Enabled' check box.
3. Click **OK**.

16 Home Media

16.1 Universal Plug and Play

Universal Plug-and-Play (UPnP) is a networking architecture that provides compatibility among networking equipment, software, and peripherals. UPnP-enabled products can seamlessly connect and communicate with other UPnP-enabled devices without the need for user configuration, centralized servers, or product-specific device drivers. This technology leverages existing standards and technologies, including TCP/IP, HTTP 1.1 and XML, facilitating the incorporation of UPnP capabilities into a wide range of networked products for the home.

UPnP technologies are rapidly adopted and integrated into widely-used consumer products such as Windows XP. Therefore it is critical that today's Residential Gateways be UPnP-compliant. Your MP252 is at the forefront of this development, offering a complete software platform for UPnP devices. This means that any UPnP-enabled control point (client) can dynamically join the network, obtain an IP address and exchange information about its capabilities and those of other computers on the network. They can subsequently communicate with each other directly, thereby further enabling peer-to-peer networking. And this all happens automatically, providing a truly zero-configuration network.

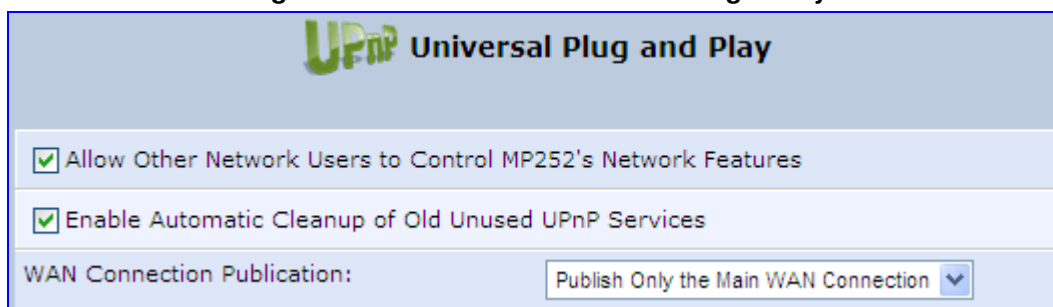
16.1.1 Enabling UPnP on MP252

The procedure below describes how to enable the UPnP feature on MP252.

➤ **To enable UPnP:**

1. In the 'Advanced' screen, click the **Universal Plug and Play**  icon; the 'Universal Plug and Play' screen appears.

Figure 16-1: Advanced - Universal Plug n Play



2. Select the 'Allow Other Network Users to Control MP252's Network Features' to enable the UPnP feature. This allows you to define UPnP services on any of the LAN hosts.
3. Select the 'Enable Automatic Cleanup of Old Unused UPnP Services' to enable automatic cleanup of invalid rules. This feature checks the validity of all UPnP services every five minutes, and removes old and obsolete services, unless a user-defined rule depends on them.
4. From the 'WAN Connection Publication' drop-down list, select which WAN information is published by MP252. By default, MP252 publishes only its main WAN connection, which is controllable by UPnP entities. However, you may select the 'Publish All WAN Connections' option if you wish to grant UPnP control over all of MP252's WAN connections.

16.1.2 Adding UPnP-enabled PC to Home Network

If your computer is running an operating system that supports UPnP such as Windows XP, you can add the computer to your home network and access the Web-based Management directly from Windows.

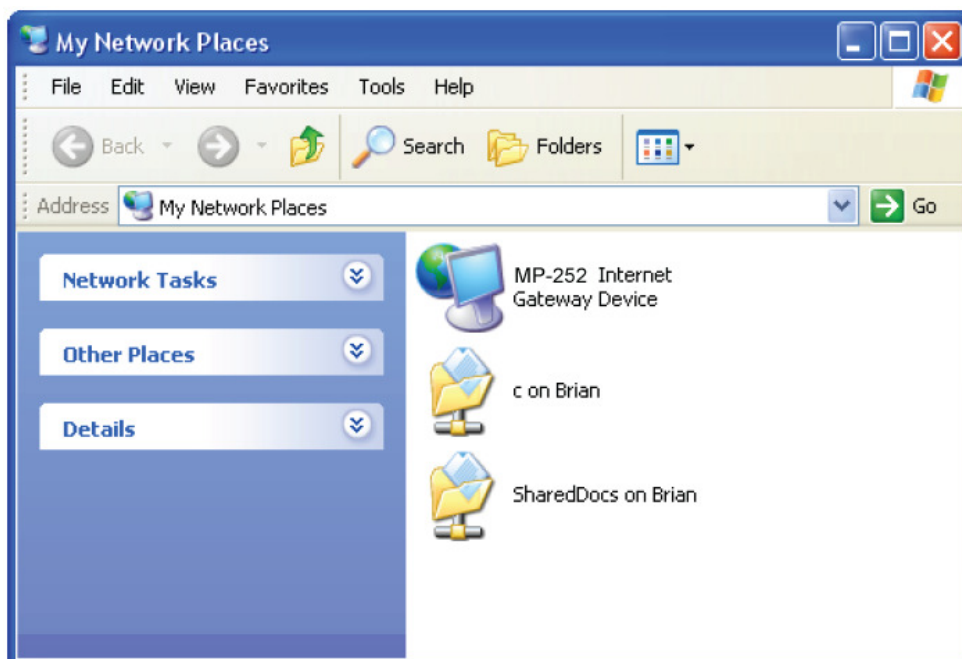
➤ **To add a UPnP-enabled computer to the home network:**

- Connect the PC to MP252; the PC automatically recognizes and adds to the home network. MP252 is added to 'My Network Places' as the Internet Gateway Device and allows configuration via a standard Windows interface. A message appears on the notification area of the taskbar notifying that the PC has been added to the network.

➤ **To access the Web-based management directly from Windows:**

1. Open the 'My Network Places' window by double-clicking its desktop icon.

Figure 16-2: My Network Places



2. Double-click the **MP252 Internet Gateway Device** icon. The MP252 Web interface 'Login' screen appears in a browser window. This method is similar to opening a browser window and typing in '192.168.1.1'.

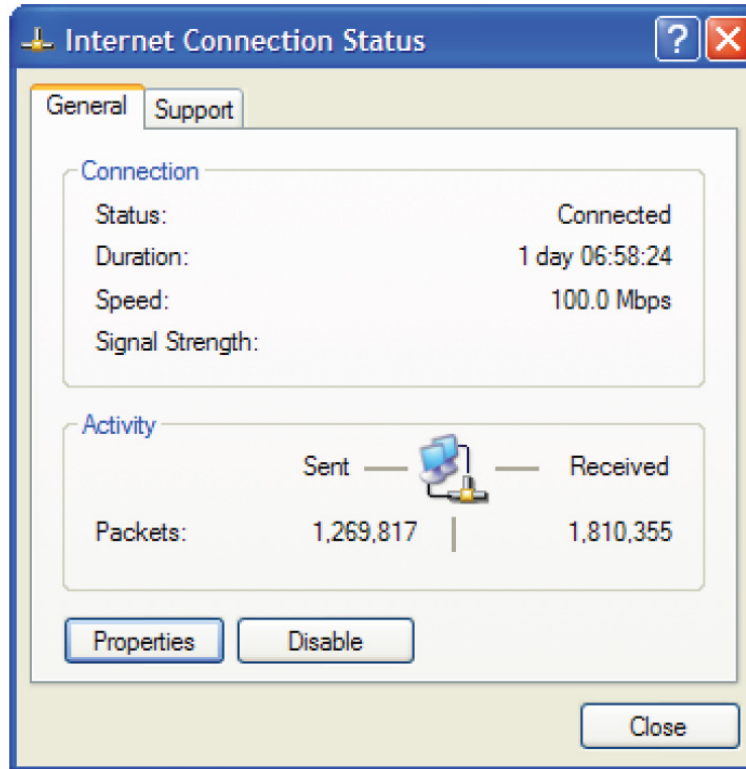
16.1.3 Monitoring Connection between MP252 and Internet

The procedure below describes how to monitor the status of the connection between MP252 and the Internet.

➤ **To monitor the status of the connection between MP252 and the Internet:**

1. Open the 'Network Connections' control panel.
2. Double-click the **Internet Connection** icon. The 'Internet Connection Status' window appears:

Figure 16-3: Internet Connection Status



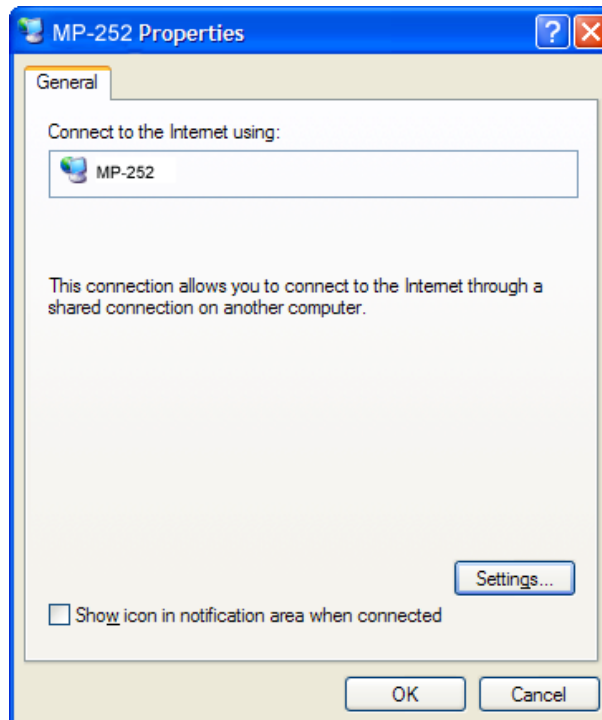
16.1.4 Making Local Services available to PCs on Internet

You can make services provided by computers in the home network available to computers on the Internet. For example, you may designate a PC in your home network to act as a Web server, allowing computers on the Internet to request pages from it. Or a game that you want to play over the Internet may require that specific ports be opened to allow communication between your PC and other players.

➤ **To make local services available to computers on the Internet:**

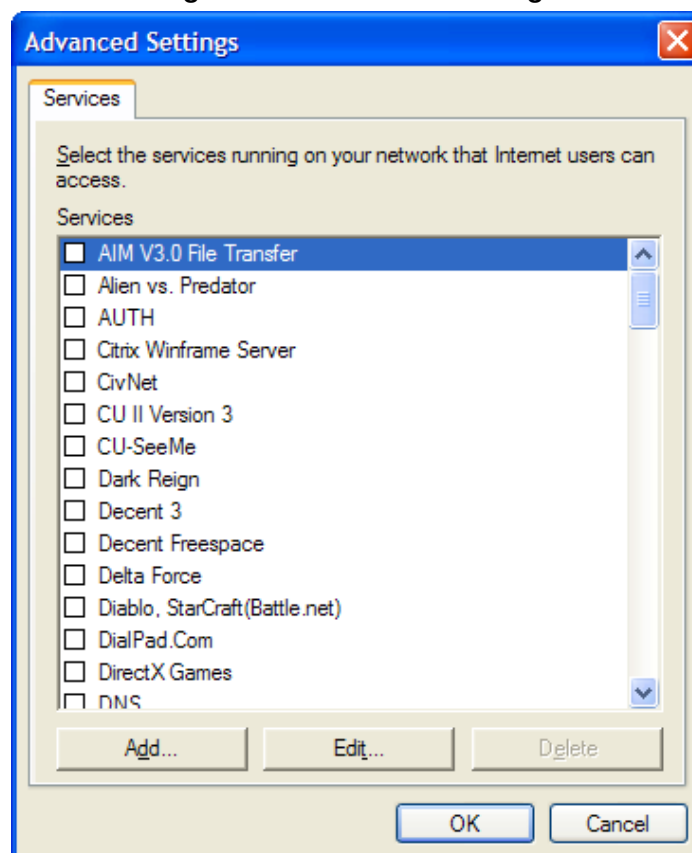
1. Open the 'Network Connections' control panel.
2. Right-click 'Internet Connection', and then choose **Properties**; The 'Internet Connection Properties' window appears.

Figure 16-4: Internet Connection Properties



3. Click the **Settings** button; the 'Advanced Settings' window.

Figure 16-5: Advanced Settings



4. Select a local service that you would like to make available to computers on the Internet; the 'Service Settings' window automatically appears.

Figure 16-6: Service Settings

5. Enter the local IP address of the computer that provides this service and then click **OK**.
6. Select other services as desired and repeat the previous step for each.
7. Click **OK** to save the settings.

➤ **To add a local service that is not listed in the 'Advanced Settings' window:**

1. Follow steps 1-3 above.
2. Click the **Add** button; the 'Service Settings' window appears.

Figure 16-7: Service Settings – Add Service

3. Complete the fields as indicated in the window.
4. Click **OK** to close the window and return to the 'Advanced Settings' window; the service is selected.
5. Click **OK** to save the settings.

17 Add-On Servers and Disk Management

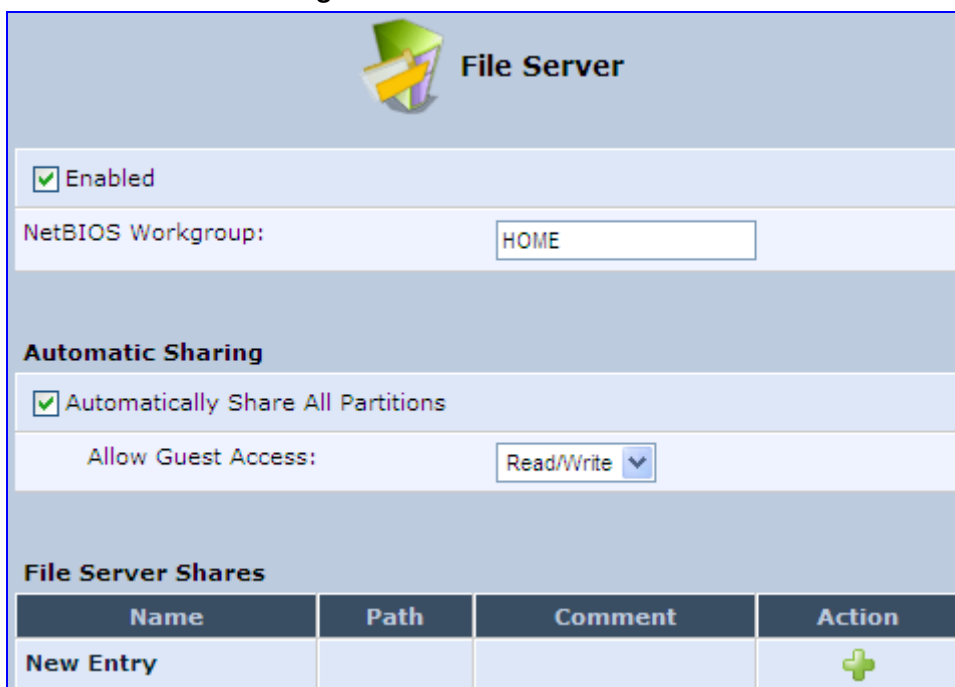
17.1 External File Server


MP252 provides a file server utility, allowing you to perform various tasks on your files, such as manage file server shares and define access control lists. The file server utility complements MP252's disk management.

➤ **To configure the file server:**

1. In the 'Advanced' screen, click the **File Server**  icon; the screen 'File Server' opens.

Figure 17-1: File Server Screen



Name	Path	Comment	Action
New Entry			

2. Configure the following:
 - **Enabled:** Select or clear this check box to enable or disable this feature.
 - **NetBIOS Workgroup:** MP252 workgroup name that is displayed in the Windows network map of LAN hosts.
 - **Automatic Sharing:**
 - ◆ **Automatically Share All Partitions:** A partitioned storage device connected to MP252 is automatically displayed and shared by all LAN computers. This feature is enabled by default.

- ◆ **Allow Guest Access:** From the drop-down list, select a permission level, according to which the LAN users access the share:
 - ✓ **Read/Write:** Every LAN user can read and write the shared files without authentication.
 - ✓ **Read Only:** Every LAN user can only read the shared files.
 - ✓ **Disabled:** LAN users must authenticate themselves to access the share. They can use the share according to their permissions defined in the 'User Settings' screen.
- **File Server Shares:** Define file shares on your disk partitions, as described in the following sections.

17.1.1 Automatic File Sharing

By default, all partitions are automatically shared and displayed.

➤ To share specific directories or partitions:


1. Clear the 'Automatically Share All Partitions' check box, and then click **Apply**. The list of all automatically shared partitions disappears.
2. In the 'File Server Shares' table, click **New**  icon to define a new share; the 'File Server Share Settings' screen appears.

Figure 17-2: File Server Share Settings Screen



File Server Share Settings		
Name:	<input type="text" value="share"/>	
Path:	<input type="text"/>	
Comment:	<input type="text"/>	
Users		
Name	Access Level	Action
New User		
Groups		
Name	Access Level	Action
New Group		

3. Enter the share's name (default is "share"), path, and (optionally) comment. The share's name is not case sensitive. Even if entered in upper-case letters, the name is displayed in lower case after saving the setting.
4. Associate a user or group of users with the share to grant them access to the shared files, by clicking the **New User** or **New Group** link in the Users or Groups table. Note that the user's settings must have the 'Microsoft File and Printer Sharing Access' check box selected under the 'Permissions' section (see 'Configuring Users' on page 44); the 'User' screen appears:

Figure 17-3: User Screen

- d. From the 'Name' drop-down list, select the user name and the allowed access.
 - e. Click **OK**.
5. Click **OK** to save the settings. The 'File Server' screen appears, displaying the share.

Figure 17-4: File Server Screen with the Share


File Server Shares			
Name	Path	Comment	Action
share	A, B/my_documents		
New Entry			

Click the share's name to view its content. The screen refreshes as the share is accessed. This screen enables you to modify and view the content of your file share. In the upper section of this screen, you can modify your file share by adding files or directories to it. Use the drop-down list to select an action:

- **Upload a File:** Uploads a file to the share. The screen refreshes - enter the location of the file to upload, or click the **Browse** button to browse for the file. Click the **Upload** button to upload the file.
- **Upload a Directory:** You can also upload an entire directory of files, by performing the following:
 - a. Create a tarball archive out of the target directory.
 - b. Enter the location of the archive, or click the **Browse** button to browse to its location.
 - c. Click the **Upload** button to upload the archive.
- **Create a new Directory:** You can create a new directory by simply typing its name and clicking **Go**.
- **Paste from Clipboard:** This option appears only after using the 'Copy to Clipboard' option to copy a directory or file from one directory to another.

The lower section of the screen displays your share's content. You can click the different directory names to access them or you can download, rename, copy or remove the directories using the standard action icons.

17.2 Disk Management

The **Disk Management**  icon allows you to configure disk management. MP252 can operate as a disk manager for either internal disks connected through IDE, or external storage devices connected through USB or FireWire. Your home-network's LAN devices can share this storage device as a mapped network drive and exchange information without directly accessing each other. The Web interface provides disk management utilities such as partitioning and formatting.

An internal disk or a connected storage device appears in the Network Map (see Section 5 on page 55). You can view information about the disk by clicking its icon.

The device supports storage devices with FAT32, NTFS, and Linux EXT2/3 file systems. These file systems have different sharing and security settings. If the connected storage device or at least one of its partitions has the NTFS file system, a message appears in the 'Disk Management' screen appears.

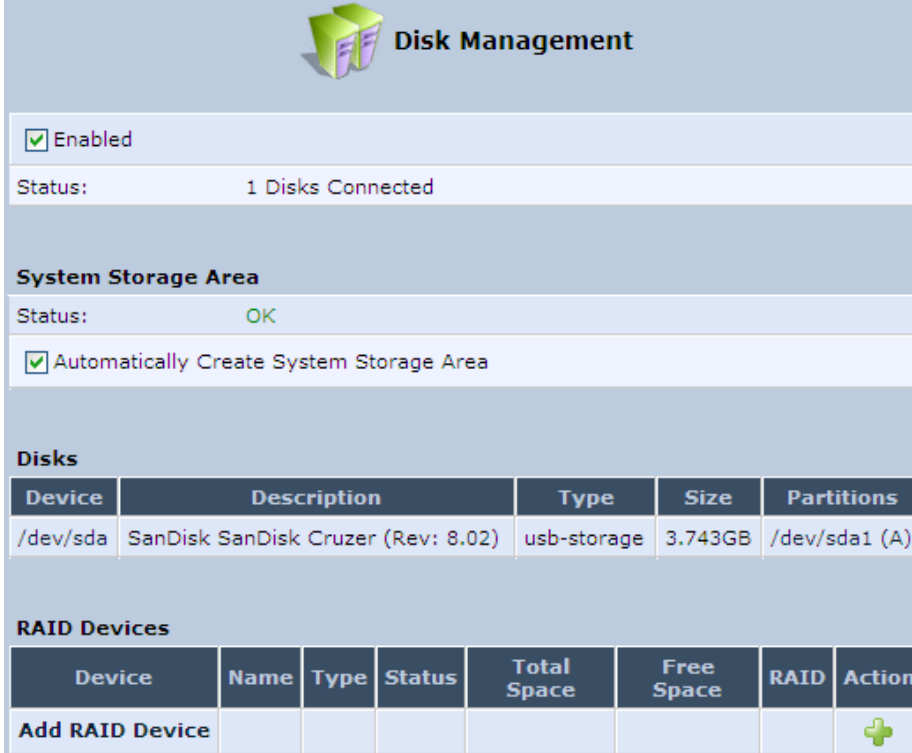


Note: MP252 based on the Conexant Solos, Mindspeed Malindi2 or Freescale platform allows both read and write access to an NTFS partition.

➤ **To configure disk management:**

1. In the 'Advanced' screen, click the  icon; the 'Disk Management' screen appears.

Figure 17-5: Disk Management Screen




System Storage Area
Status: OK
 Automatically Create System Storage Area

Disks

Device	Description	Type	Size	Partitions
/dev/sda	SanDisk SanDisk Cruzer (Rev: 8.02)	usb-storage	3.743GB	/dev/sda1 (A)

RAID Devices

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
Add RAID Device							



Note: To define a system storage area, the disk or at least one of its partitions should be formatted. This storage area holds the data used by the MP252's services. For security, it is recommended to format the disk or its partition in the EXT2 or EXT3 file system, although FAT32 is supported as well.

2. To enable disk management, select the 'Enabled' check box.

3. To set the first identified formatted partition as the location of the system storage area, select the 'Automatically Create System Storage Area' check box. This setting is valid until the storage device is disconnected. When reconnected, MP252 may select another partition for this purpose. To define the system storage area manually, clear this check box. The screen refreshes, displaying the 'System Storage Area' field in which you must enter the partition's letter. In this scenario, the setting remains permanent even after the storage device is disconnected and reconnected afterwards.

Figure 17-6: Manually Defining System Storage Area

System Storage Area	
Status:	The system storage disk <A> is not connected, mounted and formatted. Advanced web, VoIP and mail services are disabled
<input type="checkbox"/> Automatically Create System Storage Area	
System Storage Area:	<input type="text" value="A"/>

4. In the **Disks** table, you can view a list of your connected storage devices. The 'Device' column displays the names MP252 grants connected devices. Click this link to view the device's 'Disk Information' screen. If a disk is partitioned, the 'Partitions' column displays its partition names. If the partitions are formatted, their name includes a letter.
5. In the **RAID Devices** table, you can view the RAID devices (if configured).

17.2.1 Disk Partitions

This section describes how to configure partition and format storage devices.

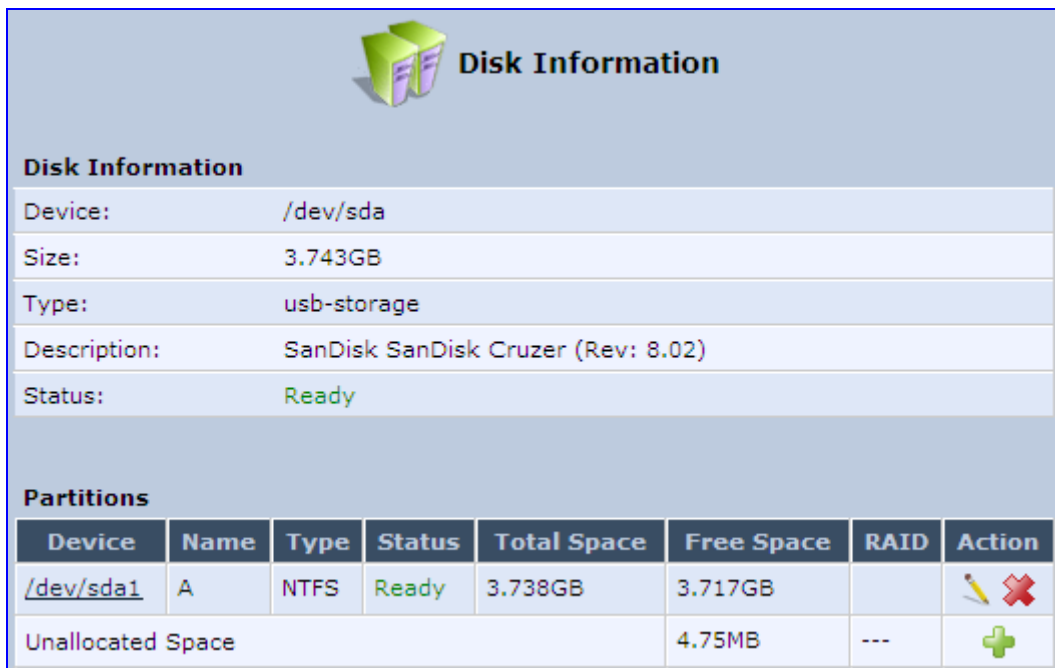
17.2.1.1 Connecting a Mass Storage Device

To set up a file server that is shared by all LAN computers, you need to connect a mass storage device (e.g. disk-on-key or hard drive) to the USB port on your MP252. A mass storage device must first be partitioned and formatted. If your device is already partitioned, it is recommended that you delete its partitions before proceeding, as a partition can only be added on unallocated disk space.

➤ **To add a Windows formatted partition:**

1. In the **Disks** table in the 'Disk Management' screen, click the disk device link. The 'Disk Information' screen appears.

Figure 17-7: Disk Information






Disk Information

Disk Information

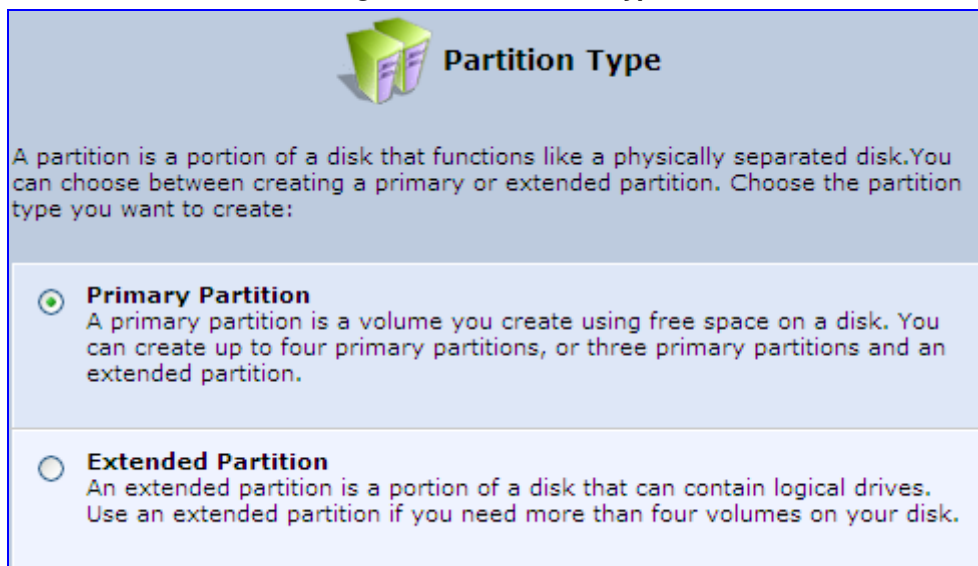
Device: /dev/sda
 Size: 3.743GB
 Type: usb-storage
 Description: SanDisk SanDisk Cruzer (Rev: 8.02)
 Status: Ready

Partitions

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/sda1	A	NTFS	Ready	3.738GB	3.717GB		 
Unallocated Space					4.75MB	---	

2. In the 'Partitions' table, click the **Add New Partition** icon; the 'Partition Type' screen appears.

Figure 17-8: Partition Type



Partition Type

A partition is a portion of a disk that functions like a physically separated disk. You can choose between creating a primary or extended partition. Choose the partition type you want to create:

Primary Partition
 A primary partition is a volume you create using free space on a disk. You can create up to four primary partitions, or three primary partitions and an extended partition.

Extended Partition
 An extended partition is a portion of a disk that can contain logical drives. Use an extended partition if you need more than four volumes on your disk.

3. Select 'Primary Partition', and then click **Next**; the 'Partition Size' screen appears.

Figure 17-9: Partition Size

Choose a partition size. Make sure that the partition size is between the following minimum and maximum sizes.

Maximum Disk Space:	5 MB
Minimum Disk Space:	4 MB
Partition Size:	<input type="text" value="5"/> MB

4. Enter a volume for the new partition (in mega bytes), and then click **Next**; the 'Partition Format' screen appears.

Figure 17-10: Partition Format

You must format the partition in order to store data on it. Choose whether you want to format the partition:

- Format the Partition**
You will be able to store data on the partition.
- Do not Format the Partition**
You will not be able to store data on the partition. You may format the partition at a later time.

5. Select 'Format the Partition', and then click **Next**; the 'Partition File System' screen appears.

Figure 17-11: Partition File System

Choose the file system to be used on the partition:

File System:

Check for Bad Blocks (This may take a long time)


- Select 'Windows (FAT32) (LBA)' as the file system for the partition and then click **Next**; the 'Partition Summary' screen appears.

Figure 17-12: Partition Summary



- Click **Finish** to create the new partition; the 'Disk Information' screen reappears, refreshing as the partition formatting progresses, until the status changes to 'Ready'.





Figure 17-13: Formatting Complete – Partition Ready

 **Disk Information**

Disk Information

Device:	/dev/sda
Size:	3.743GB
Type:	usb-storage
Description:	SanDisk SanDisk Cruzer (Rev: 8.02)
Status:	Ready

Partitions

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/sda1	A	NTFS	Ready	3.738GB	3.717GB		 
/dev/sda2	B	Windows FAT32 (LBA)	Ready	3.681MB	3.68MB		 

The new partition names are designated as "A", "B" etc, and appear under the 'Name' column of the 'Partitions' section.

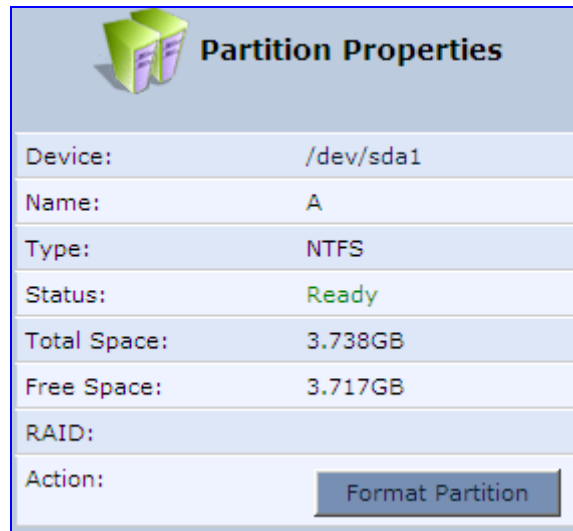
17.2.1.2 Formatting a Partition

A partition can be formatted in EXT2, EXT3, FAT32 and NTFS file systems.

➤ **To partition a disk:**

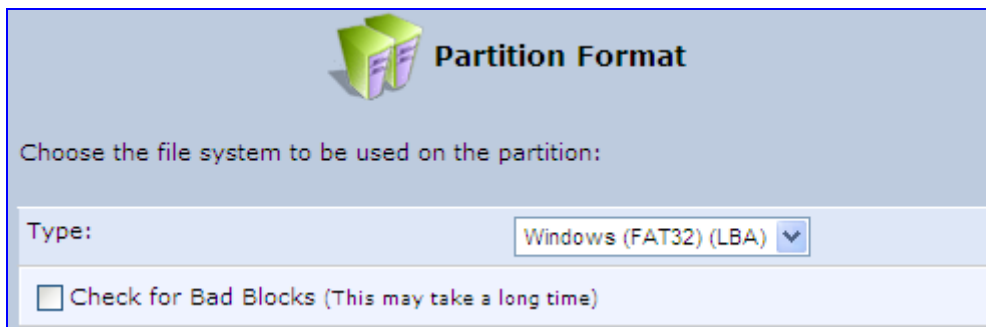
1. In the **Disks** table in the 'Disk Management' screen, click the disk device link; the 'Disk Information' screen appears.
2. In the 'Partitions' table, click the **Edit Partition** icon of the partition you would like to edit; the 'Partition Properties' screen appears.

Figure 17-14: Partition Properties



3. Click **Format Partition**; the 'Partition Format' screen appears.

Figure 17-15: Partition Format



4. Select a file system for the partition and then click **Next**. A warning screen appears, alerting you that all the data on the partition will be lost.
5. Click **OK** to format the partition; the screen refreshes as the partition formatting progresses. When the format is complete, the status will change to 'Ready'.

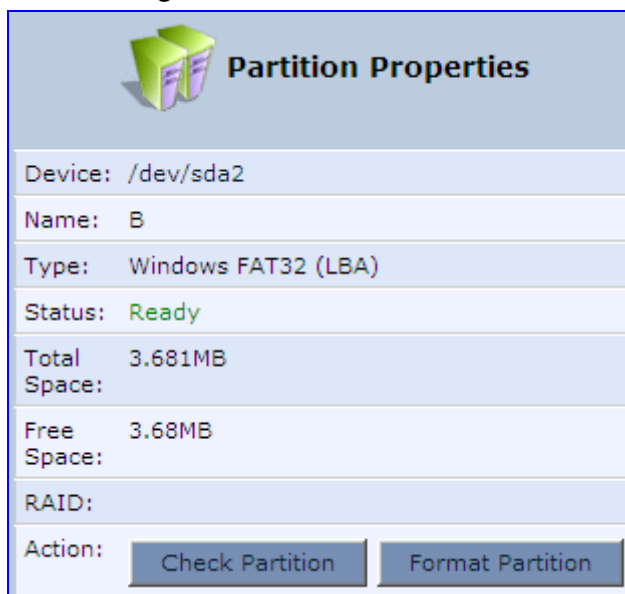
17.2.1.3 Checking a Partition

The procedure below describes how to check a partition.

➤ **To check a partition:**

1. In the **Disks** table in the 'Disk Management' screen, click the disk device link; the 'Disk Information' screen appears.
2. In the 'Partitions' section, click the **Edit Partition** icon of the partition you would like to check; the 'Partition Properties' screen appears.

Figure 17-16: Partition Format



3. Click **Check Partition**; a warning screen appears, alerting you that the partition will be set to offline.
4. Click **OK**; the screen refreshes as the partition checking progresses. When the check is complete, the status changes to 'Ready'.

17.2.1.4 Deleting a Partition

The procedure below describes how to delete a partition.

➤ **To delete a partition:**

1. In the **Disks** table in the 'Disk Management' screen, click the disk device link; the 'Disk Information' screen appears.
2. In the 'Partitions' section, click the **Remove Partition** icon of the partition you would like to delete; a warning screen appears, alerting you that all the data on the partition will be lost.
3. Click **OK** to delete the partition.

17.2.2 System Storage Area

MP252 uses a specific location on a storage device for storing data used by its various services. The following are the services that use the system storage area:

- Printer spool and drivers
- Mail server spool
- Backup of MP252's configuration file (rg_conf)
- PBX-related audio files for voice mail, auto attendants and music on-hold
- FTP server
- Mail boxes information
- Users' home directories
- Web server content

Prior to enabling these services, you should create either EXT2/3 (recommended) or FAT32 partitions, as described in the previous sections, and define at least one of them as the system storage area.




Note: Data cannot be written to partitions formatted with NTFS, unless MP252 is based on the Conexant Solos, Mindspeed Malindi2 or Freescale platform. Consequently, if you define an NTFS partition as the system storage area, the services mentioned earlier will not operate on MP252.

➤ **To define a system storage area:**

1. Under the **System Storage Area** group in the 'Disk Management' screen, clear the 'Automatically Create System Storage Area' check box; the screen refreshes displaying the 'System Storage Area' field, in which you must enter the partition's letter.

Figure 17-17: Disk Management Screen – Check Box Cleared



Disk Management

Enabled

Status: 1 Disks Connected

System Storage Area

Status: OK

Automatically Create System Storage Area

System Storage Area:

Disks

Device	Description	Type	Size	Partitions
/dev/sda	SanDisk SanDisk Cruzer (Rev: 8.02)	usb-storage	3.743GB	/dev/sda1 (A) /dev/sda2 (B)

RAID Devices

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
Add RAID Device							+

2. Click **OK** to save the settings.

If you wish to view the system directories, verify that the system storage area is shared. Then, browse to \\mp252 (use a Windows Explorer window if you are using a browser other than Internet Explorer).

17.2.3 RAID Management

MP252 supports Redundant Array of Independent Disks (RAID) on storage devices connected to it by USB or by FireWire. A RAID device is a logical device that has physical devices underlying it. These physical devices are disk partitions. The supported RAID levels are:

- Level 0 – Provides data striping, or spreading out blocks of each file across multiple disk drives, but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost.
- Level 1 – Provides disk mirroring. This is a technique in which data is written to two duplicate disks simultaneously, providing data redundancy. This method improves performance and delivers fault tolerance.
- Level 5 – With a minimum of three disks, this level provides data striping and utilizes one disk for backup information, which enables it to restore any other disk in the array.

Before creating the RAID device, you must create disk partitions (as described previously) on the different disk drives. Each RAID device can have multiple underlying devices (partitions). When using RAID1, it is recommended that these partitions be of the same size to avoid disk-space loss due to mirroring. A disk partition configured with RAID can no longer be managed as a regular partition, but only be controlled by the RAID device. From the moment RAID is configured, it is the RAID device that can be shared, scanned, formatted and mounted as a regular partition.

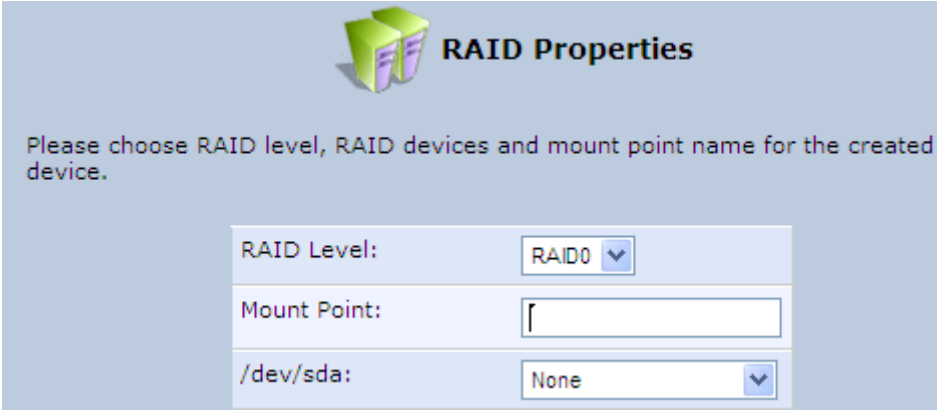
17.2.3.1 Creating a RAID Device

The procedure below describes how to create a RAID device.

➤ **To create a RAID device:**

1. In the **RAID Devices** table in the 'Disk Management' screen, click the **Add RAID Device** link; the 'RAID Properties' screen appears:

Figure 17-18: RAID Properties Screen



RAID Properties

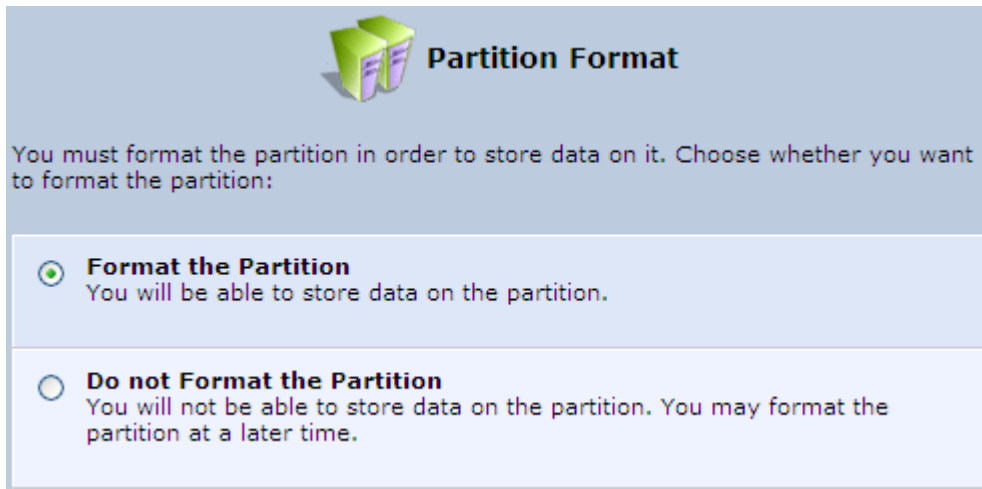
Please choose RAID level, RAID devices and mount point name for the created device.

RAID Level:	RAID0
Mount Point:	
/dev/sda:	None

2. From the 'RAID Level' drop-down list, select the RAID level (RAID0, RAID1 or RAID5).
3. In the 'Mount Point' field, enter a name for the mount point of the RAID device.
4. Choose the underlying devices (your pre-configured partitions) in the next drop-down lists. For RAID1 you may choose only one device and later add another one.

- Click **Next**; the 'Partition Format' screen appears.

Figure 17-19: Partition Format Screen



Partition Format

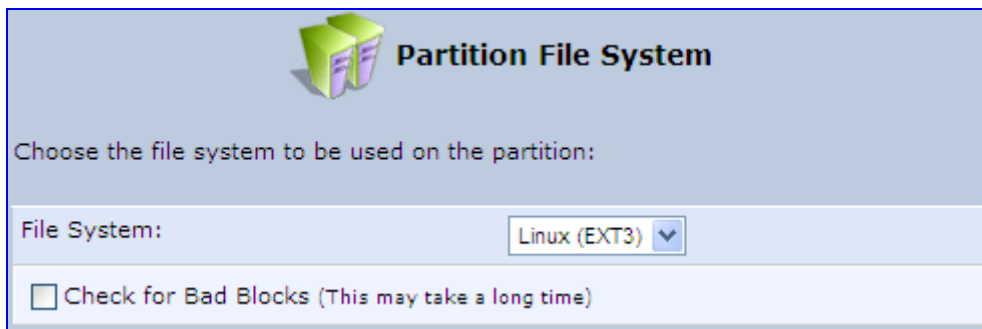
You must format the partition in order to store data on it. Choose whether you want to format the partition:

Format the Partition
You will be able to store data on the partition.

Do not Format the Partition
You will not be able to store data on the partition. You may format the partition at a later time.

- Select 'Format the partition' and then click **Next**.

Figure 17-20: Partition File System Screen



Partition File System

Choose the file system to be used on the partition:

File System: ▼

Check for Bad Blocks (This may take a long time)

- Select the format type, and then click **Next**; the 'Partition Summary' screen displays a summary of the chosen device properties.

Figure 17-21: Partition Summary Screen



Partition Summary

You have successfully completed the steps needed to create the following new partition:






- Partition Type: RAID
- RAID Level: RAID1
- Mount Point: Mount_0
- Devices:
 - /dev/sda1 **Device is online**
- **Online underlying devices will be taken offline. This may cause some disk based services to stop.**
- File System: Linux (EXT3)

- Click the **Finish** button to execute the RAID device creation.

As soon as a RAID device is created, its formatting begins. If the device is RAID1 and has two underlying devices, its re-synchronization process (partition mirroring) begins simultaneously. During re-synchronization the RAID device is fully usable and can be mounted and used.

The figure below depicts a successful configuration of two RAID devices as they appear in the **Raid Devices** table in the 'File Server' screen. The first is RAID0, consisting of two underlying partitions (one on each disk), and the second is RAID1, consisting of another set of underlying partitions. Note that the RAID0 total space is the sum of the two partitions, while the RAID1 total space is the size of one partition (due to mirroring).

Figure 17-22: Added RAID Devices

Device	Name	Type	Status	Total Space	Free Space	RAID	Action
/dev/md0	mount_0	Linux (EXT3)	Ready	154.8MB	142.8MB	RAID0: /dev/sda1, /dev/sdb1	 
/dev/md1	mount_1	Linux (EXT3)	Ready	41.39MB	35.23MB	RAID1: /dev/sda2, /dev/sdb2	 
Add RAID Device							


17.2.3.2 Using a RAID Device

When RAID is configured over the existing partitions, these partitions are no longer independent. It is therefore necessary that you update the location of the system storage area:

1. In the 'Disk Management' screen, verify that the 'Automatically Create System Storage Area' check box is selected. If you wish to define the system storage area manually, clear the check box and enter the name of the designated mount point.
2. Click **OK** to save the settings.

17.2.3.3 Maintaining a RAID Device

A RAID device differs from a regular partition by not being part of a physical disk. It therefore resides and is maintained on MP252. RAID maintenance is divided into two aspects:

- Maintaining the RAID device itself:
 - In the **RAID Device** table in the 'Disk Management' screen, click the **Edit**  icon of the RAID device; the 'RAID Properties' screen appears in which you can:
 - ◆ Enable or disable the RAID device using the 'Enabled' check box.
 - ◆ Change the mount point assigned to the device.
 - ◆ Add or remove the underlying devices (can be done for RAID1 and RAID5 only).
- Maintaining the partition:
 - In the 'RAID Properties' screen, click the device name; the 'Partition Properties' screen appears in which you can check and format the RAID partition.

17.2.3.4 Replacing RAID Underlying Devices

Adding or removing a RAID underlying device can only be performed on RAID1 and RAID5 configurations. RAID1 can operate with just one device (although mirroring is unavailable), and RAID5 can operate with one device less than its original amount of devices.

The names of the RAID underlying devices appear on the 'RAID Properties' screen. Each device is followed by a status:


- Active: The device is controlled by RAID.
- Inactive: The device failed to join the RAID array or does not exist.
- Faulty: The device joined the RAID array but was marked as faulty due to an error. It is inactive and should be replaced.

Replacing a device on RAID1 or RAID5 is done by first removing the faulty device and then adding a new one. The new device's size must be at least the size of the existing one.

➤ **To remove a faulty device from RAID1:**

1. In the 'RAID Properties' screen, click the faulty device's **Delete** icon.
2. Click **OK**.

➤ **To add a new device instead of the one removed:**

1. In the **RAID Device** table in the 'Disk Management' screen, click the **Edit**  icon of the RAID device; the 'RAID Properties' screen appears with a drop-down list allowing you to choose the new partition to be added.
2. Choose the partition, and then click **OK**.

After adding a new device, RAID1 starts a recovery process in which the content of the existing partition is mirrored to the new device. If the addition or recovery fails, the device status is set to inactive (this status appears in the 'RAID Properties' screen. In such cases, the device should be removed and another may be added. You can manipulate your disk partitions. However, it is recommended to configure your disks before setting up RAID. Once RAID is configured, you will not be able to delete an underlying partition, or create a new partition on a disk that one of its partitions is underlying RAID, unless you disable or delete the RAID device. Changing a disk's partition table when its partitions are under RAID (even if RAID is disabled) may result in the need to reconstruct the RAID.

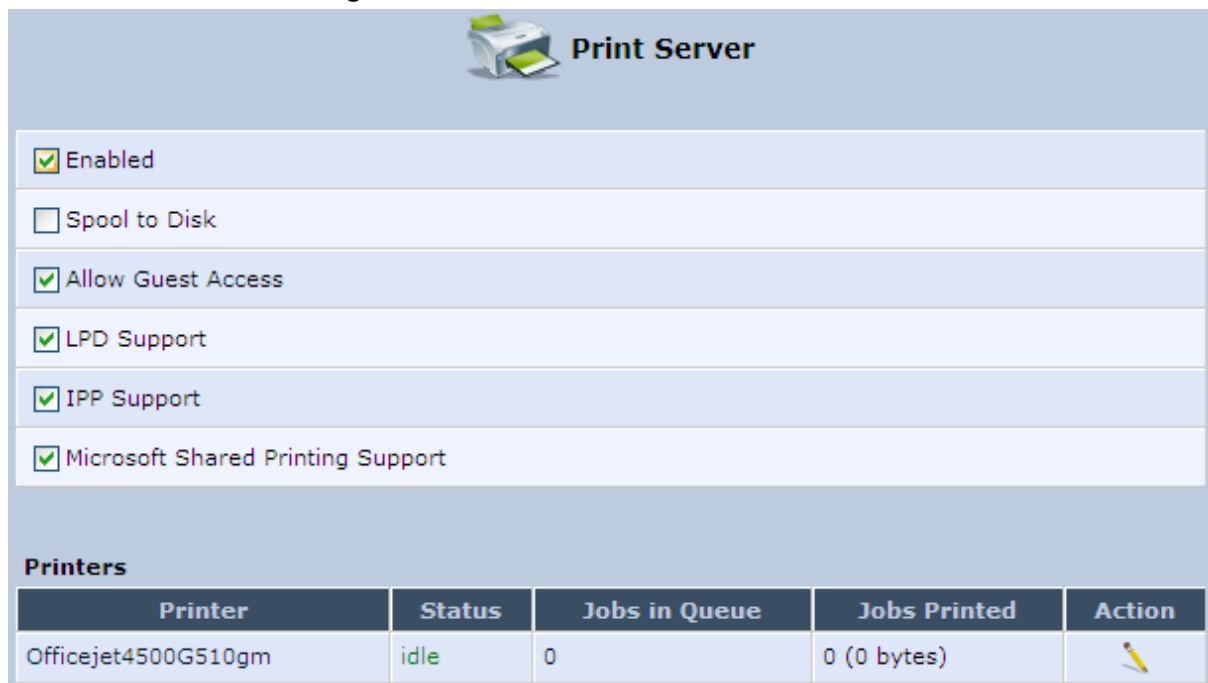
17.3 Print Server

MP252 includes a print server that allows printers attached to MP252 through the USB connection(s) to be shared by all computers on the LAN. Such a printer appears in the Network Map. You can access the printer settings directly, by clicking the printer icon in the Network Map or as described below.

➤ **To configure a print server:**

1. In the 'Advanced' screen, click the **Print Server**  icon; the 'Print Server' screen appears.

Figure 17-23: Advanced – Print Server Screen





2. Select or clear (as required) the following check boxes:
 - **Enabled:** Enables or disables the print server feature.
 - **Spool to Disk:** Allows print jobs to be written to a disk before printing.
 - **Allow Guest Access:** Allows network users that have not logged in with a username and password to use the shared printer. If you want to restrict access to the network printer, you can clear this check box and grant user-specific permissions by creating a user set to 'Internet Printer Access' (see Section 4.4).
 - **LPD Support:** Enables the LPD protocol.
 - **IPP Support:** Enables the IPP protocol.
 - **Microsoft Shared Printing Support:** Enables the Samba protocol.
3. The **Printers** table lists the MP252 printers, their status as well as their print job information. To view the printer's properties and optionally, to define a new name for the printer, click the **Edit**  icon corresponding to the printer; the 'Printer' screen appears.

Figure 17-24: Advanced – Printer Screen

 Printer	
Name:	<input type="text" value="Officejet4500G510gm"/>
IPP URL:	http://MP252.home:631/printers/Officejet4500G510gm
Model:	HP Officejet 4500 G510g-m
Status:	idle
Jobs Printed:	0 (0 bytes)
<input checked="" type="checkbox"/> Create Default Device Mode	

4. To change the displayed name of the printer, in the 'Name' field, enter a new name.
5. To set the printer as the default printer, select the 'Create Default Device Mode' check box.

17.3.1 Connecting and Setting up a Printer on Windows

The procedure below describes how to set up a network printer that is connected to the MP252 USB port and shared by all LAN computers, running on the Windows operating system.

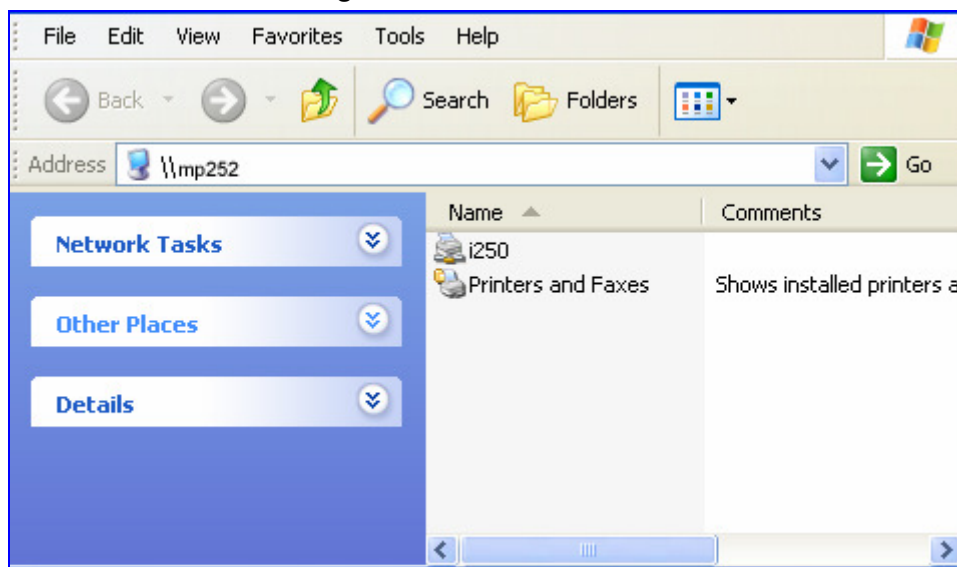


Note: The above configuration must be applied to each LAN PC individually in order to use the network printer.

➤ To set up a printer running on Windows:

1. Log in to MP252; the disk and printer shares available on MP252 is displayed:

Figure 17-25: MP252 Shares



2. Click the printer icon that you want to designate as a LAN printer; a warning appears.

3. Click **Yes**; you are prompted to select a printer driver from a list. If unavailable, you can either browse to a location on your computer where you have stored the driver, or click **Have Disk** and insert the CD containing the driver (supplied with your printer). After a short upload and installation of the driver, the printer's print queue window appears, determining that the printer is ready for use. The new printer is added to your "Printers and Faxes" list as a network printer (to view this list press, in Windows Control Panel, select "Printers and Faxes"). As any printer, you can choose to make it your default printer, or specify its use when printing.
4. Print a test page by right-clicking the printer icon in the disk and printer shares window and selecting **Properties**; the 'Print Test Page' button is located at the bottom of the **General** tab.

17.3.2 Print Protocols

The Samba protocol with which you have created a network printer in the previous section, allows you to upload Windows print drivers to MP252, enabling all Windows-based LAN hosts to connect to the network printer.

MP252 provides two additional protocols for computers to connect to its printers:

- Internet Printing Protocol (IPP) - the recommended protocol, offering fast installation and ease of use.
- Line Printer Daemon (LPD) - legacy network printing protocol, which should only be used for printing from computers that do not support IPP.

The following table compares the specifications of the three protocols:

Table 17-1: IPP, Samba, and LPD Specifications

Specification	IPP	Samba	LPD
Installation	Easy	Easy	Difficult
Driver upload	None	Supported	None
Supported clients	Windows, Unix, Mac	Windows, Mac	Windows, Unix, Mac
Job feedback and control	Print queue monitor and management console	Print queue monitor and management console	Management console only
Printer control	Print queue monitor	None	None
Access controls	Print and administrator	Print permission only	None



Note: **For Mac Users:** When connecting a print server to a MAC computer, you must verify that the printer connected to MP252 is supported by Mac OS as a network printer. Supported printers are marked with an "X" at the following URL: <http://docs.info.apple.com/article.html?artnum=301175#hpdrivers>.

17.3.2.1 Internet Printing Protocol

This section describes how to connect computers to MP252 printers, using the IPP protocol.


17.3.2.1.1 Setting Up an IPP Printer on Windows

The procedure below describes how to set up an IPP printer on Windows.

➤ **To set up an IPP printer on Windows:**

1. In the 'Network Map' screen, click the printer icon to view the 'Printer' screen.

Figure 17-26: Printer Screen – IPP URL

 Printer	
Name:	Officejet4500G510gm
IPP URL:	http://MP252.home:631/printers/Officejet4500G510gm
Model:	HP Officejet 4500 G510g-m
Status:	idle
Jobs Printed:	0 (0 bytes)
<input checked="" type="checkbox"/> Create Default Device Mode	

2. Copy the IPP URL to the clipboard.
3. On your Windows computer connected to MP252, from the **Start** menu, point to **Settings**, then **Printers and Faxes**, and then click **Add Printer**; the Add Printer Wizard starts.
4. Click **Next** to proceed with the wizard sequence.
5. Select 'A network printer...' and then click **Next**.

Figure 17-27: Local or Network Printer


Add Printer Wizard

Local or Network Printer
The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

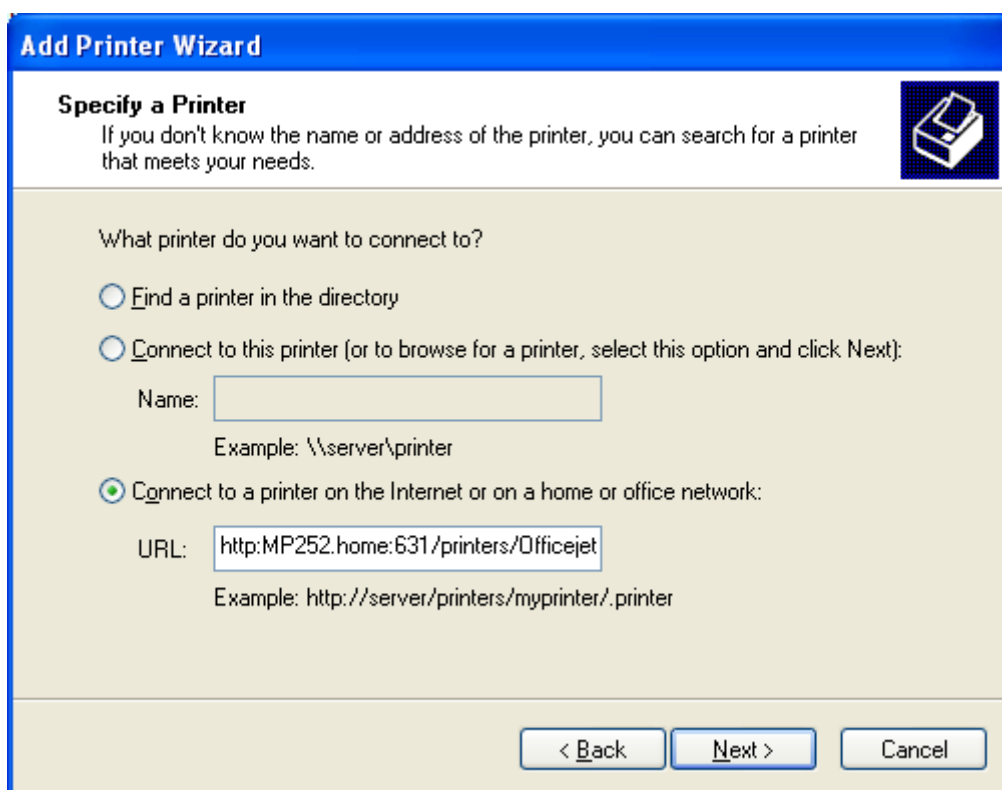
Local printer attached to this computer
 Automatically detect and install my Plug and Play printer

A network printer, or a printer attached to another computer

 To set up a network printer that is not attached to a print server, use the "Local printer" option.

6. Select 'Connect to a printer on the Internet...', and then paste the printer's IPP URL in the 'URL' field, and then click **Next**.

Figure 17-28: Specify a Printer



7. You may be asked to select the driver's make and model or its location. If so, provide the location on MP252 to where you have uploaded the driver (e.g. "\\MP252\A"), and click **Next**.
8. Click **Finish** to exit the wizard.

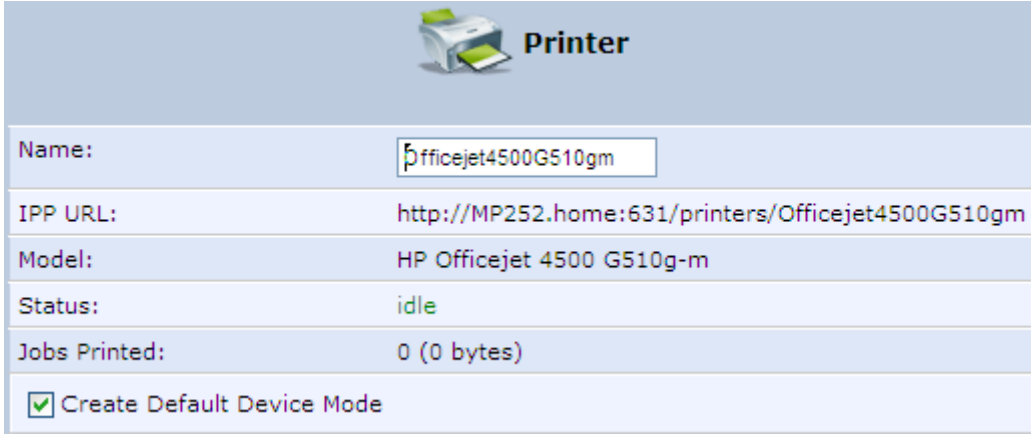
17.3.2.1.2 Setting Up an IPP Printer on Linux

The procedure below describes how to set up an IPP printer on Linux operating systems. You should use CUPS Daemon (CUPSD) when operating with Linux.

➤ **To set up an IPP printer on Linux:**

1. In the 'Network Map' screen, click the printer icon to view the 'Printer' screen.

Figure 17-29: Printer Screen – IPP URL



Printer	
Name:	Officejet4500G510gm
IPP URL:	http://MP252.home:631/printers/Officejet4500G510gm
Model:	HP Officejet 4500 G510g-m
Status:	idle
Jobs Printed:	0 (0 bytes)
<input checked="" type="checkbox"/> Create Default Device Mode	

2. Copy the IPP URL to the clipboard.
3. On your Linux computer connected to MP252, browse to <http://localhost:631>, and then choose **Manage Printers**.

Figure 17-30: Linux CUPS Management



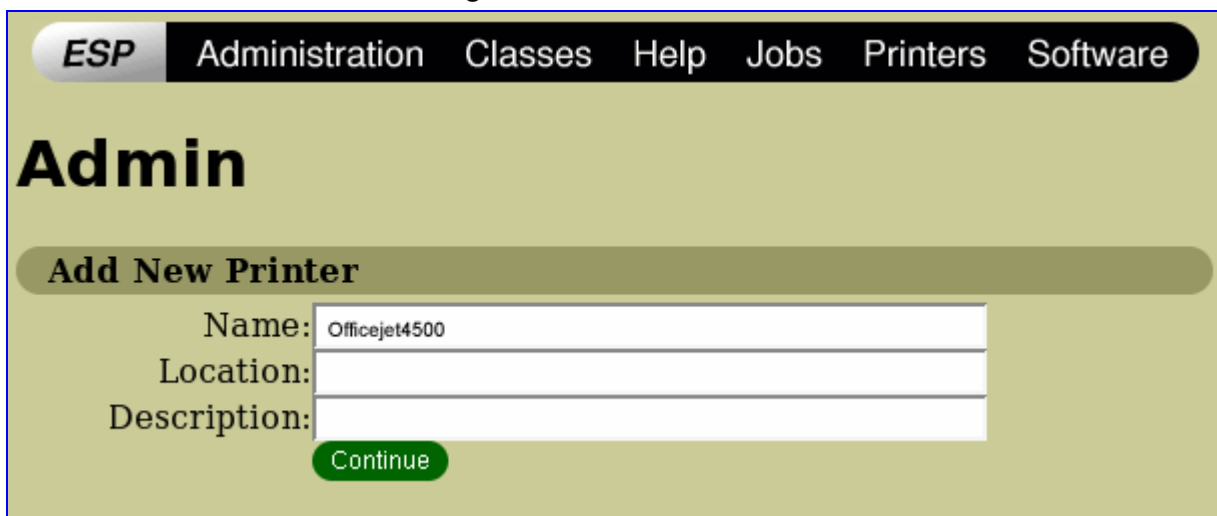
4. Click **Add Printer**.

Figure 17-31: Add Printer



5. In the 'Name' field, type the printer's name and then click **Continue**.

Figure 17-32: Printer Name



6. From the 'Device' drop-down list, select 'Internet Printing Protocol (http)' and then click **Continue**.

Figure 17-33: Printing Protocol

The screenshot shows the 'Admin' section of the ESP interface. At the top, there is a navigation bar with 'ESP' and 'Administration', 'Classes', 'Help', 'Jobs', 'Printers', and 'Software'. Below this, the title 'Admin' is displayed. A section titled 'Device for Canoni250' contains a 'Device:' label followed by a dropdown menu showing 'Internet Printing Protocol (http)'. A green 'Continue' button is located below the dropdown.

7. Paste the printer's IPP URL in the 'Device URI' field, and then click **Continue**.

Figure 17-34: IPP URL

The screenshot shows the 'Admin' section of the ESP interface. At the top, there is a navigation bar with 'ESP' and 'Administration', 'Classes', 'Help', 'Jobs', 'Printers', and 'Software'. Below this, the title 'Admin' is displayed. A section titled 'Device URI for Canoni250' contains a 'Device URI:' label followed by a text input field containing the URL 'http://MP252.home:631/printers/Officejet4500G510gm'. Below the input field, the text 'Examples:' is followed by a list of protocol examples: file:/path/to/filename.prn, http://hostname:631/ipp/, http://hostname:631/ipp/port1, ipp://hostname/ipp/, ipp://hostname/ipp/port1, lpd://hostname/queue, socket://hostname, and socket://hostname:9100. A green 'Continue' button is located at the bottom of the section.

8. The next window displays a manufacturer drop-down list. Select your printer's manufacturer and click **Continue**.
9. The next window displays a printer model drop-down list. Select your printer's model and click **Continue**.
10. The last window displays the following confirmation message: 'Printer has been added successfully'.
11. To test your printer's connection from a Linux PC, open a shell and enter the following command:

```
$ echo hello | lpr -P<Printer Name>
```

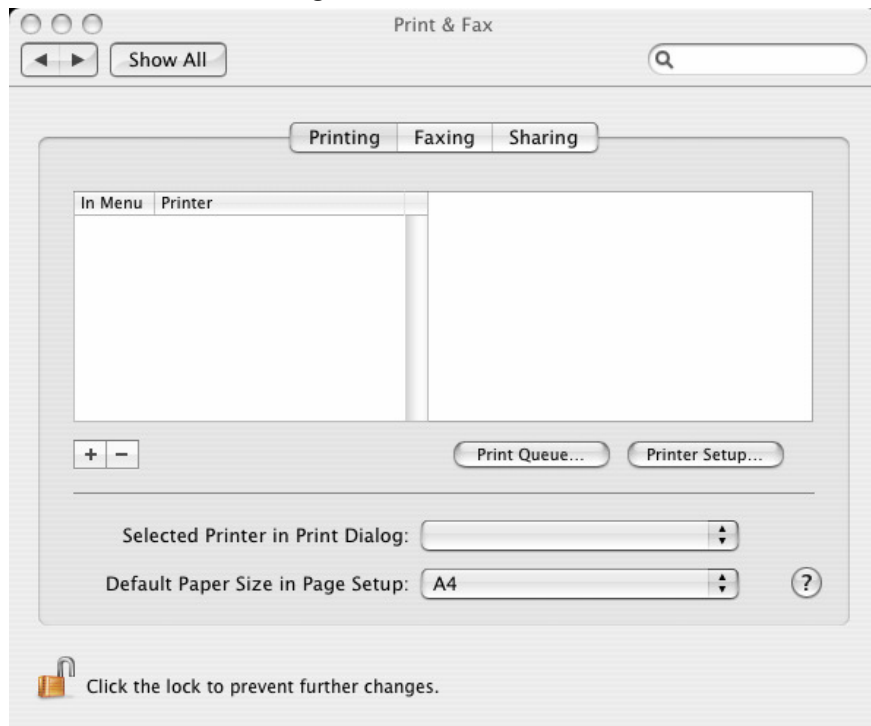
17.3.2.1.3 Setting Up an IPP Printer on Mac

The procedure below describes how to set up an IPP printer on Mac operating systems.

➤ **To set up an IPP printer on Mac:**

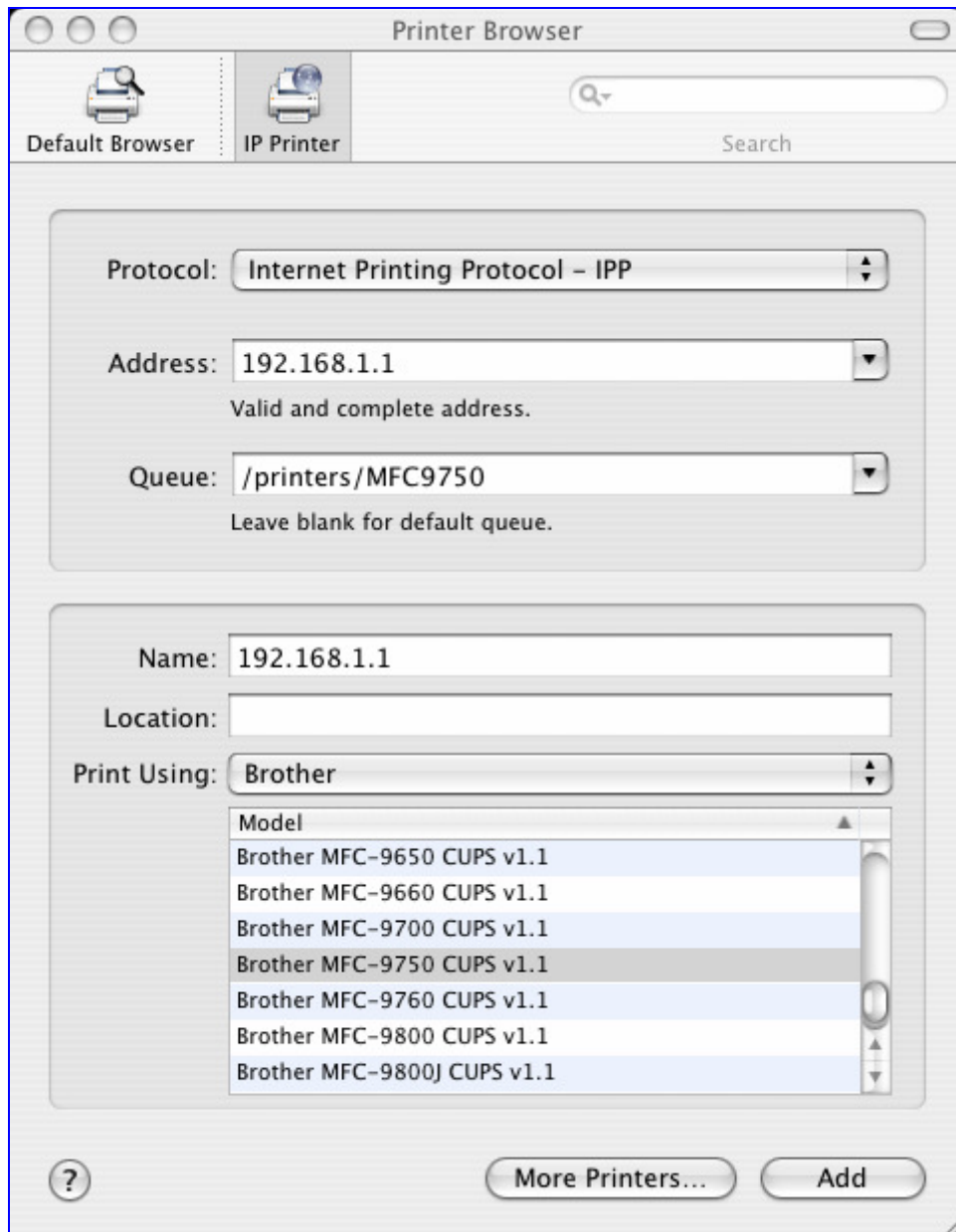
1. On your Mac computer connected to MP252, open the 'Print & Fax' utility from 'System Preferences'; the 'Print & Fax' screen appears.

Figure 17-35: Print & Fax



2. Click the + (add) button; the 'Printer Browser' screen appears.
3. Select the **IP Printer** tab.

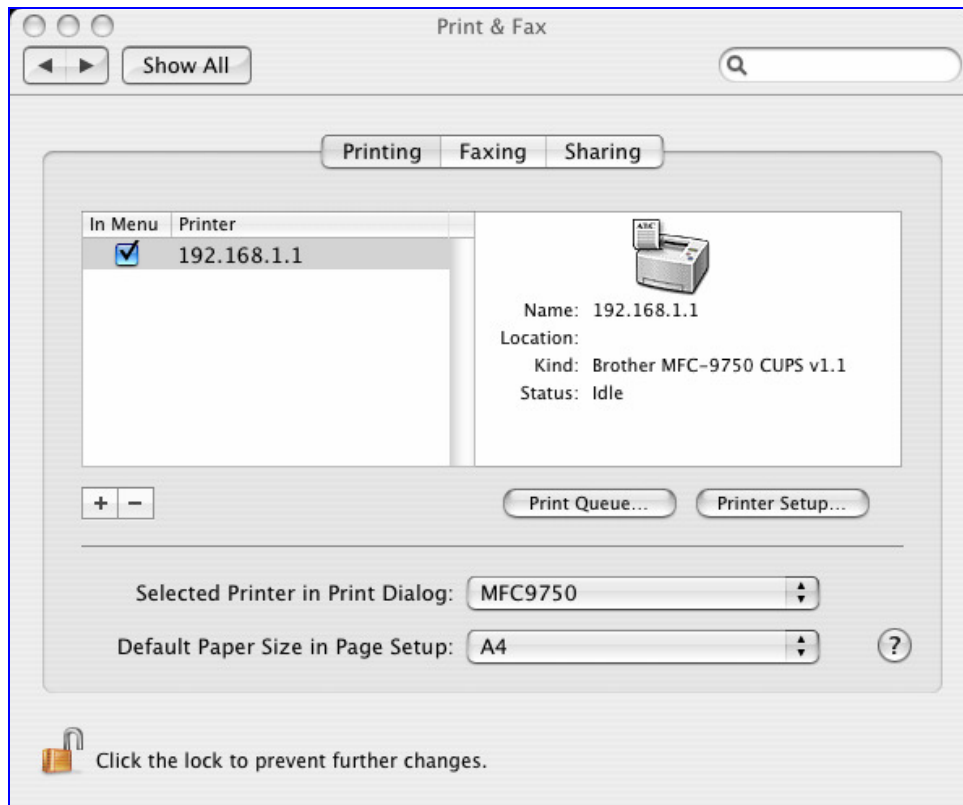
Figure 17-36: Printer Browser – IP Printer



4. In this screen, configure the following:
 - a. From the 'Protocol' drop-down list, select IPP.
 - b. In the 'Address' field, enter MP252's IP address (192.168.1.1).
 - c. In the 'Queue' field, enter the section of the path containing the folder and printer names, as it appears in the 'Printer' screen. For example, "/printers/MFC9750".
 - d. The 'Name' and 'Location' fields are optional; the default name is the gateway's IP address.
 - e. From the 'Print Using' drop-down list, select your printer's make and model.

- Click the **Add** button; the new printer appears in the 'Print & Fax' screen.

Figure 17-37: Print & Fax – New IPP Printer



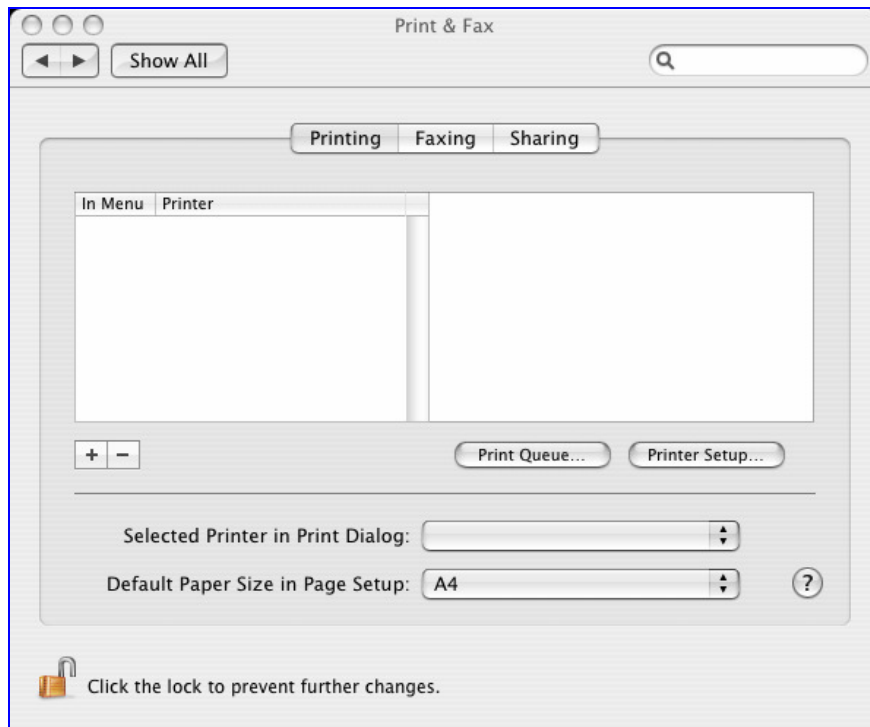
17.3.2.2 Microsoft Shared Printing (Samba)

The procedure below describes how to set up Microsoft Shared Printing (Samba).

➤ **To set up Microsoft shared printing (Samba):**

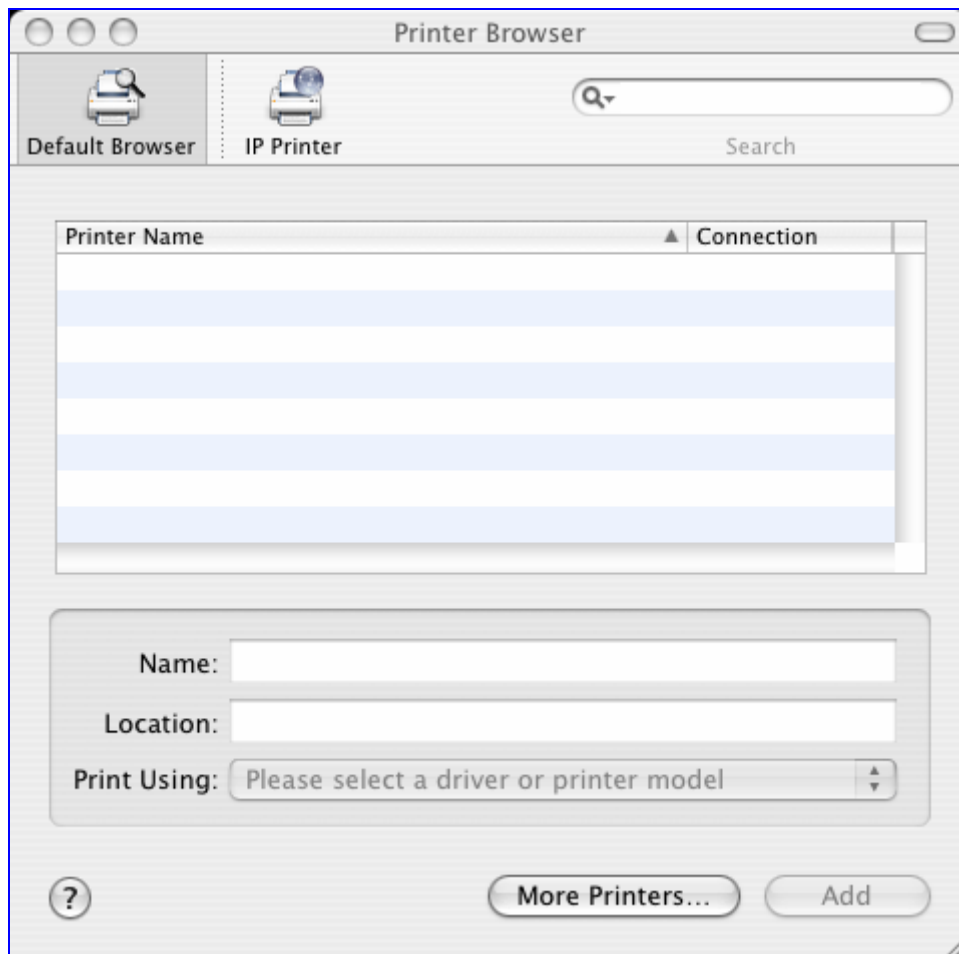
1. On your Mac computer connected to MP252, open the 'Print & Fax' utility from 'System Preferences'; the 'Print & Fax' screen appears.

Figure 17-38: Print & Fax



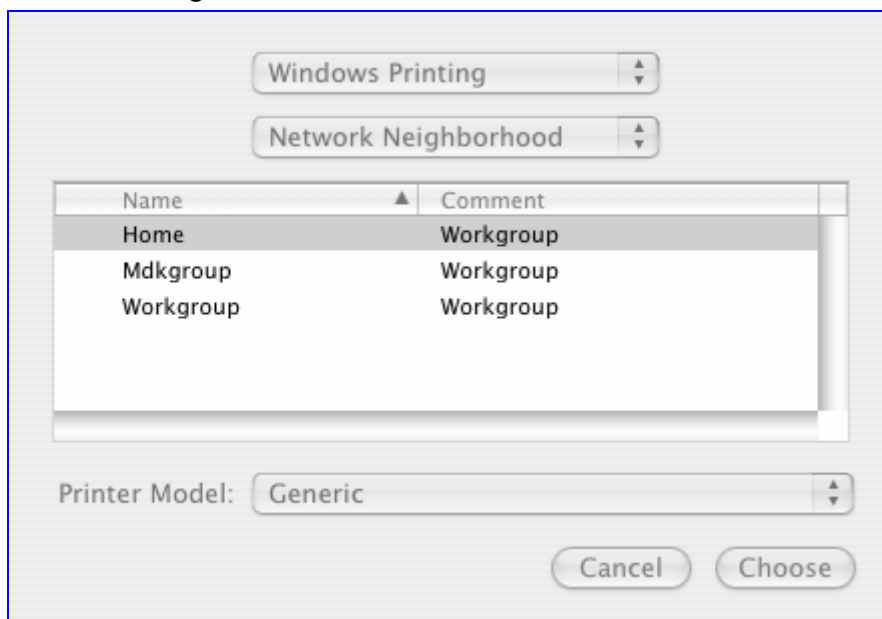
- Click the + (add) button; the 'Printer Browser' screen appears.

Figure 17-39: Printer Browser – Default Browser



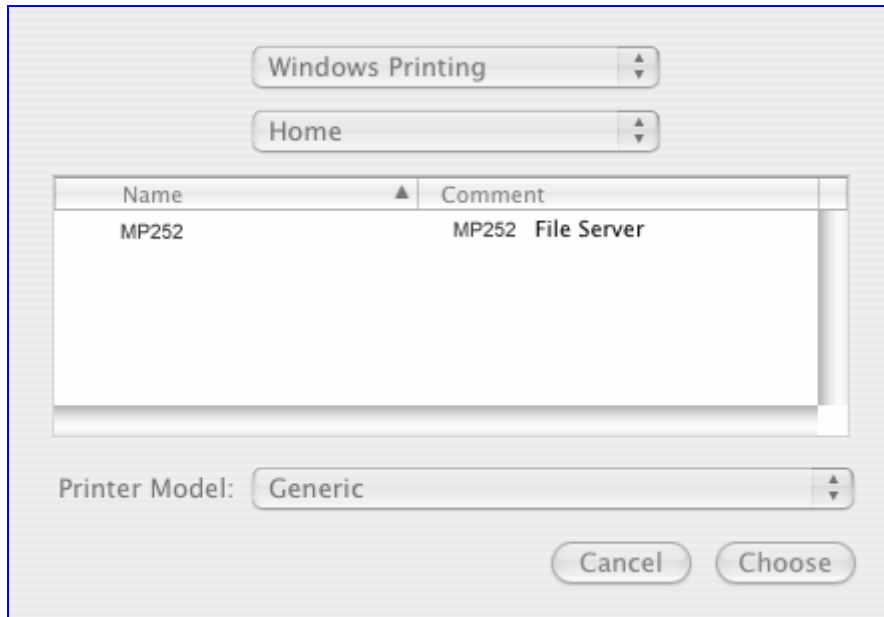
- Click the **More Printers** button; The following screen appears.

Figure 17-40: Printer Browser – More Printers



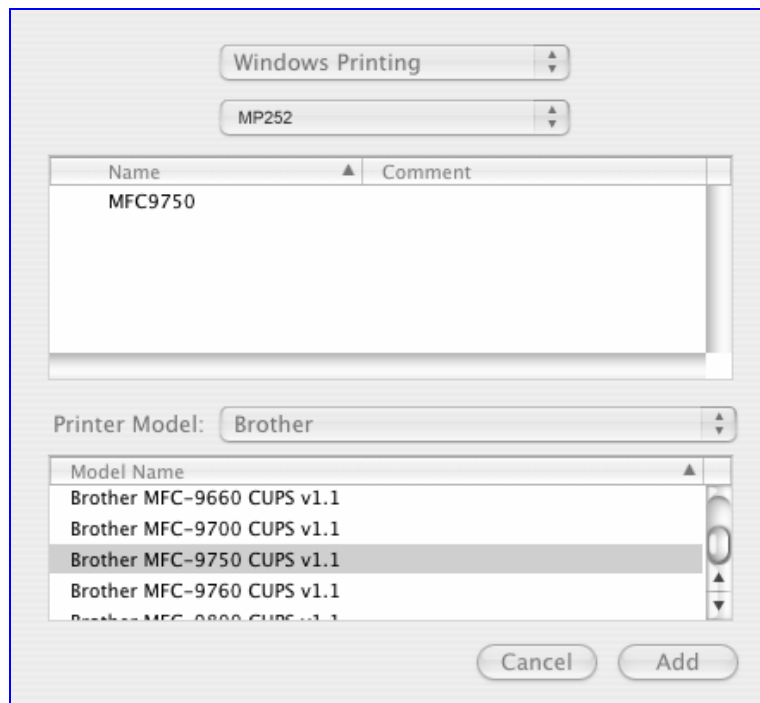
4. From the second drop-down list, select 'Network Neighborhood'.
5. Select the 'Home' workgroup and then click **Choose**.

Figure 17-41: Printer Browser – MP252



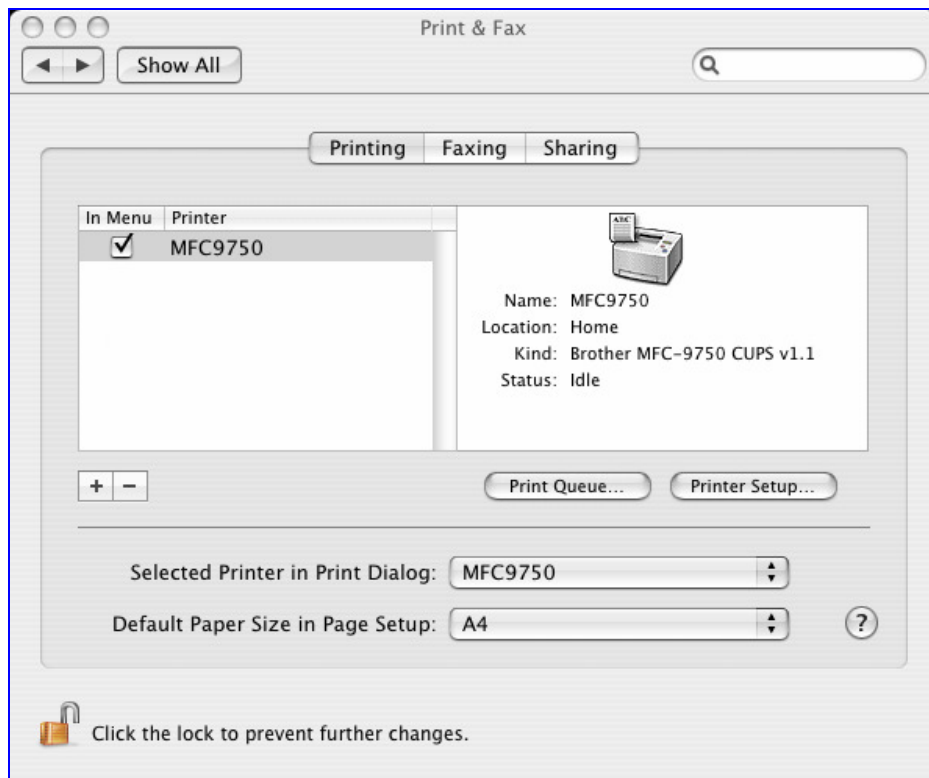
6. Select MP252, and then click **Choose**.
7. Select the printer, and from the 'Printer Model' drop-down list, select your printer's make and model.

Figure 17-42: Printer Browser – Printer Model



8. Click **Add**; the new printer appears in the 'Print & Fax' screen.

Figure 17-43: Print & Fax – New Samba Printer



17.3.2.3 Line Printer Daemon (LPD)

This section describes how to connect computers to MP252 printers, using the LPD protocol.

17.3.2.3.1 Setting Up an LPD Printer on Windows

Before configuring the LPD protocol on a LAN PC, ensure that a print driver for the specific printer is installed.

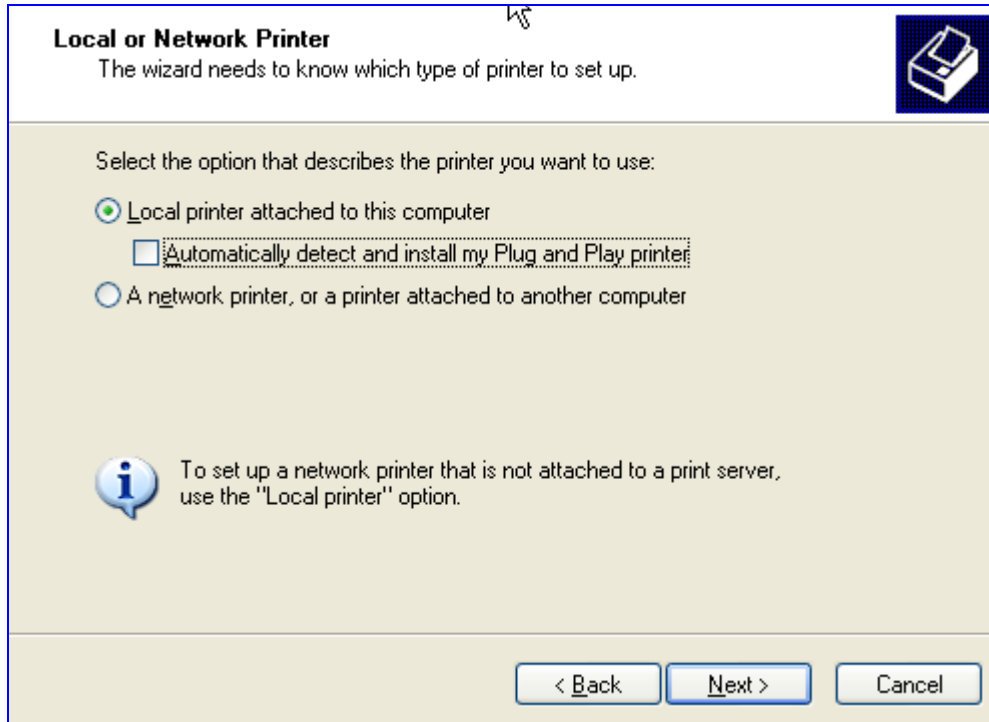


Note: The following configuration must be applied to each LAN PC individually in order to use the network printer.

➤ To set up an LPD printer on Windows:

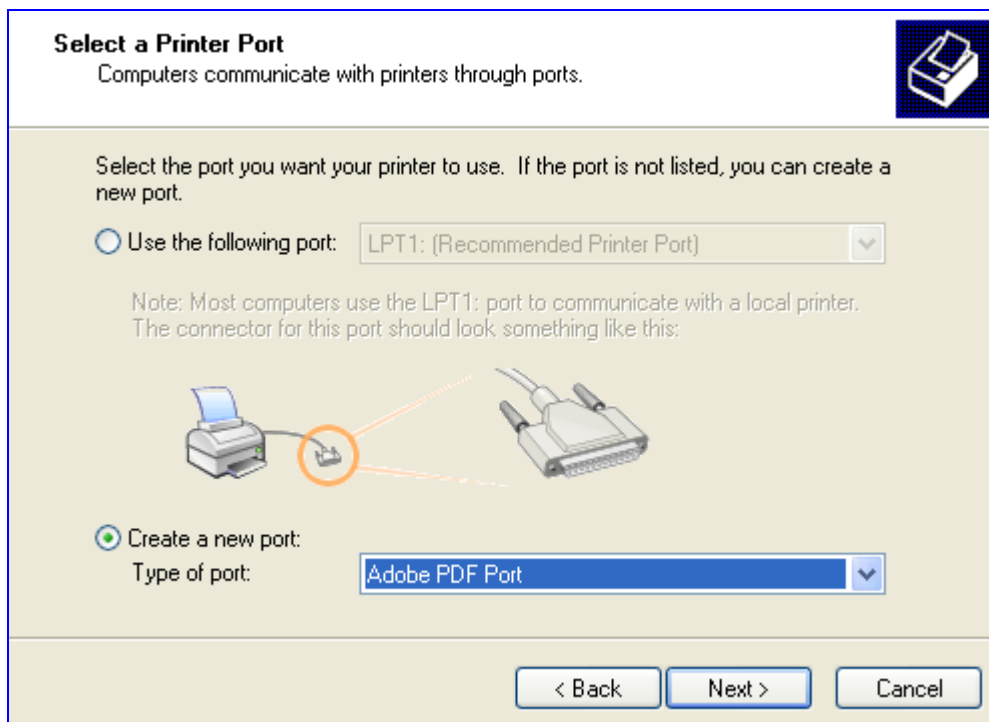
1. On your Windows computer connected to MP252, from the **Start** menu, point to **Settings**, then **Printers and Faxes**, and then click **Add Printer**; the Add Printer Wizard starts.
2. Click **Next** to proceed with the wizard sequence.
3. Select 'Local printer attached to this computer' and then click **Next**.
4. Clear the 'Automatically detect and install my Plug and Play printer', and then click **Next**.

Figure 17-44: Local Printer



5. Select the 'Create a new port' option.
6. From the 'Type of port' drop-down list, select 'Standard TCP/IP Port'.

Figure 17-45: Select a Printer Port



7. Click **Next** to activate the 'Add Standard TCP/IP Printer Port Wizard'.
8. Click **Next** to proceed with the new wizard.
9. In the 'Printer Name or IP Address' field, specify 192.168.1.1, and then click **Next**.

Figure 17-46: Add Port

Add Port
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

< Back Next > Cancel

10. Select the 'Custom' option, and then click **Settings**.

Figure 17-47: Additional Port Information

Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required
The device could not be identified.

The detected device is of unknown type. Be sure that:

1. The device is properly configured.
2. The address on the previous page is correct.

Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type

Standard Fuji Xerox NIC

Custom Settings...

< Back Next > Cancel

11. In the 'Configure Standard TCP/IP Port Monitor' window, configure the following parameters:
 - a. Select the 'LPR' option.

- b. In MP252's Web interface, open the 'Print Server' screen.
- c. Copy the printer's name (for example, "Officejet4000") and paste it in the 'Queue Name' field of the port monitor configuration window.

Figure 17-48: Printer Port Monitor Configuration

Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

Raw LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: Officejet4000

LPR Byte Counting Enabled

SNMP Status Enabled

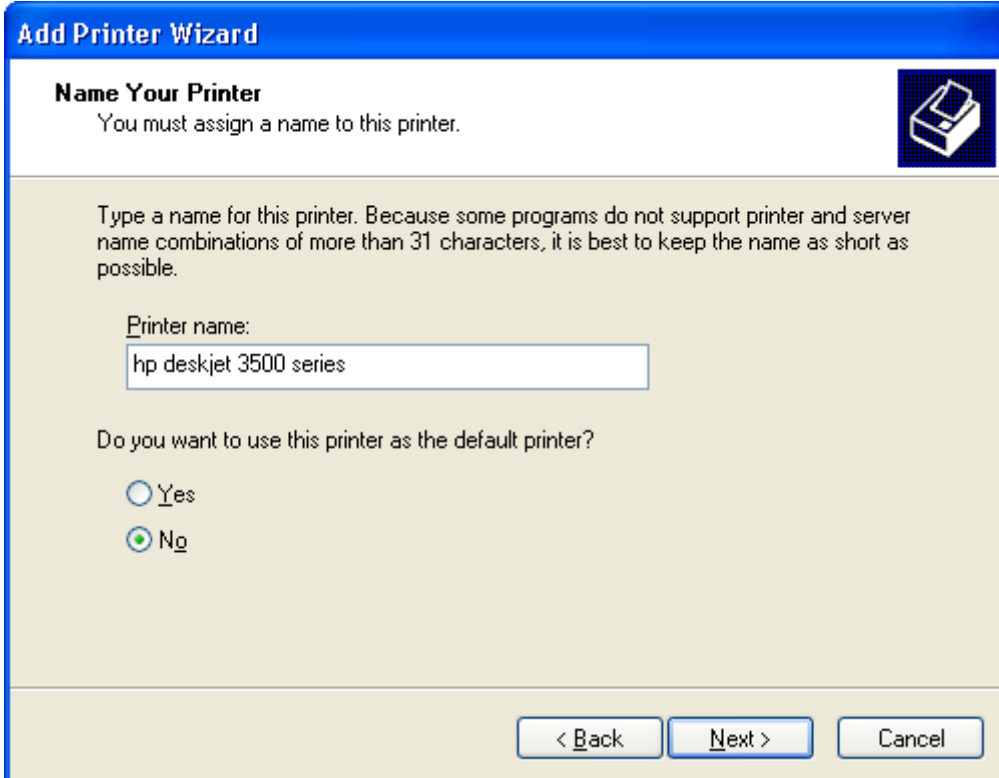
Community Name: public

SNMP Device Index: 1

OK Cancel

12. Click **OK**, and then click **Finish**; the 'Add Printer Software' wizard reappears.

Figure 17-49: Add Printer Wizard



The screenshot shows a Windows-style dialog box titled "Add Printer Wizard". The main heading is "Name Your Printer" with a sub-instruction: "You must assign a name to this printer." A printer icon is in the top right corner. The text below reads: "Type a name for this printer. Because some programs do not support printer and server name combinations of more than 31 characters, it is best to keep the name as short as possible." A text input field labeled "Printer name:" contains the text "hp deskjet 3500 series". Below this is the question "Do you want to use this printer as the default printer?" with two radio buttons: "Yes" (unselected) and "No" (selected). At the bottom are three buttons: "< Back", "Next >", and "Cancel".

13. Select your printer manufacturer and model from the lists. If it does not appear in the lists, click 'Have disk' to specify the driver location.
14. Specify the name you want to give the printer, and whether you want it to be the default printer. Click **Next**.
15. Click **Next** to proceed to the final wizard screen.
16. Select **Yes** to print a test page.
17. Click **Finish** to complete the setup procedure.

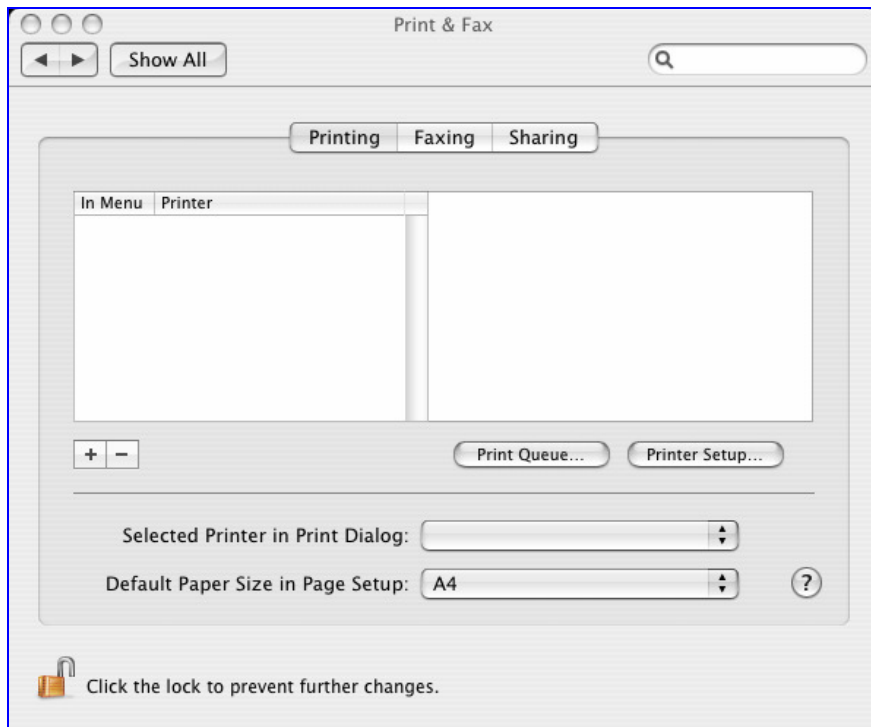
17.3.2.3 Setting Up an LPD Printer on Mac

The procedure below describes how to set up an LPD printer on Mac operating systems.

➤ **To set up an LPD printer on Mac:**

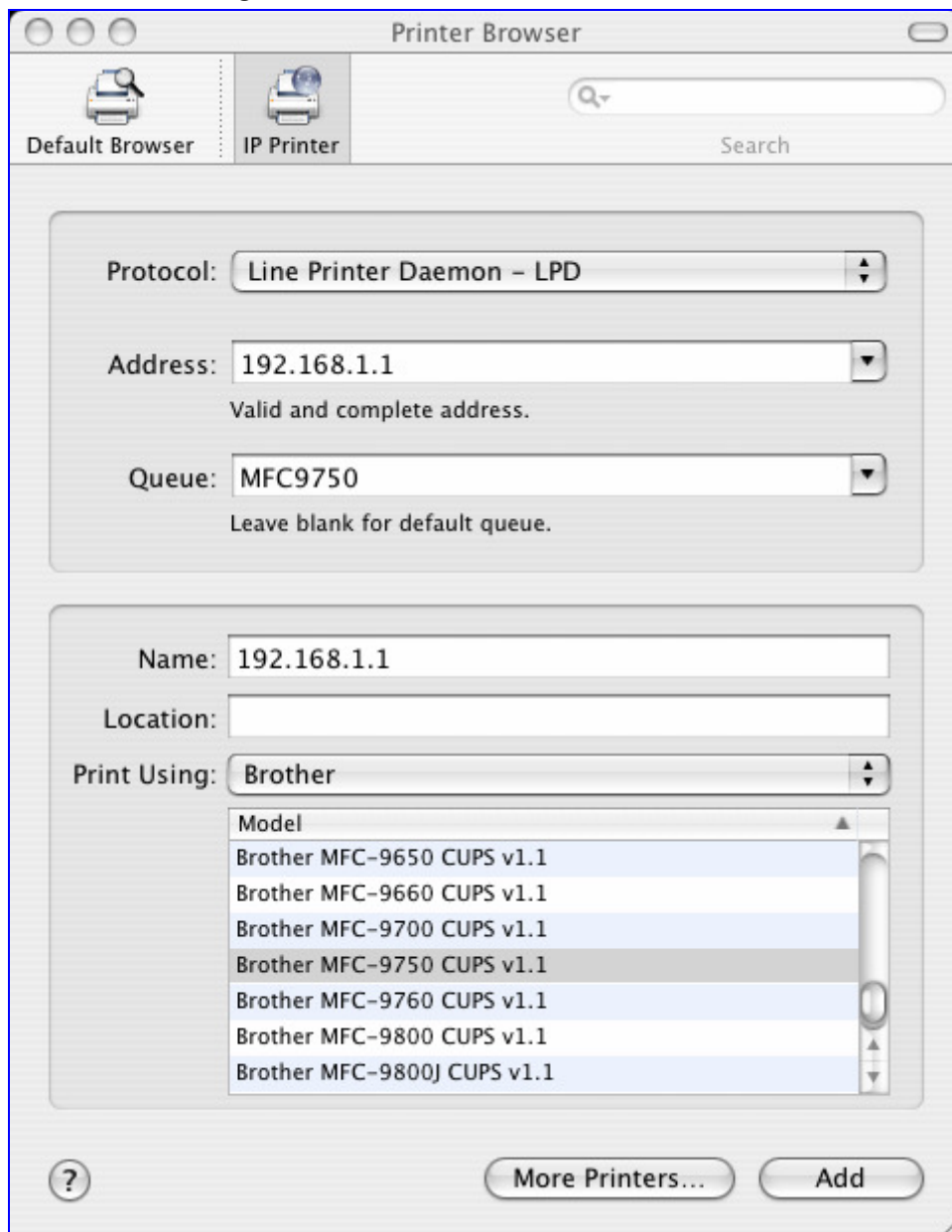
1. On your Mac computer connected to MP252, open the 'Print & Fax' utility from 'System Preferences'; the 'Print & Fax' screen appears.

Figure 17-50: Print & Fax



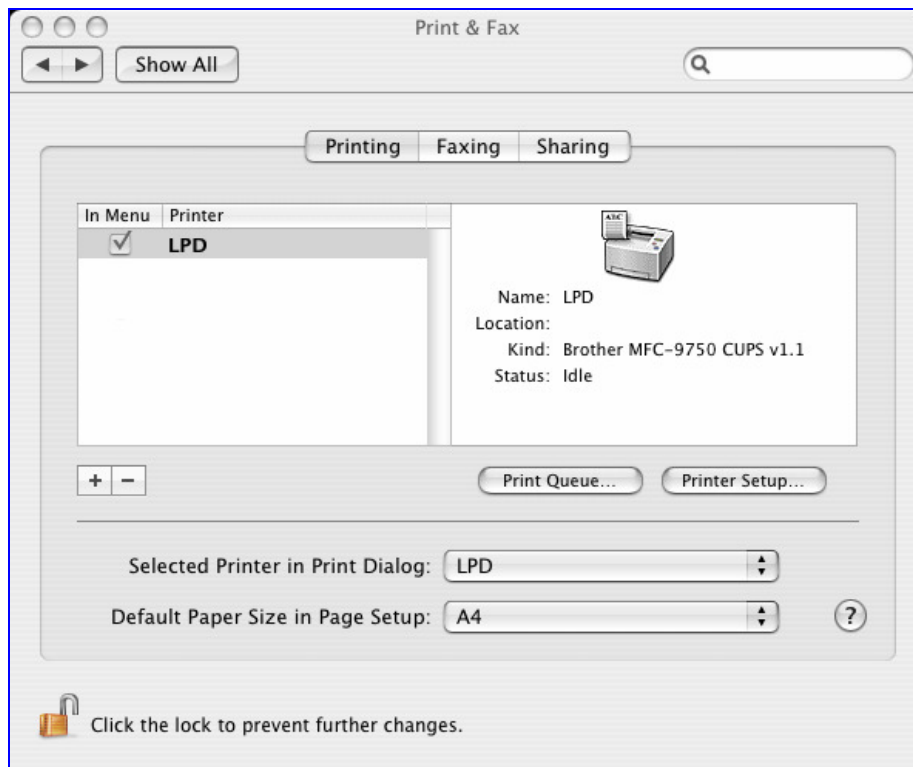
2. Click the + (add) button; the 'Printer Browser' screen appears.
3. Select the **IP Printer** tab and configure the following:
 - a. From the 'Protocol' drop-down list, select LPD.
 - b. In the 'Address' field, enter MP252's IP address (192.168.1.1).
 - c. In the 'Queue' field, enter the printer's name as it appears in the 'Printer' screen of the Web interface. For example, MFC9750.
 - d. The 'Name' and 'Location' fields are optional; the default name is the gateway's IP address.
 - e. From the 'Print Using' drop-down list, select your printer's make and model.

Figure 17-51: Printer Browser – LPD Printer



- Click **Add**; the new printer appears in the 'Print & Fax' screen.

Figure 17-52: Print & Fax – New LPD Printer



17.3.3 Storing and Using Printer Drivers

As explained earlier in this chapter, to use a shared printer connected to MP252, a driver for the printer must be installed on the LAN computer from which the print job is to be sent. You can use the MP252 file server to store printer drivers.

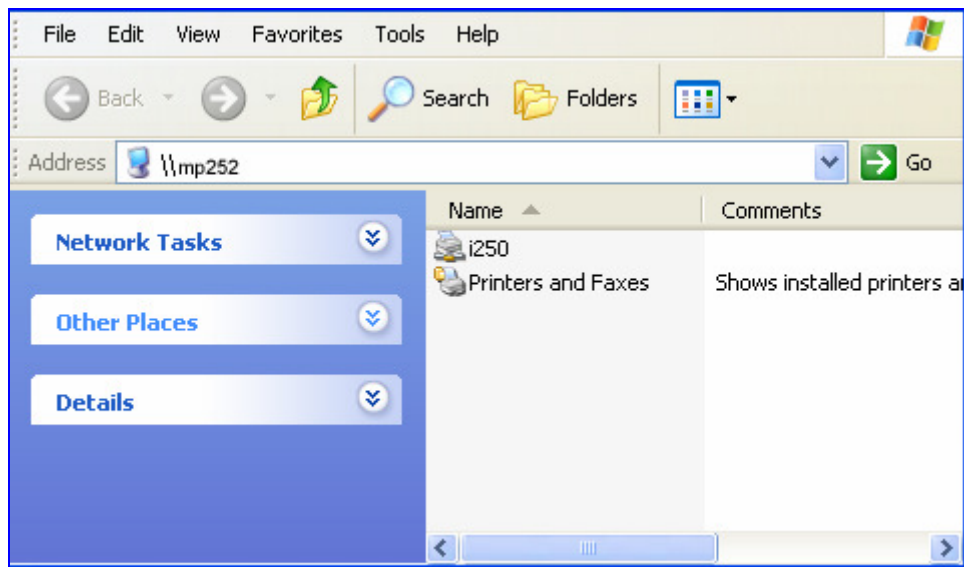
The drivers should be uploaded from a Windows computer and stored in the system storage area that you have created on one of the disk partitions. The printer can then be installed on other LAN computers using the driver stored on MP252.

➤ To upload the driver files to MP252:

- From Window's **Start** menu, click **Run**, and then type "cmd" to open a command shell.
- At the prompt, type **net use** to view the list of shares and their status.
- Type **net use /del \\mp252\share-B** to delete the specific network mapping entry. Alternatively, you can use **net use /del *** to delete all network mapping entries.
- Type **net use * \\openrg\print\$ [Admin's password] [/user:admin]**. This ensures that you are logged into the print server using the Admin user and have the permissions to upload files.

5. Browse to \\mp252 (use a Windows Explorer window if you are using a browser other than Internet Explorer). Should a Windows login dialog box appear, enter your Web username and password. The following window appears, displaying the disk and printer shares available on MP252.


Figure 17-53: MP252 Shares



6. Click **Printers and Faxes**.
7. Right-click the printer icon, and then select **Properties**.
8. If your operating system does not already have the driver, you will be asked if you want to install it now. Click **No**.
9. Select the **Advanced** tab, and then click **New driver**; the 'Add Printer Driver Wizard on MP252 starts. You are prompted to select a printer driver from a list. If unavailable, you can either browse to a location on your computer where you have stored the driver, or click **Have Disk** and insert the CD containing the driver (supplied with your printer).
10. Click **OK**; the driver is uploaded to MP252's system storage directory (e.g. "\\mp252\A").

18 Maintenance

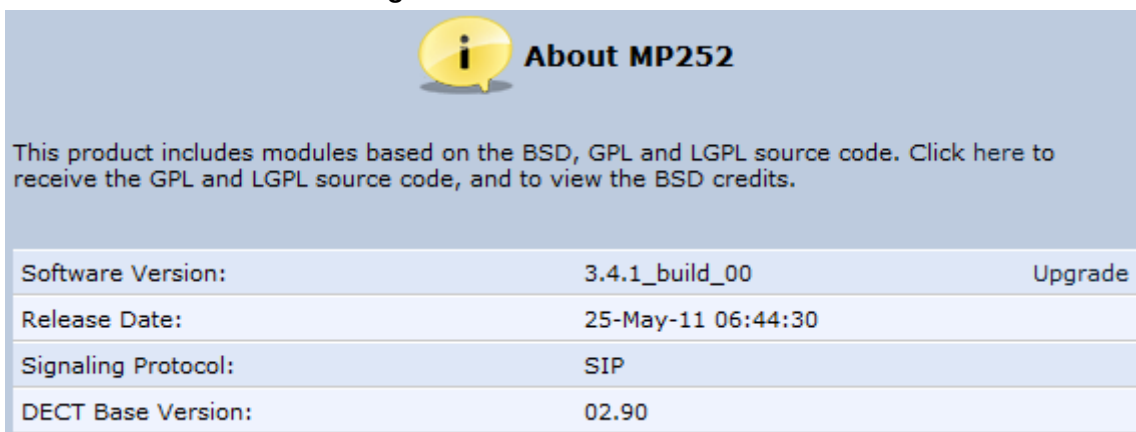
18.1 About MP252

The **About MP252**  icon displays information about MP252. This includes the software version, release date, signaling protocol, and DECT base unit version ⁵. You can also upgrade the software running on MP252, by clicking the **Upgrade** link (for more information, see Section 18.5 on page 323).

➤ **To view information about MP252:**

- In the 'Advanced' screen, click the  icon; the 'About MP252' screen appears.

Figure 18-1: About MP252 Screen



⁵ The DECT feature is applicable only to the MP252WDNB model.

18.2 Date & Time

The procedure below describes how to set the date and time.

➤ **To configure date, time and daylight savings time settings:**


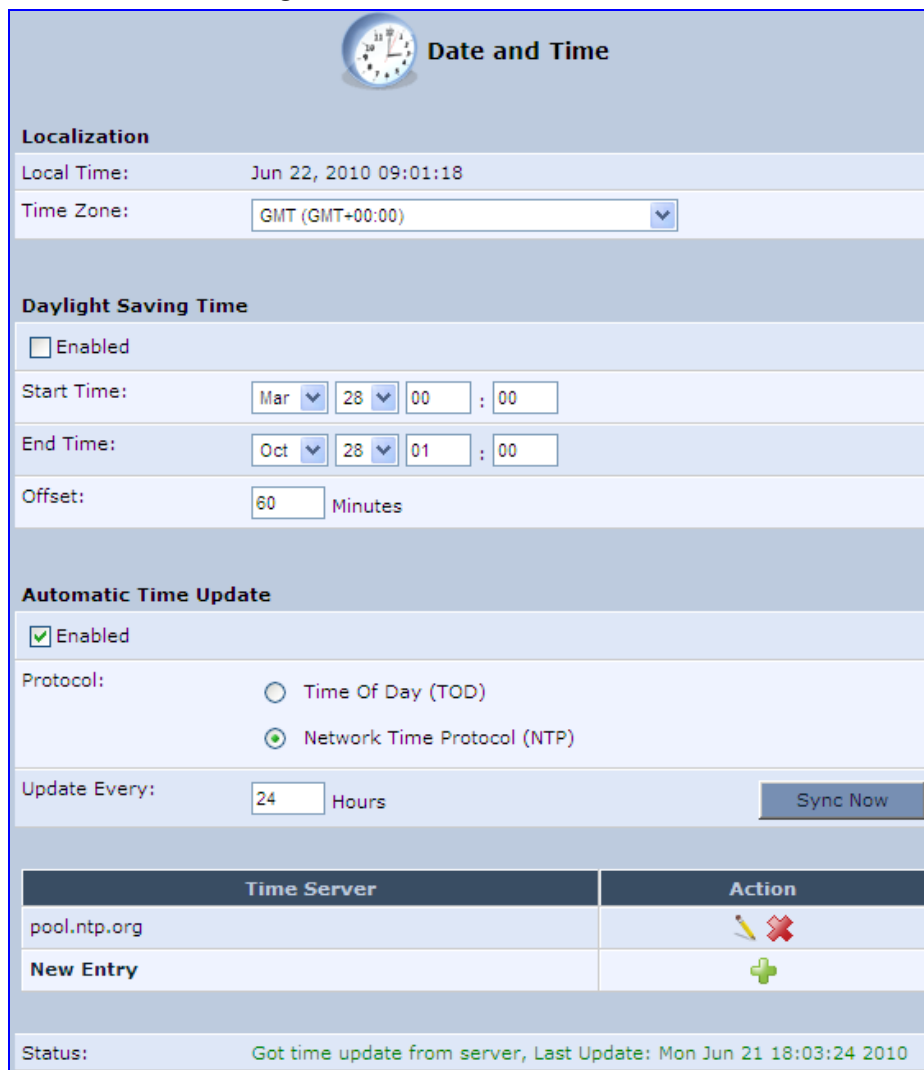
1. In the 'Advanced' screen, click the **Time Settings**  icon; the 'Date & Time' screen appears.

Figure 18-2: Date and Time Screen



Date and Time

Localization

Local Time: Jun 22, 2010 09:01:18

Time Zone: GMT (GMT+00:00)

Daylight Saving Time

Enabled

Start Time: Mar 28 00 : 00

End Time: Oct 28 01 : 00




Offset: 60 Minutes

Automatic Time Update

Enabled

Protocol: Time Of Day (TOD) Network Time Protocol (NTP)

Update Every: 24 Hours Sync Now

Time Server	Action
pool.ntp.org	 
New Entry	

Status: Got time update from server, Last Update: Mon Jun 21 18:03:24 2010

2. From the 'Time Zone' drop-down list, select the local time zone. MP252 can automatically detect daylight saving setting for selected time zones.


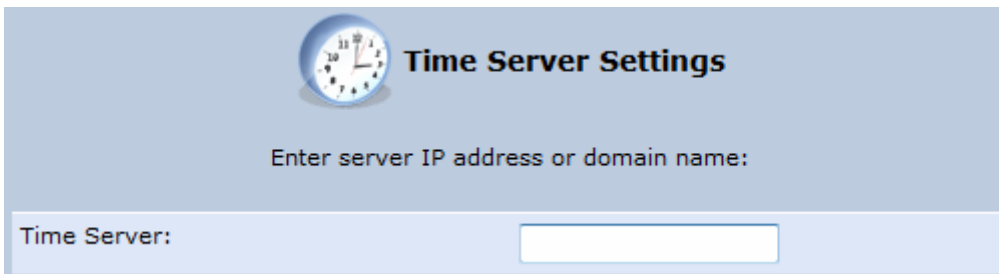
3. Under the **Daylight Saving Time** group, configure the daylight saving settings for your time zone (if they are not automatically detected):
 - **Enabled:** Select this check box to enable daylight saving time.
 - **Start:** Date and time when daylight saving starts.
 - **End:** Date and time when daylight saving ends.
 - **Offset:** Daylight saving time offset.
4. For the MP252 to perform an automatic time update, under the **Automatic Time Update** group, do the following:
 - a. Select the 'Enabled' check box.
 - b. Select the protocol to be used for time update, by selecting either the 'Time of Day' or 'Network Time Protocol' option.
 - c. In the 'Update Every' field, specify how often to perform the update.
 - d. You can define NTP servers, by clicking the **New**  icon; the 'Time Server Settings' screen appears.

Figure 18-3: Time Server Settings Screen




Time Server Settings

Enter server IP address or domain name:

Time Server:

- e. In the 'Time Server' field, enter the IP address of the Time server (NTP), and then click **OK**.

18.3 Backup and Restore

The **Backup and Restore**  icon allows you to configure the MP252 backup facility for backing up data, stored in the system storage area, to external USB disks. You may specify backups to run automatically at scheduled times.

Two prerequisites must be met before enabling the backup mechanism:

- The file server feature must be activated and configured
- The file server must consist of at least two disks



Note: The backup is done at the directory level. In other words, it is not possible to backup a single stand-alone file.


18.3.1 Backing Up Data

The procedure below describes how to backup data.

➤ **To backup data:**

1. In the 'Advanced' screen, click the  icon; the 'Backup and Restore' screen appears.
2. Select the **Backup** tab.

Figure 18-4: Backup and Restore Screen

Source	Destination	Full	Incremental	Status	Action
New Entry					

3. In the 'Backup Schedule' table, click the **New**  icon; the 'Edit Backup' screen appears.

Figure 18-5: Edit Backup Screen

The screenshot shows the 'Edit Backup' configuration window. It features a title bar with a green folder icon and the text 'Edit Backup'. Below the title bar are two text input fields: 'Source:' and 'Destination:'. Underneath these is a section titled 'Full Backup' with fields for 'Last Backup:', 'Location:', and 'Schedule:' (a dropdown menu showing 'Disabled'). Below that is a section titled 'Incremental Backup' with fields for 'Last Backup:', 'Location:', and 'Schedule:' (a dropdown menu showing 'Disabled').

4. In the 'Source' field, type the source to backup, for example, "A/homes".
5. In the 'Destination' field, type the destination of the backup files, for example, "B/backups". It is recommended that the destination is an external storage device.
6. Choose between full backup, incremental backup, or both, by scheduling a time for the backup operation. You can choose between daily, weekly or monthly backups in the 'Schedule' drop-down lists.



Note: Do not schedule a monthly backup on the 31st of the month, as backups do not run on months with 30 days.

7. Click **OK** to save the schedule settings.
8. Click **Backup Now** to run the backup operation immediately. When backing up, the screen displays the status and progress of the operation.

18.3.2 Restoring Your Data

The procedure below describes how to restore data.

➤ **To restore data:**


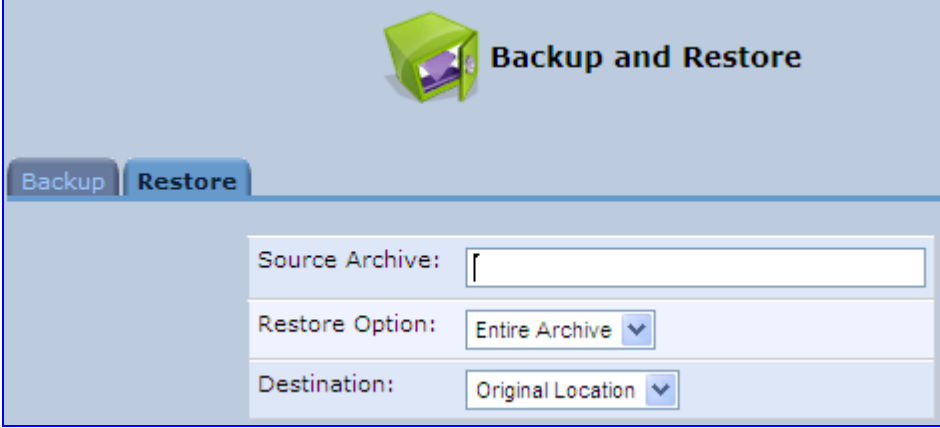

1. In the 'Advanced' screen, click the  icon; the 'Backup and Restore' screen appears.
2. Select the **Restore** tab; the 'Restore' screen appears.

Figure 18-6: Restore Screen



3. In the 'Source Archive' field, type the source to restore, for example, "A/homes".
4. From the 'Restore Option' drop-down list, select whether to restore the entire archive or only a subdirectory. If you choose subdirectory, a second field appears in which you must enter the name of the subdirectory relative to the source archive. For example, to restore "A/homes/john", type "john" as the subdirectory.
5. From the 'Destination' drop-down list, select a destination for which to restore the archive. You can choose the original location or any other directory. If you choose another directory, a second field appears in which you must enter the name of the directory. Note that the path of the restored directory is created under the path of the destination directory. For example, if you specify the directory "A/restore_dir", the result is "A/restore_dir/A/homes/john".

18.4 Configuration File

The **Configuration File**  icon allows you to view, save, and load the MP252 configuration file. Therefore, you can backup and restore your current configuration.

MP252 also supports configuration file encryption, allowing you to load encrypted configuration files (using the file name extensions *.cfg or *.inx). For more information on encrypting a configuration file, see Section 18.4.3 on page 321.

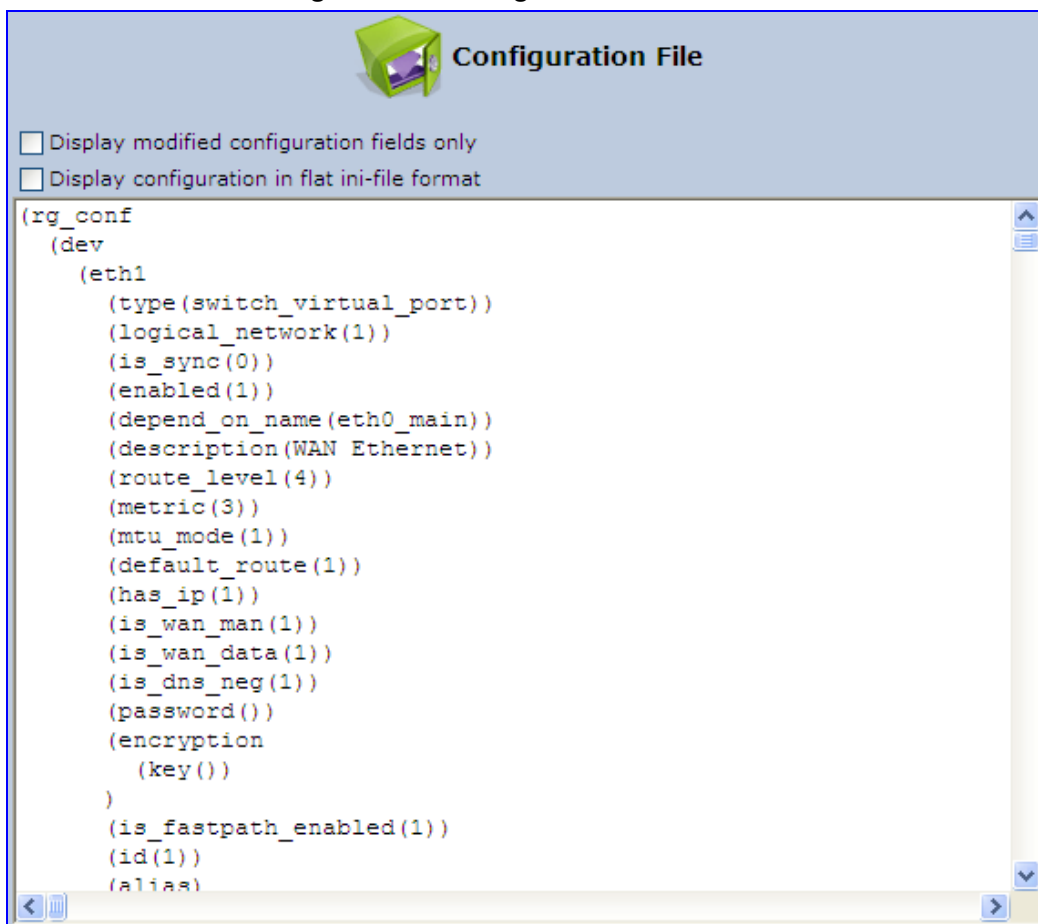
MP252 allows you to use un-encrypted passwords in the configuration file (*.cfg or *.ini) that you want to load, and then encrypt the passwords before burning to flash. This is achieved by using the format {"<value>"} in the configuration file for password fields which are normally encrypted. Below are two examples of this feature:

- **ini file:** rg_conf/voip/line/1/auth_password={"foobaa"}
- **cfg file:** (auth_password({"foobaa"}))

➤ **To save and restore the configuration file:**

1. In the 'Advanced' screen, click the  icon; the 'Configuration File' screen appears, showing the entire contents of the configuration file.

Figure 18-7: Configuration File Screen



2. You can customize the displayed configuration file, by selecting the following check boxes:
 - **Display modified configuration fields only:** Displays only the configuration parameters that have values other than default values.

- **Display configuration in flat ini-file format:** Displays the configuration file in flat INI-file format.
3. To back up your current configuration to a file on your PC, click **Download Configuration File**. The saved configuration file can be used as a backup for the specific MP252's configuration for creating a configuration file for remote configuration update, and for debugging and diagnostics. When creating a configuration backup, disable the two display check boxes (i.e. save a full configuration file in the hierarchic **conf** format). This file can be loaded back to the same MP252, using the procedure described in Section 18.4.1 on page 318.



Note: The file is generated according to the selected display option (in Step 2).

4. To restore your configuration from a file saved on your PC, click **Upload Configuration File**.



Note: Do not load this file to a different MP252 as it includes the MAC address, which is unique to MP252 from where it was saved.

When creating a file for remote configuration update, it is recommended to only select the 'Display modified configuration fields only'. This ensures that the file includes only parameters that were modified from their default value. You can choose the conf format or the flat ini-file format. In both cases, it is recommended to review the file and ensure that only the parameters that the user has intended to modify appear. This file can be placed on an FTP or HTTP server for mass configuration update, as described in Remote Configuration Download.



Note: When rebooting, MP252 restores the settings from its configuration file. However, if reboot attempts fail three times consecutively, MP252 resets the configuration file by restoring factory defaults before attempting to reboot.

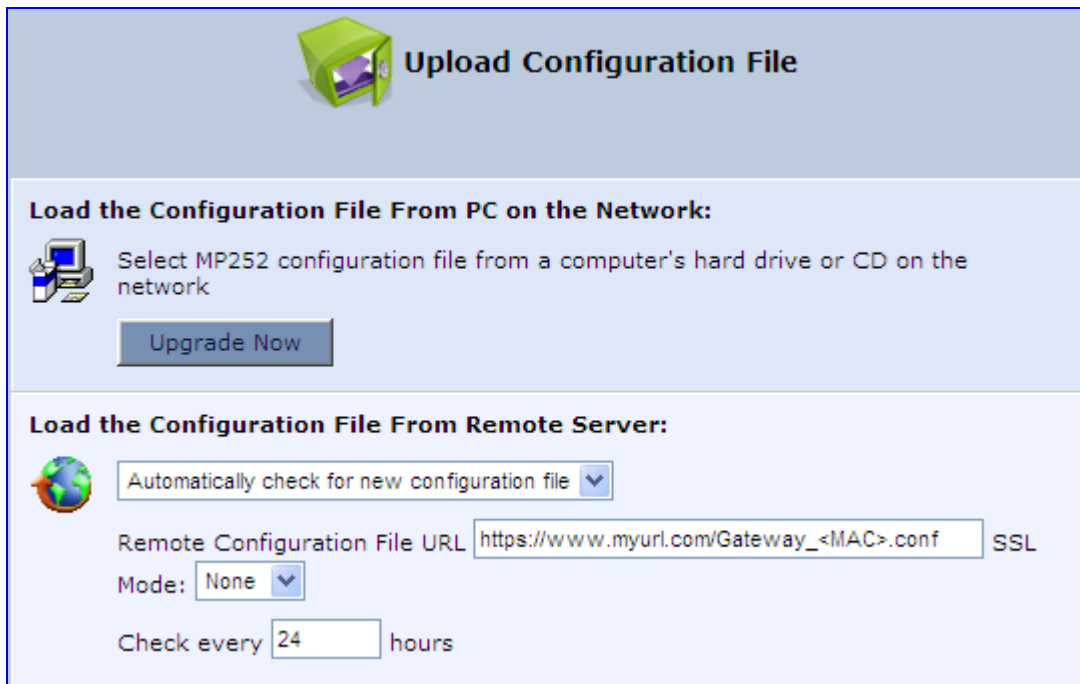
18.4.1 Uploading from PC on the Network

The procedure below describes how to upload a configuration file from a PC on the network to MP252.

➤ **To upload a configuration file to MP252 from a PC on the network:**

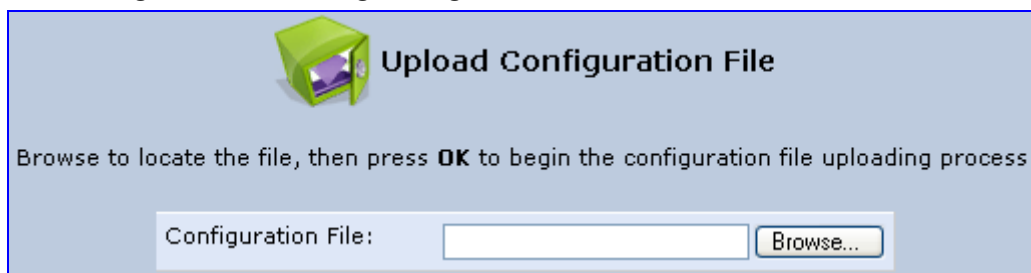
1. Click the **Upload Configuration File**; the screen 'Upload Configuration File' opens.

Figure 18-8: Upload Configuration File



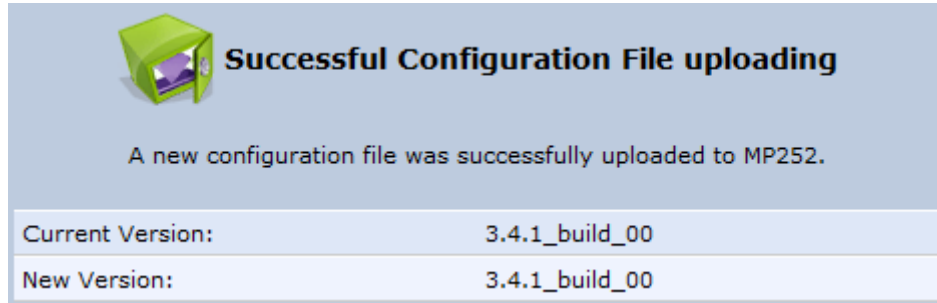
2. Under the 'Load the Configuration File From a PC on the Network' group, click **Upgrade Now**; the screen 'Upload Configuration File' opens.

Figure 18-9: Loading Configuration File from a PC on the Network



3. Enter the path of the configuration file or click **Browse** and navigate to the configuration file on your PC.
4. Click **OK**; the file starts loading from the PC to your MP252. When loading is complete, the screen 'Successful Configuration File Loading' opens, prompting you to confirm configuration file load.

Figure 18-10: Successful Configuration File Uploading



5. Click **OK** to confirm; the upgrade process commences and takes a couple of minutes to complete. At the conclusion of the file load process, the MP252 automatically reboots. When the MP252 completes the reboot, the new configuration file is applied and the 'Login' screen appears, prompting you to login again.
6. Login with your username and password.



Note: During the load process, it is recommended not to power down MP252 nor stop the file load process to avoid damage to the main firmware. However, if you do, MP252 runs a recovery firmware image (also stored on its flash memory). Except for the analog or VoIP interfaces, the recovery image supports all interfaces and enables MP252 to reconnect to the Internet and then download the primary software.

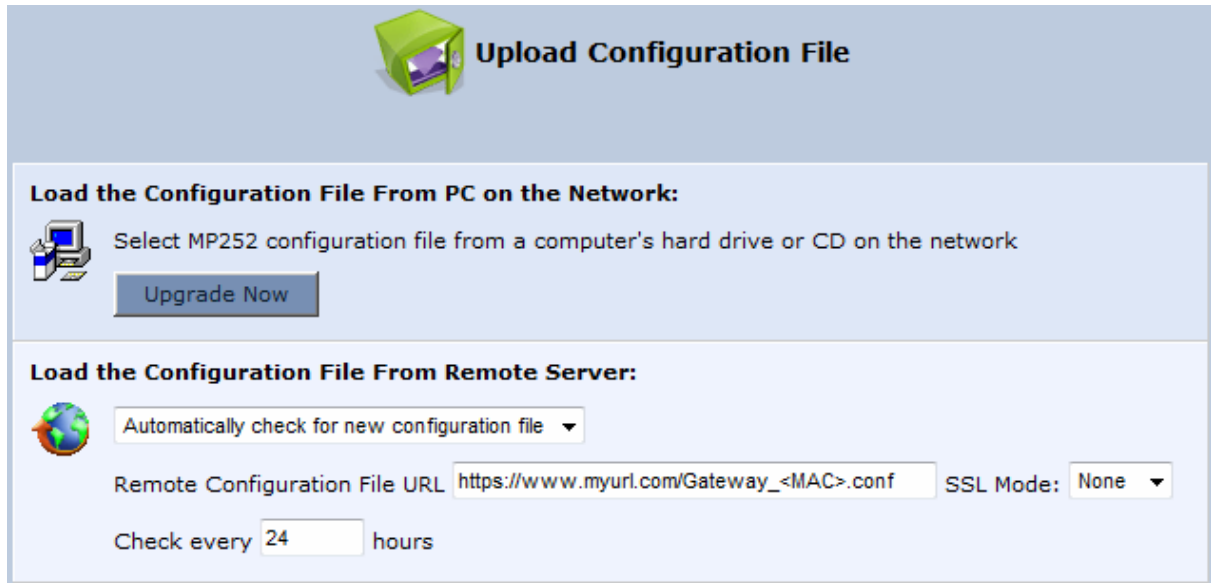
18.4.2 Uploading from a Remote Server

The procedure below describes how to upload a configuration file to MP252 from a remote server. This allows you to keep your configuration up-to-date, by performing daily checks for a newer configuration file each time MP252 restarts (i.e., automatic update), or manually checking for a newer configuration file.

➤ **To upload MP252's configuration file from a remote server:**

1. Click the **Upload Configuration File**; the screen 'Upload Configuration File' opens.

Figure 18-11: Upload Configuration File



2. Under the 'Load the Configuration File From Remote Server' group, select the checking method and interval:
 - **Automatically check for new configuration file**
 - **Automatic configuration file check disabled**
3. In the 'Remote Configuration File URL' field, enter the URL address of the remote server where the configuration file is located. The URL format is as follows: **protocol://server/filename.<conf/ini>**, for example:
 - ftp://10.10.10.10/MP20x_<MAC>.conf
 - http://20.20.20.20/MP20x_<MAC>.ini

Where <MAC> is the MAC address of MP252's WAN.
4. In the 'Check every' field, enter the interval (in hours) for which MP252 periodically checks for a new configuration file. If set to 0, MP252 checks only once for a new configuration file, and this occurs after it restarts.
5. From the 'SSL Mode' drop-down list, select the type of Secure Socket Layer (SSL) certificate's validation method for accessing the remote server using HTTPS for the following purposes: downloading a new firmware file, downloading a new configuration file, and TR-069. Upon connection, MP252 validates the server's certificate using the selected method:
 - **None:** Do not validate the server's certificate (if you do not have a certificate).
 - **Chain:** Validate the entire certificate chain (if you have a certificate, but not necessarily signed by a root CA).
 - **Direct:** Ensure that the server's certificate is signed by the root certificate (CA).

6. Click **OK**; the download process begins. When downloading completes, a confirmation screen appears, prompting you to confirm loading the new version.
7. Click **OK** to confirm. The upgrade process begins and takes about one minute to complete. At the conclusion of the upgrade process, MP252 automatically reboots and the new software version runs.

If a new version is unavailable, click the **Check Now** button to perform an immediate check (instead of waiting for the next scheduled one). The screen displays a green "Check in progress..." message.

Notes:

- For additional security, MP252 can be configured to use HTTPS client-server certification when connecting to a remote server (see Section 13.3 on page 200).
- The configuration file can have one of the following two formats: a hierarchical conf file (indicated by file extension *.conf) or a flat ini file (indicated by file extension .ini).
- The parameter '/rmt_config/version' defines the version of the configuration file. MP252 uses the new configuration file only if the version that is defined in this file is later than the current version. By default, the 'version' is set to 0. This means that each time Service Providers' operations personnel require MP252 to download a new configuration file, they need to increment the 'version' parameter in the new file (in the .conf file, the 'version' parameter is under the section 'rmt_config'). To simplify the procedure, it is possible to use the current date in YYYYMMDD format as the version field.
- The remote configuration file must include only a subset of the complete MP20x.conf file. A recommended procedure is to start with a MP252 restored to its factory settings, modify using the embedded Web server the parameters that should appear in the remote configuration file, and then upload (save) the configuration file. You must save only the modified parameters, as described in 'Remote Administration' on page 261.
- The string <MAC> enables the ISP to pre-configure all its deployed MP252s with the same URL and file details (under rmt_config/url) and still have each MP252 download its unique configuration file. Once the URL is configured with the string <MAC>, MP252 that is trying to update its configuration file automatically replaces <MAC> with its own unique MAC address. For example, if there's a MP252 with a WAN MAC address 00:01:02:03:04:05, the ISP can configure the url to http://myserver.com/my_conf_file_<MAC>.conf - and place a file called 'my_conf_file_00_01_02_03_04_05.conf' on the server.
- Downloading a configuration file from a remote server can also be performed from the CLI:
 - 1) Using Telnet, access MP252, and then enter the user name and password.
 - 2) Enter the command **rmt_config**, for example:
rmt_config -u http://myserver.com/my_conf_file.conf
 - 3) Enter **rmt_config** without any arguments for more help information.



18.4.3 Encrypting a Configuration File Using CLI

Encrypted files include the file name extension *.cfx (instead of *.cfg) or *.inx (instead of *.ini). After MP252 loads the encrypted file from the HTTP server, it automatically identifies the encrypted file by its file name extensions *.cfx or *.inx, and subsequently decrypts the file before saving it to flash memory.

The following procedure describes how to encrypt configuration files.

➤ **To encrypt a configuration file:**

- Run the following CLI shell command (on Linux or Windows PC with OpenSSL installed):

```
openssl des3 -in <original file> -out <encrypted file> -k  
<password> -S <salt value>
```

Where,

- *<original file>* is the original clear-text configuration file (*.cfg or *.ini file).
- *<encrypted file>* is the output file (an encrypted *.cfx or *.inx file).
- *<password>* is the password that is used to encrypt the file.
- *<salt value>* is the 8 bytes of a special key value that is combined with the password. The format is 16 hexadecimal digits [0-9,A-F].

An example of this command is shown below:

```
openssl des3 -in c:\temp\try_enc_conf.cfg -out  
c:\temp\try_enc_conf.cfx -k MyPassword123456 -S 0123456789ABCDEF
```



Notes:

- You can choose any *<salt value>* – MP252 does not have to know about it.
- A password can be pre-configured in MP252, using the following CLI command: `rg_conf_set_obscure /rmt_config/password <password>`
- You can also define the password in a configuration file that you download from the server.
- If you don't define a password in the configuration file, a default password is used. Different default passwords are defined per customer, according to the config-file url hostname.

18.4.4 Automatic Upload using SIP NOTIFY Message

You can enable automatic configuration update for MP252 from a remote server, using the SIP NOTIFY message. The contents of the configuration file can initiate (“push”) the remote server to update MP252 to a desired configuration version.

➤ **To “push” a configuration file when a change of parameter is needed:**

1. Create a new configuration file with the required change.
2. Place the file on the HTTP server.
3. Send the SIP NOTIFY message to MP252; MP252 integrates the contents of the new file and reboots.

➤ **To “push” a configuration file and initiate an upgrade or downgrade:**

1. Create a new configuration file that includes two important entries:
 - a. In *rg_conf/rmt_upd/chech_sync_version*, configure the details of the version to which you want MP252 to upgrade or downgrade, for example:


```
(rmt_upd
      (check_sync_version(2.6.0_build_1))
)
```
 - b. You may need to update the URL address from where MP252 is downloading the firmware (the path is configured in *rmt_upd/url*).



Note: In the case of a downgrade, the service provider MUST provide a configuration file based on a template that matches the version to which the MP252 is downgrading.

2. Place the file on the HTTP server.
3. Send the SIP NOTIFY message to MP252; MP252 integrates the contents of the new file and reboots. After rebooting, MP252 compares the currently running version with the version which is configured in *rmt_upd/chech_sync_version* and then determines whether to connect to the *rmt_upd/url* for downloading the new *.rmt file. Once the file is downloaded, its headers are parsed, and only if it represents the same version which was configured in the value of *rmt_upd/chech_sync_version*, does the upgrade/downgrade process begin.

18.5 Firmware Upgrade

MP252 provides a built-in mechanism for upgrading its software image. There are two methods for upgrading the software image:

- **Upgrading from a Computer on the Network:** This method uses a software image file that is pre-downloaded on a PC's disk drive or located on an accompanying CD. (See Section 18.5.1 on page 325.)
- **Upgrading from the Internet:** This method also referred to as 'Remote Update', upgrades your firmware by remotely downloading an updated software image file. (See Section 18.5.2 on page 326.)

MP252 provides a flash memory of 8 MB, which is capable of storing two firmware images. In addition to the primary firmware, MP252 also stores a recovery firmware, which is used only if the primary image is missing or damaged (e.g. if the user unplugs the power during firmware upgrade). Except for the analog or VoIP interfaces, the recovery image supports all interfaces and enables MP252 to reconnect to the Internet and download the primary firmware.

18.5.1 Upgrading from a Computer on the Network

The procedure below describes how to upgrade MP252 from a software image file located on a local computer or network.



Note: You can only use files with an *.rmt extension when performing the firmware upgrade procedure.

➤ **To upgrade MP252 software image using a locally available .rmt file:**


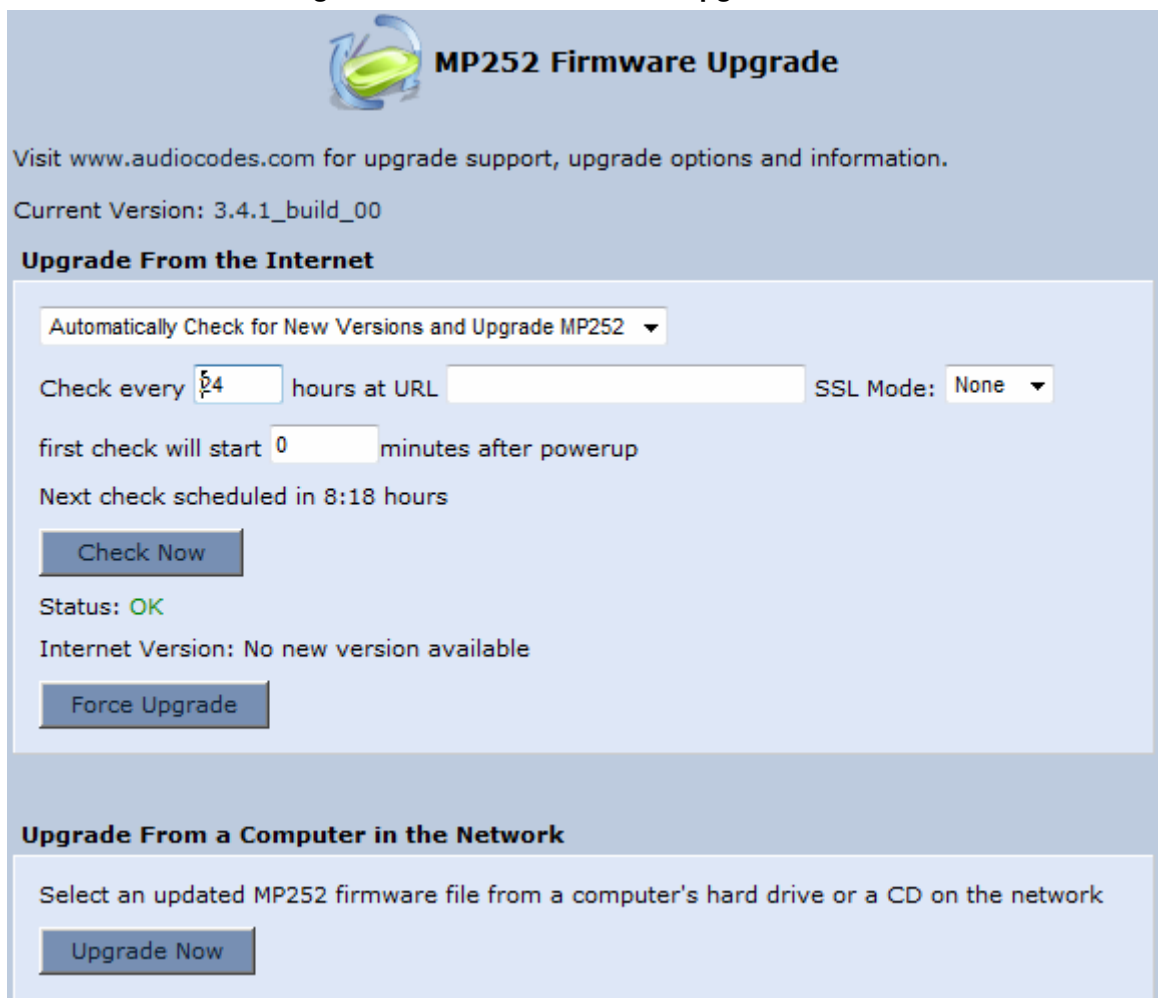
1. In the 'Advanced' screen, click the **Firmware Upgrade**  icon; the 'MP252 Firmware Upgrade' screen appears.

Figure 18-12: MP252 Firmware Upgrade Screen



MP252 Firmware Upgrade

Visit www.audiocodes.com for upgrade support, upgrade options and information.

Current Version: 3.4.1_build_00

Upgrade From the Internet

Automatically Check for New Versions and Upgrade MP252

Check every hours at URL SSL Mode:

first check will start minutes after powerup

Next check scheduled in 8:18 hours

Status: **OK**

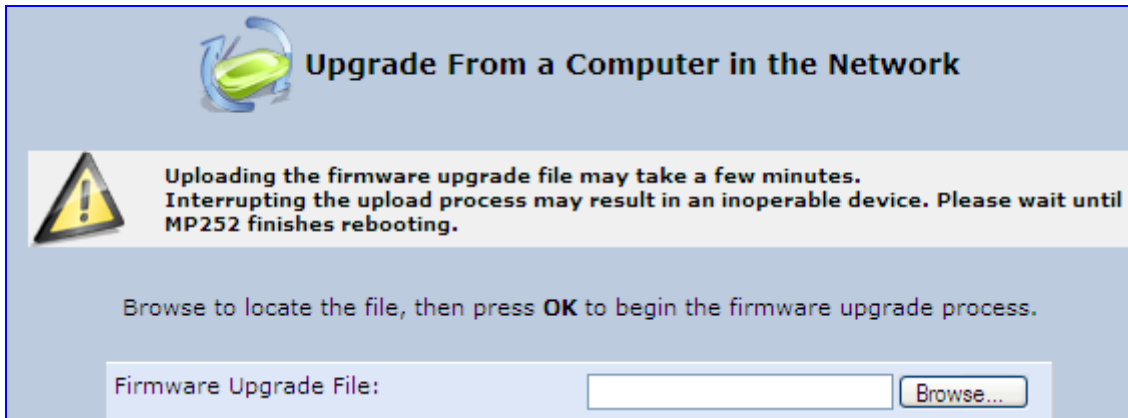
Internet Version: No new version available

Upgrade From a Computer in the Network

Select an updated MP252 firmware file from a computer's hard drive or a CD on the network

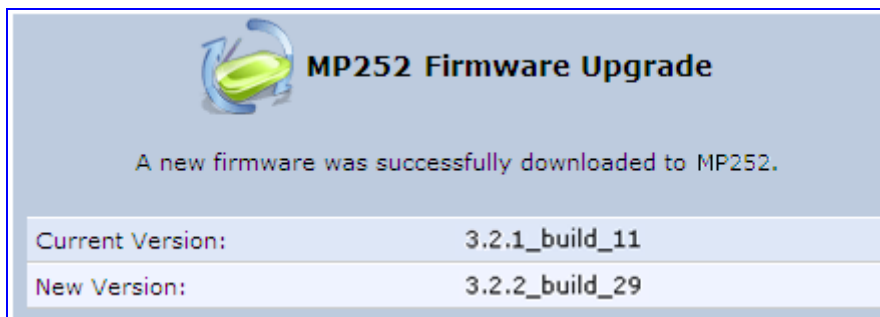
- Under the **Upgrade From a Computer in the Network** group, click the **Upgrade Now** button; the 'Upgrade From a Computer in the Network' screen appears.

Figure 18-13: Upgrade From a Computer in the Network Screen



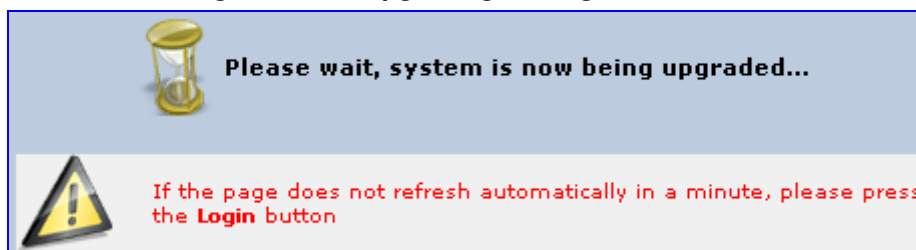
- In the 'Firmware Upgrade File' field, enter the path to the software image file or click **Browse** and navigate to the rmt file on your PC.
- Click **OK**; the MP252 uploads the file from your PC. When loading is complete, you are prompted to confirm upgrade to the new version.

Figure 18-14: Confirming Firmware Upgrade Screen



- Click **OK** to confirm; the upgrade process commences (a few minutes).

Figure 18-15: Upgrading in Progress Screen



At the conclusion of the upgrade process, MP252 automatically reboots and the new software version now runs on MP252, maintaining your configurations and settings.

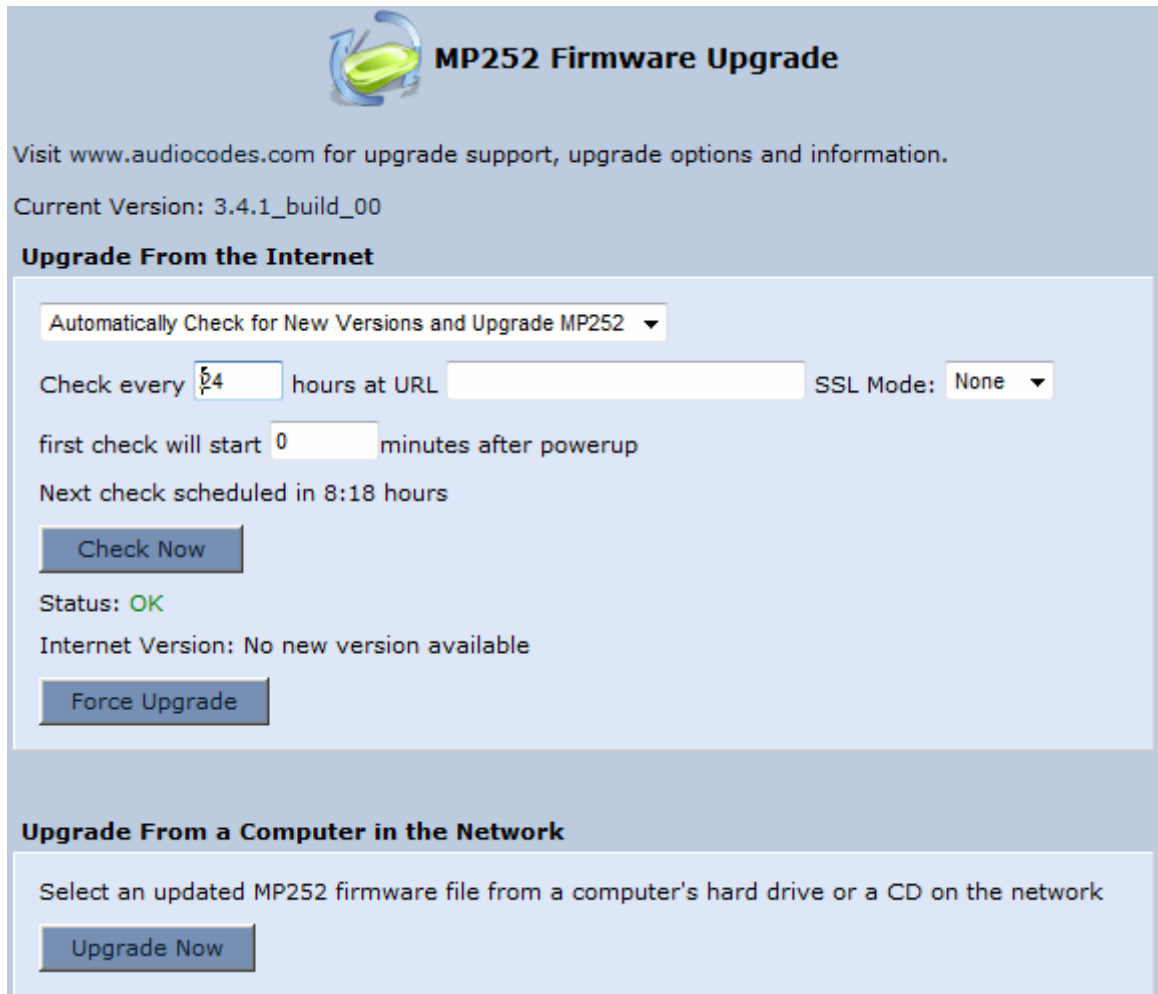
18.5.2 Upgrading From the Internet


The Remote Update mechanism helps you keep your software image up-to-date, by performing routine daily checks for newer software versions, as well as letting you perform manual checks. These updates are from a user-defined URL.

➤ **To upgrade MP252's software image from the Internet:**

1. In the 'Advanced' screen, click the **Firmware Upgrade** icon; the 'MP252 Firmware Upgrade' screen appears.

Figure 18-16: Advanced - Firmware and Configuration Upgrade



 **MP252 Firmware Upgrade**

Visit www.audiocodes.com for upgrade support, upgrade options and information.

Current Version: 3.4.1_build_00

Upgrade From the Internet

Automatically Check for New Versions and Upgrade MP252 ▾

Check every hours at URL SSL Mode: ▾

first check will start minutes after powerup

Next check scheduled in 8:18 hours

Status: OK

Internet Version: No new version available

Upgrade From a Computer in the Network

Select an updated MP252 firmware file from a computer's hard drive or a CD on the network

2. Under the **Upgrade From the Internet** group, select the utility's checking method and interval:
 - **Automatically Check for New Versions and Upgrade MP252:** MP252 automatically checks for new versions every user-defined interval (defined in the 'Check every' field) at the URL address defined in the 'URL' field. You can define the time (in minutes) after which the first check commences after MP252 is reset.
 - **Automatically Check for New Versions and Notify via Email:**
 - **Automatic Check Disable:** MP252 checks for a new version at the URL address defined in the 'URL' field, when you click the **Check Now** button.

The result of the last performed check is displayed between the **Check Now** and **Force Upgrade** buttons, indicating whether a new version is available or not.
3. If a new version is available:
 - a. Click the **Force Upgrade** button. A download process begins. When downloading is complete, you are prompted to confirm upgrade to the new version.
 - b. Click **OK** to confirm. The upgrade process begins and takes about one minute to complete. At the conclusion of the upgrade process, MP252 automatically reboots with the new software version.
4. If a new version is unavailable:
 - a. Click the **Check Now** button to perform an immediate check (instead of waiting for the next scheduled one). The screen displays the "Check in progress" message.
 - b. Click the **Refresh** button until the check is complete and the result is displayed.

18.6 System Settings

The 'System Settings' screen allows you to configure various MP252 system and management parameters.

➤ **To configure MP252 system and management settings:**


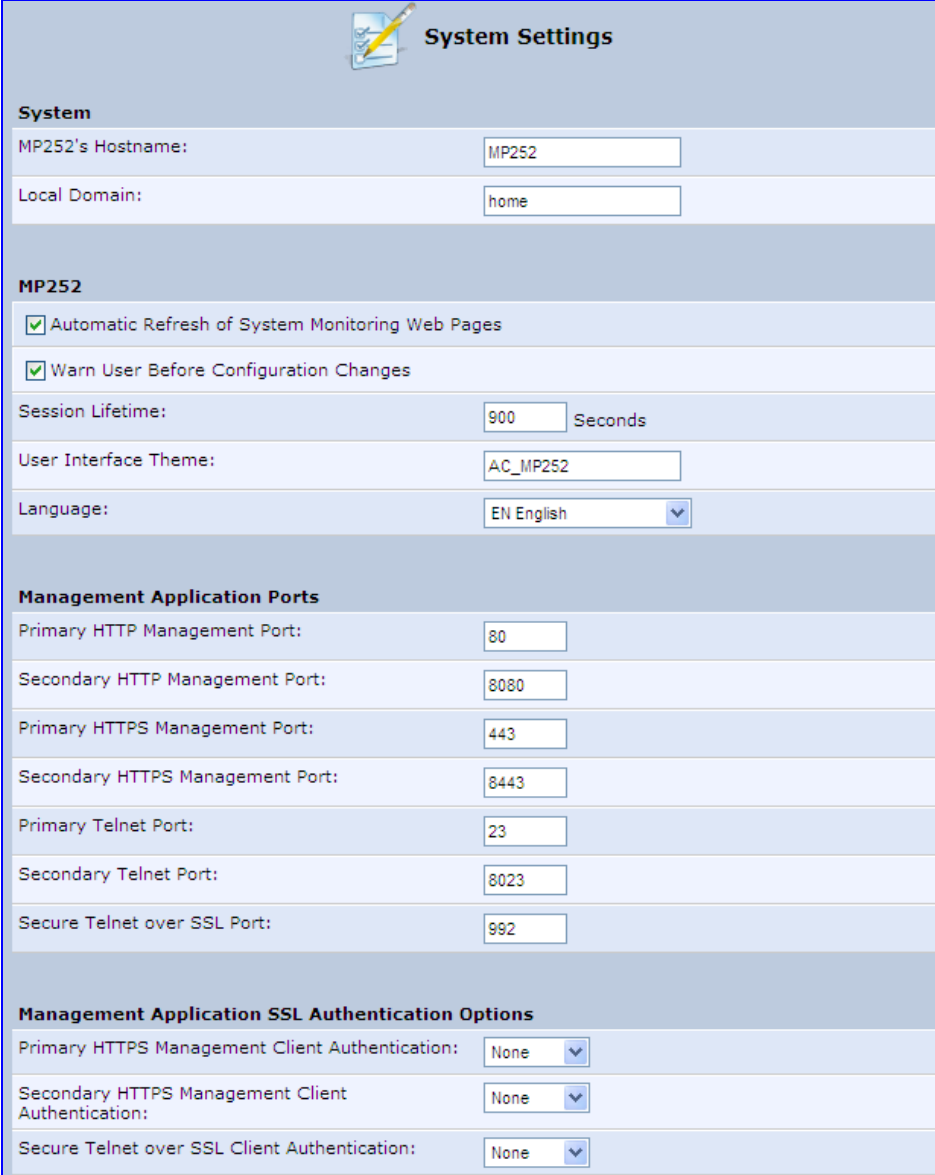
1. In the 'Advanced' screen, click the **System Settings**  icon; the 'System Settings' screen appears.

Figure 18-17: System Settings Screen (Only Partial View due to Screen Size)



System Settings

System

MP252's Hostname:

Local Domain:

MP252

Automatic Refresh of System Monitoring Web Pages

Warn User Before Configuration Changes

Session Lifetime: Seconds

User Interface Theme:

Language:

Management Application Ports

Primary HTTP Management Port:

Secondary HTTP Management Port:

Primary HTTPS Management Port:

Secondary HTTPS Management Port:

Primary Telnet Port:

Secondary Telnet Port:

Secure Telnet over SSL Port:

Management Application SSL Authentication Options

Primary HTTPS Management Client Authentication:

Secondary HTTPS Management Client Authentication:

Secure Telnet over SSL Client Authentication:



Note: Due to the size of the 'System Settings' screen, the figure above provides only a partial display.

2. Under the **System Settings** group, configure the following:

- In the 'MP252's Hostname' field, enter the MP252's host name. The host name is the MP252's URL address.
 - In the 'Local Domain' field, enter your network's local domain.
3. Under the **MP252** group, do the following:
 - **Automatic Refresh of System Monitoring Web Pages:** select this check box to enable automatic refreshing of system monitoring Web interface pages.
 - **Warn User Before Network Configuration Changes:** select this check box to activate user warnings before network configuration changes take effect.
 - **Session Lifetime:** duration of idle time (in seconds) in which the Web session remains active. When this duration times out, you must re-login.
 - **User Interface Theme:** enter an alternative GUI theme name.
 - **Language:** select a language for the Web interface GUI.
 4. Under the **Management Application Ports** group, define the following ports:
 - Primary/secondary HTTP management ports
 - Primary/secondary management HTTPS ports
 - Primary/secondary Telnet ports
 - Secure Telnet over SSL ports
 5. Under the **Management Application SSL Authentication Options** group, configure whether the following is required:
 - Primary/Secondary HTTPS Management Client Authentication
 - Secure Telnet over SSL Client Authentication
 6. Under the **System Logging** group, do the following:
 - **System Log Buffer Size:** size of the system log buffer in kilobytes.
 - **Remote System Notify Level:** MP252 sends notifications to a remote host (None, Error, Warning, Information)
 - **Persistent System Log:** saves the system log to MP252 flash memory. This prevents the system log from being erased when MP252 reboots.
 7. Under the **Security Logging** group, do the following:
 - **Security Log Buffer Size:** size of the security log buffer in Kilobytes
 - **Remote Security Notify Level:** None, Error, Warning, Information
 - **Persistent Security Log:** saves the security log to the flash. This prevents the security log from being erased when MP252 reboots.



Note: Do not leave the persistent logging feature enabled permanently, as continuous writing of the log files to the flash memory reduces MP252's performance.

8. Under the **Outgoing Mail Server** group, do the following:
 - **Server:** hostname of your outgoing (SMTP) server.
 - **From Email Address:** Each email requires a 'from' address and some outgoing servers refuse to forward mail without a valid 'from' address for anti-spam reasons.
 - **Port:** port used by your outgoing mail server.
 - **Server Requires Authentication:** If your outgoing mail server requires authentication, select this check box and enter your user name and password in the subsequent 'User Name' and 'Password' fields respectively.

To define email notifications per User to receive indications of system and security events, see Section 4.4 on page 44.
9. The **Swap** group configures the Swap feature that enables you to free a portion of the RAM by creating a swap file on the storage device connected to MP252. This is especially useful for platforms with a small RAM. To activate this feature:
 - a. Verify that a storage device is connected to MP252.
 - b. Select the 'Enabled' check box.
 - c. In the 'Swap Size' field, enter a swap file size in megabytes.
 - d. Click **Apply**; a swap file is created on the storage device and the read-only 'Status' field changes to "Ready".
10. Under the **Host Information** group, select the 'Enable Auto Detection of Host Services' check box to enable MP252 to auto-detect its LAN hosts' properties, available services, traffic statistics, and connections.
11. Under the **Installation Wizard** group, select the 'Use Installation Wizard Pre-configured Values' check box to have the wizard skip the steps for which parameters had been preconfigured and saved in the factory settings file (rg_factory).

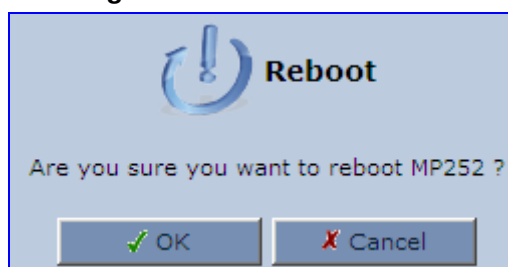
18.7 Reboot

The procedure below describes how to reboot MP252.

➤ **To reboot MP252:**

1. In the 'Advanced' screen, click the **Reboot**  icon; the 'Reboot' screen appears.

Figure 18-18: Reboot Screen



2. Click **OK** to reboot MP252. This may take up to one minute.
3. To re-enter the Web interface after rebooting MP252, refresh your Internet browser.

You can also reboot MP252 using a manual procedure, as described below:

➤ **To manually reboot MP252:**

- Insert a paper clip (or any other similar pointed object) into the Reset pin-hole button located on the rear panel of MP252, and keep the button pressed for at least 1 second (but no more than 5 seconds); the MP252 reboots.

18.8 Restoring Factory Settings

You can restore MP252 to factory default settings. This is useful when, for example, you are initially creating a new network or when you cannot recall changes made to the network.

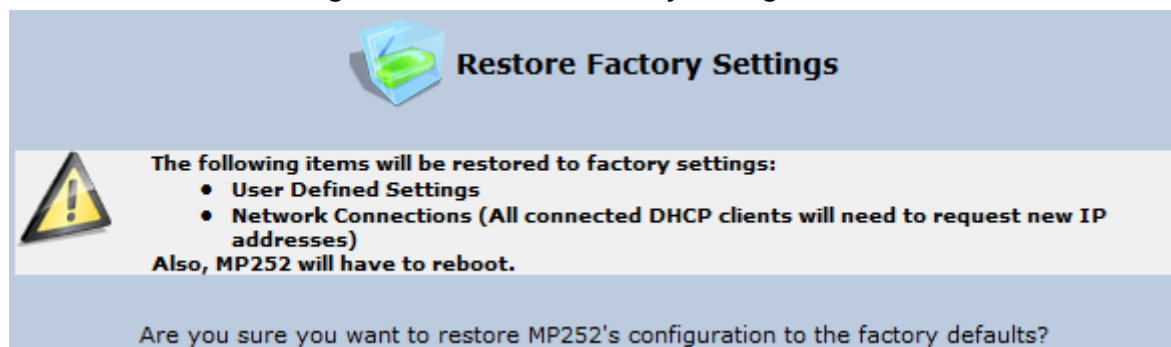
**Notes:**

- If you are accessing MP252's Web interface from the WAN, restoring factory default settings causes the connection with MP252 to be lost, since access to the Web interface from the WAN is blocked by default.
- **All** Web-based management settings and parameters are restored to their default values. This includes the administrator username and password

➤ **To restore MP252 to default settings:**

1. In the 'Advanced' screen, click the **Restore Factory Settings**  icon; the 'Restore Factory Settings' screen appears.

Figure 18-19: Restore Factory Settings Screen



2. Click **OK** to restore MP252's factory default settings.

If the MP252 Web interface cannot be accessed (for example, if the password is unknown or if the LAN is disabled), you can restore default settings manually, as described below:

➤ **To manually restore MP252 to default settings:**


- Insert a paper clip (or any other similar pointed object) into the Reset pin-hole button located on the rear panel of MP252, and keep the button pressed for **at least seven seconds**. While MP252 sets all its parameters to default, the **Status**, **Broadband**, and **Phone** LEDs blink red. After this, the **Status** LED is lit steady red while MP252 reboots.

19 Diagnostics and Performance Monitoring

The **System Monitoring** menu displays important system information and includes the following main tab screens:

- Network Connections – see Section 19.2 on page 339
- System Log – see Section 19.2.2 on page 340
- CPU – see Section 19.2.3 on page 340
- VoIP – see Section 19.2.4 on page 343
- Internet Connection Utilization - see Section 19.2.5 on page 343

19.1 Diagnostics

The **Diagnostics**  icon allows you to test network connectivity. In addition, it allows you to view statistics such as the number of packets transmitted and received, round-trip time, and success status. The test tools are platform-dependent and are not available simultaneously.

The **Diagnostics**  icon displays the 'Diagnostics' screen, as described below.

➤ **To access the 'Diagnostics' screen:**



- In the 'Advanced' screen, click the  icon.

Figure 19-1: Diagnostics Screen

 **Diagnostics**

Ping (ICMP Echo)
Destination:
Number of pings:
Status:

ARP
Destination: . . .
Status:

Traceroute
Destination:
Status:

PVC Scan
Status:

OAM Ping
Type:
VPI:
VCI:
Count:
Status:

19.1.1 Running a Ping Test

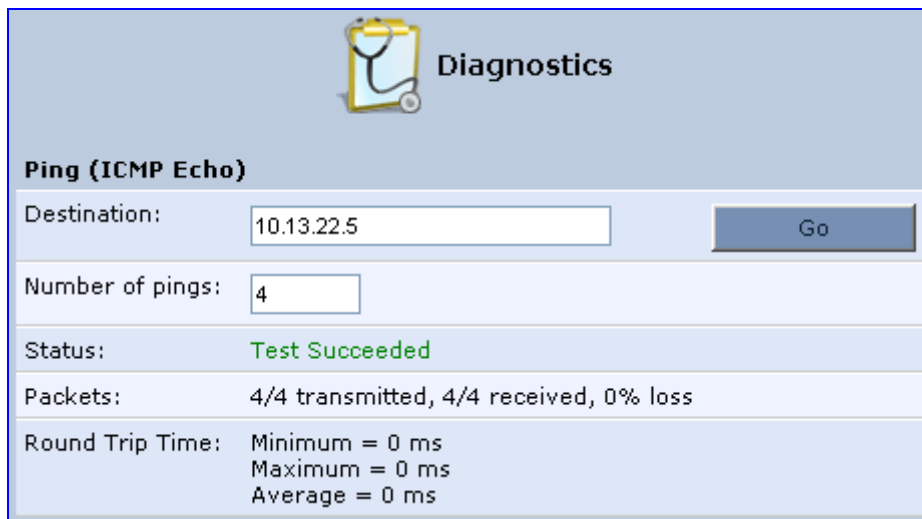
The procedure below describes how to run a ping (ICMP) test in the 'Diagnostics' screen. This test is done under the **Ping (ICMP Echo)** group.

➤ **To run a ping test:**

1. In the 'Destination' field, enter the IP address or URL to be tested.
2. In the 'Number of pings' field, enter the number of pings you want to perform.

3. Click **Go**; after a few seconds, diagnostic statistics are displayed. If no new information is displayed, click the **Refresh** button.

Figure 19-2: Running a Ping Test



19.1.2 Running an ARP Test

The ARP test is used to query the physical address (i.e., MAC) of a host.

The procedure below describes how to run an Address Resolution Protocol (ARP) test in the 'Diagnostics' screen. This test is done under the **ARP** group.

➤ **To run an ARP test:**

1. in the 'Destination' field, enter the IP address of the target host.
2. Click **Go**; after a few moments, diagnostic statistics is displayed. If no new information is displayed, click **Refresh**.

Figure 19-3: Running an ARP Test



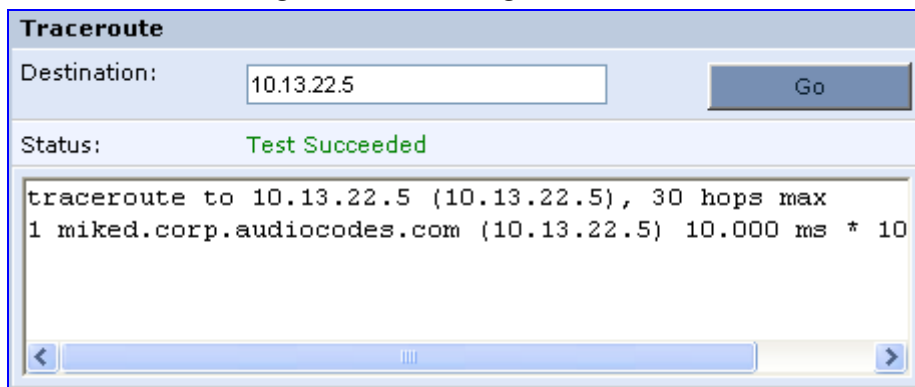
19.1.3 Running a Traceroute

The procedure below describes how to run a traceroute test in the 'Diagnostics' screen. This test is done under the **Traceroute** group.

➤ **To run a traceroute:**

1. In the 'Destination' field, enter the IP address or URL to be tested.
2. Click **Go**; a traceroute commences, constantly refreshing the screen.

Figure 19-4: Running a Traceroute



3. To stop the trace and view the results, click **Cancel**.

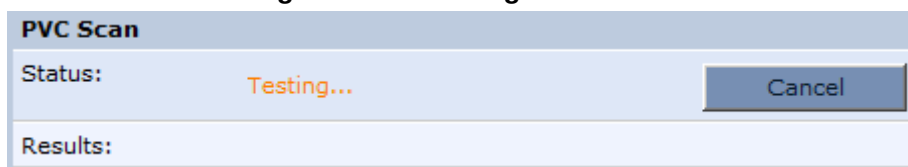
19.1.4 Running a PVC Scan Test

The procedure below describes how to run a Permanent Virtual Circuit (PVC) scan in the 'Diagnostics' screen.

➤ **To run a PVC scan:**

- Under the **PVC Scan** group, click **Go**; in a few moments, diagnostic statistics is displayed. If no new information is displayed, click **Refresh**.

Figure 19-5: Running a PVC Scan



19.1.5 Running an OAM Ping Test

The Operation and Maintenance (OAM) ping test checks the status of a Virtual Channel (VC) of the Asynchronous Transfer Mode (ATM) connection to the remote Network Access Concentrator (NAC). Each of the ATM's virtual channels has an address that consists of a Virtual Path Indicator (VPI) and Virtual Channel Indicator (VCI). The OAM ping test sends a request, either a VP loopback (F4) or a VC loopback (F5), and receives a reply from the NAC at the other end of the ATM connection.

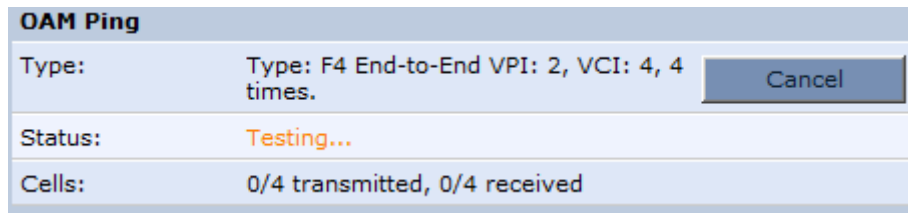
The procedure below describes how to run an OAM Ping test in the 'Diagnostics' screen. This test is done under the **OAM Ping** group.

➤ **To run an OAM ping test:**

1. From the 'Type' drop-down list, select the type of OAM ping to run:
 - F4 End-to-End
 - F4 Segment
 - F5 End-to-End
 - F5 Segment
2. In the 'VPI' field, enter the channel's VPI value.
3. In the 'VCI' field, enter the channel's VCI value. This is applicable only if you are checking the VC loopback (F5).
4. In the 'Count' field, enter a number of the ping packets sent to the destination address.

- Click **Go**; in a few moments, diagnostic statistics is displayed. If no new information is displayed, click **Refresh**.

Figure 19-6: Running an OAM Ping Test



19.2 Performance Monitoring

This section describes how to view the MP252 performance status.

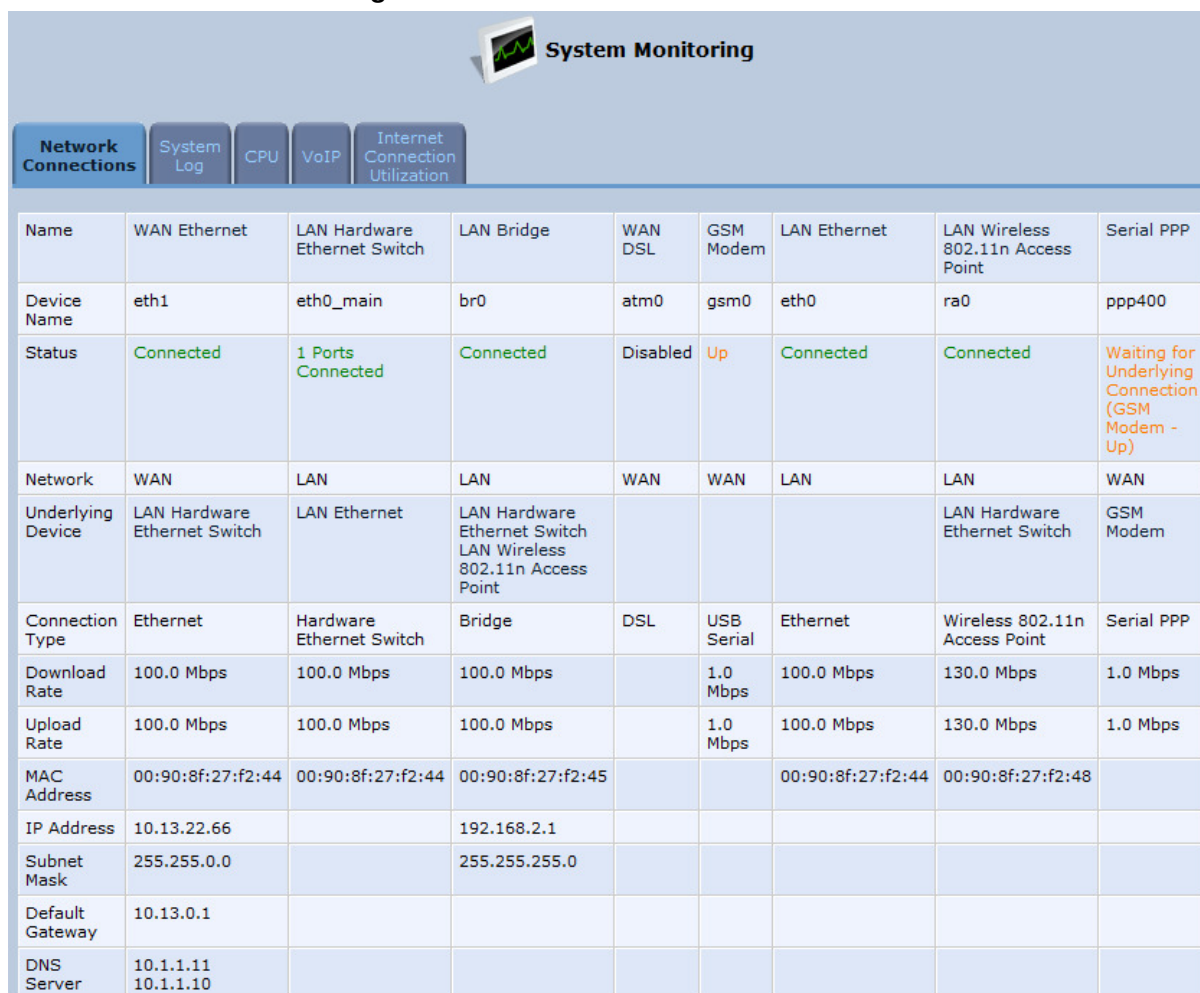
19.2.1 Network Connections

MP252 constantly monitors traffic within the local network and between the local network and the Internet. You can view up-to-the-second statistical information about data received from and transmitted to the Internet (WAN) and about data received from and transmitted to computers in the local network (LAN).

➤ **To view network connections:**

1. From the menu bar, click the **System Monitoring** menu.
2. Select the **Network Connections** tab.

Figure 19-7: Network Connections Screen



Name	WAN Ethernet	LAN Hardware Ethernet Switch	LAN Bridge	WAN DSL	GSM Modem	LAN Ethernet	LAN Wireless 802.11n Access Point	Serial PPP
Device Name	eth1	eth0_main	br0	atm0	gsm0	eth0	ra0	ppp400
Status	Connected	1 Ports Connected	Connected	Disabled	Up	Connected	Connected	Waiting for Underlying Connection (GSM Modem - Up)
Network	WAN	LAN	LAN	WAN	WAN	LAN	LAN	WAN
Underlying Device	LAN Hardware Ethernet Switch	LAN Ethernet	LAN Hardware Ethernet Switch LAN Wireless 802.11n Access Point				LAN Hardware Ethernet Switch	GSM Modem
Connection Type	Ethernet	Hardware Ethernet Switch	Bridge	DSL	USB Serial	Ethernet	Wireless 802.11n Access Point	Serial PPP
Download Rate	100.0 Mbps	100.0 Mbps	100.0 Mbps		1.0 Mbps	100.0 Mbps	130.0 Mbps	1.0 Mbps
Upload Rate	100.0 Mbps	100.0 Mbps	100.0 Mbps		1.0 Mbps	100.0 Mbps	130.0 Mbps	1.0 Mbps
MAC Address	00:90:8f:27:f2:44	00:90:8f:27:f2:44	00:90:8f:27:f2:45			00:90:8f:27:f2:44	00:90:8f:27:f2:48	
IP Address	10.13.22.66		192.168.2.1					
Subnet Mask	255.255.0.0		255.255.255.0					
Default Gateway	10.13.0.1							
DNS Server	10.1.1.11 10.1.1.10							

Click the **Refresh** button to update the display or click the **Automatic Refresh On** button to automatically refresh the displayed parameters. To reset the counters, click the **Reset Statistics** button.

19.2.2 System Log

The 'System Log' screen displays a list of the most recent activity that has occurred on MP252.

➤ **To view the system log:**

1. From the menu bar, click the **System Monitoring** menu.
2. Select the **System Log** tab.

Figure 19-8: System Log Screen

The screenshot shows the 'System Monitoring' interface. At the top, there are tabs for 'Network Connections', 'System Log' (selected), 'CPU', 'VoIP', and 'Internet Connection Utilization'. Below the tabs, there is a 'Refresh' button and a 'Clear Log' button. A 'Filters' section contains a table with columns 'Component', 'Severity', and 'Action'. The 'Severity' dropdown is set to 'Notice'. Below the filter table are 'Apply Filters' and 'Reset Filters' buttons. The main log table has columns 'Time', 'Component', 'Severity', and 'Details'. It lists several warning events related to 'Permissions' and 'LibJutil'.

Time	Component	Severity	Details
Jan 1 02:29:04 2003	Permissions	Warning	PERMISSION_CHECK USER[admin] ROLE[admin] PERMISSION [wireless_advanced] FAILED [repeated 3 times, last time on Jan 1 02:29:27 2003]
Jan 1 02:28:58 2003	LibJutil	Warning	sys_if_ioctl_mii_execute:433: Both tried MII ioctls 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on Jan 1 02:28:58 2003]
Jan 1 02:28:57 2003	Permissions	Warning	PERMISSION_CHECK USER[admin] ROLE[admin] PERMISSION [wireless_advanced] FAILED
Jan 1 02:28:42 2003	LibJutil	Warning	sys_if_ioctl_mii_execute:433: Both tried MII ioctls 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on Jan 1 02:28:42 2003]
Jan 1 02:28:42 2003	Permissions	Warning	PERMISSION_CHECK USER[admin] ROLE[admin] PERMISSION [wireless_advanced] FAILED
Jan 1 02:28:26 2003	LibJutil	Warning	sys_if_ioctl_mii_execute:433: Both tried MII ioctls 8947/89F0 failed: Operation not supported. [repeated 2 times, last time on Jan 1 02:28:26 2003]
Jan 1 02:28:26 2003	Permissions	Warning	PERMISSION_CHECK USER[admin] ROLE[admin] PERMISSION [wireless_advanced] FAILED

To update the display, click the **Refresh** button. To clear the list of logged events, click the **Clear Log** button. To save the logged events to a file (comma-separated values file) on your PC, click the **Download Log** button.

19.2.3 CPU

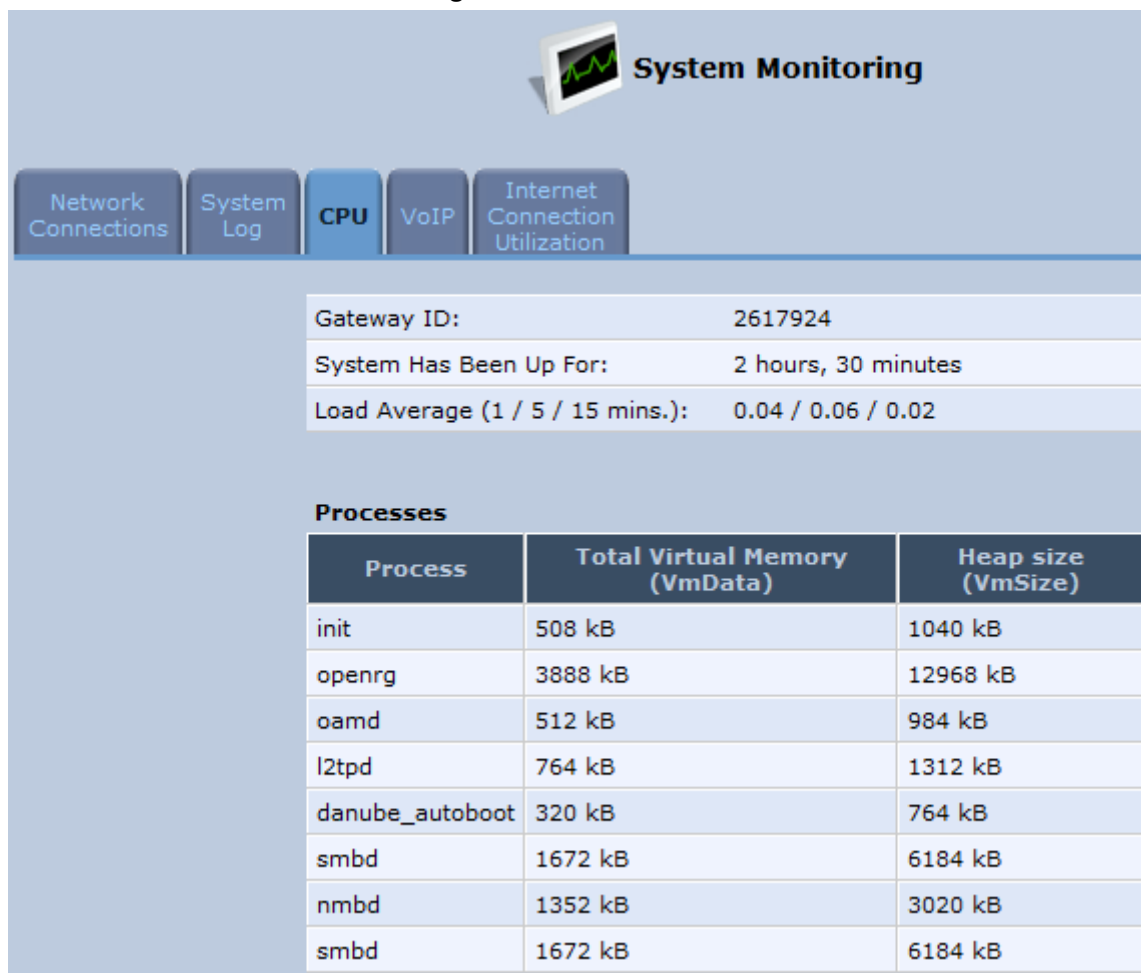
The 'CPU' screen displays the following system parameters:

- **Gateway ID:**
- **System Has Been Up For:** Time that has passed since MP252 was last started.

- **Load Average:** Average number of processes that are either in a runnable or uninterruptible state. A process in the runnable state is either using the CPU or waiting to use the CPU. A process in the uninterruptible state is waiting for I/O access, e.g. waiting for the disk. The averages are taken over the three time intervals. The meaning of the load average value varies according to the number of CPUs in the system. This means for example, that a load average of 1 on a single-CPU system means that the CPU was loaded all the time, while on a 4-CPU system this means that the CPU was idle 75% of the time.
- **Processes:** Processes currently running on MP252 and their virtual memory usage. The amount of memory granted for each process is displayed as follows:
 - **Total Virtual Memory (VmData):** Amount of memory currently utilized by the running process.
 - **Heap size (VmSize):** Total amount of memory allocated for the running process.

- **To view the CPU statistics:**
 1. From the menu bar, click the **System Monitoring** menu.
 2. Select the **CPU** tab.

Figure 19-9: CPU Screen



By default, the screen is automatically refreshed. To disable automatic refresh, click **Automatic Refresh Off**, and then click the **Refresh** button each time you want to update the display.

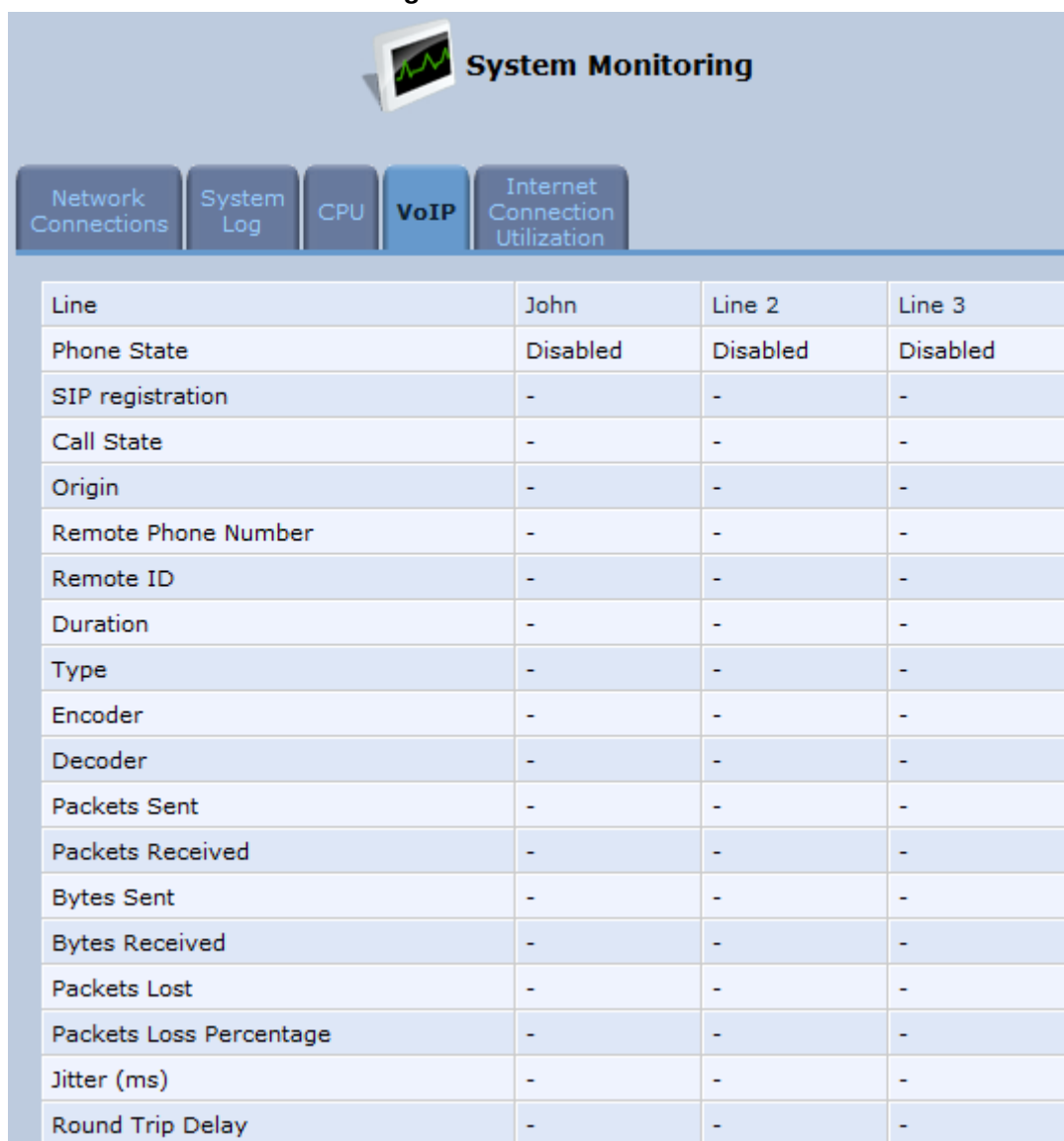
19.2.4 Voice over IP

The 'VoIP' screen displays information on VoIP traffic and settings.

➤ **To monitor VoIP traffic:**

1. From the menu bar, click the **System Monitoring** menu.
2. Select the **VoIP** tab.

Figure 19-10: VoIP Screen



Line	John	Line 2	Line 3
Phone State	Disabled	Disabled	Disabled
SIP registration	-	-	-
Call State	-	-	-
Origin	-	-	-
Remote Phone Number	-	-	-
Remote ID	-	-	-
Duration	-	-	-
Type	-	-	-
Encoder	-	-	-
Decoder	-	-	-
Packets Sent	-	-	-
Packets Received	-	-	-
Bytes Sent	-	-	-
Bytes Received	-	-	-
Packets Lost	-	-	-
Packets Loss Percentage	-	-	-
Jitter (ms)	-	-	-
Round Trip Delay	-	-	-

By default, the screen is automatically refreshed. To disable automatic refresh, click **Automatic Refresh Off**, and then click the **Refresh** button each time you want to update the display.

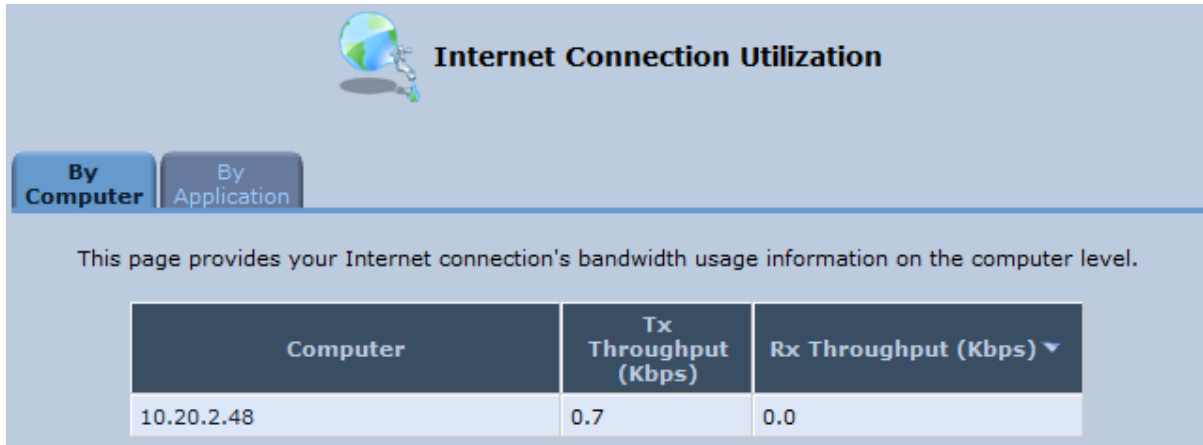
19.2.5 Internet Connection Utilization

The 'Internet Connection Utilization' screen displays the Internet connection bandwidth usage information per computer and application.

➤ **To monitor Internet connection usage:**

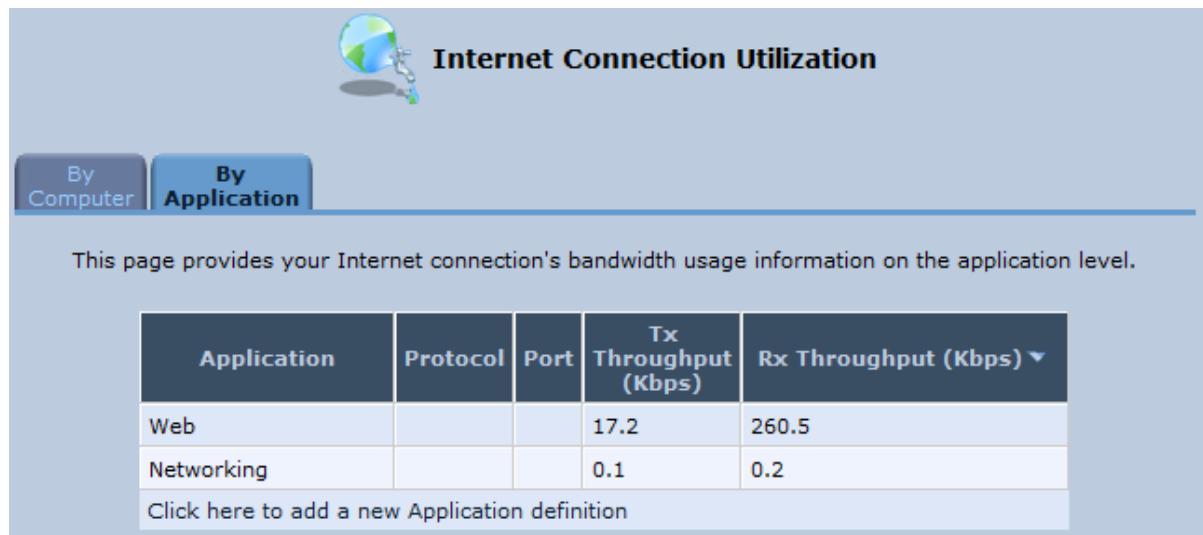
1. From the menu bar, click the **System Monitoring** menu.
2. Select the **Internet Connection Utilization** tab. By default, the **By Computer** tab is selected.

Figure 19-11: Internet Connection Utilization – By Computer Screen



3. To view bandwidth utilization per application, click the **By Application** tab.

Figure 19-12: Internet Connection Utilization – By Application Screen



By default, the screen is automatically refreshed. To disable automatic refresh, click **Automatic Refresh Off**, and then click the **Refresh** button each time you want to update the display.



Part II

DECT Phone

Part II describes the installation and configuration of the MP252 DECT phone, and includes the following chapters:

- Introduction
- Safety Instructions
- Getting Started
- General Phone Operation
- Phonebook
- Call List
- Clock and Alarm
- Customizing the Handset
- Base Settings
- Factory Defaults
- Troubleshooting



Note: This part is applicable only to **MP252WDNB**.

Reader's Notes

20 Introduction

Part I provides you with step-by-step instructions on how to use your AudioCodes MP252 cordless Digital Enhanced Cordless Telecommunications (DECT) VoIP telephone.

AudioCodes DECT phone offers the following main features:

- DECT technology providing high-definition voice quality, security and range
- Interference free for crystal clear conversations—no interference with other wireless networks and other electronic devices
- Up to 5 handsets can be registered to the MP252 base station
- Call hold
- Call transfer
- Auto-answer
- Call muting
- Silent ring mode
- Stores dialed, received and missed calls
- Last number redial
- Hands-free conversations using handset speakerphone
- Phone book directory of up to 150 contacts—easy to store and dial
- Three-way conference calls between outside call and between handsets
- Intercom between handsets
- Configurable LCD screen properties—contrast level and background wallpaper
- Handset volume control
- Built-in alarm clock with snooze
- Multi-language support for displaying the LCD screen
- Page/handset locator
- Selectable ring tones
- Keypad lock capability to prevent accidental pressing of keys
- Wall-mount bracket included
- Comfortable handset size

Reader's Notes

21 Safety Instructions

Before using your DECT phone, read the following safety instructions:

1. Read and understand all the instructions.
2. Follow all warnings and instructions marked on the product.
3. Unplug this product from the wall outlet before cleaning. Do not use liquid cleaners or aerosol cleaners. Use a damp cloth for cleaning.
4. Do not use this product near water (for example, near a bath tub, kitchen sink, swimming pool).
5. Do not overload wall outlets and extension cords as this can result in the risk of fire or electric shock.
6. Unplug this product from the wall outlet and refer servicing to AudioCodes under the following conditions:
 - When the power supply cord or plug is damaged or frayed.
 - If the product does not operate normally by following the operating instructions.
 - If the product has been dropped and the cabinet has been damaged.
 - If the product exhibits a distinct change in performance.
7. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
8. Do not use the telephone to report a gas leak in the vicinity of the leak.
9. Use only the supplied nickel-metal hydride cell (NiMH) rechargeable batteries! The operation periods for the handsets are only applicable with the default battery capacities.
10. Use only the supplied 12VDC +/-10%, tolerance, 2A, limited power source wall mount Class II power supply adapter. Before connecting MP252 to power, ensure that the VAC ratings match.
11. The use of other battery types or non-rechargeable batteries/primary cells can be dangerous. These may cause interference and/or unit damages. The manufacturer will not be held liable for damage arising from such non-compliance.
12. Do not use third-party charging bays. The batteries may be damaged.
13. Please note the correct polarity while inserting the batteries.
14. Do not immerse batteries in water, do not place in fire.



Caution

RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE.

Reader's Notes

22 Getting Started

22.1 Installing the DECT Phone

The procedure below describes how to install the DECT phone on the MP252 unit.

➤ **To install the DECT phone:**

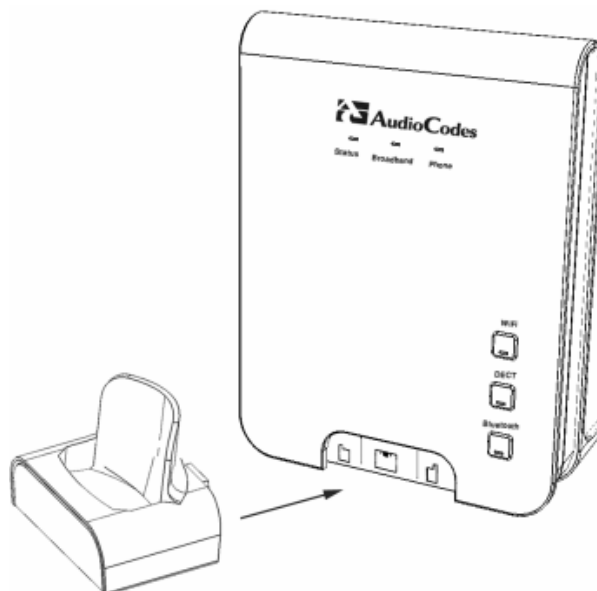
1. The handset is shipped with rechargeable batteries already installed in the battery compartment. However, a plastic sheath separates the batteries from the handset's electrical circuit. Before you can charge the handset, you need to remove this plastic sheath. On the handset, pull out the plastic tab jutting out from the battery compartment. This closes the battery circuit and provides power to the handset.

Figure 22-1: Plastic Tab jutting out from Battery Compartment



2. On the lower part of the MP252 front panel, remove the cover protecting the connector for the handset cradle.
3. Attach the handset cradle to the unit by inserting it into the exposed groove and then pushing it up so that it clicks on to the connector. Attach the removed cover to the front of the cradle.

Figure 22-2: Attaching Handset Cradle to MP252 Base Unit



4. Place the handset in the cradle and leave to charge for at least 16 hours prior to initial use.

22.2 Powering the Handset

22.2.1 Charging the Handset

Once you have installed the batteries, you need to charge them before initial operation.



Note: Charge the batteries for at least 16 hours before initial use.

➤ **To charge the handset:**


1. Ensure that the MP252 is connected to power.
2. Place the handset in the charging cradle of the base unit so that the bottom of the phone sits in the base cradle. When correctly inserted in the cradle, the phone begins charging, indicated by the display of the charging levels of the battery  icon in the phone's screen. For checking battery level, see Section 22.2.2 on page 354.

Figure 22-3: Handset Charging in Cradle



Notes:

- During a call, if your handset batteries are low, your handset will play a warning tone. Replace the handset on the base to recharge them.
- Your phone can sound an alert tone when the battery is low. To activate this alert, see Section 27.3.2 on page 392.

22.2.2 Checking the Battery Level

The battery icon located in the main screen, displays the current battery level, as shown below:



Handset battery is fully charged.



Handset battery is two-thirds charged.



Handset battery is one-third charged.



Handset battery is empty and needs charging. This icon flashes.

Your handset may power down if it is not charged after the battery is empty. If you are in a call and the battery is low, an alert tone is sounded. You can enable or disable this alert tone feature (see Section 27.3.2 on page 392).

22.2.3 Switching the Base Unit On or Off

To operate your phone, the base station must be on. You can turn the base station on or off as described in the procedure below:

➤ **To switch the base on or off:**

- On the MP252, press the **DECT** LED button. When the base station is switched off, the **DECT** LED is lit red. When switched on, the LED is green or another color depending on the state of the phone. For a description of the **DECT** LED, see Section 22.3.3 on page 363.

22.2.4 Switching the Handset On or Off

When you place the handset in the base unit to charge, the handset automatically turns on. You can turn the handset on or off, as described in the procedure below:

➤ **To switch the handset on or off:**

- On the handset, continually press the  button until the handset switches off or on.

22.2.5 Replacing the Batteries

The handset is shipped with rechargeable batteries. However, if you need to replace them, follow the procedure described in this section.



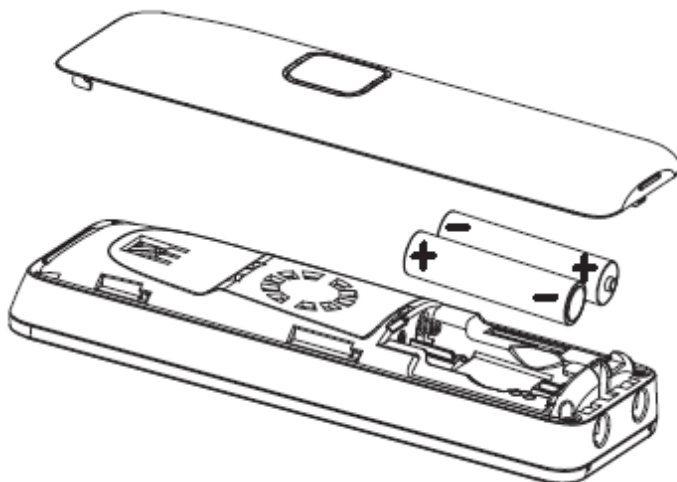
Warnings:

- Risk of explosion if battery is replaced by an incorrect battery type; use only the nickel-metal hydride cell (NiMH) rechargeable batteries as provided with your phone (for battery specifications, see Section A on page 403). The manufacturer will not be held liable for damage arising from such non-compliance.
- Verify correct polarity of the batteries when inserting the batteries. Incorrect polarity may damage the product.
- The operation periods (as stated in Section A on page 403) for the handset are only applicable with the default battery capacities.
- Do not use third-party charging bays to charge the batteries.
- Do not immerse batteries in water and do not place in fire.
- Do not mix old and new batteries.
- Do not open or mutilate the batteries. Released electrolyte from the batteries is corrosive and may cause burns or injury to the eyes or skin. The electrolyte is toxic and may be harmful if swallowed.
- Do not allow conductive materials such as rings, bracelets, or keys to touch the batteries, otherwise a short circuit may cause the batteries and/or the conductive material to overheat and cause burns.
- Avoid touching the battery ends (+, -) or the base unit contacts.

➤ To install the handset batteries:

1. Remove the battery compartment cover, by sliding the cover out from the base of the phone toward the top end (in the direction of the arrow label printed on the cover). You can use your thumb to push at the base of the cover.
2. Remove the old batteries (if any) and then place the two batteries (supplied) into the battery compartment, as indicated.
3. Slide the battery compartment cover back into place.

Figure 22-4: Installing Batteries



22.3 Getting to Know Your Phone

22.3.1 Overview of the Handset

The areas of the handset are shown in the figure below and described in the subsequent table.

Figure 22-5: Areas of the Handset

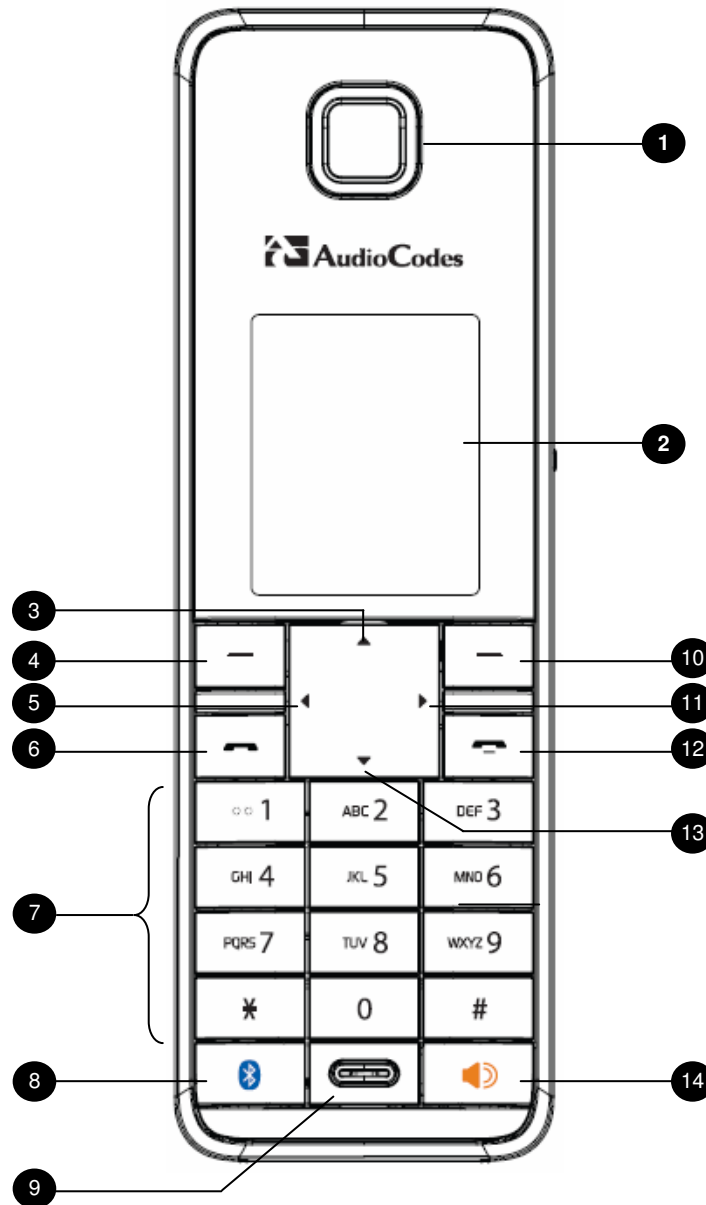












Table 22-1: Handset Description

Item	Label	Description
1	-	Earpiece
2	-	Display
3		Up Arrow / Redial List <ul style="list-style-type: none"> In idle mode: Press to access the redial list. In menu mode: Press to scroll up the menu items In Phonebook list / Redial list / Call List: Press to scroll up the list During a call: Press to increase the volume
4		Left Softkey <ul style="list-style-type: none"> In idle mode: Press to access the main menu In submenu mode: Press to confirm selection During a call: Press to access the submenu
5		Left Arrow <ul style="list-style-type: none"> In idle mode: Press to list the registered handsets. In editing/pre-dialing mode: Press to move the cursor one character to the left. During a second call: press and hold to conference your calls.
6		Talk On <ul style="list-style-type: none"> In idle / pre-dialing mode : Press to make a call In Redial list / Call List/ Phonebook entry: Press to make a call to the selected entry in the list During ringing: Press to answer a call
7		Alphanumeric Keypad, * (Star), # (Hash) Press to insert a digit / character / * / # <ul style="list-style-type: none"> * key in idle mode: Long press to turn on/off the ringer * key in editing mode: Long press to switch the character set * key during a call: Short press to switch to tone dialing mode temporarily if using pulse dialing mode currently # key in editing mode: Long press to toggle between uppercase or lowercase character input # key in Idle mode: Long press to turn on / off the keypad lock 0 key in pre-dialing / number editing mode: Long press to insert a pause
8		Bluetooth Note: This button will be supported in the next applicable release.
9	-	Microphone
10		Right Softkey <ul style="list-style-type: none"> In idle mode: Press to access the phonebook In sub-menu mode: Press to go back to previous level In editing / pre-dialing mode: Press to clear a character / digit In editing / pre-dialing mode: Long press to delete all the characters / digit During a call: Press to hold / unhold the call.
11		Right Arrow <ul style="list-style-type: none"> In pre-dialing / editing mode: Press to move the cursor one character to the right. During a second call: Press to toggle between calls.

Item	Label	Description
12		Talk Off <ul style="list-style-type: none"> ▪ During a call: Press to end a call and go back to idle screen ▪ When there are two calls and the second is an outgoing call: Press to transfer the first call to the user of the second call. ▪ In menu / editing mode: Press to go back to idle screen ▪ In Idle: Press and hold to power off the handset ▪ When the handset is power off: Press and hold to power on the handset
13		Down / Call List <ul style="list-style-type: none"> ▪ In idle mode: Press to access the call list ▪ In menu mode: Press to scroll down the menu items ▪ In Phonebook list / Redial list / Call List: Press to scroll the list ▪ During a call: Press to decrease the volume
14	-	Speakerphone <ul style="list-style-type: none"> ▪ During a call: Press to turn on / off the speakerphone. ▪ Call List / Phonebook entry: Press to make a call with speakerphone ▪ During ringing: Press to answer a call with speakerphone

22.3.2 Getting to Know your Handset LCD Screen

The handset LCD provides various icons that are displayed according to the current status and operational mode of the phone. An example of the phone's LCD is shown below and the icons are described in the table below.

Figure 22-6: Areas of the Handset LCD Screen

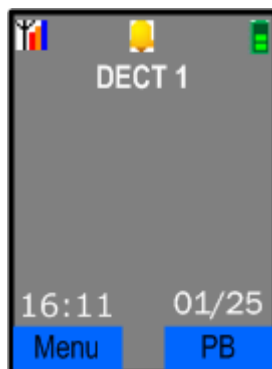
















Table 22-2: Handset LCD Icon Descriptions

Icon	Description
	Steady when the handset is in range of the base. Additional bars (red, orange, and blue) are displayed as the signal strength increases.
	Flashes when the handset is not registered to the base, in marginal range or out of range of the base. When the handset is out of range, the LCD displays "Out of Range" message.
	The alarm is set. When the alarm time is reached, this icon flashes. This icon disappears when the alarm is off.
	Intercom is in progress.
	Phone is ringing (i.e., incoming call).
	Call is in progress.
	Hands-free is in use.
	Headset is in use.
	Ringer is switched off.
	keypad is locked.
	Handset battery is fully charged.

Icon	Description
	Handset battery is one-third charged.
	Handset battery is two-thirds charged.
	Handset battery is empty and needs charging. This icon flashes.

22.3.2.1 Menu Structure

Your phone provides various features and functions that are grouped in the menus.

➤ **To access the Menu list and its submenus:**















1. Press the **Menu** softkey.
2. Use the 4-way navigation  keys to navigate to the required menu.
3. Press the **Select** softkey to access the required menu.
4. To drill-down submenus, use the  navigation keys to select the required submenu and then the **Select** softkey to access it.

Table 22-3: Handset LCD Menus and Submenus

Menu Icon		Menu Name	Submenus
Unselected	Selected		
		Call List (See Section 25 on page 381)	<ul style="list-style-type: none"> ▪ Call List ▪ Missed Calls ▪ Received Calls ▪ Redial List
		Clock/Alarm (see Section 26 on page 385)	<ul style="list-style-type: none"> ▪ Date & Time ▪ Alarm
		Base Settings (See Section 28 on page 395)	<ul style="list-style-type: none"> ▪ Manage HS ▪ Line Settings ▪ Modify PIN ▪ BS Default ▪ Product Version ▪ Nemo Mode
		Phonebook (See Section 24 on page 377)	<ul style="list-style-type: none"> ▪ View ▪ Add ▪ Edit ▪ Delete ▪ Delete All <p>Note: If the Phonebook is empty, then only the Add submenu appears.</p>

Menu Icon		Menu Name	Submenus
Unselected	Selected		
		HS Settings (See Section 27 on page 389)	<ul style="list-style-type: none"> ▪ Audio Setup ▪ Ring Setup ▪ Tone Setup ▪ Language ▪ Wallpaper ▪ Contrast ▪ Auto Answer ▪ Select Base ▪ HS Default
		Registration	<ul style="list-style-type: none"> ▪ Base 1 ▪ Base 2 ▪ Base 3 ▪ Base 4




The following menus or submenus can also be accessed using the  navigation keys when the phone is in idle mode:

Table 22-4: Handset LCD Menus and Submenus Accessed using Navigation Keys

Pressed Key	Accessed Menu/Submenu	Description
▲	Redial List	Navigate to the phone number that you want to redial, and then press the  button. For detailed description on redialing calls, see Section 23.1.5 on page 368.
▼	Call List	Navigate to the phone number that you want to dial, and then press the  button. For a detailed description on dialing from the Call List, see Section 23.1.4 on page 368.
◀	Intercom	This submenu allows you to make intercom calls between handsets. Navigate to the handset that you want to call. For a detailed description on making intercom calls, see Section 23.11.1 on page 373.

22.3.2.2 Entering Text and Digits

Your phone allows you to enter strings consisting of letters, digits (numbers) and/or symbols. These are required, for example, when defining the handset name and adding phonebook contacts. In addition, your phone supports a variety of character sets including Latin, Russian, Spanish, and Hebrew.

The character strings are entered using the phone's keypad keys.

Figure 22-7: Handset Keypad

QW 1	ABC 2	DEF 3
GHI 4	JKL 5	MNO 6
PQRS 7	TUV 8	WXYZ 9
* 0	0	#

Each key allows you to enter numerous characters in addition to those printed on the keys label. The number 1 key provides commonly used characters such as @ and #.

➤ **To select a character:**

- Press the key consecutively until the required character is displayed.

➤ **To toggle between upper and lowercase letters:**


- Press the # key until you hear a beep.

➤ **To toggle between character sets (languages):**

- Press the star key (*) until you hear a beep.

In editing mode, a cursor is displayed to indicate the current text-entry position. It is positioned at the right of the last character entered.

Writing tips:

- Once a character is selected, the cursor moves to the next position after a short pause.
- You can move the cursor within the text by using the 4-way navigation  keys to modify the text entry.
- Press the **Clear** softkey to delete the last character.
- Press and hold the **Clear** softkey to delete the entire text string..

22.3.3 Viewing Base Unit Status with DECT LED

The **DECT** LED is located on the front panel of MP252 and indicates the operating status of the cordless phone, as described in the table below:

Table 22-5: DECT LED Description

Color	State	Description
Green	On	Base unit is ready to make or receive calls with the handset.
Green	Flashing	Base is available for handset registration. To register a handset, see Section 22.4 on page 363
Red	On	The base unit is on, but no handset is registered to it.
Amber	Flashing	Handset is being paged. To page (locate) the handset, see Section 23.10 on page 372.
Red	Flash	Malfunction in DECT cordless phone.
-	Off	Phone is switched off. To switch the phone on or off, see Section 22.2.3 on page 354.

22.4 Upgrading MP252 and the Base Unit

If the software version currently running on MP252 is older than Version 3.3.0 build 17, you need to upgrade your MP252 as well as your MP252 base unit.



Note: If you are a registered customer, you can download the latest MP252 software file and base unit software file from AudioCodes Web site at <http://www.audiocodes.com/downloads>. These files include *V1MOD_SPI_app.bin* and *MP252_3_3_0_build_17_05_Jan_2011.rmt*.

You can view the current software version running on MP252 by using the Web interface, as follows:



1. Access the MP252 Web interface.
2. From the menu pane, select the **Advanced** menu, and then click the **About MP252**  icon; the 'About MP252' screen appears.

Table 22-6: About MP252 Screen

➤ **To upgrade the MP252 and base unit software versions:**

1. Upgrade the MP252 software version to 3.3.0_build_17. This is done in the Web interface's 'Firmware Upgrade' screen (**Advanced** menu > **Firmware Upgrade**  icon). For a detailed description, refer to the *MP252 User's Manual*.
2. Once upgraded, establish a telnet session with MP252, and then run the following CLI command:

```
dect save_settings_in_factory
```


3. Plug a USB flash drive containing the DECT base version file into the USB port, located on the rear panel of MP252.
4. Ensure that the **DECT** LED is lit.
5. Run the following CLI command:

```
dect upgrade
```

The upgrade process begins and the **DECT** LED blinks (fast) green. Upgrade takes approximately 8 minutes.



Note: During the upgrade process, do **NOT** power off MP252, remove the USB drive, nor any other action on MP252.

6. Once the base unit has completed its upgrade (indicated by the **DECT** LED being lit steady green again), reboot MP252. This is done in the Web interface's 'Reboot' screen (**Advanced** menu > **Reboot**  icon). For a detailed description, refer to the *MP252 User's Manual*.

22.5 Defining the MP252 Handset Line




Before you can operate the phone, the handset needs to be defined as one of the MP252 phone lines. By default, the handset is automatically assigned **Line 3** of the MP252. Configuration of this line is done using the MP252 Web interface, as described below.

➤ **To define the handset phone line on MP252:**

1. Access the MP252 Web interface.
2. From the menu pane, select the **Voice Over IP** menu; the 'Voice Over IP' screen.
3. Select the **Line Settings** tab; the 'Line Settings' screen appears.

Table 22-7: Line Settings Screen



Line	User ID	Display Name	Action
<input type="checkbox"/> 1	0000000001	Line 1	
<input type="checkbox"/> 2	0000000002	Line 2	
<input checked="" type="checkbox"/> 3	4410	4410	


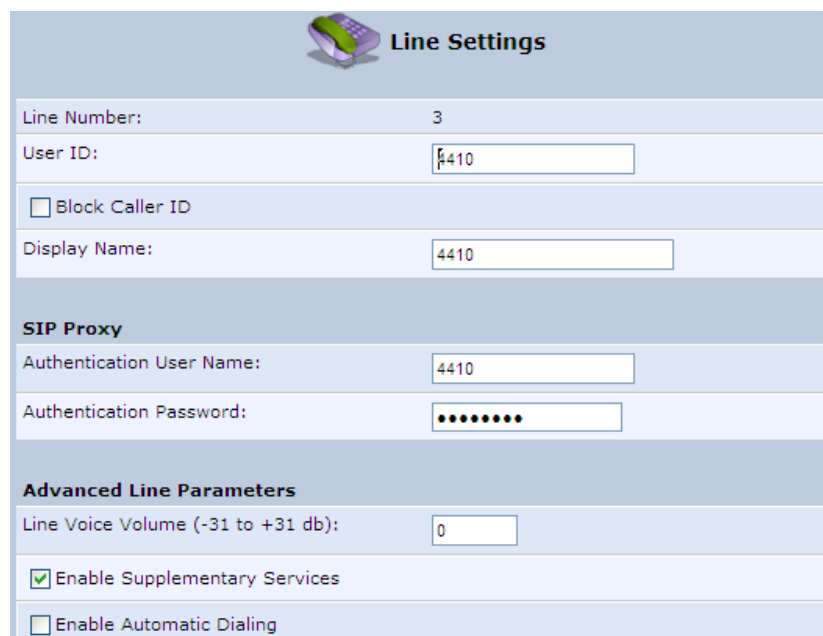
4. Click the **Edit**  icon corresponding to Line 3.

Table 22-8: Defining Line 3 Properties



Line Settings

Line Number: 3

User ID:

Block Caller ID

Display Name:

SIP Proxy

Authentication User Name:

Authentication Password:

Advanced Line Parameters

Line Voice Volume (-31 to +31 db):

Enable Supplementary Services

Enable Automatic Dialing

5. Define the following line settings:
 - **User ID:** phone number (extension) of the MP252 handset
 - **Display Name:** String displayed to remote parties as your caller ID
 - **Authentication User Name:** User name (obtained from your service provider) used when sending a response to Unauthorized or Proxy Authentication Requested (401/407)




- **Authentication Password:** Password (obtained from your service provider) used when sending a response to Unauthorized or Proxy Authentication Requested (401/407)

22.6 Registering the Handset to Base Unit

Before you can use your handset, you need to register it to the base unit. Up to five handsets can be registered to the base unit. If the handset is not registered to the base unit, the following is displayed on its screen:


- 📶 icon flashes
- “Out of Range” message appears in idle state

➤ To register the handset to the base:

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Registration**  icon, and then press the **Select** softkey.
3. On the M-252 base unit, press the **DECT** LED button until (2 – 5 seconds) it starts flashing green; the base unit enters registration mode. (The registration mode remains active for 30 seconds, after which the **DECT** LED stops flashing. Therefore, proceed to the next step before this interval expires.)
4. Press the  navigation keys to choose the base unit (i.e., “Base 1”) to which you want to register the handset, and then press the **Select** softkey; the registration process begins and the “Registering - Waiting” is displayed.
5. When the handset identifies the base, it displays its radio frequency (RF) identification (each base has a unique RF ID). Click the **Accept** softkey to confirm (or press the **Rej** softkey to cancel registration).
6. On some handsets, you are prompted to enter a PIN code. The default PIN code is 0000 (see Section 28.2 on page 397 for defining the PIN code).

If the handset successfully registers to the base, a confirmation tone is heard and the 📶 icon stops flashing. The handset is automatically allocated the next available handset number. This handset number is displayed on the handset screen in idle mode. The base unit to which the handset is successfully registered is marked with an asterisk “*” in the **Registration** menu (see Section 27.8 on page 393).

22.7 Checking the Handset Signal Strength

The antenna  icon displays the signal strength between your handset and the base unit:



Signal strength is excellent.



Signal strength is good.



Signal strength is poor.



When the icon is steady, the handset is in range of the base (but signal strength is weak). When the icon flashes, it indicates that the handset is out of range and there is no link with the base unit.

As the distance between the handset and the base increases, so the signal strength decreases and vice versa.



Notes:

- The maximum range between the base station and the handset is approximately 300 meters. Depending on the surrounding conditions as well as spatial and structural factors, the range may be reduced. The range indoors is normally less than outdoors.
- If your handset has lost its link with the base unit, you cannot make or receive calls. In addition, many other phone functions cannot be performed.

23 General Phone Operation

23.1 Making an External Call



External calls are calls made to remote parties other than another registered headset (if any) to the MP252 base.



Note: Your handset automatically displays the duration of every call. This is shown in hours, minutes and seconds format (HH:MM:SS).



23.1.1 Pre-dialing

Preparatory dialing is when you first enter the phone number and only then dial it. This therefore, allows you to make changes to the number before making the call.

1. Enter the phone number; the number is displayed on the screen. You can make changes to the number before dialing. Press the **Clear** softkey to delete digits to the left of the cursor.
2. Press  or  to dial the number.




23.1.2 Direct Dialing

Direct dialing is when you activate dialing and only then enter the phone number.

1. Press  or  to take the line.
2. Enter the phone number; the phone waits a few seconds and then dials the number.





23.1.3 Calling from your Phonebook

If you have added any contacts to your phonebook, you can dial from the phonebook.

1. Press the **PB** softkey to access the phonebook.
2. Press the  navigation keys to choose the desired phonebook entry, and then press the **Select** softkey.
3. Press  or  to dial the selected phonebook entry.

23.1.4 Calling from the Call List




You can dial numbers from previously received or missed calls, which are stored in the Call List:

1. Press the  navigation key to access the Call List.
2. Press the  navigation keys to select the desired entry, and then press the **Select** softkey.
3. Press  or  to dial the selected entry.

23.1.5 Establishing a Second Call





While you are in an active call, you can establish a second call. When you establish a second call, the first call is put on hold. You can toggle between the calls by placing one call on hold while speaking to the other call (see Section 23.11.4 on page 374).

To establish a second call, do one of the following:

- **Making a second call directly:**
 1. Press ; the Predialing screen appears.
 2. Dial the desired number, and then press  again.
- **Making a second call to a contact in your phonebook:**
 1. Press the **Menu** softkey, and then choose **Phonebook**.
 2. Select a number from the phonebook, and then press .
- **Manually placing the first call on hold before making a second call:**
 1. Press the **Hold** softkey to place the current call on hold.
 2. Establish a second call by doing one of the previously mentioned methods.



23.1.6 Redialing a Number

You can dial numbers that were previously dialed, which are stored in the Redial List.

1. Press the  navigation key to access the Redial List.
2. Press the  navigation keys to select the desired number, and then press the **Select** softkey.
3. Press  or  to dial the selected entry.



23.2 Answering a Call

When you receive a call, your phone rings and the following is displayed on your screen:

- “Incoming Call”
- Calling number is displayed
- **To answer a call:**
 - **If the handset is not on the base:** When the phone rings, press  or .
 - **If the handset is on the base and when Auto Answer is set to On:** When the phone rings, pick up the handset.

23.3 Answering or Rejecting a Second Call

While you are talking on the phone, you can receive a second call. The phone provides the following indications of a second incoming call:

- A beep tone is sounded.
- The “Call Waiting” message is displayed on the screen with the details (name and number) of the calling party.
- **To answer a second call:**
 - Press  to answer the call; the call with the second call party is established and the first call is put on hold.
- **To reject a second call:**
 - Press  to reject the second call.

Once you have answered the second call, you can toggle between the calls by placing one call on hold and speaking to the other call (see Section 23.11.4 on page 374).

23.4 Ending a Call

To end call, you can do one of the following:

- Press .
- Place the handset on the charger.

When you end the call, the screen displays “Released”.

23.5 Adjusting Earpiece and Speakerphone Volume during a Call

During a call, you can adjust the volume of the handset earpiece and hands-free. There are five volume levels provided on the handset. This is done during an ongoing call.

- **To adjust the earpiece and hands-free volume:**
 - During a call, press the up / down  navigation keys to increase or decrease the volume level respectively. The screen displays the current volume setting.



Notes:

- When you end the call, the selected volume applies to all future calls, until it is modified again.
- To adjust the earpiece and speaker volume when the phone is in idle state, see Section 27.1 on page 389.

23.6 Muting a Call

You can talk to someone nearby without letting the caller hear you during a call. This is done by muting the microphone of the handset.

- **To mute and un-mute a call:**
 1. To mute the call:
 - a. During a call, press the **Menu** softkey.

23.8.2 Deleting a Number from the Redial List

You can delete a number from the Redial List.

➤ **To delete an entry in the Redial List:**

1. Press the ▲ navigation key to access the Redial List.
2. Press the ▼ navigation keys to select the desired number, and then press the **Select** softkey.
3. Press the **Menu** softkey.
4. Press the ▼ navigation keys to choose the **Delete** option, and then press the **Select** softkey; the "Delete Confirm" message is displayed.
5. Press the **OK** softkey to confirm deletion.

23.8.3 Deleting the Entire Redial List

You can delete all the entries in the Redial List.

➤ **To delete all entries in the Redial List:**

1. Press the ▲ navigation key to access the Redial List.
2. Press the **Select** softkey
3. Press the **Menu** softkey.
4. Press the ▼ navigation keys to choose the **Delete All** option, and then press the **Select** softkey; the "Delete Confirm" message is displayed.
5. Press the **OK** softkey to confirm deletion.

23.9 Locking the Keypad

You can lock the keypad to prevent accidental presses on the handset while carrying it around. This can be done only when the handset is in idle mode.

➤ **To lock the keypad:**

1. To lock the keypad: In idle mode, press and hold the # key; the 📞 icon is displayed.
2. To unlock the keypad: In idle mode, press and hold the # key, the 📞 icon disappears.



Note: You are unable to make any calls when the keypad is locked.

23.10 Paging the Handset

You can locate the handset by paging the handset from the base.

➤ **To page a handset:**

- On the base unit, press the **DECT** button until the LED changes to orange; all handsets registered to the base ring up to 60 seconds and "Incoming Call – HS Locator" is displayed on the LCD. You can stop the paging by pressing any key on the handset except the **Silent** softkey.

23.11 Call Handling for Multiple, Registered Handsets

The MP252 supports multiple, registered handsets. This section describes call handling between multiple registered handsets. This includes how to make internal calls, transfer external calls from one handset to another handset, and make conference calls.


23.11.1 Calling (Intercom) Another Handset

An intercom call is a call from one handset to another handset that is also registered to the MP252 base unit.



Note: An intercom call can only involve two handsets that share the same base unit.

➤ To call (intercom) another handset:

1. Press the ◀ navigation key; the screen displays a list of the registered handsets.
2. Press the ▲ navigation keys to select the handset to which you want to make a call.
3. Press the **Select** softkey; the called handset rings.
4. On the called handset, press  to establish the internal call.



23.11.2 Transferring an External Call to Another Handset

You can transfer an external call (i.e., not a call from another handset) received on one handset, to another handset.

23.11.2.1 Announced Call Transfer

An announced call transfer is when you can speak to the handset to where you want to transfer the external call before transferring the call.



➤ To make an announced call transfer:

1. During the call with the external call, press the ◀ navigation key; the screen displays a list of the registered handsets.
2. Press the ▲ navigation keys to select the handset to where you want to transfer the call.
3. Press the **Select** softkey; the external call is automatically put on hold and the called handset rings.
4. On the called handset, press  or  to establish an internal call between the handsets.
5. On the calling handset, press the **Menu** softkey, and then choose the **Transfer** option; the external call is transferred to the called handset and the current call with the calling handset is terminated.

23.11.2.2 Unannounced Call Transfer

An unannounced call transfer is when you transfer the external call to a handset without speaking to the handset to where the call is transferred.

➤ **To make an unannounced call transfer:**

1. During the call with the external call, press the ◀ navigation key; the screen displays a list of the registered handsets.
2. Press the ▲ navigation keys to select the handset to where you want to transfer the call.
3. Press the **Select** softkey; the external call is automatically put on hold and the called handset rings.
4. On the calling handset, press the **Menu** softkey, and then choose the **Transfer** option; the external call is transferred to the called handset and the current call with the calling handset is terminated.
5. On the called handset, press  or  to receive the transferred call.

23.11.3 Transferring an External Call to Another External Call

If you have two external calls, one an active call and the other a waiting call (or call on hold), you can transfer the active call to the waiting call party.

➤ **To transfer an external call to a remote party:**

1. Press the **Menu** softkey, and then select the **Transfer** option
2. Press the **OK** softkey to confirm the transfer; the two external call parties are connected, and you are disconnected from the calls.

23.11.4 Toggling between External and Internal Calls

If you have established an external call, you can establish another call (i.e., internal or external) and then toggle between these calls. When one call is active, the other call is on hold.

➤ **To toggle between calls:**

- Press the ▶ navigation key; the currently active call is put on hold and the currently held party is now active.

23.11.5 Three-Way Conference Calls



You can create three-way conference calls composed of the following call party types:

- Two handsets and an external party
- Your handset and two external calls

23.11.5.1 Making a Three-Way Conference Call with Another Handset and an External Party

The conference call feature allows one external call to be shared with two handsets (in intercom). The three parties can share the conversation and no network subscription is required.

➤ **To make a three-way conference with another handset and an external call:**

1. During the call with the external call, press the ◀ navigation key; the screen displays a list of the registered handsets.
2. Press the ▲ navigation keys to select the handset with which you want to establish a three-way conference call.
3. Press the **Select** softkey; the external call is automatically put on hold and the called handset rings.
4. On the called handset, press  or  to establish the internal call.
5. On the calling handset, press and hold the ◀ navigation key for 3 seconds to establish the 3-way conference call.



Note: If any handset hangs up during the conference call, the other handset still remains connected with the external call.

23.11.5.2 Making a Three-Way Conference Call with your Handset and two External Calls

You can make a three-way conference call between your handset and two external calls. This can be done when you have two external calls, where you are talking with one and the other call is waiting (on hold).

➤ **To make a three-way conference with two external calls:**

1. Press the **Menu** softkey, and then choose the **Conference** option.
2. Press the **OK** softkey to confirm the conference; the two external calls parties are included in your conference call.





24 Phonebook

Your handset can store up to 150 phonebook contacts. Each phonebook contact can have a name of up to 12 characters long and a phone number of up to 24 digits.

24.1 Adding a New Contact

Follow the procedure below for adding a new contact to your phonebook.

➤ **To add a new contact to a phonebook:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Phonebook**  icon.
3. Press the **Select** softkey to access the Phonebook.
4. Press the  navigation keys to choose the **Add** option, and then press the **Select** softkey.
5. Enter the contact details, using the  navigation keys to move from one field to the next:
 - **F. Name:** first name
 - **Name:** family name
 - **Number:** phone number



Note: The name and phone number are mandatory fields.

6. Press the **OK** softkey to save the phonebook entry.








Note: The phonebook displays the contacts in alphabetical order.

24.2 Editing a Contact

You can edit contacts listed in your phonebook.



➤ To edit a phonebook contact:

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Phonebook**  icon.
3. Press the **Select** softkey to access the Phonebook.
4. Press the  navigation keys to choose the **Edit** option, and then press the **Select** softkey.
5. Press the  navigation keys to choose the contact that you want to edit, and then press the **Select** softkey; the contact's details are displayed.
6. Press the **Select** softkey to edit the contact's details.
7. Press the  navigation keys to move between fields, and then edit the fields as required.
8. When you have completed your modification, ensure that you are in the melody field, and then press the **OK** softkey; the "Saved" message is displayed.




24.3 Viewing Contacts

You can view a list of all contacts in your phonebook.

➤ To view all contacts in your phonebook:

1. In idle state, press the **PB** softkey; the phonebook opens, displaying a list of the contacts.
2. Search a contact, by performing one of the following:
 - **Navigation keys:** Scroll through the list of contacts using the  navigation keys.
 - **Search feature:** Using the keypad, enter the name of the contact. As you enter letters, the phonebook locates contacts that match the entered letters. For example, if you want to search for the contact "Sue", as you press the key for the es letter ("s"), the phonebook locates contacts whose names begin with this string. As you enter the next letter (i.e., "u"), so the contacts whose names begin with "su" appear, and so on.
3. To view the details of a contact, press the  navigation keys to select the contact, and then press the **Select** softkey.





You can also view the list of phonebook contacts from the Menu list:

4. In idle state, press the **Menu** softkey.
5. Press the  navigation keys to scroll to the **Phonebook**  icon.
6. Press the **Select** softkey to access the Phonebook.
7. Press the  navigation keys to choose the **View** option, and then press the **Select** softkey.
8. Follow steps 2 through 3 of the procedure above.

24.4 Deleting a Contact

You can delete a selected contact in the phonebook.




➤ **To delete a contact in the phonebook:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Phonebook**  icon.
3. Press the **Select** softkey to access the Phonebook.
4. Press the  navigation keys to choose the **Delete** option, and then press the **Select** softkey.
5. Press the  navigation keys to choose the contact that you want to delete, and then press the **Select** softkey; the contact's details are displayed.
6. Press the **Select** softkey; the "Delete Confirm" message is displayed.
7. Press the **OK** softkey to confirm deletion (or the **Back** softkey to cancel); the contact is removed from the phonebook.

24.5 Deleting All Contacts

You can delete all contacts from the phonebook.

➤ **To delete all contacts from the phonebook:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Phonebook**  icon.
3. Press the **Select** softkey to access the Phonebook.
4. Press the  navigation keys to choose the **Delete All** option, and then press the **Select** softkey; the "Delete Confirm" message is displayed
5. Press the **OK** softkey to confirm deletion (or the **Back** softkey to cancel); all contacts are removed from the phonebook.

25 Call List

If you have subscribed to a Caller Line Identification (also referred to as Caller ID) service with your network service provider, then when your phone rings for an incoming call, the phone displays the calling number (and the associated name of the caller if listed in your phonebook). If the caller's number is withheld, "Withheld" is displayed. If the caller's number is unavailable, "Out Of Area" is displayed.


The phone's Call List stores up to 100 answered and unanswered (missed) calls, displaying the date and time of the calls.

25.1 Viewing the Call List

All unanswered (missed) and answered (received) calls are saved in the Call List with the latest call displayed at the top of the list. When the Call List is full, the oldest call is replaced by a new call.

Missed calls are marked with an asterisk (*) at the beginning of the missed call entry. Once the missed call has been read, the * is removed.






You can view the Call List by performing one of the following:

- In the idle state, press the ▼ navigation key.
or
- Using the Menu:
 1. In idle state, press the **Menu** softkey.
 2. Press the ◀▶ navigation keys to scroll to the **Call List**  icon, and then press the **Select** softkey to access the Call List.
 3. Press the ▲▼ navigation keys to choose one of the following options:
 - ◆ **Call List:** displays recently answered and missed calls
 - ◆ **Missed Calls:** displays only unanswered calls
 - ◆ **Received Calls:** displays only answered calls
 - ◆ **Redial List:** displays calls that were previously dialed
 4. Press the **Select** softkey to access the selected option; the call details—call duration and date and time of the call—are displayed.

25.2 Saving a Call List Number to the Phonebook

You can save a number in the Call List to your phonebook.




➤ **To save a Call List entry to the phonebook:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Call List**  icon.
3. Press the **Select** softkey to access the Call List.
4. Press the  navigation keys to choose the required Call List option (see previous Section)
5. Press the  navigation keys to choose the entry that you want to add to the phonebook, and then press the **Select** softkey.
6. Press the **Menu** softkey.
7. Press the  navigation keys to choose the **Add to PB** option, and then press the **Select** softkey; the phonebook is accessed, prompting you to enter the contact's details (the phone number as appearing in the Call List is automatically entered in the phonebooks Number field). For a description on adding contacts to the phonebook, see Section 24.1 on page 377.

25.3 Dialing a Call List Number

You can dial a number listed in the Call List.




➤ **To dial a number listed in the Call List:**

1. Access the Call List menu (see Section 25.1 on page 381).
2. Press the  navigation keys to choose the required Call List option (e.g., Missed Calls), and then press the **Select** softkey.
3. Press the  navigation keys to choose the entry that you want to dial, and then press the **Select** softkey.
4. Press  to dial the number.

25.4 Deleting a Call List Number

You can delete an entry in the Call List.



➤ **To delete a number in the Call List:**

1. Access the Call List menu (see Section 25.1 on page 381).
2. Press the  navigation keys to choose the required Call List option (e.g., Missed Calls), and then press the **Select** softkey.
3. Press the  navigation keys to choose the entry that you want to delete, and then press the **Select** softkey.
4. Press the **Menu** softkey.
5. Press the  navigation keys to choose the **Delete** option, and then press the **Select** softkey; the “Delete Confirm” message is displayed
6. Press the **OK** softkey to confirm deletion (or the **Back** softkey to cancel); the entry is removed from the Call List.

25.5 Deleting the Entire Call List

You can delete all entries listed in the Call List. When you delete all entries, all entries in the Call List, Missed Calls, Received Calls, and Redial List groups are deleted. If you access the Call List after deleting all entries, the "List Empty" message is displayed.

➤ **To delete a number in the Call List:**

1. Access the Call List menu (see Section 25.1 on page 381).
2. Press the  navigation keys to choose the required Call List option (e.g., Missed Calls), and then press the **Select** softkey.
3. Press the **Select** softkey once again.
4. Press the **Menu** softkey.
5. Press the  navigation keys to choose the **Delete All** option, and then press the **Select** softkey; the "Delete Confirm" message is displayed.
6. Press the **OK** softkey to confirm deletion (or the **Back** softkey to cancel); all entries are removed from the Call List.

26 Clock and Alarm

You can set the phone's date and time as well as set an alarm.






26.1 Date and Time

You can set the phone's date and time as well as determine the format of the date and time.

26.1.1 Changing the Date Format

You can change the date format. This can be either DD-MM-YYYY (for example, 25-12-2011) or MM-DD-YYYY (for example, 12-25-2011).






➤ **To change the date format:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Date & Time** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Date Format** option, and then press the **Select** softkey.
5. Press the  navigation keys to choose the desired format, and then press the **Select** softkey; the new date format is applied and the "Saved" message is displayed.

26.1.2 Changing the Time Format

You can change the time format. This can be either 12-hour format (for example, 5:30 PM) or 24-hour format (for example, 17:30).

➤ **To change the time format:**








1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Date & Time** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Time Format** option, and then press the **Select** softkey.
5. Press the  navigation keys to choose the desired format, and then press the **Select** softkey; the new time format is applied and the "Saved" message is displayed.

26.1.3 Setting the Time and Date

You can set the current time and date.

➤ **To set the time and date:**

1. In idle state, press the **Menu** softkey.

2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Set Date/Time** option, and then press the **Select** softkey.
4. Press the  navigation keys to access the time or date area.
5. To set the time:
 - To move between hours, minutes and AM/PM (depending on format), use the  navigation keys.
 - If the selected format is 12 hours (see Section 26.1.2 on page 385), then to select AM or PM, use the  navigation keys.
6. To set the date, use the  navigation keys to move between day, month and year. Set the date according to the format that you selected in Section 26.1.2 on page 385.






Note: If you enter an invalid value, an error tone is emitted and the cursor flashes on the incorrect entry.

7. Press the **OK** softkey to save the new date and time.


26.2 Alarm

Your phone provides a built-in alarm clock. You can select the melody to play when the alarm time is reached. You can also activate the snooze time so that when the alarm rings, you can stop it temporarily and the alarm will sound again at the end of the snooze period (i.e., two minutes).


When an alarm is set, the alarm  icon appears on the screen. When the alarm time is reached, the alarm  and **Alarm/Clock**  icons flash on the screen, and the alarm melody plays for 45 seconds.










Notes:

- When the alarm sounds, you can stop it or snooze it even if the handset keypad is locked (described in Section 23.9 on page 372).
- The alarm volume level is the same as the settings of the handset ringer volume (see Section 23.5 on page 370). If the handset ringer is set to Volume Off, the alarm still sounds at Volume 1 level.
- During an external or internal call, if an alarm is set and the alarm time is reached, the alarm  icon and "Alarm On" flashes on the screen and the current call display details (i.e., call duration etc.) disappear. Once you press any key to activate the snooze or press the **Off** softkey to disable the alarm, the current call details is displayed again on the screen.
- If the phone rings for an incoming call and the alarm time is reached, the alarm does not sound. However, if the snooze alarm is enabled, the alarm sounds again at the end of the snooze period provided that the phone is not ringing or in paging mode at the end of the snooze period.

26.2.1 Setting the Alarm

The alarm time is set as described below. When the alarm is set, the alarm  icon is displayed on the main screen.






➤ **To set the alarm:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Alarm** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Alarm On** option, and then press the **Select** softkey.
5. Press the  navigation keys to move between hours, minutes, and AM/PM. If the time format is 12 hours (see Section 26.1.2 on page 385), then to select AM or PM, use the  navigation keys.
6. Press the **OK** softkey.
7. Press the  navigation keys to choose whether you want the snooze functionality (**Snooze On**), and then press the **Select** softkey; the alarm time is saved and the alarm icon is displayed on the main screen.

26.2.2 Defining the Alarm Melody

You can define the melody that is played when the alarm sounds.





➤ To set the alarm melody:

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Alarm** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Alarm Melody** option, and then press the **Select** softkey; a list of melodies is displayed.
5. Press the  navigation keys to choose the required melody (a sample of the melody is played when you highlight a melody), and then press the **Select** softkey; the melody is applied to the alarm and the "Saved" message is displayed.

26.2.3 Disabling the Alarm





You can set the alarm to off so that it does not ring at all.

➤ To set the alarm to off:

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Clock/Alarm**  icon, and then press the **Select** softkey to access the menu.
3. Press the  navigation keys to choose the **Alarm** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Alarm Off** option, and then press the **Select** softkey.

26.2.4 Switching Off or Snoozing the Alarm

When the alarm rings, you can either switch it off entirely or you can snooze the alarm so that it switches off temporarily and then rings again after two minutes.

- To switch off the alarm when it rings, press the **Off** softkey or  key; the alarm  icon disappears from the main screen.
- To activate the snooze alarm when it rings, press the **Snooze** softkey or any other key except the **Off** softkey or  key; the alarm  icon remains displayed in the main screen.






27 Customizing the Handset

Your phone comes with a selection of settings that you can change to personalize your handset.

27.1 Adjusting Speaker and Earpiece Volume

You can adjust the speaker volume as well as the earpiece volume. The phone supports five volume levels from which you can choose.

➤ **To adjust the volume:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Audio Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Speaker Volume** or **Ear Volume** option to adjust the speaker or earpiece volume respectively, and then press the **Select** softkey.
5. Press the  navigation keys to select the volume level.
6. Press the **OK** softkey; the volume level is saved.








Note: You can also adjust the volume during a call, as described in Section 23.5 on page 370.

27.2 Ring Settings

27.2.1 Choosing the Internal Ringer Melody

You can select the ringer melody that is played when an incoming call is received from another handset registered to the MP252 base.






➤ **To select the internal ringer melody:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Ring Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Internal Ringer** option (a sample of the melody is played when browsing the list), and then press the **Select** softkey; a list of melodies is displayed.
5. Press the  navigation keys to choose the desired melody, and then press the **Select** softkey; the melody is saved.

27.2.2 Choosing the External Ringer Melody

You can select the ringer melody that is played when an incoming call is received from an external party.












➤ **To select the external ringer melody:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Ring Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **External Ringer** option (a sample of the melody is played when browsing the list), and then press the **Select** softkey; a list of melodies is displayed.
5. Press the  navigation keys to choose the desired melody, and then press the **Select** softkey; the melody is saved.

27.2.3 Adjusting the Ringer Volume

You can adjust the handset's ringer volume.

➤ **To adjust the ringer volume:**





1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Ring Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Ring Volume** option, and then press the **Select** softkey; a volume bar is displayed indicating the volume level.
5. To increase the volume, press the  or  navigation keys; to decrease the volume, press the  or  navigation keys. Levels filled in with color indicate the selected volume level. The respective volume level is played during your selection.
6. To silence the ringer, press the  or  navigation keys until "Volume Off" is displayed. when the ringer is off, the  icon is displayed on the main screen.
7. Press the **OK** softkey to save your settings.


27.3 Alert Tones

27.3.1 Setting the Key Tone

A single beep is emitted when you press a key on the handset. You can set whether only a beep is emitted upon any key pressed or only Dual Tone Multi Frequencies (DTMF) tones are emitted (when numbers 0-9 and symbols * and # are pressed), or both. You can also turn off the key tone.

➤ **To set the key tone:**





1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Tone Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **Key Tone** option, and then press the **Select** softkey.

5. Press the  navigation keys to choose the required key tone:
 - **Beep:** a beep is emitted when any key is pressed
 - **DTMF:** only DTMF tones are emitted (and this occurs only when pressing the digit keys - numbers 0-9 and the symbols * and #)
 - **Beep and DTMF:** beep and DTMF are activated
 - **Off:** no tone is emitted
6. Press the **Select** softkey to save your settings.

27.3.2 Setting the Battery Low Tone

You can turn on the alert tone when low battery and out of range are detected.





➤ **To set the key tone:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Tone Setup** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the **On** or **Off** option to switch on or off the low battery alert tone respectively, and then press the **Select** softkey.

27.4 Setting the Display Language

The handset can be displayed in either English, Spanish, or Hebrew.



➤ **To set the display language:**



1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Language** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the desired language, and then press the **Select** softkey; the saved message appears in the language selected and the display is changed accordingly.

27.5 Selecting a Wallpaper

You can set a wallpaper image that is displayed in the background on the main screen.

➤ **To select a wallpaper:**





1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.

3. Press the  navigation keys to choose the **Wallpaper** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the desired wallpaper. Each time you press the key, the wallpaper is displayed in the background.
5. Press the **Select** softkey to apply the wallpaper.

27.6 Setting the Contrast Level

You can set the contrast level to suit your screen visibility.





➤ **To set the contrast level:**

1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Contrast** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the desired contrast level. As you browse through the level options, the contrast is displayed accordingly.
5. Press the **Select** softkey to save your settings.

27.7 Activating or Deactivating Automatic Answer

Auto Answer allows you to answer an incoming call by simply picking up the handset from the charging cradle/base. When this function is activated, you do not need to press a key to answer the call.



➤ **To activate or deactivate Auto Answer feature:**



1. In idle state, press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Auto Answer** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose whether you want to activate Auto Answer (**On** option) or deactivate it (**Off** option).
5. Press the **Select** softkey to save your settings.

27.8 Selecting a Base Station

Your handset can only operate with one base unit. If your handset is registered to more than one base unit, you can select the base unit to use.

➤ **To select a base for the handset:**

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.

3. Press the  navigation keys to choose the **Select Base** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the desired base unit, and then press the **Select** softkey; if the selected base is successfully found, "Saved!" is displayed; otherwise, "Fail" is displayed.






Note: The currently used base is displayed with an asterisk "**".

27.9 Resetting Handset to Factory Defaults

You can reset your handset settings to default settings. When you reset the handset, all your settings related to the handset are deleted and restored to factory defaults, except your phonebook entries which remain unchanged.

➤ To reset the handset to factory defaults:

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **HS Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **HS Default** option, and then press the **Select** softkey; you are prompted to enter your PIN number.
4. Enter your 4-digit PIN number, and then press the **OK** softkey. (For defining the PIN number, see Section 28.2 on 397.)
5. Press the **OK** softkey again to confirm reset; if the PIN code is correct and the handset is restored to default, a confirmation tone is played and the screen returns to idle. If the PIN code is incorrect, "PIN Invalid" is displayed and you are unable to restore the handset to defaults.






28 Base Settings

28.1 Manage Handsets

28.1.1 Renaming the Handset

By default, your handset name is “DECT”. You can assign a different name to your handset. The handset name is displayed on the main screen in idle state.

➤ **To rename the handset:**

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Manage HS** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the handset that you want to rename, and then press the **Select** softkey.
5. Press the  navigation keys to choose the **Rename HS** option, and then press the **Select** softkey.
6. Using the alphanumerical keypad, enter the required name for the handset. Press the **Clear** softkey to delete characters to the left of the cursor or press and hold the **Clear** softkey to delete the whole character string.
7. Press the **OK** softkey to save the new name; the handset name is saved and “Saved” is displayed.



Note: The handset name can be up to 12 characters.







28.1.2 De-Registering a Handset

You can de-register a handset from the base unit. The antenna icon on the de-registered handset will be off. On certain handsets, you are prompted to enter the 4-digit PIN in order to de-register a handset from the base station.



Note: You cannot de-register the handset that you are currently using.




➤ To de-register a handset:

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Manage HS** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose the handset that you want to de-register, and then press the **Select** softkey.
5. Press the  navigation keys to choose the **Delete HS** option, and then press the **Select** softkey; the “Delete Confirm” message is displayed.
6. Press the **OK** softkey to confirm; the handset is de-registered and “HS Deleted” is displayed.
7. Press the  navigation keys to choose whether to enable (**Intercept ON**) or disable (**Intercept OFF**) call interception, and then press the **Select** softkey; the “Saved” message is displayed.

28.2 Changing the PIN Number

A four-digit personal identification number (PIN) number is required for changing various settings of the base unit. The PIN number is used to protect your phone against unauthorized use. The default system PIN number is 0000.

➤ **To change the PIN number:**

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Modify PIN** option, and then press the **Select** softkey.
4. In the **Old PIN** field, enter the current PIN number, and then press the **OK** softkey.
5. In the **New PIN** field, enter a new four-digit PIN number, and then press the **OK** softkey.
6. In the **Confirm** field, enter the new PIN number again, and then press the **OK** softkey; the new PIN number is saved and “Saved” is displayed.






Note: If the old PIN code is incorrect, “Old PIN Invalid” is displayed and you are returned to the **Modify PIN** option.

28.3 Resetting the Base to Factory Defaults

You can reset your base settings to default settings. When you reset the base, all your settings related to the base are deleted and restored to factory defaults, except your phonebook entries which remain unchanged.

➤ **To reset the base to factory defaults:**





1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **BS Default** option, and then press the **Select** softkey; you are prompted to enter your PIN number.
4. For certain phones you may be prompted to enter your four-digit PIN number, and then press the **OK** softkey. (For defining the PIN number, see Section 28.2 on 397.)
5. Press the **OK** softkey again to confirm reset; if the PIN code is correct and the base is restored to default, a confirmation tone is played and “Reset” is displayed. If the PIN code is incorrect, “PIN Invalid” is displayed and you are unable to restore the base to defaults.

28.4 Viewing the Product Version

You can view the firmware, hardware, and EEPROM version of your phone.

➤ **To view the product version:**

1. Press the **Menu** softkey.





2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Product Version** option, and then press the **Select** softkey.
4. Press the  navigation keys and then press the **Select** softkey to choose the option whose version you want to view:
 - **Firmware**: displays the firmware currently running on the phone
 - **Hardware**: displays the hardware version of the phone
 - **EEPROM**: displays the version of the non-volatile memory
5. Once the version of a particular option is displayed, press the **Select** softkey to return to the previous screen to choose a different option, as listed in Step 4.

28.5 Activating Nemo Mode



Note: This function will not be supported in future release.

➤ To activate Nemo mode:

1. Press the **Menu** softkey.
2. Press the  navigation keys to scroll to the **Base Settings**  icon, and then press the **Select** softkey.
3. Press the  navigation keys to choose the **Nemo Mode** option, and then press the **Select** softkey.
4. Press the  navigation keys to choose whether you want to enable Nemo (**Nemo ON**) or disable Nemo (**Nemo OFF**), and then press the **Select** softkey; the “Saved” message is displayed.

29 Factory Defaults

The table below lists the factory defaults of various settings:

Table 29-1: Factory Defaults


Feature	Default
Handset Settings	
External Ring	Melody 15
Internal Ring	Melody 10
Handset Ring Volume	Volume 3
Earpiece Volume	Volume 3
Speaker Volume	Volume 3
Key Tone	Beep and DTMF
Battery Tone	On
Language	English
Ringer Off	Off
Wallpaper	Wallpaper 1
Contrast	Level 3
Keypad Locked	Off
Auto Answer	On
Alarm	Off
Base Settings	
Date	01-01-2008
Time	00:00
System PIN for HS/BS	0000

Reader's Notes

30 Troubleshooting

If you have difficulty with your phone, please try the suggestions listed below:

Table 30-1: Troubleshooting

Problem	Possible Cause	Solution
No Dialing Tone when  Pressed	<ol style="list-style-type: none"> 1 The connection cord of the base unit is not plugged in. 2 The adapter cord is not plugged in correctly in the base unit. 3 The line is busy, as another handset is used. 4 Wrong connection cord (no Euro AS). 	<ol style="list-style-type: none"> 1 Check the connections. Unplug and plug back in the mains. Check that the telephone line cord has been plugged into the base unit and the phone socket. 2 Check the base unit plug and the 220V plug (remove and plug-in). 3 Wait until the line is unoccupied. 4 Use the original connection cord.
When Connected to PBX, No Connection and/or Wrong Connection After Dialing	Dialing prefix is required.	Insert the dialing prefix
Phone Displays "Searching"	<ol style="list-style-type: none"> 1 Base unit out of range. 2 Base unit not connected to mains. 	<ol style="list-style-type: none"> 1 Reduce the range between the handset and base. 2 Connect base unit to mains.
Unable to Make Calls	Service not activated or wrong operator or wrong setting	Check your subscription with network or change the dial mode.
No Display	Empty battery	Recharge battery.
No Conference Call	Incorrect or no configuration for conference call feature	Ensure that 3 Way Conference is configured in the Web interface (Voice Over IP > Services tab).

Reader's Notes

A Specifications



Note: For the list of features available in the current software version, refer to the latest *Release Notes*.

A.1 Gateway Specifications

The specifications for the router and VoIP functionality are listed in the table below:

Table A-1: MP252 Router and VoIP Software Specifications

Feature	Details
ADSL Interface	<ul style="list-style-type: none"> ▪ RJ-11 ADSL Jack ▪ ITU G.992.1 (G.dmt) – ADSL ▪ ITU G.992.3 (G.dmt.bis) – ADSL2 ▪ ITU G.992.5 – ADSL2+ ▪ Automatic PVC scanning ▪ Multiple PVCs ▪ Annex B (ADSL over ISDN) support available on a separate P/N ▪ PPPoE-over-ETHoA or IP-over-ETHoA
Ethernet Interface	<ul style="list-style-type: none"> ▪ 4 ports RJ-45, 10/100Mbps, MDI/MDIX Auto-Sensing ▪ Port 4 can be configured as Ethernet WAN ▪ IEEE 802.3, IEEE 802.3u ▪ Wire-speed L2 switching between LAN ports
Wireless LAN	<ul style="list-style-type: none"> ▪ Wireless LAN - 802.11b/g/n Wireless Access Point, 2.4 GHz ▪ 2x2 MIMO internal antennas ▪ Wireless Security: <ul style="list-style-type: none"> ✓ WPA ✓ WPA2 ✓ WPA/WEP Mixed Mode ✓ TKIP Encryption ▪ MAC Filtering ▪ Virtual AP – Up to 4 SSIDs
USB Interface	<ul style="list-style-type: none"> ▪ USB 2.0 Host Interface ▪ Provides up to 1A current ▪ Network file server access to USB storage device: <ul style="list-style-type: none"> ✓ NTFS and FAT32 support ✓ Windows networking and file sharing ✓ WINS server ▪ Network printer access to USB printers: <ul style="list-style-type: none"> ✓ Support for most Linux-compatible printers ✓ LPD and Microsoft Shared Printers support

Feature	Details
FXS (Phone) Interface	<ul style="list-style-type: none"> ▪ 2 RJ-11 Loop-start FXS Ports ▪ Configurable regional settings (impedance coefficients) ▪ Up to 5 REN / 0.5km load support (default set to 3 REN)
VoIP Signaling Protocols	<ul style="list-style-type: none"> ▪ SIP - RFC 3261, RFC 2327 (SDP)
Data Protocols	<ul style="list-style-type: none"> ▪ IPv4, TCP, UDP, ICMP, ARP ▪ PPPoE (RFC 2516) ▪ L2TP (RFC 2661) ▪ PPTP (RFC 2637) ▪ DNS, Dynamic DNS ▪ WAN-to-LAN Layer-3 routing with: <ul style="list-style-type: none"> ✓ DHCP Client/Server (RFC 2132) ✓ NAT: RFC 3022, Application Layer Gateway (ALG) ✓ Stateful Packet Inspection Firewall ✓ QoS - Priority queues, VLAN 802.1p,Q tagging, traffic shaping
Media Processing	<ul style="list-style-type: none"> ▪ Voice Coders: G.711μ/a-law, G.729A/B, G.722 ▪ Echo Cancelation: G.168-2004 compliant, up to 64-msec tail length ▪ Silence Compression ▪ Adaptive Jitter Buffer 300 msec ▪ Fax bypass, Voice-Band Data and T.38 fax relay
Telephony Features	<ul style="list-style-type: none"> ▪ Call Hold and Transfer ▪ Two independent 3-Way Conferencing (one per line) ▪ Call Waiting ▪ Message Waiting Indication ▪ Call Forward ▪ Telephony Signaling: <ul style="list-style-type: none"> ✓ DTMF: Detection and Generation, TIA464B. In-band, RFC2833 or SIP-INFO relay ✓ Caller ID: Telcordia, ETSI, NTT - Type I, Telcordia Type II ✓ Configurable Call Progress Tones ✓ On/Off hook detection, Hook-flash detection
Configuration and Management	<ul style="list-style-type: none"> ▪ Embedded Web Server for configuration and management ▪ TR-069 and TR-104 for remote configuration and management ▪ Remote firmware upgrade and configuration by HTTP, TFTP, FTP, and HTTPS ▪ SIP-triggered remote firmware and configuration upgrade ▪ Command-Line Interface (CLI) over Telnet ▪ Dual image management ▪ SNMP
Packetization	<ul style="list-style-type: none"> ▪ RTP/RTCP Packetization (RFC 3550, RFC 3551) ▪ DTMF Relay (RFC 2833)
Security	<ul style="list-style-type: none"> ▪ HTTPS for Web-based configuration and for TR-069 ▪ Password-protected Web pages (MD5) ▪ Configuration file encryption (3DES)

Feature	Details
	<ul style="list-style-type: none"><li data-bbox="552 264 762 293">▪ SIP over TLS<li data-bbox="552 300 1018 329">▪ State-full Packet Inspection firewall
Physical	
Environmental	<ul style="list-style-type: none"><li data-bbox="552 392 1018 421">▪ Operating Temperature: 0 to 45°C<li data-bbox="552 427 1018 456">▪ Storage Temperature: -25 to 80°C
Power	Power +12 VDC, 2A External Power Adaptor, 100-240 VAC/50-60 Hz
Battery Backup	Optional battery backup for up to 4 hours idle/30 min. talk time (FXS)
Weight and Dimensions	170 x 225 x 35mm, 300g

A.2 DECT (Only for MP252WDNB)

The specifications of the DECT phone are listed in the table below:

Table A-2: MP252WDNB DECT Phone Specifications

Feature	Details
Standard	DECT, GAP and CAT-iq 1.0 certified (functional according to CAT-iq2) Software upgradable to comply with future CAT-iq versions
Number of Channels	10
Frequency	1.88 GHz to 1.90 GHz for EU DECT 1.92 GHz to 1.93 GHz for US DECT
Operating Range	Up to 300 meters outdoors Up to 50 meters indoors
Operating Time	Standby: 100 hrs approx. Talking: 10 hrs approx.
Battery Charging Time	16 hrs approx.
Number of Handsets	Up to 5 registered DECT handsets per MP252
Handset Dimensions	46.6 x 29 x 156 mm (W x D x H)
Handset Weight	119.1 g (with battery)
Handset Design	optional DECT handset design
Battery Information	
Battery Type	NiMH (rechargeable battery) AAA size
Rating	600 mAh 1.2V

Reader's Notes

User's Manual

MP252 Multimedia Home Gateway

Version 3.4.0



www.audiocodes.com