mck communications

Quality is our job. Customer satisfaction is our mission!

PBXgateway™ & EXTender™ 6000

System Administrator's Guide

M-6000-MUM Rev AC

March 13, 20056

Printed in USA **November 2004**

Notice
Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Your Responsibility for Your System's Security
Toll fraud is the use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system and, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your system manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The system manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Citel Technologies does not warrant that this product is immune from or will prevent unauthorized use of common-carrier telecommunication services or facilities accessed through or connected to it. Citel Technologies will not be responsible for any charges that result from such unauthorized use.

DECLARATION OF CONFORMITY

We CITEL
declare under our sole responsibility that the product:

PBXgateway

Consisting of Models E-6000G-Syy0841 and E-6000G-Syy1241

to which this declaration relates, is in conformity with the following standards:

EN 55022	1998	+ Amendments A1 + A2
EN 55024	1998	+ Amendments A1 + A2
EN 61000-3-2	2000	
EN 61000-3-3	1995	+ Amendment A1
EN 60950-1	2001	

As described in the European Directives:

89/336	(EMC)
73/23	(Safety)
93/68	(Safety)

The technical file is kept at: *CITEL Technologies*
4040 Bowness Road NW
Calgary, Alberta T3B 3R7
Canada

Calgary, 20 October 2005

Julian Sanders
Program and Validation Manager

Table of Contents

Regulatory – Compliance and Agency Approval

This equipment complies with or has obtained Regulatory Agency approval at least against the following standards:

EMC - Emission	FCC CFR 47 Part 15
	EN 55022 (1998) + Amendments A1 + A2
EMC - Immunity	EN 55024 (1998) + Amendments A1 + A2
Safety	EN 60950 (2000)
	UL 60950-1
	CSA C22.2 N° 60950-1

Compliance and Regulatory Statements

1. EN55022 and CISPR22 statement

This is a Class B product.

2. FCC Part 15 Statement

This digital equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Problems, Repair and Warranty
Should you experience trouble with this telephone equipment or for repair or warranty information, please contact Customer Support, at 1-888-454-5828. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect this equipment from the line network until the problem has been corrected.

3. **Industry Canada Statements**
   This digital equipment does not exceed Class B limits for radio noise emissions from digital apparatus, set out in Radio Interference Regulation of the Industry Canada. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

4. **Notice d'Industrie Canada**
   Cet équipement n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe B prescrites dans le Règlement sur le brouillage radioélectrique établi par l'Industrie Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions de radio et de télévision, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécessaires
   pour en éliminer les causes.

Making Changes or Modifications


Any changes and modifications not expressly approved by Citel Technologies. will void any Compliance and regulatory approval, and will void the user's authority to operate the equipment.

Lifeline or 911 Phone Notice

CAUTION: THIS IS NOT A LIFELINE or 911 PHONE.

If you dial 911 on your display telephone, when the telephone is connected to the Remote unit and linked to the PBXgateway, you will reach the 911 facility that serves the location of the corporate facility and **not** the location of your Remote unit. To ensure that you reach the correct 911 service for your area, use a telephone connected locally.
Note: Branch Office EXTender™ 6000 Remote units provide an analog port for local dialing.

Important Safety Instructions

The exclamation point in an equilateral triangle is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

To reduce the risk of fire, electrical shock, and injury to persons when installing telephone equipment, always follow basic safety precautions including:

- Read and understand all instructions.
- Follow all warnings and instructions marked on or packed with the product.
- Never install this unit, or the telephone wiring for it, during a lightning storm.
- Never install a telephone jack in a wet location unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone wiring has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Do not install this product near water, for example, in a wet basement location.
- Do not overload wall outlets, as this can result in the risk of fire or electrical shock.
- Do not attach the power supply cord to building surfaces. Do not allow anything to rest on the power cord. Do not locate this product where the cord will be abused by persons walking on it.
- Unplug the product from the wall outlet before cleaning. Use a damp cloth for cleaning. Do not use cleaners or aerosol cleaners.
- Do not operate the system if chemical gas leakage is suspected in the area. Use telephones located in some other safe area to report the trouble.

DO NOT open the PBXgateway or Branch Office units. There are no user serviceable parts inside. Only an authorized technician should open the unit for required maintenance or upgrading purposes.

Protection of the Environment – The WEEE Directive

This equipment is marked according to the European directive 2002/96/EC on Waste Electrical and Electronic Equipment (WEEE). By ensuring this product is disposed of correctly, you will help prevent potential negative consequences for the environment and human health, which could otherwise be caused by inappropriate waste handling of this product.

This symbol on this equipment indicates that this appliance may not be treated as household waste. Instead it shall be handed over to the applicable collection point for the recycling of Electrical and Electronic Equipment.
Disposal must be carried out in accordance with local environmental regulations for waste disposal.
For more detailed information about treatment, recovery and recycling of this product, please contact your local city office or your household waste disposal service.

Support Telephone Number	Call the MCK Communications Helpline (at 1-888-454-5828), or your authorized dealer if you need assistance when installing, programming, or using your system. Ask for customer service. Outside the United States or Canada, contact your local MCK Communications representative.

Security of Your System: Preventing Toll Fraud

As a customer of a new telephone system, you should be aware that there is an increasing problem of telephone toll fraud. Telephone toll fraud can occur in many forms, despite the concerted efforts of telephone companies and telephone equipment manufacturers to control it. Some individuals use electronic devices to prevent or falsify records of these calls. Others charge calls to someone else's number by illegally using lost or stolen calling cards, billing innocent parties, clipping on to someone else's line, or breaking into someone else's telephone equipment physically or electronically. In certain instances, unauthorized individuals make connections to the telephone network through the use of remote access features.

Common carriers are required by law to collect their tariff charges. While these charges are fraudulent charges made by persons with criminal intent, applicable tariffs state that the customer of record is responsible for payment of all long-distance or other network charges. Verso Technologies, Inc. cannot be responsible for such charges and will not make any allowance or give any credit for charges that result from unauthorized access.

To minimize the risk of unauthorized access to your Verso Technologies, Inc. PBXgateway, when possible, restrict the off-network capability of off-premises callers, using calling restrictions, Facility Restriction Levels, and Disallowed List capabilities. When possible, block out-of-hours calling through Time-of-Day Routing. Frequently monitor system call detail reports for quicker detection of any unauthorized or abnormal calling patterns.

Limit out-calling to persons on a need-to-have basis.
The Verso Technologies, Inc. PBXgateway, through proper administration, can help you reduce the risk of unauthorized persons gaining access to the network. However, telephone numbers and authorization codes can be compromised when overheard in a public location, lost through theft of a wallet or purse containing access information, or when treated carelessly (writing codes on a piece of paper and improperly discarding them).

Additionally, hackers may use a computer to dial an access code and then publish the information to other hackers. Substantial charges can accumulate quickly. It is your responsibility to take appropriate steps to implement the features properly, to evaluate and administer the various restriction levels, and to protect and carefully distribute access codes.

Under applicable tariffs, you will be responsible for payment of toll charges. Verso Technologies, Inc. cannot be responsible for such charges and will not make any allowance or give any credit resulting from unauthorized access.

About This Manual

Intended Audience

This manual is intended to help with the installation, configuration, and troubleshooting of the PBXgateway and compatible remote units. Additional information is provided for Remote products, which can be 'mixed & matched' to communicate with the PBXgateway depending on the clients' needs. This document is intended for use by anyone needing such information, including system administrators, support personnel, and technicians.

Terms and Conventions

The **PBX**gateway™ is a multi-user device and is henceforth referred to as the PBXgateway, Gateway or Switch unit.

The Remote products are henceforth referenced as follows:

The Branch Office **EXT**ender™ 6000 is multi-user device and is henceforth referred to as the EXTender 6000 or Branch Office unit.

The **EXT**ender™ 4000 is a single client device and is henceforth referred to as the EXTender 4000.

The Management Interface is henceforth referred to as the MI.

Product Overview

The following section provides a product overview for the PBXgateway including; a Product Feature List, Voice Compression vs. Bandwidth Requirements, Typical Installation Information, a Management Interface (MI) Overview, and Diagnostic Information.

Product Summary	The PBXgateway is a multi-user telephony device enabling remote teleworkers seamless connectivity and full functionality of the corporate Private Branch Exchange (PBX). The PBXgateway is referred as a "gateway " because it is the central receiving point for routing voice conversations from one or more locations to the PBX. Teleworkers, usually working from an off-site location, can place a call through the corporate PBX by simply dialing the number as if they were in the main office.
Single Users	Single remote users can connect their digital phones through the **EXT**ender™ 4000 for IP.
Multiple-Users	Remote offices with multiple users can be connected through one of the following devices: • **EXT**ender™ 6000, 8 & 12-user: You can use 2 EXTender 6000 8-user devices, or 2 EXTender 6000 12-user devices. The single-user devices are commonly referred to as a "Remote unit" and the multi-user devices are referred to as "Branch Office units".
Compatible Networks	The PBXgateway and Remote units are linked through a wide variety of network devices (TA, CSU/DSU) and network types (ISDN, IP)

Features

The PBXgateway has the following features:

- Support for a wide variety of network termination equipment
- Support for 8 or 12 remote users (
- Configuration via the internet (HTML Configuration)
- ConneX calling support
- Caller ID support
- Fax support on the 2nd B channel (DEFINITY and Meridian protocols)
- Setup Wizard for configuring the units
- ISDN and IP Call Suspend modes

Compatible Remote Units

The PBXgateway is compatible with the EXTender 4000 and 6000, with each unit having different network and user requirements. Complete installation and configuration information is provided with each remote unit in the form of a "Quick Installation Guide" (QIG). Please consult the QIG for information not contained in this document.

What is the EXTender™ 4000 for IP?

The EXTender 4000 provides remote voice access to a corporate PBX for a single remote user. Remote users can connect to the PBXgateway via a 10/100BaseT Ethernet connection using IP packet transmission. Remote users' phones will connect into the remote module via an RJ-45 phone jack, and their phone traffic will be placed in IP packets and sent out to the LAN via a 10/100BaseT Ethernet connection to the PBXgateway.

Types of Network Connections

The PBXgateway is designed to connect over a wide variety of third party network devices using three types of network connections:

- Synchronous-Serial connection (V.35, RS-530, RS-232)
- Asynchronous-Serial connection (RS-232)
- IP (10/100BaseT Ethernet)

Voice Transmission

At both the branch office and corporate sites, all voice and signaling information is placed into digital data packets, which are then sent out over the data network. This data is transmitted digitally over the connection as a series of “ones” and “zeroes”. The data packets are encapsulated within a MCK Proprietary protocol called Remote Voice Protocol™ (RVP)

The most important consideration for packetizing voice is defining when each character begins.

Synchronous vs. Asynchronous Transmission

One way to do this is by providing a clock signal. At a precise time, the transmission starts. This is called Synchronous (see page 14). In Asynchronous transmission, there is no clocking signal. The receiving terminal knows what’s what because each character begins with a start bit and ends with a stop bit (see page 15).

(VoIP)

The voice and signaling packets are sent using Internet Protocol (IP) over the packet-switched data networks as opposed to using the traditional circuit-switched protocols. Voice packets get delivered to the alternate device using the RVP. This protocol handles the timing and delivery of the packets (See page 16 for more information).

Connections vs. Remotes

Types of Connections		Remotes Supported		
Type	**Maximum # of Remotes per Gateway**	**Model(s)**	**Protocols**	**Connection Type**
RVP_Direct	2	6000	*RVP over HDLC	Serial WAN Ports
RVP_IP	2	6000	*RVP_over_IP	Ethernet (10 or 100 BaseT)
RVP_IP	1	4000	*RVP_over_IP	Ethernet (10 or 100 BaseT)

Table 1: Connections vs. Remotes

* Remote Voice Protocol™ (RVP), MCK Proprietary protocol.

Compatible Telephones

Nortel (Meridian and Norstar)	Avaya
Meridian M2006 ***** M2008 ***** M2216 M2250 M2317 M2616 M2616CT M3110 M3901 M3902 M3903 M3904 M3905 **Norstar** M7100 ***** M7208** M7310 M7324 M7410 ATA2 T7316 T7316E T7208** ** This digital display telephone is NOT recommended for administrative purposes.* *** Recommended if a set must be extended via the ConneX port.*	6402+ ***** 6408+ 6416D+ 6424D+ 8403 8410D 8411D 8410DR 8434DX CallMaster III CallMaster IV CallMaster V CallMaster VI Gray Market 9031DCP ** This digital display telephone is NOT recommended for administrative purposes.*
Toshiba	**Magix Digital Telephones**
DKT2004 DKT2010 DKT2020 **Compatible Voice System:** Toshiba Strata DK	4424LD+ 4424D+ 4412D+ 4406D+ 4400D DSS 4450 (add on module for 4424LD+ and 4424D+) 4400 **Compatible Voice System:** Avaya™ MERLIN MAGIX®
Alcatel	**Ericsson**
Reflexes 4023 Reflexes 4034 Reflexes 4035 Compatible Voice System: Alcatel 4400 Alcatel 4200	Dialog 3200 Dialog 3201 Dialog 3202 Dialog 3203 Dialog 3210 Dialog 3211 Dialog 3212 Dialog 3213 DBY 409 – Add on Module Key for Dialog 3213 Compatible Voice System: Ericsson MD 110

Compatible Telephones, continued

Panasonic DBS	Iwatsu
44210 44220 44223 44224 44225 44230 44233 Compatible Voice System: Panasonic DBS 576 Panasonic DBS 576 HD	IX-MKT IX-12KTD-2 IX-24KTD-2 IX-12KTD-3 IX-24KTD-3 Compatible Voice System: Iwatsu ADIX APS

Table 2: Compatible Phone Sets

Typical Installation

Typical Installation

The PBXgateway can be installed with a variety of different configurations depending on available bandwidth, the type of third-party termination equipment, and the type of EXTender installed at the remote location.

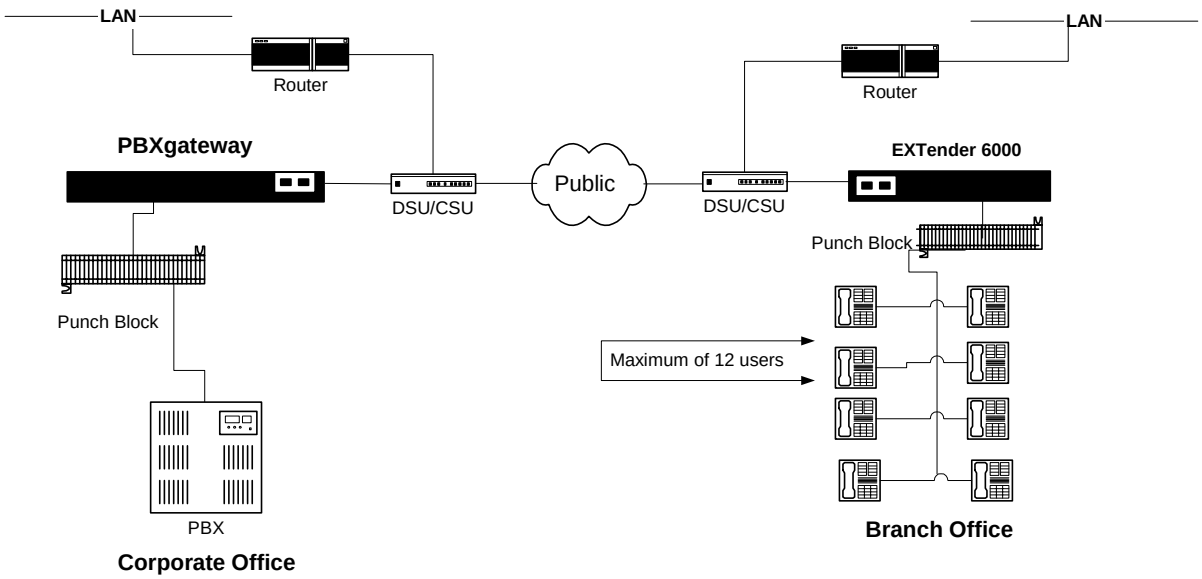


Figure 1: Synchronous (RVP_Direct) Installation

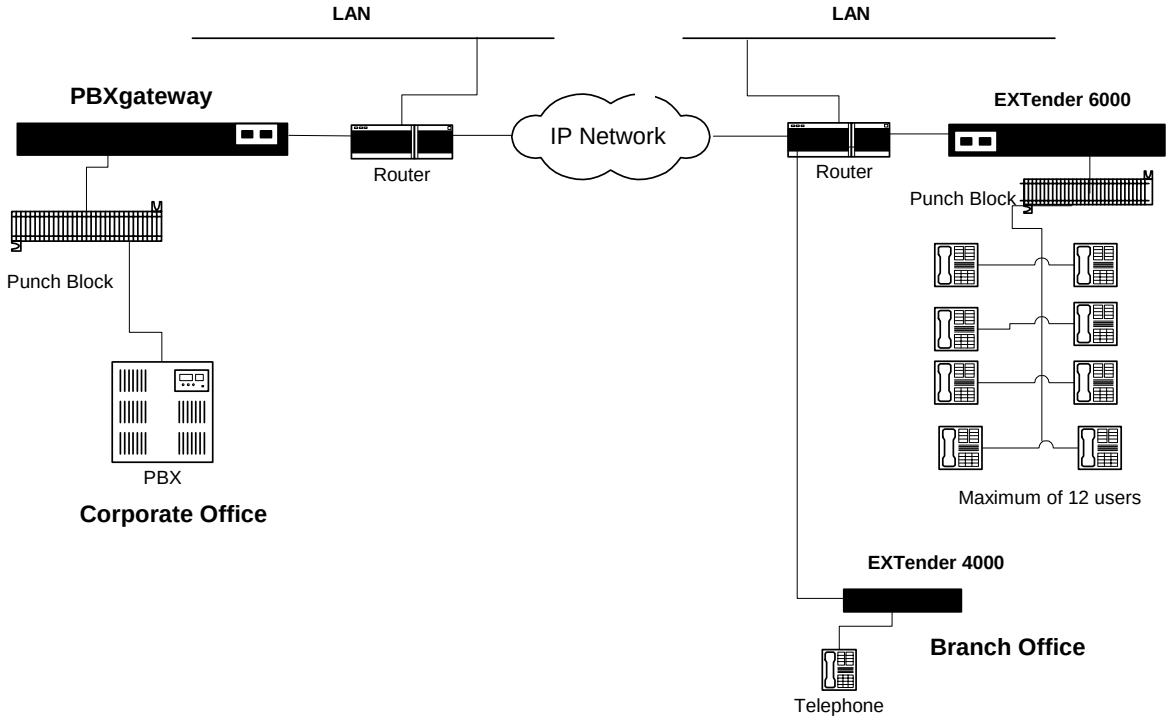


Figure 2: RVPoIP (RVP_IP) Installation

Synchronous-Serial Connection

Synchronous -Serial

A connection type utilizing the RVP protocol, encapsulated over HDLC, to send voice packets over the network (using traditional network devices: TA, CSU/DSU, FRAD) using a synchronous-serial bit stream via the WAN port of the unit. A synchronous connection relies on a master clock (an oscillator generated signal) to identify the starting point of each digital bit (ons & offs or "ones" and "zeroes") being sent. Voice packets are spaced by time.

Connection Type:

RVP_Direct
Advantages:

- Synchronous transmission of data requires fewer bits (and takes less time).
- Uses common network circuits.
- Circuit switched networks are generally more reliable for voice transmission.

Network Types:

- Switched 56/64K
- ISDN

Connection:
(2) DB-25 male connectors (WAN ports)

Interface Types:

- RS-232
- V.35
- RS-530

Remote Office EXTender Models:
EXTender 6000 for Branch Offices

Asynchronous-Serial Connection

An Asynchronous-Serial Connection is a connection where voice packets are sent at irregular intervals. Each voice packet is preceded with a Start Bit and followed by a Stop Bit. The timing of the transmission is not determined by the timing of a previous character.

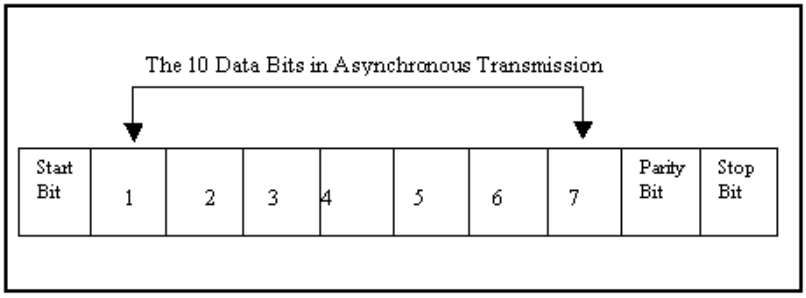


Figure 3: Asynchronous Transmission Data Bits

Connection Type:
RVP_Direct

Advantages:

- Used in lower speed transmission
- Less expensive

Network Types:

- Switched 56/64K
- ISDN

Connection:
(2) DB25 male connectors (WAN ports)

Remote Extender Models:
EXTender 6000 for Branch Offices

Voice Over IP (RVP__Over_IP)

Voice over IP (VoIP)

A network connection allowing voice packets to be delivered to the alternate site using the Internet Protocol (IP). In most IP circuits two types of devices are utilized. A server (PBXgateway) is the main hub of information being requested, and a client (the Remote unit) or user obtaining the information. The Remote unit receives the voice packets from the user phone and transmits the packets via the LAN and sends them over the WAN to the PBXgateway at the corporate facility.

Connection Type:
RVP_Over_IP

Advantages:

- Avoids toll charges charged by ordinary telephone services.
- IP connections are common and readily available.
- Makes use of existing network infrastructure.
- Avoids fixed costs associated with T1 & ISDN circuits.

Network Types:

- Switched 56/64K
- ISDN

Connection:
(1) RJ-45 10 or 100 BaseT connector

Extender Models:

- EXTender 4000 for IP
- EXTender 6000 for Branch Offices

Digital Telephone/PBX Features

Digital phones extended by the PBXgateway have the full functionality of phones located in the corporate facility.

Features include:

- the ability to place and receive calls
- extension-to-extension dialing
- speed dialing
- caller ID
- conference calls
- transfer calls
- full access to voicemail
- the use of the auto-attendant
- the utilization of ACD systems and call accounting software

Call Suspend

The Call Suspend feature allows the telecom manager to reduce dialup ISDN/IP costs by bringing down the ISDN/IP connection when all phones are inactive for a configurable period of time. When the line is disconnected the phones will display that they are in the Call Suspend mode. Whenever a user goes off-hook or an incoming call occurs, the ISDN/IP connection is brought back up and all phones are taken out of Call Suspend mode.

In addition, the *Rlogin* to remote and *Copy file* to remote features of the management interface also cause the ISDN/IP connection to be brought up and down as a phone would.

The Call Suspend feature has been designed with the assumption that if the ISDN/IP connection is brought down, it is possible to get busy signals from the ISDN/IP network preventing the extenders from communicating, causing an interruption of phone service to the branch office. This assumption leads to setting the Call Suspend timer to a value that will not allow the ISDN/IP connection to go down during normal business hours.

Note: The Call Suspend feature is configured at the remote site. Refer to the EXTender 6000 Quick Installation Guide (QIG) for more information.

Normal Behavior

The expected usage pattern for the ISDN connection will be that at the beginning of the business day, the phones will be brought out of Call Suspend mode bringing up the IDSN connection when the first user either goes off-hook or an incoming call arrives. The ISDN connection will remain up for the remainder of the business day because all phones will not be idle longer than the Call Suspend timeout value. At the end of the day, all phones will become inactive for the Call Suspend timeout value and the ISDN connection will be brought down. If anyone is working late or comes in early, normal usage will bring back up the ISDN connection.

Reconnection Failures

If the remote attempts to reconnect and fails, all the phones are brought back to “Suspended ….” State and the connection will be retrieved at the next “Off-hook”.

Rebooting the Remote or the Gateway

When the remote and Gateway go into Call Suspend mode, they each keep track of the connection information, e.g. phone number, call identifier, so that the units can be reconnected when Call Suspend mode is exited. If any unit reboots while in Call Suspend mode, it will attempt to reconnect after starting.

Note: the TA’s can take a while to sync up with the Central office, so connection is not attempted immediately.

Gateway

There is a problem when the gateway reboots because the remote unit has no way of knowing that the gateway has lost synchronization. Until the two units re-synchronize, all incoming calls will be ignored. To resolve this issue, the gateway unit will attempt to re-connect to the remote unit a configurable number of times (assumes the network link and the remote unit are still functioning). If the connection cannot be made, it is up to a user at the remote to cause the connection to be made.

Dynamic Reconfiguration

Changing voice parameters at the gateway which need to be sent to the remote, will cause the ISDN connection to be reestablished. Changing Call Suspend parameters at the remote will take effect immediately.

Call Suspend Modes

The Call Suspend feature is primarily designed for EXTender configurations using ISDN as the primary WAN link, although it can also be used in IP configurations (see below). Call Suspend, in ISDN networks, is intended to take the ISDN WAN connection down while the branch office is closed, in order to save on ISDN usage charges.

When Call Suspend is activated, the EXTender 6000/PBXgateway will take down the ISDN WAN link after an administrator defined amount of time (minimum 30 minutes) during which there is no phone activity. When phone activity occurs, the ISDN link will automatically be brought back up, re-establishing the connection between the PBXgateway and EXTender 6000 units. When using Call Suspend, one of following two modes can be used.

Remote Only Wakeup - Disabled

This mode will become the default setting when Call Suspend is selected. In this mode, when the ISDN BRI line is down with the units in Call Suspend, the line will be brought back up by activity at the Branch location (a set going off-hook or a key being pressed), or by an incoming call.

Remote Only Wakeup - Enabled

In this mode, the ISDN line between the Branch and PBXgateway will only be brought back up by activity at the Branch (a set going off-hook or a keypress). Incoming calls to the Branch will not bring the line up – they will ring into voice mail. The intention of this feature is to prevent ISDN connection charges from being incurred due to calls being made to a branch after hours, while still allowing employees at that branch to use the phones outside of normal business hours.

When using Call Suspend in IP network environments, the EXTenders will not tear down the WAN link, as this is controlled by the IP network. However, Call Suspend is useful in IP environments as it reduces bandwidth usage by preventing unnecessary PBX signaling traffic from being sent across the WAN link when the phones at the branch are not being used (minimum timeout of 30 minutes, as with ISDN configurations).

Using ConneX

The ConneX application is supported on MCK's ConneX™ PBXgateway™. This application puts PBX features and dialtone in your hands when using a mobile phone. The ConneX application is especially attractive to mobile workers because they can receive calls and access the corporate PBX system and commonly used voice applications from anywhere. PBX applications that are accessible through your mobile phone include: internal dialing, hold, transfer, conferencing and dialtone. ConneX provides survivability as well, in cases where your digital desk set goes down, you are still able to receive calls on your mobile phone.

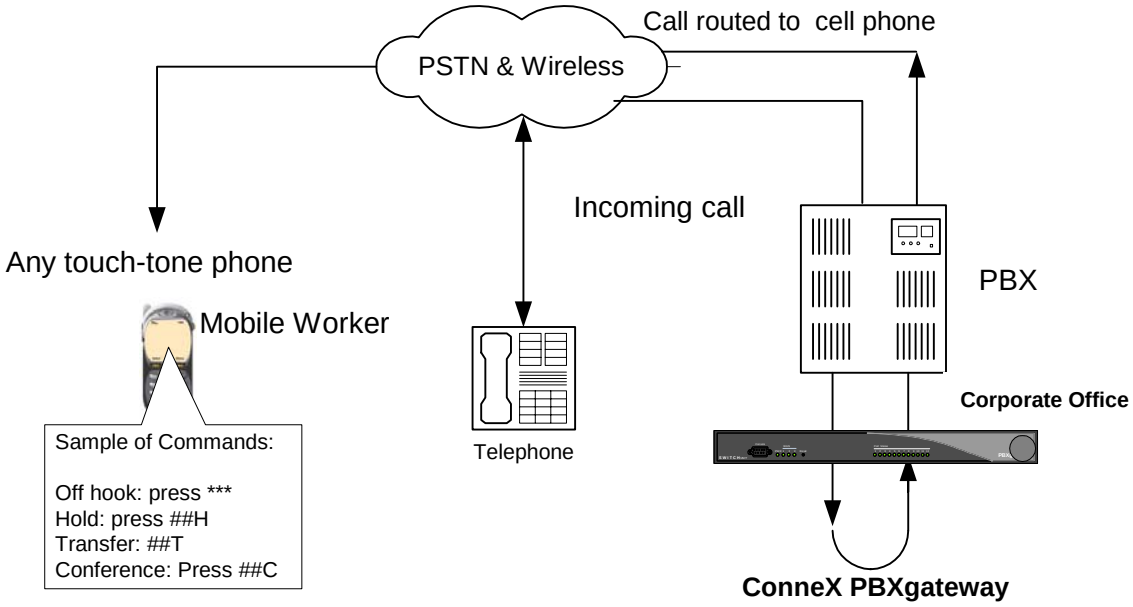


Figure 4: ConneX

Example: Jane's mobile phone rings. Jane is required to press any key on her mobile phone's dial pad to accept the call and to prevent the call from going into her corporate voicemail. After she accepts the call, she is able to talk to the caller, place the call on hold, transfer the call or set up a conference call as if she were using her office phone. (See the ConneX Commands starting on page 255 to learn which keys to press to imitate digital handset push buttons). If Jane chooses not to accept the call, the call is forwarded to her corporate phone voicemail.
When Jane wants to bypass long-distance toll charges, she dials into the ConneX PBXgateway using the number provided by the System Administrator to get PBX dialtone. Once she has accessed the dialtone she can place calls through the PBX system.

For information of configuring the ConneX application, as well as your ConneX phone please refer to Using ConneX on page 250.

Fax Traffic (DEFINITY and Meridian)

You are able to send fax traffic over the 2nd B channel (B2) of each port on a remote or a PBXgateway unit. The data is compressed using 32 Kbps ADPCM.

Each of the ports on an EXTender 6000 or PBXgateway will extend both of the PBX B channels, allowing the use of the second B channel for analog applications such as fax. You can send faxes by simply connecting the fax machine to the expansion card in the digital phone connected to the remote unit.

The analog port will have the label based upon the telephone type and protocol used:

Protocol	Telephone	Name of Analog Port
DEFINITY	6400 Series	100A Analog Interface Module
	8411D	Analog Adjunct
Meridian	2616	ATA (Analog Terminal Adapter)

Voice Compression vs. Bandwidth

The PBXgateway provides a choice of voice compression algorithms to allow up to 12 phones to be extended. The compression algorithm selected determines the bandwidth required.

DS0: The worldwide standard speed for digitized voice conversation at 64,000 bits per second.
ISDN: A digital transmission link consisting of two “B” channels (bearer) for voice and one “D” channel (data). Each “B” channel transmits voice signals at 64,000 bits per second.

The following are user selectable voice compression methods supported by the PBXgateway to accommodate the available bandwidth; G.729A (8 Kbps), ADPCM 24 (24 Kbps), ADPCM 32 (32 Kbps), G.711 (64 Kbps)

***Note**: These numbers indicate the bandwidth required per phone, not including overhead (8k).*

Physical Characteristics

The PBXgateway is an enclosed metal chassis, which can be stacked and installed in a standard 19” telecommunications or data communication rack.

Additional physical characteristics:

Front of Unit (See Front of PBXgateway on page 29)

- One DB-9 port used to connect a PC or terminal to the Management Interface
- Four dual-color system status LEDs
- Twelve or eight single-color port status LEDs

Back of Unit (Back of PBXgateway on page 29)

- One 50-pin, RJ-21 connector used to connect to the PBX
- Two DB-25 WAN ports to connect to the network device.
- One RJ-45 Ethernet port for LAN connection for Voice over IP traffic and/or Telnet management access.
- Four Ethernet Status LEDs
- Fan
- Power Switch

Configuration and Management

Configuration and Manageme

The configuration, operational, and troubleshooting features of the PBXgateway and EXTender are accessible through the Management Interface (MI). The MI can be accessed with a PC or terminal connected in one of three ways:

- Direct Serial connection (see page 44).
- TCP/IP-based Telnet access (see page 46).
- Inband login between the Switch and Remote units. (see page 105)

The MI

The MI is a menu system compatible with VT-100 Enhanced Terminal Interface (ETI) enabling the system administrator:

- the capability for full configuration of the phone and WAN ports plus IP configuration.
- the access for full management capabilities
- the access to status information on port usage
- the information necessary to troubleshoot problems
- the ability to review and monitor log messages (for possible signs of error)
- the ability to perform complete software upgrades.

Phone Set Interface (Remote only)

The **Phone-Set** user interface allows limited access (to the MI) including: Console port configuration for serial access and IP configuration for Telnet access.

The Phone-Set interface is accessible through any phone at the Remote site and provides a few useful diagnostic commands, status displays, and a limited set of configuration options-TCP/IP, console bit rate, and connection.

(Refer to Appendix C, *Phone-Set Interface* for more information)

Diagnostic Capabilities

The PBXgateway Management Interface (MI) provides the system administrator with numerous diagnostic capabilities. In addition, each time the PBXgateway is powered-up, it performs a diagnostic self-test.

Through the MI, you can:

- View statistics of the unit
- Reset the WAN and Telephony ports
- Test the WAN ports
- View results of the power-up self-test.
- Set up SNMP traps for capturing and viewing statistics and error conditions.

References:

- Refer to the chapter on Troubleshooting for more information.
- Refer to Appendix D *SNMP* for more information on SNMP traps.

Chapter 1: Product Specifications

This Chapter provides information and specifications including; Regulatory approvals, system architecture, memory, WAN design, interfaces, voice, and electrical specifications.

Specifications

This section contains information on specific electrical and mechanical parameters. These specifications are provided as a reference for design characteristics of the PBXgateway.
Note: Specifications for each Remote unit are contained within the individual Quick Installation Guide (QIG). *Specifications are subject to change without notice as technological or manufacturing changes warrant.*

Regulatory Approvals

FCC	47 CFR Part 68 US: 2DKOT01BEXT6001; 47 CFR Part 15 Subpart B
CE	EN55024+A1, A2; EN55022+A1, A2; EN6100-3-2; EN6100-3-3
Industry Canada	CS-03; 3807B-EXT6001
Safety	UL60950-1; C22-2 Nº60950-1; EN60950-1; IEC60950-1

System Architecture

CPU	Motorola MPC 852T, 50MHz
DSP	5 Analog Devices 2185 75 MIPS per Device

Memory

DRAM	16MB
Flash Memory	8MB

WAN Ports

Protocol	Synchronous-serial; Asynchronous-serial
Interface	RS-232, V.35, or RS-530
Encapsulation	High-level Data Link Control (HDLC)

Interfaces

Ethernet	Single 10 / 100 megabit, RJ-45
Serial/WAN	EIA/TIA-232, EIA/TIA-530, EIA/TIA-V35
Management	Serial RS-232, DB9
PBX/KSU	Up to 8 digital line interfaces over a 25 pair RJ-21 cable

Voice

Voice compression	G.729a, G.711, G.726 (ADPCM 32 and ADPCM 24

Protocols and Services

LAN	RVP over Internet Protocol (IP)
WAN	Remote Voice Protocol (RVP™) (proprietary) over HDLC

Electrical

Line Voltage	100-240 VAC
Frequency	50-60 Hz
Max Power Consumption	60 W
Protection	Over Current/Voltage and short circuit protection

Environment

Temperature	32° - 130° F (0° - 55° C)
Relative Humidity	5 to 95%

Dimensions

17 in x 8 in 1 3/4 in (432 mm x 203 mm x 44 mm)

Weight

6 lbs 7 oz (3 kg)

Chapter 2: Installation

This Chapter provides the following information for installing both the Switch and Remote units:

- Pre-installation requirements
- How to install the hardware
- How to wire the hardware
- Complete power-up sequence

Safety Checklist

IMPORTANT SAFETY INSTRUCTIONS

- Do not install this product near water, for example, in a wet basement location.
- Do not overload wall outlets, as this can result in the risk of fire or electrical shock.
- Do not attach the power supply cord to building surfaces.
- Do not allow anything to rest on the power cord.
- Do not locate this product where someone walking on it will damage the cord.
- Do not operate the system if chemical gas leakage is suspected in the area. Use telephones located in some other safe area to report the trouble.
- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

Hardware Components

The figures below show the PBXgateway front panel display and rear panel connectors. Refer to the table below for component descriptions.

***Note**: For details on the components of the Remote Units, refer to the specific Quick Installation Guides (QIG) shipped with each device.*

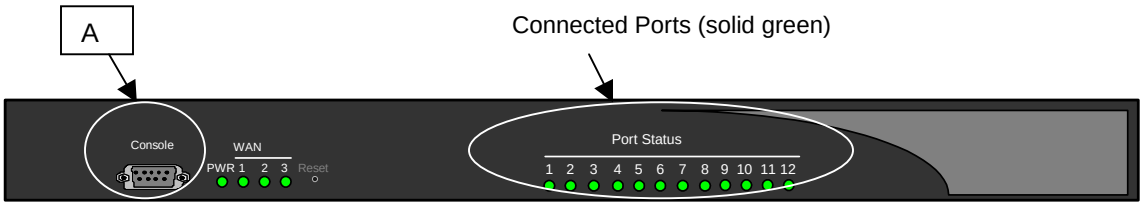


Figure 5: Front of PBXgateway

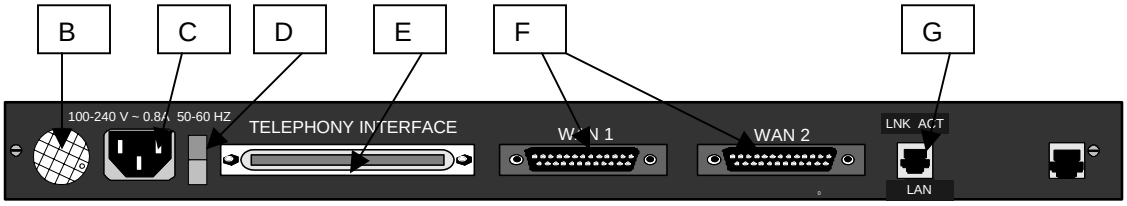


Figure 6: Back of PBXgateway

Letter	Label	Cable Type	Description
A	Console	DB-9	Connect to a PC COM port *Note: Set the COM port as follows: Baud rate: 9600, Databits: 8, Parity: none, Stopbits: 1, Software flow control: Xon/Xoff.*
B	Fan	-	Cools unit.
C	Power	-	Connect to a 120 VAC outlet
D	Power Switch	-	Turns unit on and off.
E	Telephony Interface	RJ-21	Wire to a punchdown block and then to the PBX.
F	WAN1 WAN2	DB-25, serial. straight-through	Connects the Gateway to a synchronous or asynchronous- serial device (CSU/DSU or other network device). *Note: Use an RS-530 type cable or DB-25 to M34 cable should for high-speed links to V.35 equipment.*
G	LAN	RJ-45 Ethernet	Connects the Gateway to the LAN for use in VOIP applications.

Table 3: Component Description

Pre-Installation Requirements

MCK Supplied Equipment

PBXgateway	• One eight or twelve user, rack mountable device • Two Mounting brackets and hardware • One power cord • One RS-530 Cable • One System Administrator's Guide • One QIG (Quick Installation Guide)
EXTender 6000	• One Remote unit • Two Mounting brackets and hardware • One power cord • One RS-530 Cable • One DB-9 Console Cable • One QIG (Quick Installation Guide)
EXTender 4000	• One Remote unit • One Power Supply • One QIG (Quick Installation Guide)

Customer Supplied Equipment

***Note**: This includes information for installing the PBXgateway and EXTender 6000. For information on "Customer Supplied Equipment" for each Remote unit, refer to the specific User's Guide.*

The customer must supply the following equipment:

- Telephones and line cords **Note**: Use two-wire digital display phones only.
- Two 50-pin RJ 21 female connectors for connecting the PBX to the PBXgateway and digital phones to the EXTender 6000.
- Punch blocks capable of cross connecting the PBXgateway to the PBX and digital phones to the Remote locations.
- A PC (or VT-100 compatible terminal) for configuration.
- One 10 or 100 BaseT RJ-45 cable if connecting the units to the Ethernet network.
- ISDN circuit at both Remote and Switch locations. Must be capable of connecting the remote branch office to the Switch location.
- A network-terminating device capable of interfacing with the PBXgateway and Remote units. Must support synchronous serial protocol using RS-232, V.35, or RS-530 interface types, or a 10 or 100 BaseT Ethernet for an IP connection.
- PBX digital ports programmed correctly for the telephone type being used at the remote location.

Network Requirements

The PBXgateway and EXTender 6000 must be installed on an existing LAN or WAN network.

- Each unit requires a network device that supports a synchronous-serial interface, asynchronous serial or an Ethernet connection to a TCP/IP network.
- The network must be operational and active to complete the installation of the PBXgateway.
- The network device must support one of the following:

  Synchronous serial signaling on its data port using an RS-232, V.35, or RS-530 interface.

  Or

  Asynchronous serial signaling on its data port using an RS-232.

  Or

  10/100BaseT Ethernet connection.

Power Requirements

The system has been designed to operate from 100-240 VAC, 50-60Hz. Power should not be applied to the PBXgateway and EXTender 6000 until specified in the installation procedures.

Location Requirements

- The maximum length of cable between the PBXgateway and the PBX is 500 ft (150 meters).
- The maximum length of cable between the Remote unit and the digital phones is 500 ft (150 meters).
- The PBXgateway and EXTender 6000 power supply and cabling should be installed away from high power/high RF noise devices such as computers, fans, fluorescent ballast, power supplies, etc.
- Use good wiring practices. Do not run wires over fluorescent lights, computers, air conditioners, etc. as this can introduce noise to the signals.
- The PBXgateway and EXTender 6000 must be installed in a secure location. Unauthorized access could lead to toll fraud.

Installation

Connecting the PBX/KSU to the PBXgateway

Required Components

- One RJ-21 cable with a 50-pin female connector.
- Up to twelve digital lines from the PBX.
- Active network from the Branch Office to the corporate facility over ISDN or 10/100 IP connection.
- Installed network device at each location.
- Cross-connection telephony wiring blocks sufficient for the installation
- Additional wiring sufficient for the digital lines.

***Note**: For detail wiring information, see the next page.*

Procedure

1. Install (2) cross-connect wiring blocks.
2. Connect the digital lines from the PBX to one of the cross-connect blocks via an RJ-21 cable.
3. Connect the PBXgateway telephony port to the other cross-connect block using an RJ-21, 50-pin cable.
4. Cross-connect the PBXgateway digital ports to the PBX digital lines via (2) cross-connection blocks.

***IMPORTANT**: DO NOT connect phones to a PBXgateway Unit.*

Connections to the PBX *continued*

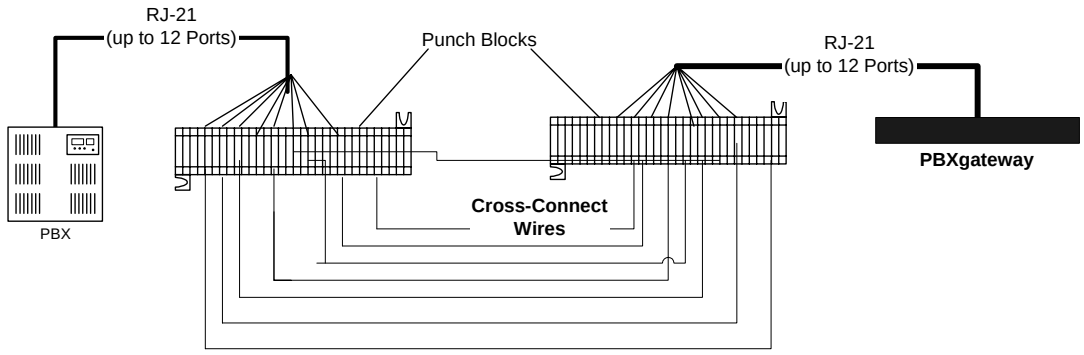


Figure 7: Connections to the PBX

Pin	Cable Pair	Port	Pin	Cable Pair	Port	Pin	Cable Pair	Port
26 1	WH/BL BL/WH	1	34 9	RD/BR BR/RD	5	42 17	YL/OR OR/YL	9
28 3	WH/GN GN/WH	2	36 11	BK/BL BL/BK	6	44 19	YL/BR BR/YL	10
30 5	WH/SL SL/WH	3	38 13	BK/GN GN/BK	7	46 21	VI/BL BL/VI	11
32 7	RD/OR OR/RD	4	40 15	BK/SL SL/BK	8	48 23	VI/GN GN/VI	12

Wire Color Abbreviations:

BK=Black, BR=Brown, RD=Red, OR=Orange, YL=Yellow, GN=Green, BL=Blue, VI=Violet, WH=White
SL=Slate

Mounting the PBXgateway and EXTender 6000

Introduction The following procedure explains the steps necessary to secure the PBXgateway and EXTender 6000 to a standard 19-inch communications rack.

***Note**: The Rack is not supplied with the unit*.

Procedure

1. Attach the mounting brackets to the unit.
2. Position the unit so the mounting brackets are aligned with the mounting holes of the chassis.
3. Secure the unit with mounting hardware (4 screws) provided.

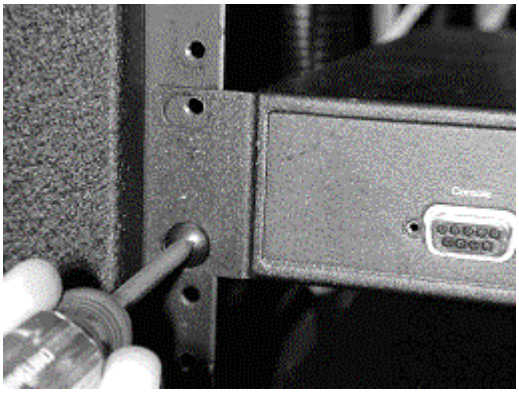


Figure 8: Mounting the Unit

Connections to the Network Device

Introduction

The PBXgateway and EXTender 6000 connects to a variety of network devices through a Synchronous-serial connection, or 10/100 BaseT Ethernet connection. The physical connection is accomplished through two DB-25 connectors labeled WAN1 and WAN2, or an RJ-45 Ethernet connector. The following protocols are recommended:

Synchronous

Protocol

- High level Data Link Control (HDLC)
- A link layer protocol standard for point-to-point and multi-point communications.

Connection Types

- RS-232 (see page 37 for pinouts)
- V.35 (see page 37 for pinouts)
- RS-530 (see page 38 for pinouts)

Asynchronous

Protocol

- V.120
- Clear-async-bonding

Connection Types

- RS-232 (see page 37 for pinouts)

Internet Protocol

Protocol

- Internet Protocol (IP)
- Standard network protocol.

Connection Type

- 10 or 100 BaseT Ethernet

Wiring Information

Wiring Info Figure 8 through 10, lists each pin within the DB-25 connector with the signal description and signal/voltage source, using the Electronics Industry Association (EIA) standard.

RS-232 (DB-25) Serial Connector Pinouts

Signal/Voltage Source	Shield Designations		Shield Designations	Signal/Voltage Source
			1 Shield	Common
DTE	Secondary Tx Data 14		2 (TD) Transmitted Data	DTE
DCE	Tx Clock 15		3 (RD) Received Data	DCE
DCE	SecondaryReceived Data 16		4 (RTS) Request to Send	DTE
DCE	Receiver Clock 17		5 (CTS) Clear to Send	DCE
DTE	Local Loopback 18		6 (DSR) DCE Ready	DCE
DTE	Request to Send (Return) 19		7 Signal Ground	Common
DTE	Data Terminal Ready 20		8 (DCD) Rcvd Line Signal Detect	DCE
RL-DE SQ-DCE	Remote Loopback 21		9 (+) DC Test Voltage	Common
DCE	Ring Indicator 22		10 (-) DC Test Voltage	Common
CH-DTE Cl-DCE	Data Signal Rate Selector 23		11 Unassigned	- -
DTE	Tx Clock 24		12 (SCF/Cl) Secondary Rcvd Line	DCE
DCE	Test Mode 25		13 Secondary Clear to Send	DCE

Figure 9: RS-232 Cable Pinouts

V.35 (DB-25) Serial Connector Pinouts

Signal/Voltage Source	Shield Designations		Shield Designations	Signal/Voltage Source
			13	-
DCE	Test Mode 25		12 Transmit Clock (b)	DCE
DTE	External Transmit Clock (a) 24		11 External Transmit Clock (b)	DTE
-	23		10	-
-	22		9 Receive Clock (b)	DCE
DTE	Remote Loopback 21		8 Carrier Detect	DCE
DTE	Data Terminal Ready 20		7 Signal Ground	-
-	19		6 Data Sent Ready	DCE
DTE	Local Loopback 18		5 Clear to Send	DCE
DCE	Receive Clock (a) 17		4 Request to Send	DTE
DCE	Receive Data (b) 16		3 Receive Data (a)	DCE
DCE	Transmit Clock (a) 15		2 Transmit Data (a)	DTE
DTE	Transmit Data (b)14		1 Frame Ground	-

Figure 10: V.35 Cable Pinouts

RS-530 (DB-25) Serial Connector Pinouts

Signal/Voltage Source	Shield Designations		Shield Designations	Signal/Voltage Source
			1 Shield	Common
Common	Tx Data (Return) 14		2 Transmitted Data	DTE
DCE	Tx Clock 15		3 Received Data	DCE
Common	Received Data (Return) 16		4 Request to Send	DTE
DCE	Receiver Clock 17		5 Clear to Send	DCE
DTE	Local Loopback 18		6 DCE Ready	DCE
Common	Request to Send (Return) 19		7 Signal Ground	Common
DTE	Data Terninal Ready 20		8 Carrier Detect	DCE
DTE	Remote Loopback 21		9 Receive Clock (Return)	Common
Common	Data Set Ready (Return) 22		10 Carrier Detect (Return)	Common
Common	Data Terminal Ready (Return) 23		11 DTE Tx Clock (Return)	Common
DTE	DTE Tx Clock (Return) 24		12 Tx Clock (Return)	Common
DCE	Test Mode 25		13 Clear to Send (Return)	Common

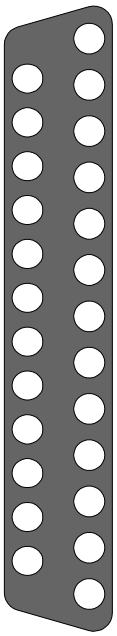


Figure 11: RS-530 Cable Pinouts

Compatible Remote Units

The PBXgateway is compatible with the following Remote units:

EXTender 6000 – for Branch Offices.

Provides connectivity for up to 12 remote users from a single branch office location. Each phone is cross-wired to a port on the unit.

EXTender 4000 – for IP

Provides connectivity for a single user client via an IP network. The single user phone is simply plugged into the Remote unit "phone" port.

Connecting the Remote Unit to the User phones

Required Components

- One RJ-21 cable with 50-pin female connector.
- Active network from the Branch Office to the corporate facility over an ISDN or IP.
- Installed network device.
- Digital phone(s) and line cord(s)
- Cross-connection wiring block or break-out box sufficient for the installation
- Additional RJ-11 or RJ-45 phone cords.

***Note**: For detailed wiring information please refer to page 39.*

Procedure

1. Install (2) cross-connect wiring block or use a single breakout box.
2. Connect the Remote phones to a punch block or breakout box.
3. Wire breakout box or punch block to 50-pin cable RJ-21 connector.
4. Connect the 50-pin, RJ-21 cable to telephony interface at the Remote unit.

   ***IMPORTANT**: DO NOT connect the Remote Unit to a PBX/KSU.*

Connecting the EXTender 6000 Remote Unit to the Remote Phones

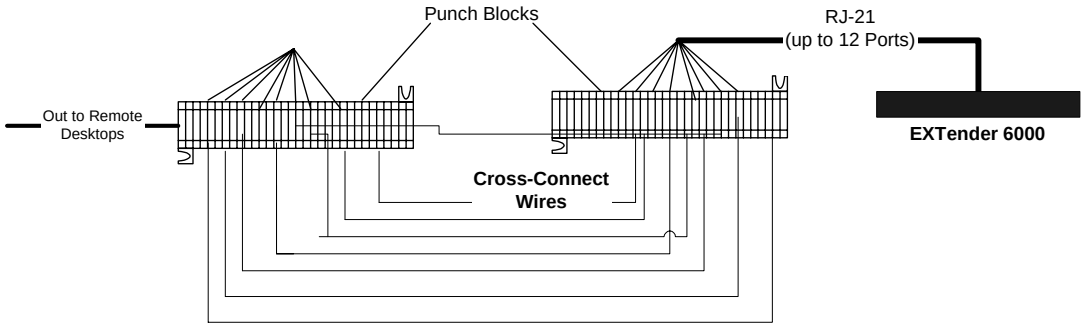


Figure 12: Connections to the EXTender 6000

Pin	Cable Pair	Port	Pin	Cable Pair	Port	Pin	Cable Pair	Port
26 1	WH/BL BL/WH	1	34 9	RD/BR BR/RD	5	42 17	YL/OR OR/YL	9
28 3	WH/GN GN/WH	2	36 11	BK/BL BL/BK	6	44 19	YL/BR BR/YL	10
30 5	WH/SL SL/WH	3	38 13	BK/GN GN/BK	7	46 21	VI/BL BL/VI	11
32 7	RD/OR OR/RD	4	40 15	BK/SL SL/BK	8	48 23	VI/GN GN/VI	12

Table 4: Assignments (25-Pair Cable)

Wire Color Abbreviations:

BK=Black, BR=Brown, RD=Red, OR=Orange, YL=Yellow, GN=Green, BL=Blue, VI=Violet, WH=White SL=Slate

Before you Power-Up the PBXgateway and EXTender 6000

Introduction This procedure will detail the necessary steps to perform BEFORE bringing the units online.

Checklist The units are secured to a rack or placed on a shelf within the rack.

The appropriate 50-pin female, RJ-21 connectors are connected to the Telephony Interface and wired to the PBX (PBXgateway) and remote user phones (Remote unit).

At least one WAN port is connected to the appropriate network-terminating device.

or

The LAN port is connected to your network using a standard RJ-45 Ethernet cable.

Power Up If the above checklist is OK, plug the power cord into an AC outlet.

Power-Up Sequence The WAN (PWR, 1, 2) and the Port Status LEDs (1-8 or 1-12) will begin to flash. The unit automatically runs through a series of self-tests. After the tests are complete, all active WAN port LEDS and connected phone ports should be lit solid “Green”.

***Note**: If the LEDs do not light as described above, see the Troubleshooting chapter.*

Chapter 3: Configuration

This Chapter provides information for configuring the PBXgateway and the Remote units through the Management Interface (MI).

***Attention System Administrator**: All configuration parameters for the Remote units can be accessed from the PBXgateway unit via the "Remote Login" menu selection within the MI. Units must be in an up-active-working status.*

Connecting to the PBXgateway

Interface Methods

The PBXgateway has a terminal based user interface for access to the MI for configuration purposes.

Console User Interface:
VT-100 Enhanced Terminal Interface (ETI) accessed from a PC via one of three possible methods:

- Direct Serial connection through the console port located on the front of the PBXgateway. (refer to page 44)
- LAN-based Telnet access (see page 46)
- In-band management connection between the Switch and Remote (see page 105)

Security

It is recommended that an administrator password be assigned to prevent unauthorized access to the Remote and PBXgateway. The PBXgateway has two separate levels of password security:

Connect Password: Set by the system administrator, provides a secure WAN link between the Gateway and Remote units. (see page 67 for more information).
Your password should be alphanumeric only. In other words, only use numbers or letters that are on the telephone keypad. DO not use symbols such as $, & or *, as these cannot be entered on a digital deskset keypad.

Admin Password: Set by the system administrator and provides security to restrict access to the MI. (See page 86 for more information).

***Note**: Connect Passwords for Remotes and Gateway must match*.

System Administrator

A system administrator is defined as the sole person responsible for the maintenance and administration of the PBXgateway at the corporate facility.

What a System Administrator Must Know

- The type of network connectivity used at the Corporate and Branch location. (ie: Serial or IP).The type of network through which the PBXgateway communicates with the branch location. (ie: ISDN or IP)

  ***Note**: The type of connectivity used at the Branch location, should match the Corporate location.*
- The types of units installed at the remote location, (ie: EXTender 6000, IP EXTender 4000).
- Information on which phones communicate with which PBXgateway ports.

Connecting to the Management Interface (MI)

Direct Serial Connection

Introduction The console port provides a direct serial connection for the PBXgateway and EXTender 6000 allowing access to all features and functions of the MI and the ability to configure, monitor and troubleshoot the unit.

Required Cable A standard RS-232 serial straight-through (DB-9, Male) cable is required. Use this cable to connect the PC's COM Port to the console port on the front of the unit.

***Note**: Cable length should not exceed 50 ft.*

Before you conn Before connecting to the PBXgateway you must confirm that the PC's COM port settings match the console port settings as follows:

Baud rate: 9600
Databits: 8
Parity: none
Stopbits: 1
Flow Control: XON/XOFF

***Note**: See Setting the Console Baud on page 83 for more information on setting the PBXgateway baud rate.*

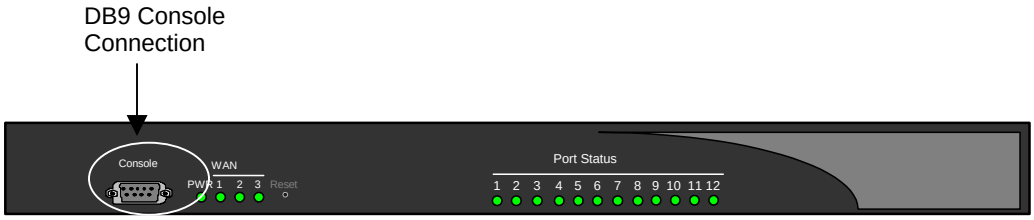


Figure 13: Console Port Connection

Procedure

1. Once the PC is connected to the unit through the console port, open an Enhanced Terminal Interface (ETI) program on the PC.

   Example: Windows Hyperterminal

   Note: The MI configuration menus can be accessed through any generic Windows 95, or Windows 98, VT-100 Enhanced Terminal Interface (ETI) program.

2. Within the ETI program, change the data settings to match those shown on the previous page.

3. Save the changes within the ETI and restart the program for the changes to take effect.

4. Power up the Gateway or Extender 6000.

   The unit performs a series of boot-up tests and upon finishing the boot-up process, displays the following message:

   Press "Enter" to start the Gateway shell…….

***IMPORTANT**: If the unit is already powered-up the screen may display garbage characters. Press **F4** to refresh the screen.*

5. Press **Enter**.
6. The MI Welcome Screen appears (refer to page 47).

Internet Access

You can also configure the PBXgateway and the EXTender units via a web browser interface (Internet Explorer 5.X or higher). The HTML configuration editor menus will follow the same tree structure as the current Management Interface (MI).

Login Procedures

1. Start your browser.
2. Point your browser to the IP address of the unit you wish to configure.
3. Follow the directions on the screen.

EXTender Window

A new browser window, titled EXTender appears. At the top of this window is a graphical representation of the Gateway or EXTender unit, complete with WAN and Port Status LEDs. This display updates automatically to ensure that the LEDs indicate the current status of the unit.

At the top right of the EXTender window is a link named LED Definitions. Click this link to see the definition of each type of WAN and LAN LED.

The left side of the EXTender window is for navigation. From here, you can configure any part of the EXTender by first locating the appropriate sub-menu. A plus sign (+) before a menu item indicates that additional menu items are beneath it. Click on this menu item to show the items underneath.

The left side of the EXTender window has the main menu items listed below:

+Configuration
+Status
+Utilities
Gateway Login
Logout

The Support and Help options lead you to the MCK website, www.MCK.com.

Click on a menu item that is preceded by a minus (-) sign to hide the menu items that are beneath it.

The right side of the EXTender window displays the configuration information. When an item on the left side of the window has items beneath it, you have the option of accessing the sub-items from the right side of the window as well.

Printing

Use standard procedures to print pages in the EXTender window from your browser.

***Note**: In order to print pages from Internet Explorer versions 5 and above, you need to enable "Print background color and images".*

To enable this setting:

1. Go to the browser window.
2. In the pulldown menu, select Tools->Internet Options.
3. Click on the Advanced tab. If necessary, scroll down to Printing.
4. Be sure that 'Print background color and images" is checked.

Telnet Connection

Introduction The PBXgateway and EXTender can be configured using a Telnet session over the existing LAN connection. There is a maximum of four Telnet connections per unit at one time.

***IMPORTANT**: All IP parameters must be configured before a Telnet session can be established to a unit. (see page 76 for more information).*

Procedure

1. On a computer running Windows, open the Telnet application by selecting **Start/Run** from the desktop.
2. Enter telnet command along with the IP address assigned to the unit (see Figure below).

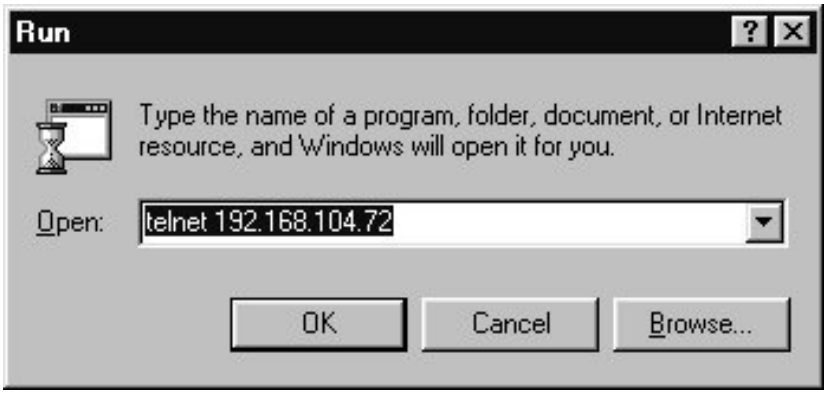


Figure 14: Telnet address

3. Click **OK**. The MI Welcome Screen appears (see next page).

Welcome Screen

Once the system administrator has connected to the MI the following Welcome Screen appears.

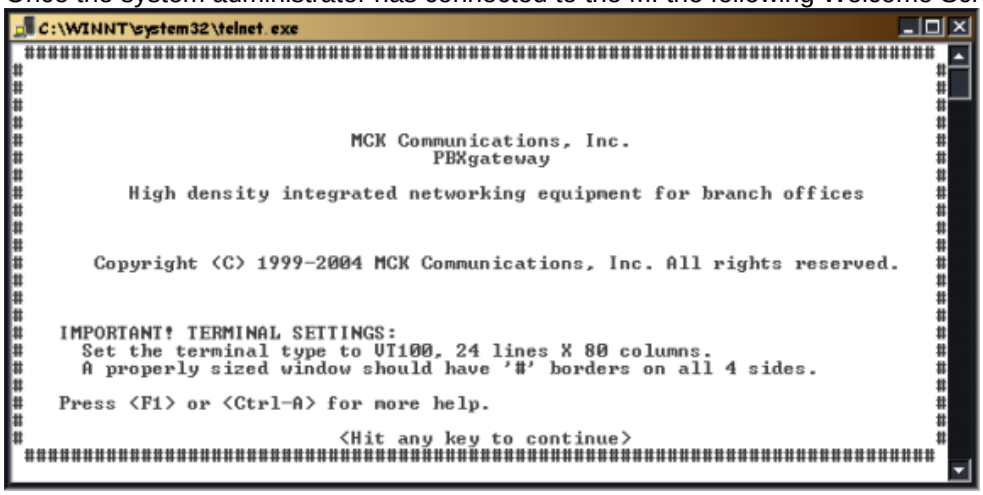


Figure 15: Welcome Screen

IMPORTANT TERMINAL SETTINGS
The MI requires a screen size of 24 lines X 80 columns. Make sure the Welcome Screen is bordered on all four sides with a # symbol

To enlarge the screen (within the VT-100 application):

1. Click any corner of the screen.
2. Drag the screen to enlarge.
3. Check that the screen is bordered by "#" symbols.
4. Press Enter to access the Main Menu.

***Note**: See page 49 for detailed information on a typical menu or press **F1** for the MI Help Screen (see next page).*

Help Screen

The MI has a built-in Help Screen that provides basic information for navigating through the interface.

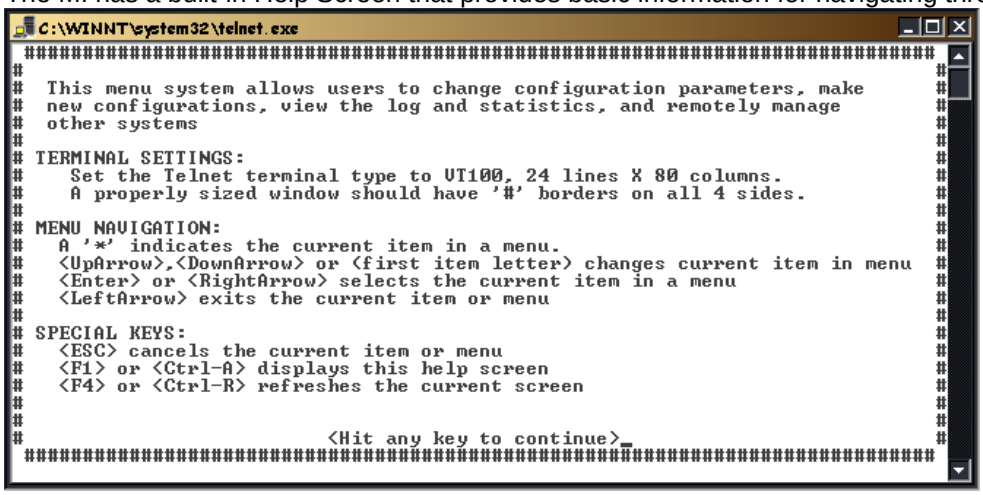


Figure 16: Help Screen

The following information is provided:

Terminal Settings - These settings are necessary for properly displaying the configuration screens.

Menu Navigation – Explains the necessary command keys used for navigating through the MI. (see page 51 for more information).

Special Keys – Explains the function keys used for special commands.

Press **Enter** to access the Main Menu.

***Note**: See the next page for detailed information on a typical menu*.

Typical Menu

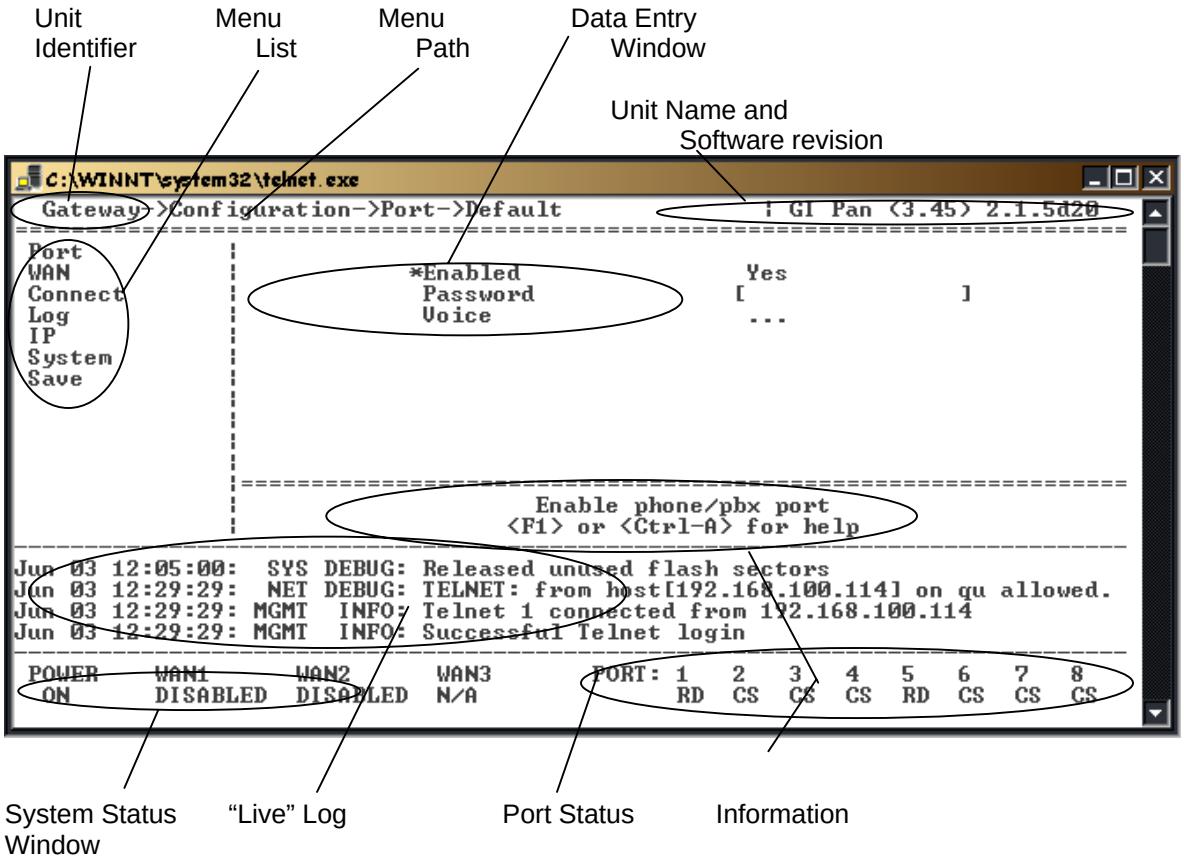


Figure 17: Typical Menu

***Note**: See the next page for information on the Menu Components.*

Menu Components

Area	Description
Unit Identifier	Displays either “Remote” or “Gateway” depending on which unit you are connected to.
Menu List	List of sub-menus used to configure the PBXgateway Switch and Remote units. An * indicates the active menu selection.
Menu Path	Displays the menu hierarchy.
Data Entry Window	This is the only area on the main menu where information can be changed. It is also where submenus are selected.
Unit Name and Software Revision	Displays the name assigned to the unit, and the software revision of the firmware.
Information Window	Each menu contains specific parameters. This window provides a context sensitive help message which provides a brief description of the selected item
Port Status	Provides status information on all phone ports.
“Live” Log	This window provides the system administrator with log messages on the status of the unit and error conditions. Last four messages are displayed. This is not the entire log file. The entire log file can be viewed using the following path: (**Path**: Status->Display Log) ***Note****: This log is not “live” via Remote Login menu item. Use F4 (Ctrl R) to refresh the screen.*
System Status	Provides status info for power, and both WAN ports

Table 5: Menu Components

Command Keys

Introduction The Management Interface (MI) utilizes a minimal set of command keys to navigate through the different sub menus.

The following keys are used:

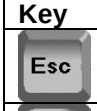
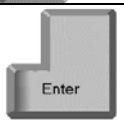
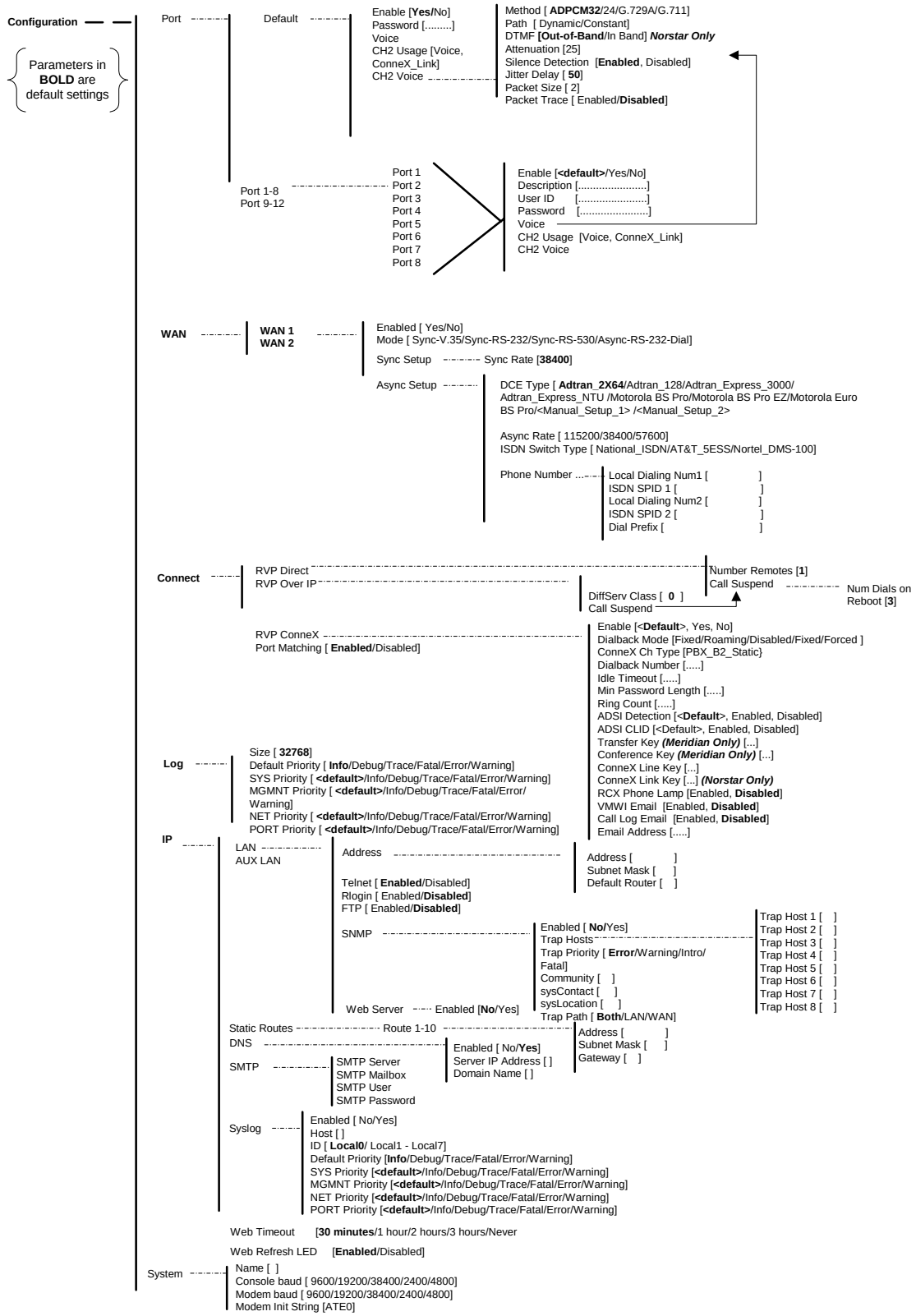
Key	Description
	Cancel
	Accepts the change or menu, or exits the current menu.
 **or** 	Selects the current item in a menu.
 **or** 	Changes the current item in a menu. ***Note**: Selecting an item can also be accomplished by typing in the first character*.
 **or**  **A**	Help screen.
 **or**  **R**	Refreshes the current screen.

Table 6: Command Keys

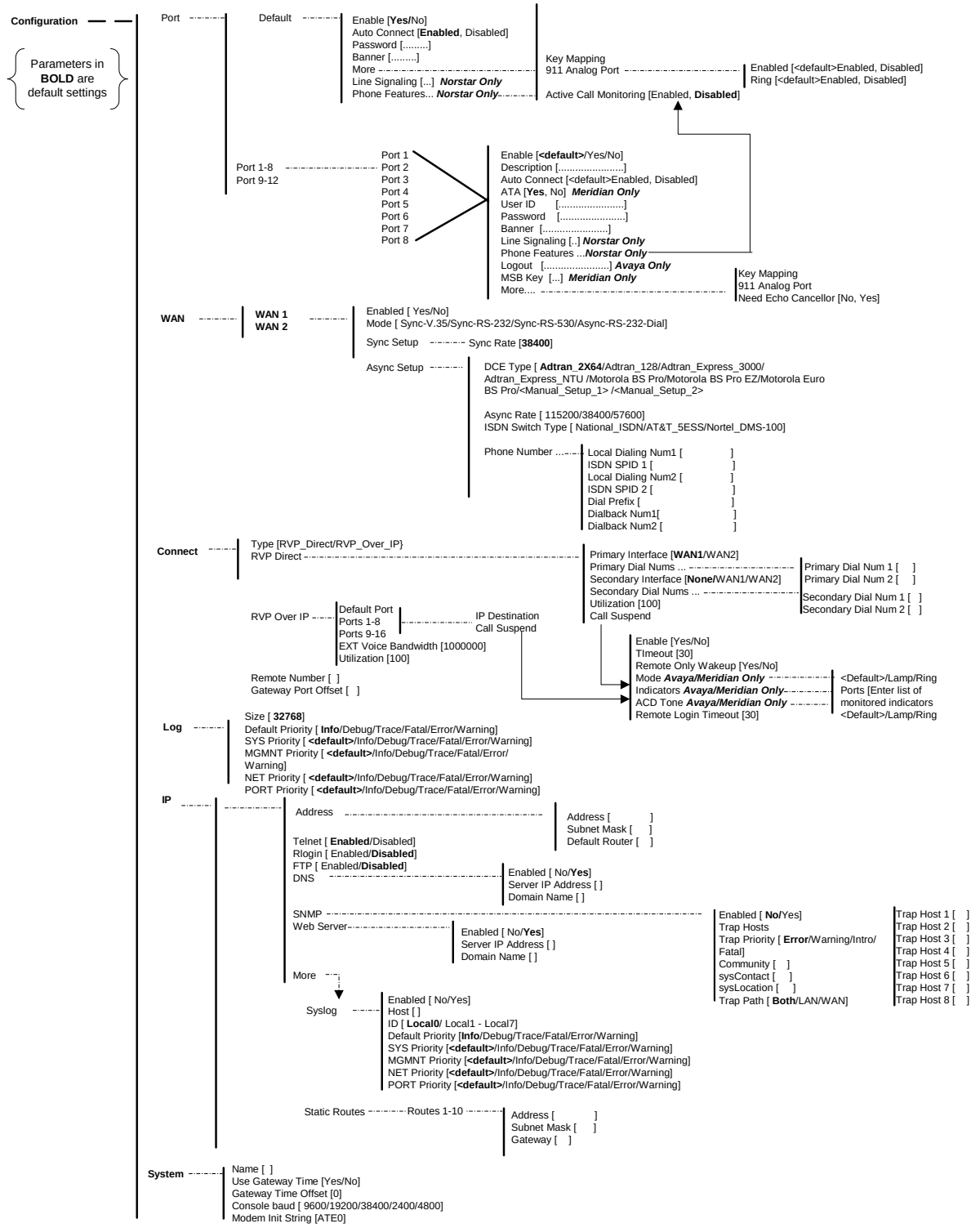
PBXgateway Menu Items and Structure

The figure below outlines the menu structure for the PBXgateway, using the MI.



Remote Unit Menu Items and Structure

This section of the manual provides a list of parameters for configuring each Remote. All configuration parameters necessary for the installation and configuration for the Remote unit are contained within this guide.



Remote Unit Menu Structure

Network Environments

Types of Networks

Introduction This section of the manual provides the necessary information to configure the PBXgateway and EXTender 6000 using the Management Interface (MI). The units are programmed at the factory with “default” settings providing basic parameters to accommodate most network environments.

Which type of Network Device do you have? Before beginning the configuration process, it is necessary to identify which type of network device is connected to the PBXgateway and EXTender 6000. Once you know the type of connection the table, below, will direct you to the appropriate checklist that should be used for configuration.

To configure the PBXgateway with	See page
a Synchronous-Serial device (RVP_Direct)	55
a Asynchronous-Serial device (RVP_Direct)	57
an IP device (RVP_IP)	59

Synchronous-Serial Device Configuration (RVP_Direct)

This section of the manual provides the necessary information to configure the PBXgateway and EXTender 6000 for connection to a synchronous-serial device. The units are programmed at the factory with “default” settings providing basic parameters to accommodate many network environments.

Prerequisites for Configuration

Both units must be installed properly (see Chapter 2) and the network link between both devices must be operational.

Basic Configuration – EXTender and PBXgateway

You must …….	to…….	Follow these steps…….
Set the voice compression algorithm for all active phone ports.	Provide adequate bandwidth for all users.	Refer to page 63 Refer to Appendix B, Bandwidth Requirements.
Adjust the Jitter setting. (PBXgateway Only)	Match network characteristics.	Refer to page 63
Adjust the Attenuation. (PBXgateway Only)	Decrease echo.	Refer to page 63
Enable/Disable WAN ports	Enable WAN ports to connect to network device.	Refer to page 70
Set the Sync Rate of the WAN port	Match the data rate (sync rate) of the network device.	Refer to page 71
Set the mode (interface type) of the WAN	Match the interface type of the network device.	Refer to page 71
Configure the Remote unit.	Set the required parameters.	Refer to page 106

Table 7: Basic Configuration Steps

Synchronous-Serial Device Configuration continued

Optional Configuration - EXTender and PBXgateway

This section of the manual provides information for setting up optional parameters providing customization, identification and security for the Gateway and Remote units.

To ……	**for……**	**Refer to page……**
Enable/Disable individual phone ports	Managing and isolating the ports for troubleshooting purposes.	66
Set up a Connect Password	Providing a secure WAN connection restricting access to the PBXgateway from the Remote unit.	67
Set IP Information	Telnet/FTP access to both the Gateway and Remote units. ***Note**: The network administrator must allocate an IP address for each unit.*	76
Provide a System Name	Identification purposes. (not an IP Host name)	82
Set the Date/Time	Accurate time and date stamps for troubleshooting and for system maintenance.	85
Set an Admin Password	Restricting access to the MI.	86
Set User ID	Map remote users with specific PBX ports.	68
Set SNMP parameters.	Configuring necessary information to utilize the Simple Network Management Protocol functions of the MI.	Appendix D

Table 8: Optional Administrative Items

Asynchronous-Serial Device Configuration (RVP_Direct)

This section of the manual provides the necessary information to configure the **PBX**gateway™ for connection to an asynchronous-serial device. The units are programmed at the factory with “default” settings providing basic parameters to accommodate many network environments.

Prerequisites for Configuration

The PBXgateway (at the corporate site) and the **EXT**ender 6000 (at the branch office) must be installed properly and the network link between both devices must be operational.

Basic Configuration - EXTender and PBXgateway

You must …….	to…….	Default Setting	Refer to page..
Enable the WAN port and set the mode (interface type).	Match the interface type of the network device.	V.35	70
Set the Async parameters for the selected WAN port.	Match the settings for the device being used.	-	73
Set the “Jitter” and “Compression” settings.	Match the available bandwidth and quality.	Jitter: 5 Compression : ADPCM32	63

Table 9: Configuration Steps

Asynchronous-Serial Device Configuration continued

Optional Configuration - EXTender and PBXgateway

This section of the manual provides information for setting up optional parameters providing customization, identification and security.

To ……	for……	Refer to……
Enable/Disable individual phone ports	Managing and isolating the ports for troubleshooting purposes.	page 66
Set up a Connect Password	Providing a secure WAN connection restricting access to the PBXgateway from the Remote unit.	page 67
Set IP Information	Telnet/FTP access to both the PBXgateway and Remote units. Note: The network administrator must allocate an IP address for each unit.	page 76
Provide a System Name	Identification purposes. (not an IP Host name)	page 82
Set the Date/Time	Accurate time and date stamps for troubleshooting and for system maintenance.	page 85
Set an Admin Password	Restricting access to the MI.	page 86
Set User ID	Map remote users with specific PBX ports.	page 68
Set SNMP parameters.	Configuring necessary information to utilize the Simple Network Management Protocol functions of the MI.	Appendix D

Table 10: Optional Administrative Items

IP Network Configuration (RVP_Over_IP)

MCK's IP-based products utilize Voice over IP (VoIP) technology to deliver remote voice solutions. The voice quality of these solutions is dependent on variables such as available bandwidth, network latency and quality of service (QoS) initiatives, all of which are controlled by the network and internet service providers. Because these variables are not in MCK's control, it cannot guarantee the performance of the user's IP-based remote voice solution.

This section of the manual provides the necessary information to configure the PBXgateway for connection within an IP network.

***Note**: The units are programmed at the factory with RVP_Direct "default" settings. The "connect" parameter (see page 106) must set to RVP_Over_IP.*

Prerequisites for Configuration

Both units must be installed properly (see Chapter 3) and the network link between both devices must be operational. The network administrator must allocate an IP address for each unit.

Basic Configuration - EXTender and PBXgateway

You must …….	**to……**	**Follow these steps…….**
Set IP parameters.	Allow the PBXgateway to communicate over the IP network.	Refer to page 76
Set up voice parameters for all active phone ports, and tune Jitter delay and packet size. (Gateway Only)	Enable each port to select compression method and tune voice parameters to accommodate IP network.	Refer to page 63
Disable both WAN ports.	Disable ports that are unnecessary for RVP_IP.	Refer to page 70
Configure the Remote unit.	Set the required IP and Connect parameters.	Refer to page 106

Table 11: Basic Configuration Steps

TCP/UDP Requirements

Ensure that the correct TCP/UDP ports have been opened to allow the EXTender 6000 to connect to the PBXgateway through your company firewall. The following TCP/UDP port requirements must be met:

The EXTender 6000 and 4000 use even numbered ports 12,288 to 12,544. The port numbers start at 12,288 and increment by 2 to the total number of ports used. For example, if you have an 8 port EXTender 6000 with 3 phones connected, then you would need to make sure ports 12,288, 12,290, and 12,292 are opened.

The Gateway unit uses TCP/UDP port 2698.

Optional Configuration - EXTender and PBXgateway

This section of the manual provides information for setting up optional parameters providing customization, identification and security for the PBXgateway.

To ……	**for……**	**Refer to page……**
Enable/Disable individual phone ports	Managing and isolating the ports individually.	66
Set up a Connect Password	Providing a secure connection to restrict access to the PBXgateway.	67
Provide a System Name	Identification purposes. (not an IP Host name)	82
Set the Date/Time	Providing accurate time and date stamps for troubleshooting and for system maintenance.	85
Set an Admin Password	Restricting access to the MI.	86
Set User ID	Map remote users with specific PBX ports.	68
Set SNMP parameters.	Utilizing the Simple Network Management Protocol (SNMP) functions of the MI.	Appendix D

Table 12: Optional Administrative Items

Setting PBXgateway and EXTender Parameters

IMPORTANT: Changes made in this section, via the MI, are saved to the “Active” config file stored on the Gateway and EXTender unit. All configuration files are saved with a .rem extension for Remote unit files, and a .swt extension for PBXgateway files. The MI will prompt you to save changes as necessary. There are options for saving these parameters under a different file name, or creating and editing a “non-active” configuration file. (see page 175, for more information)

IMPORTANT INFORMATION

Initial MI Connection
The initial set up of the PBXgateway MUST be done through a direct serial connection (see page 44), until the IP parameters have been entered (see page 76) allowing configuration via Telnet through the Ethernet port.

Default Settings
The units are programmed at the factory with “default” settings providing basic parameters to accommodate many network environments. It may be necessary to change these settings depending on the network.

Set up Wizard
This is a setup program accessed through a direct-serial connection. The wizard prompts you to enter required information necessary for configuring the PBXgateway. (see page 104, for more information)

Multiple Remotes (RVP_Over_IP only)
The PBXgateway can interface with multiple clients from one to twelve users. It is necessary to know the type of Remote units that are communicating with the PBXgateway for proper configuration.

Port Setup

<Default> vs. Individual Port Settings

Introduction

The PBXgateway provides voice connectivity for up to twelve remote users. All phone ports on the PBXgateway are cross-wired to a digital port on the PBX. This provides the remote user with full PBX functionality as if they were placing calls from the corporate office. The Branch Office EXTender unit is connected to the remote phones through an RJ-21 connector wired to a punch down block or wall field.

Once the units are connected (see *Chapter 2: Installation*) the Management Interface (MI) has two methods for setting up the PBXgateway ports:

<Default> settings vs. individual settings

The <Default> settings: Sets all eight or twelve ports identically. With <Default> selected for a specific parameter for any port, that parameter will be set to whatever value the `Port-><Default>` parameter is set to. When configuring ConneX user's DO NOT use the default settings. Configure single ports for each ConneX user.

Example: If the `Port-><Default>` value for "Voice method" is set to ADPCM 32, and Port 1 has <Default> selected for "Voice Method" then Port 1 will utilize ADPCM 32 for its voice compression.

Individual port settings: Sets each port individually. This method is used for customizing ports by providing the flexibility of changing parameters for specific users. Use this method when configuring ports for ConneX users. Note, however that some items, such as Voice Settings, are applicable to only the Gateway.

Example: If Port 1 has the "Voice method" set to G.729A, rather than the <Default>, Port 1 will utilize G.729A for its voice compression.

Setting Voice Parameters (Gateway Only)

Introduction The MI provides a menu for setting voice parameters for each phone port for the PBXgateway. The following parameters are covered:

Method (of compression)-Selectable voice compression methods reduce network bandwidth requirements. (refer to *Appendix B* for more information on Bandwidth Settings)

Path – This will set the voice path to Dynamic or Constant. Dynamic means that the Branch Office unit uses the available bandwidth when the remote user goes off-hook. Constant means that the voice path is always reserved.

DTMF (Avaya Only) – The method of sending tones, which correspond to numbers, pressed on the telephone, across the network. The tones can be sent as voice (In-band), or as signals (Out-of-band).

Attenuation– Attenuation decreases the signal being sent to the PBX. This can be adjusted to decrease the amount of echo during calls.

Silence Detection - When enabled, the Extender detects silent periods during a conversation, and as a result sends no data during these periods. This dramatically reduces bandwidth usage, so this parameter should be Enabled (default setting).

Jitter-The amount of delay (in msec) in sending voice packets. Used to accommodate jitter (or variable delay) in an IP network. If not set properly voice may sound choppy.

Packet Size-The number of voice windows included within HDLC on an IP Packet. It generally reduces packet loss and bandwidth needs, but it will cause some additional delay in voice delivery.

Packet Trace-Used for debug purposes only.

Calculating Jitter and Compression

Calculating the Number of EXTended phones

Using a single ISDN line, you will only be able to extend a maximum of 8 phones using G.729a compression. If you plan to extend more than 8 phones, then you will need more bandwidth, in other words another ISDN Line and another set of ISDN TAs.

The Jitter time should be set to a multiple of the Voice Packet Size Time Equivalent. The Voice Packet Size Time Equivalent is the amount of time, in milliseconds (ms) of the combined voice packets.
For example, if using G729A (where each voice packet is equivalent to 10 ms of time) and have a packet size of 2, then the Voice Packet Size Time Equivalent value is 20 ms (2 packets x 10 ms for a G729A voice packet). We recommended Jitter settings should be multiples of 20 ms.

Minimum Jitter

- IP only: 2 multiples of Voice Packet Size Time Equivalent should be needed
- Sync only: 1 multiple of Voice Packet Size Time Equivalent should be needed

- Async only: 3 multiples of Voice Packet Size Time Equivalent should be needed

The other option is setting the path on the Gateway unit to “Dynamic”. If using dynamic voice you may need to increase the multiple number by one, in turn increasing the Jitter Delay. We recommend using the Dynamic setting for the Async setup to avoid Remote Login problems, due to lack of bandwidth.

Path: Gateway->Configuration->Port->Default->Voice

The following menu appears:

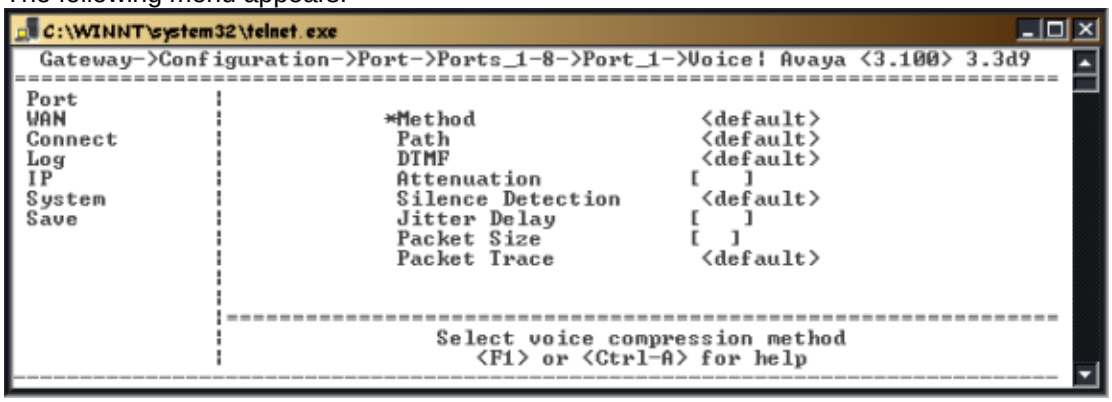


Figure 18: Voice Menu

***Note**: This does not mean that all of the ports can go off-hook and be in use at the same time. Therefore it is recommended, that the path be left at Constant and if you plan to extend more than 10 phones, use two ISDN Lines.*

Procedure

1. Access the Voice Menu for the specific phone port from the main menu using the following path:

   Path: Gateway->Configuration->Port->Default->Voice

   The following menu appears:

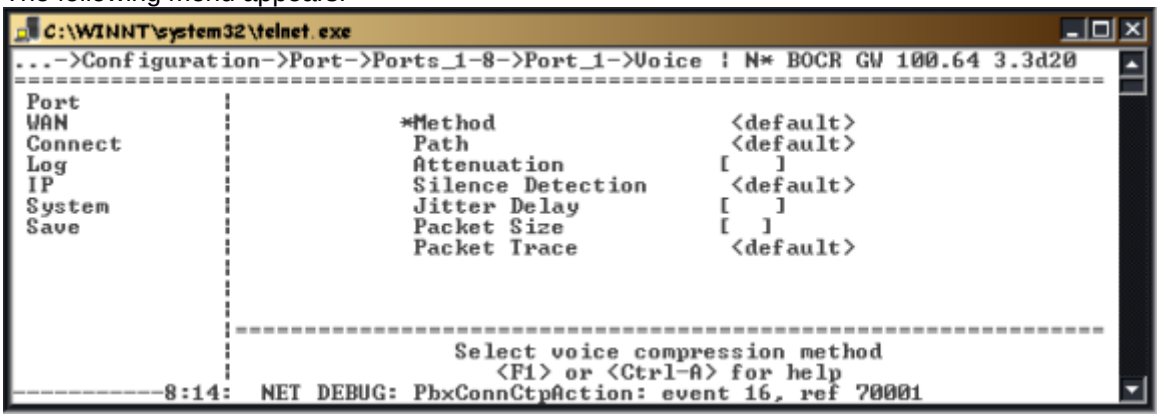


Figure 19: Voice Menu

2. Press the → key to access the **Method** parameter and press the → key to scroll through the various compression methods available.
3. Press the → key to access the **Path** parameter and press the → key to select *Constant* or *Dynamic*.
4. (Avaya Only) Press the ↓ key to the **DTMF** parameter. Select *In-Band* and *Out-of-Band*.
5. Press the ↓ key to the **Attenuation** to limit the amount of echo you may hear during a call.

7. Press the ↓ key to the **Silence Detection.** When enabled, the Gateway detects silent periods during a conversation, and as a result sends no data during these periods. This dramatically reduces bandwidth usage, so this parameter should be *Enabled*.
8. Press the ↓ key to the **Jitter Delay** parameter and set to *20* or greater if using RVP_IP. Otherwise leave at *0*.
9. Press the ↓ key to the **Packet Size** parameter and set to *2*. May need to increase to *4* if using RVP_IP.
10. Press the ↓ key to the **Packet Trace** parameter. Enabling this allows you to trace lost voice packets. This is used for debugging and diagnostic purposes.
11. Press the ← key to accept changes and go back to the Configuration Menu.
11. Press the ↓ key to the **Save** parameter.
12. Press **Enter** to save changes to the active config (.swt) file.

Enabling/Disabling Telephony Ports (Gateway and Remote)

The system administrator can disable unused phone ports through the MI. The following procedure describes the process for disabling individual phone ports.

***Note**: The `Port-><Default>` setting enables all 12 or 8 ports.*

Procedure

1. Access the specific Port Menu from the Main Menu using the following path:

   Path: ->Configuration-> Port->Port 1 through 8 ->Port 1
   The following menu appears:

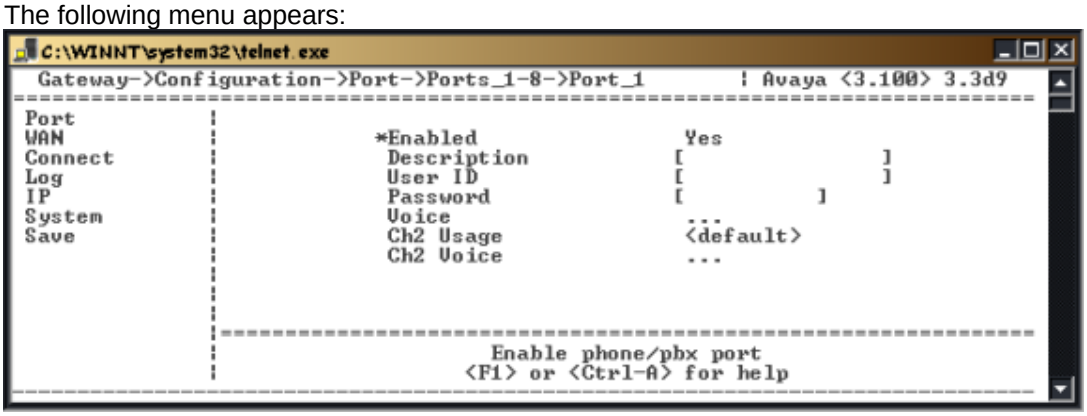


Figure 20: Enabling a Port

2. Press the → key to change the parameter of the port. Choices are: Enabled (**Yes**), or (**No**), or <default>.
3. Press the ← key to accept changes and go back to the Configuration Menu.
4. Press the ↓ key to the **Save** parameter.
5. Press **Enter** to save changes to the active config (.swt) file.

Setting a Connect Password (Gateway and Remote)

A connect password provides an authorized link between the Remote unit and the PBXgateway. A Connect Password restricts access to the phone port and is matched to the User ID. Both must be entered for access.

***Note**: A Connect password is required at the Branch site if the System Administrator has set the password at the PBXgateway.*

Procedure

1. Access the Port Menu from the Main Menu using the following path:

   Path: ->Configuration-> Port->Port 1 through 8->Port 1

   The following menu appears:

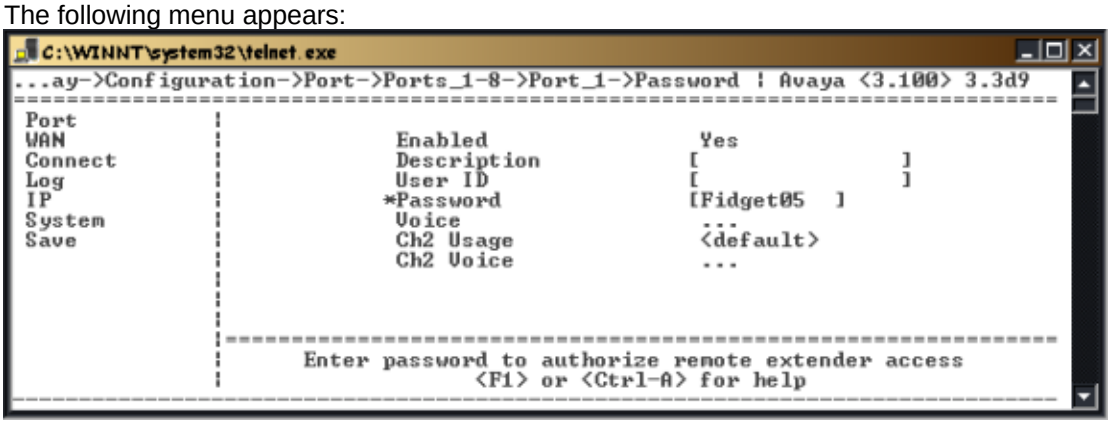


Figure 21: Default Menu

2. Press the → key and ↓ key to access the **Password** parameter.
3. Press the ← key to accept changes and go back to the Configuration Menu.

Assign a connect password (16 characters maximum) using the following guidelines:

Security Alert:

Passwords should be hard to guess and therefore should not contain:

- all the same numbers

  Example: 88888888
  sequential numbers
  Example: 987654321

- number strings associated with you or with the remote user or with your business. These include:

  Birthdays
  Telephone numbers
  Social security numbers

- Passwords should be changed regularly, at least on a quarterly basis. Do not recycle old passwords.

  ***Note**: The Connect password assigned to the Remote unit must match the password assigned by the system administrator, otherwise, each user will be prompted individually for the connect password on their phones (not recommended). Keep the password in a safe place*.

4. Press the ↓ key to the **Save** option and press **Enter**.

Set User ID (Gateway and Remote)

The PBXgateway is wired to 8 or 12 different digital lines on the PBX. Each of these lines reflects a remote user extension. If remote users are connected through different Remote units or EXTenders, it is important to “Map” the extensions to the appropriate remote user. This is accomplished by using a User ID. A User ID is a text field that identifies which user is connected to which digital port on the PBX.

***Note**: User IDs override the Port Matching*.

IMPORTANT NOTE:
By default, ‘Port Matching’ is enabled in the PBXgateway, and Port X (1 -8) on the Remote unit will connect to Port X (1-8) of the PBXgateway (i.e. matching the port number). Also, if a remote user enters a numeric value (1-8) as a User ID on the remote phone, the phone will be connected to that port number of the PBXgateway.

To **override** this 'Port Matching' functionality and enforce the usage of User ID assignment for security purpose; use the following path to disable the 'Port Matching' on the PBXgateway:

Path: Gateway>Configuration>Connect>Port Matching

Procedure

1. Access the specific Port Menu from the Main Menu using the following path:

   Path: ->Configuration-> Port->Port 1 through 8

   The following menu appears:

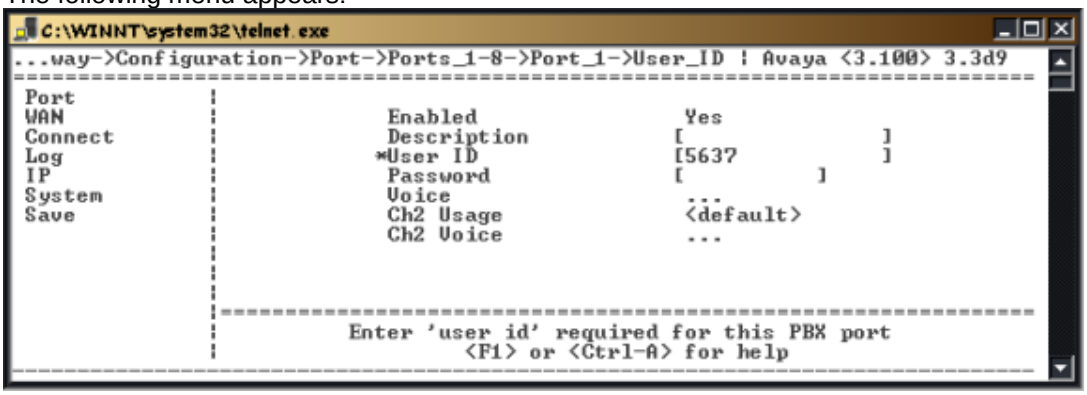


Figure 22: Port Selection Screen

3. Press the → and ↓ key to User ID parameter.

4. Type in the User ID for the port.

   ***Note**: It is recommended that the User ID reflect the phone port, extension, or name of the remote user.*

5. Press the ← key to accept changes and go back to the Configuration Menu.

6. Press the ↓ key to the **Save** parameter.

7. Press **Enter** to save changes to the active config (.swt or .rmt) file.

Set Port Description (Gateway and Remote)

The Description parameter provides 15 characters of text to identify the user or specific port. It is used for administration purposes only.

Example: If Shauna Robar'sextension (5637) is connected to Port 1 on the PBXgateway, the Port Description field for port 1 could be set to: SRobar

Procedure

1. Access the specific Port Menu from the Main Menu using the following path:

   Path: ->Configuration-> Port->Port 1 through 8

   The following menu appears:

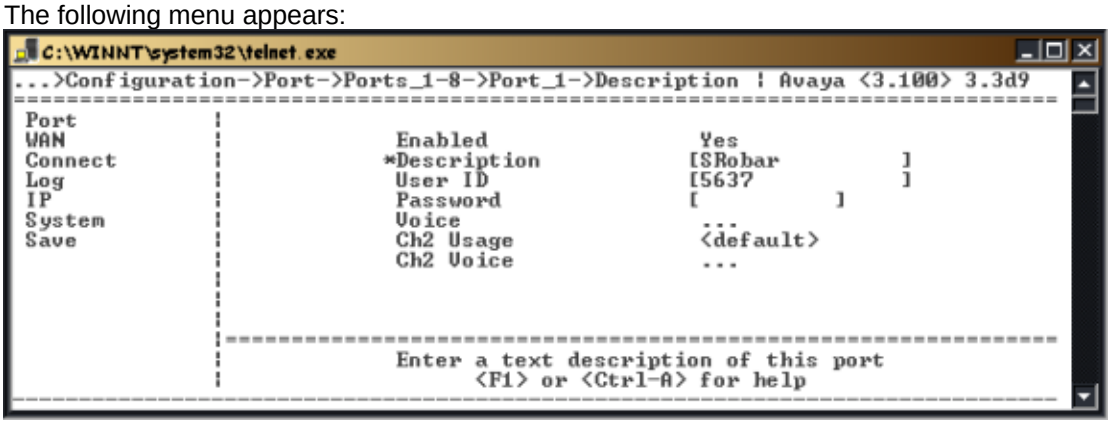


Figure 23: Port Selection Screen

2. Press the → and ↓ key to the Description parameter.

3. Type in the Description for the port.

   ***Note**: It is recommended that the Description parameter reflect the user connected to the specific phone port.*

4. Press the ← key to accept changes and go back to the Configuration Menu.

5. Press the ↓ key to the **Save** parameter.

6. Press **Enter** to save changes to the active config (.swt or .rmt) file.

WAN Port Set up (Gateway and Remote)

Introduction	The PBXgateway and Remote have two WAN ports (WAN 1 and WAN 2) used for a synchronous or asynchronous-serial connection. The ports communicate via an RS-232, RS-530 or V.35 interface and provide the connections to the third party network devices. ***Note**: Used for RVP_Direct only.*
Settings	**Enabling/Disabling WAN ports**- Individually Enable or Disable a specific WAN port. ***Note**: It is recommended that you disable ports not in use.* **Setting the Interface Mode -** Choose the interface signaling type (synchronous or asynchronous) used to communicate with the network device.
Synchronous-Serial	**Setting the Sync Rate** – Sets the specific WAN port to the sync rate (synchronous serial port transfer speed) of the network device (CSU/DSU). (refer to page 71)
Asynchronous-Serial	**Setting the Async Parameters** – Sets the required parameters to match the specific asynchronous device connected to the WAN port.

Enabling/Disabling WAN Ports

Procedure

1. Access the WAN 1 or WAN 2 Menu using the following path:

   Path: ->Configuration->WAN-> WAN 1 or WAN 2

   The following menu appears.

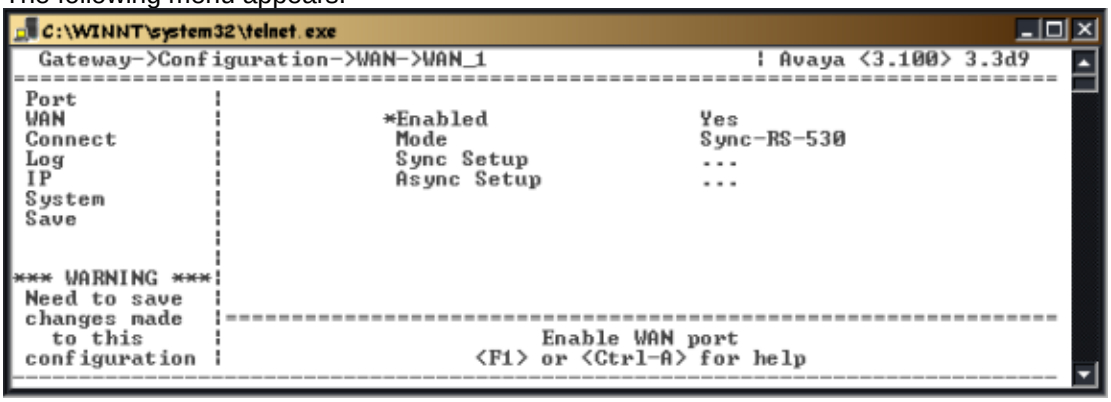


Figure 24: WAN Menu

2. Press the → key to change the availability of the port to: Enabled (**Yes**) or Disabled (**No**).
3. Press the ← key to accept changes and go back to the Configuration Menu.
4. Press the ↓ key to the **Save** parameter.
5. Press **Enter** to save changes to the active config (.swt or .rmt) file.

Setting the WAN Sync Rate (Gateway and Remote)

Procedure

1. Access the WAN 1 or WAN 2 Menu using the following path:

   Path: ->Configuration->WAN-> WAN 1 or WAN 2

2. Press the → key to access the parameters.

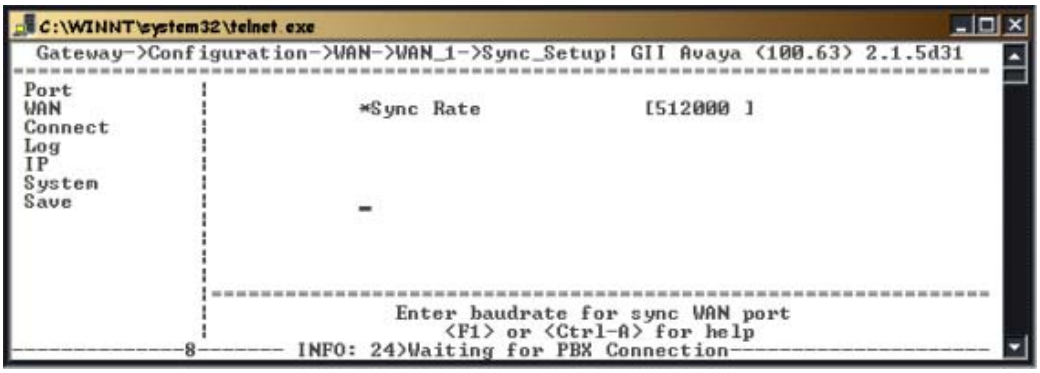


Figure 25: WAN Menu

3. Press the → key to the **Sync Rate** parameter and type in the correct Sync rate. This parameter sets the synchronous data transfer speed of the WAN port and must match the network device speed.

   ***Note**: This Sync Rate information, displayed in bytes, must be obtained through the network device documentation and corresponds to network rate.*

4. Press the ← key to accept changes and go back to the Configuration Menu.

5. Press the ↓ key to the **Save** parameter.

6. Press **Enter** to save changes to the active config (.swt or .rmt) file.

Setting the Mode - Signaling Protocol – (Gateway and Remote)

Procedure

1. Access the WAN 1 or WAN 2 Menu using the following path:

   Path: ->Configuration->WAN-> WAN 1 or WAN 2

   The following menu appears. Press the → key to access the parameters

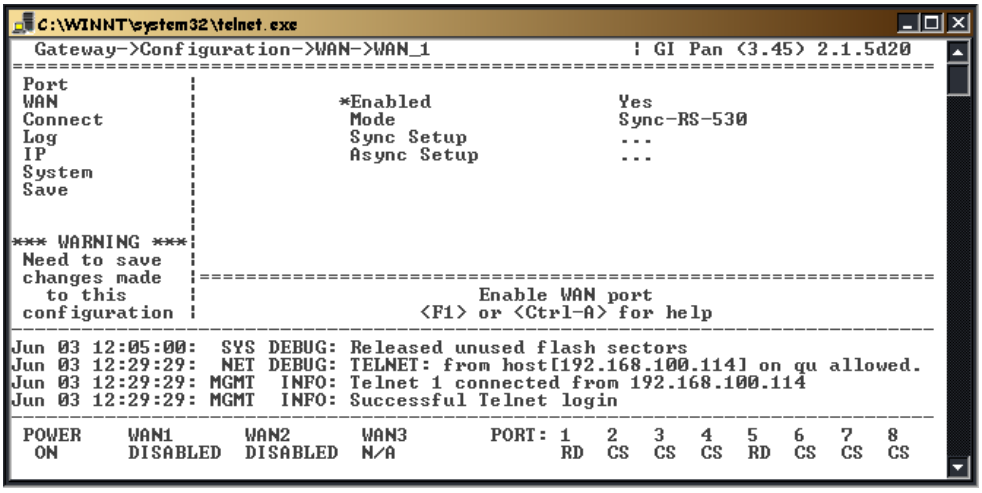


Figure 26: WAN Menu

2. Press the ↓ key to the **Mode** parameter. This parameter must match the protocol (V.35, RS-530, or RS-232) used by the network device connected to the WAN port. Press the → key to scroll through the available protocols.
3. Press the ← key to accept changes and go back to the Configuration Menu.
4. Press the ↓ key to the **Save** parameter. Press **Enter** to save changes to the active config (.swt) file.

Setting the Async Parameters (Gateway and Remote)

Procedure

1. Access the *WAN 1* or *WAN 2 Menu* using the following path;

   Path: ->Configuration->WAN 1 or 2->Async_Setup

   The following menu appears.
2. Press the → key to access the parameters.

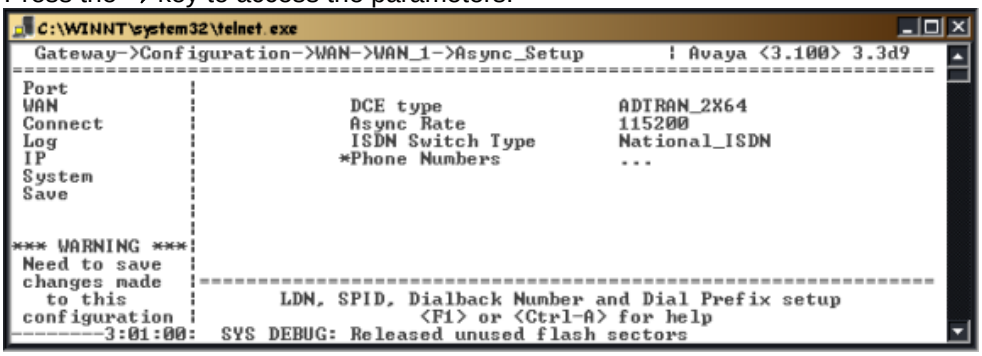


Figure 27: Async_Setup Menu

3. Press the → key to the **DCE Type** parameter. Press the → key to select the network device being used. A list of recommended devices is in the table below.

TA's (for Async)	**MFG**	**Model(s) (see note)**
	Motorola	Bitsurfr Pro Bitsurfr Pro EZ
	Adtran	ISU 128 (see note) ISU 2X64 Express 3000 Express NTU
	3Com	ISDN TA
TA's (for Sync 128k bonding)	Motorola	Bitsurfr Pro
	Adtran	ISU 128 (see note) ISU 2X64
CSU/DSU's	Paradyne	Acculink 3165 7110 SNMP
	Adtran	TSU LT
	General DataComm	DeskTop 554A
	RAD	FCD-1L
	ADC Kentrox	DataSmart Max 72761, 78640
	Motorola	FT100S
	Larscom Orion	56/T1

Table 13: DCE Models

***Note**: In order for the Async-RS 232 Dial feature to work properly for these devices, you need to set each device to "RS232", and setup each device to accept incoming "AT Commands". Consult the documentation provided with each device for proper instructions.*

4. Press the ↓ key to the **Async Rate** parameter. This parameter sets the asynchronous data transfer speed of the WAN port and must match the network device speed.

   ***Note**: This Async Rate should be left at the <default> setting of 115200.*

5. Press the ← and ↓ key for each of the Phone Numbers parameters.

   ***Note**: Press the → key to enter the appropriate information provided by the system administrator.*

   ISDN Switch Type parameter. Select the type of Central Office (CO) switch being used for the ISDN connection.

   Local Dialing Num1 parameter. Enter the DN 1 number assigned to the ISDN line.

   ISDN SPID 1 parameter. Enter SPID 1assigned to the first ISDN B-channel.

   Local Dialing Num2 parameter. Enter the DN 2 number assigned to the ISDN line.

   ISDN SPID 2 parameter. Enter SPID 2 assigned to the second ISDN B-channel.

   Dial Prefix parameter. Enter the dial prefix for outgoing calls on this WAN port.

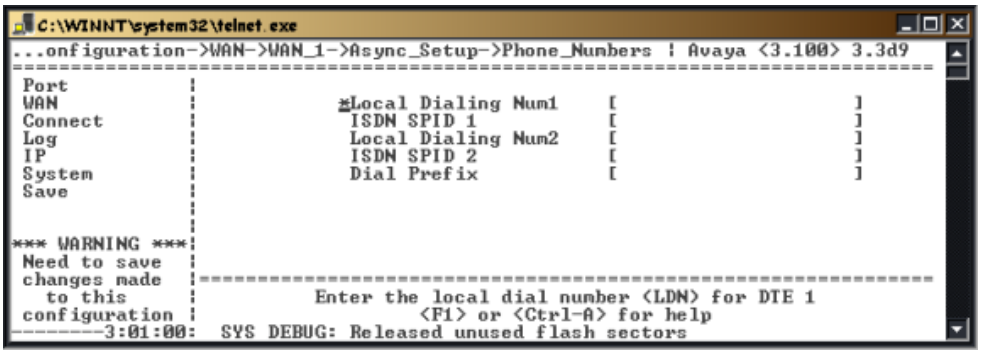


Figure 28: Async_Setup – Phone_Numbers

6. Press the ← key to accept changes and go back to the Configuration Menu.
7. Press the ↓ key to the **Save** parameter. Press **Enter** to save changes to the active config (.rmt) file.

Problems with Remote Login from Gateway – Async Setup

Problems may arise with the Async setup when attempting to perform a Remote login from the Gateway, when Call Suspend has been enabled.

To allow for Remote Login from the PBXgateway, ensure that Silence Detection is enabled and the Path is set to **Dynamic**. If set to Constant, there is not enough bandwidth available for the remote login to occur.

***Note**: Only use Constant for selected ports that must always have voice path available, this will limit how many ports you can extend and could prevent being able to Rlogin.*

Path: Gateway->Configuration->Port_X-Y->Port_X (or Default Port)->Voice

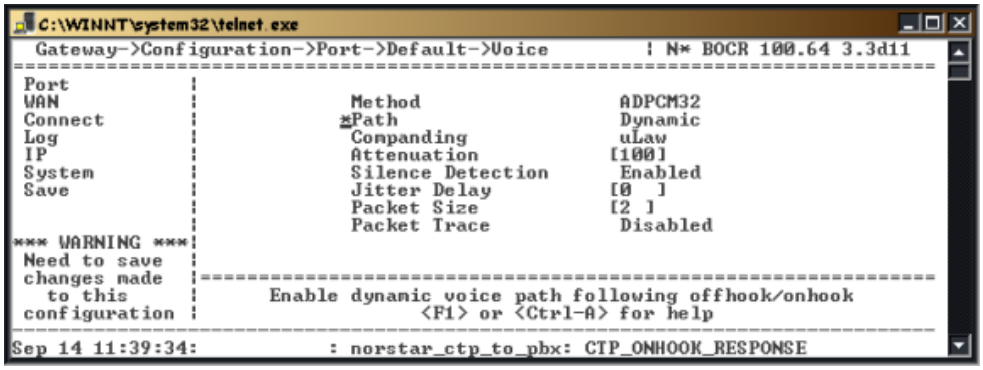


Figure 29: Async Remote Login Settings

Setting the IP Parameters (Gateway and Remote)

IP Address Parameters

An Internet Protocol (IP) address and associated routing parameters must be entered within the IP menu to locate the PBXgateway on the LAN (Local Area Network) over an IP connection. This is required to manage the PBXgateway using Telnet or to configure the PBXgateway to use RVP_IP.

***Note**: The IP address (as well as any required mask or router addresses) must be provided by the network administrator.*

Procedure

1. Access the IP Menu using the following path;

   Path: ->Configuration->IP ->Address

   The following menu appears:

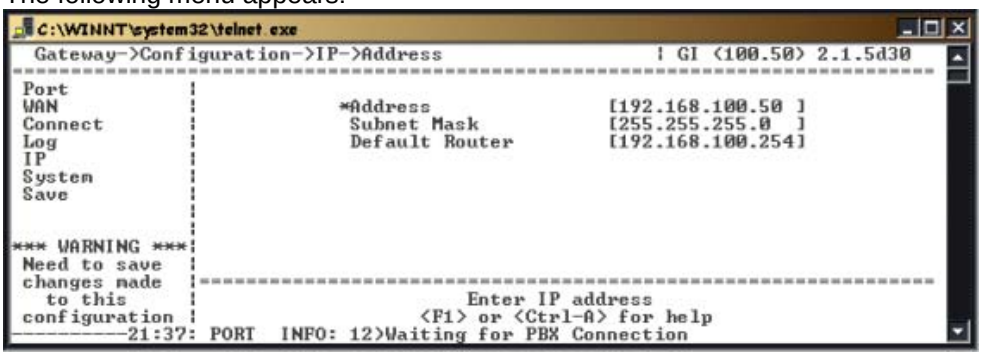


Figure 30: Address Menu

2. Press the → key to access the parameters

   ***Note**: The following parameters must be assigned by the network administrator.*

3. Press the → key to the **Address** parameter. Enter the IP Address of the PBXgateway and press **Enter**.

4. Press the ↓ key to the **Subnet Mask** parameter. Enter the IP Address of the Subnet Mask and press **Enter**.

5. Press the ↓ key to the **Default Router** parameter. Enter the IP Address of the Default Router and press **Enter**.

6. Press the ← and ↓ key to the Save option.

7. Press Enter to save changes to the active config (.swt) file.

Rlogin & Login via IP (Gateway and Remote)

This parameter allows for Remote Login Access from another EXTender or Gateway unit, assuming that both units are active. Rlogin will use whatever the connect type has been set to. Alternatively you may use the Login via IP feature to log into an EXTender by specifying the Remote's IP address. This IP address is configured in the IP menu.

Procedure

1. Access Rlogin configuration using the following path:
   Path ->Configuration->IP

2. Press the ↓ key to select Rlogin.

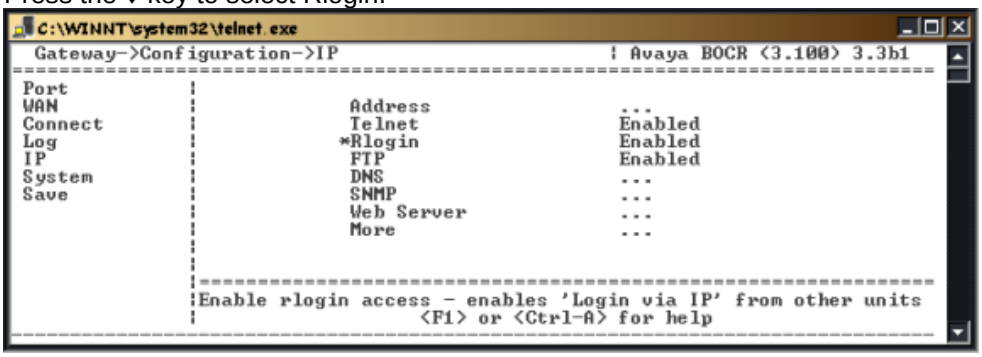


Figure 31: Rlogin

2. Press the → key to toggle between Enabled and Disabled.
3. Save your changes.

Using Rlogin

1. From the main menu select Remote Login. A list of remotes will appear.

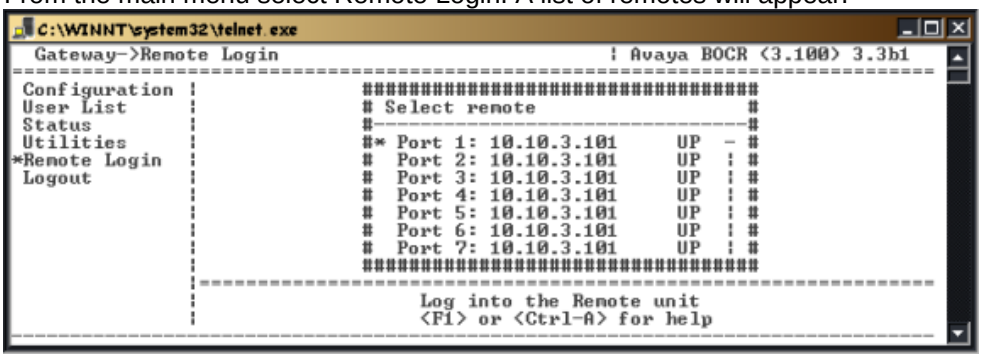


Figure 32: Remote Login

2. Use the ↓ to select a remote and press Enter.

Telnet/FTP Set up (Gateway and Remote)

The PBXgateway can be configured through a Telnet session and files can be saved or retrieved through an FTP session.

Telnet
By default, Telnet is Enabled. Disabling it will prevent anyone from accessing the unit through Telnet.

FTP
By default, FTP is disabled. Disabling it will prevent anyone from saving files to or retrieving files from the unit through FTP. This is normally done to upgrade the unit's software.

Enabling/Disabling Telnet

1. Access the IP Menu from the Main Menu using the following path:

   Path: ->Configuration->IP
   The following menu appears:

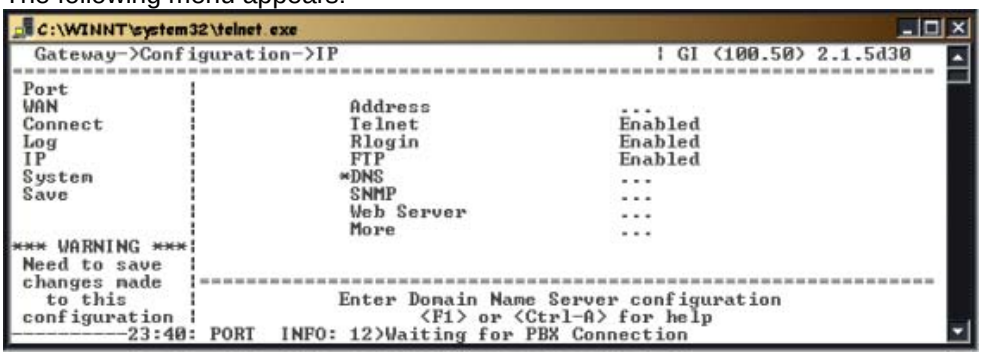


Figure 33: Telnet/FTP

2. Press the → and ↓ key to the **Telnet** parameter. Toggle the **Telnet** parameter between Enabled and Disabled.

3. Press the ← key to go accept changes and go back to the Configuration Menu

4. Press the ↓ key to the Save option.

5. Press **Enter** to save changes to the active config (.swt or .rmt) file.

Web Server Set up

Configure the PBXgateway using a standard web server over an existing LAN connection. This feature provides the system administrator complete management capabilities as well as status information for both WAN and PORT connections.

IMPORTANT:
All IP parameters for the Remote must be configured before the web server session can be established. The Remote must be connected to the LAN via the LAN port. The Remote must be powered up and online.

Procedure

1. Access the Management Interface (MI) using a Telnet session or via the Console Port.

2. Access the Web Server parameter using the following path:

   Path: Configuration->IP->Web Server

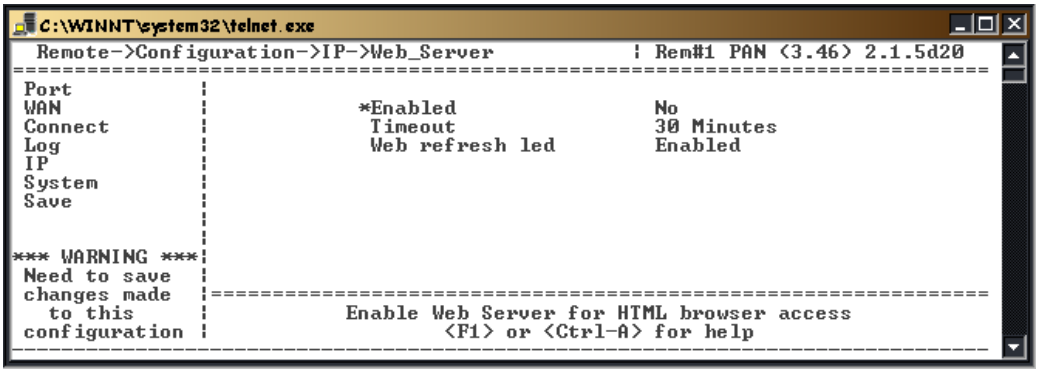


Figure 1: Enabling the Web Server

3. Select **YES** for Enabled. Set the Timeout to **30**.

4. Save the settings and Log out.

Enabling/Disabling FTP (Gateway and Remote)

1. Press the → and ↓ key to the **FTP** parameter. Toggle the **FTP** parameter between Enabled and Disabled.

2. Press the ← key to go accept changes and go back to the Configuration Menu

3. Press the ↓ key to the Save option.

4. Press Enter to save changes to the active config (.swt or .rmt) file.

DNS Set up (Gateway and Remote)

The Domain Name System (DNS) is used in IP networks for translating host domain names (ie: MCK.com) into IP addresses. Basically, if you are not sure of the IP address of the device you are trying to connect to, and there is a DNS server on the network with DNS enabled, simply type in the name of the device and the IP address will be displayed.

Settings The following DNS settings are required:

Enabled- This simply enables or disables the parameter.

Server IP Address – This is the IP Address of the DNS. Used to resolve names to IP addresses.

Domain Name – Name assigned to the network subnet on which the DNS server resides.

***Note**: At this time, DNS is not required for any PBXgateway or Remote unit operation. Therefore, we recommend leaving this parameter disabled.*

Enabling/Disabling DNS (Gateway and Remote)

1. Access the IP Menu from the Main Menu using the following path:

   Path: ->Configuration->IP -> DNS
   The following menu appears:

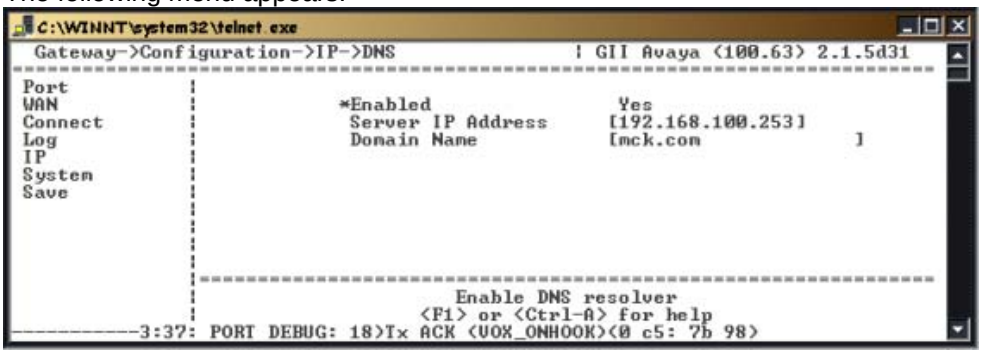


Figure 34: DNS Menu

2. Press the → key to the **Enabled** parameter. Enabled (Yes) or (No).

3. Press the → and ↓ key to the **Domain Name** parameter. Type in the name of the domain that the PBXgateway belongs to. Example: MCK.com

   ***Note**: The Domain name must be provided by the network administrator*.

4. Press the and ↓ key to the **Server IP Address**. Type in the address of the server that the PBXgateway belongs to.

   ***Note**: The Server IP Address must be provided by the network administrator.*

5. Press the ← key to go accept changes and go back to the Configuration Menu. Press the ↓ key to the **Save** option.

6. Press Enter to save changes to the active config (.swt or .rmt) file.

System Parameters

Assign a Name to the Unit (Gateway and Remote)

The MI provides a means of identifying the Gateway/EXTender on the network. This procedure explains the method of assigning a name to the PBXgateway for identification purposes.

***Note**: This name is used strictly for ID purposes only. It is not an IP host name.*

Procedure

1. Access the System Menu from the Main Menu using the following path:

   Path: ->Configuration->System

   This is where the name of the Gateway is displayed.

   The following menu appears:

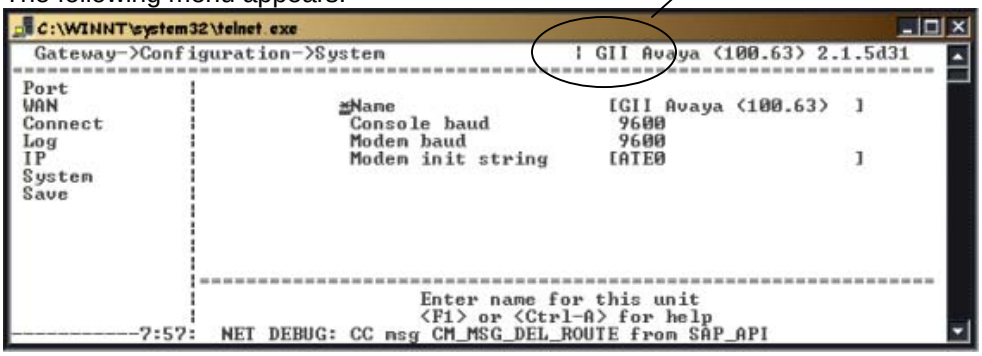


Figure 35: System Menu

2. Assign a Name to the PBXgateway continued
3. Press the → key and type in a name for the PBXgateway.

   ***Note**: The name must not exceed 20 characters*.

4. Press the ← key to accept changes and go back to the Configuration Menu.
5. Press the ↓ key to the **Save** parameter.
6. Press Enter to save changes to the active config (.rem or .swt) file.

Console Baud (Gateway and Remote)

The Console Baud is the speed at which information is transmitted to and from the PBXgateway/EXTender through the console port (DB-9) located on the front of the unit.

***Note**: This setting must match the baud rate of the PC serial port connected to the console port.*

Gateway Procedure

1. Access the System Menu from the Main Menu using the following path:

   Path: ->Configuration->System

   The following menu appears:

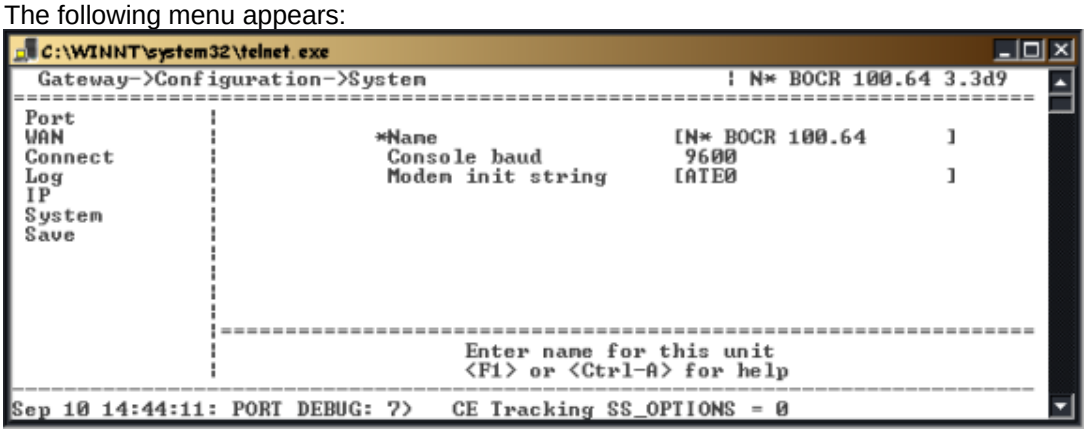


Figure 36: System Menu

2. Press the ↓ key to the **Console Baud** parameter.
3. Press the → key to modify the setting. The <Default> setting is 9600.
4. Press the → key to the **Modem Init String**. This is the AT Command used to initialize the modem.
5. Press the ← key to accept changes and go back to the Configuration Menu.
6. Press the ← key to the **Save** parameter.
7. Press Enter to save changes to the active config (.swt) file.

System Parameters - Remote Only

1. Access the System Menu from the Main Menu using the following path:

   Path: Remote->Configuration->System

   The following menu appears:

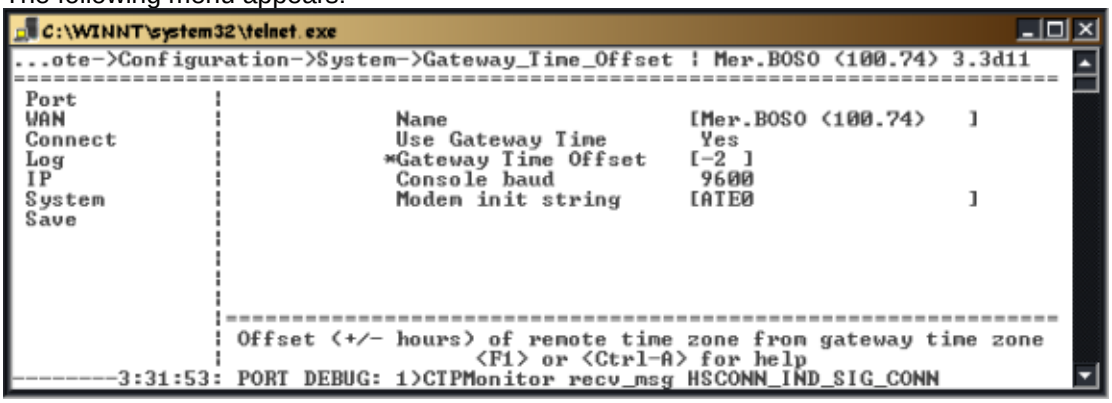


Figure 37: Gateway Time Offset - Remote System Menu

2. Select **Use Gateway Time**. When enabled [Yes], the EXTender will use the PBXgateway time to stamp all logging once connected to the PBXgateway.

3. Enter a value the represents the ***time difference*** between the Remote and the PBXgateway. This is used to compensate for a time difference between cities. For example the Gateway is at a corporate office in Boston and the Remote is in Calgary. Set the value to -2. A call made from Boston to Calgary at 10:00am central time will show up as 8:00am mountain time. This will ensure that the time stamp on logs as well as the time appearing on your phone set will be correct.

4. Press the ↓ key to the **Console Baud** parameter. Press the → key to modify the setting. Note: The <Default> setting is 9600.

5. Press the → key to the **Modem Init String**. This is the AT Command used to initialize the modem.

6. Press the ← key to accept changes and go back to the Configuration Menu.

7. Press the ← key to the **Save** parameter.

8. Press Enter to save changes to the active config (.rmt) file.

Utilities (Gateway and EXTender)

Setting the Date (Gateway and EXTender)

The Real Time Clock (RTC) provides an accurate date/time stamp for log messages and statistics used in the Management Interface (MI) in both the Remote and Gateway. The time is displayed using a 24 hour clock.

Example:
Date: September 10, 2004
Time: 14:49:24 (no a.m. or p.m.- 24 hour clock)

Procedure

1. Access the Set Date Menu from the Main Menu using the following path:

   Path: ->Utilities->System->Set date

   The following menu appears:

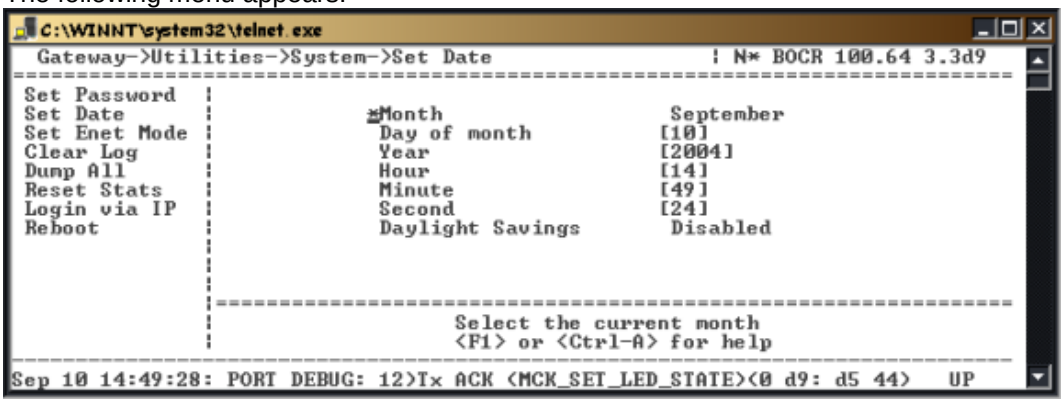


Figure 38: Set Date Menu

2. Press the ↓ key to access each parameter and fill in the appropriate information as required.

   ***Note**: Press the → key to scroll through the choices for Month*.

3. Press the ← key to accept changes and go back to the **System** menu.

   ***Note**: The PBXgateway and EXTender 6000 preserve their date and time even when power is lost. The EXTender 4000 will lose its date and time after loss of power but will retain it once it connects to a Gateway.*

Set Enet Mode (Gateway and EXTender)

The Set Enet Mode parameter on the Gateway and Remote allows you to select the AUX LAN or LAN mode.

Procedure:

1. Select **Set Enet Mode** using the following path:
   Path: Utilities->System->Set Enet Mode

2. The LAN setting will be displayed. Hit Enter to continue.
3. Set LAN Mode to either 10 Mb-Half Duplex, 100 Mb-Half Duplex or Auto.

Setting the Administrator's Password (Gateway and EXTender)

How the administrator password work

The administrator password provides access to the Management Interface (MI). It is very important to set up an initial administrator password because the units are shipped without one programmed. You should set an administrator's password for both the Branch Office unit and PBXgateway for security reasons.

Security Alert:

Administrator Password Guidelines

Passwords should be hard to guess and therefore should not contain:

all the same numbers or characters

Example: 88888888 or aaaaaaaa

sequential numbers or characters

Example: 987654321 or abcdefg

number strings associated with you or with the remote user or with your business. These include:
Birthdays
Telephone numbers
Social security numbers

Passwords should be changed regularly, at least on a quarterly basis. Do not recycle old passwords.

Procedure

1. Select Set Password from the Main Menu using the following path:

Path: ->Utilities->System->Set Password

You will be prompted to enter the **Old Password.** Note that there is no default admin password.

2. Press **Enter**. You will be prompted to enter the **New Password.**
3. Assign an administrator password keeping the length of password to 16 characters.
4. Type in New password and Press Enter.
5. You will be prompted to confirm the **New Password,** press **Enter.**
6. When the password has been changed, "Password changed" appears on the screen.
7. Press the ← key to go back to the **System** Menu.

***Note**: Write the password down, and keep in a secure place.*

Resetting Ports (Gateway and EXTender)

There may be times when a port, or all the ports have to be reset on the EXTender 6000. Resetting ports may cause damage to the older phones as the voltage parameters for older versus new phones differ.

Remote Only: To reset port on a remote that has a variety of older and newer models, unplug all phones. Not doing this will result in damage to the phones. ***Note****: This applies to the Remote unit only.*

Procedure

1. Login into the Extender or Gateway.
   Path: →Utilities→Diagnostics→Reset Port

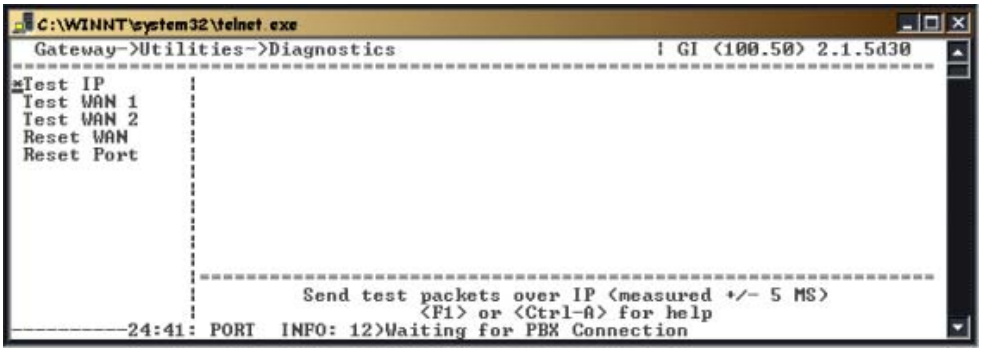


Figure 39: Diagnostic Menu

2. Press → and enter an individual port number or type in 'all'.

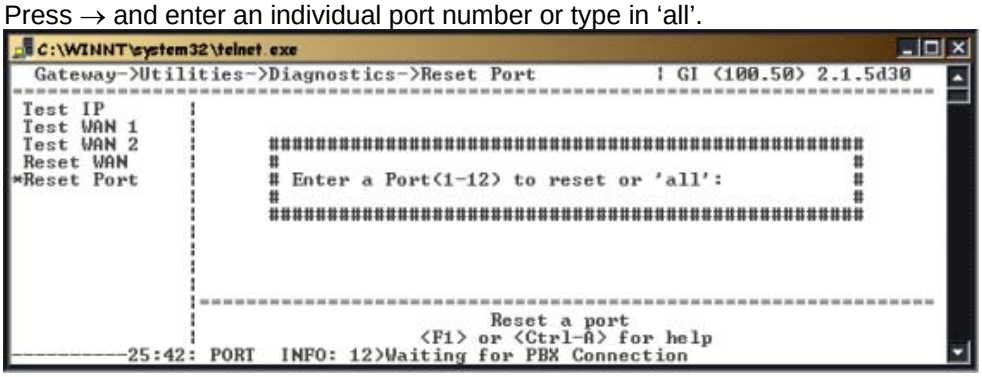


Figure 40: Reset Port

3. Press Enter. A warning appears telling you that *"All connections on all ports will be lost"* or if you selected a single port to reset *"All connections on Port_x will be lost".*

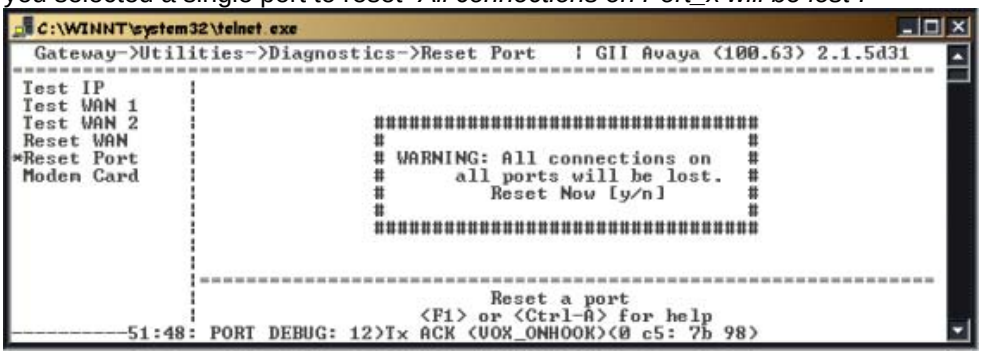


Figure 41: Reset Port - Warning

4. Enter Y if you are prepared to lose connections on all ports. It is best to perform this task during business down hours.

Optional PBXgateway Parameters

The following pages describe helpful but optional parameters. Refer to these parameters when needed.

2:1 Configuration

Included in this release is the ability to connect two EXTender 6000 remote units, using RVP_Direct to the two WAN ports of the PBXgateway.

Typical Installation

The first EXTender 6000 is connected to WAN1 of the PBXgateway. The second EXTender 6000 is connected to WAN2 of the PBXgateway. This must be the configuration; otherwise warning log messages will be logged.

Configuring the Gateway and Remote

1. In the "RVP_Direct" menu, set the *Number of Remotes* to [2].

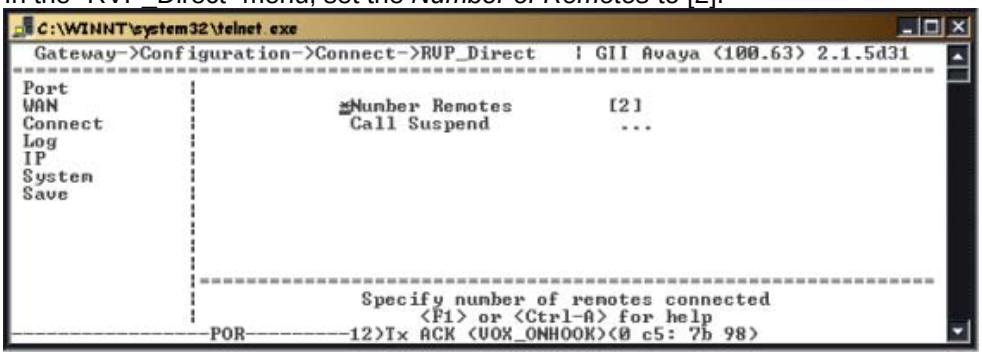


Figure 42: Number of Remote in 2:1

2. In the "WAN 2" menu, enable WAN 2.
3. Set the WAN Mode. See page 70.
4. Set the Sync Setup parameters. See page 71.

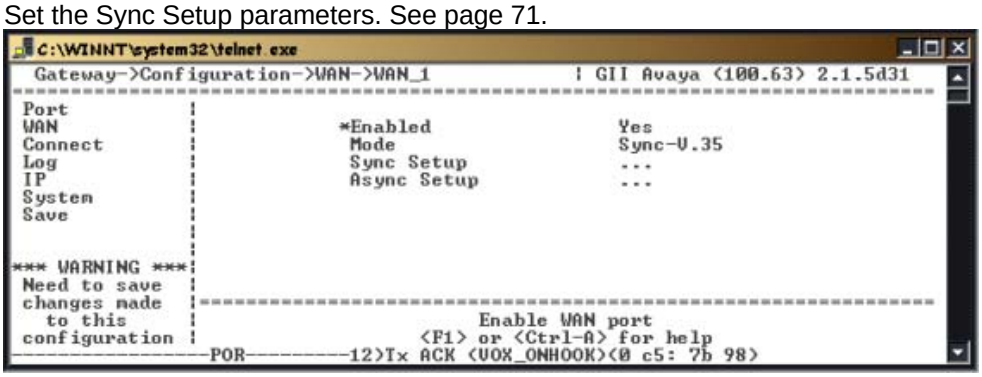


Figure 43: Enabling WAN

3. Reboot the PBXgateway.

***IMPORTANT**: You cannot "Rlogin" to either remote unit until each remote has at least one phone connected. And WAN stats shows Active.*

Configuring the Remote Units (RVP_Direct)

When configuring the remote units for 2:1 operation, you need to set the **Remote Number** and **Gateway Port Offset** parameters correctly.

For example, if you are using two 8-user remotes, PBXgateway ports 1 through 8 will be for the first unit, and ports 9 through 16 will be for the second remote.

1. When configuring the first remote unit, set the **Remote Number** parameter to 1.
2. When configuring the second remote unit, set the **Remote Number** parameter to 2, and set the **Gateway Port Offset** parameter to 8.

   Path: Remote ->Configuration -> Connect -> Gateway Port Offset

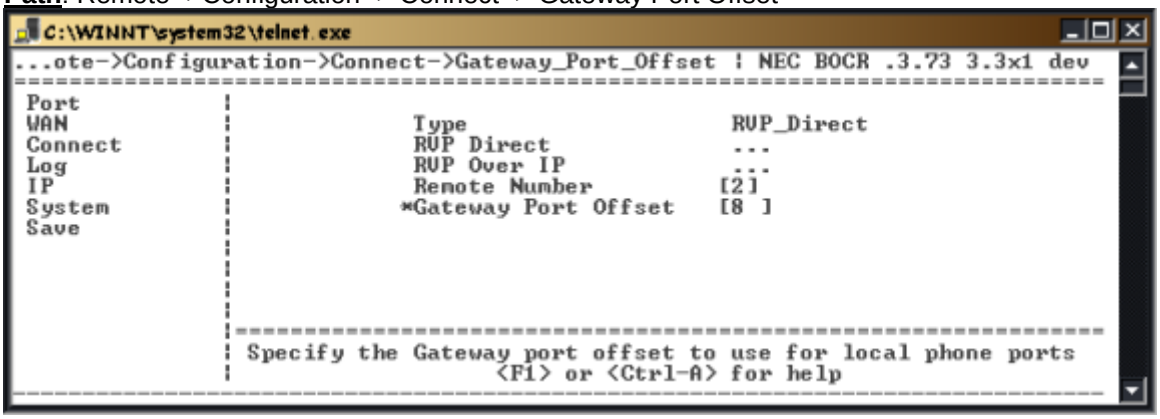


Figure 44: Gateway Port Offset

3. After rebooting the units, ports 9 through 16 from the PBXgateway will be assigned to the second remote unit.
4. Set the Port Compression for WAN 1 and WAN 2 to provide adequate bandwidth for the phones extended off of each remote. Default setting ADPCM32.
   Gateway ->Port->Default->Voice

Determining Compression for 2:1 Configuration

The best voice quality is achieved by using the ADPCM 32 compression. The maximum quality comes at the expense of the highest utilized bandwidth. The largest voice compression is achieved by using G.729A. If you are using this algorithm, you will save on bandwidth and still achieve voice quality that is regarded as near toll. If absolute conversation quality is your focus and bandwidth is no object, you probably want to select ADPCM 32. If bandwidth is a priority you will employ G.729A.

The compression for both WAN ports does not have to be the same. WAN1 may have 4 phones extended, while WAN2 may have 8. Set the Method (Compression) for each port, or use the default port menu.
If you are using different compression algorithms for each individual user (port), use the following formula to establish your aggregate data bandwidth needs.

A x 16 + **B** x 32 + **C** x 40 = **D**

A: number of G.729A Users
B: number of ADPCM 24 Users
C: number of ADPCM 32 Users
D: Total Bandwidth

Divide this bandwidth by either 64 or 56, in order to establish the correct number of DS0 channels to be used.

Example: If your DS0s on your CSU/DSUs are set up for 56Kbps, use 56 and if they are set up for 64Kbps DS0s, use 64.

Configuring the Remote Units (RVP_Over_IP)

When configuring the remote units for 2:1 operation, you need to set the **Remote Number.** With RVP_Over_IP instead of using the Gateway Port Offset parameters to distinguish ports on each remote the Port User ID's may used as well, to determine what ports on the Remote will match up to what ports on the Gateway.

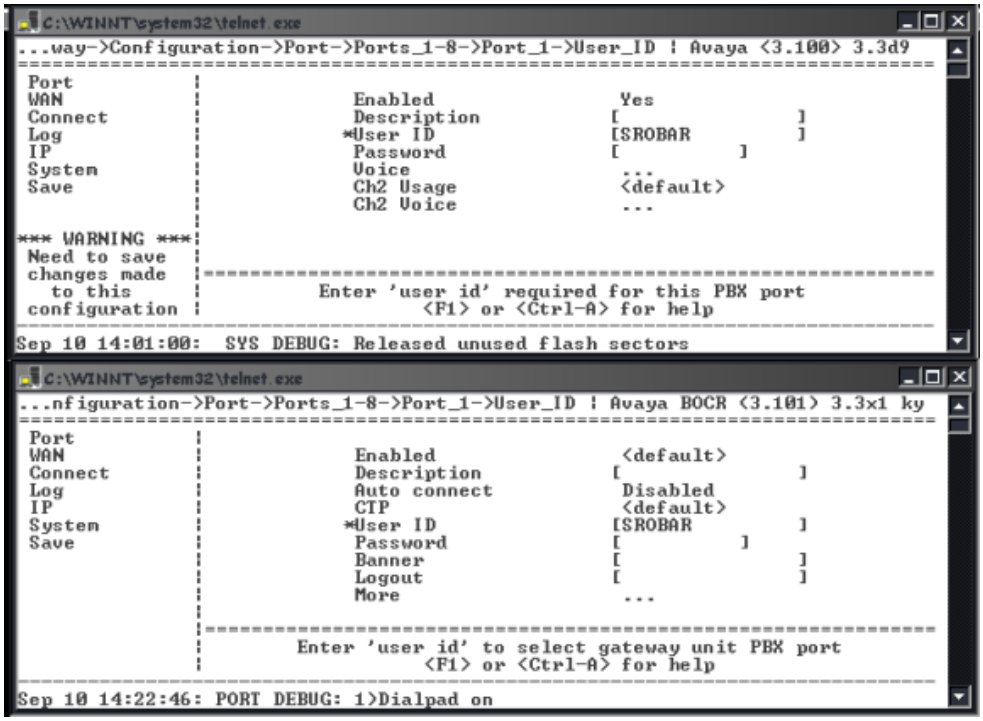


Figure 45: User IDs – 2:1 RVP_Over _IP

***Note**: Remote User ID's must match Gateway User ID's.*

Simultaneous Direct and Telnet Connections to the MI

The PBXgateway/EXTender now supports the configuration that combines the use of RVP and RVPoIP. In this configuration it will be possible to connect Branch Office EXTender remote modules using RVP and have other client modules connected to the same PBXgateway using RVPoIP, simultaneously.

Dial-Up Management Console and Modem Support (Gateway and Remote)

The PBXgateway software supports the Zmodem protocol on the Management Interface console port. Support for this protocol will allow software upgrades to be uploaded into a PBXgateway/Branch unit through the console port. Included is support for accessing the Management Interface on the PBXgateway and EXTender 6000 units through a dial-up modem connected to the DB9 console port. The system administrator can access the Management Interface by dialing into a Fax modem over an analog phone line. The modem is connected to the Branch/PBXgateway via a non-standard DB25 to DB9 cable, which will allow the administrator to log into the Management Interface and access the full functionality of the MI. When the system administrator has finished using the MI they may log out and disconnect, or simply disconnect the connection, which will automatically log them out of the MI.

***Note**: Refer to the PBXgateway Installation Guide for more information on setting up the Dial-Up Management Console.*

Zmodem Connection

The PBXgateway Modem port provides connectivity to a Zmodem for remote configuration. This connection allows access to all features and functions of the MI and the ability to configure, monitor and troubleshoot the unit from a remote location.

Required Cable

RS-232, DB25 to DB9 modem cable [male-male] (see pinout information, below). Use this cable to connect the modem to the modem port on the front of the unit.

Modem Connection

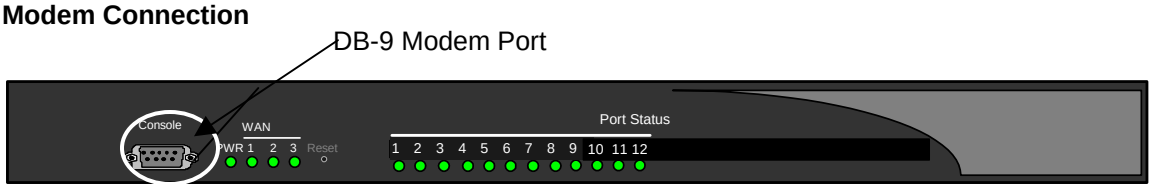


Figure 46: DB-9 Modem Port

Modem Pinout Information

DB25 Male		DB9 Male	
Pin	**Function**	**Pin**	**Function**
2	Tx	2	Rx
3	Rx	3	Tx
7	Common	5	Common
8	DCD	7	RTS
20	DTR	8	CTS

Modem DIP Switch (Gateway and Remote)

The modem used for remote access may have a DIP switch located somewhere on the outside of the unit. This switch controls modem functionality. Below is an example of the settings required for a US Robotics 33.6 Fax modem (not supplied). These switches must be set prior to installation.

Table 14: (US Robotics 33.6 Fax Modem) DIP Switch Settings

Switch #	Function	Setting	Description
1	DTR Normal mode	UP	Computer must provide DTR signal for modem to accept commands: dropping DTR terminates a call.
2	Verbal result codes	UP	-
3	Display result codes	DOWN	-
4	No echo on offline commands	DOWN	Suppress echo.
5	Auto answer ON	UP	Modem answers on first ring, or higher.
6	Carrier Detect (CD) normal	UP	Modem sends CD signal when it connects with another modem, drops CD on disconnect.
7	Load HVRAM Defaults	DOWN	Not used for modem connection to MCK equipment.
8	Smart Mode	DOWN	Reads network settings.

Modem Connection Procedure

1. Connect the analog phone line to the modem.

2. Plug the modem cable (provided with the modem) into the back of the modem.

3. Power-up the modem. The modem will run through a series of self-diagnostic tests.

4. Plug the other end of the modem cable into the port labeled “Console” on the front of the PBXgateway.

5. The modem status LED for “Data Terminal Ready” should be lit RED indicating the modem is ready to receive data.

   ***Note**: Refer to the Modem User’s Guide for specific LED information.*

Type of Service Support

The PBXgateway software supports the Type of Service packet prioritization protocol. When an EXTender is running in RVPoIP mode the system administrator can choose to use Type of Service to prioritize voice packets within the network (note that all nodes in the network must be configured to prioritize traffic based on Type of Service in order for this feature to function properly).

Each RVPoIP voice packet contains a ToS (type of service) byte. Within this byte are three bits, which are the class of service field. The class of service field is always automatically set to low delay for RVPoIP voice packets by the EXTender. Also within the ToS byte are three bits for Differentiated Services. With the Type of Service implementation the system administrator is given the option of choosing how the 3 Type of Service bits are set. These bits will tag the traffic among other packets that have the class of service field set to low delay, according to the way the customer has configured their network to prioritize Type of Service traffic.

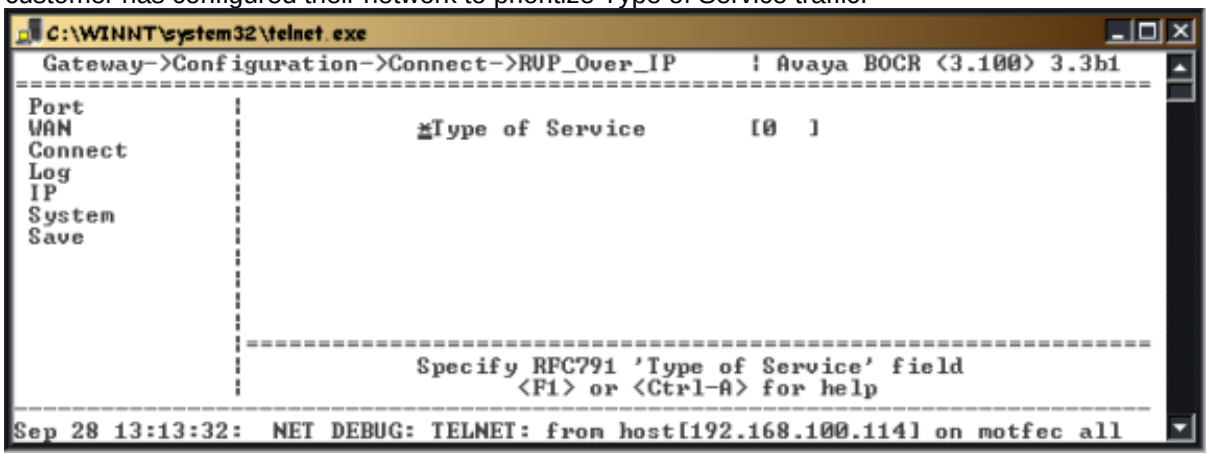


Figure 47: Type of Service

Setting up Call-Suspend (Gateway and Remote)

The Call Suspend feature allows the telecom manager to reduce communication costs by bringing down the ISDN/IP connection when all phones are inactive for a configurable period of time. When the line is disconnected the phones indicate that they are in the Call Suspend mode. Whenever a user goes off-hook or an incoming call occurs, the ISDN/IP connection is brought back up and all phones are taken out of Call Suspend mode.

The Call Suspend feature operates with the assumption that if the ISDN connection is brought down, it is possible to get busy signals from the ISDN/IP network preventing the EXTenders from communicating and causing an interruption of telephone service to the branch office. This assumption leads to setting the Call Suspend timer to a value that does not allow the ISDN/IP connection to go down during normal business hours.

The expected usage pattern for the ISDN/IP connection is that at the beginning of the business day, the phones are brought out of Call Suspend mode bringing up the IDSN/IP connection when the first user either goes off-hook or an incoming call arrives. The ISDN/IP connection remains up for the remainder of the business day because all phones are not idle longer than the Call Suspend timeout value. At the end of the day, all phones become inactive for the Call Suspend timeout value and the ISDN/IP connection is brought down. If anyone works late or comes in early, normal usage brings up the ISDN/IP connection again.

Procedure for Avaya and Meridian (Gateway and Remote)

***Note**: When using an RVP_Direct connection, and Call Suspend is enabled, all ports will have call suspend enabled. If using and RVP_Over_IP connection Call Suspend can be enabled on a port-by-port basis.*

1. Access the *Call_Suspend Menu* using the following path;

   Path: Remote->Configuration->Connect->RVP_Direct->Call_Suspend
   Path: Remote->Configuration->Connect->RVP_over_IP->Default_Port

   Or for individual ports:
   Path: Remote->Configuration->Connect->RVP_Direct->Port_x-y->Port_x

   The following menu appears.

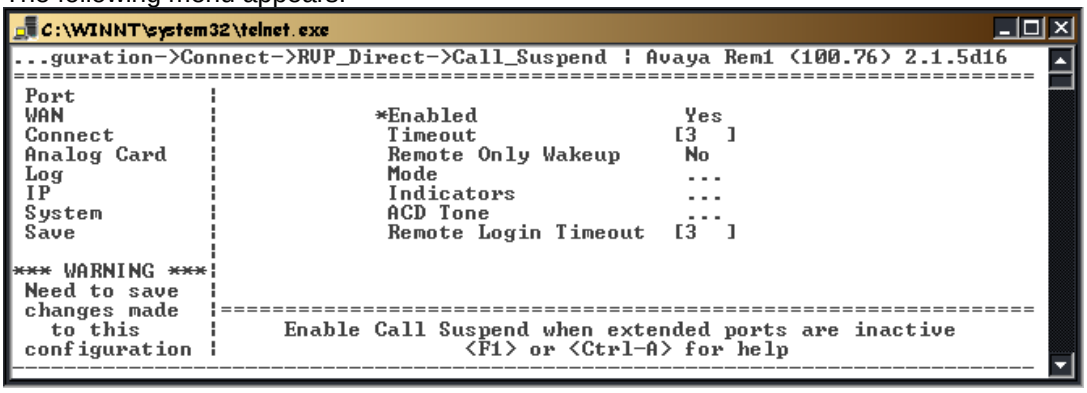


Figure 48: RVP_Direct Call Suspend

2. Press the → key to access the parameters.

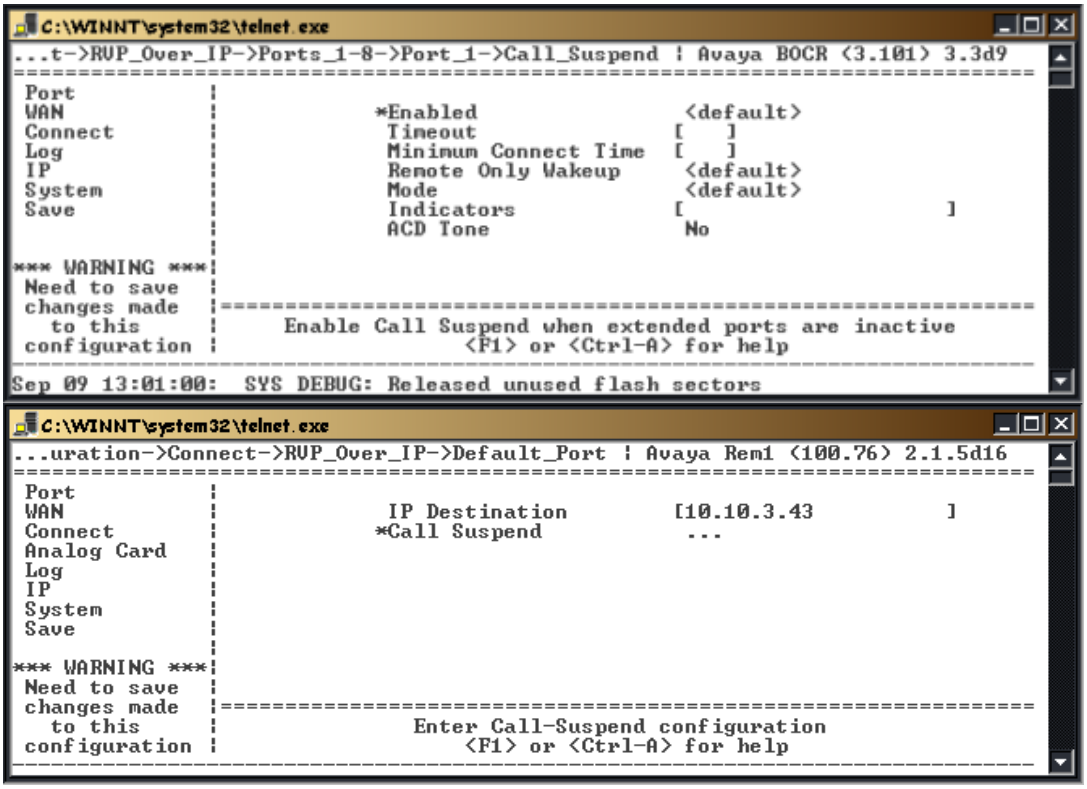


Figure 49: RVP_Over_IP Call Suspend

3. Press the→ key to the **Enabled** parameter. Press the → key to select *Yes*.

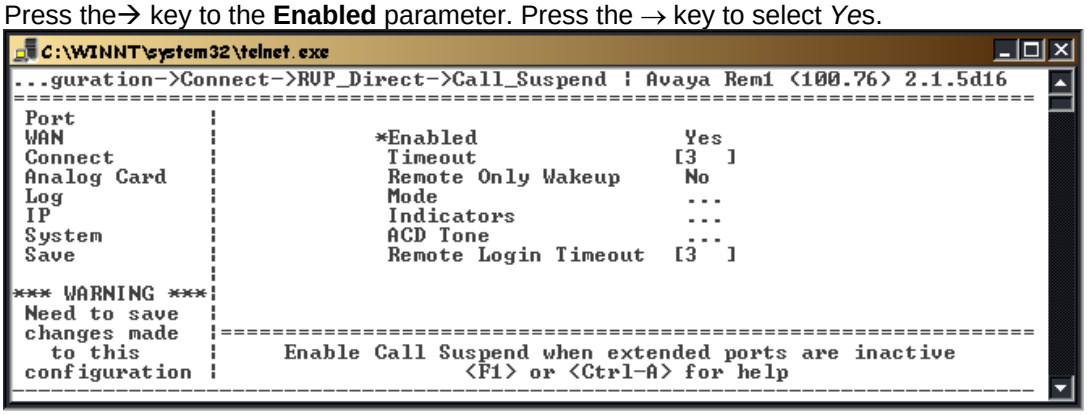


Figure 50: Call_Suspend Settings

4. Press the ↓and →key to the **Timeout** parameter. This parameter causes the units to go into Call Suspend mode when no activity occurs for the set Timeout value. Set the value between 15 and 240 minutes.
5. Press the ↓ and →key to the **Minimum Connect Time** parameter. Enter a value, in minutes (0 –240) that the EXTender will be connected to the Gateway before falling into Call Suspend.
6. Press the ↓ and →key to the **Remote Only Wakeup** parameter. If you set this parameter to Yes, you enable wakeup from Call Suspend on activity at the Branch site only (for example, when a telephone set goes off-hook or a key is pressed). If you set this parameter to No (disabled), incoming calls can also cause wakeup from Call Suspend.
7. Press the ↓and → key to the **Mode** parameter. This sub-menu sets the Call Suspend mode for each port. The choices are *Ring, or Lam*p.
   ***Note**: Use Ring mode for non-ACD sets, and use "Lamp" for ACD sets*.

8. If you have selected *Lamp* mode for any ports, press the ↓ and →key to the **Indicators** parameter. This parameter sets the Lamp indicators that you want to monitor on the telephone.
   ***Note**: Normally you should select call-appearance Lamps*.
9. If the Remote has ACD sets with Headsets, press the ↓ and →key to the **ACD Tone** parameter. Enable the ACD Tone for each port that has an ACD telephone with Headset.
10. Press the ←key to accept changes and go back to the Configuration Menu.
12. Press the ↓key to the **Save** parameter. Press **Enter** to save changes to the active config (.*re*m) file.
13. Make sure the "Dial-up" and "Dialback" numbers are programmed. Use the table below:

PBXgateway `Configuration → WAN`	• Local dialing Numbers • SPID Numbers • Dial Prefix
Remote `Configuration → WAN`	• Local dialing Numbers • SPID Numbers • Dial Prefix • Dialback Num1 • Dialback Num2
Remote `Configuration → Connect → RVP_Direct`	• Primary Dial Nums • Secondary Dial Nums
Remote `Configuration →Connect → RVP_Over_IP`	Ports_1-8 → Port_1 • IP Destination

Procedure for Norstar (Gateway and Remote)

1. Access the *Call_Suspend Menu* using the following path;

   ***Note**: When using an RVP_Direct connection, and Call Suspend is enabled, all ports will have call suspend enabled. If using and RVP_Over_IP connection, Call Suspend can be enabled on a port-by-port basis, using individual port values or the <Default> values.*

   Path: Remote->Configuration->Connect->RVP_Direct->Call_Suspend
   Path: Remote->Configuration->Connect->RVP_over_IP->Default_Port
   Or for individual ports:

   The following menu appears.

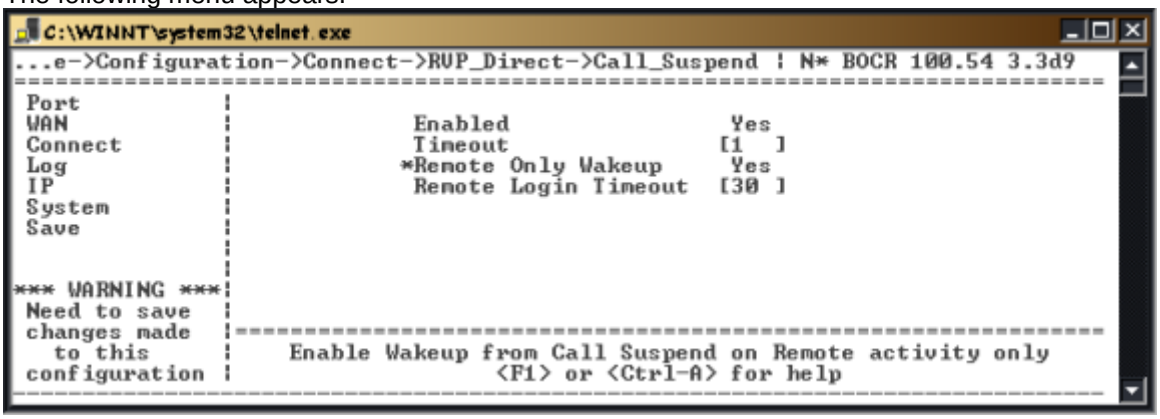


Figure 51: RVP_Direct Call Suspend

2. Press the→ key to the **Enabled** parameter. Press the → key to select *Yes*.

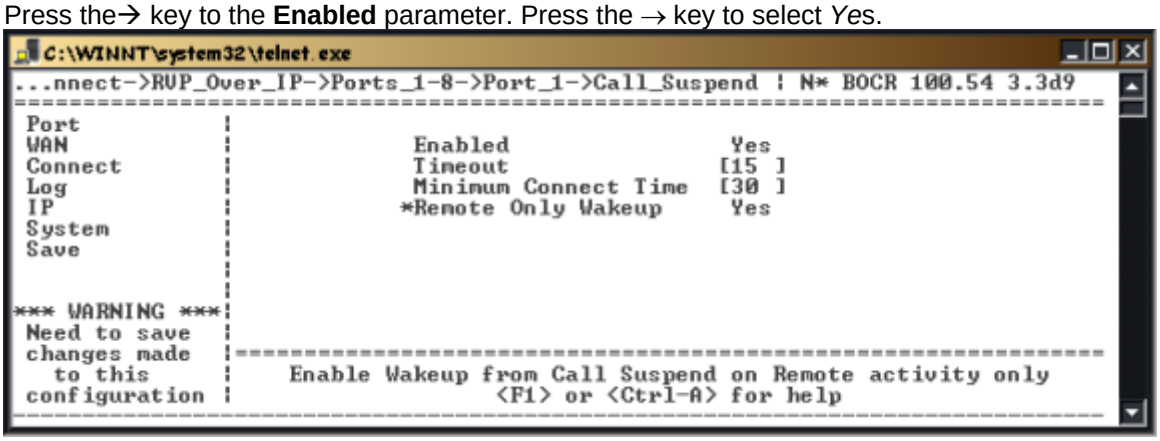


Figure 52: RVP_Over IP Call_Suspend Settings

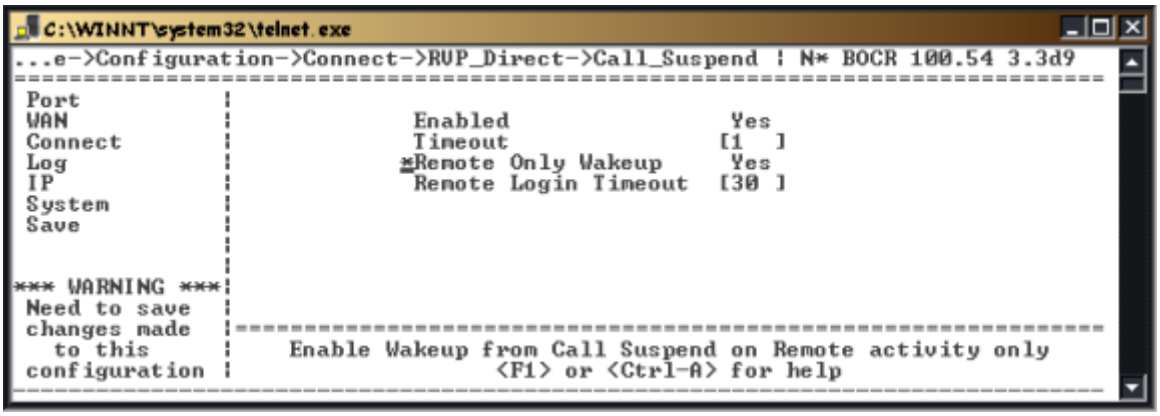


Figure 53: RVP_Direct Call_Suspend Settings

3. Press the ↓and →key to the **Timeout** parameter. This parameter causes the units to go into Call Suspend mode when no activity occurs for the set Timeout value. Set the value between 15 and 240 minutes.
4. Press the ↓ and →key to the **Minimum Connect Time** parameter. Enter a value, in minutes (0 –240) that the EXTender will be connected to the Gateway before falling into Call Suspend.
5. Press the ↓ and →key to the **Remote Only Wakeup** parameter. If you set this parameter to Yes, you enable wakeup from Call Suspend on activity at the Branch site only (for example, when a telephone set goes off-hook or a key is pressed). If you set this parameter to No (disabled), incoming calls can also cause wakeup from Call Suspend.
6. Press the ↓ and →key to the **Remote Login Timeout** parameter. Enter a value, in minutes (15 – 240) that the EXTender will be in idle, before Call Suspend is enabled.
7. Press the ←key to accept changes and go back to the Configuration Menu.
8. Access the Call Suspend Menu on the Gateway. Set the Num Dials On Reboot, this is the number of times the Gateway will dial the Remote on a reboot, while in Call Suspend.

Path: Gateway ->Configuration->Connect->RVP_Direct->Call_Suspend

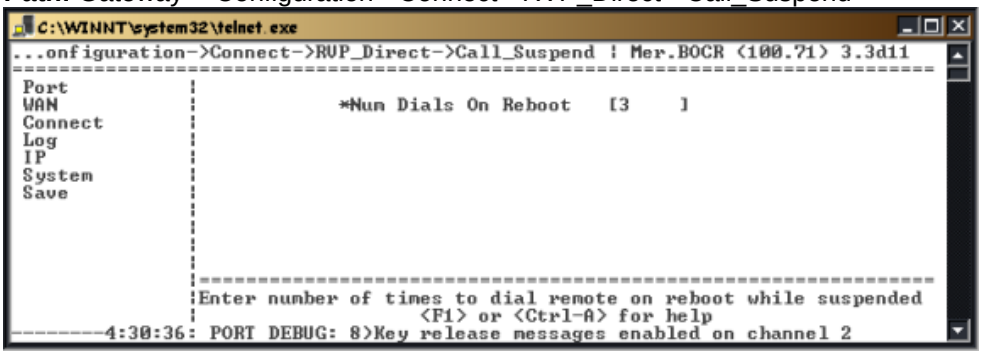


Figure 54: Num Dials on Reboot

Enabling ConneX

The PBXgateway supports the ConneX features. This application puts PBX features and dialtone in the hands of users of remote telephones. For instructions on setting up your ConneX phone please see Appendix F: ConneX Application Guide starting on page 250.

***Note**: If ADSI (Analog Display Service Interface) enabled phones are being used the user will have access to all the RemoteConneX features. If Analog or mobile phones are being used by a remote worker the MobileConneX features will be accessible to the user. The prompts for this application are very similar but may differ in some instances.*

The PBXgateway is an application-specific gateway capable of extending dialtone and features of the enterprise PBX to up to 12 users of ConneX Phones and/or mobile phones. ConneX features can be enabled on a port-by-port basis.

***Note**: Setting the ConneX port values in the default port menu will assign these values, and the associated ConneX features to all ports. If you wish to use a single port for ConneX then configure an individual port.*

***Note**: Norstar Only – Set the Handsfree menu item, on the KSU, to None.*
DN for Connex_Link = Handsfree = None
DN for Voice = Handsfree = None

Procedure (Gateway Only)

1. ***(Norstar Only)*** Access the Port menu and set the **CH1 Usage** to *ConneX_Link*. Set this for the ports that you will be using for ConneX users only. Do not set this in the Default port menu.
2. **(Meridian and Avaya)** Access the Port menu and set the **CH2 Usage** to *ConneX_Link*. Set this for the ports that you will be using for ConneX users only. Do not set this in the Default port menu.
3. ***(Norstar Only)*** Create the ConneX Link and Voice on the same DSP. For example select Port_1 and set the Ch1 Usage to ConneX_Link. Access Port_2 and set the CH1 Usage to Voice. You can use any two ports in sequential **pairs** starting at Port_1. So you can use Port_1 and 2, Port_3 and 4, Port_5 and 6 etc.

***IMPORTANT**: The Norstar KSU may take up to 5 minutes to initialize. It is recommended that you wait for this specified time period before attempting to place a call. Not doing this may result in failed calls.*

Path: Gateway->Configuration->Port->Port_x

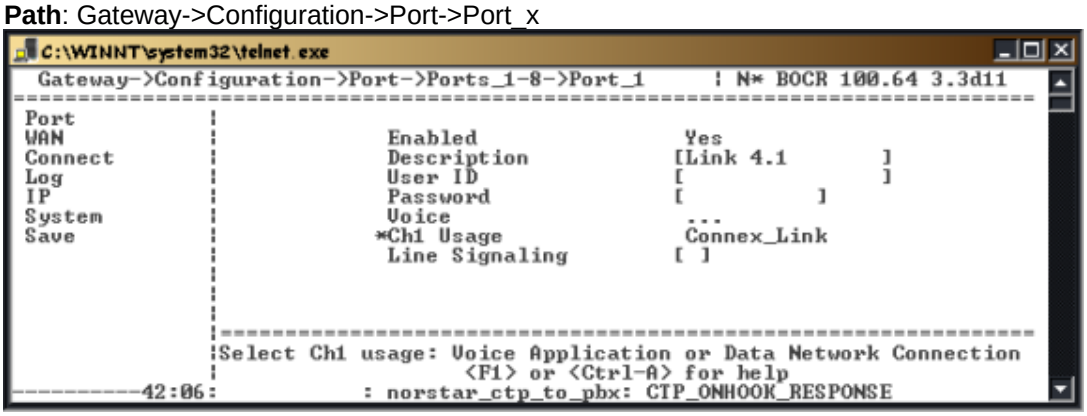


Figure 55: (Norstar) CH1 Usage - ConneX_Link

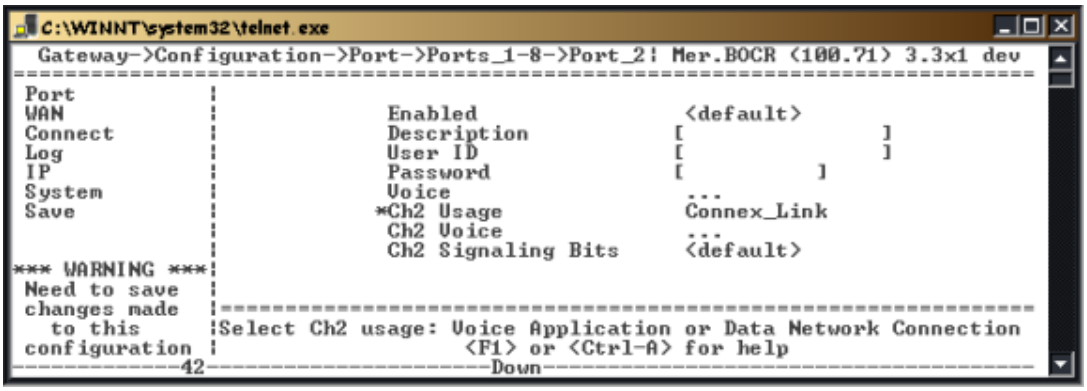


Figure 56: (Meridian and Avaya) CH2 Usage - ConneX_Link

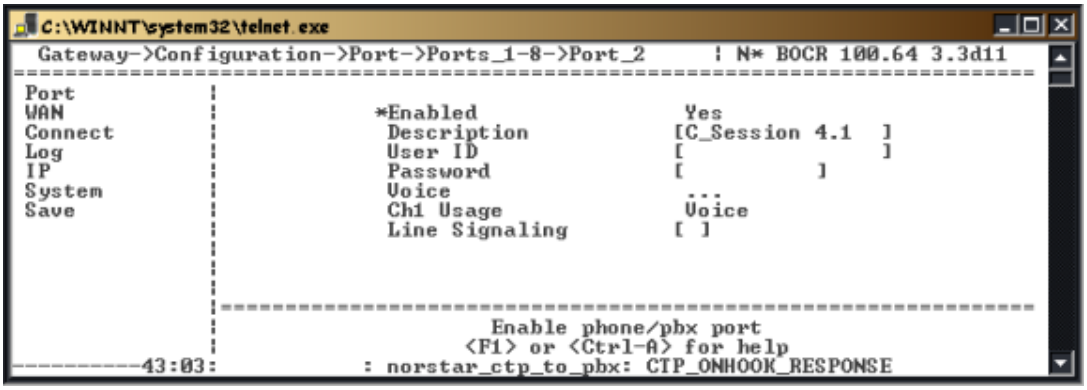


Figure 57: CH1 Usage - Voice

4. Access the ConneX Port parameters using the following path:

   Path: Gateway->Configuration->Connect -> RVP_ConneX ->Port_x - y
   Or
   Path: Gateway->Configuration->Connect -> RVP_ConneX ->Default Port

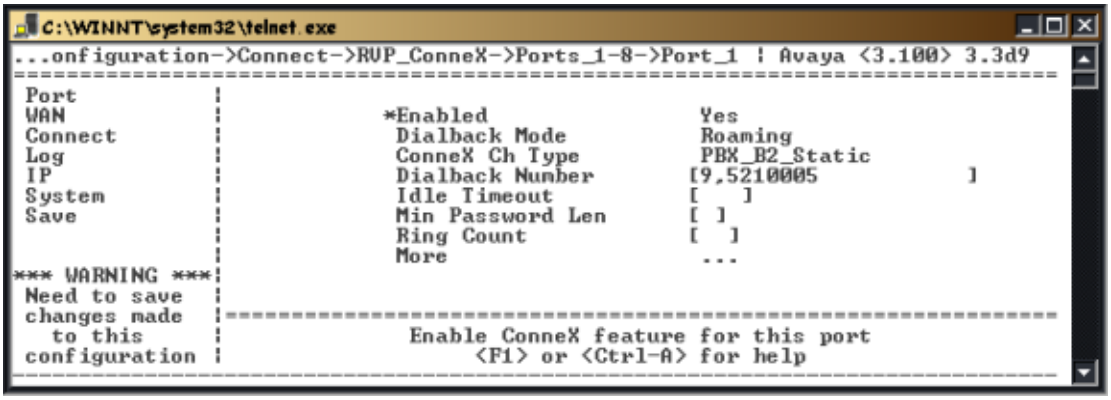


Figure 58: ConneX – Individual Port

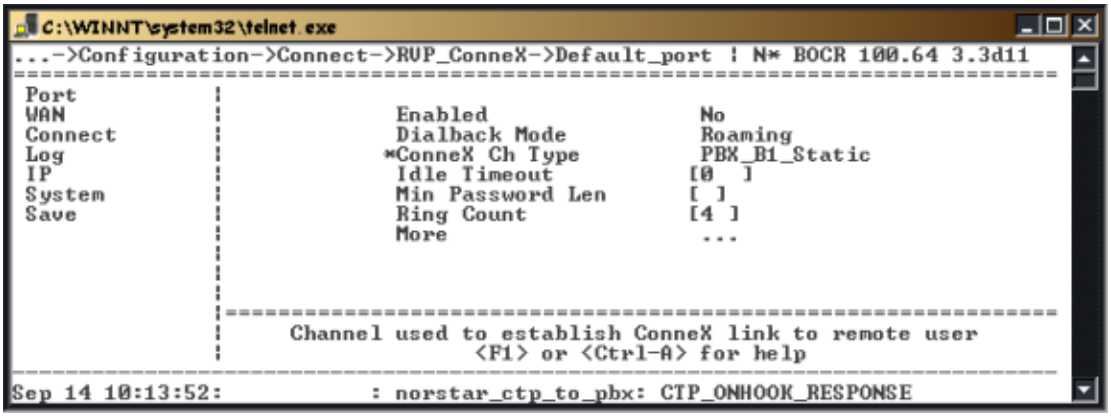


Figure 59: ConneX – Default Port

5. The number of ports configured for ConneX usage will depend on the number of remote users.
6. Press the → key to the access individual ports, and use the table on the following page to help you set the values for the port parameters.
7. Access the More parameter. Use the table below to help you select the proper values.

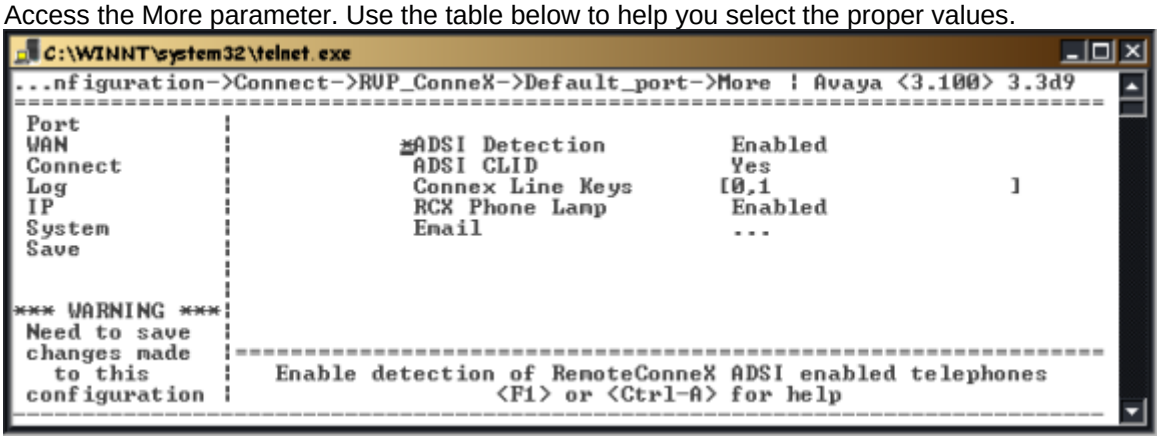


Figure 60: ConneX Parameters

ConneX Parameters

Table 1: ConneX Port Parameters

Parameter	Description
Enable	This will enable ConneX features on the selected port. Select No, Yes or Default.
Dialback Mode	A configurable setting that determines where the PBXgateway routes your calls. There are four different Dialback Modes and the level of security varies from one to another: Roaming, Disabled, Fixed and Fixed/Forced. The System Administrator is the only person who can change the Dialback Mode.
ConneX Ch Type	This parameter identifies the port the ConneX session will use to connect the mobile/remote user to the office gateway. In the case of the Definity or Meridian protocol, the default will be the current digital port's B2 channel (PBX_B2_Static). In the case of the Norstar protocol, the default link port is the adjacent B1 port (PBX_B1_Static) Note: If this field is set to disable, ConneX capability is disabled.
Dialback Number	The telephone number that the PBXgateway uses to reach you on your analog or mobile phone. Incoming calls to your office extension are routed to the dialback number that is currently set. . *Note: Dialback number must include prefix (9+ 1 e. g.) necessary to access outside line.* *Note: If necessary, a comma (,) will be used as a pause in the dialstring.*
Idle Timeout	This is the amount of time a channel will be in the Idle mode (connected but no active calls) before the phone is disconnected. Set this value to zero to disable the Idle Timeout. Range:0-192 minutes.
Min Password Length	This parameter ensures the minimum length of the ConneX login password for security purposes. Also, it provides the following features for a newly configured user: The System Administrator can assign a ConneX user an initial password by entering a value in the Password field of the Port Menu. Also, the Administrator can let the ConneX user enter their own password by configuring the 'Min Password Len' parameter. When the user first attempts to access the ConneX port from their remote phone, they will be prompted to enter a password with the specified length. *Note: The minimum value for this field is 2 (maximum is 9). To disable the limitation of password length, leave the field blank.*
Ring Count	Properly setting this ring count will ensure calls are routed to your Corporate Voice Mail instead of your mobile service provider's voicemail. Ring count will dictate the number of audible rings the GW will send to the remote phone, via dialback before going to your corporate voice mail. Set this count at least one ring higher then your service provider's voicemail ring count. In most cases a Telco will set their voicemail ring count to 4 rings. We suggest setting this value to at least 5 rings to ensure your Corporate Voicemail will receive this unanswered call.
More...	
ADSI Detection	Enabled, Disabled. Select Enabled only when the remote client is using an ADSI enabled RemoteConneX Phone. This will enable RemoteConneX and allow RemoteConneX Phone user to use the special phone features.
ADSI CLID	This item is a RemoteConneX specific feature. This parameter is used to enable or disable the RemoteConneX Phone to display Caller ID information.
ConneX Line Keys	This parameter specifies the PBX line appearance keys for the ConneX port. Please assign this value according to the PBX configurations for

	this port. Note: The PBXgateway uses a zero base key mapping. For example, in Definity PBX key 1 is the first line appearance key, you should assigning key '0' in the PBXgateway as the line key.
ConneX Link Key (Norstar Only)	When the EXTender needs to call the ConneX user it needs to know what key to “press” to access a line and dial the user. Use 0 (zero).
RCX Phone Lamp	This item is a RemoteConneX specific feature. This parameter is used to enable or disable the 'Message Waiting Lamp' on the RemoteConneX Phone. ***Note**: The lamp indication will only be updated upon login/logout of the ConneX port.*
Transfer Key (Meridian Only)	Assigns Transfer call function to a specific key mapped on the PBX.
Conference Key (Meridian Only)	Assigns Conference call function to a specific key mapped on the PBX.
Email...	*The **SMTP Server** must be configured. Please see the procedure below.*
VMWI Email	Voice Message Waiting Indicator (VMWI). Enabling this feature will trigger an email to be sent to you every time a voice mail has been left in your corporate mailbox.
Call Log Email	Enabling this feature will trigger an email to be sent to you with the Caller information. This is useful when you have lost access to your voice services. Note, that with Norstar, if you receive a 2nd call while on an active call, an email will not be sent, the call will behave normally otherwise. It is not desirable to interrupt the voice path to send this information.
Email Address	Enter the email address of the ConneX user. Note, that invalid characters may be entered in this field such as the $ symbol. Ensure you have entered the correct address. To edit an address simply use your backspace, delete, right arrow, or left arrow keys to scroll and insert characters. Press Enter to accept the address.

Configuring the SMTP Server (Gateway Only)

1. Access the SMTP Server Menu using the following path:

   Path Gateway->Configuration->IP->SMTP

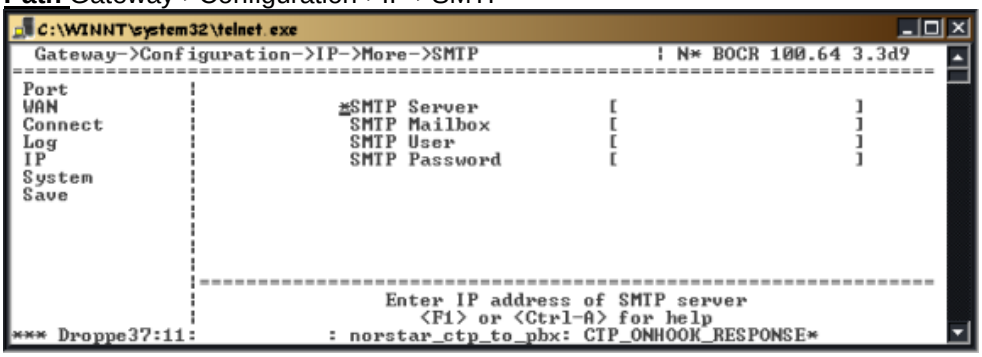


Figure 61: SMTP Parameters

2. Enter the IP address or Name of your corporate SMTP Server. Ensure DNS has been enabled and configured when entering name instead of IP Address. See ‘DNS on page’ 81 for details on enabling the DNS service.
3. Enter the email address of the ConneX user in the SMTP Mailbox field. This parameter specifies the FROM address of the email being sent out. Usually, you would assign a virtual email address (eg.ConneX@PBXgateway) as a notification to the user who receive the email.
4. Enter the ConneX User Name in the SMTP User field. Ask your System Administrator if you are unsure if this is required for your SMTP services.

5. Enter a password so the user can access their email. (optional) Ask your System Administrator if you are unsure if this is required for your SMTP services.

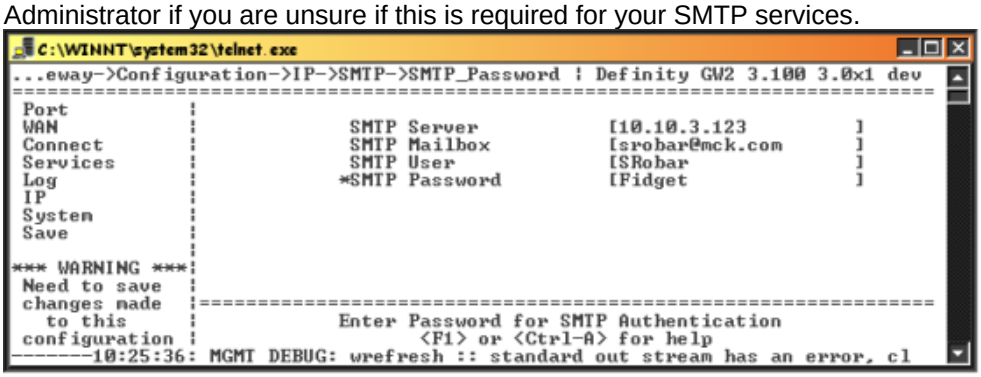


Figure 62: SMTP Server Configuration

Console Setup Wizard (Gateway and EXTender)

A console setup wizard has been created for the PBXgateway and EXTender 6000, and a phone interface setup wizard has been created for the EXTender 4000. The setup wizard will guide a user through most of the required programming and configuration required to complete the initial setup of the units, via the VT100 management console accessed through the DB9 serial port on the PBXgateway. Parameters not configurable through the wizard can be set through the Management Interface.

When a unit is first powered up it will check a Setup Wizard flag. If the flag is set then the standard console UI will be displayed. If the flag is not set then the user will be asked whether they would like to run the Setup Wizard. After this initial prompt the Setup Wizard flag will be set, preventing the user from being asked to run the Wizard again. The Setup Wizard can also be accessed through the console Management Interface in case the user wants to run it later.

Portion of the variables configured through Setup Wizard:

- Unit Name
- Region Code
- PBX Type (Note: This is the **only** location to set this parameter)
- Network Connections
- Enable All Ports
- Voice Compression
- IP Configuration

Login to Alternate Remote Unit (Gateway)

The system administrator can connect to each Remote unit from the PBXgateway through the "Remote Login" command within the Management Interface (MI). This command allows the system administrator to access all Remote units for configuration, troubleshooting, and file transfers.

Procedure

1. Access the Main Menu.
2. Press the ↓ key to select Remote Login and press **Enter**. A menu will appear displaying the Remotes that are connected and can be accessed from the PBXgateway.
3. Select the Remote from the list displayed.

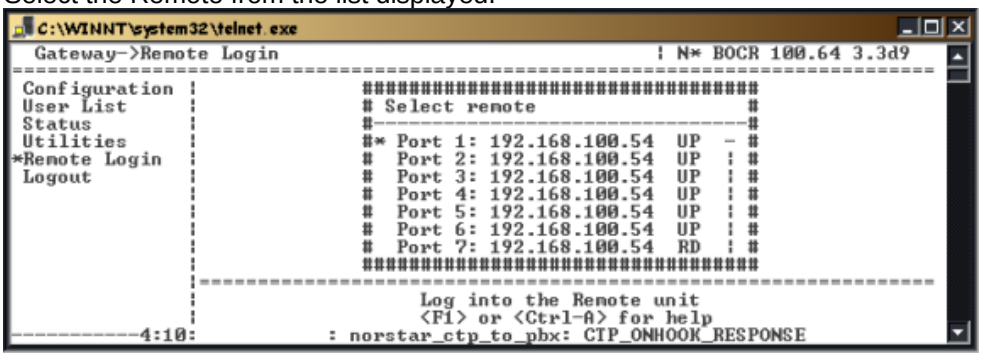


Figure 63: Available Remotes

***Note**: This menu only appears if you run in RVP_IP mode. Otherwise, "Remote Login" just connects to the corresponding Branch EXTender*.

The screen will display:

`Connecting.....`, and the Welcome Screen appears for the unit at the alternate site.

***Note**: You may have to enter the Administrator Password if passwords are used.*

The live log window will not automatically update. Press F4 to update the log messages.

You can also do a Gateway login from the Extender by using the same pathway:
Path: Remote -> Gateway Login.
As there is only one Gateway connected to the Remote, no list will appear. You will automatically access the Gateway welcome screen.

Remote Unit Configuration

Direct Serial Connection (RVP_Direct)

The EXTender 6000 Branch Office unit utilizes a direct serial connection to provide remote user connectivity. This means that the WAN port is plugged directly into a network device. The WAN port (WAN 1 or WAN 2) that is used as the main or "primary" port must be identified on the RVP_Direct menu.

***Note**: The WAN port must already be enabled and properly configured (see page 70).*

Connect Menu – Remote Only

Procedure

1. Access the Connect Menu from the Main Menu using the following path:

   Path: Remote->Configuration->Connect

2. Set the "Connect Type" to RVP_Direct and access the Menu.

   The following menu appears:

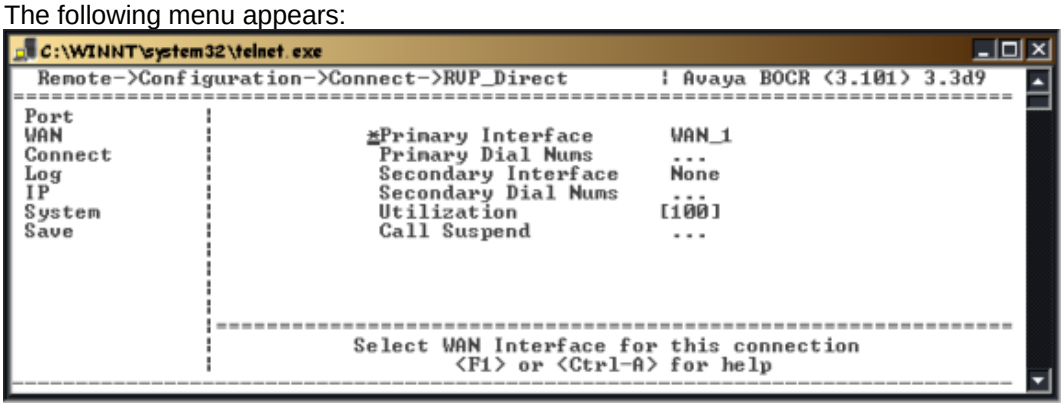


Figure 64: RVP_Direct Menu

3. Press the → key to the Primary Interface parameter. This is the main WAN port (usually WAN1) that connects the Remote unit to the network device.

4. Press the → key to scroll through the choices.

5. Press the ↓ key to the Secondary Interface parameter. This identifies the secondary WAN port.

   ***Note**: This parameter is normally set to None.*

6. Press the ↓ key to the Utilization parameter. This parameter is a numeric value that represents the percentage of bandwidth used by the remote unit. See page 144 for more information on setting this parameter. This should be left at 100.

7. Press the ← key to accept changes and go back to the Configuration Menu.

8. Press the ↓ key to the **Save** option. Press **Enter**.

IP Connection (RVP_Over_IP) – Remote Only

The EXTender 6000 and the EXTender 4000 Remote units utilize an IP connection to provide remote user connectivity. This means that the Ethernet port on the back of the unit is plugged directly into the existing network through an RJ-45 connector.

The PBXgateway IP address must be entered within the Management Interface (MI) of the Remote unit to locate the PBXgateway within the IP network.

Procedure

1. **For the EXTender 4000 Remote unit**, access the Connect Menu from the Main Menu using the following path:

   Path: Remote->Configuration->Connect

   The following menu appears:

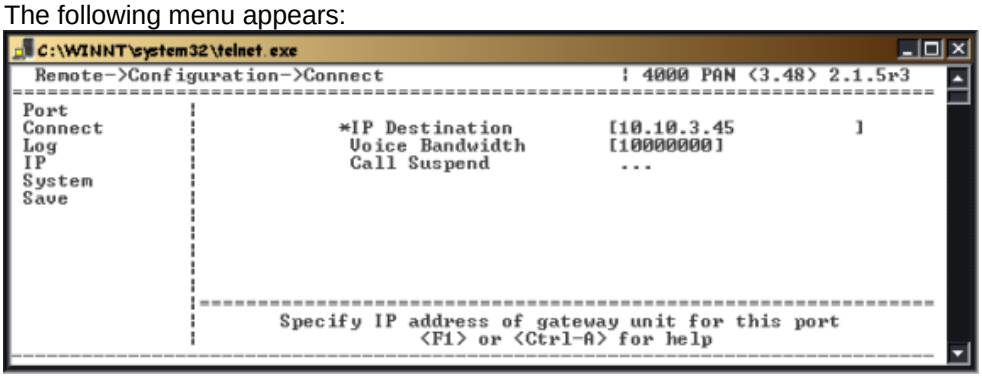


Figure 65: Connect Type

3. Press the → key to access the IP Destination parameter.
4. Enter the IP address of the PBXgateway.

   ***Note**: This address must be assigned by the network administrator*.

5. Press the ← key to accept changes and go back to the Configuration Menu.
6. Press the ↓ key to the **Save** option. Press **Enter**.
7. **For the EXTender 6000 Branch unit** access the Connect Menu from the Main Menu using the following path:

Path: Remote->Configuration->Connect->RVP_Over_IP->Default Port

The following menu appears:

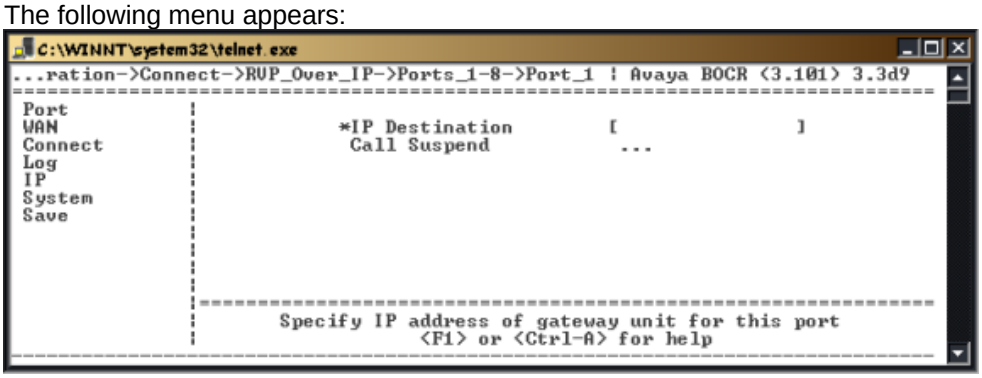


Figure 66: RVP_over_IP Menu

***Note**: The <Default> setting will connect all ports to the same PBXgateway. Individual ports can be set to connect to different PBXgateway units by simply selecting the port.*

7. Press the → key to the IP Destination parameter.

8. Enter the IP address of the PBXgateway.

   ***Note**: Each port can actually have a unique IP Destination if you have multiple PBXgateways. This address must be assigned by the network administrator.*

9. Press the ← key to accept changes and go back to the Configuration Menu.
10. Press the ↓ key to the **Save** option. Press **Enter**.

Customizing Individual Ports (Gateway and Remote)

The system administrator can customize each individual port for phones connected to the Remote unit. The following parameters are described:

- Description (See page 131)
- Auto-Connect
- ATA (Merdian only)
- User ID (See page 68)
- Password
- Banner
- Line Signaling (Norstar only)
- Phone Features – Active Call Monitoring (Norstar Only) See page 116.
- Logout (Avaya only) See page 111.
- MSB Key (Merdian only) See page 111.
- More

Procedure

1. Access the specific Port Menu from the Main Menu using the following path:

   Path: Remote->Configuration->Port->Port_x-y -> Port_x

   The following menu appears:

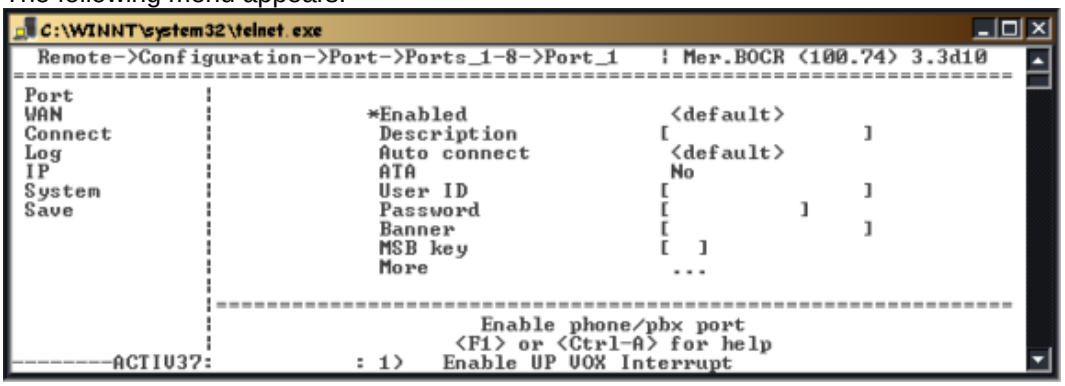


Figure 67: Port Selection Screen

Auto Connect (Remote Only)

This feature attempts to permanently keep the Remote connected to the Gateway and prevents user from having to press '1' to connect.

1. Press the ↓ key to access the Auto Connect parameter.

2. Press the → key and select, Enabled (**Yes**), (**No**), or Default. The Default setting is Auto Connect: Disabled

3. Press the ← key to accept changes and go back to the Configuration Menu.

4. Press the ↓ key to the **Save** parameter. Press **Enter** to save changes to the active config (.rem) file.
5. *(Meridian Only)* Press the ↓ key to access the ATA parameter. Enabled (**Yes**), if you have an ATA device present.

Banner (Gateway and Remote)

1. Press the ↓ key to access the Banner parameter.

2. Press the → key and type in a line of text to be displayed on the Remote phones. Example: Acme Inc.

   ***Note**: The description is limited to alphanumeric (1,2,3, a, b, c etc) characters only, and the total length must not exceed 15 characters.*

3. Press the ← key to accept changes and go back to the Configuration Menu.

4. Press the ↓ key to the **Save** parameter. Press **Enter** to save changes to the active config (.rem) file.

Line Signaling (Norstar Remote Only)

Added port support for the Norstar Line Signaling configuration item. This will resolves audio crackle problems and phone signaling issues. Set the desired Line Signaling value (= duty cycle) as needed.

Valid range: 0 - 7, default is 2 (50% duty cycle).
Suggested working range is 2 - 5 (56% DC), each value represents a 2% increase: 0 = 46% and 7 = 60%.

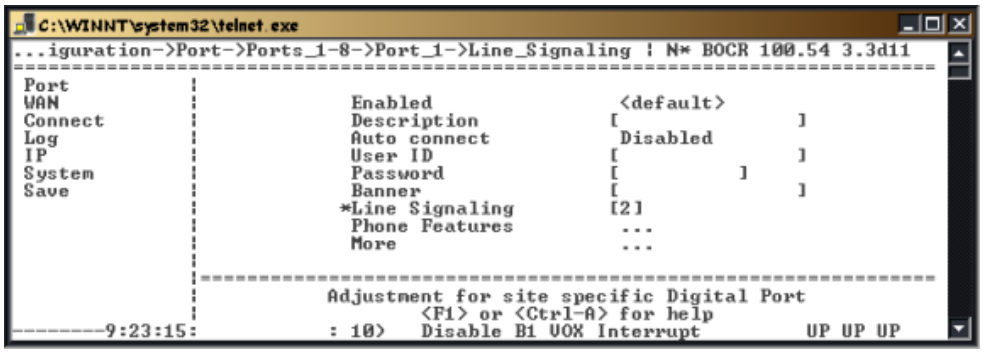


Figure 68: Norstar - Line Signaling

Password (Gateway and Remote)

A (connect) password provides a secure WAN link between the PBXgateway and Remote Unit. If assigned, the connect password must be entered for communication between the PBXgateway and a Remote unit.

Your password should be alphanumeric only. In other words, only use numbers or letters that are on the telephone keypad. DO not use symbols such as $, & or *, as these cannot be entered on a digital deskset keypad.

1. Press the ↓ key to access the Password parameter.

2. Press the → key and type in a password.

Security Alert:

Passwords should be hard to guess and therefore should not contain:

- all the same numbers or characters
- Example: 88888888 or aaaaaaaa

- sequential numbers or characters
- Example: 987654321 or abcdefg
- number strings associated with you or with the remote user or with your business. These include:

  Birthdays
  Telephone numbers
  Social Security numbers

Passwords should be changed regularly, at least on a quarterly basis. Do not recycle old passwords.

3. Press the ← key to accept changes and go back to the Configuration Menu.
4. Press the ↓ key to the **Save** parameter.
5. Press **Enter** to save changes to the active config (.rem) file.

Logout Code Set up (Avaya Only)

The Logout Code is the sequence of commands sent to the PBX when you disconnect the phone port (go offline) from the Branch Unit.

*Note: This only applies to the **Avaya** protocol units.*

Procedure

1. Select Logout Code command using the following path:

   Path: Remote->Configuration->Port

2. Press the → key the ↓ key to access the specific port (1-12).

3. Press the → key access the port menu.

4. Press the ↓ key to access the Logout code parameter.

5. The following buttons are used to set the logout code sequence:

   Use the Digits 0 through 9 as their own value.
   #0 = “D” represents a press of the switchhook.
   #1 = “U” represents the release of the switchhook.

   ***Note**: The normal on-site operation of logging out your telephone using logout codes is to lift the receiver, dial the logout code, then hang up. When you program the Logout Code you must enter the character sequences that simulate the same three actions.*

   Example: for a logout code of *89, enter #1*89#0.

If your Logout Code begins with a ‘#’ you must precede the Logout Code with a “#’. For example, for a logout code of #89, enter #1##89#0.

Setting the Make Set Busy Key (Meridian Remote Only)

The MSB (Make Set Busy) key sends a command from the Gateway to the PBX. This command is used to log agents out of the ACD queue in the event of an abnormal disconnect. This prevents ACD agents from receiving calls during a network outage. The MSB function is programmed to represent a button on the telephone which will be pressed in the event of an abnormal disconnect. In an ACD agent application, this key should be programmed as the Unavailable Key. In a non-ACD application, this key should be programmed as the Hold/DND or Hold/Quick Forward Key.

Procedure (Remote Only)

1. Go to any Port menu using the following path as an example:

   Path: Remote>Configuration->Port->Ports_1-8->Port_1

   The following menu appears:

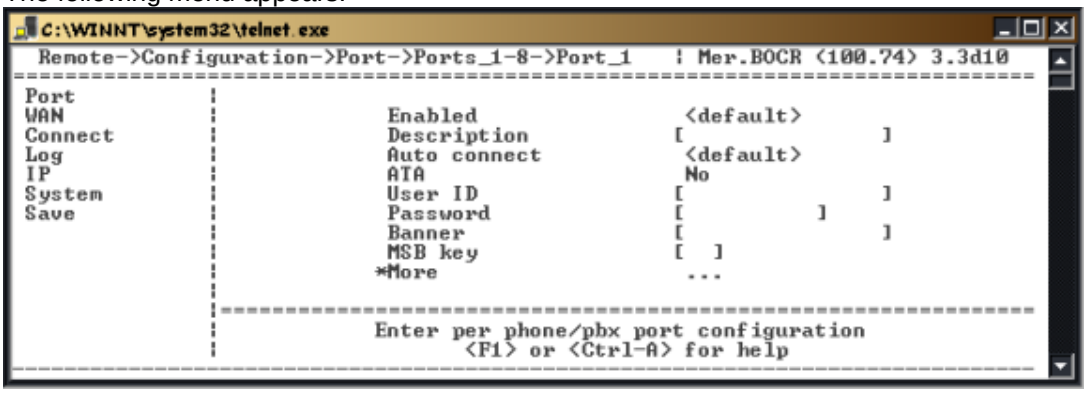


Figure 69: MSB Key

2. Press the ↓ key to scroll down to the **MSB key** parameter.
3. Enter the location of the MSB key on the telephone.
4. Press the ← key to accept changes and go back to the Configuration Menu.
5. Press the ← key to the **Save** option. Press **Enter.**

Setting up the Analog Port (Remote Only)

***Note**: When using the Analog Port ensure that you selected the correct region using the Setup Wizard.*

The EXTender 6000 may be equipped with an extra RJ-11 port on the back panel. This port is labeled “Analog” and it provides a connection to an analog telephone line (provided at the remote location) for the purpose of placing local or emergency calls.

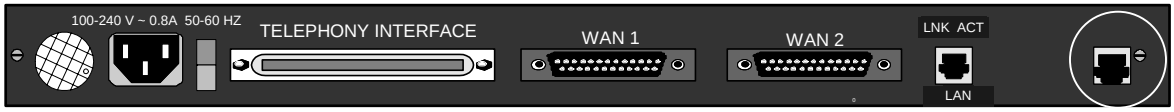


Figure 70: Remote – Analog Line

Once the unit is connected to the analog line, the remote user simply presses the assigned key on the digital telephone and dials the telephone number. Only one remote user can dial out at any one time.

IMPORTANT: *If power to the remote unit fails, the Analog port is not available to the digital telephones. If another telephone tries to use the analog line while it is busy, it hears a "Busy" tone.*

Procedure

1. Select Analog Card using the following path:

   Path: Remote->Configuration->Port_1-8->Port_1->More->911_Analog_Port
   The following menu appears:

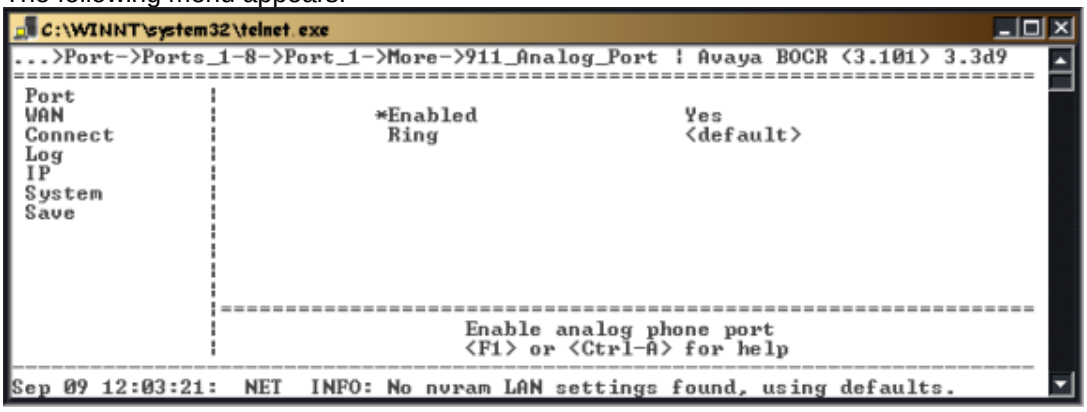


Figure 71: Individual Port – 911 Analog Port Setup

2. Press the → key to enable (Yes) analog port access for all 8 or 12 ports, or press the ↓ key to set individual ports. You may also set this in the Default Port menu and have all other ports read from this as the <Default>.
   Note*: This procedure sets the <Default> setting for all ports.*

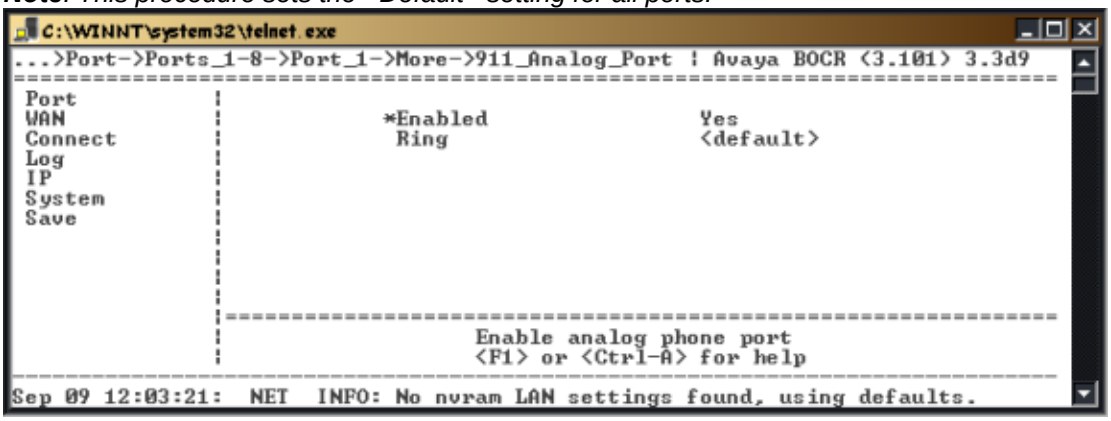


Figure 72: Default Port - 911 Analog Port Setup

3. Press the →key to enable or disable the analog port.

4. Press the ↓key to enable Ring *(yes*) on incoming analog calls.

5. Access the 911 Analog Key using the following path:

   Path: Remote->Configuration->Port_1-8->Port_1->More->Key Mapping

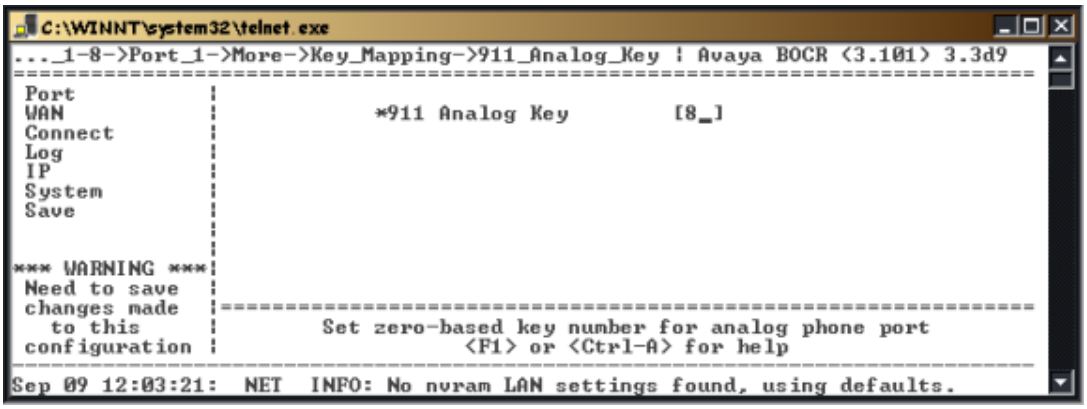


Figure 73: 911 Analog Key Mapping

6. Press the ↓ key to set the numeric "key", which must be pressed on the remote telephone before placing an analog call.
   ***Note**: Do not use a key that already has a function programmed.*

7. Press the ←key to accept changes and go back to the Configuration Menu.

8. Press the ↓key to the **Save** option. Press **Enter.**

System Reboot (Gateway and Remote)

The PBXgateway or any remote can be rebooted through the Management Interface (MI). This parameter is used for resetting the unit during troubleshooting or software upgrades. The MI Reboot is a "soft" reboot, which means that the unit is re-started through the software. A "hard" reboot refers to a re-start by unplugging the unit.

Procedure

1. Select Reboot command using the following path:

   Path: Utilities->System->Reboot

   The following Warning appears:

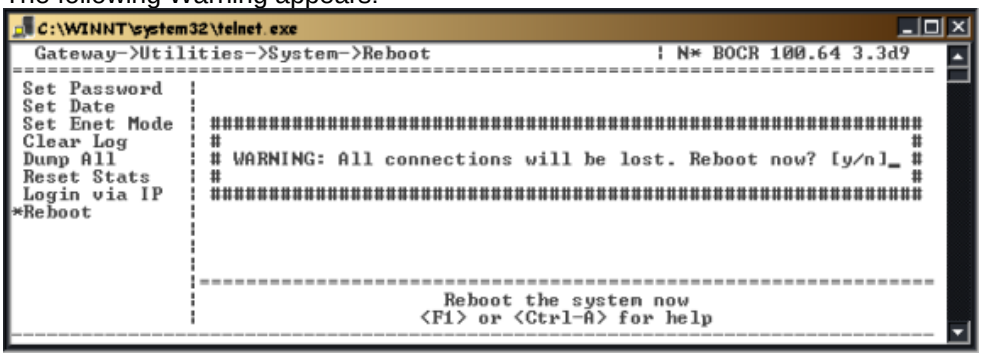


Figure 74: Reboot Warning

***IMPORTANT NOTE**: If the "y" selection is chosen, the following connections will be terminated: All active phones, Telnet connection, FTP connection and in-band logins.*

Logout (Gateway and Remote)

Procedure

1. Select the **Logout** parameter from the Main Menu, the following message appears:

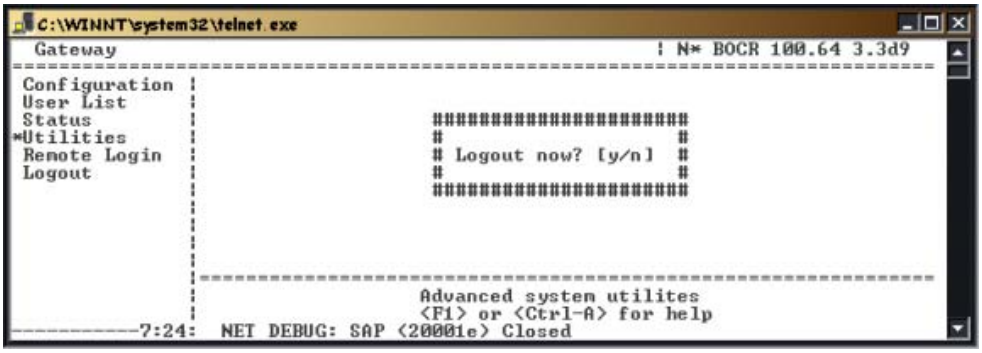


Figure 75: Logout Warning

2. The Management Interface (MI) will ask for confirmation. Press **Y** to 'Logout' out of the PBXgateway.

   Note: After Configuring a Gateway or Remote you should logout for security reasons.

Active Call Monitoring (Norstar EXTender 6000 Only)

This setting, if enabled, allows a receptionist or other user to monitor active calls unobtrusively and perform other related tasks such as answering calls for other users, directing calls or voice mail. This item should be enabled on a port-by-port basis.

Path: Remote -> Configuration -> Port ->Port_x-y -> Port x -> Phone Features -> Active Call Monitoring

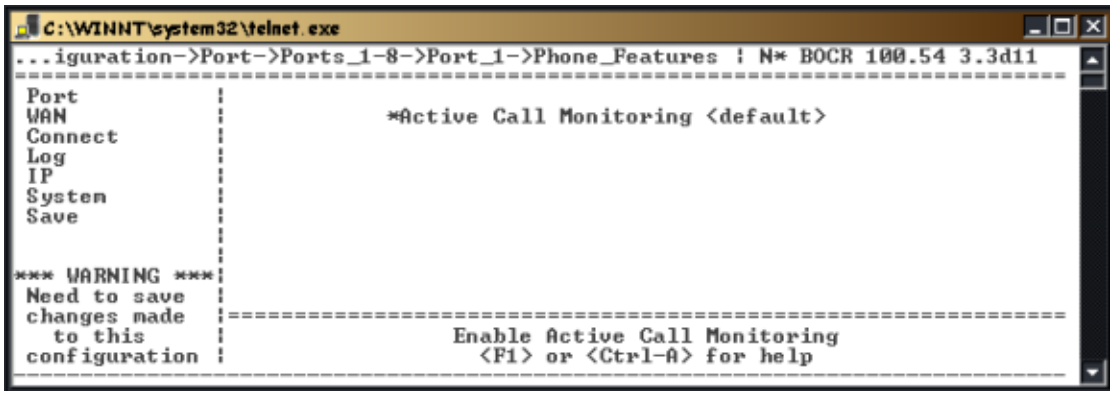


Figure 76: Active Call Monitoring

Chapter 4: The Management Interface (MI)

This Chapter provides information on all parameters within the Management Interface (MI). Information includes the parameter description, usage, location, and references.

Introduction

This Chapter provides background information for each parameter within the Management Interface (MI). The parameters are defined using two different methods:

Parameters listed by menu location
Parameters listed alphabetically using the name displayed within each menu.

Parameters liste by menu locatio

This method sorts all parameters within the MI by the configuration menu on which the parameter appears. All applicable menus are displayed with reference information for each parameter.

***Note**: For information on every parameter within the MI including default settings and all available values see Appendix A.*

The following menus are detailed in this section:

Gateway/Remote units

- Port Menu
- Voice Menu
- WAN Menu
- Sync Setup
- Async Setup
- Connect Menu
- RVP_Direct Menu
- RVP_over_IP Menu
- Log Menu
- IP Menu
- Address Menu
- DNS Menu
- SNMP Menu
- Web Server Menu
- Syslog Menu
- System Menu

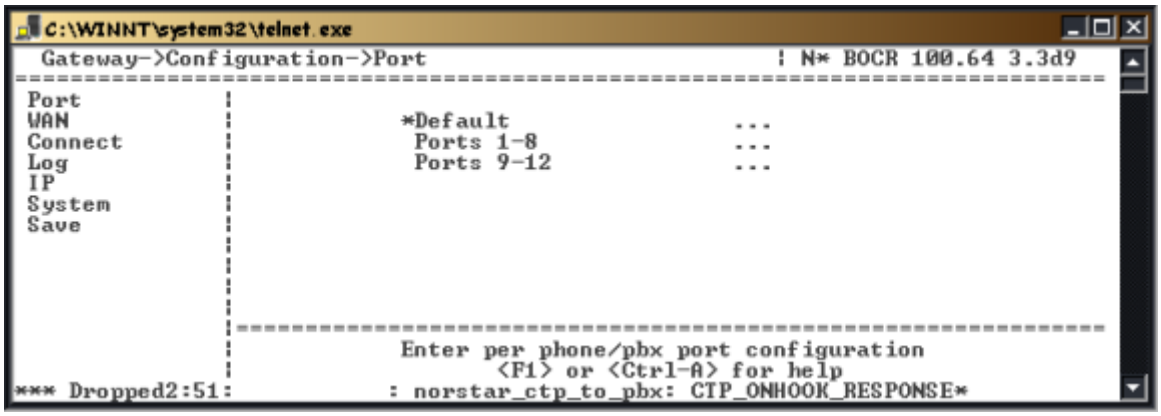
Each entry includes the following support information:

Parameter Location: The Parameter Location text shows you where to find the parameter within the MI.
Description: the Description text explains the parameter.
Usage: The Usage text explains how to use the parameter.
Example: The Example text shows you an example or setting.
Dependencies: The Dependencies text tells you what other information you need to configure and use the parameter.

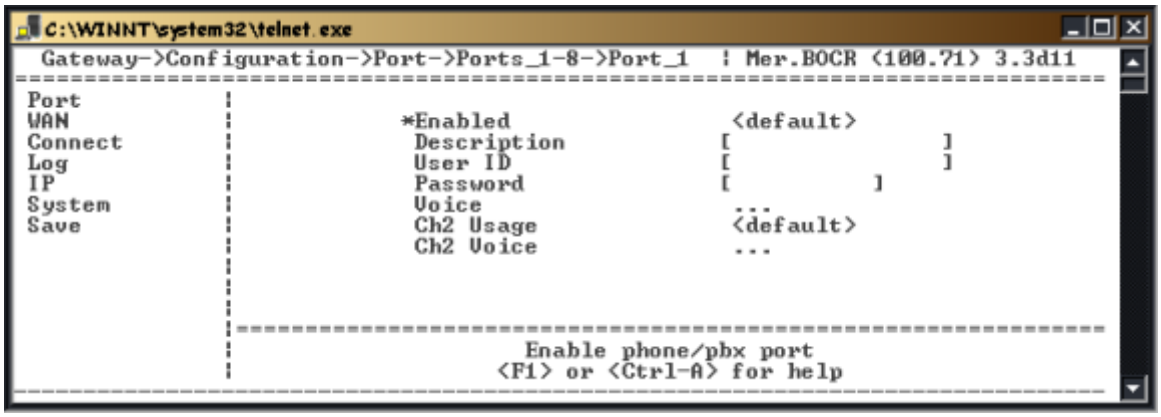
See Also: The See Also text points you to related parameters within the MI.

Gateway & Remote Menus

Port Menu



Port Configuration (Gateway)



Port Configuration (Remote)

Menu items may vary, depending on protocol.

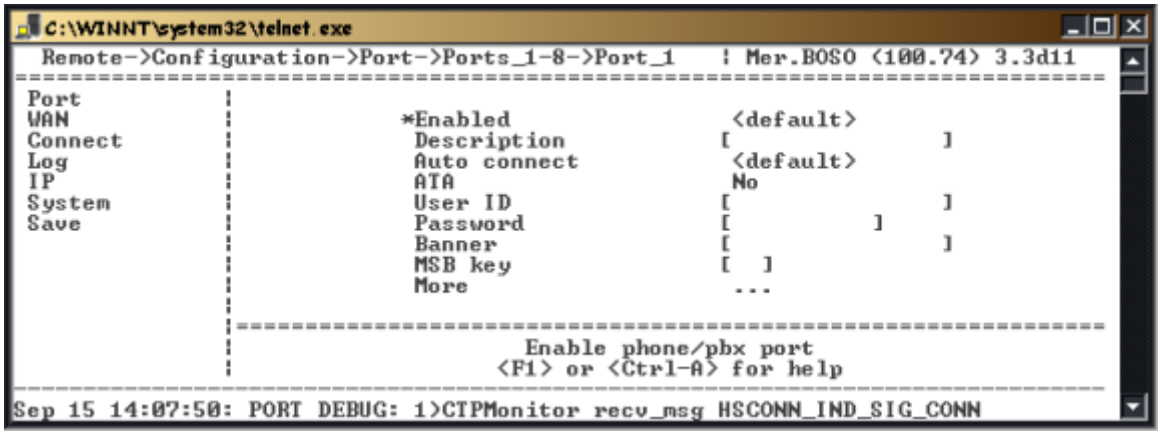


Figure 77: Meridian Port Configuration Menu

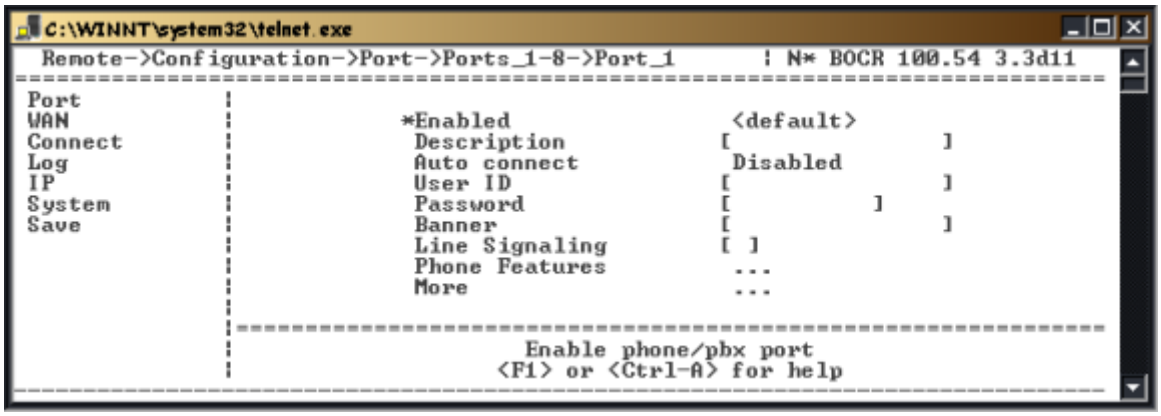
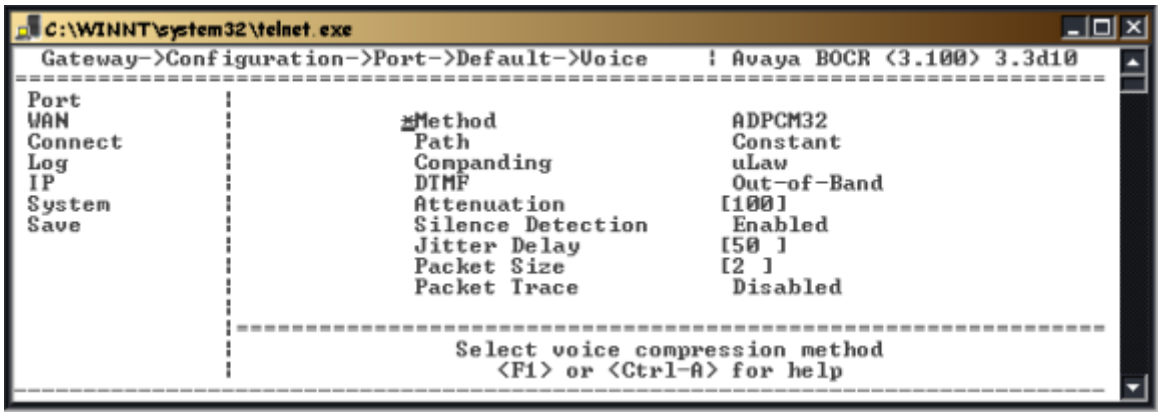


Figure 78: Norstar Port Configuration Menu

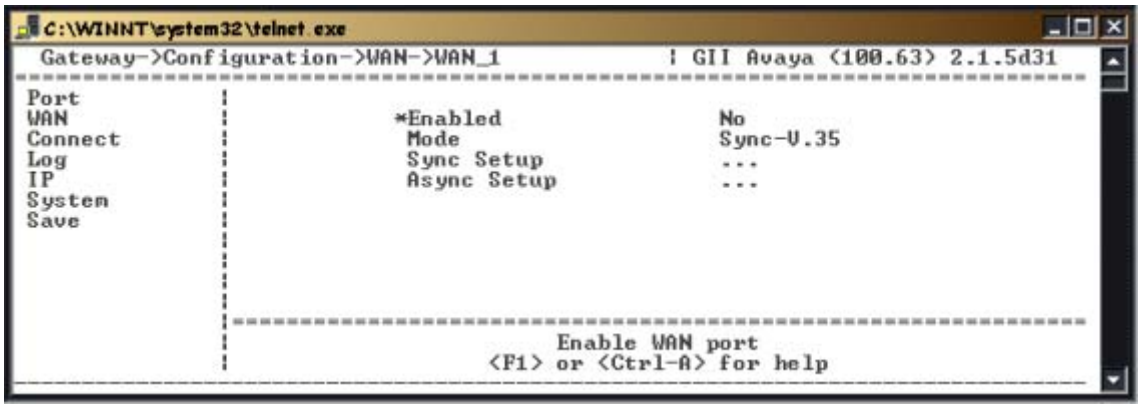
Parameter	To set this parameter see page	For more information on this parameter see page
Enable	-	-
Description	69	131
Auto Connect	109	128
ATA	109	-
User ID	68	144
Password	110	137
Banner	110	129
Line Signaling (Norstar Only)	110	-
Phone Features – Active Call Monitoring. (Norstar Only)	116	-
MSB Key	112	136

Voice Menu (Gateway only)



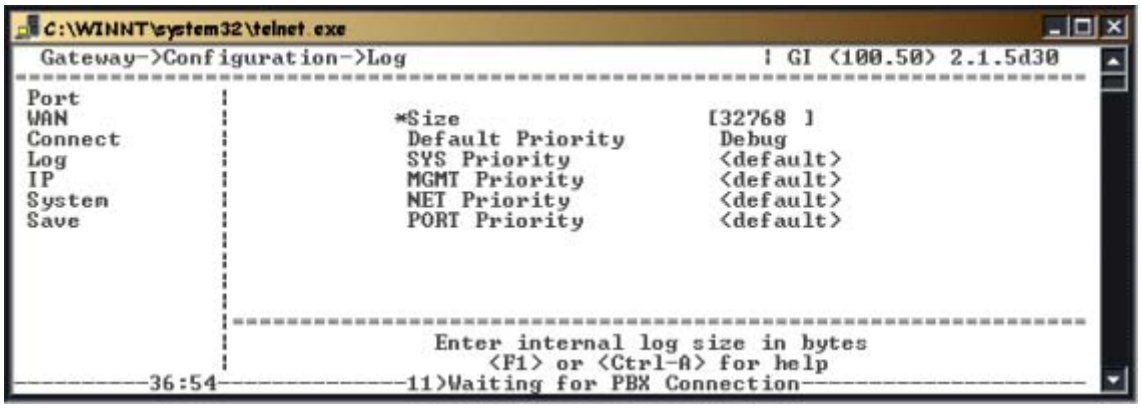
Parameter	To set this parameter see page	For more information on this parameter see page
Method	63	135
Path	-	-
Companding	63	-
DTMF (Avaya Only)	63	131
Attenuation	63	-
Silence Detection	63	-
Jitter Delay	63	134
Packet Size	63	136
Packet Trace	63	136

WAN Menu (Remote and Gateway)



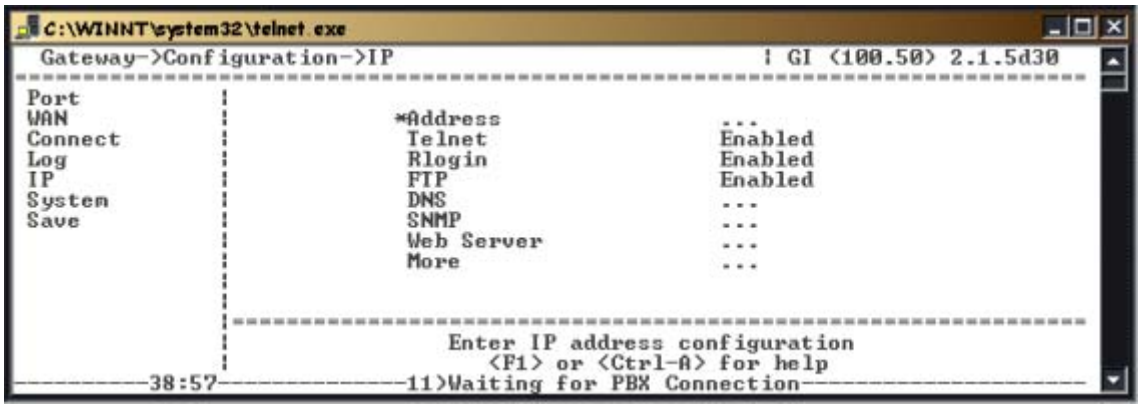
Parameter	To set this parameter see page	For more information on this parameter see page
Enabled	70	-
Mode	71	135
Sync Setup	71	141
Async Setup	74	128

Log Menu (Remote and Gateway)



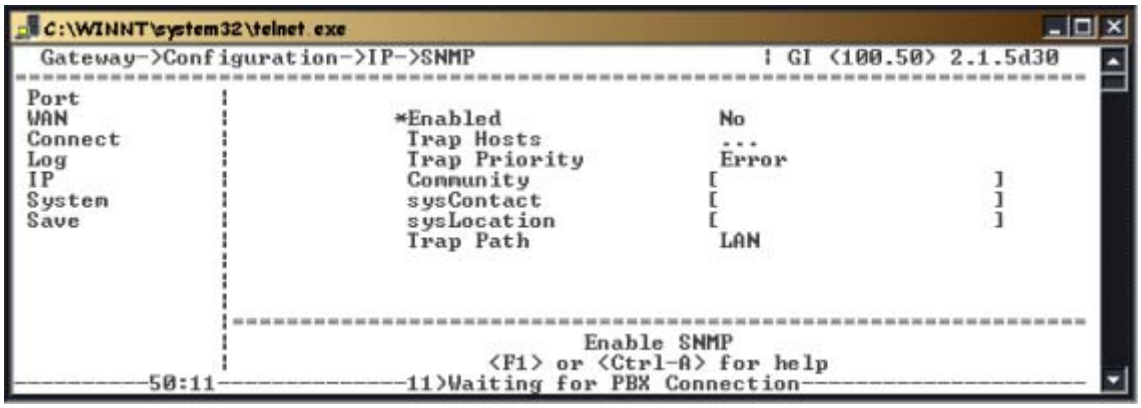
Parameter	To set this parameter see page	For more information on this parameter see page
Size	-	140
Default Priority	-	138
SYS Priority	-	138
MGMT Priority	-	138
NET Priority	-	138
PORT Priority	-	138

IP (Remote and Gateway)



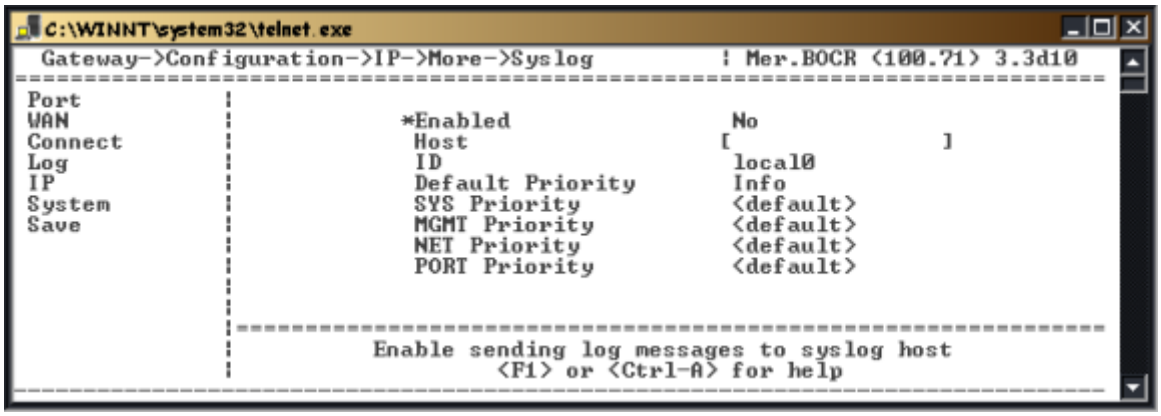
Parameter	To set this parameter see page	For more information on this parameter see page
Address	76	128
Telnet	78	142
Rlogin	77	-
FTP	78	133
DNS	80	131
SNMP	-	123
Web Server	-	144
Syslog	-	123
SMTP	99	-
Static Routes	-	133

SNMP Menu (Remote and Gateway)



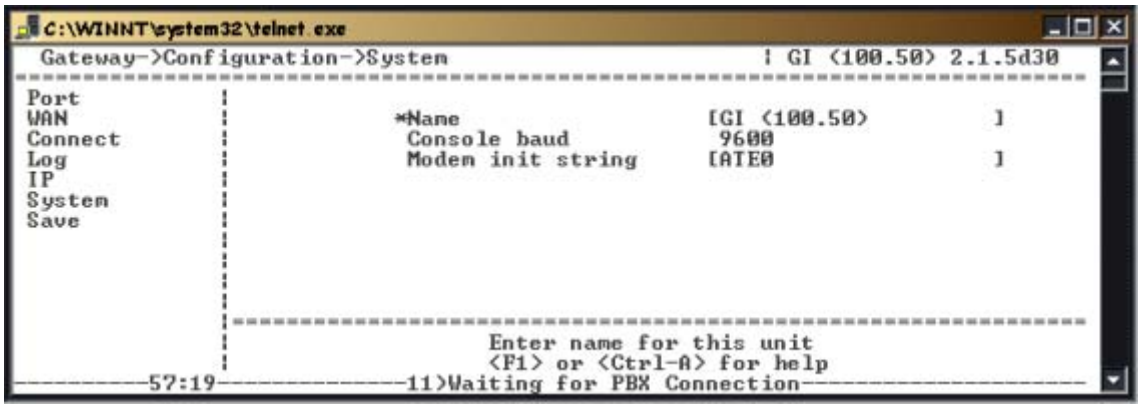
Parameter	To set this parameter see page	For more information on this parameter see page
Enabled	-	-
Trap Hosts	-	142
Trap Priority	-	143
Community	-	130
Trap path	-	143
Sys Contact	-	141
Sys Location	-	142

SysLog Menu (Remote and Gateway)

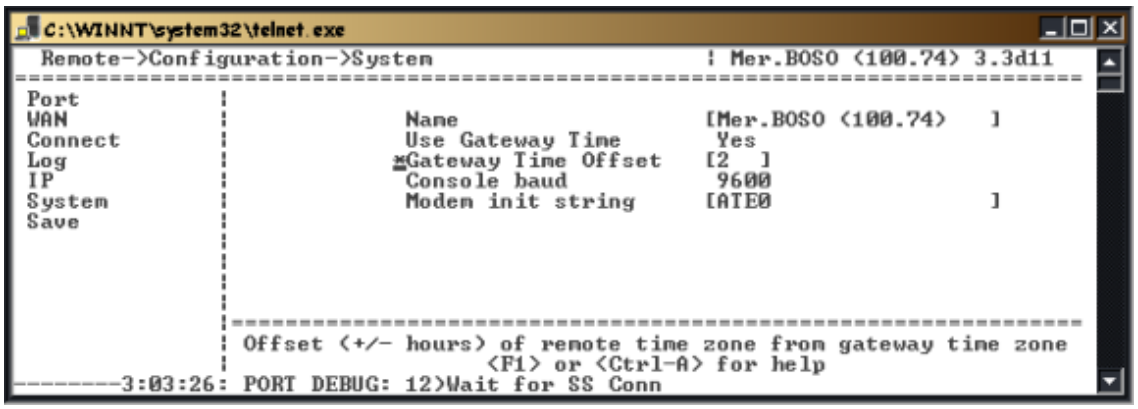


Parameter	To set this parameter see page	For more information on this parameter see page
Enabled	-	-
Host	-	133
ID	-	133
Default Priority	-	139
SYS Priority	-	139
MGMT Priority	-	139
NET Priority	-	139
PORT Priority	-	139

System Menu (Gateway)

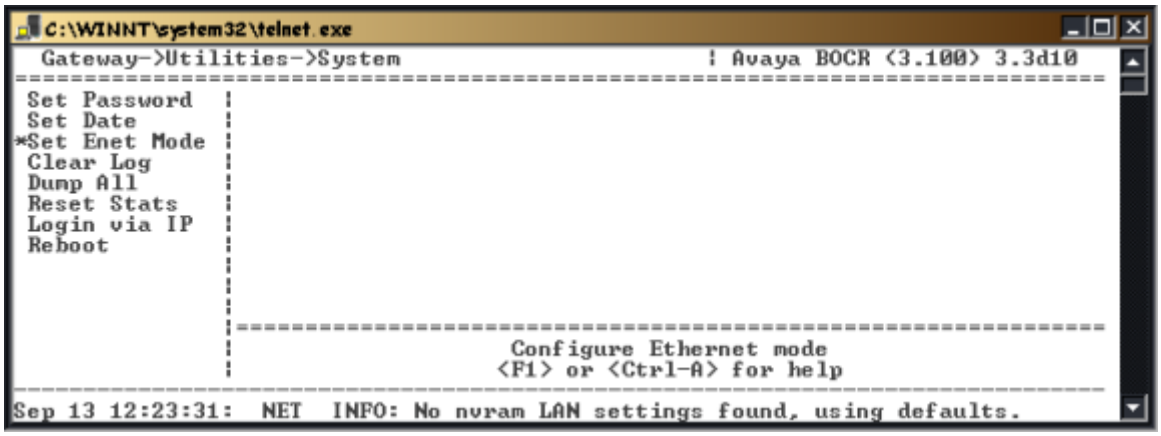


System Menu (Remote)



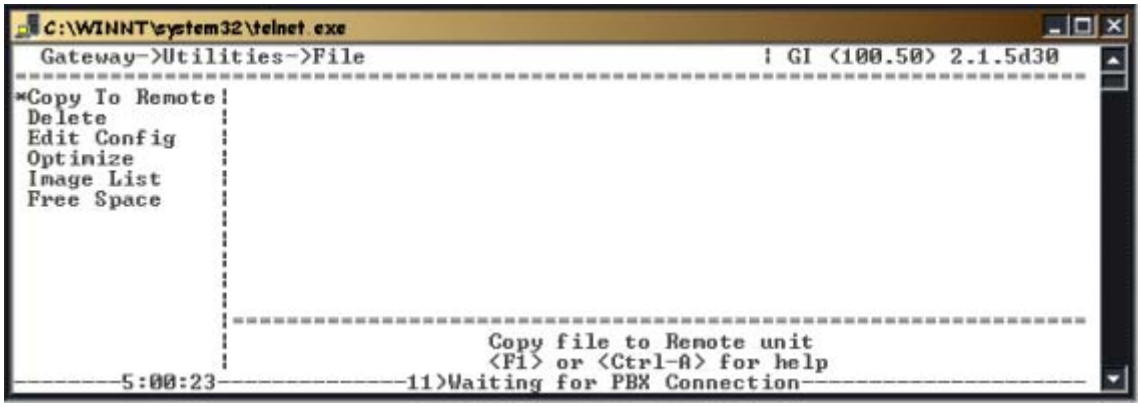
Parameter	To set this parameter see page	For more information on this parameter see page
Name	82	-
Console Baud	83	130
Modem init string	-	-
Use Gateway Time	84	-
Gateway Time Offset	84	-

Utilities->System Menu (Remote and Gateway)



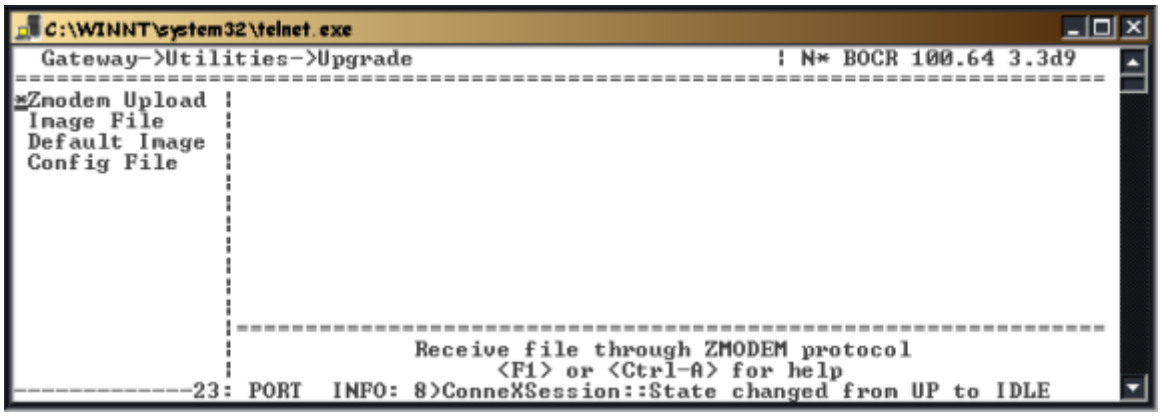
Parameter	To set this parameter see page	For more information on this parameter see page
Set Password	86	-
Set Date	85	-
Set Enet Mode	85	-
Clear Log	-	129
Dump All	-	132
Reset Stats	-	139
Login via IP	-	-
Reboot	114	-

Utilities->File Menu (Remote and Gateway)



Parameter	To set this parameter see page	For more information on this parameter see page
Copy to Remote (GW) Copy to Gateway (Remote)	177	-
Delete	-	-
Edit Config	175	132
Optimize	-	136
Image List	-	133
Free Space	-	132

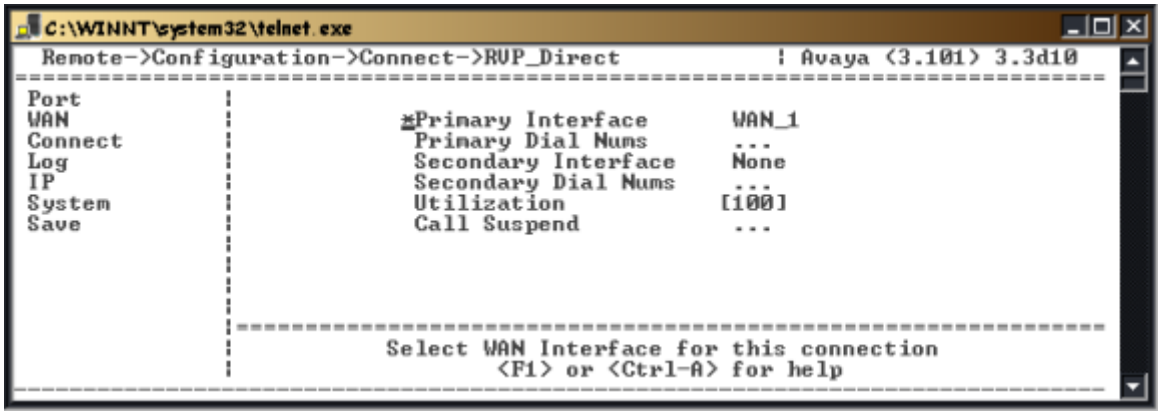
Utilities->Upgrade Menu (Remote and Gateway)



Parameter	To set this parameter see page	For more information on this parameter see page
Zmodem Upload	91	-
Image File	**Error! Bookmark not defined.**	-
Default Image	-	-
Config File	174	-

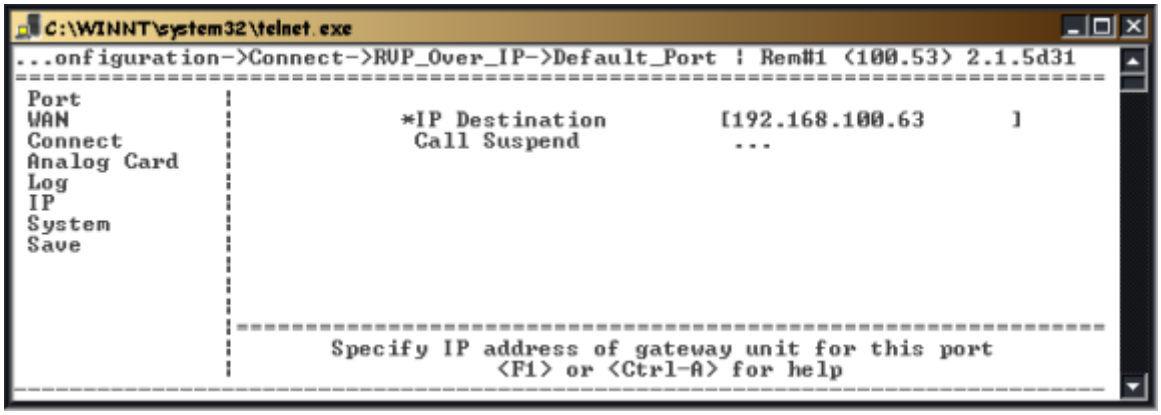
Remote Menus

Connect->RVP_Direct



Parameter	To set this parameter see page	For more information on this parameter see page
Primary Interface	106	138
Primary Dial Nums	106	-
Secondary Interface	106	140
Secondary Dial Nums	106	-
Utilization	106	144
Call Suspend	94	-

Connect->RVP_over_IP Menu



Parameter	To set this parameter see page	For more information on this parameter see page
IP Destination	107	134
Call Suspend	94	-

MI Parameters

Address

(IP->LAN ->Address)

Parameter Location:
`Gateway/Remote ->Configuration->IP->Address`

Description: The Internet Protocol (IP) Address

Usage: A 3-bit address used for IP connectivity. When assigned, the IP Address identifies the PBXgateway and Remote on the network.

Example: 193.245.101.67

Dependencies:

- Must be assigned by the network administrator
- IP Address is required for unit management and RVP_IP connections.
- Must be an assigned static (fixed) address

See Also: Chapter 4 Setting IP Parameters.

Async Rate

Parameter Location:
`Gateway/Remote ->Configuration->WAN->WAN_X->Async_Setup`

Description: The asynchronous data transfer rate.

Usage: This parameter identifies the asynchronous data transfer speed of the WAN port. This value must match the network device speed.

***Note**: This Async Rate typically would be left at the <default> setting of 115200.*

Dependencies: N/A

Auto Connect

Parameter Location:
`Remote->Configuration->Port->Default or Port x`

Description: If Enabled, the phone ports automatically connect when the PBXgateway and Remote units are powered up. This feature also includes a retry timer with backoff. This means that the unit will wait a few seconds between retries and will only try and connect up to a minute before it stops.

Usage: No need to press “1” on Remote phone to connect.

Dependencies: Remote unit only

Banner

Parameter Location:
`Gateway/Remote ->Configuration->Port->Banner`

Description: A message or banner is displayed on the Remote phone on power-up or reboot while the phone is offline.

Usage: Used for ID purposes and customization.

Example: Acme Inc.- Service Division

Dependencies:

- Remote unit only
- Auto-Connect must be disabled, works with two-wire display phones only.

See Also: Chapter 4 *Banner*

Begin Test (IP)

Parameter Location:
`Gateway/Remote ->Utilities->Diagnostics->Test IP`

Description: A function that ensures IP communication is working correctly.

Usage: Same as the MS-DOS PING command. Sends packets back and forth to the unit specified by the IP Address parameter, which is directly below the Begin Test parameter. Upon successful test completion, messages describing the test will appear on the screen.

Dependencies: N/A

Begin Test (WAN)

Parameter Location:
`Gateway/Remote ->Utilities->Diagnostics->Test WAN 1`

Description: A function that ensures WAN communication is working correctly.

Usage: Sends packets back and forth over the WAN. Upon successful test completion, messages describing the test will appear on the screen.

Dependencies: N/A

Clear Log

Parameter Location:
`Gateway/Remote ->Utilities->System->`

Description: Clears the log of events that occur on the PBXgateway and Remote units.

Usage: When you want to clear the log of boot-up and other information that you don't need.

Dependencies: N/A

WARNING: Cannot "Undo" this command. Once selected the Log Messages are permanently removed.

Community

Parameter Location:
`Gateway/Remote ->Configuration->IP->SNMP`

Description: Used for SNMP. The Community string can be set to any character string, but note that a network manager wishing to access a particular EXTender must use the same Community string. This is only a weak form of security as this Community string is passed in plain text in each SNMP packet.

Usage: This variable serves as a password to allow Network Managers to read SNMP information on the EXTender. You should normally set the string to PUBLIC.

Example: If SNMP is used for control and not for management, we recommend using "Public" as a read only community string.

Console Baud

Parameter Location:
`Gateway/Remote ->Configuration->System`

Description: Baud rate of the Console port. The correct Console Baud is a data transfer speed, measured in Kbps (kilobits per second)

Usage: The Console Baud rate is required for the PBXgateway to properly communicate with a PC via the console (serial) port.

Example: 9600

Dependencies: The Console Baud rate of the PBXgateway must match the PCs COM (serial) port speed.

Default Router

Parameter Location:
`Gateway/Remote ->Configuration->IP->Address`

Description: Enter Internet Protocol (IP) address of the default router to use to access device not on your network.

Usage: A 3bit address used as part of the complete IP Default gateway address. When assigned, the default router is used to reach an IP Address not on the local subnet.

Example: 193.245.101.1

Dependencies: Must be assigned by the network administrator

See Also: IP Network Configuration.

Description

Parameter Location:
`Gateway/Remote ->Configuration->Port->Port 1 - 24`

Description: Entering text in this field identifies individual phone ports on the PBXgateway and Remote.

Usage: The description field provides up to 15 characters for customizing each port with descriptive text.

Example: Mary Ellen in Dallas TX

See Also: *Set Port Description* on page 69.

DNS

Parameter Location:
`Gateway/Remote ->Configuration->IP->DNS`

Description: Domain Name System (DNS) works in conjunction with a DNS Server. The DNS server resolves Domain names to IP addresses.

Usage: Use this field to specify the IP address of your DNS Server and the fully qualified Domain Name.

Example: MCK.com

See Also: *DNS Setup* on page 80.

DTMF

(Avaya Only)

Parameter Location:
`Gateway->Configuration->Port->Voice`

Description: DTMF is a signal generated by pressing numbers on the keypad of a phone. These tones can be sent across the network and received at the alternate unit as an in-band (voice) signal. The in-band signal is generated by the PBX/KSU or remote phone.

If the DTMF tone is sent out-of-band (signaling) the DSP on the alternate unit generates the tone. Enable/Disable sending Dual Tone Multi-Frequency (DTMF) tones as voice (in-band) as opposed to signaling (out-of-band).

Usage: Out-of-band provides a clearer tone for higher compression algorithms (G.729A).

Dependencies: Avaya Protocol only.

See Also: *DTMF* on page 63.

Dump All

Parameter Location:
`Gateway/Remote ->Utilities->System`

Description: This parameter will dump the entire log and configuration files to the screen to allow a terminal program to capture the text.

Dependencies: A PC must be connected to the console port.

Usage: This provides an easy way to transfer the log file to a text file on the PC.

Edit Config

Parameter Location:
`Remote/Gateway->Utilities->File`

Description: This is a file saved within the EXTender Flash file system, which contains all configuration parameters. Use this command to create a new config file.

Example: Runtime.rem (remote) or Runtime .swt (Gateway)

Dependencies: Must use the correct file type for the unit.

See Also: *Editing Non-Active Configuration Files* on page 175.

Free Space

Parameter Location:
`Remote/Gateway->File->Free Space`

Description: This parameter indicates how much flash file space is available (bytes) to load another file. Your free space should exceed the size of the file that you are downloading.

Example: Runtime.rem (remote) or .swt (Gateway)

Dependencies: NA.

See Also: NA

FTP

Parameter Location:
`Remote/Gateway->Configuration->IP`

Description: Enable/Disable File Transfer Protocol (FTP) access.

Usage: When FTP is enabled, files can be transferred to/from the flash file system via the LAN.

Dependencies:
IP Address
LAN
IP Network

See Also: See page 78 for more info on FTP set up.

Gateway (Static Routes)

Parameter Location:
`Remote/Gateway->Configuration->IP->More ->Static Routes->route_x`

"x" is a number from 1 to 10.

Description: The IP address of a local router which controls IP traffic to a static route.

Host (Syslog)

Parameter Location:
`Remote/Gateway->Configuration->IP->More ->Syslog->More`

Description: Used to send Syslog messages to a Syslog Host. Consult with your O/S vendor regarding configuration information.

ID (Syslog)

Parameter Location:
`Remote/Gateway->Configuration->IP->More ->Syslog`

Description: Enter Syslog ID

Image List

Parameter Location:
`Remote/Gateway->->Utilities->File ->Image List`

Description: Queries the flash file system for a list of image files.
.rem = Remote, .swt = Switch 9GW) and .mlb = 4000P

Usage: Helps you determine what files are on the Gateway and Remote, useful when grading

Dependencies: NA

IP Destination

Parameter Location:
`Remote->Configuration->Connect->RVPoIP->Port_x`

Description: This is the IP address of the PBXgateway. It is programmed on remote units.

Usage: When connected over an IP network, it is necessary to provide a destination address so that the Remote unit can locate the PBXgateway.

Dependencies: Must be assigned by the System Administrator.

Jitter Delay

Parameter Location:
`Gateway ->Configuration->Port->Default->Voice`

Description: Jitter is the deviation or displacement of voice packets between network devices. Jitter can cause pops and clicks (noise) in the voice transmission. The Jitter Delay parameter provides storage (in milliseconds, up to 250 maximum) capabilities for a delay buffer.

Usage: The jitter delay parameter reduces audible audio noise. Prevents audio from sounding choppy. Only necessary on packet IP networks.

Dependencies: PBXgateway only. The more Jitter Delay, the more tolerant for jitter in the network, but voice is actually delayed.

Recommendations: Start setting at 20-30 msec.

See Also: *Setting Voice Parameters* on page 63

Logout

Parameter Location:
`Remote/Gateway ->Main menu`

Description: This parameter will end the current MI session; either Telnet or VT-100.

Logout Code

Parameter Location:
`Remote->Configuration->Port`

Description: A code sent by the Gateway to the PBX. This code is used to log ACD agents out of the ACD queue in the event of an abnormal disconnect. This prevents ACD agents from receiving a call during a network outage.

Dependencies: Avaya protocol remote units only.

See Also: Extender 6000 Quick Installation Guide

Method (Voice)

Parameter Location:
`Gateway ->Configuration->Default->Port->`

Description: Select voice compression method. Voice is compressed to reduce bandwidth requirements.

Usage: Provides the system administrator with the ability to change the compression method on a port-by-port basis.

Example: G.729A

Dependencies: PBXgateway only. The network must provide adequate bandwidth.

See Also:
Chapter 4: The Management Interface
Voice Quality Expectations on page 161.
Appendix B: Bandwidth Requirements

Mode (WAN)

Parameter Location:
`Remote/Gateway ->Configuration->WAN 1 or WAN 2`

Description: Selects the WAN port connection type.

Usage: The WAN port of the PBXgateway connects the unit to the network device (i.e. CSU/DSU). The mode or interface type selects the protocol used by the unit.

RS-232, RS-530, and V.35 for Synchronous connections

Dependencies: The mode must match the interface type of the network device.

See Also: Chapter 4 Setting the Mode on page 70.

MSB Key

Parameter Location:
`Remote>Configuration->Port`

Description: The MSB (Make Set Busy) key sends a code from the Gateway to the PBX. This code is used to log agents out of the ACD queue in the event of an abnormal disconnect. This prevents ACD agents from receiving calls during a network outage.

Dependencies: Meridian Only.

Optimize

Parameter Location:
`Remote/Gateway ->Utilities->File>`

Description: This parameter will optimize the internal flash file system.

Usage: Used for advanced troubleshooting. Often used to prepare file system for upgrade.

IMPORTANT: Do not use on an active system

Packet Size

Parameter Location:
`Gateway ->Configuration->Port->Default->Voice`

Description: A packet is a generic term for a bundle of data, usually in binary form, which includes the data itself and certain control information. The packets are sent via HDLC over a synchronous-serial connection or via IP over Ethernet. The size of the voice packet can increase voice quality while reducing bandwidth needs. A bigger packet size contains less overhead, but will increase the delay in sending the packets.

Usage: PBXgateway only. This parameter selects the number of voice frames or windows to be included in a single RVP voice packet.

Recommendation: 2 (may need to increase to 4 for some packet networks such as IP)

See Also: Page 63, Setting Voice Parameters.

Packet Trace

Parameter Location:
`Gateway ->Configuration->Port->Ports_x-y ->Port_x->Voice`

Description: Enable/Disable detection of lost voice packets

Usage: If a problem with voice is suspected, enable this feature to allow viewing sent voice packets over the connection.

Dependencies: Enabling this feature will add overhead to the system and may affect voice quality. Only used for debugging.

See Also: Page 63, Setting Voice Parameters.

Password

(Connect)

Parameter Location:
`Remote/Gateway ->Configuration->Port`

Description: A connect password provides a secure link between the PBXgateway and Remote Unit.

Usage: If assigned, the connect password must be entered for communication between the PBXgateway and a Remote unit.

Example: 427stamp

Dependencies: The connect passwords for both units must match.

See Also: Chapter 3, page 67.

Path (Voice)

Parameter Location:
`Gateway ->Configuration->Port->Default->Voice`

Description: Dynamic/Constant voice path following off-hook/on-hook.

Dynamic means that the Branch Office unit uses the available bandwidth when the remote user goes off-hook.

Constant means that the voice path is always reserved.

Usage: Used for applications that are “oversubscribed” allowing the maximum use of available bandwidth. If bandwidth is not available to a user and dynamic voice path is enabled, they hear a “fast busy” and the call will be blocked.

For example, using dynamic would allow all 8 phones to connect on a 128 k connection, but not all phones could go offhook at the same time. Using constant would not allow all the phones to connect, but the connected phones would all be able to go off-hook at the same time.

Dependencies: PBXgateway only.

Recommendations: Constant. Although for Async configurations we recommend Dynamic.

See Also: Page 63, Setting Voice Parameters.

Port Matching

Parameter Location:
`Gateway ->Configuration->Connect->Port Matching`

Description: Port 1 on the Gateway will connect to Port 1 on the Remote, unless User IDs have been assigned to the ports. In a 2:1 config, using RVP_Direct, the Gateway Port Offset is used to determine what Remote is calling. Using RVP_Over_IP, the User ID field is used.

Usage: For 2:1 configs, when you want one remote to have dedicated port to port matching and the 2nd remote to connect on a first come first serve basis. It ensures that the users on remote #1 will always have a port available.

Dependencies: PBXgateway only. User IDs (RVP_Over_IP) override Port Matching.

Primary Interface

Parameter Location:
`Remote>Configuration>Connect->RVP_Direct`

Description: This parameter tells the PBXgateway which Serial WAN port it should try to use in order to bring up phone connections and voice paths. Your Primary Connection port must coincide with the WAN port that is enabled and connected to an appropriate network device. In other words, if you select WAN 1 you must have WAN 1 enabled and connected to a network device.

Available Options:
WAN 1
WAN 2

Dependencies: The WAN port corresponding to this connection parameter must be enabled and connected to appropriate network equipment.

See also: Secondary Interface on page 140.

Priority (Log)

Parameter Location:
`Remote/Gateway ->Configuration->Log`

Description: Selects log message priority

Usage: Used to determine which messages are logged. The log message priority is used to customize the level of troubleshooting desired. This info applies to:Sys, Mgmt, NET and Port priority parameters as well.

Log messages include:
Fatal: Unit is not functioning
Error: Failure
Warning: Problem with unit, still operational
Info: EXTender session, someone connected
Debug: Detailed message (for troubleshooting)
Trace: Packet type tracing

Example: If the (Log) Priority was set to “Info”, then the only log messages that would NOT be saved are messages related to “Debug” and “Trace”.

Priority (Syslog)

Parameter Location:
`Remote/Gateway ->Configuration->IP->More->Syslog`

Description: Selects log message priority to Syslog host.

Usage: Used to determine which messages are logged. The Syslog message priority is used to customize the level of troubleshooting desired.

Log messages include:
Fatal: Unit is not functioning
Error: Failure
Warning: Problem with unit, still operational
Info: EXTender session, someone connected
Debug: Detailed message (for troubleshooting)
Trace: Packet type tracing

Example: If the (Syslog) Priority was set to “Info”, then the only log messages that would NOT be saved are messages related to “Debug” and “Trace”.

Reset Stats

Parameter Location:
`Remote/Gateway->Utilities->System`

Description: Resets the WAN stats and Connect stats.

Usage: Used to clean up the statistics and to help pinpoint problems associated with the unit.

Secondary Interface

Parameter Location:
`Remote ->Configuration->Connect->RVP_Direct`

Description: This parameter tells the PBXgateway which Serial WAN port it should try to use if the Primary Interface fails or runs out of bandwidth. The Secondary Interface is used as a backup or network overflow of the Primary Interface. If you do not have both WAN ports enabled, you do not need a Secondary Interface.

Available Options:
None
WAN_1
WAN_2

Dependencies: The WAN port corresponding to this connection parameter must be enabled and connected to appropriate network equipment.

See also: Primary Interface on page 138.

Size (Log)

Parameter Location:
`Remote/Gateway->Configuration->Log`

Description: The size of the log message in bytes.

Note: After the log is full, the log messages are written over each other, starting from the first message.

Usage: Limits the size of Log messages. Value ranges 4096 to 131072.

Example: [409131072]

Set Password

(Admin)

Parameter Location:
`Remote/Gateway->Utilities->System`

Description: This parameter sets the admin password for the PBXgateway/Remote. This is NOT the Connect Password.

Usage: The admin password will restrict access to the Management Interface (MI).

Example: doc345

See Also: Chapter 3 page 86.

Subnet Mask

Parameter Location:
`Remote/Gateway ->Configuration->IP->Address`

Description: Enter Subnet Mask IP Address

Usage: A Subnet Mask identifies the network number (class) and the range of valid machine addresses on the network.

Example: 255.255.255.0

Dependencies: Must be assigned by the network administrator

See Also: Chapter 3 page 76.

Sync Setup

Parameter Location:
`Remote/Gateway ->Configuration->WAN1 or WAN2`

Description: Enter data rate of device connected to the WAN port of the EXTender unit.

Usage: Matches the synchronize data transfer rate of the Gateway and Remote units connected to the network device (CSU/DSU).

Example: 384,000

Dependencies: Sync rate of the EXTender units must match the CSU/DSU device

See Also: Chapter page 71.

SysContact

Parameter Location:
`Remote/Gateway ->Configuration->IP->SNMP`

Description: Used for SNMP. The name, phone number, etc. of the individual to contact with errors or questions about the EXTender.

Usage: Used for reference purposes.

Example: Ralph Jones

Dependencies: SNMP must be enabled.

See Also: Page 235.

SysLocation

Parameter Location:
`Remote/Gateway ->Configuration->IP->SNMP`

Description: Used for SNMP. The location of the EXTender.

Example: Boston, MA

Dependencies: SNMP must be enabled.

See Also: Page 235.

Telnet

Parameter Location:
`Remote/Gateway ->Configuration->IP`

Description: Enable/Disable Telnet Access

Usage: Enabling this parameter provides Telnet access to the PBXgateway through a PC connected to an IP network.

Dependencies: The IP Address must be assigned by the network administrator.

See Also: Chapter 3 page 76.

Trap Host

Parameter Location:
`Remote/Gateway ->Configuration>IP->SNMP`

Description: Used for SNMP. This menu allows the user to input one to eight IP addresses of nodes or devices (PCs) to which to send SNMP Traps. These nodes should be capable of running some sort of Network Management software (HP Openview®) that is compatible with the SNMPv2c standard. Only these devices will be targeted for Traps. The EXTender does not broadcast Trap packets over the network.

Usage: Used to Set up SNMP.

Dependencies: SNMP must be enabled.

See Also: See page 235.

Trap Path

Parameter Location:

`Remote/Gateway ->Configuration->IP->SNMP`

Description: Used for SNMP. This variable determines the path the EXTender should use to send Traps to the Trap Hosts entered above. The choices are [LAN | WAN | BOTH].

If this variable is set to LAN then the SNMP agent will attempt to send Trap packets out via a wire connection such as Ethernet. If such a connection does not exist then the packet is dropped.

Setting the variable to WAN will cause the SNMP agent to attempt to send Trap packets via the proprietary WAN connection. This is necessary if the Remote is not directly connected to the Net and is being serviced via the proxy SNMP server on the Gateway. If such a connection fails, then the packet is dropped.

Setting the variable to BOTH will cause the SNMP agent to send the Trap packet via both the LAN and WAN connections. If both paths are valid this will produce duplicate Trap messages on the Trap Hosts.

Dependencies: SNMP must be enabled.

See Also: Page 235 for more information.

Trap Priority

Parameter Location:

`Remote/Gateway ->Configuration->IP->SNMP`

Description: This variable sets the minimum priority of log messages to be sent as Traps. It has the possible values of:

Warning
Info
Error
Fatal

Notes:

Setting the value to Warning will allow Traps of priority Warning and above. Setting the value to Error will also allow Traps of priority Fatal, but will exclude Warning and Info.

Usage: This variable is useful for controlling the amount and type of Traps being sent to network managers.

Dependencies: SNMP must be enabled.

See Also: See page 235 for more information.

User ID

Parameter Location:
`Remote/Gateway ->Configuration->Port->Port_x`

Description: The User ID is a numeric value assigned to the phone port.

Usage: The system administrator assigns a User ID for identification purposes and security. It also determines which PBXgateway port a remote connects to.

Dependencies: Must be entered for access to the phone port.

See Also: Chapter 3 page 68.

Utilization

Parameter Location:
`Remote>Configuration->Connect->RVP_Direct`

Description: This parameter allows the system administrator to oversubscribe the network link. It is the amount of total required bandwidth to actually reserve for each phone. This parameter would remain at the default setting of 100 for the majority of installations.

Example: Need 128K of bandwidth but only have 115 K available.

Required bandwidth = 115k = 90%
Available bandwidth 128k

A value of “90” would be entered under Utilization.

Dependencies: Remote unit only.

Web Server

Parameter Location:
`Remote/Gateway ->Configuration->IP`

Description: This parameter enables you to configure the PBXgateway & Branch Office units via a Web server, as opposed to a Telnet or direct connection.

This page intentionally left blank.

Chapter 5: Troubleshooting

This Chapter provides information to locate, isolate, and correct operational errors, communication errors, and functional problems with the PBXgateway, Branch Office, and EXTender 4000 units.

This Chapter is divided into six principal areas for troubleshooting:

- Baseline Checklist
- Status LEDs
- Troubleshooting Procedure
- Voice Issues
- Status Menus
- Remote Phone Messages

Baseline Checklist The baseline checklist is a list of simple checks used as a starting point for troubleshooting the devices. It covers basic installation requirements, wiring info and network information.

Status LEDs

Single and tri-color LEDs, located on the front and back panels of each unit. The LEDs blink in specific sequences indicating the unit status during Power-Up as well as providing status information on the System, WAN Port and Ethernet (LAN) connections, during normal operations.

Troubleshooting Procedures A set of procedures providing step-by-step instructions to identify and rectify problems.

Voice Quality Expectations Information on common issues associated with voice compression.

Status Menus

Diagnostic menus providing statistical information on all 8 or 12 phone ports, both WAN ports, Connect stats, Log and IP stats and general System information.

Remote Phone Messages A chart listing error messages that are displayed on the Remote phones (connected to the Remote unit).

Baseline Checklist

The Baseline Checklist is a logical list of items that are associated with an active and operational installation. These items should be checked-off BEFORE you attempt to troubleshoot either the Gateway or Remote unit.

***Note**: If any of the items are NOT true as stated, they should be corrected as detailed herein, and then continue with the remaining items for both units to verify a complete installation*.

Network Checklist

Verify that the existing network is capable of transmitting and receiving data packets.

Verify the correct cable is used to connect the unit to the network device.

Synchronous Serial/RVP_Direct

Check that the sync rate of the network device matches the sync rate setting for both the PBXgateway and Branch unit.
(see page 71 for setting the Sync Rate)

Make sure the sync mode of the Gateway and Branch units match the network device signaling type (V.35, RS-530, RS-232).
(see page 71 for setting the Sync Mode)

IP/RVP_IP

Check that the IP address information (IP Address, Subnet Mask, Default Router) for the PBXgateway, Branch unit and EXTender 4000 is set correctly. (see page 76 for setting IP Parameters)

PBXgateway Unit Checklist

Verify that the unit is plugged into an active AC outlet.

Verify that the RJ-21 cable between the unit and the PBX or punch-down block is secure.

Verify that the DB-25 cables are secure between the units and network devices. (Synchronous-serial connection only)

Verify that the Ethernet cable is connected and that there is an active link status on the Gateway and Network Hub (IP Connections).

Branch Office Unit Checklist

Verify that the unit is plugged into an active AC outlet.

Verify that the RJ-21 cable between the Branch Unit and the break-out box or punch-down block is secure.

Verify that the DB-25 cables are secure between the unit and network devices. (RVP_Direct connection only)

Verify that the Ethernet cable is connected and there is an active link status on the Branch and Network Hub.

EXTender 4000 Unit Checklist

Verify that the power supply is plugged into an active AC outlet and the power cable is plugged into the unit.

Verify that the Ethernet cable is connected and there is an active link status on the EXTender 4000 and Network Hub.

Status LEDs

PBXgateway and Branch Office EXTender

When the units are powered-up, a series of self-diagnostic tests are performed and displayed as a series of LED blinks. The following chart lists the different status sequences.

Power Up Sequence

The following steps are performed automatically when the PBXgateway and Branch Office units are powered-up.

DRAM Tests – Checks the internal DRAM (Dynamic Random Access Memory) chips.
Selftest – Diagnostic routine to verify operation of various hardware components of the unit.
ROM Countdown – A series of LED blinks that display the process of loading the Runtime image.
Runtime Image – This is the software executable file.

Figure 79: PBXgateway Power up Test

***Note**: The EXTender 4000 utilizes only one LED, labeled "Status" to display results of all four tests. (see page 155 for more information)*

Step #1 DRAM Tests

When the unit is powered up it runs four DRAM tests. The Power LED flashes green while these run. If you look closely the Power LED flashes at slightly different speeds as the different tests run. If the tests pass then the Power LED goes solid green. If any of the tests fail then all four status LEDs go solid red and the EXTender halts. (Refer to the System Status LED chart on page 153 for more information)

***Note**: The DRAM tests are only run when the unit is powered on, rebooting the device without power cycling it will jump right into the selftest diagnostics.*

Step # 2 Selftest

After the DRAM tests a set of selftest diagnostics run. The selftest diagnostics only affect the LEDs if there is a failure. On failure, the Power LED changes from solid green to solid yellow (and remains that way as long as the unit is powered on, or the selftests are run again and pass). The Power LED will remain "Yellow" (indicating a failure) instead of "Green".

Additionally, the first four Port Status LEDs are temporarily lit with a code indicating the last selftest failure. The pattern is a binary number indicating the kind of failure. Table 15, shown below, provides information on the port failure patterns including a short description and required action.

***Note**: If there are multiple failures you will only see the pattern for the last failure. (refer to the System Status LED chart, on page 153, for more information)*

Power LED	**Port LI**				**Description**	**Action**
	1	2	3	4		
Yellow	ON	OFF	OFF	OFF	RTC failure (error code 0x8)	Hardware Fault- Power cycle the units If self-test fails repetitively, contact customer service.
Yellow	ON	OFF	OFF	ON	DSP failure (error code 0x9)	
Yellow	ON	OFF	ON	OFF	I^2C failure (error code 0xA)	
Yellow	ON	OFF	ON	ON	Ethernet failure (error code 0xB)	
Yellow	ON	ON	OFF	OFF	PLD failure (error code 0xC)	

Table 15: Failure Patterns

Step #3 ROM Countdown

After the diagnostics run the ROM goes through a short countdown on the console. During this time the WAN1 LED flickers green. The WAN1 LED goes solid green and the WAN2 LED 'flickers' green while the runtime image is being loaded into memory. WAN2 goes solid green when the runtime image is successfully loaded into memory. Control is then passed to the runtime image (see Step #4).

Step #4 Runtime Image

The runtime image first turns all system status and Port Status LEDs off, except for the Power LED (which is solid green if there are no self-test failures or solid yellow if there are self-test failures).

During initialization the runtime image flickers Port Status LED1 while it's downloading the Programmable Logic Device (PLD), and then makes Port LED1 solid once the PLD download is complete. Similar flickering and solid LED patterns are used when downloading each Digital Signal Processor (DSP), where Port LED2 is the signaling DSP, and Port LED3-LED8 are the voice DSPs. So when the runtime image is starting up you see each Port LED 1 through 8 successively flicker and go solid until all eight are solid.

After the PLD and DSP downloads are complete the Port LEDs drop into their normal operating patterns.

System Status LEDs

The PBXgateway and Branch Office units have four tri-color LEDs – (RED, Yellow, and Green) indicating the unit status once the runtime image is operating and the status condition of the WAN ports has been determined.

IMPORTANT: Refer to page 156 for troubleshooting the units using the System Status LEDs.

	LED States						
LED LABEL	**Off**	**Solid Red**	**Solid Yellow**	**Flashing Yellow**	**Solid Green**	**Slow Green Flash**	**Fast Green Flash**
PWR	Off	DRAM Test failed	Self-test Diagnostic Error	-	Has power	-	-
WAN1	Not enabled	No Device connected	DCE Ready	DCE Ready	Carrier Up	Remote Up	Remote test
WAN2	Not enabled	No Device connected	DCE Ready	-	Carrier Up	Remote Up	Remote test
WAN3	Not enabled	No Device connected	DCE Ready		Carrier UP	In Use	Remote test
*Analog	-	-	Card detected and Onhook	Ringing	Onhook on analog call.	-	-

* Applies to **EXT**ender 6000 equipped with an Analog Port only.

Table 16: WAN and Power Status LEDs

DRAM Test Failed: This indicates that one or all of the four DRAM tests have failed. This hardware failure condition can be caused by a faulty internal DRAM chip. Recycle the power on the unit and contact MCK if the light remains “Red”.

Selftest Diagnostic Error: This indicates that there is a problem with a selftest, indicating a possible hardware problem. Recycle the power on the unit and contact Customer Support if the light remains “Yellow”.

Not Enabled: Enable the WAN port, if the WAN port is needed.

No Device Connected:
Check the wiring and cable pinouts between both units and the network device. *(see page 37 for pinout information)*
Check the cable.

DCE Ready: Device connected but no network link to the alternate site. Possibly a network error between devices. Check all cables and power to the units.

Carrier Up: Network link established. Try to establish phone connection from the Remote unit.

Remote Up: Phone at the remote site is online.

Remote test: This test sends packets to the alternate site to check the network condition. (see page 158 for more info)

Port Status LEDs

The PBXgateway and Branch Office units each have eight or twelve LEDs indicating the status of the twelve user phones (Branch unit) or PBX/KSU ports (PBXgateway).

IMPORTANT: Refer to page 157 for troubleshooting the unit using the Port Status LEDs.

Off	Solid Green	Slow Green Flash	Fast Green Flash	Green Flicker
Port is disabled	Port is enabled, but not extended	Extended, and user is on-hook (phone is not in use).	Extended and the user is off-hook. (phone is in use)	Port is enabled, there is a bad connection to the PBX or phones.

Table 17: Port Status LEDs

Enable the Phone port as follows:
Connect the Gateway or Branch unit to the Management Interface (MI).

Navigate to the Port menu using the following path:
->Configuration->Port

Check the “Enabled” field indicates “YES” or if the field is set to <Default>, check that the default setting has all ports enabled.

Check the following:

Check that the correct module is installed at the location. (Gateway unit installed at the corporate facility, and a Remote unit at the Branch office)
Check the wiring to the punch-down block.
Check for a loose connection on the back of the units.
Check for a damaged RJ-21cable.
If you are sure everything is correct, you may have a bad telephony port on the EXTender or PBX.

***Note**: The most common cause of this problem is faulty wiring. You should double-check all wiring*.

EXTender 4000

Once the **EXT**ender™ 4000 is properly connected it will begin a series of self-diagnostic tests that are displayed as a series of LED flashes. The "Status" LED will blink for several seconds as the module is initializing.

Once the power-up sequence has finished, (see page 151) the state of the LEDs should be:

Figure 80: Front Panel

Label	Description
Status	Blinking while module is initializing.. Off when not powered. After unit is powered: On Solid Green when enabled but not extended. Slow Green Flash when extended and on-hook. Fast Green Flash when extended and off hook. Green Flicker when there is no connection to a telephone.
CLN	Blinking when an ethernet collision condition exists.
PC	Off if nothing plugged in or connection is bad. On solid when a good connection is established. Blinks when traffic is sent.
LAN	Off if nothing plugged in or connection is bad. On solid when a good connection is established. Blinks when traffic is sent.
EXT	Normally off, blinks when the **EXT**ender™ 4000 sends ethernet traffic.

Table 18: EXTender 4000 LED States

Troubleshooting Procedure

PBXgateway & Branch Office units

The following procedure provides a step-by-step process for identifying and rectifying problems with the PBXgateway and Branch Office units. Each step is a question requiring a “Yes” or “No” response. Each response has a series of checks or actions necessary to correct the problem.

Prerequisites:
Both units must be powered-up with some LED blinking patterns visible.
Both units must be connected to an active network capable of sending and receiving packets.

System Status LEDs

After the units have gone through the self-diagnostics tests (see page 151) the PWR LED should light solid Green.

Is the PWR LED lit “Green” on each unit?

No
If the PWR LED is lit “Yellow” this indicates a self-diagnostic problem with the unit.
(Refer to page 153 for more information)
If the PWR LED is lit “RED” this indicates the DRAM test has failed. (Refer to page 153 for more information)

Yes
The active WAN port (WAN 1 or WAN 2) that is connected to the network device should be lit solid “Green”. This indicates that the carrier or network link is established.

Note*: If the LED is a slow “Green” flash, this indicates that a phone at the remote site is online. A fast “Green” flash indicates that the Remote is in a test mode.*

Go to next page

Is the active WAN port LED lit solid “Green”?

No
If the LED is lit “Yellow”, this means that the network device is connected, but there is no network link to the alternate site. (Refer to page 153 for more information)
If the LED is lit “RED” there is no network device connected to the unit. (Refer to page 153 for more information)
If the LED is OFF, this means that the WAN port is not enabled. (Refer to page 153 for more information)

Yes
Continue with Port Status LEDs on the next page

Note*: If you are using your Gateway and Branch in RVP_IP mode, you do not need your WAN port enabled.*

Port Status LEDs

After the units have gone through the self-diagnostics tests (see page 151) and loading the runtime image, all eight or twelve phone port LEDs should light solid “Green”. This indicates that the phone port is connected to a digital port on the PBX and to a phone connected to the Remote, but not extended.

Are the Port LEDs (labeled 1 through 8 or 12) lit solid “Green” ?

No
If the Port LED is OFF this indicates the port is disabled. All phone ports are enabled by default. (Refer to page 154 for more information)
If the port LED blinks with a green flicker this indicates that the port is enabled but there is a bad connection to the PBX or phones. (Refer to page 154 for more information)

Yes

Ports are ready. Press ‘1’ to connect. (If Auto-connect is enabled, it is not necessary to press ‘1’.) As each remote phone is connected the LED will begin to flash slowly. This means that the phone is enabled but still not in use (on-hook).

Does the port LED blink with a slow, green flash?

No

Check the log messages within the MI for obvious Port errors.
(see Appendix E *Log Messages* for more info)
If using WAN connectivity, test the WAN connection. (Refer to page 158 for more information)

Are there any messages displayed on the Remote phones?

No

Place a call using a phone connected to the Remote unit. As each remote user places a call the LED will begin to flash faster. This means that the phone is extended and in use (off-hook) by the remote user.

Yes
Refer to page 171, for a detailed list of Remote Phone Messages.

Check that the phone is plugged into the breakout box or equivalent.
Check the line cord from the phone to the box.

Can you place a call? (The port LED should blink with a fast, green flash)

No
Check the wiring to the PBX. (see the page 37, for pinout information)

Is the Voice Quality acceptable?

No
Go to “Voice Quality Expectations” on page 161.

Yes
Everything is Ok

Test the WAN Connection

If all of your Port and WAN LEDs indicate the units are installed properly, but you still cannot connect the remote phones, you should test the WAN connection.

***Note**: This is only applicable for connecting over a synchronous-serial network (RVP_Direct).*

Test the WAN connection as follows;

***IMPORTANT**: This test will not run if any phones are off-hook.*

Access the Management Interface (MI) on the Switch or Remote unit.

Reset the WAN Port.

Navigate to the Diagnostics menu using the following path:
Utilities->Diagnostics->Test WAN

Select the proper WAN Port and using the Default values, select “Begin test”. This test will send voice packets to the offsite unit and will count the packets as they are sent back.

The MI will run the test and, upon its completion a “Test Results window” appears.

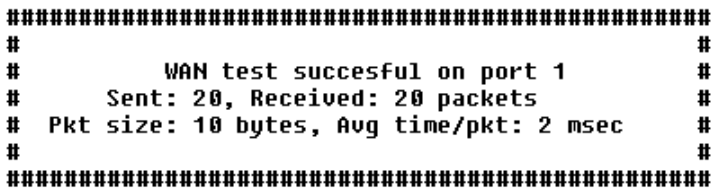
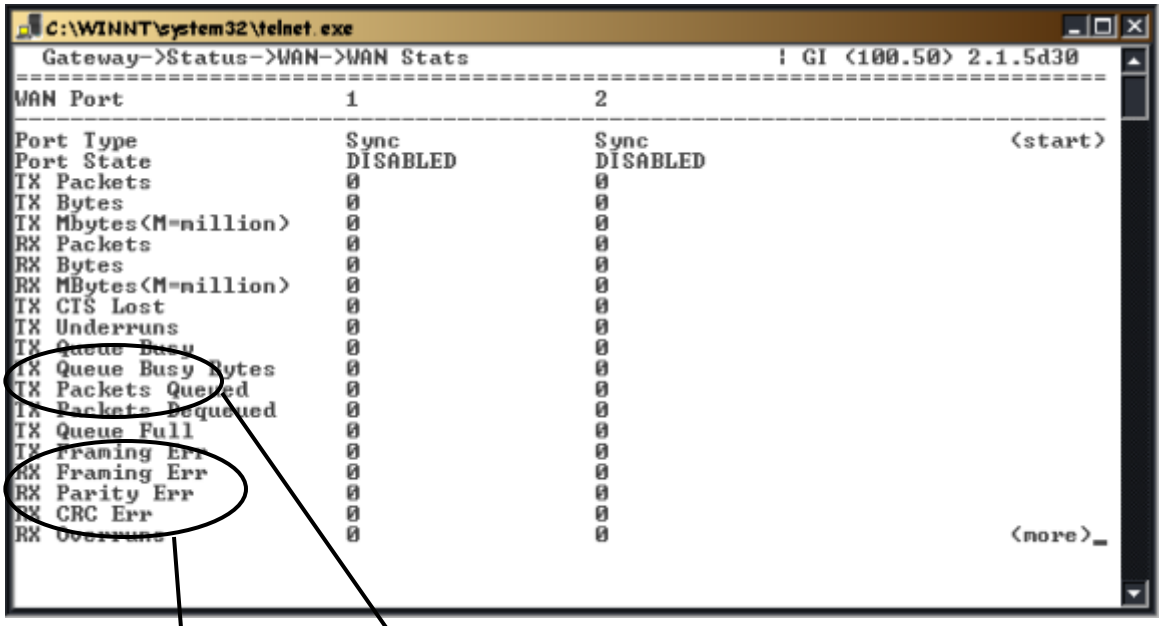


Figure 81: Test Results Window

The test results are shown below;



If the items circled register any values the problem is firmware related. Power-cycle the unit to clear the values and retest.

If any of the circled items (shown with a “0” value) display any values, there is a problem with the network. The network device may be in a loop-back, which means the packets are sent to the device at the remote site, but the packets are not received by the Remote unit. Verify the network devices are working properly.

Test the IP Connection

If all of your Status LEDs indicate the units are installed properly, but you still cannot connect the remote phone, you should test the IP connection.

***Note**: This is only applicable for connecting over a synchronous-serial network (RVP_IP).*

Test the IP connection as follows;

***IMPORTANT**: This test will not run if the phone is off-hook.*

Access the Management Interface (MI) from the unit.

Reset the IP Port.

Navigate to the Diagnostics menu using the following path:
Utilities->Diagnostics->Test IP

Using the Default values, select “Begin test”. This test will send voice packets to the offsite unit and will count the packets as they are sent back.

The MI will run the test and, upon its completion a “Test Results window” appears.

Figure 82: Test Results Window

From a PC on the remote network make sure that you can reliably ping the PBXgateway.

From a PC on the corporate network, make sure you can ping the EXTender 6000 and 4000 on the remote network.

Voice Quality Expectations

EXTenders use industry-standard voice compression methods to allow multiple users to connect using less bandwidth. While the voice quality should remain excellent in all circumstances, you may notice some minor affects depending on the voice compression selected. The person you are talking to on the other end should not notice these affects in most instances.

The G.729A algorithm only uses 8Kbps for its audio path (plus overhead). It therefore dramatically reduces the amount of network bandwidth required to extend multiple phones. It also provides excellent voice quality to all parties involved in a conversation. However, this algorithm is designed to optimize audio in the frequency range of the human voice. Tones outside of that range may sound muffled. Also, listening to audio that has already been compressed may sound slightly less clear. Here are some of the affects you may notice with compressed audio:

Hold music ay sound less clear.
Dial Tone, DTMF Tones, and phone Rings may sound garbled particularly on speakerphone. They still should function properly 100% of the time.
May experience some minor echo and reduced audio clarity when calling some Cell phones. They often already compress audio.
May hear some echo and notice minor delay in the conversation if calling internationally. This is caused by the delay in providing compressed audio and the fact that calling internationally may already introduce some delay.

If you are experiencing any of these problems and feel that it is not presenting you with adequate voice quality, we recommend using the ADPCM 32 voice compression method. While it requires more network bandwidth, it uses less voice compression and therefore minimizes the chances that any of these affects ever occur.

It is important to know the following.

The type of audio problem

Example: Echo (see next page) , broken or choppy audio, lost calls, etc.

When does the problem occur?

All calls
Internal calls only
External calls only
Intermittently some external calls

Do all users experience the problem?

Echo Problems

Understanding and Correcting Echo Problems

The PBXgateway and both EXTender 6000 and 4000 employ the industry standard G.165 echo canceller with some proprietary MCK improvements to help eliminate or reduce echo even further. However, it is not possible to cancel all instances of echo 100% of the time. It should be noted that echo perceived by extended PBX users, will not be perceived by the party on the other end of the call.

EXTender's Impact on Echo

Because EXTenders deal exclusively with digital audio on the line side of a PBX, they cannot cause any echo. However, if you experience any echo from your connection to the PSTN (Public Switched Telephony Network), the EXTender application could make it noticeable because of increased delay in the audio path. For example, if echo occurs on a line after only a few milliseconds, your ear cannot detect the echo. However, if the echo occurs after 100, 50, or even 20 milliseconds, your ear will likely detect the problem. The G.165 echo canceller can cancel echo up to certain limitations. If you have a noticeable echo problem, you should look into the following:

If you experience echo on all external calls, you probably have a problem with your PSTN trunk lines. Most likely they are analog, and those analog lines are generating a great deal of echo when interfacing with your PBX. Non-extended PBX phones may not perceive the echo, due to the fact that echo without delay, does not sound like echo.

Cause: The most common cause of consistent echo on all external calls, are analog trunk lines that are out of specification, or a problem with the termination within the PBX. Most commonly there is an impedance mismatch between the analog line and your PBX. Also, the db level of the analog circuit may be too high. Analog circuits that are "hot" are a common cause of echo. Again, that echo may not be perceived on non-extended phones, but that is only because there is no delay.

Possible Solution: If you have analog lines, you should consult your local phone company and ask for the exact specifications of that line. They may need to go onsite to measure the characteristics of your analog circuits.

If you only experience echo occasionally on external calls, your system is probably fine. The echo probably only occurs when calling to or receiving calls from a party that is using a) analog lines, b) a cell phone, or c) analog trunks on their phone system. In this case there is little you can do. The echo canceller included with the EXTenders usually will cancel this echo after a second or two, but occasionally the echo goes beyond its capabilities. However, it should be noted that the party on the other end of the call will not experience this echo.

If you experience a slight echo on all external calls, but it goes away after a second or two, that is normal with analog trunk lines. If you have analog trunks into your PBX, the echo canceller frequently takes a second or two to detect levels of what is echo and what is voice. Then it starts to cancel the echo. The only way to improve that situation is to replace your analog trunks with digital trunk lines.

Management Interface (MI) Status Menus

RVP_DIRECT Menus

Port Status

Look for:

Significant “NC” values on any phone port. This value indicates that the port is enabled but there is a bad connection between the Remote unit and the phone or the PBXgateway and the PBX.

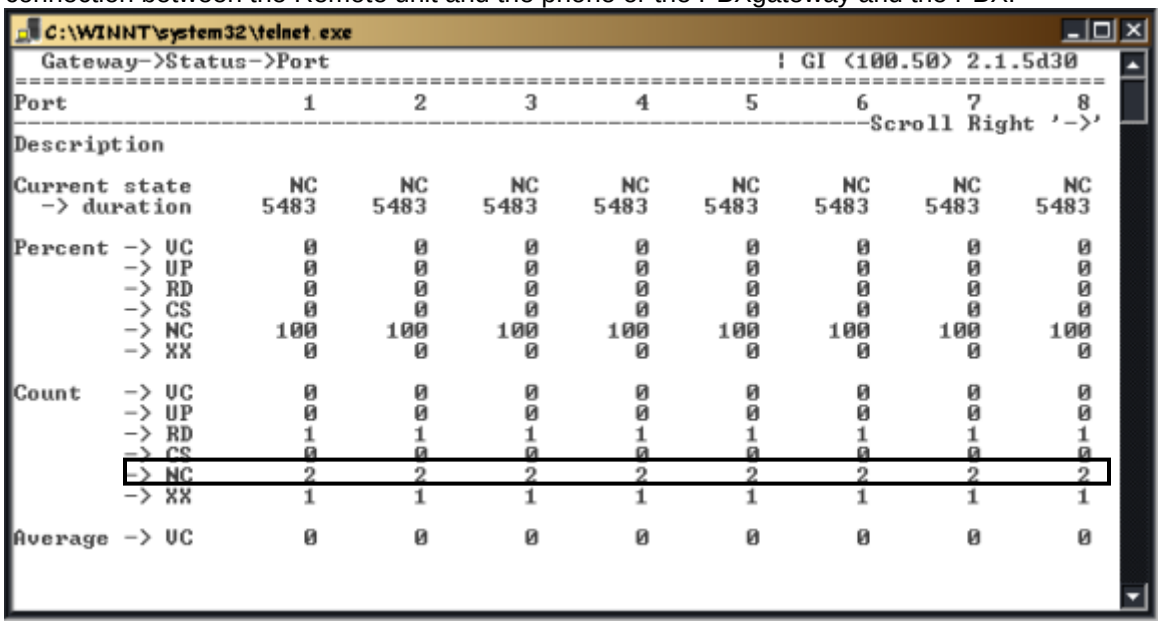


Figure 83: Port Stats

WAN Stats

Look for:

Any “Framing Errors”, “Parity Errors”, “CRC Errors”, “Overruns”, “DCD Lost”, “CTS Lost” or any “Busy” type errors. Significant values indicate WAN device problems.

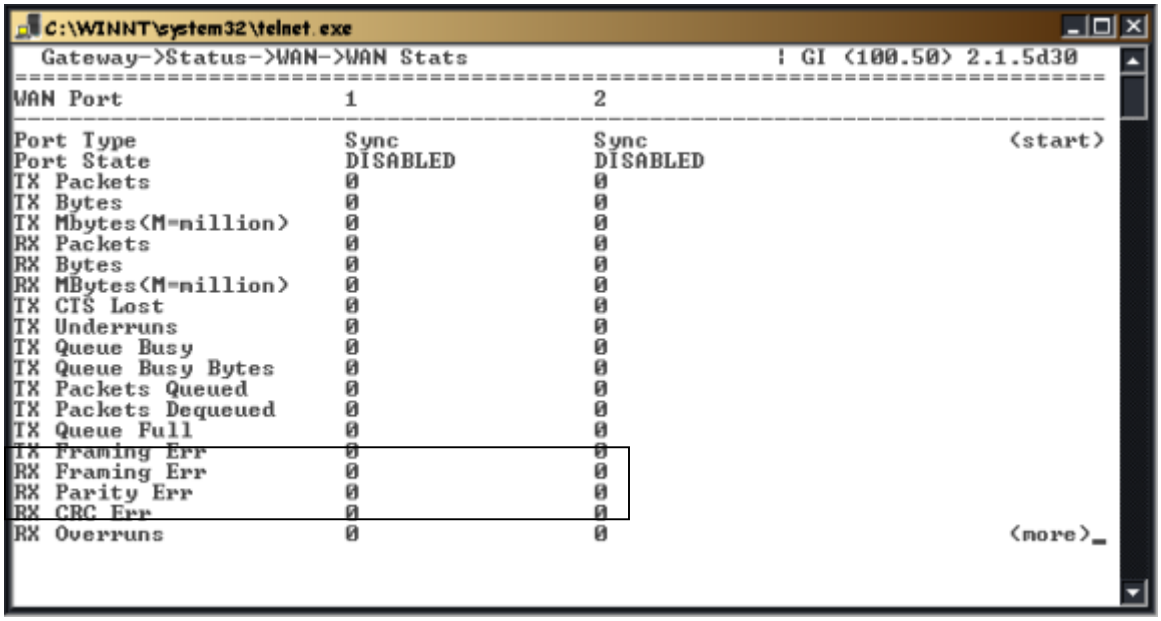


Figure 84: WAN Stats

WAN Bandwidth

Look for:

Any “Clipped ” (Kbps) count. This indicates packets that were not sent as there may not have been enough bandwidth. If this value exceeds the actual Bandwidth that you have assigned in the WAN menu, you may need to increase the WAN Bandwidth.

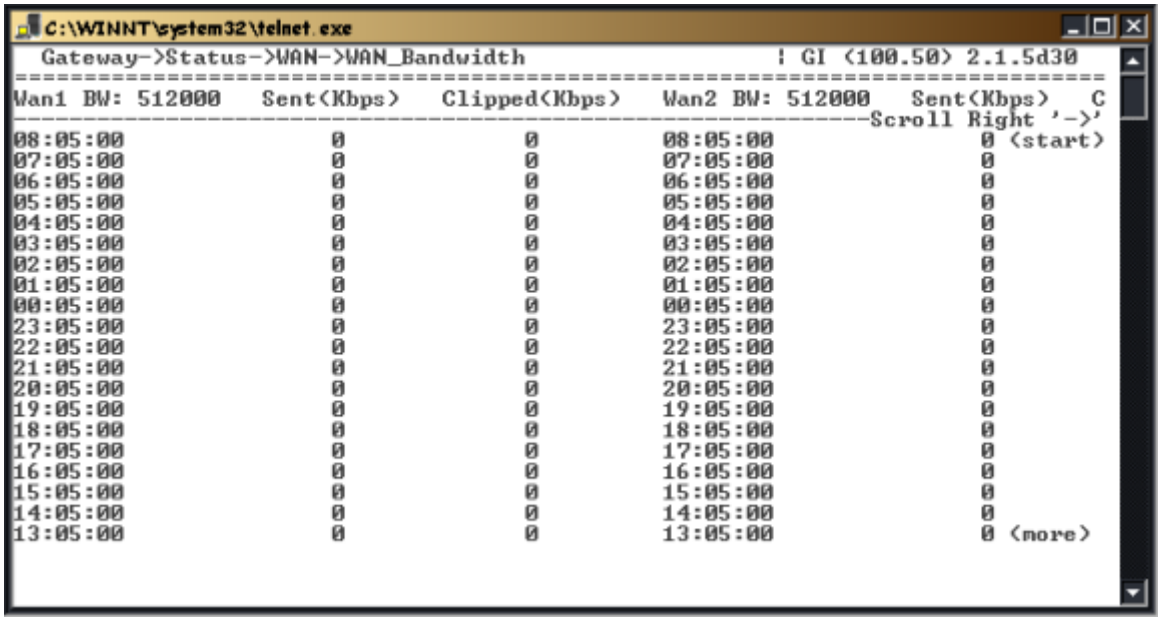


Figure 85: WAN Bandwidth

Connect Info

Look for:

A “Current State -> extended” value of “No”. This indicates that the remote phone is not extended, or may not be connected.
Significant “Lost Signal” values on any phone port. This value indicates that the port has not completed phone connections.
V42 “resync” errors indicates that the network device may have reset itself due to significant network errors.

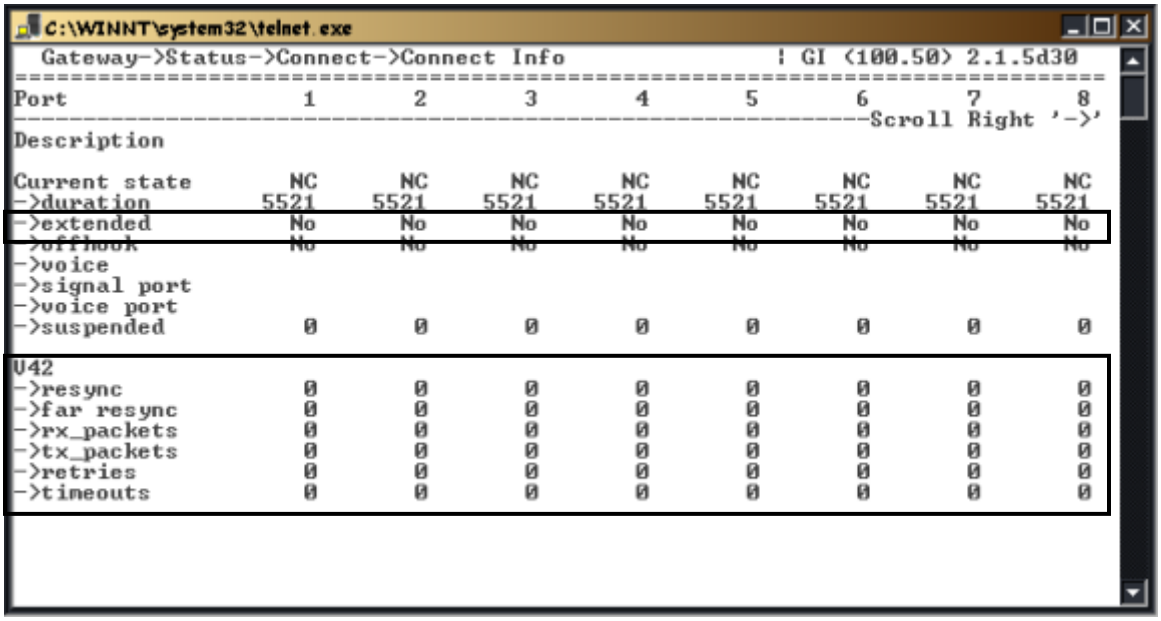


Figure 86: Connect Info

Connect Stats

Look for:

- A high number of "Connect tries". This indicates the remote is trying to connect to the PBXgateway. If this value is high (maybe above 20), there could be a WAN problem.
- A high number of "Disconnect->carrier lost". This directly relates to WAN outages. The WAN devices may be intermittent.
- Any "Disconnect by port offline" values. This indicates the remote port has been disconnected - possibly a wiring problem.
- Any "Disconnect by port in use" values. Indicates the remote is connecting to a port that is already being used. There may be a configuration problem, or the port itself has a problem.
- Any "Disconnect by no voice" values. The voice path has been lost. This could be related to a port problem or even a wiring problem.
- Significant amount of "Disconnect by bad password" values. If this value is high (maybe more than 20), an unauthorized user may be attempting to connect from the remote phone.
- Significant “Blocked call” values on any phone port. This value indicates that the unit has been oversubscribed, indicating that because of bandwidth limitations, some of the phone calls must be “Blocked” or stopped from making a connection if there is no bandwidth available.
- “Lost signal” values on any port indicate that the unit has phone connection problems. Check all wiring.

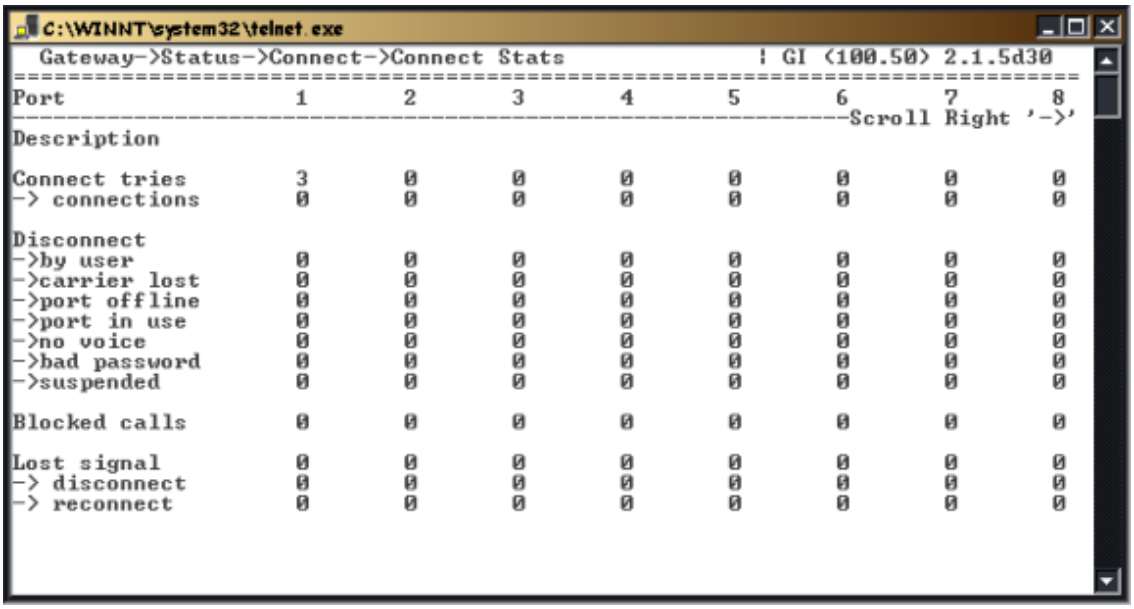


Figure 87: Connect Stats

RVP_IP Menus

IP Active

Make sure correct information is shown. If this is not correct, go to the "Configuration->IP->Address" menu, and enter the correct info. A large number of collisions could indicate network traffic problems.

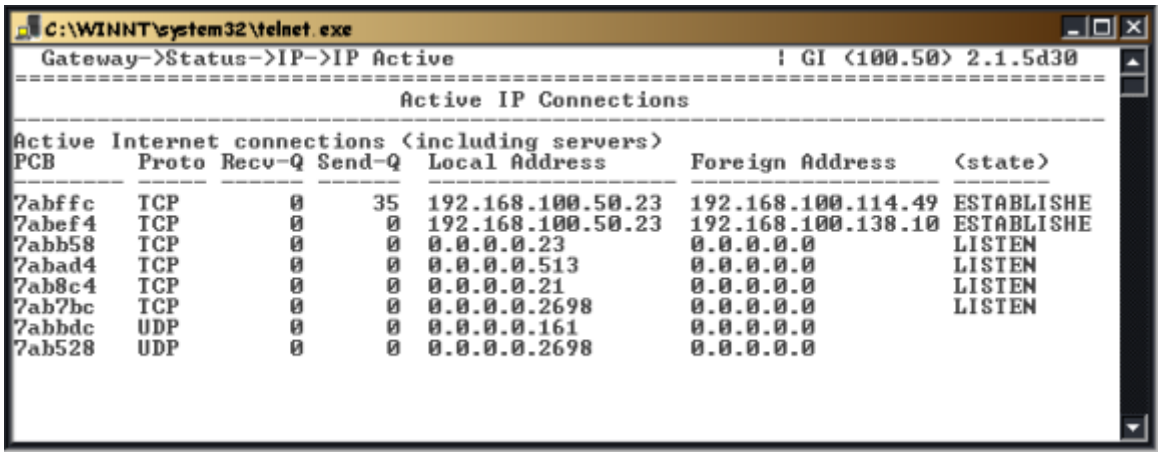


Figure 88: IP Info

IP Rx Stats

Look for:

Any value, that increments other than "total", and "cantforward".

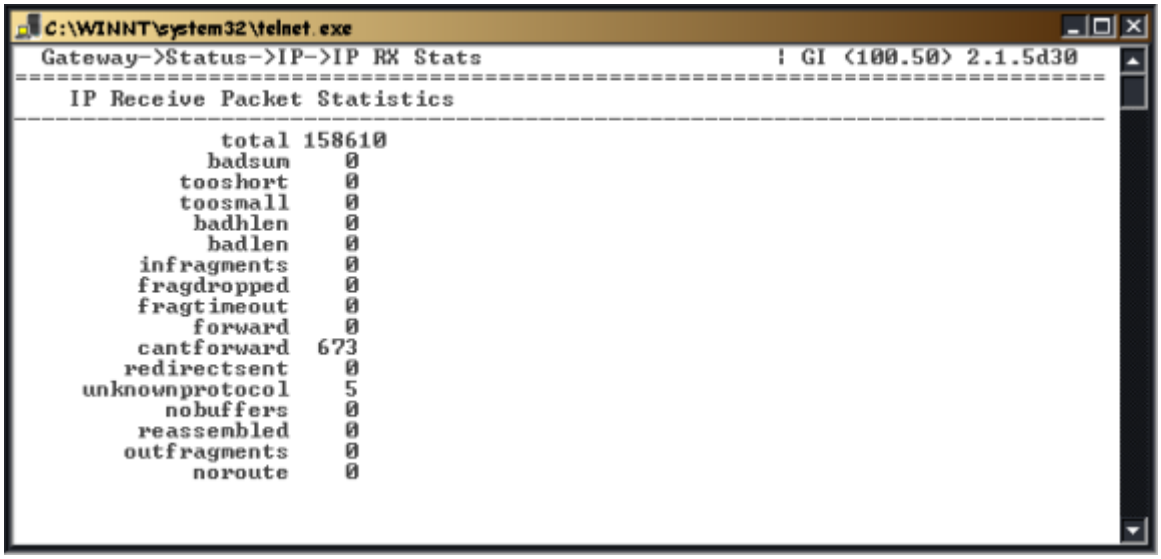


Figure 89: IP RX Stats

IP ARP

Make sure you can see your "Default gateway" in this table; especially if your Branch Office unit is on a remote LAN.

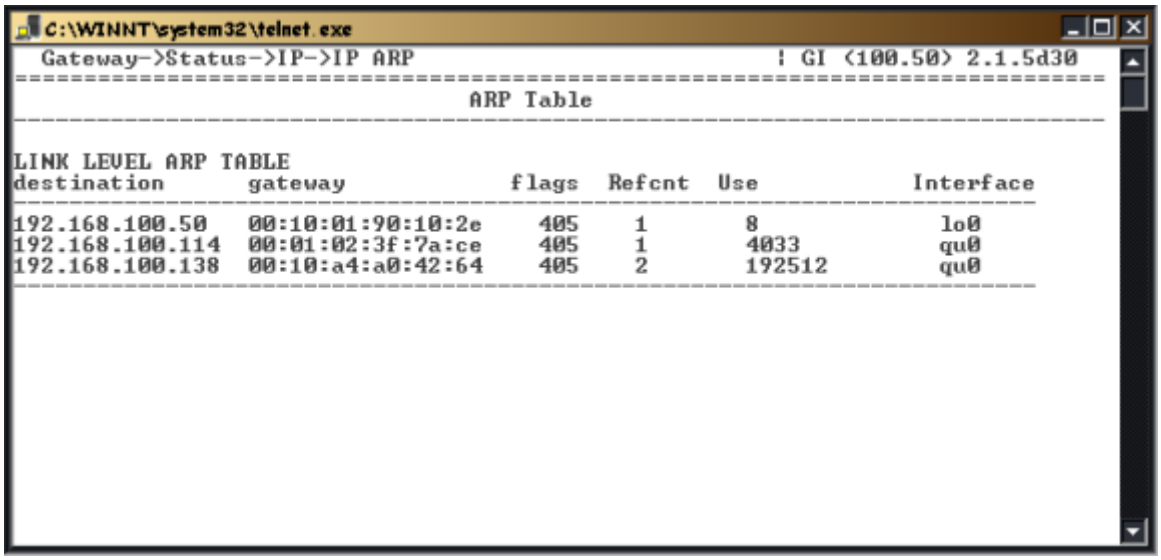


Figure 90: IP ARP

IP Routes

The path (IP) to the PBXgateway should be shown in this table.

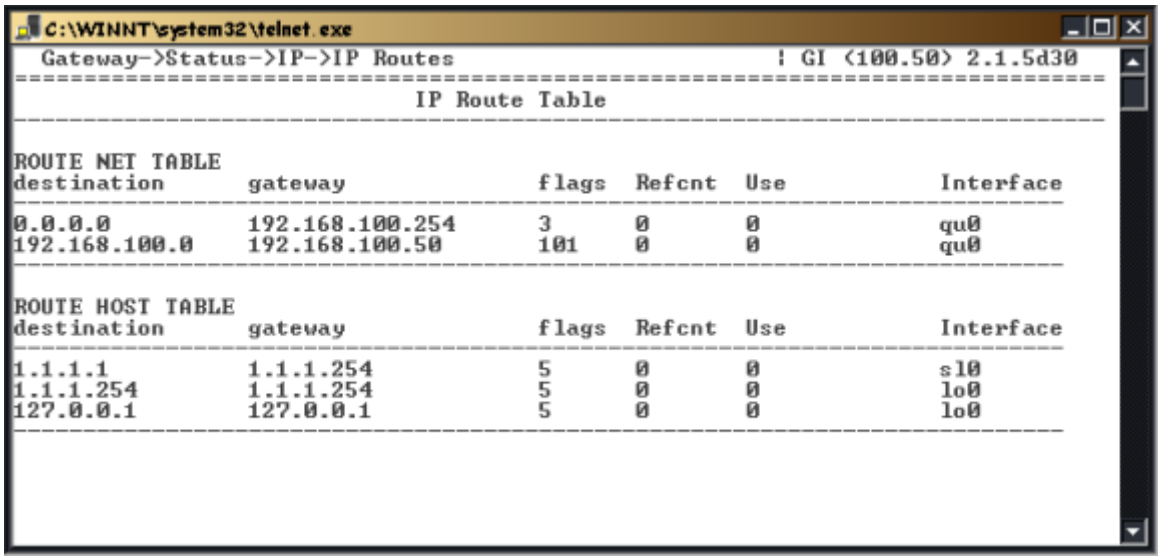


Figure 91: IP Routes

General System Info

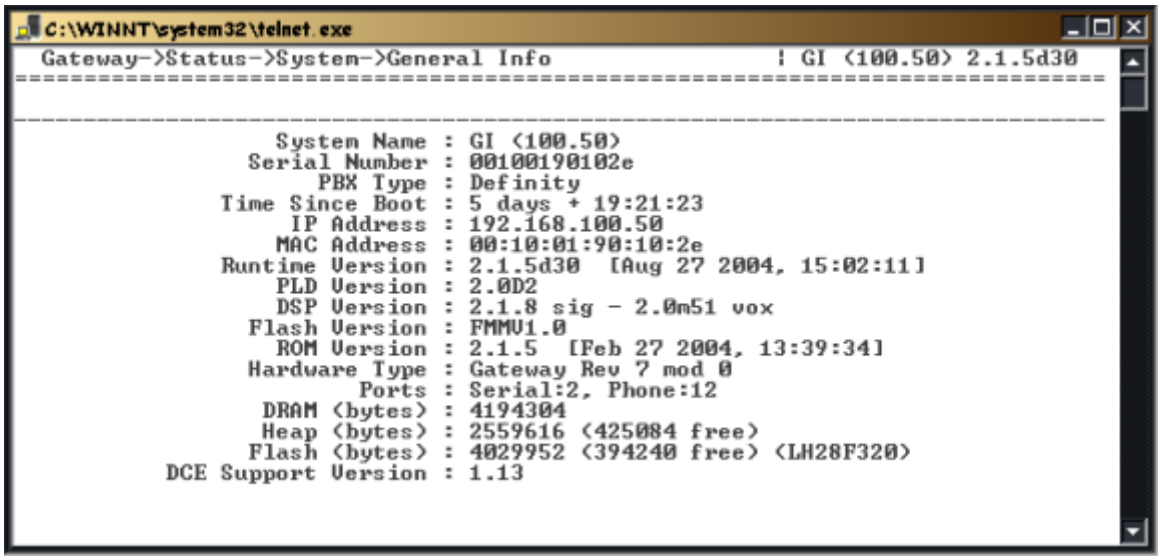


Figure 92: System Info

Remote Phone Messages

The following messages appear on the remote telephone display connected to the Branch Office or EXTender 4000 remote units when a connection attempt fails. The telephone shows 'Connect Error,' followed by a message. Table 19 and 20 contains the possible Connect Error messages.

Message	Description	Action
Already connected	Remote port is already connected.	Reset port at PBXgateway.
Assigned port Busy (see note)	The switch port is being used by another user.	Wait until port is available or reset port on Gateway and try to re-connect.
Assigned port Down (see note)	The switch port is not available, due to problems (green flicker) with the port.	Check port connection at PBXgateway.
Carrier Lost (see note)	Displayed if the network connection to the PBX is lost.	Check network links. Attempt to reconnect after network is up and running.
Connect rejected	The PBX/KSU rejects the connection request.	Possible connect password is incorrect. Check network links. Attempt to reconnect.
Connect Timeout	Remote cannot connect to PBXgateway.	Check WAN connection on PBXgateway unit.
Network disabled	The network device is not connected, being used, or is not active.	Check network link and device.
Network down	The network device has a problem.	Check network link and device.
Network in use	The network device is being used by another device.	Reset WAN and try to re-connect.
Network not ready	The network device is not ready for use. (yellow LED)	Make sure primary connect matches "enabled" WAN port.
No bandwidth	The unit bandwidth is oversubscribed. No network bandwidth is available from phone signaling.	Check synch rate or change voice compression.

Table 19: Connect Error Messages

***Note**: These messages are not preceded by "Connect Error".*

Chapter 6: File Management and System Upgrades

This chapter contains information and instruction on upgrading your EXTender and PBXgateway.

Introduction

The PBXgateway and Remote units contain a flash file system to retain basic configuration files, the actual firmware, and the instructions necessary for starting the units. The flash memory system does not require continuous power to retain its memory.

Flash memory file system has the following properties:

- Contains the operating software known as firmware. This firmware is upgradable.
- Non-volatile storage, so it retains all saved information even when the power to your EXTender is turned off.
- Stored EXTender configuration files, containing specific set up parameters. These files are unit specific and include an appropriate unit extension (.swt for Switch or Gateway files and .rem for Remote files)
- Stores any other files that have been copied to the unit.

Access to the Flash File Syste

The EXTender Flash File system can be written to for copying files or updating firmware. Access to flash file system is done through various connections using a PC. Example: Direct serial connection, FTP etc.

***Note**: FTP must be enabled (see page 78). Access to the Flash file system can be secured by setting up an administrator's password (See page 86), used by the system administrator.*

Firmware

All firmware images stored in the Flash file system are saved with the following extensions:

- EXTender 6000 & PBXgateway: .m6b
- EXTender 4000: .mlb

***Note**: All .m6b and .mpb files are binary files.*

Config Files

EXTender configuration parameters are contained within the Flash file system under a .rem (Remote) or .swt (Switch) file extension. All changes made to items pertaining to the configuration of the units MUST be saved to Flash file system before they become active.

Boot.cfg

***IMPORTANT:** The Management Interface (MI) will prompt you when changes must be saved.*

Call Back Files

This is unit specific information required to startup or "boot" both the Switch and Remote units.

Boot information includes:

- IP Address information
- the active config file to be loaded
- the firmware (.m6B or .mpb) file to boot with.

The PBXgateway unit saves .cbk files to enable it to contact remote users that are currently disconnected.

***Note**: This file is used specifically for Remote Login capabilities. See page 105 for more information.*

Configuration File Management

Changing the Active Config file

Introduction

When the PBXgateway is powered-up, the Flash file system loads a configuration file (called the “active” .rem (Remote) or .swt (Switch) file) which contains all the parameters necessary for operation. The system administrator can change this “active” .rem (Remote) or .swt (Switch) file so that a different set of parameters loads.

***Note**: The default configuration file shipped with the units is runtime.rem or runtime.swt.*

Procedure

Access the Config Menu using the following path:

Path: `Utilities->Upgrade->Config File`

Select an existing .rem (Remote) or .swt (Switch) file from the list displayed.

The display reads;

Change Configuration file to……

Enter (**Y**) or (**N**).

The unit will then prompt you to reboot. This change requires a reboot in order to take affect.

All changes made to the Switch or Remote parameters will be saved under the new config file.

Edit Non-Active Configuration Files

Introduction

The PBXgateway can be used in different applications requiring different parameters. The system administrator may need to set up separate configuration files to accommodate custom parameters for each application.

The ability to modify any non-active configuration file, allows the system administrator a method for quickly setting up new units based on existing configuration parameters.

IMPORTANT: *To edit the "active" config file, use the Configuration Menu (see Chapter 4).*

Procedure

Access the Edit Configuration Menu using the following path:

Path: `Utilities->File->Edit Config`

Choose Switch or Remote and select a config file from the available files, press **Enter.**

Modify the necessary parameters as required.
(Refer to Chapter 3, for more information)

As required, select **Save** and press **Enter** to save changes. The following message appears:

Save changes to Filename _____.rem (Remote) or .swt (Switch)?

(Y)es (N)o (S)pecify different filename

Press (**Y**) to save changes
Press (**N**) to not save changes
or Press (**S**) to specify a different file name.

Creating a New Config File

Introduction

The PBXgateway can be used in different applications requiring different parameters. The system administrator may need to set up separate configuration files to accommodate custom parameters for each application.

Example: The creation of a new Remote config file on the PBXgateway, and copying that new file to the Remote unit.

The ability to modify any configuration file not in use, allows the system administrator a method for quickly setting up new units based on existing configuration parameters.

Procedure

Access the Edit Configuration Menu using the following path:

Path: `Utilities->File->Edit Configuration`

Message reads: Create a new:

Select (**R)** for Remote file. Press **Enter**
or
Select **(S)** for Switch file. Press **Enter**

Select <new file>. Press Enter.

Enter New file name:_____, (without extension)
press **Enter.**

Note*: File name must not exceed twelve characters and does not require a file extension. The MI will automatically assign an extension depending on the unit*.

Modify the necessary parameters as required.
(Refer to Chapter 3, page 55 for more information)

Select **Save Action** and press **Enter** to save changes. The following message appears:

Save changes to Filename _____.rem (Remote) or .swt (Switch)?

(Y)es (N)o (S)pecify different file name

Press (**Y**) to save changes.
Press (**N**) to not save changes.
or Press (**S**) to specify a different file name.

Upgrading the Software

Visit the Service & Support section of www.mck.com to download the latest software files. The software file can be placed to the PBXgateway/EXTender 6000 for upgrading via FTP, Zmodem methods.

The upgrade process involves three phases. These should be executed in the following order:
1. File Management.
2. File Upload
3. File Upgrade

Note:
*The PBXgateway/EXTender 6000 use image files with ***.mcb** extension, while the EXTender 4000 uses image file with ***.mlb** extension. The file management, upload and upgrade instructions are the same for all versions.*

File Management

This phase includes the tasks of examining the flash file system, saving an active image file as the default, deleting outdated files and optimizing the flash file system.

Examining the flash file system

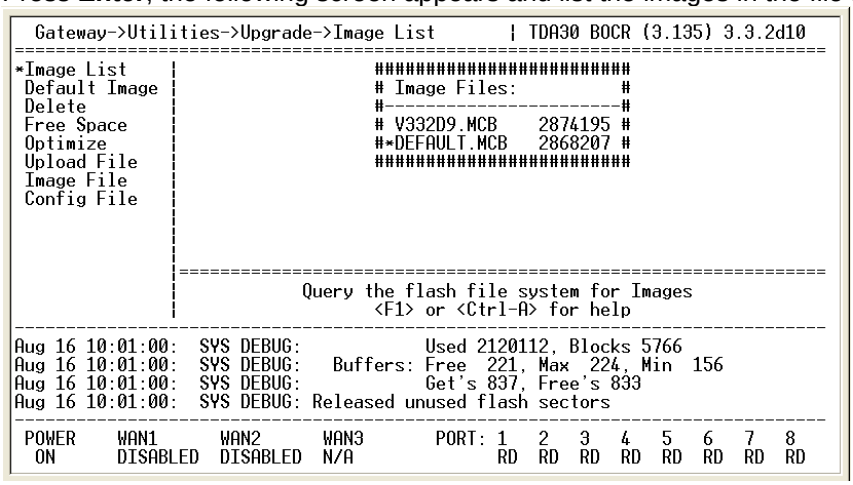
This procedure determines how many image files are on the flash file system.

Procedure

1. Connect to the MI via a HyperTerminal or a Telnet session.

2. Access the **Image List** menu using the following path:
   Path: `Gateway->Utilities->Upgrade->Image List`

3. Press **Enter**, the following screen appears and list the images in the file system:



4. If there is only the “Default.mcb” in the list goes to the section “Optimize the Flash File System”; otherwise follow the steps to save the active image file as the default.

Save Active File as the Default

This will delete the existing “default.mcb” file from the unit and take the image that is currently “live” and rename it to “default.mcb”. We are going to leave a copy of the currently “live” image on the unit after the upgrade is complete. If the currently live image is “default.mcb”, you will receive this message, “Currently running default image”.

Caution:
This process requires system to be rebooted and causing active phones to be out of service for a few minutes.

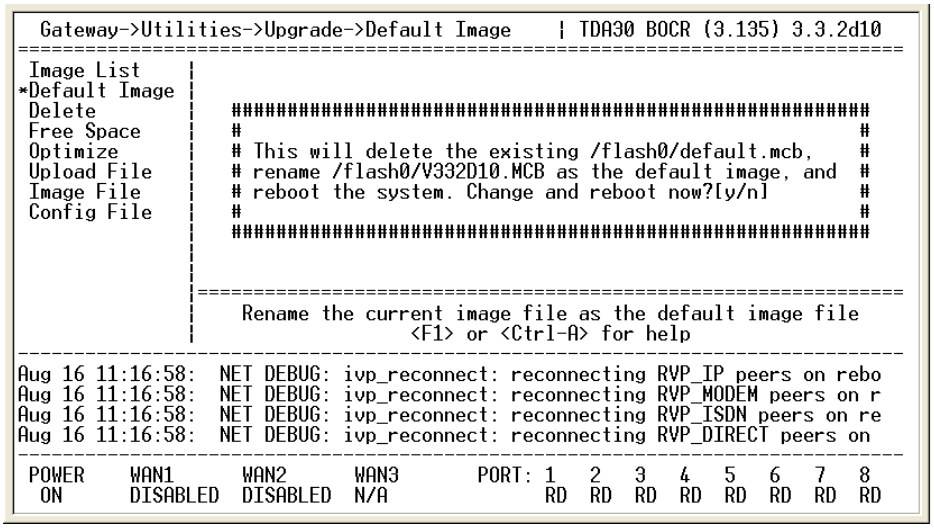
The procedure outlined below includes all the steps to save an active image file as the default.

Procedure

1. Connect to the MI via a HyperTerminal or a Telnet session.

2. Access the **Default Image** menu using the following path:
   Path: Gateway->Utilities->Upgrade->Default Image

3. Press **Enter** and the following screen appears:



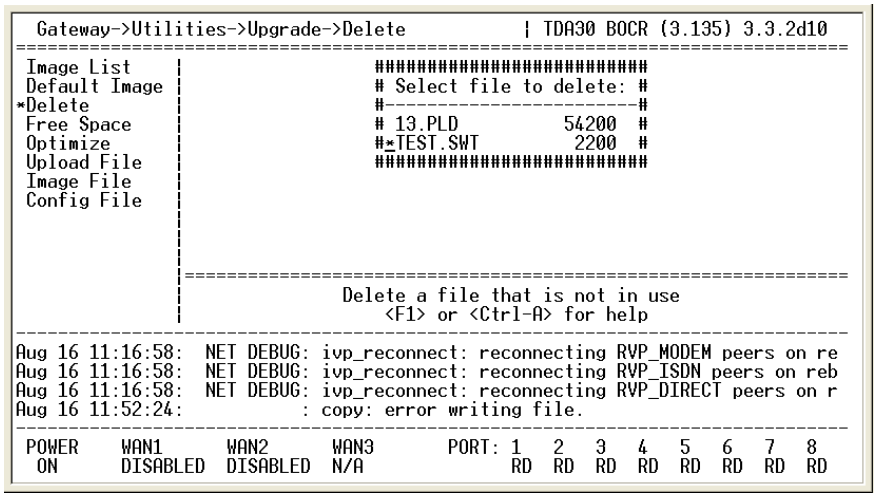
4. Type **y** (Yes) to save the image file being used as **default.mcb**, and reboot the system.

Delete Outdated Files

The procedure outlined below includes all the steps to delete files out-of-date.
Procedure:

1. Access the **File Delete** menu using the following path:
   Path: Gateway->Utilities->Upgrade->Delete

2. All files not in use are listed.



3. Place the asterisk next to the file(s) to be deleted and press **Enter**.

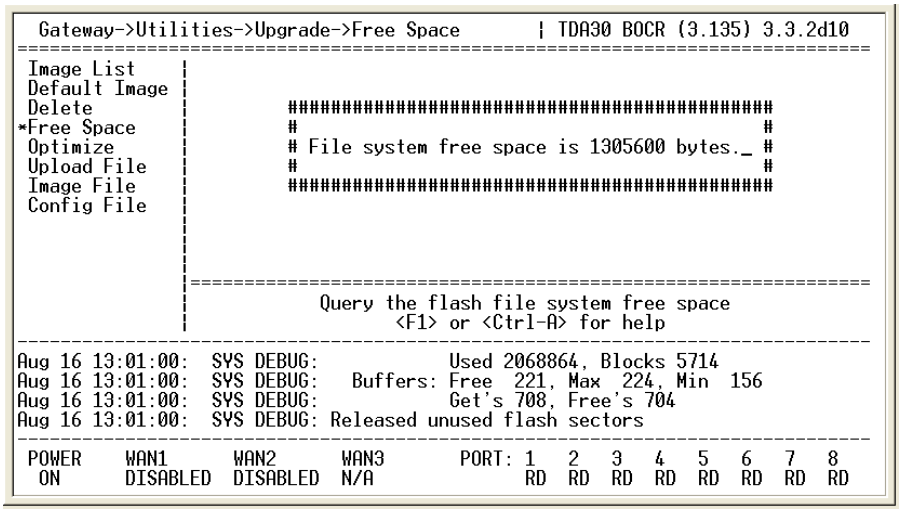
4. Press **y** (Yes) to permanently delete a file. Repeat this step until there are no more files to delete. It is necessary to delete all other mcb files from the unit to make room for the new file.
   Note: The file saved as **default.mcb** and the active image file will not be included in the list of files that can be deleted.

Query Flash Memory Space

Before loading image file into the Flash File System, ensure that there is enough free memory space in the Flash File System for the image file. If the free space is less than 3000000 bytes, please consider delete files which is not in used by the system (See Delete Outdated Files).

Procedure:

1. Access the **Free Space** menu using the following path:
   Path: `Gateway->Utilities->Upgrade->Free Space`

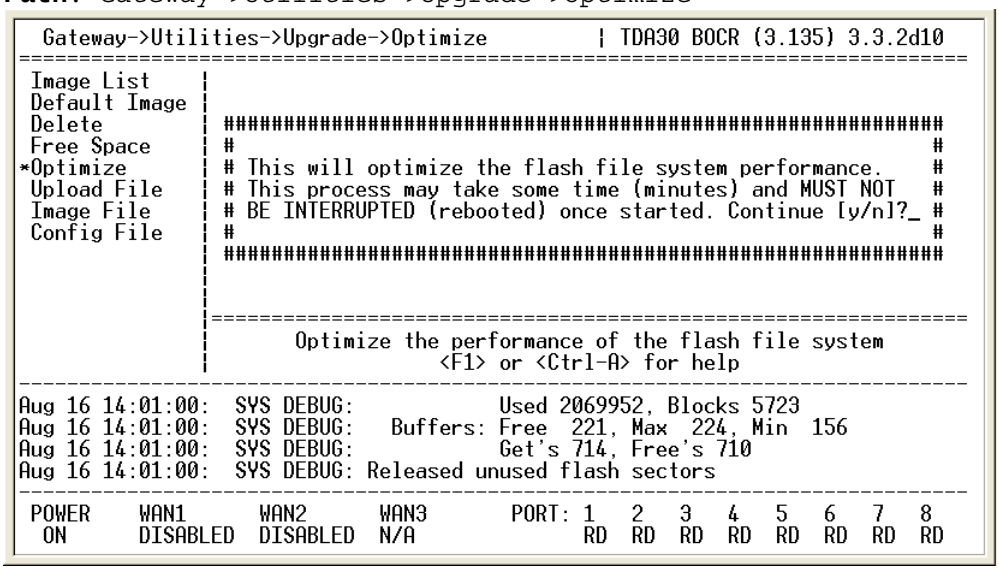


Optimize the Flash File System

The procedure outlined below includes all the steps to optimize the flash file system. This will speed up the subsequent file upload.
***Warning**: Do not optimize the flash file when the PBXgateway/Extender 6000 is active. If the flash file is optimized while the unit is being used, the voice prompts for the Interactive Voice Response (IVR) system will be non-operational.*

Procedure

1. Access the **Optimize** menu using the following path:
   Path: Gateway->Utilities->Upgrade->Optimize



2. Press Y to optimize the flash file system performance.

File Upload

This section covers methods for uploading images files: FTP, Zmodem Console and In-band Upload.

Via FTP Upload

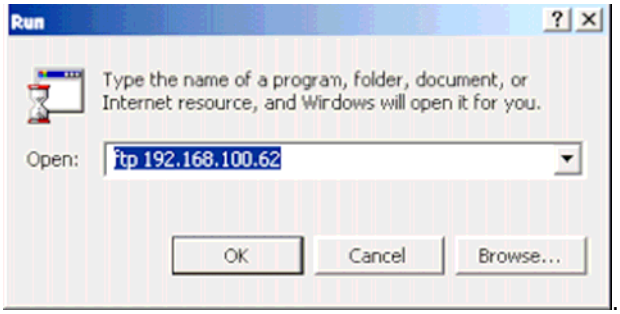
The procedure outlined below includes all the steps to upload image files into the PBXgateway/Extender 6000 using the FTP Upload method.

Note:

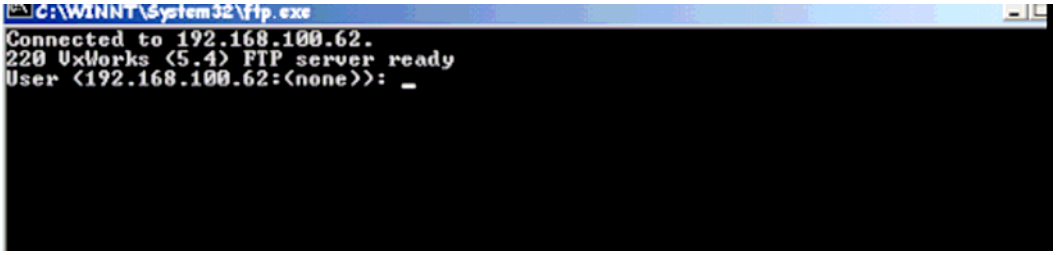
- **Each MCK unit should have Telnet and FTP enabled and an accessible (pingable) IP address assigned before proceeding. Please refer to your System Administrator's Guide for more information.**
- **Note: Files to be uploaded to the PBXgateway/Extender 6000 via FTP must have extensions *.mcb.**

Procedure

1. Begin an FTP session to the PBXgateway/Extender 6000 by selecting **Start/Run** from the Windows taskbar. The screen below appears. Press **OK**



2. Press Enter at the **User** prompt.



3. At the **Password** prompt, press Enter if no password has been assigned to the unit. If a password has been assigned to the unit, enter the password and then press Enter.

4. At the **ftp>** prompt, type in **binary** and press Enter.

5. At the **ftp>** prompt, type in **hash** and press Enter.

   You are now ready to begin uploading the file to the MCK unit. Please be sure you know the location of the mcb file on your local PC before continuing.

6. At the 'ftp>' prompt, type **put c:\ ___ \ v?????.mcb** and press Enter. The '___' represents the full path to the file on your local PC. The "**v?????.mcb**" represents the proper filename of the image file (i.e. v332r2.mcb).The file transfer begins. Transference status is indicated by a stream of # signs running across the screen. The transfer should be completed in approximately 15 minutes or less.

7. At the **ftp>** prompt, type **quit** and press Enter once the upload is completed. The new image file has been uploaded. Continue with section 'In-band Upload' if you need to use the in-band connection to get the file to the other unit via its in-band connection (i.e. over the T1 or IP network). Once completed, the image file is ready for upgrade, go to the section 'File Upgrade'.

Via FTP Client

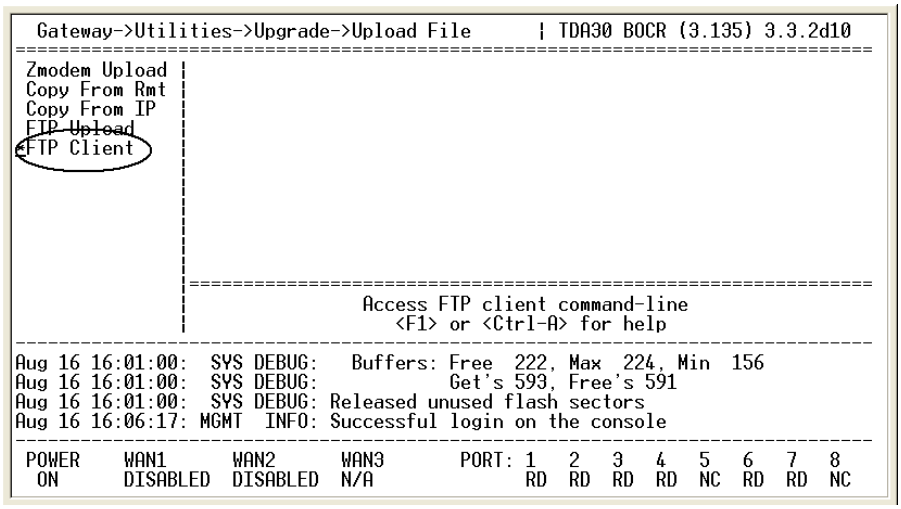
The PBXgateway/EXTender 6000 can be act as a FTP client to download the image file from a FTP Server via a LAN connection or Ethernet crossover cable.

Note: Each MCK unit should have Telnet and FTP enabled and an accessible (pingable) IP address assigned before proceeding. Please refer to your System Administrator's Guide for more information.

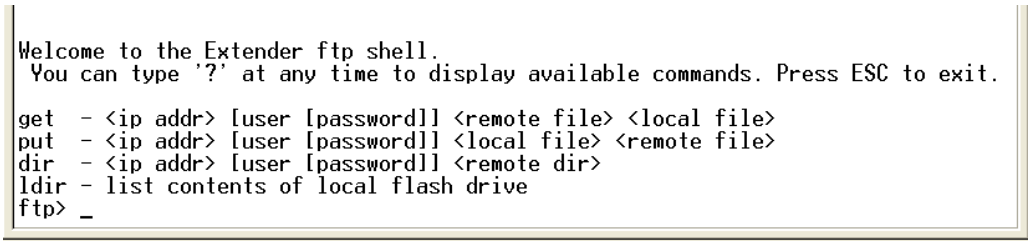
The procedure outlined below includes all the steps to download image files into the PBXgateway/Extender 6000 using FTP Client method.

Procedure

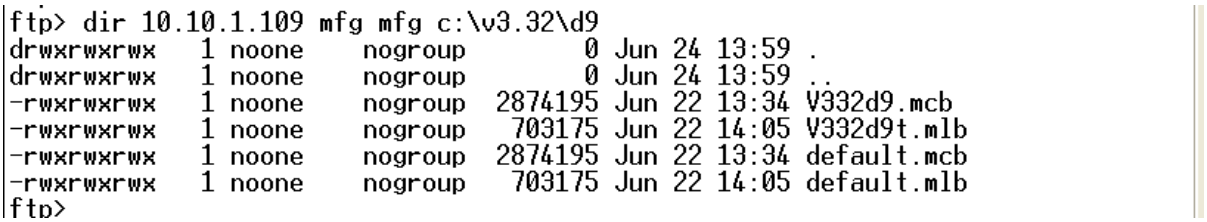
1. Access the **FTP Client** menu using the following path:
   Path: Gateway->Utilities->Upgrade->Upload File->FTP Client



2. Press **Enter** and the Extender FTP Shell will appear:



3. At the **ftp>** prompt, type **dir xxx.xxx.xxx yyy zzz c:___** and press enter to check if the *.mcb image file to be download is available in the directory of the FTP Server. (Where **xxx.xxx.xxx** represents the IP Address of the FTP Server, **yyy zzz** represents the login User /Password for the FTP Server and **c:____** represents the full path which contents the image file.)



4. At the **ftp>** prompt, type **get xxx.xxx.xxx yyy zzz c:___\v???.mcb v???.mcb** and press enter to download the image file to the unit. (Where **xxx.xxx.xxx** represents the IP Address of the FTP Server, **yyy zzz** represents the login User /Password for the FTP Server. **c:____\v???.mcb** represents the full path and the file name of the image file on the FTP Server. And the last **v???.mcb** parameter represents the local file name to be saved on the Flash File System.)

The file transfer begins. Transfer status is indicated by a stream of **...** signs running across the screen. The transfer should be completed in approximately 15 minutes or less.

```
ftp> get 10.10.1.109 mfg mfg c:\v3.32\d9\v332d9.mcb v332d9.mcb

Retrieving remote file: c:\v3.32\d9\v332d9.mcb
         as local file: v332d9.mcb
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
................................................................................
.
2874195 bytes copied.
ftp> _
```

5. Once the upload is completed, at the ftp> prompt, press the ESC to exit the Extender FTP Shell. Continue with section 'In-band Upload' if you need to use the in-band connection to get the file to the other unit via its in-band connection (i.e. over the T1 or IP network). Once completed, the image file is ready for upgrade, go to the section 'File Upgrade'.

Via Zmodem Console upload

The procedure outlined below includes all the steps to upload image files into the PBXgateway/EXTender 6000 using the Zmodem protocol. Files to be uploaded using the Zmodem protocol must have extensions *.mcb.

Establish a direct serial connection to the Gateway via the console port located in the front of the unit.

Procedure

1. Access the **Zmodem Upload** menu using the following path:
   Path: `Gateway->Utilities->Upgrade->Upload File->Zmodem Upload`

```
...ilities->Upgrade->Upload File->Zmodem Upload | TDA30 BOCR (3.135) 3.3.2d10
================================================================================
*Zmodem Upload |
 Copy From Rmt |
 Copy From IP  | ##################################################################
 FTP Upload    | #                                                                #
 FTP Client    | # Upload new software (.mcb file) via the console port.          #
               | # Before starting this process, it is recommended that           #
               | # the flash file system be optimized. Optimize now [y/n]?_       #
               | #                                                                #
               | ##################################################################
               |
               |
               |================================================================
               |             Receive file through ZMODEM protocol
               |                  <F1> or <Ctrl-A> for help
--------------------------------------------------------------------------------
Aug 16 15:31:32: MGMT DEBUG: wgetch :: getchar returned EOF, (EOF or Read Erro
Aug 16 15:31:34: MGMT  WARN: Console connection lost
Aug 16 15:31:44: MGMT  INFO: No modem detected on console port
Aug 16 15:31:52: MGMT  INFO: Successful login on the console
--------------------------------------------------------------------------------
 POWER    WAN1      WAN2      WAN3       PORT: 1   2   3   4   5   6   7   8
  ON      DISABLED  DISABLED  N/A              UP  RD  RD  RD  NC  RD  RD  RD
```

2. Select **n** (No) when asked to optimize. The flash file system was optimized in the file management process.

3. The next screen will contain a warning about interrupting the upload. Press **y** (Yes) to continue.

4. When you see this message: "Starting Zmodem Session - Hit Ctrl-X 5 Times to Cancel", go to the HyperTerminal menu bar and select Transfer / Send File. Browse to the location to the file on your PC. Highlight the file (mcb extension), and select Open. Be sure the protocol is set as Zmodem. Press Send to begin the transfer.

5. Once the transfer has begun, Hyperterminal will display a status window indicating the progress of the upload and inform you when it has been uploaded successfully. Continue with section 'In-band Upload' if you need to use the in-band connection to get the file to the other unit via its in-band connection (i.e. over the T1 or IP network). Once completed, the image file is ready for upgrade, go to the section 'File Upgrade'.

In-Band Upload

Getting the new image file across the in-band connection to the other unit –
Note: You will only be able to transfer the file across the in-band connection when 1.) The current WAN1 and/or WAN2 state is ACTIVE, or 2.) There is at least one phone active via an IP connection between units.

Very Important: ONLY *.mcb files should be transferred between a PBXgateway and an EXTender 6000. Other MCK products use other file types, so make sure you know which product is at the other end of the connection. Please refer to www.mck.com to download the proper files for each product and instructions on how each is upgraded.

A. Copy To Gateway/Remote

In this case, the new image file has been uploaded to the local (PBXgateway/EXTender 6000) unit, and the file will be sent to far-end (PBXgateway/EXTender 6000) unit.
Procedure

1. On the Main Menu of the Management Interface, choose **Gateway Login** or **Remote Login** (depends on which unit you're logged into). Press *Enter*.

2. Once logged in to the other unit, please perform steps in "File Management' section to cleanup the Flash File System. We need to do the same file management techniques with the other unit. Once the file management of the other unit is complete, log out of that unit and return to the original unit.

3. Navigate to **Utilities** >**File** >**Copy to Remote** or **Utilities** > **File Copy to Gateway** (again, this will depend on which unit you are logged into). Press *Enter*.
   A dialog box displaying how each port is connecting back and forth between units will appear. Put the asterisk on the port that you want to transfer the file to (it's actually the port of the local unit so you should know which ports go to which units) and press *Enter*. You will be prompted for a password. This is the password of the "far-end" unit. If there is a password, enter it now; otherwise just press *Enter* to continue. A dialog box listing the files that can be transferred will appear. Choose the file that you just uploaded from the list and press *Enter*. When asked to enter the destination filename, put in the proper name of the file, but leave off the mcb extension. Once you press *Enter*, the transfer will begin. Time of an in-band transfer will vary depending on the type of connection. You will receive a "Copy Succeeded" message when the transfer is complete. Now we just need to get the units upgraded.

B. Copy From Gateway/Remote

In this case, the new image file has been uploaded to the far-end (PBXgateway/EXTender 6000) unit, and the file will be copy to the local (PBXgateway/EXTender 6000) unit.

Procedure

1. Connect to the MI via a HyperTerminal or a Telnet session.

2. Once logged in, please perform steps in “File Management’ section to cleanup the Flash File System. We need to do the same file management techniques with the other unit.

3. Navigate to **Utilities** >**File** >**Copy From Gtwy/Rmt** or **Utilities>Upgrade>Upload File>Copy From Gtwy/Rmt** (again, this will depend on which unit you are logged into). Press *Enter*.
   A dialog box displaying how each port is connecting back and forth between units will appear. Put the asterisk on the port that you want to transfer the file to (it’s actually the port of the local unit so you should know which ports go to which units) and press *Enter*. You will be prompted for a password. This is the password of the “far-end” unit. If there is a password, enter it now; otherwise just press *Enter* to continue. A dialog box listing the files that can be transferred will appear. Choose the file that you just uploaded from the list and press *Enter*. When asked to enter the destination filename, put in the proper name of the file, but leave off the mcb extension. Once you press *Enter*, the transfer will begin. Time of an in-band transfer will vary depending on the type of connection. You will receive a “Copy Succeeded” message when the transfer is complete. Once completed, the image file is ready for upgrade, go to the section ‘File Upgrade’.

File Upgrade

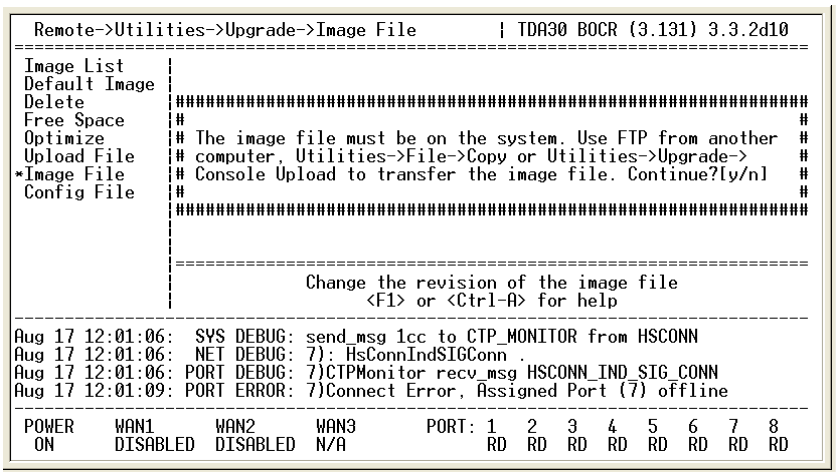
The procedure outlined below includes all the steps to upgrade an image file.

Caution:
This process requires system to be rebooted and will cause active phones to be out of service for a few minutes.

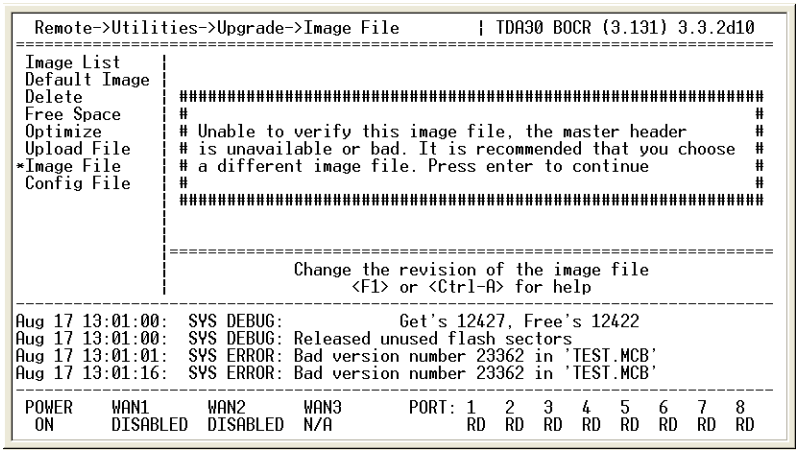
Procedure

1. Go to the **Image File** menu using the following path:
   Path: `Gateway->Utilities->Upgrade->Image File`

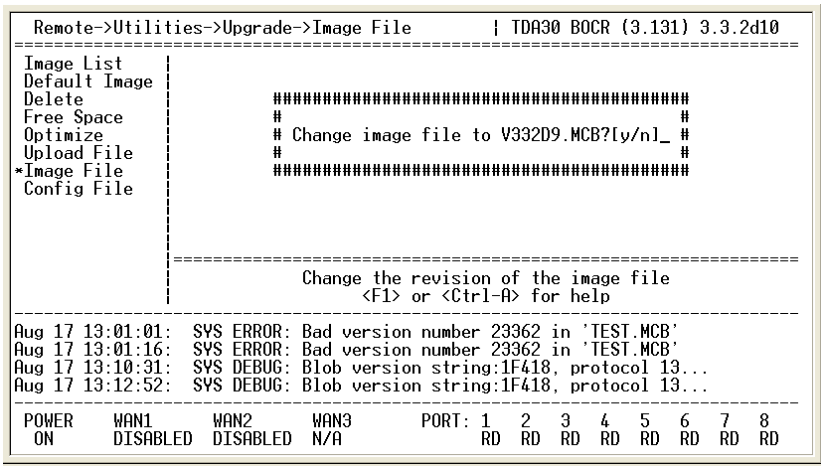
2. Press Enter. A note about the need for the file to be on the unit will appear. Press **y** (Yes) to continue.



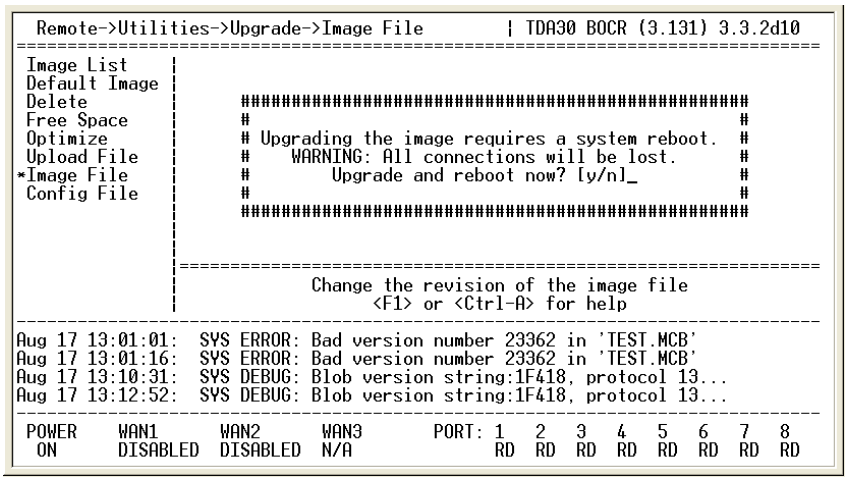
3. Select the new image file (file uploaded) and press **Enter**. This will include a process to verify the integrity of the uploaded file. If the image file fails the verification, error will be display on screen. If this occurs please re-start the Upgrade Process.



4. Once the file verification has been passed, press **y** (Yes) when prompted to change the image file.



5. A warning screen will appear. Press y (Yes) to continue upgrade with the selected image file and reboot the system. Otherwise, select n (No) to abort the upgrade.



***Caution**: Users will be dropped during the reboot. Service will be reinstated in approximately 3 minutes.*

Using an External WAN Connection

Introduction The PBXgateway is capable of transferring files using the external WAN connection between the Gateway and Remote units. This procedure is used to "put" a new file (.m6b or .rem (Remote) or .swt (Switch)) onto the Flash file system of the opposite unit.

Procedure

1. Access the Copy to Remote/Switch Menu using the following path:

   Path: `Utilities->File->Copy to (Remote/Switch)`

2. Enter the **Admin password,** if required for the unit you are accessing.

3. Select a file to copy from the list displayed.

4. When prompted, Enter a **Destination Filename**.

   ***Note**: File name must not exceed twelve characters and should not include a file extension. The Management Interface (MI) will automatically assign an extension depending on the type of file (Switch or Remote).*

5. Press **Enter**. The upload process will begin.

   Note: The transfer process may take some time especially if you have active phones.

6. When the download is complete, the MI displays the message:
   `Copy Succeeded`

Using a Direct Console Connection

The PBXgateway is capable of transferring text files using a direct console connection between an EXTender unit and a PC.

EXTender 6000 and PBXgateway: .m6t

EXTender 4000: .mlt

This procedure is helpful when a LAN connection is not available.

Note: This procedure is only used for uploading an encoded text file to the unit. An encoded text file is a firmware file encoded as text.

Procedure

1. Connect a PC to the PBXgateway through the console port. (see Chapter 3, page 44, for more information)

2. Open an Enhanced Terminal Interface (ETI) program. Example: Hyperterminal

3. Access the Console Upload Menu using the following path:

   Path: `Utilities->Upgrade->Console Upload`

   ***Note**: You will be prompted to "Optimize the Flash File System", select (Y) or yes to optimize.*

4. The following screen will appear. Press **"y"** to continue**.**

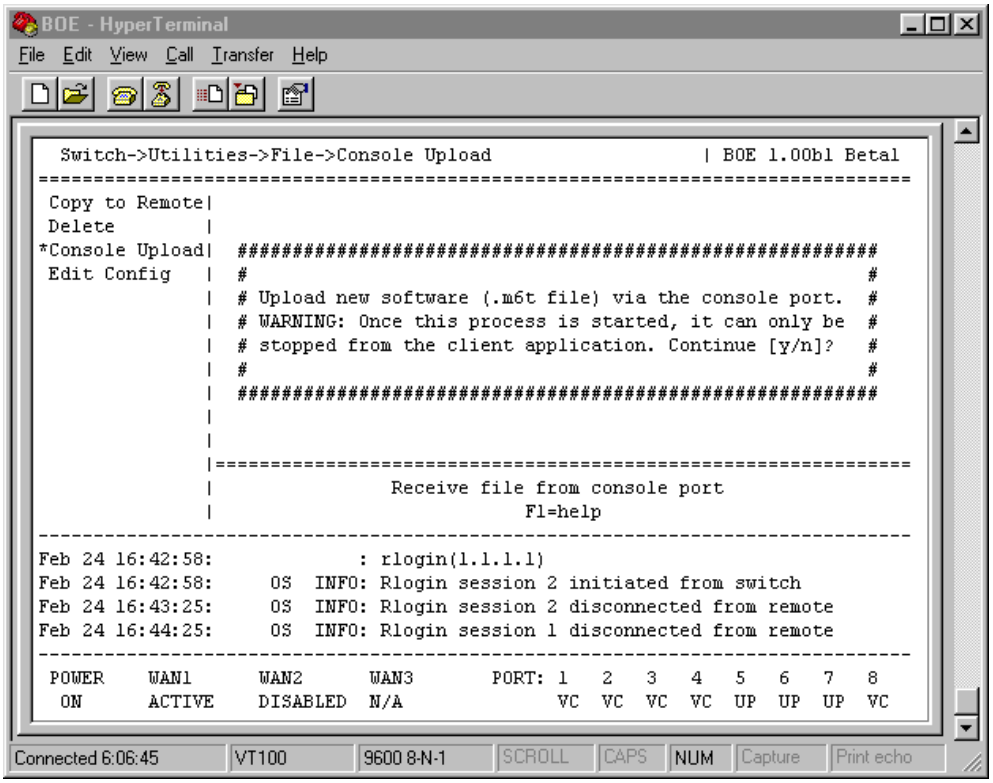


Figure 93: Console Upload Screen

5. Select **Transfer-Send Text File** command from the ETI program. Locate the text file to be sent and press **Open**.

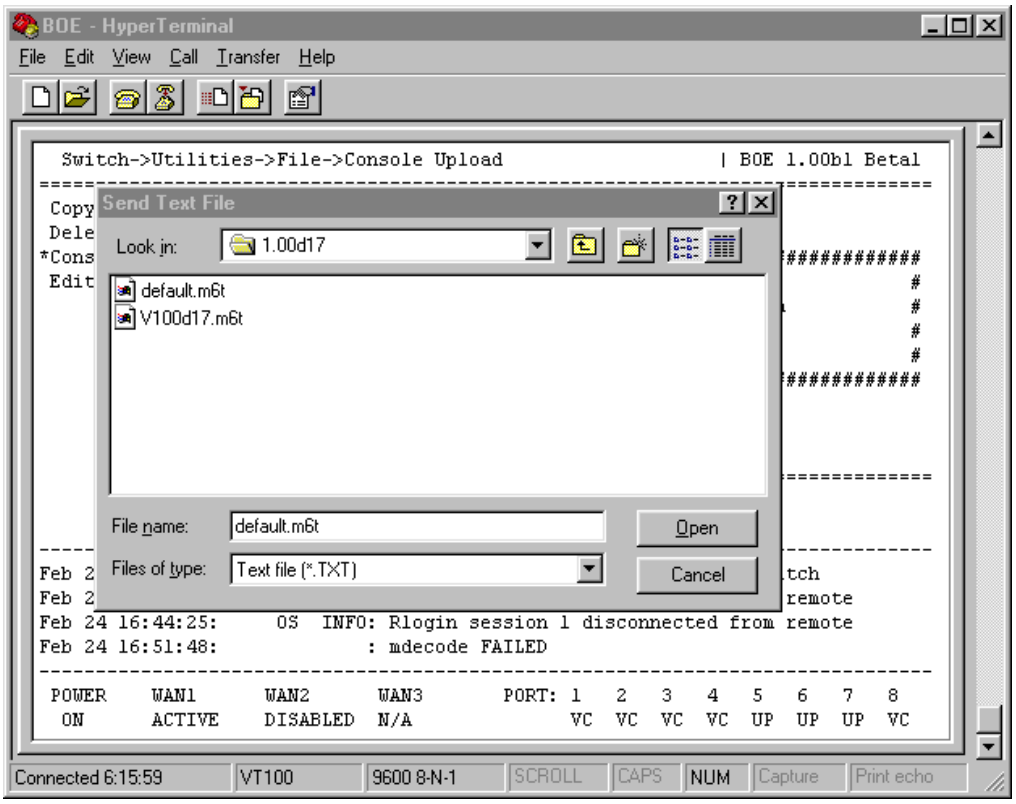


Figure 94: Send text file screen

The file upload will begin.

Note: Files labeled ".m6t or .mlt" are text versions of the firmware, where as ".m6b or .mpb" files are binary files.

The screen will display the Flash activity by a series of dots (…….).

***Note**: Do not quit the application or stop the file upload until the process is complete. Once the file is copied to the unit, it is automatically saved as binary and renamed with a M6B extension or MLB for the 4000.*

Chapter 7: Glossary

This Chapter provides a list of terms that are used in the operation and set up of the PBXgateway and Remote as well as other MCK communications products.

10/100Base-T

A networking standard that supports data transfer rates up to 100 Mbps (100 megabits per second). 100Base-T is based on the older Ethernet standard of 10Base-T. Because it is 10 times faster then Ethernet it is referred to as “Fast Ethernet”. Officially, the 100Base-T standard is IEEE 802.3u.

120 vac

120 volt alternating current (North American standard electrical supply).

A

ACD

Automated Call Distributor. A telephone facility that handles incoming calls and distributes them among several employees, usually in a particular department. For example, a Help Desk would use ACD to distribute calls to the employees who are currently not on a call.

ADPCM

Adaptive Differential Pulse Code Modulation. A reduced bit rate variant of PCM (Pulse Code Modulation) audio encoding.

ADSI

Analog Display Service Interface. This is a Bellcore standard that defines the protocol on the flow of information – between a switch, server, voicemail system or a service bureau – and a telephone, PC, data device or another communicating device that has a screen. In simpler terms, it is a system that allows a consumer’s telephone to receive, display and interact with a wide array of services.

Algorithm

A formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point. A compression algorithm uses a formula to compress and decompress voice when transmitted across a network.

ARP

Address Resolution Protocol. A network layer protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.

AT Commands

In modems, a set of commands that control the modem or alter its characteristics. Originally developed by Hayes, the AT command set is now an industry standard.

Auto-Attendant

Is used to relay company information or allow callers to direct themselves to a specific user’s extension without the need for human interaction.

B

Bandwidth

The width of a communications channel. Measured in bits per second (bps).

Baud Rate
The speed in Kbps at which digital data can be transmitted.

Branch Office
The remote location of the corporate office.

C

CSU
Channel Service Unit. A device to terminate a digital channel on a customer's premise.

ConneX
MCK's proprietary feature allowing single remote users to access the corporate PBX/KSU features from an analog or cell phone when away from the corporate office.

D

DB-25
The standard 25-pin connector used for RS-232 serial data communications.

DB-9
The standard 9-pin RS-232 serial port on most computers

DCE/DTE
Short for Data Terminal Equipment, a device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232C standard. This standard defines the two ends of the communications channel as being a DTE and Data Communications Equipment (DCE) device. In practical terms, the DCE is usually a modem and the DTE is the computer itself, or more precisely, the computer's UART chip. For internal modems, the DCE and DTE are part of the same device.

Dedicated Subscriber Lines
Communication lines (usually twisted pair) that are used to connect on-premise telephone equipment (such as a PBX/KSU) to the Central Office. Also referred to as direct lines.

Default Gateway
Normally the IP address of a router. Used to specify where IP packets are to be sent that are not destined for the same network number.

Dial Line
A telephone line which is part of the Public Switched Telephone Network and is accessed through an automatic dial-up function.

DNS
Domain Naming System. A mechanism used in the internet for translating names of host computers into addresses.

Example: DNS would change a computer name such as MCK.com to the actual numeric IP address of xxx.xxx.xxx.xxx.

Domain Name
The fully qualified name of a domain of a network. Example “MCK.com”.

DRAM
Dynamic Random Access Memory. A readable/writable memory chip used to store data.

DS0
Digital Service, Level 0. It is 64,000 bps, the worldwide standard speed for digitizing one voice conversation using PCM.

DSP
Digital Signal Processor. A specialized computer chip designed to perform speedy and complex operations on digitized signals.

DTMF
Short for Dual Tone Multi-Frequency, the system used by touch-tone telephones. DTMF assigns a specific frequency (consisting of two separate tones) to each key so that it can easily be identified by a microprocessor.

E

Ethernet
A local area network used for connecting computers, printers, workstations, terminals, servers, etc. Ethernet operates over twisted wire and over coaxial cable at speeds up to 100Mbps.

F

Facility
Transmission facilities. Usually a two metallic pair set of cords, but can be telephone company carriers, T-1, microwave or dial-up telecommunications lines.

Firewall
A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Full Duplex
Refers to the transmission of data in two directions simultaneously. For example, a telephone is a full-duplex device because both parties can talk at once. In contrast, a walkie-talkie is a half-duplex device because only one party can transmit at a time.

FTP
File Transfer Protocol. A connection protocol used to send and receive files.

G

G.729A
The ITU (International Telecommunications Union) standard voice algorithm for the coding of speech signals in telecommunication networks.

H

Half Duplex
Refers to the transmission of data in just one direction at a time. For example, a walkie-talkie is a half-duplex device because only one party can talk at a time. In contrast, a telephone is a full-duplex device because both parties can talk simultaneously. Duplex modes often are used in reference to network data transmissions.

HDLC
High-level Data Link Control, a transmission protocol used at the data link layer (layer 2) of the OSI seven-layer model for data communications. The HDLC protocol embeds information is a data frame that allows devices to control data flow and correct errors.

Host Name
The name of a computer or HOST as specified on a DNS server.

HTML
Short for HyperText Markup Language, the authoring language used to create documents or applications on the World Wide Web. HTML is similar to SGML, although it is not a strict subset. HTML defines the structure and layout of a Web document or application by using a variety of tags and attributes.

I

ISDN
Integrated Services Digital Network. ISDN comes in two basic types: BRI, which is 144,000 bps and designed for the desktop, and PRI, which is 1,544,000 bps and designed for telephone switches. BRI uses four unshielded normal telephone wires (two twisted pairs) to deliver two “Bearer” (B channel) of 64K bps each and one “data” (D channel) of 16K bps.

In-Band
Transmission within a frequency range normally used for voice transmission. Contrasted with Out-of-Band signaling, which uses frequencies outside of the voice range.

IP
Internet Protocol. The most important protocol on which the Internet is based. The IP Protocol is a standard describing software that keeps track of the internetwork addresses for different nodes, routes outgoing messages, and recognizes incoming messages.

IP Address
A 32-bit address, used in IP routing. Basically, this address identifies a device within a network using a sequence of numbers.

J

Jitter Delay
Is caused by transmission delays in an Internet telephony (VoIP) network . As the device receives voice packets, it adds small amounts of delay to the packets so that all the packets appear to have been received without delays. Voice signals are sequential by nature (i.e., the must be played back in the order in which they were sent) and this ensures that the resecived packets are in the correct order. Jitter can result in choppy audio signals. Generally, any distortion of a signal or image caused by poor synchronization.

L

LAN
Local Area Network. A short distance data communications network used to link computers and peripheral devices (such as printers).

LED
Light-emitting diode. A semiconductor diode which emits light when a current is passed through it, indicating that the power is on.

M

MI
Management Interface. A VT-100 style Terminal Emulation (TA) program which provides the system administrator with full configuration and status capabilities for the PBXgateway and multiple Remote units.

N

Network Hub
A common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Network Number
Often associated with Subnet. Specifies an individual network of devices that communicate via IP to each other. Example “192.168.1.0”.

O

Out-of-Band
With out-of-Band signaling a separate narrow signaling band within the 4-kHz bandwidth is used to control signals.

P

Packet Transmission
A piece of a message is transmitted over a packet switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagram.

PBX
Private Branch Exchange. A small version of the phone company’s larger central switching office usually installed in a corporate facility.

Phone-Set Interface
An interface with the Remote units through a users phone providing a limited set of configuration parameters.

PSTN
Public Switched Telephone Network..

Punch Block
A device used to connect one group of wires to another. A punch block is used to connect the digital lines from the PBX to the RJ-21 cable connected to the PBXgateway.

Q

QOS
Quality of Service. A measure of the telephone service quality provided to a subscriber.

R

Remote Unit
The device that connects to the remote telephones and communicates with the PBXgateway at the Corporate facility.

RJ-11
A six conductor modular jack that is typically wired for four conductors. It is the most common jack used for connecting telephones, modems and fax machines.

RJ-21
A 25-pair connector used for connecting the PBXgateway to the PBX.

Router
A device used to forward packets from one or more Network Numbers, to the intended destinations.

RS-232
9 or 25 Position Non-Synchronous Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange (ANS/EIA/TIA-574-90)

RS-530
Physically it is the same as an RS-232 cable, except the RS-530 cable is designed for devices that transmit at higher speeds.

RTP
Real Time Protocol. A protocol designed to address problems caused when real-time exchanges, such as voice are transported over LANs designed for data.

RVP™
Remote Voice Protocol packet encapsulation protocol.

S

SNMP
Simple Network Management Protocol.

SPID
Service Profile Identifier, a number that identifies a specific ISDN line. When you obtain ISDN service, your telephone company assigns a SPID to your line. Part of the initialization procedure is to configure your ISDN terminal adapter to use this SPID.

Subnet
A smaller network that is part of a main network.

Subnet Mask
Used to mask bits of an IP address to determine which packets are destined for the Network that the device is connected to.

Switch Unit
The PBXgateway unit that connects to the PBX/KSU

Synchronous
A method of communication utilizing a master clock to synchronize the timing between successive bits, characters or events.

Sync Rate
The data transfer speed or rate of the synchronous serial port of the network device connected to the WAN port of the PBXgateway or EXTender 6000 Remote unit. The Sync Rates of the serial ports must match.

System Administrator
Basically, the person in charge of managing the network.

T

T1
A digital transmission link with a capacity of 1.544Mbps.

TA
Terminal Adapter. Allows non-ISDN terminals to operate on ISDN lines.

TCP
Tele Connect Protocol. An IP port, as specified in the OSI model.

TCP/IP
Transport Control Protocol / Internet Protocol.

Teleworker
An employee that works from home while communicating with the corporate office by telephone, fax and/or computer.

Telnet
A connection type protocol.

U

UDP
User Datagram Protocol. An IP port as specified in the OSI model.

V

V.35
A ITU-T standard for a synchronous serial interface between the Switch or Remote unit and a network device for data rates greater than 19.2Kbps.

Voice Compression
Enables voice to be transmitted over a network that may not have adequate or required bandwidth without a major reduction in voice quality.

Voice Link
A proprietary term referring to MCK's method of connecting a remote user.

VOIP
Voice Over IP. Providing voice communications over the IP network.

W

WAN
Wide Area Network, group of two or more computer systems linked together. With a WAN the computers are farther apart and are connected by telephone lines or radio waves.

Appendix A: Management Interface (MI) Menus

Introduction

The PBXgateway Management Interface (MI) provides the system administrator with a VT-100 style interface for the complete configuration of both the Gateway and Remote units.

Main Menu

The Main Menu which appears when the MI is first entered, displays the following submenus;

Configuration
The Configuration submenus contain Port and WAN set up, Log information, and System parameters.

Status
The Status submenus display specific functional information necessary to troubleshoot and analyze unit performance.

Utilities
The Utilities submenus contain system and diagnostic utilities used for copying or deleting configuration files.

Remote/Switch Login
This command will connect you to the unit at the alternate site.

Logout
This command will terminate the MI session.

Main Menu

Menu	Sub-Menus	For more Info see
Configuration	Port	Page 201
	Default	Page 201
	Ports 1-8	Page 201
	WAN	Page 203
	Connect (R)	Page 204
	Analog Card (B)	Page 204
	Log	Page 207
	IP	Page 208
	System	Page 210
	Save	-
Status	Port	Chapter 5
	WAN	Chapter 5
	Connect	Chapter 5
	Log	Chapter 5
	IP	Chapter 5
	System	Chapter 5
Utilities	System	Page 211
	File	Page 211
	Diagnostics	Page 213
	Upgrade	Page 211
Remote Login		Page 105
Logout		Page 115

Table 20: Main Menu

(R) Applies to the Branch Office & EXTender 4000 units only.
(B) Applies to the Branch Office unit only.

Port Menu

Menu	Parameters	Possible Value	Default value	For more info see page
Default	**Enabled**	Yes No	Yes	65
	Password	[ ]		67
	Auto Connect (R)	Disabled Enabled	Disabled	109
	Banner (R)	[ ]		110
	Voice (G)	--	--	202
Ports 1-8 or 12	Enabled	Default Yes No	Default	65
	Auto Connect (R)	Enabled Disabled	Default	109
	User ID	[ ]		68
	Password	[ ]		67
	Description	[ ]		-
	Voice (G)	--		202
	Banner (R)	[ ]		110
	Logout Code (R) (Avaya Protocol)			134
	MSB Key (R) (Nortel Protocol)			136

Table 21: Port Menu
(R) Applies to the Branch Office & EXTender 4000 units only.
(G) Applies to the PBXgateway unit only
.

Voice Menu

Parameters	Possible Values	Default value	For more info see page
Method	ADPCM 32 ADPCM 24 G.729A, G.711,	ADPCM 32	63
Path	Dynamic or Constant	Constant	63
Attenuation	25-150	25	63
DTMF (Avaya Protocol only)	In-band Out-of-band	Out-of-Band	131
Silence Detection	Enabled Disabled	Enabled	63
Jitter Delay	0-250	0	134
Packet Size	1-12	2	136
Packet Trace	Enabled Disabled	Disabled	136

Table 22: Voice Menu

WAN Menu (WAN 1 & WAN 2)

Parameters	Possible Value	Default value	For more info see page
Enabled	Yes No	WAN 1 - Yes WAN 2 - No	70
Mode	Sync-V.35 Sync-RS232 Sync-RS530	Sync-V.35	71
Sync Set up-Sync Rate	Multiples of 56K or 64K	[384000]	71

Table 23: WAN Menu

Connect Menu (R)

Parameters	Possible Value	Default value	For more info see page
Type	RVP_over_IP RVP_Direct	RVP_Direct	106
RVP_Direct	--		106
RVP_over_IP	--		107

Table 24: Connect Menu

(R) Applies to the Branch Office & EXTender 4000 units only.

Analog Card (G) & (B)

Menu	Parameters	Possible Value	Default value	For more info see page
Defaults Ports 1-8	Enabled	Yes No	Yes	112
	Key	[ ]	4	112
	Ring	Yes No	Yes	112

Table 25: Analog Menu

(G) Applies to the PBXgateway unit only.
(B) Applies to the Branch Office unit only.

RVP_Direct Menu (R)

Parameters	Possible Value	Default value	For more info see page
Primary Interface	WAN1 WAN2	WAN1	106
Secondary Interface	NONE WAN1 WAN2	NONE	106
Utilization	[ ]	100	144

Table 26: RVP_Direct Menu

(R) Applies to the Branch Office & EXTender 4000 units only.

RVP_over_IP Menu (R)

Parameters	Possible Value	Default value	For more info see page
Default Port-IP Destination	Valid IP address	[ ]	107
Ports 1 to 8 or 12-IP Destination	Valid IP address	[ ]	107

Table 27: RVP_over_IP Menu

(R) Applies to the Branch Office & EXTender 4000 units only.

Log Menu

Parameters	Possible Value	Default value	For more info see Page
Size	4096-131072	32768	140
Default Priority	Info	Info	138
SYS Prior	Debug	<Default>	138
MGMT Prior	Trace	<Default>	138
NET Prior	Fatal	<Default>	138
Port Prior	Error	<Default>	138
	Warning		

Table 28: Log Menu

IP Menu

Parameters	Possible Value	Default value	For more info see page
Address	Valid IP address	[ ]	76
Subnet Mask	Valid IP address	[ ]	76
Default Router	Valid IP address	[ ]	76
Telnet	Enabled Disabled	Enabled	78
FTP	Enabled Disabled	Disabled	78
DNS	Enabled – Yes/No	No	81
	Server IP Address	[ ]	81
	Domain Name	[ ]	81
SNMP	-	-	209
Web Server	-	-	144
Syslog	-	-	209

Table 29: System Menu

SNMP Menu

Parameters	Possible Value	Default value	For more info see page
Enabled	Yes No	No	-
Trap Hosts	]		142
Trap Priority	Error Warning Info Fatal	Error	143
Trap Path	LAN WAN Both	LAN	143
Sys Contact	]		141
Sys Location	]		142

Table 30: SNMP Menu

Syslog Menu

Parameters	Possible Value	Default value	For more info see page
Enabled	No Yes	No	-
Host	]		133
ID	]		133
Default Priority	Info	Info	139
SYS Prior	Debug	<Default>	139
MGMT Prior	Trace		139
NET Prior	Fatal		139
Port Prior	Error Warning		139

Table 31: SysLog Menu

System Menu

Parameters	Possible Value	Default value	For more info see page
Name	[ ]		82
Use Switch Time (R)	Yes No	No	-
Switch Time Offset (R)	[ ]	0	-
Console Baud	9600 19200 38400 2400 4800	9600	83

Table 32: System Menu

(R) Applies to the Branch Office unit only.

Utilities Menu

Menu	Parameters	Possible Value	Default value	For more info see page
System	Set Password	-	-	86
	Set Date	-	-	212
	Clear log	-	-	129
	Dump All	-	-	132
	Reset Stats	-	-	139
	Reboot	-	-	114
File	Copy to (unit)	-	-	187
	Delete	-	-	-
	Edit Config	-	-	175
	Optimize	-	-	136
Diagnostics	-			213
Upgrade	Console Upload	-	-	188
	Image File	-	-	**Error! Bookmark not defined.**
	Configure File	-	-	174

Table 33: Utilities Menu

Set Date Menu

Parameters	Possible Value	Default value	For more info see page
Month	Jan-Dec	Current month	85
Day of month	]		85
Year	]		85
Hour	]		85
Minute	]		85
Second	]		85
Daylight Savings	Enabled Disabled	Enabled	85 85

Table 34: Set Date Menu

Diagnostics Menu

Menu	Parameters	Possible Value	Default value	For more info see page
Test IP	Begin Test			
	IP Address	]		
	Count	]	5	
Test WAN	Begin Test			158
	WAN Port	]	1	-
	Count	]	20	-
	Packet Size	]	10	-
	Timeout	]	10	-
Reset WAN				-
Reset Port				-

Table 35: Diagnostics Menu

Appendix B: Bandwidth Requirements

This Appendix provides information on the required bandwidth necessary to accommodate remote users connected to the PBXgateway using a synchronous-serial connection via a WAN port.

Overview

One of the most important factors in the success of your PBXgateway is to determine the necessary network bandwidth needed for your application. This Appendix will explain how to determine the size of the required bandwidth that will be needed in your application of the PBXgateway units. Determining the appropriate bandwidth is truly a function of two factors:

- Number of Users (Phones)
- Voice Compression for Each User

Number of Users

The number of users is the number of simultaneous users (digital PBX phones) that will be extended at any given branch location. Physically, there could be up to twelve simultaneous users for each PBXgateway unit.

Voice Compression

The PBXgateway deploys voice compression in order to extend multiple users across fewer data channels. The PBXgateway supports the following voice compression algorithms: 32 Kbps ADPCM, 24 Kbps ADPCM and G.729A. Depending on the voice compression algorithm selected, you may need anywhere from 16 Kbps (G.729A) up to 40 Kbps (ADPCM 32) per user.

Compression Algorithms vs. Corresponding Bandwidth Size

G.711	ADPCM 32	ADPCM 24	G.729A
64 (72) Kbps	32 (40) Kbps	24 (32) Kbps	8 (16) Kbps

( ) Maximum value of the combined compression bandwidth and the signaling between the Switch and Remote units. This number reflects both parties talking simultaneously in a voice conversation. Under normal conditions, this number will be lower.

Using the bandwidth management formula on the next page, you can determine the total bandwidth necessary to support your application. If you have excess bandwidth on your network circuit, your network terminating devices could allow you to use that bandwidth to connect to a router or even another PBXgateway. In order to accomplish this, you must have the multi-port capability on your CSU/DSU. For more information on your network terminating devices, please see the Network Terminating Equipment section of the Quick Installation Guide.

Selecting the Proper Voice Compression

The best voice quality is achieved by using the ADPCM 32 compression. The maximum quality comes at the expense of the highest utilized bandwidth. The largest voice compression is achieved by using G.729A. If you are using this algorithm, you will save on bandwidth and still achieve voice quality that is regarded as near toll. If absolute conversation quality is your focus and bandwidth is no object, you probably want to select ADPCM 32. If bandwidth is a priority you will employ G.729A.

If you are using different compression algorithms for each individual user (port), use the following formula to establish your aggregate data bandwidth needs.

A x 16 + **B** x 32 + **C** x 40 = **D**

A: number of G.729A Users
B: number of ADPCM 24 Users
C: number of ADPCM 32 Users
D: Total Bandwidth

Divide this bandwidth by either 64 or 56, in order to establish the correct number of DS0 channels to be used.

Example: If your DS0s on your CSU/DSUs are set up for 56Kbps, use 56 and if they are set up for 64Kbps DS0s, use 64.

Appendix C: EXTender 6000 Phone-Set Interface

Provided for reference only.

This Chapter provides information on the Phone-Set Interface. This interface provides the system administrator with limited configuration parameters using a digital telephone keypad for input commands.

Phone-Set Interface

Introduction

The Phone-Set interface is used for setting limited configuration parameters for the EXTender 6000 and EXTender 4000 remote units from a two-wire digital phone.

Settings include:

- Console Data Rate
- IP Parameters
- Default Route

Accessing the Phone-Set interface

Press ‘Hold’ key (on the phone) four times.

Menu Legend

The user navigates through the Phone-Set interface using the keypad on the phone. The menu legend below, shows each applicable numeric key and the screen or command that it corresponds to within the interface.

Prv: Previous Screen
Nxt: Next Screen
Ok: Accept changes

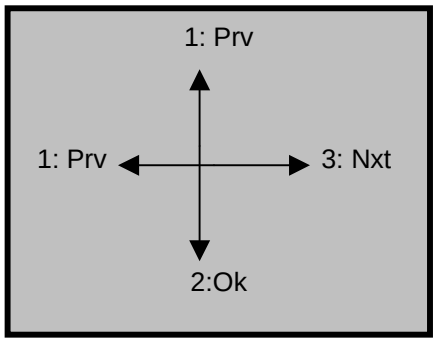
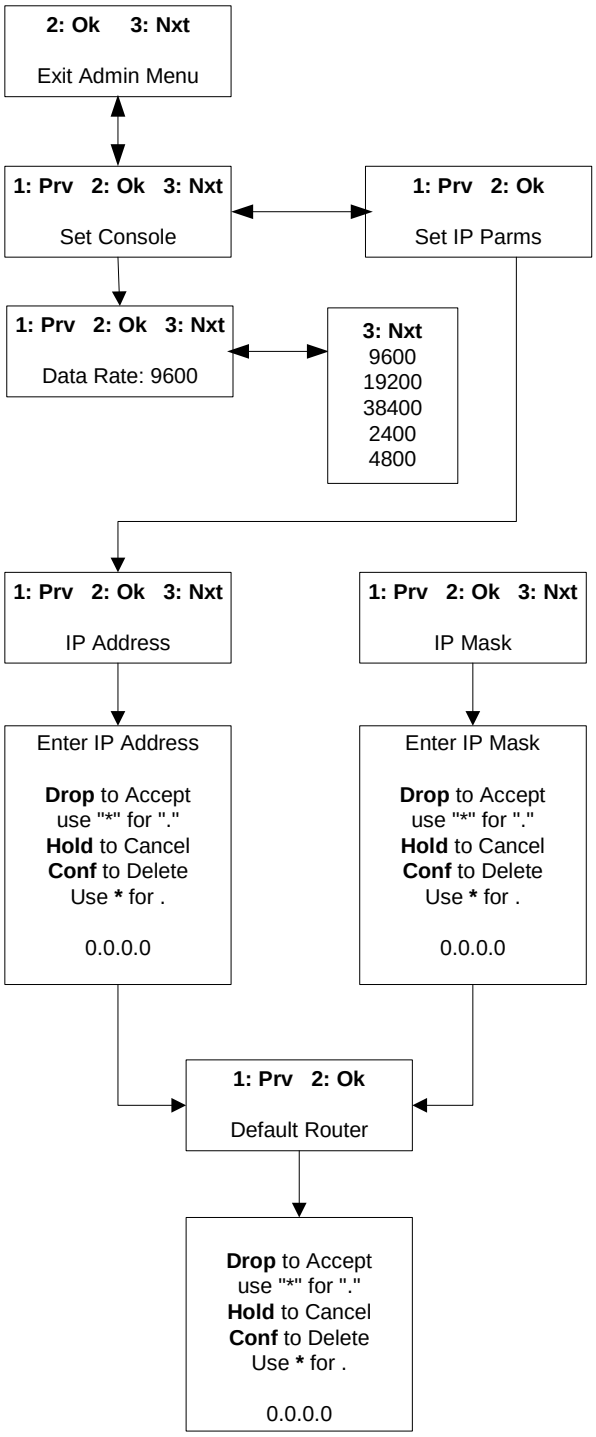


Figure 95: Menu Legend

***Note**: Once in the interface this is the first screen displayed.*



Appendix D: SNMP

This Chapter provides information on the PBXgateway Simple Network Management Protocol (SNMP) parameter.

Introduction

The PBXgateway supports the Simple Network Management Protocol (SNMP) for monitoring the PBXgateway and multiple Remote units.

SNMP: The network management architecture for managing virtually any network type including TCP/IP and other protocols (IPX, etc…). SNMP operates on top of the Internet Protocol (IP). The purpose of SNMP is to flag failures, or error conditions with the Switch and/or Remote units and to automatically notify the network administrator. Error conditions are sent as SNMP "traps".

Trap: SNMP mechanism permitting a device to send an alarm to a management workstation.

MIB: The network administrator must load a MIB file (Management Information Base) to properly monitor the PBXgateway Switch and remote units. This file contains numerous tables based on the MI Status tables and provides information such as error counts, and the on/off status of both the Switch and Remote units. (for reference see page D-*223 MIB vs. Status Menu comparison*)

The latest MIB files are available at www.MCK.com.

EXTender MIB files:

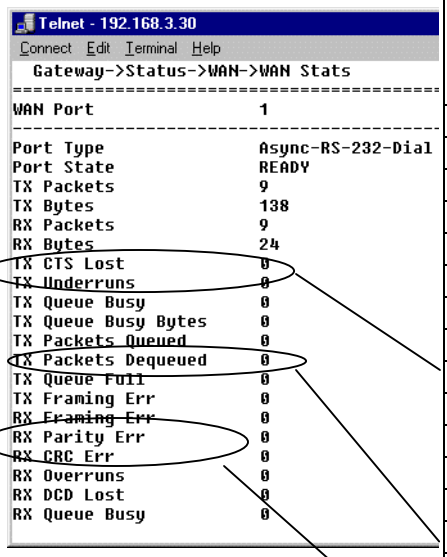
***.mib:** This file contains necessary information for controlling the EXTenders.

HP® Openview **(or equivalent)**
A third party software package that must be installed and running on the network administrator's workstation to view and monitor all SNMP traps.

MI Status Menu vs. MIB Group Table

MI Status Menu

(path: Switch->Status->WAN Stats)



Group Name: extWANStatGroup
extWAN
extWANPortType
extWANPortState
extWANPortEnabled
extWANTxPackets
extWANTxBytes
extWANRxPackets
extWANRxBytes
extWANTxCTSLost
extWANTxUnderruns
extWANTxQueueBusy
extWANTxQueueBusyBytes
extWANTxPacketsQueued
extWANTxPacketsDequeued
extWANTxQueueFull
extWANTxFramingErr
extWANRxFramingErr
extWANRxParityErr
extWANRxCRCErr
extWANRxOverruns
extWANRxDCDLost
extWANmode

Table 36: Status Menu vs. MIB Table

IMPORTANT:
This is an example of the MIB files internal group, in this case it is the extWANStatsgroup. This is an internal table within the EXTender MIB file which accommodates every status entry for the Status menu within the MI.

Major Groups of the EXTender MIB

MIB Group	Management Interface (MI) Menu	Page
extSystemGroup	Status->System->General Info	225
extInfoTable	Status->Connect->Connect Info	226
extStatisticsTable	Status->Connect->Connect Stats	227
extPortStatTable	Status->Port	228
extWANStatTable	Status->WAN->WAN Stats	229
extBandwidthUsageTable	Status->WAN->WAN Bandwidth	230
extDiagnosticTable	Status-> System->HW Diagnostics	230
extPortTable	Status->Port->Port Stats	231
extAlarmNotificationGroup	The “LOG messages” that appear in the LOG.	232
extSnmpControlGroup	Configuration->IP	232
extTopologyGroup	Defines product relationships	233
extSuspendTable	Call Suspend information, if available.	233
extRVPDirectGroup	Remote->Config->Connect->RVPDirect	234
extRVPOverIPGroup	Remote->Config->Connect->RVPoverIP	234

Table 37: MIB verses MI

MIB Group Tables

Group Name: extSystemGroup	Description
extHardwareType	Indicates if unit is “Switch (Gateway)” or “Remote”.
extSystemName	This is the name specified in the “Configuration->System” menu.
extSerialNumber	Serial number of unit.
extTimeBooted	Time that the unit was last booted.
extIPAddress	The IP address of the unit.
extMACAddress	The MAC address of the unit.
extRuntimeVersion	The version of software that is running.
extPLDVersion	Version of PLD.
extSignalDSPVersion	Version of Signal DSP.
extVoiceDSPVersion	Version of Voice DSP.
extFlashVersion	Version of FLASH.
extROMVersion	Version of ROM.
extHardwareVersion	Version of Hardware.
extSerialPorts	Number of serial ports.
extPhonePorts	Number of digital phone ports.
extDRAM	Size of DRAM.
extHeap	Size of HEAP.
extFlash	Size of FLASH.
extBandwidthAvailable	The bandwidth available on WAN port.
extDCESupportVersion	Version of DCE Support.

Table 38: extSystemGroup

Group Name: extInfoTable	Description
extInfoPort	Ports 1-8.
extInfoCurrentState	State of port: UP, RD, NC, XX, VC, AN, CS
extInfoDuration	The duration in current state.
extInfoExtended	Indicates if port is extended.
extInfoOffHook	Indicates ports offhook.
extInfoVoice	The compression algorithm used.
extInfoSignalPort	Connection method for Signal: WAN1, WAN2, IP
extInfoVoicePort	Connection method for Voice: WAN1, WAN2, IP
extInfoLostSignal	Amount of Lost Signal errors.
extInfoV42Resync	Number of V42 Resync errors.
extInfoV42FarResync	Number of V42 FarResync errors.
extInfoV42Retries	Number of V42 Retry errors.
extInfoV42Timeouts	Number of V42 Timeout errors.

Table 39: extInfoTable

Group Name: extStatisticsTable	Description
extStatConnectTries	Amount of connect attempts.
extStatConnections	Amount of successful connections.
extStatByUser	Amount of Disconnects by User.
extStatCarrierLost	Amount of Disconnects from Lost Carrier.
extStatPortOffline	Amount of Disconnects from port being offline.
extStatPortInUse	Amount of Disconnects because port was in use.
extStatNoVoice	Amount of Disconnects because there was no Voice Path (no bandwidth).
extStatBadPassword	Amount of Disconnects from wrong Password being entered.
extStatBlockedCalls	Number of Blocked Calls (no bandwidth).
extStatLostSignalStat	Total Disconnects from Lost Signal
extStatLostSigDisconnect	Number of Disconnections due to Lost Signal.
extStatLostSigReconnect	Number of Reconnections due to Lost Signals (only applies to Call Suspend).

Table 40: extStatisticsTable

Group Name: extPortStatTable	Description
extPstatPercentVC	Percentage value of all call types that User/Port was on a “VC” (Voice Call).
extPstatPercentUP	Percentage value of all call types that User/Port was “UP” (connected).
extPstatPercentRD	Percentage value of all call types that User/Port was “RD” (ReaDy).
extPstatPercentNC	Percentage value of all call types that User/Port was “NC” (Not Connected).
extPstatPercentXX	Percentage value of all call types that User/Port was “XX” (disabled).
extPstatVCcount	Number of “Voice Calls” in minutes.
extPstatVCaverage	The average number of “Voice Calls”.
extPstatUPcount	The number of minutes the User/Port has been “UP”.
extPstatUPaverage	The average number of minutes the Port has been “UP”.
extPstatRDcount	The number of minutes the User/Port has been “RD”.
extPstatRDaverage	The average number of minutes the Port has been “RD”.

Table 41: extPortStatTable

Group Name: extWANStatTable	Description
extWAN	Shows WAN ports: WAN1, WAN2
extWANPortType	Shows WAN port type: Sync
extWANPortState	State of WAN port: UP, DN, INIT, CNCT
extWANPortEnabled	WAN enabled state: Enabled, Disabled.
extWANTxPackets	Number of Transmited packets.
extWANTxBytes	Number of Transmited bytes.
extWANRxPackets	Number of Received packets.
extWANRxBytes	Number of Received bytes.
extWANTxCTSLost	Number of times CTS signal was lost
extWANTxUnderruns	Number of times WAN Transmit buffer was empty.
extWANTxQueueBusy	Number of times Transmit queue was busy.
extWANTxQueueBusyBytes	Number of Transmit bytes queued.
extWANTxPacketsQueued	Number of Transmit packets queued.
extWANTxPacketsDequeued	Number of Transmit bytes dequeued (lost).
extWANTxQueueFull	Number of times the Transmit queue was full.
extWANTxFramingErr	Number of Transmit Framing errors.
extWANRxFramingErr	Number of Receive Framing errors.
extWANRxParityErr	Number of Receive parity errors.
extWANRxCRCErr	Number of Receive Cyclic Redundancy Check errors.
extWANRxOverruns	Number of times Receive buffer was full, and data had to be resent.
extWANRxDCDLost	Number of times Receive DCD signal was lost.
extWANRxQueueBusy	Number of times Receive queue was busy.
extWANRxNoBuffers	Number of times no Receive buffers available.
extWANRxTaskBusy	Number of times Receive capability was busy.
extWANRxApplBusy	Number of times Receive Applet was busy.
extWANRxErrors	Number of Receive errors.
extWANspeed	WAN port speed.
extWANmode	WAN mode setting: Sync

Table 42: extWANStatTable

Group Name: extBandwidthUsageTable	Description
extBandwidthIndex	Indicates the sample times: every hour
extBandwidthTime	Time at which each sample occurred.
extBandwidthSent	Bandwidth sent during sample period.
extBandwidthClipped	Bandwidth clipped during sample period.
extBandwidthPercentage	The percentage of available bandwidth, equals (BW Sent / BW Clipped).

Table 43: extBandwidthUsageTable

Group Name: extDiagnosticsTable	Description
extDiagTest	Names of Diagnostics tests.
extDiagResult	Results of Diagnostics tests.

Table 44: extDiagnosticsTable

Group Name: extPortTable	Description
extPtabPortID	The Port ID names.
extPtabEnabled	The “Enabled” value in the Ports Default & 1-8 menus.
extPtabAutoConnect	The “Auto connect” value in the Ports Default & 1-8 menus.
extPtabBanner	The “Banner” value in the Ports Default & 1-8 menus.
extPtabDescription	The “Description” value in the Ports 1-8 menus.
extPtabUserID	The “User ID” value in the Ports 1-8 menus.
extPtabLogout	The “Logout” value in the Ports 1-8 menus (Remote only).
extPtabVoiceMethod	The “Voice” value in the Ports Default & 1-8 menus (Switch only).
extPtabVoicePath	The “Path” value in the Ports Default & 1-8 menus (Switch only).
extPtabVoiceCompanding	The “Companding” value in the Ports Default & 1-8 menus.
extPtabVoiceDTMF	The “DTMF” value in the Ports Default & 1-8 menus.
extPtabVoiceSwitchEcho	
extPtabVoiceRemoteEcho	
extPtabVoiceSilenceDetection	The “Silence Detection” value in the Ports Default & 1-8 menus (Switch only).
extPtabVoicePacketTrace	The “Packet Trace” value in the Ports Default & 1-8 menus (Switch only).
extPtabVoiceJitterDelay	The “Jitter Delay” value in the Ports Default & 1-8 menus (Switch only).
extPtabVoicePacketSize	The “Packet Size” value in the Ports Default & 1-8 menus (Switch only).

Table 45: extPortTable

Group Name: extAlarmNotificationGroup	Description
extAlarm	Log messages that appear in the Log file.

Table 46: extAlarmNotificationGroup

Group Name: extSnmpControlGroup	Description
extSnmpEnabled	Indicates SNMP is enabled.
extTrapPriority	Indicates the Priority setting for SNMP traps to be sent.
extTrapHost1	The IP address or HOST name to send first trap message.
extTrapHost2	The IP address or HOST name to send second trap message.
extTrapHost3	The IP address or HOST name to send third trap message.
extTrapHost4	The IP address or HOST name to send fourth trap message.
extTrapHost5	The IP address or HOST name to send fifth trap message.
extTrapHost6	The IP address or HOST name to send sixth trap message.
extTrapHost7	The IP address or HOST name to send seventh trap message.
extTrapHost8	The IP address or HOST name to send twelfth trap message.
extTrapPath	Path where traps are sent: WAN, LAN, BOTH

Table 47: extSnmpControlGroup

Group Name: extTopologyGroup	Description
extTopType	The device type of the main unit: Switch, Remote
extTopDevice1	Device type connected to Port 1.
extTopDevice2	Device type connected to Port 2.
extTopDevice3	Device type connected to Port 3.
extTopDevice4	Device type connected to Port 4.
extTopDevice5	Device type connected to Port 5.
extTopDevice6	Device type connected to Port 6.
extTopDevice7	Device type connected to Port 7.
extTopDevice8	Device type connected to Port 8.

Table 48: extTopologyGroup

Group Name: extSuspendTable	Description
extSuspendEnabled	Indicates if Call Suspend is Enabled.
extSuspendRvpMethod	
extSuspendIpDestination	The IP address or HOST name to connect to, from Call Suspend.
extSuspendRemLoginTimeout	
extSuspendTimeout	Call Suspend timeout value.
extSuspendMode	Call Suspend mode used: Ring, Lamp
extSuspendACDTone	Indicates if ACD Tone is enabled for individual Port (Remote only).

Table 49: extSuspendTable

Group Name: extRvpDirectGroup	Description
extRvpDirectPrimaryInterface	The RVP_Direct Primary interface: WAN1, WAN2
extRvpDirectPrimaryDialNum1	The first Primary dial number.
extRvpDirectPrimaryDialNum2	The second Primary dial number.
extRvpDirectSecondaryInterface	The RVP_Direct Secondary interface: WAN1, WAN2
extRvpDirectSecondaryDialNum1	The first Secondary dial number.
extRvpDirectSecondaryDialNum2	The second Secondary dial number.
extRvpDirectUtilization	The RVP_Direct % utilization.
extRvpDirectDialback	Indicates if Dialback is enabled over RVP_Direct.

Table 50: extRvpDirectGroup

Group Name: extRvpOverIpGroup	Description
extRvpOverIpInterface	The IP destination address.

Table 51: extRvpOverIPGroup

SNMP Setup

This Addendum covers information for installing all support software, accessing and identifying specific trap information, viewing the “Alarm Log” and viewing the MIB.

Set up steps

1. Load a third party-network management software package, such as HP OpenView®, onto the PC used to manage the PBXgateway Switch and Remote units.

   ***Note**: There are many applications that can be used to manage the SNMP parameters for the Switch and Remote units.*

2. Install the EXTender configuration files, available on MCKs web site (www.MCK.com), onto the same PC mentioned in step 1.

3. Add the EXTender’s MIB to the third party-network management software package database. This will allow the software to access the status and configuration variables of the EXTender.

4. Set the password (Community String) to allow access to the EXTender.

5. Format the Trap error messages from the EXTender into an easily read form.

6. Enable SNMP within the MI.

Install the EXTender MIB Files

The EXTender MIB files are necessary for the third party software to read the Remote unit status tables, and to receive readable SNMP Trap error messages.

***Note**: This procedure assumes that a third party software package has been installed on a PC*.

Copy the following files into the directories as specified below:

mibs\EXTenderxxxx.mib - (where xxxx refers to the EXTender release).
Copy to: c:\ov\mibs subdirectory

This file is the MIB for control of the EXTender. This file must be compiled into the third party software package.

Setting the Community Password

The EXTender comes with a default SNMP read password also known as a Community String. This password must be specified inside the third party software to allow the user to view MIB objects.

Note: Before setting the password, the units must have an IP Address assigned by the network administrator and must be part of the software "Network View".

Procedure

1. Access the "Network View" menu from within the third party software. Click on the Icon of the device to be configured.

   Note: Each Icon should be titled with the IP Address for the device.

   The default read (community) password is: public

2. Type in the password next to Community. Click **OK**.

   ***Note**: The Set Community password is not used by the EXTender and may be ignored.*

Configuring the Trap Host

The EXTender will send alarm messages (SNMP Traps) to any Trap Host who's IP Address has been entered into one of the 12 slots provided in the User Interface SNMP Configuration Menu. These slots are named Trap Host 1, Trap Host 2, etc.

Once an address has been entered into one of these slots, the EXTender will send Traps to that address. See page 142, for information on setting the SNMP Trap Hosts.

Trap Customization

The third part software will receive and display Trap messages from the EXTender. But without some configuration these messages will be a confusing list of numbers, as shown in Figure D.2.

Figure 96: Confusing Results from No Configuration

To display friendly and readable Trap messages, the software can be configured to display all the information contained in the Trap Error messages sent by the EXTender.

***Note**: The Trap messages correlate with "log messages" within the MI. (see Appendix E for more information on Log Messages).*

Defining a Fatal Trap

Below is an example of setting up “HP Openview for Windows” to receive the Log messages from the PBXgateway EXTender.

1. From within the third party software, navigate to the Add Trap window.
2. In the box Number: type: “1”
3. In box Name: type “EXTender Fatal Error”
4. In box Severity: select choice “Critical”
5. In box Description: type “$E, $1”

   ***Note**: Delete any existing text.*

6. Click on the OK button.

Defining an Error Trap

1. From within the third party software, navigate to the Add Trap window.
2. In the box Number: type: “2”
3. In box Name: type “EXTender Error”
4. In box Severity: select choice “Major”
5. In box Description: type “$E, $1”
6. Click on the OK button.

Defining a Warning Trap

1. From within the third party software, navigate to the Add Trap window.
2. In the box Number: type: “3”
3. In box Name: type “EXTender Warning”
4. In box Severity: select choice “Warning”
5. In box Description: type “$E, $1”
6. Click on the OK button.

Defining an Info Trap

1. From within the third party software, navigate to the Add Trap window.
2. In the box Number: type: “4”
3. In box Name: type “EXTender Info”
4. In box Severity: select choice “Informational”
5. In box Description: type “$E, $1”
6. Click on the OK button.

Viewing the Customized Alarm Log

1. Click the Alarm icon. The Following screen appears:

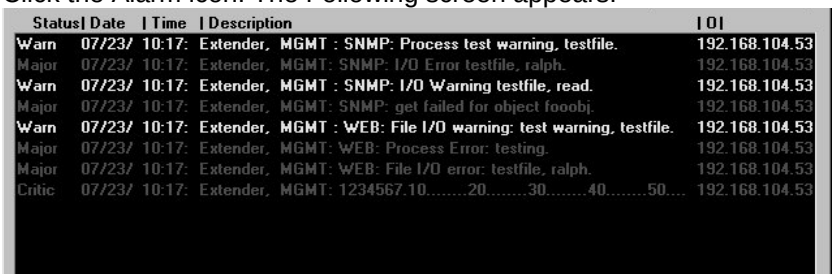


Figure 97: Customized Trap Messages

2. The Customized trap messages are color coded for identification purposes:

   “Red” – Trap messages that are considered Major/Critical.

   “Yellow” – Trap messages that are considered a “Warning”

   “Purple” – Trap messages that are considered simply “Information”.

Using SNMP to Monitor & Troubleshoot Problems

Below is an example of how to use SNMP management to monitor the PBXgateway EXTender.
Example: You have a PBXgateway EXTender with an IP address of “10.2.1.50”. The Remote Branch has an IP address of “10.5.3.50”.

You want to monitor if there are lost signal conditions.

Use your SNMP manager to browse the “EXTender.mib” and create a TRAP condition on the object name “extStatLostSignalStat”. Get the current threshold value, for example “0”. Trigger the TRAP on when the threshold exceeds “0”.

If there is a Lost Signal condition, as shown in the Management Interface menu under “Status->Connect->Connect Stats”, or anything higher than zero, a message will be indicated on the SNMP manager.

You want to monitor if the CSU/DSU or ISDN Terminal Adapter is failing.

Use your SNMP manager to browse the “EXTender.mib”, for example, the Branch Office unit (IP address “10.5.3.50”) and create a TRAP condition on the object name “extWANRxFramingErr”. Get the current threshold value, for example “0” (should be zero). Trigger the TRAP on when the threshold exceeds “0”.

If the value exceeds zero, the ISDN line or Fractional T1 could be having problems. Investigate the problem.

This page is intentionally left blank.

Appendix E: Log Messages

This Chapter provides information on Log Messages. A partial list is provided to define the log message, provide an example for reference, and any required action that should be taken.

Log Messages

Introduction

Each menu within the MI contains an area to display log messages that provide detailed information on the status and condition of the unit. These messages are grouped into four categories with each one detailing a specific functional area of the EXTender operation.

Message Categories

The Log Message categories are:

MGMT: These messages include information on configuration and diagnostic conditions of the unit.

SYS: These messages include information on the operating system and utilities related to the config files.

PORT: These messages include status information for all phone ports and issues related to voice compression and connection details.

NET: These messages include status information for both WAN ports and issues related to network connectivity.

Typical messa

A typical log message is shown in the figure below.

***Note**: Every log message contains similar information to provide a date/time stamp followed by a descriptive message.*

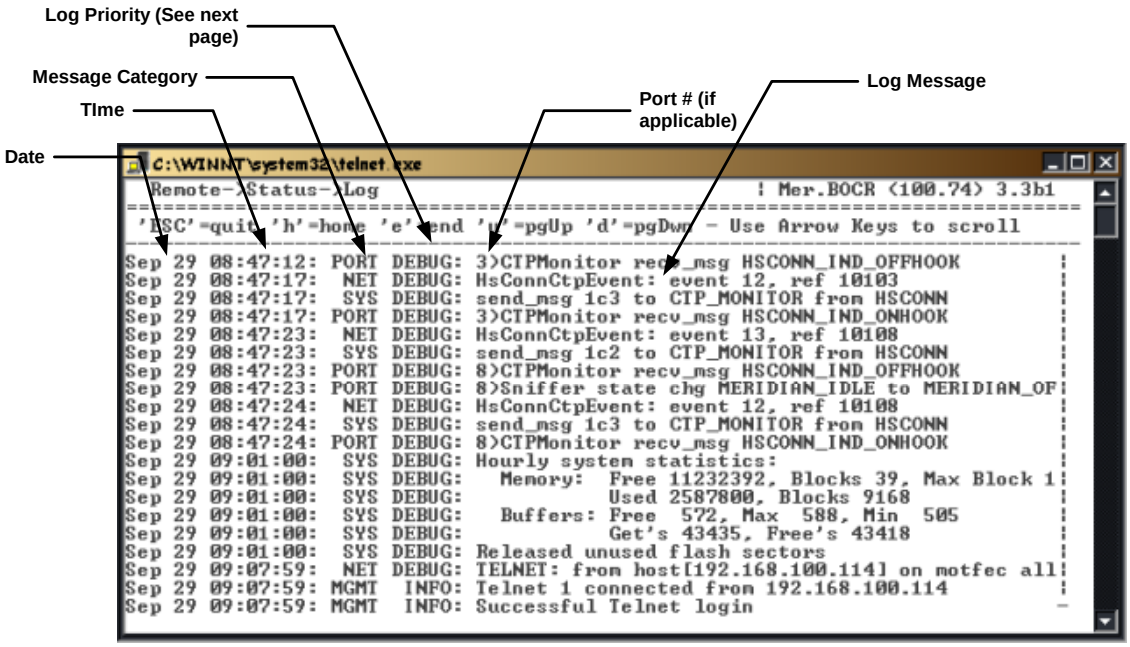


Figure 98: Typical Log Message

Log Priorities

Log Priority	Definition
Fatal	Unit failed. Contact customer service.
Error	Unit failed but may recover. Try rebooting the unit.
Warning	Unexpected error but unit should still function.
Info	Routine event occurred.
Debug	Details on every event only seen with priority set to “Debug” or “Trace”. Note: Debug messages are NOT included in the following list.
Trace	Details on each and every activity. Only seen with priority set to “Trace”. Note: Trace messages are NOT included in the following list.

Table 52: Log Priorities

Partial list of Log Messages

*Notes: This list is sorted by: **1)** Priority**, 2)** Category, and **3)** Message*
The ‘SNMP’ column identifies messages which are captured (YES or NO) with and SNMP Trap (see Appendix ‘D’ for more info).

Priority	Category	Message	Description/Action	SNMP
INFO	MGMT	Administrator password changed	The administrator changed the administrator password via the MI.	YES
INFO	MGMT	Console logout	The administrator has logged off the console port.	NO
INFO	MGMT	Console upload started	The administrator began uploading a file via the console port.	YES
INFO	MGMT	Console upload succeeded	The file transfer on the console has completed successfully	YES
INFO	MGMT	Flash optimization completed	The administrator completed optimizing the flash file system.	YES
INFO	MGMT	Flash optimization started	The administrator began optimizing the flash file system via the MI for better performance.	YES
INFO	MGMT	IP test started, sending 5 packets to 192.168.155.1	IP test began sending the indicated number of packets to the initiated IP Address.	NO
INFO	MGMT	IP test complete: round-trip (ms) min/avg/max = 0/2/5	IP test has finished with minimum, average and maximum round-trip packet delay (with a granularity of 5ms).	NO
INFO	MGMT	Completed test on WAN 1	Test WAN completed with no errors.	NO
INFO	MGMT	Resetting all ports(1-8)	The administrator reset all of the phone ports.	YES

INFO	MGMT	Resetting Port 2	The administrator reset the indicated phone port.	YES
INFO	MGMT	Resetting WAN 1	The administrator reset the indicated WAN via the MI.	YES
INFO	MGMT	Rlogin logout	The administrator has logged out of the Rlogin session.	NO
INFO	MGMT	Rlogin session 1 connected from 192.168.155.1	An incoming Rlogin connection was made.	YES
INFO	MGMT	Rlogin session 1 disconnected	The Rlogin session was disconnected.	NO
INFO	MGMT	Rlogin session 1 initiated from 192.168.155.1	An outgoing Rlogin connection was made.	NO
INFO	MGMT	Starting test on WAN 1	Test WAN started.	NO
INFO	MGMT	Successful FTP login	The administrator has logged on via ftp.	YES
INFO	MGMT	Successful login on the console	The administrator has logged on via the console port.	YES
INFO	MGMT	Successful Rlogin login	The administrator has logged in via Rlogin (Remote/Switch Login)	YES
INFO	MGMT	Successful Telnet login	The administrator has logged on via telnet.	YES
INFO	MGMT	Telnet 2 connected from 192.168.155.1	An incoming Telnet connection was made.	YES
INFO	MGMT	Telnet 2 disconnected from 192.168.155.1	The telnet session was disconnected.	NO
INFO	MGMT	Telnet logout	The administrator has logged out via telnet.	NO
INFO	MGMT	The system clock has been updated	The administrator set the system time.	NO
INFO	MGMT	The system configuration has changed	The administrator changed and saved the system configuration.	YES
INFO	MGMT	The system configuration has changed and requires a reboot	The administrator changed and saved the system configuration and requires a reboot to take effect.	YES
INFO	MGMT	The system configuration has changed and requires a WAN reset	The administrator changed and saved the system configuration and requires a WAN port to be reset to take effect.	YES
INFO	MGMT	The system statistics have been reset.	The systems stats have been reset, and requires a reboot to take effect.	YES
INFO	MGMT	WAN 1 sent 20 (10 byte) packets, received 20. Avg time: 11(msec)	Test WAN completed. The number of packets sent, received average round trip time, and the size of the packet is displayed.	NO

Priority	Category	Message	Description/Action	SNMP
WARNING	MGMT	Console upload failed	The file transfer on the console has failed. Check to make sure the baud rates on Branch/Terminal Application are the same. Verify attempting to transfer a .m*t file.	YES
WARNING	MGMT	Failed login on the console	There was a failed administrator login attempt on the console (invalid user/password combination)	NO
WARNING	MGMT	Failed Rlogin login	There was a failed administrator login attempt via Rlogin (invalid user/password combination)	NO
WARNING	MGMT	Failed Telnet login	There was a failed administrator login attempt via telnet (invalid user/password combination)	NO
WARNING	MGMT	SNMP: I/O Warning Trap I/O Write, failed.	The unit was unable to send an SNMP Trap over IP	YES
WARNING	MGMT	Failed FTP login	There was a failed FTP login attempt (invalid user/password combination).	YES
Priority	Category	Message	Description/Action	SNMP
WARNING	MGMT	SNMP: Process Trap Packet build, failed.	The unit was unable to send an SNMP Trap because it had a problem building the Trap message.	YES
WARNING	MGMT	Successful FTP login	The administrator logged in via FTP to transfer files.	YES
WARNING	MGMT	Unable to test WAN 1, ports are in use	The administrator attempted to Test WAN while phone ports are in use. Need to ensure the phone ports are not in use to ensure voice quality.	NO
WARNING	MGMT	WEB: File I/O Error: /flash0/default.m6b, open.	The unit was unable to open or create a file on the flash file system or ramdisk, which the Web server requires.	YES
ERROR	MGMT	Password is corrupt - access denied	The stored password was corrupted. Contact tech support.	YES
ERROR	MGMT	SNMP: I/O Error proxy I/O Write, failed.	An attempt failed to send an SNMP Trap across a WAN link via a SNMP proxy.	YES
ERROR	MGMT	WAN 1 test failed: Network Error	Test WAN failed due to a network error. Check WAN configuration, DSU/CSU configuration and cabling.	NO
ERROR	MGMT	WEB: File I/O Error: int_msg.txt, open.	An error occurred while the web server was trying to perform a file I/O operation (such as open, read, write, or rename) on the specified file. This may prevent the web server from launching.	YES
ERROR	MGMT	WEB: Process Error: Init. OCB, unable launch HTTP server.	An error occurred during initialization of the unit, which prevents it from launching the Web server.	YES

Appendix F: ConneX Application Guide

Use this Appendix to help you get your ConneX phone up and running. Quick Setup steps, as well as key presses and screen displays are included to help you with your ConneX application.

Personal ConneX Information

IMPORTANT: *The terms RemoteConneX and MobileConneX will be referred to as ConneX, unless otherwise noted in this document.*

This guide was prepared for:

_____

(A) What number will I dial to access the ConneX PBXgateway?

_____

(B) What extension will I dial to access my corporate voicemail?

_____

(C) What is my password?

_____

(D) Do I have to program my own dialback number?

Yes _____ No _____

Using ConneX

The following pages provide step-by-step instructions for programming and operating your mobile phone when enabled with the ConneX Application.

What is the ConneX Application?

The ConneX application is supported on the ConneX™ PBXgateway™. This application puts PBX features and dialtone in your hands when using a mobile phone. The ConneX application is especially attractive to mobile workers because they can receive calls and access the corporate PBX system and commonly used voice applications from anywhere. PBX applications that are accessible through your mobile phone include: internal dialing, hold, transfer, conferencing and dialtone. ConneX provides survivability as well, in cases where your digital desk set goes down, you are still able to receive calls on your mobile phone.

Why Use the ConneX Application?

The two main reasons why we recommend you use the ConneX application on your mobile phone are:

a) you can receive your office-bound calls anywhere at anytime;
b) you can leverage the corporate PBX for long-distance and/or international calls.
c) access to PBX features such as conference, transfer and 4-digit dialing.

Your mobile phone connected to the ConneX PBXgateway can be used as your business phone, resulting in significant cost savings for your company, or as a supplement to your office phone. If you spend little time at the office, there is no need to have and maintain a digital set. With the ConneX application you can receive calls and access most-commonly used PBX features and dialtone from anywhere using your mobile phone.

How Does the ConneX Application Work?

For you to receive calls anywhere, you must enable the ConneX application on your mobile phone. On the surface, your mobile phone appears to be a portable extension of your office phone because both devices will ring when a call comes in, if you choose to use both phones. But in reality, the ConneX application gives your mobile phone access to PBX voice applications once limited only to your digital deskset. Now, how does it really work?

Let's say Jane wants to use the ConneX application on her mobile phone. This is as easy as 1…2…3!

1. The PBX System Administrator (SA) assigns a port on the ConneX PBXgateway for Jane.
2. Jane* (or the SA**) enters her mobile phone number as an authorized number to which the gateway routes calls (a.k.a. dialback number) either from the Admin Menu on the ConneX phone or through the Interactive Voice Response (IVR) system from the mobile phone*.
3. Jane now can use the ConneX application on her mobile phone. She can take calls from anywhere and access critical PBX-supported voice applications (i.e. conferencing, internal dialing) through her mobile phone.

** When operation mode is set to Roaming.*
*** When operation mode is set to Fixed or Fixed/Forced*

Technically speaking, incoming calls are processed by the PBX and the ConneX PBXgateway simultaneously. The PBX routes the call to Jane's office extension while the ConneX PBXgateway places an outbound call to her mobile phone. If Jane accepts the call, the gateway completes the connection (see call path on the diagram on the next page).

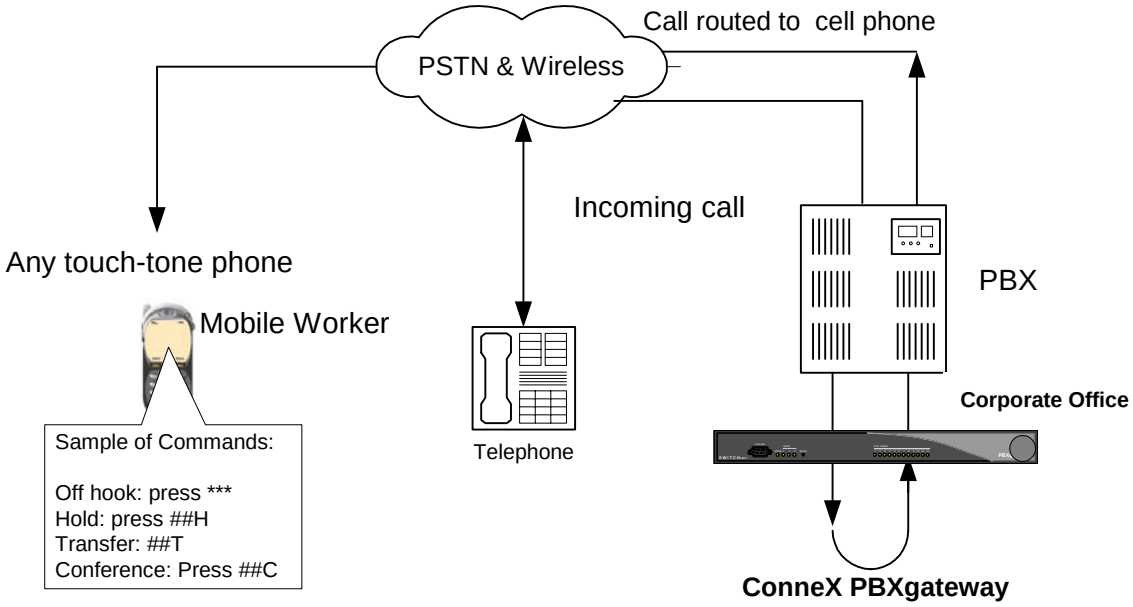


Figure 99: ConneX

Example: Jane's mobile phone rings. Jane is required to press any key on her mobile phone's dial pad to accept the call and to prevent the call from going into her corporate voicemail. After she accepts the call, she is able to talk to the caller, place the call on hold, transfer the call or set up a conference call as if she were using her office phone. (See the ConneX Commands starting on page 255 to learn which keys to press to imitate digital handset push buttons). If Jane chooses not to accept the call, the call is forwarded to her corporate phone voicemail.
When Jane wants to bypass long-distance toll charges, she dials into the ConneX PBXgateway using the number provided by the System Administrator to get PBX dialtone. Once she has accessed the dialtone she can place calls through the PBX system. As a System Administrator, ensure each person has a unique DN to access the PBX dialtone to prevent problems when two users dial into the PBX at the same time.

Programming Your Mobile Phone

This section includes detailed information on the configurable operation modes, set up instructions and overall operation of your mobile phone when enabled with the ConneX application.

Alert: Before getting started, make sure your phone is setup to access automated calling systems like voicemail and Interactive Voice Response (IVR) (i.e.: Motorola TDMA digital StarTAC™ phone users, for example, must turn Scratchpad Tones ON). The ConneX application includes an IVR system thus requiring your phone to be properly configured. Consult your phone's manual for specific instructions.

DEFINITIONS
Dialback Mode: A configurable setting that determines where the ConneX PBXgateway routes your calls. There are four different operation modes and the level of security varies from one to another. The SA is the only person who can change the operation mode. See information on each of the modes for more details.

Dialback Number (DN): The telephone number that the ConneX PBXgateway uses to reach you on your mobile phone. Incoming calls to your office extension are routed to the dialback number that is currently set.

***Note**: Dialback number must include prefix (9+1 e.g.) necessary to access outside line.*

Operation Modes

Roaming

This mode allows you to program/modify the Dialback Number (DN) only via the IVR system. The DN is automatically saved in the ConneX PBXgateway. You can change the DN anytime via the IVR system. The DN is your mobile phone number. When you ENABLE your mobile phone in this dialback mode, all office-bound calls will be routed to that device for as long as it is turned on. Unanswered calls are routed to your office voicemail.

Fixed

This mode requires the SA to program a permanent Dialback Number (DN) in the ConneX PBXgateway. In Fixed mode, you cannot modify the DN via the IVR system. When you ENABLE your mobile phone in this dialback mode, all office-bound calls will be routed to that device for as long as it is turned on. Unanswered calls are routed to your office voicemail. In this mode, the ConneX PBXgateway will authenticate Jane via her port password (if assigned) and the DN (her mobile phone number). Once the ConneX PBXgateway confirms that Jane is an authorized user, it will call her mobile phone back to connect her to the PBX. The user is not prompted to press the PBX key to accept the call.
Security precautions prevent unauthorized access to the PBX system: Configure Jane's port to Fixed or Fixed/Forced modes.

Fixed/Forced

This mode requires the SA to program a permanent Dialback Number (DN) in the ConneX PBXgateway. In Fixed/Forced mode, you cannot modify the DN via the IVR system. This mode is the most secure of all four modes because it requires the ConneX PBXgateway to call the pre-assigned DN back to allow access to PBX dialtone and features. When you ENABLE your mobile phone in this dialback mode, all office-bound calls will be routed to that device for as long as it is turned on. Unanswered calls are routed to your office voicemail. In this mode, the ConneX PBXgateway will authenticate Jane via her port password (if assigned) and the DN (her mobile phone number). Once the ConneX PBXgateway confirms that Jane is an authorized user, it will call her mobile phone back to connect her to the PBX.

Disabled

This mode allows you to call into the central voice system (a.k.a. PBX) to get dialtone to place outgoing calls to anywhere in the world. In this mode, incoming calls are NOT routed to your mobile phone. While connected to the corporate PBX, you can transfer calls to another 4- or 5-digit internal extension or to an external number (if supported by your company's PBX); set up conference calls (up to 3 numbers); and place calls on hold as if you were using a digital phone set.

Operating Your Mobile Phone

After your organization's System Administrator configures the PBX and the ConneX PBXgateway to support your mobile phone, the System Administrator will provide you with a number to call in to ENABLE or DISABLE the ConneX application at your convenience. The same number is used to access PBX dialtone and features.

ENABLE the ConneX Application on Your Mobile Phone for the First Time

1. Call the number provided by the System Administrator to ENABLE the application on your mobile phone. You will hear "Welcome to ConneX." The message you will hear will depend on the mobile phone type being used. ADSI phone users will here "Welcome to RemoteConneX" non ADSI phone users will hear "Welcome to MobileConneX".

2. Press ## 0 (zero) to ENABLE the application. When you hear "Mobile/Remote ConneX enabled", you have completed the task.

Assign/Change Your Password

The user password is an optional feature of the ConneX application. However, we highly recommend that you assign a password to prevent unauthorized access to the corporate PBX. The SA may assign a password for you. You can change that password at anytime via the IVR system.

1. Call the number provided by the SA to access the corporate PBX.
2. Press ### to access the IVR system and follow prompts. NOTE: The password can be a combination of numbers and letters, up to 10 digits.

DISABLE/ RE-ENABLE the ConneX Application on Your Mobile Phone

1. Call the number provided by the SA to ENABLE the application on your mobile phone. You will hear "Welcome to Mobile/Remote ConneX" and be prompted to enter a password followed by the # key, if a password has been assigned. You may change your password at any time via the IVR system.
2. Press ## 0 (zero) to DISABLE the ConneX application. When you hear "ConneX disabled", you've completed the task. End the call.
3. To RE-ENABLE, call the same number provided by the SA to ENABLE the ConneX application.
4. Press ## 0 (zero) to ENABLE. When you hear "ConneX enabled", you've completed the task.
5. End the call.

Set/ Modify the Dialback Number (Roaming Mode ONLY)

1. Call the number provided by the SA to access the PBX.
2. You will hear "Welcome to Mobile/Remote ConneX" and be prompted to enter a password followed by the # key, if a password has been assigned. You may change your password at any time via the IVR system.
3. Press ### to access the IVR system to modify the Dialback Number (DN) and follow prompts. When entering the DN, add all prefixes required for the PBX to place an outbound call. For example, if you normally dial 9 1 + the phone number to reach someone outside of the organization, these prefixes must be entered in the DN. An asterix (*) can be used to enter a pause in a dialstring, if required.

Access corporate PBX dialtone (Roaming, Fixed and Disabled Modes)

1. Call the number provided by the SA to access the PBX.
2. You will hear "Welcome to Mobile/Remote ConneX" and be prompted to enter a password followed by the # key, if a password has been assigned. You may change your password at any time via the IVR system.
3. Press * * * to get a dialtone.
4. Dial the desired phone number. When placing calls through the PBX, remember to add all prefixes required for the PBX to place an outbound call (i.e. 9,1).
5. If you want to place multiple calls while connected to the PBX, hang up or release first call and press * * * to get dialtone to make the next call. You will hear dialtone again. You can place as many calls as needed. While connected to the PBX, you will be able to transfer your calls to another 4- or 5-digit internal extension or to an external number (if supported by your organization's PBX) by pressing ##T; set up conference calls by pressing ##C; and place calls on hold by pressing ##H as if you were using a digital phone set.
6. While on a call, a short tone will alert you of another incoming call. Press * * * to put the first call on hold and answer the second call. Press * * * to return to first call or switch between calls. See the ConneX Commands section starting on page 255, for the complete list of features supported.

Access PBX dialtone (Fixed/Forced Mode ONLY)

1. Call the number provided to you by the SA to access the PBX.
2. You will hear “Welcome to Remote/Mobile ConneX” and be prompted to enter a password followed by the # key, if a password has been setup. You may change your password at any time via the IVR system.
3. You will hear “Starting Dialback” and will be asked to disconnect.
4. End the call.
5. Your mobile phone will ring and you will be asked to press any key to accept the call. You are now connected to the central PBX.
6. Press *** to get PBX dialtone. When you hear dialtone, dial the desired phone number. When placing calls through the PBX, remember to add all prefixes required for the PBX to place an outbound call (i.e. 9,1).
7. If you want to place multiple calls while connected to the PBX, hang up or release first call and press * * * to get dialtone to make the next call. You will hear a dialtone again. You can place as many calls as needed. While connected to the PBX, you will be able to transfer your calls to another 4- or 5-digit internal extension or to an external number (if supported by your organization’s PBX) by pressing ##T; set up conference calls by pressing ##C; and place calls on hold by pressing ##H as if you were using a digital phone set.
8. While on a call, a short tone will alert you of another incoming call. Press * * * to put the first call on hold and answer the second call. Press * * * to return to first call or switch between calls. See ConneX Commands section on the following page for the complete list of features supported.

ConneX Mobile Application Commands - DEFINITY

The following table lists the DEFINITY MobileConneX application commands and corresponding actions:

Action	Commands
Off Hook (get PBX dialtone) *Note: this accesses the first unlit button. If not a line key, user must press **key*	Call the PBX → Press * * * → wait for dialtone
Hook Flash (to answer another call or switch between calls). A short tone will indicate another incoming call	Press * * * to answer second call → press *** again to return to first call
Access a specific feature/line key. These are pre-programmed for the user's extension on the PBX	Press * * key to access the feature. Use 1 for a, 2 for b, 3 for c, etc … use 0 for j
Put call on Hold	Press # # H → follow prompts to take call off hold.
Hang Up Call	Press # # O (letter)
Drop a call	Press # # D → you will hear dial tone after caller is released
Set up a conference call	Press # # C → hear dialtone → dial number to conference → press # # C to add attendee
Transfer a call	Press # # T → hear dialtone → dial extension → press # # T again to transfer call
Enable/Disable ConneX application[1]	Call the PBX → Press # # 0 (zero) → follow prompts
Access Interactive Voice Response (IVR) System[2]	Press # # # → follow prompts
Check Voicemail Status	Press # # 1→ follow prompts
Do Not Disturb (DND)	Press # # 9 when on an active call to enable DND (Do Not Disturb). If not on an active call use the DND softkey.
Reset the ConneX Session on the port.	Press # # 5→ follow prompts

Tip: Press the keys (i.e. ## T) at a consistent pace to envoke the PBX feature "transfer". The other party will hear the key presses.

[1] You control when incoming calls are directed to your mobile phone depending on your needs.

[2] You can use the IVR system to setup password and dialback number or test dialback number if mode is set to Roaming.

ConneX Mobile Application Commands - Meridian

The following table lists the Meridian MobileConneX application commands and corresponding actions:

Action	Commands
Off Hook (get PBX dialtone) *Note: this accesses the first unlit button. If not a line key, user must press **key*	Call the PBX → Press * * * → wait for dialtone
Hook Flash (to answer another call or switch between calls). A short tone will indicate another incoming call	Press * * * to answer second call → press *** again to return to first call
Access a specific feature/line key. These are pre-programmed for the user's extension on the PBX	Press * * key to access the feature. Use 1 for a, 2 for b, 3 for c, etc … use 0 for j
Put call on Hold	Press # # H → follow prompts to take call off hold.
Release Call	Press # # R → caller is released
Set up a conference call	Press # # C → hear dialtone → dial number to conference → press # # C to add attendee
Transfer a call	Press # # T → hear dialtone → dial extension → press # # T again to transfer call
Enable/Disable ConneX application[1]	Call the PBX → Press # # 0 (zero) → follow prompts
Access Interactive Voice Response (IVR) System[2]	Press # # # → follow prompts
Check Voicemail Status	Press # # 1→ follow prompts
Do Not Disturb (DND)	Press # # 9 when on an active call to enable DND (Do Not Disturb). If not on an active call use the DND softkey.
Reset the ConneX Session on the port.	Press # # 5→ follow prompts

Tip: Press the keys (i.e. ## T) at a consistent pace to evoke the PBX feature "transfer". The other party will hear the key presses.

[1] You control when incoming calls are directed to your mobile phone depending on your needs.

[2] You can use the IVR system to setup password and dialback number or test dialback number if mode is set to Roaming.

Labels with the ConneX mobile commands are shipped with each ConneX PBXgateway. Need more labels for free? Please, call 1-888-459-7979.

ConneX Mobile Application Commands - Norstar

When using a Norstar digital set, select Feature **808** to invoke "**Long Tones**" after logging into the IVR. This will enable the phone to see all other subsequent phone commands.

The following table lists the Norstar MobileConneX application commands and corresponding actions:

Action	**Commands**
Off Hook (get KSU dialtone) *Note: This accesses the first unlit button. If not a line key, user must press **key.*	Call the KSU → Press * * * → wait for dialtone
Hook Flash (to answer another call or switch between calls). A short tone will indicate another incoming call	Press * * * to answer second call → press *** again to return to first call
Access a specific feature/line key. These are pre-programmed for the user's extension on the PBX	Press * * key to access the feature. Use 1 for a, 2 for b, 3 for c, etc … use 0 for j
Put call on Hold	Press # # H → follow prompts to take call off hold.
Hang Up/Release Call	Press # # O → caller is released
Set up a conference call	Press # # H → hear dialtone → Press * * key number for next line→ hear dialtone → dial DN of attendee → press # # C to add attendee.
Transfer a call	Press # # T → hear dialtone → dial extension → press # # O again to transfer call
Enable/Disable ConneX application [1]	Call the KSU → Press # # 0 (zero) → follow prompts
Access Interactive Voice Response (IVR) System [2]	Press # # # → follow prompts
Check Voicemail Status	Press # # 1→ follow prompts
Do Not Disturb (DND)	Press # # 9 when on an active call to enable DND (Do Not Disturb). If not on an active call use the DND softkey.
Reset the ConneX Session on the port.	Press # # 5→ follow prompts

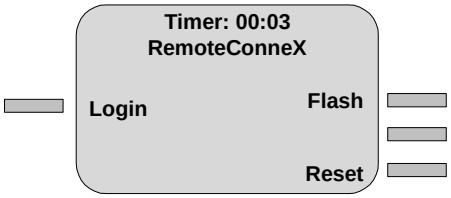
[1] You control when incoming calls are directed to your mobile phone depending on your needs.
[2] You can use the IVR system to setup password and dialback number or test dialback number if mode is set to Roaming.

Getting Started on a RemoteConneX Phone

Congratulations on your purchase of the RemoteConneX™ Phone. This Quick Reference Guide will assist you when using the office functionality of your phone.
***Important**: In order to use the RemoteConneX Phone, you must perform the first use setup procedure outlined in the RemoteConneX Phone User Guide!*

The login Procedure

1. Raise the handset, or press the Speaker key. The following menu will appear:



2. Press the Login Softkey.
3. When prompted to enter your password, enter the password and press the OK softkey. If you do not know your password, refer to the 'Personal RemoteConneX Info' section or contact your System Administrator. A password is optional but highly recommended.
4. You are now logged into the system and should be able to see the PBX: Idle Menu.

There are two methods to use your phone for office functionality:

- Logging in and staying connected at all times.
- Not logging in and using Dialback functionality to make/ receive office calls.

Dialback Instructions

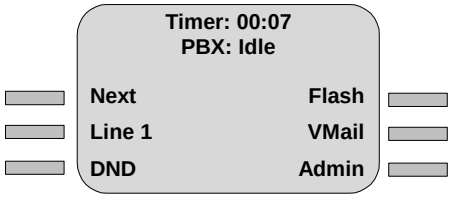
The Dialback number is the telephone number that the ConneX PBXgateway uses to reach you at your home location. Incoming calls to your office extension are routed to the Dialback number currently set. Refer to the 'Personal RemoteConneX Info' section to find out if you need to set your own Dialback number.

Dialback Setup Instructions

1. From the *PBX: Idle* menu, press the Admin softkey.
2. Press the ***SetDB*** softkey.
3. Enter your 10-digit phone number as if you were sitting at your office attempting to call home. Include any prefix numbers such as '9' or '1' (i.e 9-1-xxx-xxx-xxxx) when setting the number.
4. Press the ***Enter*** softkey to store.
5. Press the ***CheckDB*** softkey to replay.

Feature Softkeys

Once logged into the system, the following menu will appear:



Next LN	Cycles through the pool of available lines to answer/retrieve office calls.
Line 1	Selects the first line appearance for use.
DND	Disables Incoming Call notification. If on an active call (DND softkey not available) press ##9. This feature will be retained for the entire connect session; there would be no indication on the phone.
Flash	Performs a hook flash with home phone line. See the 'Answering an Incoming Home Call.' section for more info.
VMail	Allows access to the following voice mail features:
VMLogin	Initiate a login to the corporate voicemail system.
VMStat	Relays audible status of your voice maibox - "You've got voicemail!"
Admin	Allows access to the following administrative features:
Dialback	Dials the dialback number currently set. Press **PBX** softkey to answer call.
SetDB	Set the Dialback number.
Check DB	Replays the current Dialback number.
Passwd	Sets the password.
On/Off	Enable/Disable dialback.

Making and Answering a Call

Placing an Office Call

1. Press the ***Line 1*** or ***Next LN*** softkeys to draw a dialtone. You will enter the PBX: Active Call menu.
2. Dial the phone number of the desired party. Remember that this IS your office phone so you must dial any pre-fixes needed to make a call from your office (i.e '9').

Ending an Office Call

1. Press the ***HangUp*** softkey.
2. If using the handset, press the Speaker key before hanging up the handset to keep your RemoteConneX session active. You will return to the *PBX: Idle* menu.

Answering an Incoming Office Call...

...At the PBX: Idle Menu

1. You will hear a voice prompt indicating an incoming call.
2. Press the ***Next LN*** softkey to answer the call.

...At the PBX: Active Call Menu

1. Your will hear a stutter tone.
2. Press the ***Next LN*** softkey to answer the incoming call. Your current call will be placed on hold.
3. When completed, press the ***Next LN*** softkey again to retrieve the call that was placed on hold.

Answering an Incoming Home Call...

(Call Waiting must be enabled on this home line)

...At the PBX: Idle Menu

1. You will hear a standard call waiting tone.
2. Press the ***Flash*** softkey to answer the call.
3. When completed, press the ***Flash*** softkey again to return to *PBX: Idle* menu.

...At the PBX: Active Call Menu

1. You will hear a standard call waiting tone.
2. Press the ***Flash*** softkey to answer the incoming call. Your current office call will be placed on hold.
3. When completed, press the ***Flash*** softkey again to return to the *PBX: Idle* menu.
4. Press the ***Next LN*** softkey to retrieve the office call that was placed on hold.

Using Active Call Commands – Remote ConneX

Conference (Conf)

1. Press the ***Conf*** softkey.
2. Dial the extension of the party.
3. Press the ***Conf*** softkey.
4. Return to Step 1 to add other parties as needed.

(Norstar) Conference (Conf)

1. Press the ***Conf*** softkey.
2. Press ***Next LN*** to access another line.
3. Dial the extension of the party.
4. Press the ***Conf*** softkey.
5. Return to Step 1 to add other parties as needed.

Transfer (Xfer)

1. Press the ***Xfer*** softkey.
2. Dial the extension of the party.
3. Press the ***Xfer*** softkey to complete the transfer.

(Norstar) Transfer (Xfer)

1. While on an active call, press the ***Xfer*** softkey.
2. Dial the extension of the party.
3. Press the ***Hang up*** softkey (Rel Key can also be used). Your transfer is complete and your initial login screen will be displayed. If you are using **Norstar PBX**, pressing the ***Xfer*** softkey will disconnect the call.

Hold

1. Press the **Hold** softkey to place an active call on hold.
2. To retrieve the “on hold” call, press the **Next LN** softkey (to cycle through the available lines).
3. To place another call while the first call is on hold press ***Line 1***.

Drop a Call (Drop) (Used with DEFINITY™ ONLY)

“Drops” the current call but does not hang up the line;
“Drops” the last person joined to a conference call.

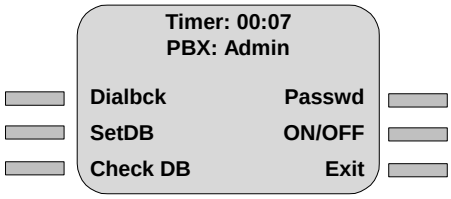
1. Press the ***Drop*** softkey.

Hang Up (HangUp)

Hangs up the active call, but keeps the RemoteConneX session active. This softkey will also act like the "Release" key of a Nortel Meridian phoneset.

1. Press the ***HangUp*** softkey
2. If using the handset, press the **Speaker** key freeing up the handset.

PBX:Admin Menu

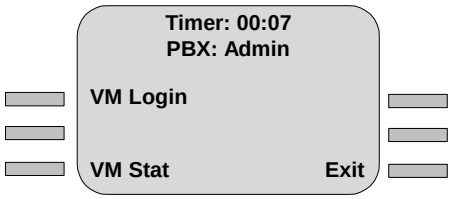


Dialback

1. Press the ***Dialbck*** softkey. This confirms dialback number has been set.
2. Press ***SetDB.*** Enables dialback.
3. Press ***Check DB.*** Recites the entered DB number.

PBX:Voice Mail Menu

This menu is displayed during the phoneset ConneX software download, when the Voicemail password screen is skipped.



Voice Mail

1. Press the ***VM Login*** softkey. You will be prompted to enter a password.
2. Press ***VM Stats.*** Old and New messages are displayed.

Using Active Call Commands – Mobile ConneX

Conference (Conf)

1. Press # # C to place existing call on hold.
2. Press * * * for next line.
3. Dial new DN.
4. press # # C to add attendee

(Norstar) Conference (Conf)

1. Press ##H to place existing call on hold.
2. Press * *Key Num (## followed by any key number) for next line.
3. Dial new DN.
5. When the new call is active, press # # C.

Transfer (Xfer)

1. Press the # # T when on an existing call.
2. At dialtone dial new DN.
3. Press # # T to transfer call.

(Norstar) Transfer (Xfer)

1. Press the # # T when on an existing call.
2. At dialtone dial new DN.
3. Press # # O to transfer call.

Hold

1. Press # # H to place an active call on hold.
2. Follow prompt to take call off Hold (* *key Num)
3. To retrieve the call on Hold press ##1.
1. To place another call while the first call is on hold, press ## Key Num (## followed by any key number) to access another line and place your call.
2. To retrieve the first call you put on hold while you make the second call press ##1.

(Norstar) Hold

1. Press # # H to place an active call on hold.
2. Follow prompt to take call off Hold (* *key Num)

Drop a Call (Drop) (Used with DEFINITY™ ONLY)

"Drops" the current call but does not hang up the line;
"Drops" the last person joined to a conference call.
1. Press the ***Drop*** softkey.

Hang Up (HangUp)

Hangs up the active call, but keeps the MobileConneX session active. This softkey will also act like the "Release" key of a Nortel Meridian phoneset.
1. Meridian ##R or Release Key
2. Definity - ##O

Dialback

1. Press ### to access the IVR and follow the prompts. If you wish to verify your Dialback Number select option 4.

Appendix G: PBX/KSU ConneX Configuration

The following KSU/PBX configurations enable basic ConneX functionality on the PBXgateway.

Two basic configurations are described:

- a standard ConneX configuration with no digital sets and one remote client,
- a Bridged or Ghost configuration where the ConneX client acts as a ghost set receiving calls targeted to an actual desk set (either extended from a Remote Extender or directly connected to the KSU).

Norstar KSU ConneX Configuration

This section illustrates two variations of Norstar KSU settings to enable ConneX functionality on the PBXgateway for the two basic ConneX configurations;

1. Line Assignment Method - ConneX configuration with no digital set and one remote client,
2. ConneX Session Port - Bridged or Ghost configuration where the ConneX client acts as a ghost set receiving calls targeted to an actual desk set (either extended from a Remote Extender or directly connected to the KSU).

Notes:

- The configurations assume that proper call routing has been configured in the KSU, and the PBXgateway has been properly programmed for ConneX.
- Consult the appropriate Norstar documentation for setting locations and variations to the settings listed below (may change depending on KSU).
- Caller ID settings are not included. See the appropriate Norstar documentation for the proper Caller ID settings available on the system the PBXgateway unit is to be connected to.

Voice Mail

If Voice Mail is to be used then the appropriate Norstar Voice Mail setup is required on the desired port. If configuring without a desk set then the mailbox will be programmed for the ConneX_Session port, if a bridged configuration, then all Voice Mail settings as well as the mailbox will be programmed on the digital desk set. See the appropriate Norstar Voice Mail documentation for configuration.

It should be noted that a delay of 1 to 2 rings occurs when the KSU indicates ringing and the remote set starts ringing. This requires the Ring Count setting in the Gateway to be at least one greater then the number of rings set in the KSU before the call is forwarded to Voice Mail. Third party Voice Mail (Cellular company, etc.) forward settings should be at least one ring greater then the Norstar settings to prevent ConneX messages from being forwarded to the third party system

KSU Configuration – Line Assignment Method

Link Port

The Link Port is restricted to one Intercom Key assignment and no line appearances to ensure correct operation. If the user is required to login via the link from an external set either Direct Ring Transfer of a Target Line to the port should be used. The link can also be reached externally via a call to the Company Directory if an Automated Attendant is configured. The user can login internally via the port DN at any time.

Terminals and Sets

1. Enable *Line Pool Access* for outbound dialing (PRI or Pool).
2. Set *Prime Line* to **I/C**, with a minimum or 1 I/Cs assigned.
3. Set *Answer DN* to **None**.
4. Set *Foreward on No Answer* and *Forward on Busy* to **None**.
5. Set *Do Not Disturb on Busy* to **N**.
6. Set *Handsfree* to **None**.
7. Set *Allow Redirect* to **Y** and *Redirect Ring* to **Y**.

Lines

Settings here are used for inbound external calling to login to the IVR utilizing calls with KSU functionality or set administration. The line type will be dictated by the lines/trunks connected to the KSU. The following example is for a PRI trunk connected to card PRI-A in the KSU.

The following example is for a PRI trunk connected to card PRI-A in the KSU.

1. Under the *Target Line* assigned in *Terminals and Sets*, set the line to **Public**.
2. Set *Received Number/Digits* to a number in the range included in the PRI trunk.
3. Set *If Busy to Prime* and *Prime Set* to the **DN** of the set configured in Terminals and Sets. Ensure that you enter a unique DN for each ConneX user. Duplicating this number will cause problems when two or more users assigned the same DN attempt to login to ConneX simultaneously.
4. In System Programming set **DRT to Prime** to Y (system-wide setting).

KSU Configuration - ConneX_Session Port

When configuring the ConneX_Session port for inbound external calling note that if line assignments are used the ConneX Line Keys assigned in the Gateway MI will be 0, 1, 2, and 7 (where 0,1 and 2 correspond to a setting of 3 IC keys and 7 corresponds to the assigned line as the port will default to a M7208 set). If DRT to Prime is used then the ConneX Line Keys will be 0, 1 and 2 (corresponds to a setting of 3 IC keys). As with the Link, an Auto-Attendant may also be used to reach the ConneX_Session from an external caller if no outside lines are available for individual ports.

Stand Alone Configuration – No Desk Set (Bridged Appearance)

The following configuration has no digital sets attached to the ConneX_Session port, although a digital set may be connected to a Extender 6000 corresponding to the ConneX_Session port (i.e. if port 1 on the Gateway is the ConneX_Session then a digital set may be extended on port 1 of the Extender 6000). If the digital set is extended, calls will not be forwarded to the remote user but will ring at the digital set instead. It is recommended that a M7208 digital set be used in this situation to avoid possible set recognition issues when ConneX is re-enabled.

Consult the appropriate Norstar documentation for setting locations and variations to the settings listed below. Note, that settings may vary with different KSUs.

In this configuration **only** the Remote phone will ring.

Terminals and Sets

1. Assign a *Target* line to **Appear** and **Ring**, one appearance. Line Appearance method only.
2. Enable *Line Pool Access* for outbound dialing.
3. Set *Prime Line to I/C*, with a minimum or 3 I/Cs assigned.
4. Set *Answer DN* to **None**.
5. Set *Foreward on No Answer* and *Forward on Busy* to **None** or to the appropriate System Voice Mail DN if applicable (mailbox creation required).
6. Set **Do Not Disturb on Busy** to *N.*
7. Set *Handsfree* to **None** (allows for calls on Line 1 - **1, etc.).
8. Set Allow Redirect to **Y** and Redirect Ring to **Y**.

Lines

1. Under the *Target Line assigned in Terminals and Sets*, set the line to **Public**.
2. Set *Received Number/Digits* to a number in the range included in the PRI trunk.
3. Set *If Busy* to **Prime** and *Prime Set* to the **DN** of the set configured in Terminals and Sets. Ensure that you enter a unique DN for each ConneX user. Duplicating this number will cause problems when two or more users, assigned the same DN, attempt to login simultaneously.
4. In System Programming set **DRT to Prime** to Y (system-wide setting – if this setting was performed when setting up the Link then no action is required here).

Bridged Appearance– Remote Set Bridged to Desk Set

The incoming call will ring at both the desk set and at the remote set. The call will be dropped at the unanswered set when answered at the other set.

The desk set that is bridged to the ConneX_Session port is configured as a normal set with no special programming required. The Answer DN setting in the ConneX_Session programming handles the call process for the bridge from the desk set. Voice mail should be configured on the desk set in this situation, as per Norstar documentation.

Terminals and Sets

1. Enable *Line Pool Access* for outbound dialing.
2. Set *Prime Line* to **I/C**, with a minimum or 3 I/Cs assigned.
3. Set *Answer DN* to the DN of the appropriate desk set.
4. Set *Foreward on No Answer* and *Forward on Busy* to **None**.
5. Set *Do Not Disturb on Busy* to **N**.
6. Set *Handsfree* to **None** (allows for calls on Line 1 - **1, etc.).
7. Set *Allow Redirect* to **Y** and *Redirect Ring* to **Y**.

Lines

No settings specifically related to ConneX.

Definity PBX ConneX Configuration

The instructions below are applicable for the configuration of Avaya's DEFINITY ECS running release 3 or higher:

SCENARIO #1: Office Phone Used in Conjunction with the ConneX Phone

There is only one change required on the user's office extension when he/she wishes to use the ConneX phone as a complementary business tool. The number of rings should be increased to six (06) before going into voicemail. This is required to allow enough time for the gateway to call the ConneX phone.

***Note**: No wiring changes are required on this extension.*
***Note**: This extension MUST be capable of DID.*

1. Perform a **change station** to modify the **Coverage Path** of the user's office extension to allow it to ring 6 times before going into voicemail. **Tech Tip:** Create a new **Coverage Path** in the DEFINITY to accommodate this "class" of users.
2. Hit the **Enter** key on the number pad (far right of keyboard) to save the change made to this extension.

Provisioning a New Extension for the ConneX Phone

1. Provision a new extension for the ConneX phone (Ch1) on the DEFINITY. Wire this extension into the ConneX PBXgateway on an available port. ***Note**: This extension does NOT require DID capability*.
2. Go to Page 1 of the Definity terminal session to configure the CH1 extension.
3. Change **Type** to a DEFINITY phone set that supports the "analog adjunct" feature. We recommend phone set *8411D*, however other phones like the *6416D+* and *6424D+* also support the analog adjunct feature. Notice the **Data Option** field appears in the middle of the screen when this change is made. **Tech Tip**: It is NOT necessary for the phone type to match the type used at the office extension, since only the first ten (10) line/feature buttons are accessible from a mobile phone.
4. Complete the **Name** field. Be sure to give this extension a clear name (i.e. ConneX Port 1).
5. Change **Data Option** to *analog* (notice the page number increases by 1 when this change is made).
6. Change the **Message Lamp Ext** to the user's office extension.
7. Go to Page 2 and set **Bridged Call Alerting** to Y.
8. Go to Page 3 of the DEFINITY terminal session for this extension (Ch1).
9. On Page 3: Change **all** *call-appr* assigned buttons to *brdg-appr* → Btn: *assignment #* → Ext: *Office Extension.*

   Note: Program keys 0-9 on this extension to match the office phone's keys 0-9. This is required to make the features accessible from the mobile phone.

10 Go to last page (note: last page number may vary depending on phone model). Heading should read *Analog Adjunct*.
11. On last page: Assign the **Data Extension** a new or unused extension (Ch2) on the DEFINITY. **This extension MUST be capable of DID**. This is the extension number that the ConneX users will call to access the RCX (DID of the Ch2). Ensure you use a different DID for each user as only one person per DID can login. This will either be a DID extension, or accessible through a transfer from a main number (i.e. Intuity, Vector, IVR,etc.).
12. Type in the extension **Name.** Give this extension a descriptive name so it is clear what it is being used for (i.e. Username B2 - Mobile #1).
13. Hit the **Enter** key on the number pad (far right of keyboard) to save all changes made to extension Ch1 and its now corresponding extension Ch2.

14. Perform a **display station** on extension Ch1 to certify that all changes have been saved. Ensure that *all* appearances are bridged to the office extension and that an Analog Adjunct to extension Ch2 exists.
15. Done. The DEFINITY PBX is now configured to support **one** user.

SCENARIO #2: Only ConneX Phone Is Used

Provisioning a new extension for the ConneX Phone.

1. Provision an extension for the ConneX phone (Ch1) on the DEFINITY. Wire this extension into the RemoteConneX PBXgateway on an available port.
2. Go to Page 1 of the DEFINITY terminal session to configure the Ch1 extension.
3. Change **Type** to a DEFINITY phone set that supports the "analog adjunct" feature. We recommend phone set *8411D*, however other phone types like the *6416D+* and *6424D+* also support the analog adjunct feature. Notice the **Data Option** field appears in the middle of the screen when this change is made.
4. Enter the **Name** field. Be sure to give this extension a clear name (i.e. ConneX – Port 1).
5. Change **Data Option** to *analog*. Notice the page number increases by 1 when this change is made.
6. Go to last page (***Note****: last page number may vary depending on phone model).* Heading should read Analog Adjunct.
7. On last page: Assign the **Data Extension** a new or unused extension (Ch2) on the DEFINITY. This is the extension number that the ConneX users will call to access RCX. Assign a different DID for each user. Assigning the same DID for more then one user will create problems if two people, with the same DID try to access the RCX IVR simultaneously. This will be either a DID extension, or accessible through a transfer from a main number (i.e. Intuity, Vector, IVR,etc.).
8. Type in the extension **Name**. Give this extension a descriptive name so it is clear what it is being used for (i.e. Username B2 - Mobile #1).
9. Set the **call-appr** field to **Y**.
10. Perform a **display station** on Ch1 extension to verify that all changes have been saved. And ensure that an Analog Adjunct to the corresponding Ch2 extension exists.
11. Done. The DEFINITY PBX is now configured to support **one** user.

Meridian PBX ConneX Configuration

These instructions are applicable for the configuration of Nortel's Meridian PBX running release 22 or higher:

SCENARIO #1: Office Phone Used in Conjunction with the ConneX Phone

There is only one change required on the user's office Terminal Number (TN) when he/she wishes to use the ConneX phone as a complementary business tool. The number of rings should be increased to six (06) before going into voicemail. This is required to allow enough time for the gateway to call the mobile phone.
Note*: No wiring changes are required on this TN.*

1. On the Meridian maintenance terminal, go to **>LD 15** (a.k.a. overlay) to change the (Call Redirection) **RDR_DATA** field to *YES* and set (Call Forward No Answer) **CFN2** to *6* rings.
2. Go to **>LD 11** to CHG (Change) the (Ringing Cycle Option for Call Forward No Answer) **ITEM RCO** to *2 (for example RCO 2= the phone will ring six times before going into voicemail)*. **Tech Tip**: Create a new RCO profile for mobile users. Six rings are recommended for this new profile.
3. On **>LD 11**, program a Ringing Pickup Group (**RNPG**) value for this TN when prompted.

4. Set the Class of Service to Call Forward No Answer allowed (FNA) **ITEM CLS** to FNA.
5. Done. The office TN is configured to ring 6 times before going into voicemail.

Provisioning the Primary Voice Channel of the Mobile Phone's TN – Ch1

1. Provision a new TN for the remote phone on the Meridian. Wire this TN into the RemoteConneX PBXgateway on an available port. ***Note****: This port does NOT require DID capability.*

   Tech Tip: Nortel's Reach Line cards do no support the secondary channel required for the RemoteConneX application.

2. On the Meridian maintenance terminal, use **>LD 11** (a.k.a. overlay) to configure this TN to the same Directory Number (DN) assigned to the user's office phone.
3. Select a phone **TYPE** that supports Analog Terminal Adapter (ATA) functionality. We recommend phone type M2616, however other Meridian phone sets that also support the ATA functionality are: M2006, M2008, M2016, M2216 and M2617. Configure the selected phone with the same class of service as the user's office TN. **Tech Tip**: It is NOT necessary for the phone type to match the type used at the office TN, since only the first ten (10) line/feature buttons are accessible from a mobile phone.

   WARNING*: Do not configure a key as Message Waiting Key (MWK) for this TN to prevent interference with voicemail and call routing functions.*

4. On **>LD 11**, program this TN with the same **RNPG** value as the office TN when prompted.
5. Program **KEY 00 to 9** to match the line keys of the office TN so that all inbound calls will ring at the office and at the remote phones at the same time.
6. This TN must have a ***CLS of FLX*****D, CPT****A, VCE, WTA.**
7. Program any of the first 10 keys to allow A06 (Conference) & TRN (Transfer). Remember these settings when programming the RemoteConneX PBXgateway.

Provisioning the Secondary Data Channel of the Mobile Phone's TN – Ch2

1. On the Meridian maintenance terminal, use the **>LD 11** to add Analog Terminal Adapter (ATA) functionality to this TN. Refer to the *Meridian 1* documentation for more details on programming an ATA. Although no ATA adapter is used for the RemoteConneX application, the programming required for the ATA applies to the remote phone's TN configuration. The ATA functionality must be added to this TN. **Tech Tip**: Nortel's Reach Line cards do no support the secondary channel required for the MobileConneX application.
2. This TN must have a ***CLS of FLX*****A, CPTD, VCE, WTA. Tech Tip**: If Ch1 is "TN 3 0 5 0" (loop 3, shelf 0, card 5, unit 0), then Ch2 would be "TN 3 0 5 16".
3. Program **KEY 00** as Single Call Ringing SCR yyyy. The "yyyy" field should contain the Directory Number (DN). The SCR appearance MUST be DID capable to allow the mobile user to dial the Directory Number to access the corporate PBX.
6. Done. The Meridian 1 PBX is now configured to support **one** user.

SCENARIO #2: Only Mobile Phone Is Used

Provisioning the Primary Voice Channel of the Mobile Phone's TN – Ch1

1. Provision a TN for the remote phone on the Meridian 1. Wire this TN into the MobileConneX PBXgateway on an available port. ***Note****: This port must be DID capable*. **Tech Tip**: Nortel's Reach Line cards do no support the secondary channel required for the MobileConneX application.
2. On the Meridian maintenance terminal, use **>LD 11 (i.e. overlay)** to configure this TN.

3. Select a phone **TYPE** that supports Analog Terminal Adapter (ATA) functionality. We recommend phone type M2616, however other Meridian phone sets that support the ATA functionality are: M2006, M2008, M2016, M2216, and M2617. Configure the selected phone according to the company's standard class of service.
4. Program **KEY 00** as SCR (Single Call Ringing). This TN must have a ***CLS of FLX*D, CPTA, VCE, WTA.**
5. Assign a voicemail box for this TN.

   WARNING: Do not configure a key as Message Waiting Key (MWK) for this TN to prevent interference with voicemail and call routing functions.

6. Program any of the first 10 keys to allow A06 (Conference) & TRN (Transfer). Remember these settings when programming the RemoteConneX PBXgateway.

Provisioning the Secondary Data Channel of the Mobile Phone's TN – Ch2

1. On the Meridian maintenance terminal, use the **>LD 11** to add Analog Terminal Adapter (ATA) functionality to this TN. Refer to *Meridian 1* documentation for more details on programming an ATA. Although no ATA adapter is used for the RemoteConneX application, the programming required for the ATA device applies to the mobile phone's TN configuration. The ATA functionality must be added to the Ch2 channel. **Tech Tip**: Nortel's Reach Line cards do no support the secondary channel required for the MobileConneX application.
2. This TN must have a ***CLS of FLX*A, CPTD, VCE, WTA**. **Tech Tip***:* If Ch1 is "TN 3 0 5 0" (loop 3, shelf 0, card 5, unit 0), then Ch2 would be "TN 3 0 5 16".
3. Program **KEY 00** as Single Call Ringing SCR yyyy. The "yyyy" field should contain the Directory Number (DN). The SCR appearance MUST be DID capable to allow the mobile user to dial the Directory Number to access the corporate PBX.
4. Done. The Meridian 1 PBX is now configured to support **one** user.

Example for Scenario #1 – Programming the Primary Voice Channel (Ch1)

```
TN      002     0       00      13
DATE
PAGE
DES     VAL
TN      002     0       00      09
TYPE    2616
CDEN    8D
CUST    0
AOM     0
FDN     Enter voicemail box number (optional)
TGAR    1
LDN     NO
NCOS    0
SGRP    0
RNPG    0
SCI     0
SSU
XLST
CLS     CTD     FBD     WTA     LPR     MTD     FND     HTD     ADD     HFD
        MWA     LMPN    RMMD    SMWD    AAD     IMD     XHD     IRD     NID     OLD     VCE     DRG1
        POD     DSX     VMD     CMSD    CCSD    SWD     LND     CNDD
        CFTD    SFD     MRD     DDV     CNID    CDCA    MSID    DAPA    BFED    RCBD
        ICDD    CDMD    MCTD    CLBD    AUTU
        GPUD    DPUD    DNDD    CFXD    ARHD    CLTD    ASCD
        CPFA    CPTA    ABDD    CFHD    FICD    NAID    BUZZ    AHD
        DDGA    NAMA
        DRDD    EXR0
        USRD    ULAD    RTDD    RBDD    RBHD    OCBD    FLXD    FTTC
CPND_LANG       ENG
HUNT    Enter voicemail box number (optional)
LHK     0

PLEV    02

AST
IAPG    0
AACS    NO
ITNA    NO
DGRP
MLWU_LANG       0
DNDR    0
KEY     00      SCR     2009    0
        01
        02      TRN     (Transfer)
        03      AO6     (Conference)
        04
        05
```

Message Waiting Allowed (**MWA**) is required.

The required Class of Service is **bold**.

Directory Number (DN) for office and remote phones must be the same

Does not have to be specific keys. However, the keys utilized for Transfer and Conference must be entered in the RemoteConneX PBXgateway.

Figure 100: Programming the Primary Voice Channel (CH1)

Example for Scenario #1 – Programming the Secondary Data Channel (Ch2)

```
TYPE:   TYPE    2616
TN      002     0       00      29
DATE
PAGE
DES     B2
TN      002     0       00      25
TYPE    2616
CDEN    8D
CUST    0
AOM     0
FDN
TGAR    1
LDN     NO
NCOS    0
SGRP    0
RNPG    0
SCI     0
SSU
XLST
CLS     CTD     FBD     WTA     LPR     MTD     FND     HTD     ADD     HFD
        MWD     LMPN    RMMD    SMWD    AAD     IMD     XHD     IRD     NID     OLD     VCE     DRG1
        POD     DSX     VMD     CMSD    CCSD    SWD     LND     CNDD
        CFTD    SFD     MRD     DDV     CNID    CDCA    MSID    DAPA    BFED    RCBD
        ICDD    CDMD    MCTD    CLBD    AUTU
        GPUD    DPUD    DNDD    CFXD    ARHD    CLTD    ASCD
        CPFA    CPTD    ABDD    CFHD    FICD    NAID    BUZZ    AHD
        DDGA    NAMA
        DRDD    EXR0
        USRD    ULAD    RTDD    RBDD    RBHD    OCBD    FLXA    FTTC
        CPND_LANG       ENG
HUNT
PLEV    02
AST
IAPG    0
AACS    NO
ITNA    NO
DGRP
MLWU_LANG       0
DNDR    0
DTMK
KEY     00      SCR     4726    0       MARP
        01
        02
        03
```

The required Classes of Service are **bolded**. The new CLS options should be entered in REVERSE order (i.e. VCE and WTA).

A DID number (i.e. 270-4726) can be used when calling into the CH2 directly. Another way to reach the Ch2 is by calling the main toll-free number, if available, and dialing the specific extension for the Ch2 (i.e. 4726)

Figure 101: Programming the Secondary Data Channel (CH2) Example

***Note**: Both of these examples also apply for Scenario#2 as well.*

Index