



Operations Manual

VoiceWise™ Universal Integrated Device (UAD)



VoiceWise™ Universal Access Device (UAD)

VOICE OVER IP TECHNOLOGIES

EdgeAccess, Inc.
Tampa, Florida 33634
Customer Support: support@edgeaccess.net

Table of Contents

Introduction	4
Chapter 1 – Quick Start	
Install UAD	9
Connecting Devices	16
Check Connections	16
Chapter 2 – Management Options	
Setup Manager	17
Web-Based Manager	17
Chapter 3 – Set Up Manager	
Setup Manager	18
Setup Menu	19
Hostname	20
WAN Menu	20
WAN DHCP Menu	22
WAN T1 Configuration Menu	24
LAN Menu	33
LAN DHCP Menu	33
Static Routes	33
Firewall Menu	34
Traffic Control	35
Miscellaneous Menu	37
Utilities Menu	38
MS VPN Client Menu	39
Update Menu	40
IPSecurity	42
OSPF	46
BGP	47
Chapter 4 – Web-Based Manager	
Web-Based Manager	47
Network Configuration	49
Telephony Configuration	55
Security Configuration	62
Services Configuration	64
Index	69

Introduction

This guide provides users with operational procedures, which will be used when working with the EdgeAccess VoiceWise™ UAD.

- **Chapter 1** provides a Quick Start to the UAD and also covers some basic system concepts.
- **Chapter 2** provides an overview of both the Configuration Management Utilities.
- **Chapter 3** covers the UAD's Setup Configuration Manager.
- **Chapter 4** covers the UAD's Web-Based Configuration Manager.
- An **Index** is provided at the end of the document.

Audience

This guide is written for the installation and maintenance technician and other Telecommunications' professionals working with the EdgeAccess VoiceWise™ UAD equipment.

Technical Support

For complete technical support information, check our Web site at www.edgeaccess.com or call (301) 547-7010.

Overview

The EdgeAccess VoiceWise™ UAD is a broadband integrated access device for the customer premise that supports up to 4 analog phone lines, Ethernet connectivity to a local LAN, and a variety of Wide Area Network (WAN) interfaces. EdgeAccess UAD key features are PBX/Centrex functionality and Web-based instant service provisioning. In addition, EdgeAccess UAD offers several optional capabilities such as: Router, Firewall, RSVP, IPSec, DHCP and NAT (Network Address Translation). These router capabilities enable service providers to have multiple computers routing traffic to a single UAD while still being able to manage outside access to each computer utilizing one network address. Designed as customer premise equipment, the EdgeAccess UAD offers the most efficient means of voice communications by converting voice to IP at the edge of the network. Service providers will receive an "ideal" network (IP), which drastically reduces costs, space, personnel, and network management. To further enhance UAD applications and flexibility, FXO trunks provision to provide OPX circuits to customers creating a seamless migration path from circuit switching to packet switching. The IP backbone can be either public or private as UADs have several mechanisms to compensate for jitter, latency, packet loss and bandwidth utilization.

System Specifications:

Inbound Interfaces

8 FXO, 8 FXS Ports Each physical connector supports both one FXS and one FXO line interfaces Meets LSSGR and CCITT Requirements for Telephone Interface 10/100 Base T Ethernet

Outbound Interfaces

- Single T1/E1 Data
- 10/100 Base T Ethernet
- xDSL
- Wireless
- Cable
- Dial-Up

VoIP Protocols

- VSP (Virtual Switch Protocol)
- SIP* (Session Initiation Protocol)

Call Control Protocols

- TOS bit

Compression Methods

- G.729 CS - ACELP codec @ 8 kbps
- G.723.1 MP-MLQ codec @ either 5.3 or 6.3 kbps
- G.726 / G.727
- ADPCM and E-ADPCM codecs
- G.711 PCM

Enhanced Capabilities

- Router
- DHCP
- Firewall
- NAT (Network Address Translation)
- RSVP
- IPSec

Other

Group 3 fax Automatic fax/voice switching Voice Activity Detector Comfort Noise Generator TIA 464A DTMF detection and generation Call Progress Detection

*Also available in other EdgeAccess products.

CLASS Features

The EdgeAccess UAD currently supports the following CLASS features.

Caller ID

Displays the ANI (Automatic Number Information) of the incoming call.

Call Waiting

Alerts caller to second incoming call while on the phone and allows you to switch between to two callers.

Call Forwarding

Allows an incoming call to be sent to an alternate phone number. Select from: All, On Busy and On Ring No Answer.

Authorization Codes

When Account Verification is enabled on the SoftSwitch, the UAD will prompt user to enter the 2-12 digit Authorization Code prior to call setup.

Call Restriction

Allows any caller to restrict any incoming or outgoing call on a dial plan basis.

Call Barring

Restricts the type of call that may be placed from a telephone line (1+ dialing or dial around).

Network Features:

SIP Proxy

The SIP Proxy module enables service providers to build scalable, reliable Voice over IP networks. Based on the Session Initiation Protocol (SIP), the SIP Proxy provides a full array of call routing capabilities to maximize network performance in both small and large packet voice networks to include “hairpin” routing for use during a WAN network outage.

MPLS VLAN Tagging

S-VLAN tunnels can be created as an efficient way to configure Ethernet layer 2 services over MPLS. An S-VLAN tunnel is a special type of S-VLAN that tunnels traffic from multiple VLANs across an MPLS network. The S-VLAN tunnel enables multiple VLANs, each configured with a unique VLAN ID, to share a common S-VLAN ID when they traverse an MPLS network.

The only interface that you can stack over an S-VLAN tunnel is an MPLS tunnel. Attempting to configure any other interface type over the S-VLAN tunnel will cause an error.

SNMP

The *Simple Network Management Protocol* (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between network devices. By using SNMP-transported data (such as packets per second and network error rates), network administrators can

more easily manage network performance, find and solve network problems, and plan for network growth.

802.11G Wireless AP

The 802.11g Wireless Network Access Point module connects to your network switch and lets you join your wireless-equipped PCs to your wired network. It is based on 802.11g wireless technology that transfers files and downloads at a high speed. When connected to a gateway, the device can increase your network's coverage area and allow you to take advantage of expanded wireless roaming capabilities. Featuring a simple setup, the Access Point allows you to share data and peripherals, as well as a single Internet account among all your computers. The Access Point uses the wireless 802.11g 2.4 GHz standard to offer you a working range up to 1800 ft and interoperability in mixed networking environments. The 802.11g technology is also backward-compatible with the 802.11b Wi-Fi networking standard. An added Turbo Mode feature isolates your network from 802.11b wireless clients and allows your network to transmit data at 54 Mbps.

NAT/Proxy

The Network Address Translation (NAT) Proxy module has been designed to provide private IP inter-networks that use non-registered IP addresses to connect to the Internet. It is an internal standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network, the Internet.

Firewall

A firewall is a set of rules, applications, and policies that should ensure that users get access to network services. A firewall should also ensure that the internal network remains secure from attackers via the Internet or other networks. There are two basic firewall architectures: **Proxy services** work between external and internal networks and provide replacement connections instead of direct connections with remote services. Proxies try to act more or less transparently.

Filtering gateway firewalls use a special rule set to filter IP, TCP, ICMP, and other packets that pass through the network interface. Arriving and outgoing packets are filtered by the type, source address, destination address, and port information contained in each packet. A filtering gateway doesn't require a powerful machine to run on and doesn't provide user authentication. Most of the modern firewall applications are hybrid products that cannot be easily classified into either of the above groups. However, the main distinction between a filter and a proxy remains. Firewalls usually contain additional security that supports software like a VPN server, strong authentication services (tokens, smart cards), or virus scan engines. The standard firewall support in the kernel is built upon two components -IP chains and IP Masquerading. IP chains is a mechanism for filtering IP packets; its inclusion means that any flavor of can be configured to run as a filtering gateway/firewall almost right out of the box. The second important firewall component in the kernel is IP Masquerading - a network address translation (NAT) implementation feature with which you can hide real IP addresses used in an internal network so you can use non-routing IP addresses in your LAN.

DHCP

The Dynamic Host Configuration Protocol (DHCP) is a TCP/IP protocol that enables the obtainment of temporary or permanent IP addresses (out of a pool) from a centrally administered server. The EdgeAccess UAD is capable of both DHCP Server and DHCP Client functionality.

WAN Overview

The UAD includes WAN interface capability. WAN Protocols supported by the UAD include:

- Frame Relay
- Synchronous Point-to-Point Protocol
- HDLC
- Multi-Link Point-to-Point Protocol
- Raw IP

Physical and Environmental Requirements

- Operating Temperature: 0° to 50° C
- Humidity: 80% non-condensing maximum
- Dimensions: 7.5" x 6" x 3.5"
- Power: 100-240 VAC (Auto Switching), 50/60Hz, 60 watts

Install UAD

Equipment Needed Using Telephone Key Pad

- Power Supply and Cable
- Network Cable (CAT 5 RJ-45)
- Analog Telephone

Procedures For LAN (eth0):

1. To set the IP Address:
 - Press **5 “IP Address” # (To use the “dot” for octet separation use the “asterisk” (*). For example: (192*168*10*5 is equal to 192.168.10.5)
2. To set the Subnet Mask IP:
 - Press **6 “Subnet Mask IP” #
3. To set the Default Gateway IP:
 - Press **7 “Default Gateway IP” #
4. To set the UAD for DHCP Client :
 - Press **8 #

For WAN (eth1):

5. To set the IP Address:
 - Press **1 “IP Address” # (To use the “dot” for octet separation use the “asterisk” (*). For example: (192*168*10*5 is equal to 192.168.10.5)
6. To set the Subnet Mask IP:
 - Press **2 “Subnet Mask IP” #
7. To set the Default Gateway IP:
 - Press **3 “Default Gateway IP” #
8. To set the UAD for DHCP Client:
 - Press **4 #

Install UAD

Equipment Needed Using Terminal Emulator

- Power Supply and Cable
- Network Cable (CAT 5 RJ-45)
- Serial Cable (RS-232, 9 Pin Both Ends Female)
- PC with a Terminal Emulation Utility Installed

Procedures

1. Connect PC serial port to UAD (UAD) terminal port utilizing a serial cable.
2. Connect UAD to LAN via RJ-45 Ethernet Port.
3. Start a Terminal Emulator session. Ensure you select the same Com Port used in step #1. Use the following Port Settings:
 - Baud = 9600
 - Data Bits = 8
 - Parity = None
 - Stop Bits = 1
 - Flow Control = Hardware
4. Turn on the UAD power switch.
5. Login: **manager** [**Enter**]
6. Password: [**Enter**] The user is now presented with a menu driven configuration interface. Each level of the menu offers various parameters to be set. In general, the Current or default setting can be selected by pressing [**Enter**] when prompted for a value. Sometimes a value is selected from a list of choices.
7. To configure the LAN Settings at the prompt type: **4** [**Enter**]
8. If you are going to be using a Dynamic IP Address, at the prompt type: **5** (MODE) [**Enter**] from the LAN Configuration Menu. If you are going to be using a Static IP Address, go to step **12**.
9. After selecting (MODE) from the LAN Configuration Menu, at the prompt type: **4** (dynamic) [**Enter**] from the MODE Configuration Menu.
10. From the Mode Configuration Menu, at the prompt type: **1** (previous menu) [**Enter**]. When asked “OK to save” press [**Enter**].
11. Restart the UAD by powering Off and On again.

12. After selecting (MODE) from the LAN Configuration Menu, at the prompt type: **3** (static) **[Enter]** from the MODE Configuration Menu.
13. From the LAN Configuration Menu, at the prompt type: **6** (IPADDR) **[Enter]**. Type the IP Address **[Enter]**.
14. From the LAN Configuration Menu, at the prompt type: **7** (NETMASK) **[Enter]**. Type the Sub net Mask **[Enter]**.
15. From the LAN Configuration Menu, at the prompt type: **8** (NETWORK) **[Enter]**. Type the Network IP Address **[Enter]**.
16. From the LAN Configuration Menu, at the prompt type: **9** (BROADCAST) **[Enter]**. Type the Network Broadcast IP Address **[Enter]**.
17. From the LAN Configuration Menu, at the prompt type: **10** (GATEWAY) **[Enter]**. Type the Network Default Gateway IP Address **[Enter]**.
18. From the LAN Configuration Menu, at the prompt type: **2** (previous menu) **[Enter]**. When asked “OK to save” press **[Enter]**.
19. Restart the UAD by powering Off and On again.
20. The unit is now ready for configuring via the Web Based Configuration Application.
21. To access the administration tool, open a browser window and in the address field, type the IP address of the UAD.
22. At the login screen, enter Login – **manager** **[Enter]** and Password – **[Enter]**.
23. The Web applet is java based so, you may be asked to install the Java Plug-In if it is not currently installed. Click on the **Yes** button. When the Java™ Plug-In Installation screen is displayed, click on **Install**. The Java files will be downloaded. Click **Yes** to accept the Software Agreement. To use the default file save location, click on the **next** button. The Java plug-in will be installed and the UAD Administration Application will be started.
24. To configure a hostname, double-click on **Network** folder and then double-click on the **Hostname** file. Enter a *Fully Qualified Domain Name*.
25. Click **Submit** to save the changes.

26. To configure the Telephony settings on an UAD, double click on the **Telephony** folder and then the **UAD** file. Edit the fields using the table below for reference.

Encoding	u-Law -Select this box to enable A/D encoding in North America. A-Law - Select this box to enable A/D encoding in Europe and other areas outside North America.
Listening Port	Enter the socket port # that the application will use to listen for voice packets (VSP Protocol).
SoftSwitch Registration	Check this box to enable user registration. When this box is selected, SoftSwitch and Backup SoftSwitch boxes will be editable.
SoftSwitch	Enter primary SoftSwitch IP address.
Backup SoftSwitch	Enter backup SoftSwitch address.
CDR	Enter the IP address of the machine that will accept CDRs (Call Detail Record).

27. Click **Submit** to save changes.
28. Double-click on the **Channel(s)** file. Click on the **Channel Number** field and select a channel. Click on the **Display** button. Note: Only one channel can be configured at a time. When you are done making changes to all tabs, click **Submit** to save the changes. It is not necessary to click **Submit** until changes on all tabs have been entered. Clicking **Cancel** will discard all changes on all tabs.
29. Edit the fields using the table below for reference.

Channel Enabled	Select this box to enable the port.
Logical Port #	Select a logical port number to be associated with this channel. The selection is similar to the trunking association of channel.
Coder Type	Select the speech coder to be used for transmission. Note: The higher the speech rate, the more bandwidth used for voice transmission.
Connection Type	Use this option to select whether connecting to a phone (FXS) or a phone line (FXO). (8 Port Cards Only)

30. Click on the **Connectivity** tab and edit the fields using the table below for reference.

Note: For Direct connection to a remote UAD, user must match the settings specified in Remote IP, Remote Logical Port and Remote IP Port to the setting on the remote system.

SoftSwitch Lookup	Select this box if the UAD is going to be a part of a network where a SoftSwitch is being used.
Remote IP	If SoftSwitch Lookup is not selected, enter the remote IP that the local channel connects to when a call is received.
Remote Logical Port	If SoftSwitch Lookup is not selected, enter the logical port number (trunk) of the channel on the remote machine. This port number associated with the Remote IP determines the call routing.
Remote IP Port	If SoftSwitch Lookup is not selected, enter the IP port number on which the remote machine listens for VoIP packets.
DNIS (optional)	If SoftSwitch Lookup is not selected, you may enter a DNIS for the remote to outdial.
Log CDR	Select this box enable “Call Detail Records”, logging to a central server as specified on the Telephony-UAD page.

31. Click on the **Dialing** Tab and edit the fields using the table below for reference.

Prefix Connect	Select this box to enable the prefix connect feature. When selected, the Prefix Connect box should contain the digit or string of digits used for out dialing. Typical use is for FXO lines, when you must dial a ‘9’ for an outside line.
Country Code	Country code of which the system is part.
Area Code	Area code of which the system is part.
Assigned Number	The Virtual phone number assignment for this port. May be an actual PSTN number depending on service provider.
Digits to Collect	Number of digits that the UAD should accept before assuming that dialing is complete.
International Access code	String of digits used to access international dialing services.
Voice Prompt Directory	Used to specify the subdirectory where the speech files (wave) are located. Use “default” when electing to use default files provided in the system. This feature is only available in G.723.1 coder.

32. Double-click on the **Toll Calling** file. Ensure the Local Area Code Tab is selected. To add a Local Area Code, enter a local area code in the box and click on the **Add** button. The Local Area Code will be added to the Local Area Codes box at the bottom of the screen.
33. Click **Submit** to save changes.
34. Select the Toll Calling Permission Tab.
35. To enable direct dial on a channel, select the Direct Dial box. (1+numbers)
36. To enable around dial on a channel, select the Around Dial box. (10+dial around code+numbers)
37. Click **Submit** to save changes.
38. Double-click on the **Call Progress** file. Select the applicable Call Progress Detection. When **User Defined Tones** is selected, the **User Defined Values** will be enabled. Edit the fields using the table below for reference.

Call Progress Detection	ANSI Standard Tones ITU-T Standard Tones User Defined Tones - Allows user to define tones by modifying the User Defined Values found at the bottom of the screen.
Dial Tone	Allows use to select the Frequency, Cadence and Output Level associated with the Dial Tone.
Audible Ring	Allows use to select the Frequency, Cadence and Output Level associated with the Audible Ring
Busy Tone	Allows user to select the Frequency, Cadence and Output Level associated with the Busy Tone.
Fast Busy	Allows user to select the Frequency, Cadence and Output Level associated with the Fast Busy.

39. Click **Submit** to save the changes.

40. Double-click on the **FXO Connection** file. Edit the fields using the table below for reference.

Require Line_Seize before dialing?	TRUE – Line seize indication will be required before dialing. Enter the amount of time to wait for the line seize in the Line_Seize Wait Time field. If no line seize indication is received before wait time expires, call originator will be sent an error indication, and the call will be dropped. FALSE - Line seize indication is not required before dialing.
Line Provides Connect Supervision Loop Reversal	TRUE - Yes FALSE - No
Connect Supervision Timeout	If no indication is received positive or negative, the amount of time to wait before issuing connect signal to call originator.
Delay After Line_Seize Before Dialing	Enter amount of time to wait after line seize to ensure line is stable before dialing number.

41. Click **Submit** to save the changes.

Connecting Devices & Checking Connectivity

Use (Figures 1-1 & 1-2) for the following devices.

- All channels are FXS/FXO compatible.
- Connect PC serial port to UAD (UAD) terminal port utilizing a serial cable.
- Connect UAD to LAN via RJ-45 Ethernet Port. Use only CAT 5 UTP cable to connect 100Mbps devices. To connect 10Mbps devices, use CAT 3, 4, or 5 UTP cable.
- Check the port LEDs to confirm the link status.
- A solid green LED for power.
- A solid green LED for the LAN Port indicates a valid link.
- A solid green LED for the UAD Lines indicates an active telephone line.



Figure 1-1



Figure 1-2

The UAD provides 2 management utilities to properly configure both Network (LAN/WAN) and Telephony configurations. The two utilities are the Basic Setup Manager (*Figure 2-1*) and Setup Manager with DHCP (*Figure 2-2*), which is accessed via Serial Terminal Emulation or terminal session, and the Web-Based Manager (*Figure 2-3*), which is accessed via Web Browser. The following chapters will go into detail how these are accessed and used.

NOTE: Configuration options may vary depending upon actual software release.

Setup Manager

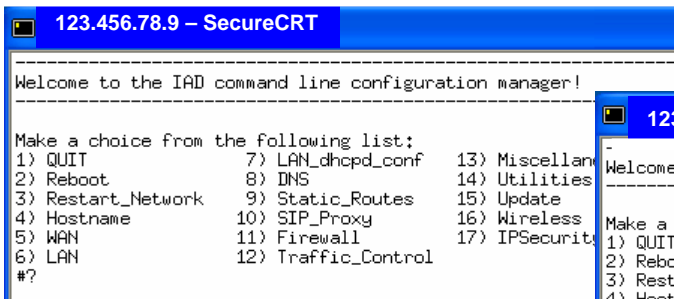


Figure 2 -1. Basic Setup Manager

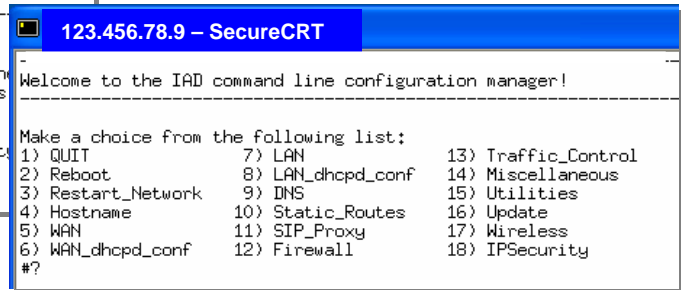


Figure 2 -2. Setup Manager with DHCP

Web-Based Manager



Figure 2-3. Web Manager Login

Accessing the Setup Manager

To Connect Serially follow steps 1- 6; to connect by Ethernet follow steps 4- 6.

1. Connect PC serial port to UAD (UAD) terminal port utilizing a PC-to-PC serial cable.
2. Connect UAD to LAN via RJ-45 Ethernet Port.
3. Start a Hyper Terminal session or similar Terminal Emulator. Ensure you select the correct COM Port. Use the following Port Settings:
 - Baud = 9600
 - Data Bits = 8
 - Parity = None
 - Stop Bits = 1
 - Flow Control = Hardware
4. Plug in the power on the EdgeAccess UAD.
5. Login: manager [Enter]
6. Password: [Enter]

Once you have logged in, the Main Configuration Menu will be displayed (*Figure 3-1*) if DHCP Server is NOT enabled and (*Figure 3-2*) if DHCP Server IS enabled. Most of the procedures covered in this section are usually only performed once during the initial setup and are global settings. These settings should not be changed often. There are limitations when changing network settings using a telnet session, i.e., when configuring your UAD to use DHCP (client) the telnet session may be lost and you must use a serial connection to access system afterwards. Warning messages are displayed when applicable. Some options require the user to enter a password before the changes will be implemented. When prompted, enter the current user's password to continue.

You may change any or all of the current settings in any menu by selecting that item from the menu and answering the prompts as they are presented.

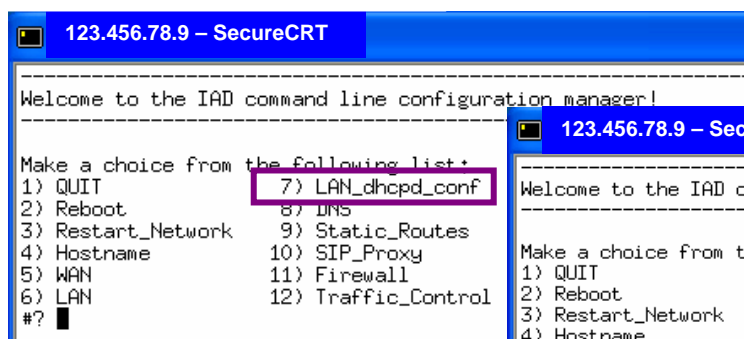


Figure 3-1. Sample main menu

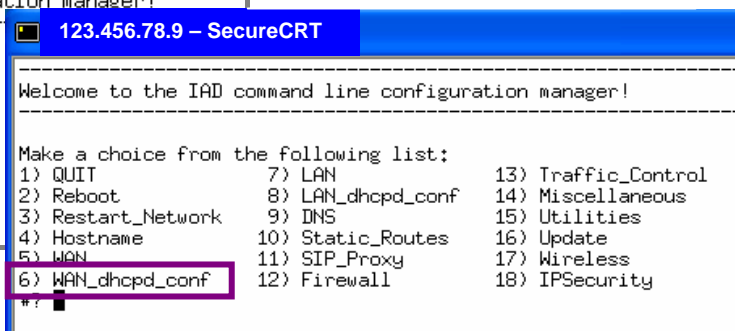


Figure 3-2. Sample main menu if DHCP IS enabled

Overview

Please enter all Selections/Options by typing the number that corresponds with your selection and pressing **[Enter]**. When returning to “previous_screen” from any sublist, simply type **[n]** for no OR **[y]** for yes to save changes if applicable. *Main menu options are defined below.*

REMEMBER: Configuration options may vary depending upon software release.

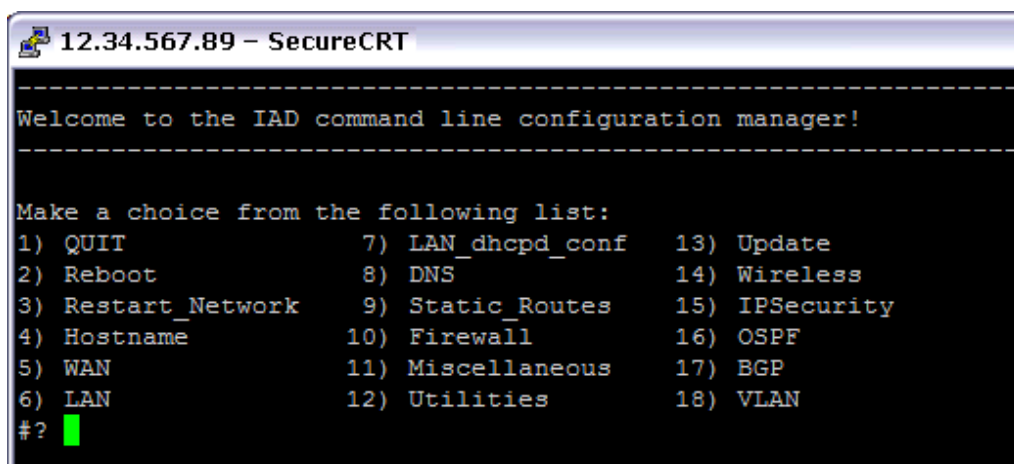


Figure 3-3. Main Menu

QUIT

When (Quit) from the Main Configuration Menu is selected, the current Telnet session will be terminated and disconnect from the UAD.

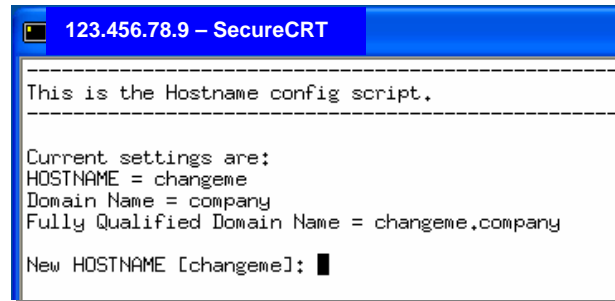
Reboot

When (Reboot) from the Main Configuration Menu is selected, the UAD will reboot immediately after you press **[Enter]**.

Hostname

When (Hostname) from the Main Configuration Menu is selected, you will be prompted to enter a new value for the UAD Hostname **[Enter]** and a new value for UAD Domain Name **[Enter]** as shown in example (Figure: 3-3). Hostname is used by the UAD to register with the SoftSwitch and Gateway. All UADs within a network should have a unique Hostname.

The current or default value is shown in the square brackets [], if this is your desired value, you may select it by pressing **[Enter]**, otherwise type the new value and then press **[Enter]**.



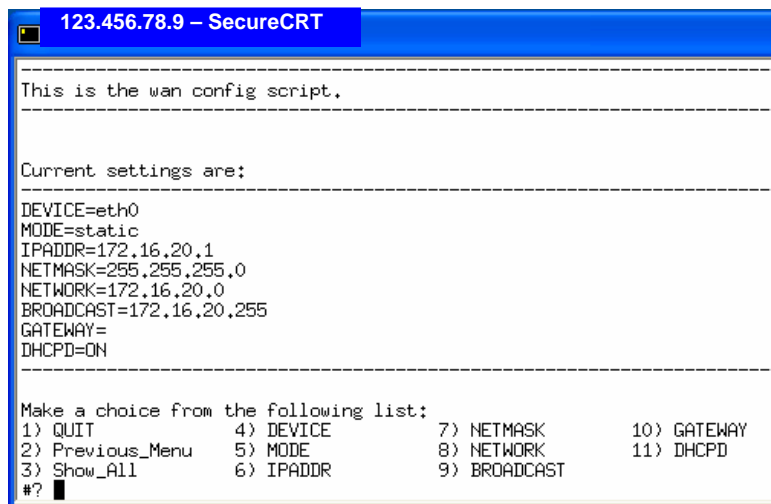
```
123.456.78.9 - SecureCRT
-----
This is the Hostname config script.
-----
Current settings are:
HOSTNAME = changeme
Domain Name = company
Fully Qualified Domain Name = changeme.company
New HOSTNAME [changeme]: █
```

Figure 3-4. Hostname screen

The values entered are displayed for confirmation. If the information is correct and you want to save, type **y** for yes and press **[Enter]**. A message confirming that the changes have been saved is displayed. If you do not want to save the changes, type **[n]** for no and press **[Enter]**. You will be returned to the Main Configuration Menu.

WAN

The (WAN) option from the Main Configuration Menu, allows you to configure the WAN Interface for the UAD. The Setup Manager will automatically display the parameters for the WAN interface that is installed and the WAN Configuration Menu will be displayed (Figure 3-4).



```
123.456.78.9 - SecureCRT
-----
This is the wan config script.
-----
Current settings are:
-----
DEVICE=eth0
MODE=static
IPADDR=172.16.20.1
NETMASK=255.255.255.0
NETWORK=172.16.20.0
BROADCAST=172.16.20.255
GATEWAY=
DHCPD=DN
-----
Make a choice from the following list:
1) QUIT          4) DEVICE       7) NETMASK      10) GATEWAY
2) Previous_Menu 5) MODE         8) NETWORK      11) DHCPD
3) Show_All     6) IPADDR      9) BROADCAST
#? █
```

Figure 3-5. WAN

QUIT

When (Quit) is selected from the WAN Configuration Menu, the current Telnet session will be terminated and disconnect from the UAD.

Previous_Menu

When (Previous_Menu) from the WAN Configuration Menu is selected, it will take you back to the previous menu.

Show_All

When (Show_All) from the WAN Configuration Menu is selected, the system will display the current configuration of all network interfaces.

DEVICE

When (DEVICE) from the WAN Configuration Menu is selected, you will be prompted to enter the UAD WAN Interface that you would like to configure and press [**Enter**].

MODE

The (MODE) option from the WAN Configuration Menu allows you to configure the mode on the WAN Interface for the UAD. The Setup Manager will automatically display the Mode Configuration Menu.

down

When (down) from the WAN Mode Configuration Menu is selected, the WAN Interface will not be initialized on power up.

static

When (static) from the WAN Mode Configuration Menu is selected, the WAN Interface mode will be set to static (using a static IP address).

dynamic

When (dynamic) from the WAN Mode Configuration Menu is selected, the WAN Interface will get its IP address dynamically from a DHCP Server.

pppoe

When (pppoe) from the WAN Mode Configuration Menu is selected, the WAN Interface mode will be set to pppoe. This is normally used by some ISPs who require PPPoE for their network connections using xDSL.

ppp

When (ppp) from the WAN Mode Configuration Menu is selected, the WAN Interface mode will be set to ppp. This is normally used for Modem Dial-Up connections. The PPP connection will not be initialized automatically. Use the Web configuration pages to bring up the connection when desired.

IPADDR

When (IPADDR) from the WAN Configuration Menu is selected, you will be prompted to enter new values for the UAD IP Address. You will be returned to the WAN Configuration Menu after the UAD IP Address is entered.

Netmask

When (NETMASK) from the WAN Configuration Menu is selected, you will be prompted to enter new values for the UAD Sub Netmask IP Address. You will be returned to the WAN Configuration Menu after the UAD IP Sub Netmask is entered.

Note: *Based on the IP Address and the Netmask values, the Network and Broadcast fields will be automatically populated.*

Network

When (NETWORK) from the WAN Configuration Menu is selected, you will be prompted to enter new values for the UAD Network IP Address. You will be returned to the WAN Configuration Menu after the UAD Network IP is entered.

Broadcast

When (BROADCAST) from the WAN Configuration Menu is selected, you will be prompted to enter new values for the UAD Broadcast IP Address. You will be returned to the WAN Configuration Menu after the UAD Broadcast IP Address is entered.

Gateway

When (GATEWAY) from the WAN Configuration Menu is selected, you will be prompted to enter new values for the UAD Default Gateway IP Address. You will be returned to the WAN Configuration Menu after the IAD Default Gateway IP Address is entered.

DHCPD

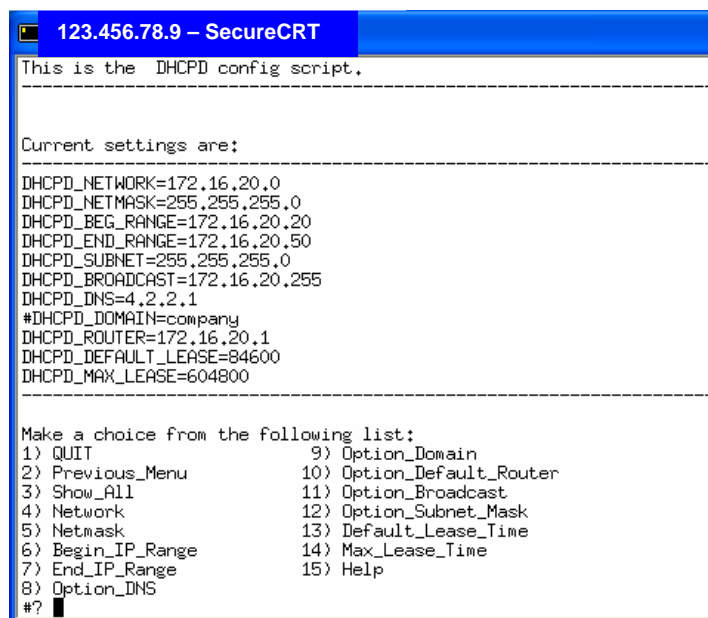
When (DHCPD) is selected from the WAN Configuration Menu, the DHCP server is turned ON or OFF. Selecting DHCPD from the menu, toggles turning the Server ON or OFF. Once you have turned the Server ON or OFF, you will be prompted to save the change and then returned to the WAN Configuration Menu after your selection is entered.

Wireless_AP (Only applies if wireless card is installed)

When (WIRELESS_AP) from the WAN Configuration Menu is selected, you will be prompted to enter [ON] if you would like to enable Wireless Access Point functionality or [OFF] if you would like to disable Wireless Access Point functionality. You will be returned to the WAN Configuration Menu after your selection is entered.

WAN_dhcpd_conf

The (WAN_dhcpd_conf) option from the Main Configuration Menu allows you to set the DHCP Server parameters for the UAD to serve as a DHCP Server on the WAN side. When the WAN_dhcpd_conf option is selected from the Setup Manager Main Menu, the WAN_dhcpd_conf Menu shown in (Figure 3-5) will be displayed. From this menu, the WAN DHCP Server parameters can be set.



```
123.456.78.9 - SecureCRT
This is the DHCPD config script.
-----
Current settings are:
-----
DHCPD_NETWORK=172.16.20.0
DHCPD_NETMASK=255.255.255.0
DHCPD_BEG_RANGE=172.16.20.20
DHCPD_END_RANGE=172.16.20.50
DHCPD_SUBNET=255.255.255.0
DHCPD_BROADCAST=172.16.20.255
DHCPD_DNS=4.2.2.1
#DHCPD_DOMAIN=company
DHCPD_ROUTER=172.16.20.1
DHCPD_DEFAULT_LEASE=84600
DHCPD_MAX_LEASE=604800
-----
Make a choice from the following list:
1) QUIT
2) Previous_Menu
3) Show_All
4) Network
5) Netmask
6) Begin_IP_Range
7) End_IP_Range
8) Option_DNS
9) Option_Domain
10) Option_Default_Router
11) Option_Broadcast
12) Option_Subnet_Mask
13) Default_Lease_Time
14) Max_Lease_Time
15) Help
#? █
```

Figure 3-6. WAN DHCP

Network

When (Network) from the WAN DHCPD Menu is selected, you will be prompted to enter the value for the WAN Network IP Address. You will be returned to the WAN DHCPD Menu after the Network IP is entered.

Netmask

When (Netmask) from the WAN DHCPD Menu is selected, you will be prompted to enter the value for the WAN Sub Netmask IP Address. You will be returned to the WAN DHCPD Menu after the Sub Netmask IP is entered.

Begin_IP_Range

When (Begin_IP_Range) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the beginning of the IP range that the DHCP Server will use to distribute IP Addresses for DHCP Clients. You will be returned to the WAN DHCPD Change Parameters Menu after you have entered the beginning of the IP Range.

End_IP_Range

When (End_IP_Range) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the end of the IP range that the DHCP Server will use to distribute IP Addresses for DHCP Clients. You will be returned to the WAN DHCPD Change Parameters Menu after you have entered the end of the IP Range.

DNS

When (DNS) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the value for the WAN DNS IP Address that the DHCP Server will use to distribute for DHCP Clients. You will be returned to the WAN DHCPD Change Parameters Menu after the DNS IP is entered.

Domain

When (Domain) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the Network's Domain Name. You will be returned to the WAN DHCPD Change Parameters Menu after the Network's Domain Name is entered.

Default_Router

When (Default_Router) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the value for the WAN Default Router IP Address that the DHCP Server will use to distribute for DHCP Clients as their Default Gateway. You will be returned to the WAN DHCPD Change Parameters Menu after the Default Router IP is entered.

Broadcast

When (Broadcast) from the WAN DHCPD Menu is selected, you will be prompted to enter the value for the WAN Broadcast IP Address. You will be returned to the WAN DHCPD Change Parameters Menu after the Broadcast IP is entered.

Lease_Time (Seconds)

When (Lease_Time) from the WAN DHCPD Menu is selected, you will be prompted to enter the value for the WAN Lease Time for the DHCP Clients IP Addresses. You will be returned to the WAN DHCPD Change Parameters Menu after the Lease Time is entered.

Sub_Net_Mask

When Sub_Net_Mask from the WAN DHCPD Menu is selected, you will be prompted to enter the value for the Sub_Net_Mask. You will be asked to save changes by selecting Y for yes or N for no. Once you make your selection and hit enter, you will be returned to the WAN DHCPD menu.

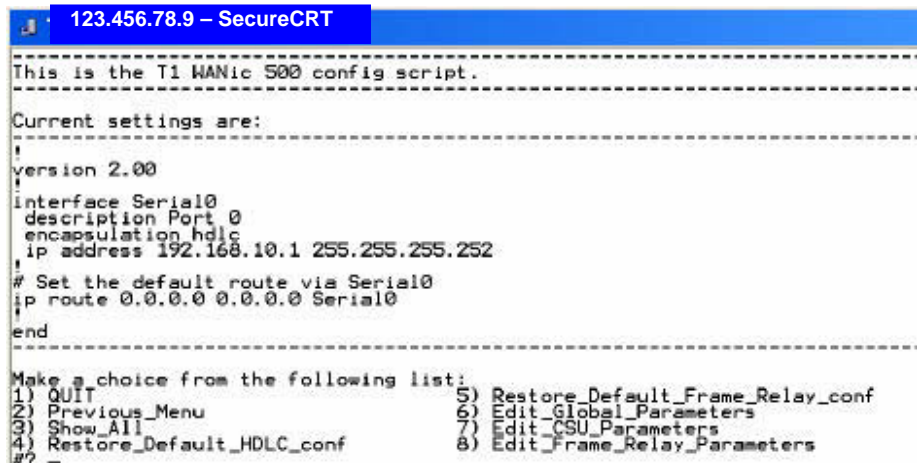
Max_Lease_Time (Seconds)

When (Max_Lease_Time) from the WAN DHCPD Change Parameters Menu is selected, you will be prompted to enter the value for the WAN Maximum Lease Time for the DHCP Clients IP Addresses. You will be returned to the WAN DHCPD Change Parameters Menu after the Maximum Lease Time is entered.

WAN_T1_conf

This option will only appear on the Main Menu, if the UAD has a T1 WAN Interface Card installed. The (WAN_T1_conf) option from the Main Configuration Menu, allows you to set WAN T1 interface configuration for the UAD. When this option is selected, the Setup

Manager will automatically display the parameters for the T1 interface that is installed and the T1 WAN Interface Configuration Menu will be displayed (*Figure 3-7*).



```
123.456.78.9 - SecureCRT
-----
This is the T1 WANic 500 config script.
-----
Current settings are:
-----
!
version 2.00
interface Serial0
description Port 0
encapsulation hdlc
ip address 192.168.10.1 255.255.255.252
# Set the default route via Serial0
ip route 0.0.0.0 0.0.0.0 Serial0
end
-----
Make a choice from the following list:
1) QUIT                               5) Restore_Default_Frame_Relay_conf
2) Previous_Menu                       6) Edit_Global_Parameters
3) Show_All                             7) Edit_CSU_Parameters
4) Restore_Default_HDLC_conf           8) Edit_Frame_Relay_Parameters
#? =
```

Restore_Default_HDLC_conf

When (Restore_Default_HDLC_conf) from the WAN_T1_conf Menu is selected, the system will restore the HDLC configuration to the system default values.

Restore_Default_Frame_Relay_conf

When (Restore_Default_Frame_Relay_conf) from the WAN_T1_conf Menu is selected, the system will restore the Frame Relay configuration to the system default values.

Edit_Global_Parameters

When (Edit_Global_Parameters) from the WAN_T1_conf Menu is selected, it allows you to configure the WAN T1 interface Global parameters for the UAD (*Figure 3-10*).

encapsulation

When (encapsulation) from the Edit_Global_Parameters Menu is selected, it will allow you to choose the encapsulation type.

description

When (description) from the Edit_Global_Parameters Menu is selected, it will allow you to specify a description for the serial interface.

Static ip address and route

When (static_ip_address_and_route) from the Edit_Global_Parameters Menu is selected, you will be prompted to enter values for the Serial Interface IP Address, Netmask and Route. You will be returned to the Edit_Global_Parameters Menu after the IP Address and/or route have been entered.

Remove static routes

When (remove_static_routes) from the Edit_Global_Parameters Menu is selected, it allows you to remove one or all of the configured static routes.

Edit_CSU_Parameters

When (Edit_CSU_Parameters) from the WAN_T1_conf Menu is selected, it allows you to configure the WAN T1 CSU parameters for the UAD (*Figure 3-11*).

clock_source

When (clock_source) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the clock source.

data_coding

When (data_coding) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's data coding.

framing

When (framing) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's framing.

lbo

When (lbo) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's lbo (Line Buildout).

linecode

When (linecode) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's line coding.

timeslots

When (timeslots) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's timeslot.

egl

When (egl) from the Edit_CSU_Parameters Menu is selected, it will allow you to select the CSU's egl (Equalizer Gain Limit).

ip_address

When (ip_address) from the Edit_CSU_Parameters Menu is selected, you will be prompted to enter values for the Serial Interface IP Address, Netmask and Route. You will be returned to the Edit_CSU_Parameters Menu after the IP Address and/or route have been entered.

Edit_Frame_Relay_Parameters

When (Edit_Frame_Relay_Parameters) from the WAN_T1_conf Menu is selected, it allows you to configure the Frame Relay parameters for the T1 WAN interface on the UAD (*Figure 3-12*).

Edit_Master_Interface_Commands

When (Edit_Master_Interface_Commands) from the Edit_Frame_Relay_Parameters Menu is selected, , it allows you to configure the Master Interface Commands for the T1 WAN interface on the UAD (*Figure 3-13*).

lmi_type

When (lmi_type) from the Edit_Master_Interface_Commands Menu is selected, it allows you to select the lmi (Local Management Interface) type for the T1 WAN interface on the UAD.

mode

When (mode) from the Edit_Master_Interface_Commands Menu is selected, it allows you to select the Mode for the T1 WAN interface on the UAD.

Add_Subinterface

When (Add_Subinterface) from the Edit_Frame_Relay_Parameters Menu is selected, it will allow you to add a serial interface and you will be prompted to enter values for the Serial Interface DLCI (Data Link Connection Identifier, IP Address, Netmask and Route. You will be returned to the Edit_Master_Interface_Commands Menu after the all of the parameters have been entered.

Delete_Subinterface

When (Delete_Subinterface) from the Edit_Frame_Relay_Parameters Menu is selected, it will allow you to delete a configured Subinterface.

This doc assumes that the T1 card is installed and is working properly.

To set up a Frame-Relay connection, use the following steps:

1. Login as manager or start the manager script.
2. Select "WAN" interface.
3. Change "DEVICE" name to Serial0.
4. If mode is going to be static configure the interface setting on the WAN menu. IP ADDRESS, NETMASK, NETWORK, BROADCAST, GATEWAY. If mode is dynamic there is no need to set the settings in step (4)
5. Select Previous_Menu from the WAN menu. Select "y" to apply your changes.
6. From the main menu select "WAN_T1_conf".
7. Though settings may already be set for frame-relay I will take you through restoring the factory default frame settings. So from the "WAN_T1_conf" menu select "Restore_Default_Frame_Relay_conf".
8. You will now see the default frame-relay settings. This is as far as this document can go as to telling you what needs to be done. Any settings that need to be changed/added or deleted will depend on the remote side of the frame-relay connection. So below is a list of all the frame setting that can be set and how to find them in the manager scripts.

Interface CSU commands

Main Menu > WAN_T1_conf > Edit_CSU_Parameters

```
service-module {t1} clock source { line | internal }
```

Set the internal CSU's clock source to external/line (default) or internal.

```
service-module {t1} data-coding { normal | inverted }
```

Set the internal CSU's coding to normal (default) or inverted.

```
service-module t1 framing { esf | sf }
```

Set the internal CSU's framing to esf (Extended Super Frame-default) or sf (Super Frame also known as D4).

```
service-module t1 lbo { -22.5 db | -15 db | -7.5 db | none }
```

Set the internal CSU's line buildout. Use only if the cable between your card's TX connector to the demarcation point is greater than 225 feet.

```
service-module t1 linecode { b8zs | ami }
```

Set the internal CSU's line coding to b8zs (default) or ami.
service-module e1 linecode { hdb3 | ami }

Set the internal CSU's line coding to hdb3 (default) or ami.
service-module {t1} timeslots { range | all } [speed { 56 | 64 }]

Set the internal CSU's timeslot usage and speed per timeslot. 56K channel speeds require the use of D4 framing.

Example: service-module t1 timeslots 1-12 for a 768K circuit.

Example: service-module t1 timeslots 1-4, 5, 6-10, 12-18, 19, 23 speed 56.

Example: service-module e1 timeslots 1-28 for a 1.792Mbps circuit.
service-module {t1} egl

Set the internal CSU's equalizer gain limit on.

Frame Relay Commands

Frame relay master interface commands

Main Menu > WAN_T1_conf > Edit_Frame_Relay_Parameters > Serial0

- **description**
has no affect on frame connection, for your identification only
- **encapsulation frame -relay ietf**
Required command to set the protocol for the frame relay subinterface.
- **frame-relay lmi-type type**
Set the lmi type for an interface. Valid only in main interface configurations and not in subinterfaces.
- **frame-relay interval interval**
Sets the LMI interval in Mhz.
- **frame-relay mode {dte | dce}**
Sets the frame-relay mode to dte (default) or to dce

Main Menu > WAN_T1_conf > Edit_Frame_Relay_Parameters > [select sub interface you wish to configure]

Frame relay subinterface commands

- **description**
has no affect on frame connection, for your identification only.
- **encapsulation frame -relay ietf**
Required command to set the protocol for the frame relay subinterface.
- **frame-relay interface-dlci dlci**
Assigns a data link connection identifier (DLCI) to a specified frame relay sub interface on the router.
- **ip address ip-address mask**
To set IP addresses for a subinterface, use the ip address command.
- **ip-address IP address**
mask Network mask (netmask)

This is a sample of a frame-relay configuration file:

```
!  
version 2.00  
!  
interface Serial0  
description Main  
encapsulation frame-relay ietf  
frame-relay lmi-type ansi  
!  
interface Serial0.1  
description Sub1  
ip address 172.16.10.2 255.255.255.0  
encapsulation frame-relay ietf  
frame-relay interface-dlci 50  
frame-relay mode dce  
!  
ip route 172.16.10.1 255.255.255.0 Serial0.1  
!  
end
```

With the following menu selections you can setup a functioning frame relay connections.

Frame Relay Unnumbered IP

1. First follow the setup instructions for a default frame relay configuration.
2. When changing from a number frame configuration to an unnumbered configuration, there are two important steps. First, the IP address on the interface you are configuring needs to have the same address as the ethernet side of your IAD and the subnet mask needs to be all 255. Second, specific route entries must be made for a frame relay connection.

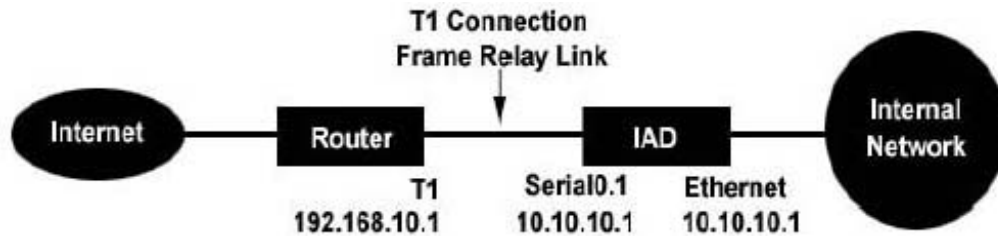
IP Address

If your ethernet interface ip was 10.10.10.1 then the IP entry for frame relay would look like this:

```
!  
version 2.00  
!  
interface Serial0  
description Main  
encapsulation frame-relay ietf frame-  
relay lmi-type ansi  
!  
interface Serial0.1  
description Sub1  
ip address 10.10.10.1 255.255.255.255  
encapsulation frame-relay ietf frame-  
relay interface-dlci 50 frame-relay  
mode dce  
!  
end
```

Routes for a Frame Relay Connection

You need to make specific route entries for your configuration. Here is a sample setup diagram.

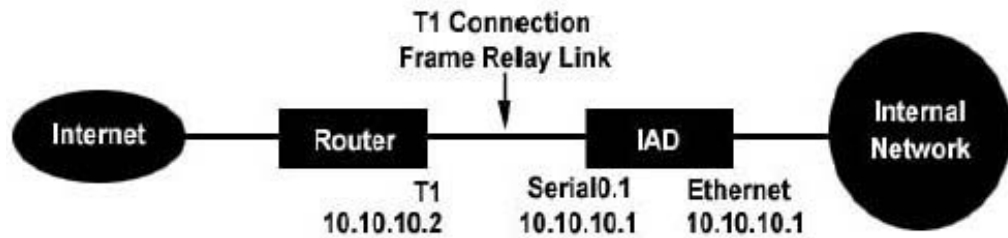


For this setup you would have the following route entries:

```
!  
version 2.00  
!  
interface Serial0  
description Main  
encapsulation frame-relay ietf  
frame-relay lmi-type ansi  
!  
interface Serial0.1  
description Sub1  
ip address 10.10.10.1 255.255.255.255  
encapsulation frame-relay ietf  
frame-relay interface-dlci 50  
frame-relay mode dce  
!  
ip route 192.168.10.0 255.255.255.0 Serial0.1  
ip route 0.0.0.0 0.0.0.0 192.168.10.1  
!
```

These 2 entries change the default route to be the routers T1 interface. You **MUST** have the 192 entry before the 0.0.0.0 entry and you **MUST** specify the interface in this case Serial0.1 for the 192 entry.

There is another scenario for this setup and that is if the router is on the same network segment as the UAD. The following diagram illustrates this.



In this diagram, the router, UAD and the internal network are on the same network segment. In this scenario the ip routes would look like this.

```

!
version 2.00
!
interface Serial0
  description Main
  encapsulation frame-relay ietf
  frame-relay lmi-type ansi
!
interface Serial0.1
  description Sub1
  ip address 10.10.10.1 255.255.255.255
  encapsulation frame-relay ietf
  frame-relay interface-dlci 50
  frame-relay mode dce
!
ip route 10.10.10.0 255.255.255.0 Serial0.1
ip route 0.0.0.0 0.0.0.0 10.10.10.0
!

```

To set the default gateway to the network ID requires rebooting the UAD.

HDLC Configuration

If you have selected to run a frame connection using the hdlc encapsulation there are only 2 settings you can modify, IP address and routes.

IP address for the connection:

Main Menu > WAN_T1_CONF > Edit_HDLC_Parameters > IP_Address

Routes:

Main Menu > WAN_T1_conf > Edit_DHLC_Parameters > IP_Routes

LAN

The (LAN) option from the Main Configuration Menu, allows you to set LAN configuration for the UAD. In order to communicate with the UAD within the network you must first configure the LAN settings. When this option is selected, the Setup Manager will automatically display the parameters for the LAN interface that is installed and the LAN Configuration Menu will be displayed.

NOTE: All the options listed on the LAN main menu are the same as those detailed in the WAN selection. Please refer to the WAN section for option definitions.

LAN_dhcpd_conf

The (LAN_dhcpd_conf) option from the Main Configuration Menu allows you to set the DHCP Server parameters for the UAD to serve as a DHCP Server on the WAN side. When the LAN_dhcpd_conf option is selected from the Setup Manager Main Menu, the LAN_dhcpd_conf Menu will be displayed.

Static_Routes

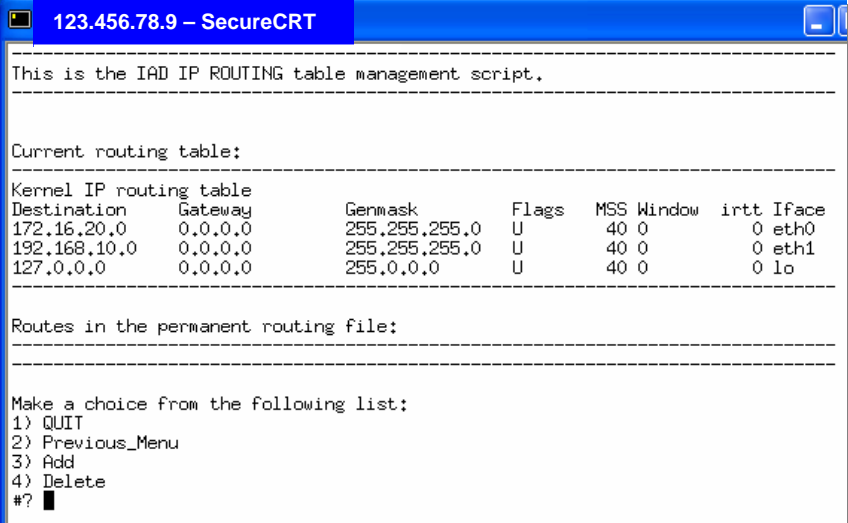
When (Static_Routes) from the Main Configuration Menu is selected, it allows you to Add or Delete static routes that your system may need, other than the default configured routes (Figure 3-8).

Add

When (Add) from the Static_Route Configuration Menu is selected, the system will prompt you to enter the Destination Network IP Address, Netmask, Default Gateway and the Interface to use to reach the Gateway.

Delete

When (Delete) from the Static_Route Configuration Menu is selected, the system will prompt you to enter the static route that you would like to delete.



```
123.456.78.9 - SecureCRT
-----
This is the IAD IP ROUTING table management script.
-----
Current routing table:
-----
Kernel IP routing table
Destination Gateway Netmask Flags MSS Window irtt Iface
172.16.20.0 0.0.0.0 255.255.255.0 U 40 0 0 eth0
192.168.10.0 0.0.0.0 255.255.255.0 U 40 0 0 eth1
127.0.0.0 0.0.0.0 255.0.0.0 U 40 0 0 lo
-----
Routes in the permanent routing file:
-----
Make a choice from the following list:
1) QUIT
2) Previous_Menu
3) Add
4) Delete
#? █
```

Figure 3-8. Routing

Firewall

The (Firewall) option from the Main Configuration Menu, allows you to configure the Firewall and set Port Mapping parameters for the UAD. When the Firewall option is selected from the Main Configuration Menu, the Firewall Menu shown in (Figure 3-9) will be displayed.

Port Mapping

This feature goes by many names, but what it does is allow you to open holes (ports) in your firewall. You'll need to do this for most any Internet applications that depend on the ability of someone on the WAN (Internet) side of your router to send a data request to a computer on your LAN.

When (Port_Mapping) from the Firewall Configuration Menu is selected, the system will display the Port_Mapping Menu, which will allow you to add or remove Port Mappings on the Firewall.

IP Masquerading

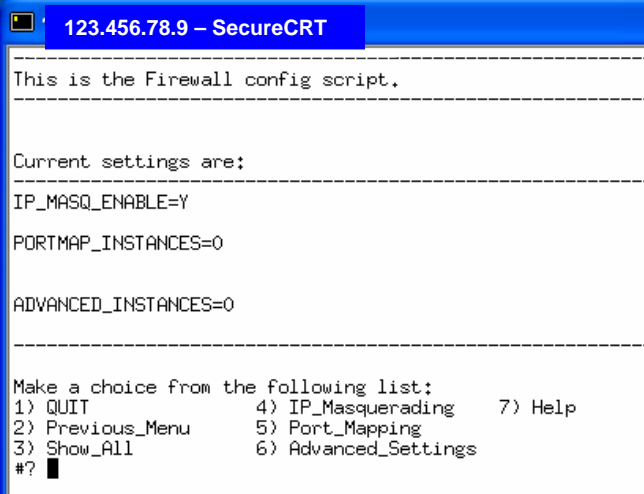
IP Masquerading is a form of network address translation that many routers already support. It lets you use a single Internet-connected machine running with a real IP address as a gateway for non-connected machines with "fake" IP addresses. The machine with the real IP address handles mapping packets from your intranet out to the Internet, and when responses come back, it maps them back to your intranet. This lets you browse the web and use other Internet functions from multiple machines without having a special network setup from your ISP.

This is only a basic firewall setup. For more rigorous protection, additional firewall rules can be added to the firewall scripts.

When (IP_Masquerading) from the Firewall Configuration Menu is selected, the system will prompt you to enable or disable IP Masquerading on the Firewall.

Advanced Settings

When (Advanced_Settings) from the Firewall Configuration Menu is selected, the system will display the Advanced Settings Menu.



```
123.456.78.9 - SecureCRT
-----
This is the Firewall config script.
-----
Current settings are:
-----
IP_MASQ_ENABLE=Y
PORTMAP_INSTANCES=0
ADVANCED_INSTANCES=0
-----
Make a choice from the following list:
1) QUIT                4) IP_Masquerading    7) Help
2) Previous_Menu      5) Port_Mapping
3) Show_All           6) Advanced_Settings
#? █
```

Figure 3-9. Firewall

Traffic_Control

Traffic Control or Traffic Shaping is the general term given to a broad range of techniques designed to enforce prioritization policies on the transmission of data over a network link.

The traffic control mechanism in the kernel consists of the following components:

- queuing disciplines (qdisc)
- classes
- filters
- policer

Qdiscs are responsible for transmitting the data.

Classes are attached to qdiscs and contain traffic. Each class with no child classes attached to it, always has 1 qdisc associated with it to transmit the packets and this qdisc holds all the traffic that flows in that class.

Filters are attached to qdiscs and classes and split the traffic into different child-classes.

Policers are used to make sure filters match only a certain rate of packets. The (Traffic_Control) option from the Main Configuration Menu, allows you to configure the Traffic Control commands and set

the root qdisc, classes and filters for a specific interface on the UAD. When the Traffic_Control option is selected from the Main Configuration Menu, the Traffic_Control Menu shown in (Figure 3-10) will be displayed.

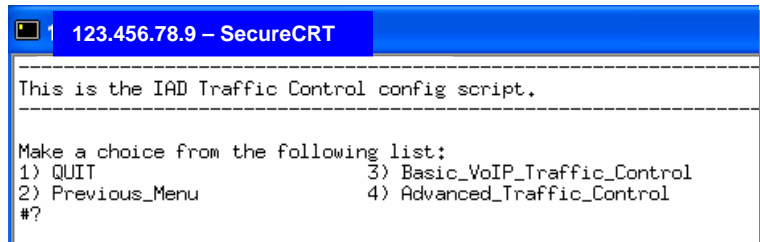


Figure 3-10. Traffic Control

When (Start_Basic_Traffic_Control) from the Traffic Control Configuration Menu is selected, the system will start Basic Traffic Control.

Stop_Basic_Traffic_Control

When (Stop_Basic_Traffic_Control) from the Traffic Control Configuration Menu is selected, the system will stop Basic Traffic Control.

Advanced_Traffic_Control

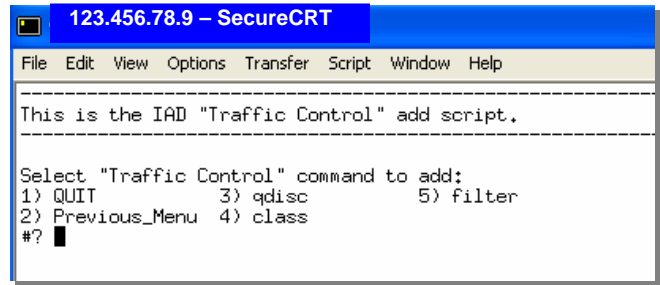
When (Advanced_Traffic_Control) from the Traffic Control Configuration Menu is selected, the system allows you to configure Advanced Traffic Control commands for a specific interface.

ADD

When (Add) from the Advanced Traffic Control Configuration Menu is selected, the system allows you to add Traffic Control Commands for a specific UAD interface (*Figure 3-11*).

qdisc

When (qdisc) from the Advanced Traffic Control Add Configuration Menu is selected, the system will prompt you for the necessary information to create a new qdisc for the specified interface.



```
123.456.78.9 - SecureCRT
File Edit View Options Transfer Script Window Help
-----
This is the IAD "Traffic Control" add script.
-----
Select "Traffic Control" command to add:
1) QUIT          3) qdisc        5) filter
2) Previous_Menu 4) class
#? █
```

Figure 3-11.

class

When (class) from the Advanced Traffic Control Add Configuration Menu is selected, the system will prompt you for the necessary information to create a new class or Class ID for the specified interface.

filter

When (filter) from the Advanced Traffic Control Add Configuration Menu is selected, the system will prompt you for the necessary information to create a new filter for the specified interface.

Delete

When (Delete) from the Advanced Traffic Control Configuration Menu is selected, the system will allow you to delete any of the created Traffic Control Commands.

Start Advanced Traffic Control

When (Start_Advanced_Traffic_Control) from the Advanced Traffic Control Configuration Menu is selected, the system will allow you to start any of the Advanced Traffic Control commands that you have created for a specific interface.

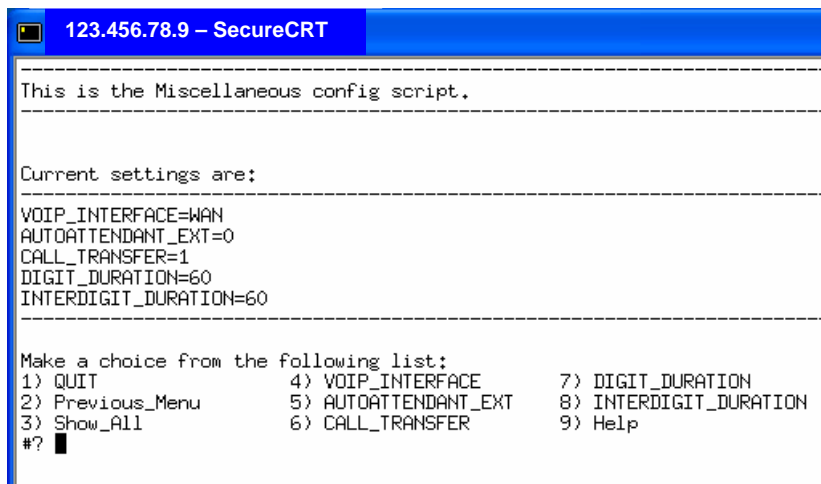
Stop Advanced Traffic Control

When (Stop_Advanced_Traffic_Control) from the Advanced Traffic Control Configuration Menu is selected, the system will allow you to stop any of the Advanced Traffic Control commands that you have started for a specific interface.

Miscellaneous

The (Miscellaneous) option from the Main Configuration Menu, allows you to configure several miscellaneous parameters (VoIP Interface, Call Transfer, etc). When the Miscellaneous option is selected from the Main Configuration Menu, the Miscellaneous Menu shown in (Figure 3-12) will be displayed.

If you are not sure about any of these settings, **DO NOT** change them, or the UAD may not function properly.



```
123.456.78.9 - SecureCRT
-----
This is the Miscellaneous config script.
-----
Current settings are:
-----
VOIP_INTERFACE=WAN
AUTOATTENDANT_EXT=0
CALL_TRANSFER=1
DIGIT_DURATION=60
INTERDIGIT_DURATION=60
-----
Make a choice from the following list:
1) QUIT                4) VOIP_INTERFACE      7) DIGIT_DURATION
2) Previous_Menu      5) AUTOATTENDANT_EXT  8) INTERDIGIT_DURATION
3) Show_All           6) CALL_TRANSFER       9) Help
#? █
```

Figure 3-12

VOIP_INTERFACE

When (VOIP_INTERFACE) from the Miscellaneous Configuration Menu is selected, the system will prompt you to select the Voice Interface (LAN, WAN or IP Address) that the application will use when calculating which address to register with the Softswitch.

AUTOATTENDANT_EXT

When (AUTOATTENDANT_EXT) from the Miscellaneous Configuration Menu is selected, the system will prompt you to enable (1) or disable (0) the Auto Attendant function for the UAD.

CALL_TRANSFER

When (CALL_TRANSFER) from the Miscellaneous Configuration Menu is selected, the system will prompt you to enable (1) or disable (0) the Centrextype Call Transfer function for the UAD.

DIGIT_DURATION

When (DIGIT_DURATION) from the Miscellaneous Configuration Menu is selected, the system will prompt you to enter the amount of time in milliseconds that a DTMF tone will be played by the DSP when pumping digits out a phone line.

INTERDIGIT_DURATION

When (INTERDIGIT_DURATION) from the Miscellaneous Configuration Menu is selected, the system will prompt you to enter the amount of time in milliseconds for the time between DTMF digits when pumping digits out a phone line.

Utilities

The (Utilities) option from the Main Configuration Menu, allows you to change Console passwords, Web passwords, PING a network, etc. When the Utilities option is selected from the Main Configuration Menu, the Utilities Menu shown in (Figure 3-13) will be displayed.

Change_Console_Password When

(Change_Console_Password) from the Utilities Menu is selected, the system will prompt you to confirm that you want to change your password and then prompt you to enter, first the Old Password and then it will prompt you to enter the New Password and to confirm the New Password (Figure 3-14).

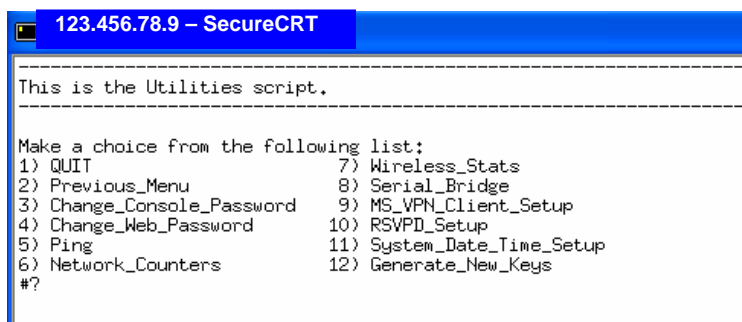
Change_Web_Password

When (Change_Web_Password) from the Utilities Menu is selected, the system will prompt you to confirm that you want to change your password and then prompt you to enter the New Password and to confirm the New Password (Figure 3-15).

Ping

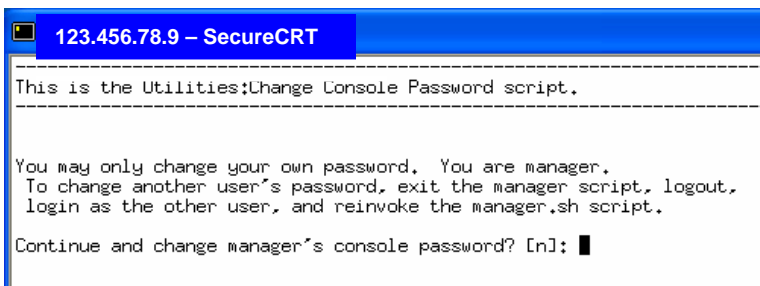
When (Ping) from the Utilities Menu is selected, the system will ask you to enter the IP address or Hostname of the device that you would like to Ping (Figure 3-16).

The Ping command is used to test the IP connection of a network device. If the Ping result is "0% packet loss", that means you have a network connection to the device identified by the IP



```
123.456.78.9 – SecureCRT
-----
This is the Utilities script.
-----
Make a choice from the following list:
1) QUIT                      7) Wireless_Stats
2) Previous_Menu             8) Serial_Bridge
3) Change_Console_Password   9) MS_VPN_Client_Setup
4) Change_Web_Password       10) RSVPD_Setup
5) Ping                      11) System_Date_Time_Setup
6) Network_Counters         12) Generate_New_Keys
#?
```

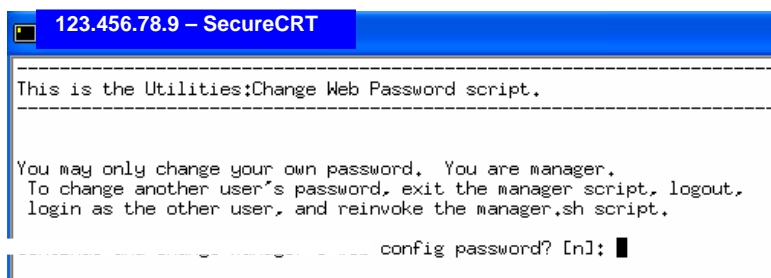
Figure 3-13. Utilities



```
123.456.78.9 – SecureCRT
-----
This is the Utilities:Change Console Password script.
-----
You may only change your own password. You are manager.
To change another user's password, exit the manager script, logout,
login as the other user, and reinvoke the manager.sh script.

Continue and change manager's console password? [n]: █
```

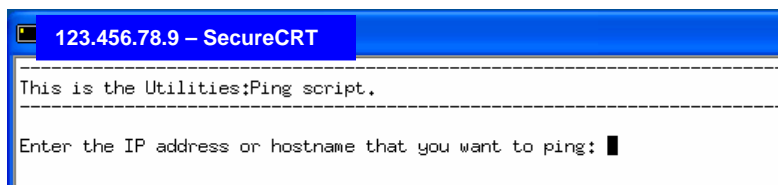
Figure 3-14. Console Password



```
123.456.78.9 – SecureCRT
-----
This is the Utilities:Change Web Password script.
-----
You may only change your own password. You are manager.
To change another user's password, exit the manager script, logout,
login as the other user, and reinvoke the manager.sh script.

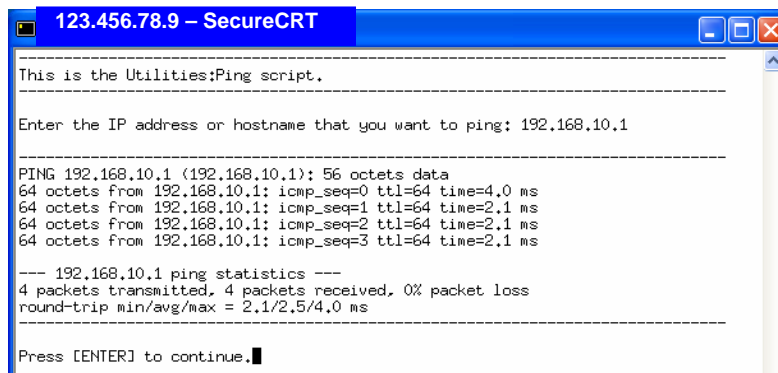
..... config password? [n]: █
```

Figure 3-15. Web Password



```
123.456.78.9 – SecureCRT
-----
This is the Utilities:Ping script.
-----
Enter the IP address or hostname that you want to ping: █
```

Figure 3-16. Ping



```
123.456.78.9 – SecureCRT
-----
This is the Utilities:Ping script.
-----
Enter the IP address or hostname that you want to ping: 192.168.10.1

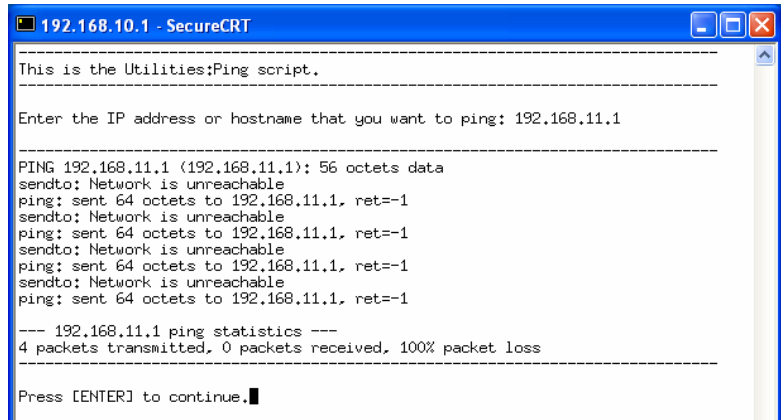
-----
PING 192.168.10.1 (192.168.10.1): 56 octets data
64 octets from 192.168.10.1: icmp_seq=0 ttl=64 time=4.0 ms
64 octets from 192.168.10.1: icmp_seq=1 ttl=64 time=2.1 ms
64 octets from 192.168.10.1: icmp_seq=2 ttl=64 time=2.1 ms
64 octets from 192.168.10.1: icmp_seq=3 ttl=64 time=2.1 ms

--- 192.168.10.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.5/4.0 ms
-----
Press [ENTER] to continue.█
```

Figure 3-17

address. Failure of a Ping does not necessarily indicate that your unit's network (either a local network or a WAN, including the Internet) connection is not working. It may simply be because the destination device is not connected to the network. So before using Ping to test your network connection, be sure that the destination device is properly connected to the network. When this option is

selected, you will be prompted to enter the Pinging System's IP Address, once entered you will see the status of the packets. (Figure 3-17) shows you an successful Ping command and (Figure 3-18) shows you a unsuccessful Ping command.



```
192.168.10.1 - SecureCRT
-----
This is the Utilities:Ping script.
-----
Enter the IP address or hostname that you want to ping: 192.168.11.1
-----
PING 192.168.11.1 (192.168.11.1): 56 octets data
sendto: Network is unreachable
ping: sent 64 octets to 192.168.11.1, ret=-1
sendto: Network is unreachable
ping: sent 64 octets to 192.168.11.1, ret=-1
sendto: Network is unreachable
ping: sent 64 octets to 192.168.11.1, ret=-1
sendto: Network is unreachable
ping: sent 64 octets to 192.168.11.1, ret=-1
-----
--- 192.168.11.1 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
-----
Press [ENTER] to continue.█
```

Figure 3-18

Once operation is complete, you can hit [**Enter**] to go back to the previous menu.

MS_VPN_Client_Setup

The (MS_VPN_Client_Setup) option from the Utilities Menu allows you to configure the Microsoft VPN Client on the UAD.

start

The (start) option from the MS VPN Client Configuration Menu allows you to START a configured VPN.

stop

The (stop) option from the MS VPN Client Configuration Menu allows you to STOP a configured VPN.

setup

The (setup) option from the MS VPN Client Configuration Menu allows you to setup and manage authentication, tunnels, etc.

Manage CHAP secrets

The (Manage CHAP secrets) option from the MS VPN Setup Menu allows you to manage the CHAP secrets.

Manage PAP secrets

The (Manage PAP secrets) option from the MS VPN Setup Menu allows you to manage the PAP secrets.

List PPTP Tunnels

When (List PPTP Tunnels) from the MS VPN Setup Menu is selected, all of the configured PPTP tunnels will be displayed.

Add NEW PPTP Tunnel

The (Add a NEW PPTP Tunnel) option from the MS VPN Setup Menu allows you to add a new PPTP tunnel.

Delete a PPTP Tunnel

The (Delete a PPTP Tunnel) option from the MS VPN Setup Menu allows you to delete a specific PPTP tunnel.

Configure resolv.conf

When (Configure resolv.conf) from the MS VPN Setup Menu is selected, you will be prompted to enter some parameters in order to configure the resolv.conf file.

Select a default tunnel

The (Select a default tunnel) option from the MS VPN Setup Menu allows you to select a default tunnel.

quit

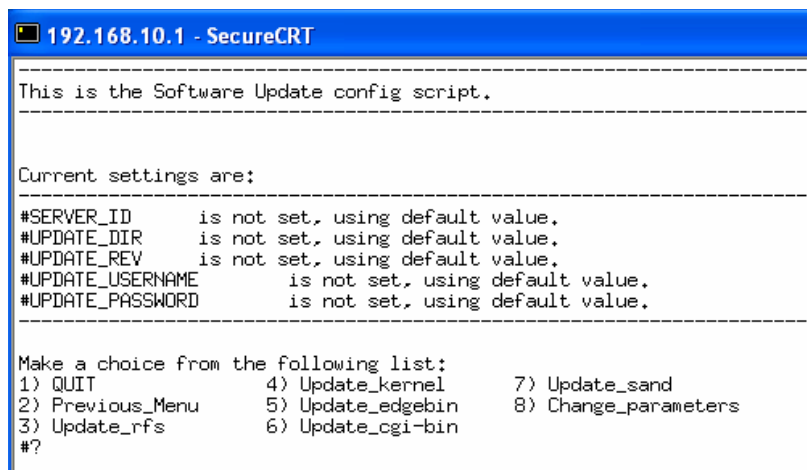
When (quit) from the MS VPN Client Configuration Menu is selected, the system will take you back to the MS VPN Client Configuration Menu.

RSVP_Setup

The (RSVP_Setup) option from the Utilities Menu allows you to Start or Stop the RSVP on the UAD.

Update

The (Update) option from the Main Configuration Menu allows you to Update software and set the Update parameters for the different software modules. When the Update option is selected from the Main Configuration Menu, the Update Menu shown in (Figure 3-37) will be displayed.



```
192.168.10.1 - SecureCRT
-----
This is the Software Update config script.
-----
Current settings are:
-----
#SERVER_ID      is not set, using default value.
#UPDATE_DIR     is not set, using default value.
#UPDATE_REV     is not set, using default value.
#UPDATE_USERNAME is not set, using default value.
#UPDATE_PASSWORD is not set, using default value.
-----
Make a choice from the following list:
1) QUIT          4) Update_kernel    7) Update_sand
2) Previous_Menu 5) Update_edgebin  8) Change_parameters
3) Update_rfs    6) Update_cgi-bin
#?
```

Figure 3-37

Update_rfs

When (Update_rfs) from the Update Menu is selected, the Setup Manager will connect to the FTP Server configured in the Update Parameters and Update the Root File System Image.

Update_kernel

When (Update_kernel) from the Update Menu is selected, the Setup Manager will connect to the FTP Server configured in the Update Parameters and Update the Operating System Kernel File.

Update_edgebin

When (Update_edgebin) from the Update Menu is selected, the Setup Manager will connect to the FTP Server configured in the Update Parameters and Update the Maintenance, Script Files and Telephony Application.

Change_parameters

The (Change_parameters) option from the Update Menu allows you to change the UAD Update parameters. When the Change_parameters option is selected from the Update Menu, the Update Parameters Menu shown in will be displayed.

SERVER_ID

When (SERVER_ID) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the IP address of the Update Server.

UPDATE_DIR

When (UPDATE_DIR) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the Directory Path for Update Files.

UPDATE_REV

When (UPDATE_REV) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the Update Version.

UPDATE_USERNAME

When (UPDATE_USERNAME) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the Username for the FTP Update Server.

UPDATE_PASSWORD

When (UPDATE_PASSWORD) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the Password for the Username in the FTP Update Server.

IPSecurity

The (IPSecurity) option from the Main Configuration Menu allows you to configure the IP Security parameters for the UAD. The Setup Manager will automatically display the IP Security Configuration Menu (*Figure 3-19*).

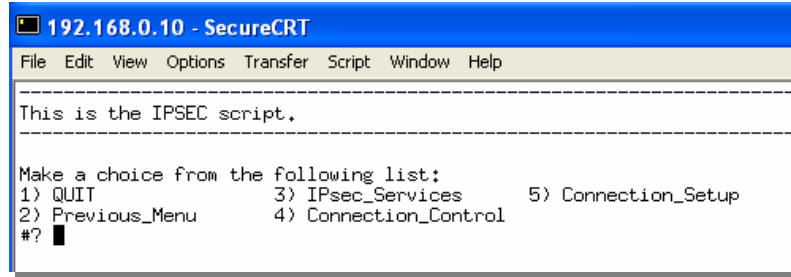


Figure 3-19. IPSEC

IPsec_Services

The (IPsec_Services) option from the IPSecurity Menu allows you to control the IP Services for the UAD. The Setup Manager will automatically display the IP Services Control Menu (*Figure 3-20*).

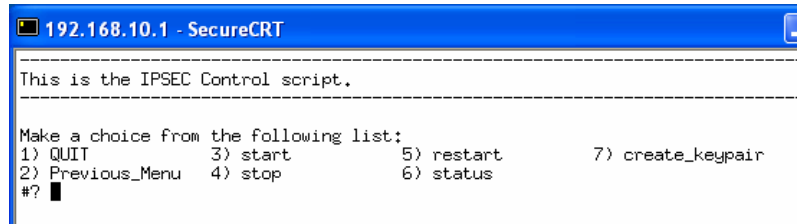


Figure 3-20

start

When (start) from the IPsec_Services Control Menu is selected, the system will START the IP Security Service on the UAD.

stop

When (stop) from the IPsec_Services Control Menu is selected, the system will STOP the IP Security Service on the UAD.

restart

When (restart) from the IPsec_Services Control Menu is selected, the system will RESTART the IP Security Service on the UAD.

status

When (status) from the IPsec_Services Control Menu is selected, the system will display the current status of the IP Security Service on the UAD.

create_keypair

When (create_keypair) from the IPsec_Services Control Menu is selected, you select a key for the data to be encrypted.

Connection_Control

The (Connection_Control) option from the IPSecurity Menu allows you to control the IPsec Connection for the UAD. The Setup Manager will automatically display the Connection Control Menu (*Figure 3-21*).

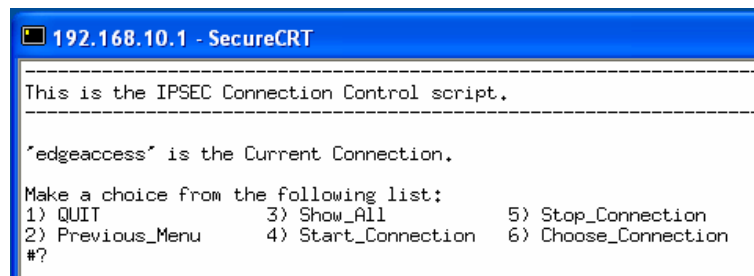


Figure 3-21

Start_Connection

When (Start_Connection) from the Connection Control Menu is selected, the system will START a specific IPsec connection.

Stop_Connection

When (Stop_Connection) from the Connection Control Menu is selected, the system will STOP a specific IPsec connection.

Choose_Connection

When (Choose_Connection) from the Connection Control Menu is selected, the system will display all of the available connections for you to choose a specific IPsec connection.

Connection_Setup

The (Connection_Setup) option from the IPsec Menu allows you to Setup the IPsec Connection on the UAD. When the Connection Setup option is selected from the IPsec Menu, the Connection Setup Menu shown in (Figure 3-22) will be displayed.

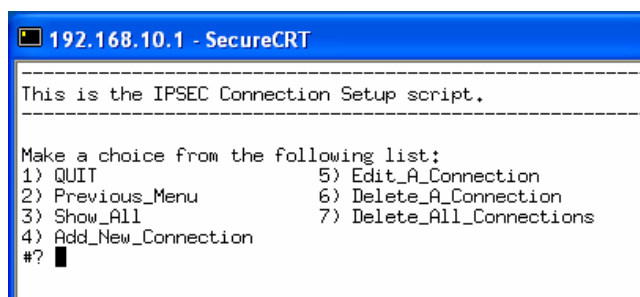


Figure 3-22

Add_New_Connection

The (Add_New_Connection) option from the Connection Setup Menu allows you to create a new IPsec Connection on the UAD.

When the Add New Connection option is selected from the Connection Setup Menu, the Add New Connection Menu shown in (Figure 3-23) will be displayed.

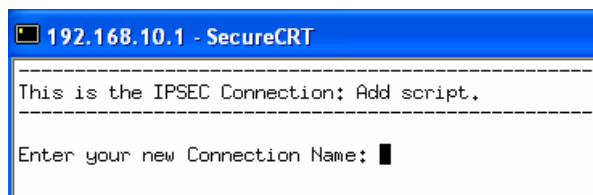


Figure 3-23

Edit_A_Connection

The (Edit_A_Connection) option from the Connection Setup Menu is selected, allows you to edit an existing IPsec Connection on the UAD. When the Edit A Connection option is selected from the Connection Setup Menu, the Edit A Connection Menu will be displayed.

From the Edit_A_Connection option, select the IPsec Connection you want to edit. When you choose the IPsec Connection, the following menu will be shown.

left

When (left) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the LEFT side of the connection (IP address of the left participant's public-network interface). You will be returned to the Add New Connection Menu after the left IP address is entered.

leftsubnet

When (leftsubnet) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the leftsubnet of the connection (private subnet behind the left participant, expressed as network/netmask; if omitted, essentially assumed to be left/32, signifying that the left end of the connection goes to the left participant only). You will be returned to the Add New Connection Menu after the leftsubnet is entered.

leftnexthop

When (leftnexthop) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the leftnexthop of the connection (next-hop gateway IP address for the left participant's connection to the public network). You will be returned to the Add New Connection Menu after the leftnexthop IP address is entered.

right

When (right) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the RIGHT side of the connection (IP address of the right participant's public-network interface). You will be returned to the Add New Connection Menu after the right IP address is entered.

rightsubnet

When (rightsubnet) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the rightsubnet of the connection (private subnet behind the right participant, expressed as network/netmask; if omitted, essentially assumed to be left/32, signifying that the right end of the connection goes to the right participant only). You will be returned to the Add New Connection Menu after the rightsubnet is entered.

rightnexthop

When (rightnexthop) from the Edit a Connection Menu is selected, you will be prompted to enter the values for the IP address of the rightnexthop of the connection (next-hop gateway IP address for the right participant's connection to the public network). You will be returned to the Add New Connection Menu after the rightnexthop IP address is entered.

esp

When (esp) from the Edit a Connection Menu is selected, you will be prompted to enter the encryption/authentication algorithm to be used for the connection.

spi

When (spi) from the Edit a Connection Menu is selected, you will be prompted to enter the SPI number to be used for the connection

espenckey

When (espenckey) from the Edit a Connection Menu is selected, you will be prompted to enter the ESP encryption key (may be specified separately for each direction using leftespenckey and rightespenckey parameters) for the connection.

espauthkey

When (espauthkey) from the Edit a Connection Menu is selected, you will be prompted to enter the ESP authentication key (may be specified separately for each direction using leftespauthkey and rightespauthkey parameters) for the connection.

Delete A Connection

The (Delete_A_Connection) option from the Connection Setup Menu allows you to delete a specific configured connection.

Delete All Connections

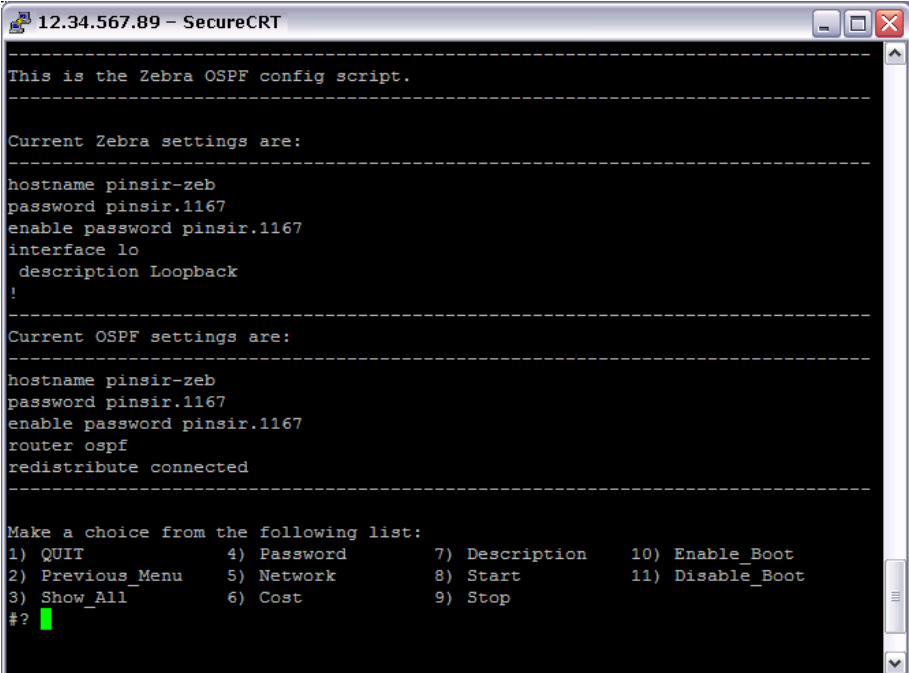
The (Delete_All_Connections) option from the Connection Setup Menu allows you to delete all of the configured connections.

OSPF

Open Shortest Path

First (OSPF) is a hierarchical Interior Gateway Protocol (IGP) routing protocol used to calculate the shortest path tree. It uses *cost* as its routing metric. A link state database is constructed of the network topology which is identical on all routers in the area.

OSPF is perhaps the most widely used IGP in large networks. A natural successor to RIP, it was VLSM capable or *classless* from its inception. A newer version of OSPF (OSPFv3) now supports IPv6 as well. Multicast extensions to OSPF



```
12.34.567.89 - SecureCRT
-----
This is the Zebra OSPF config script.
-----
Current Zebra settings are:
-----
hostname pinsir-zeb
password pinsir.1167
enable password pinsir.1167
interface lo
  description Loopback
  !
-----
Current OSPF settings are:
-----
hostname pinsir-zeb
password pinsir.1167
enable password pinsir.1167
router ospf
redistribute connected
-----
Make a choice from the following list:
1) QUIT          4) Password      7) Description   10) Enable_Boot
2) Previous_Menu 5) Network       8) Start        11) Disable_Boot
3) Show_All      6) Cost          9) Stop
#? █
```

3-24. OSPF

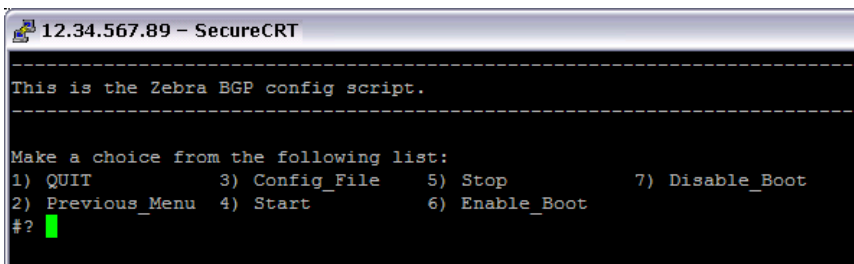
(MOSPF) have been defined, however these are not widely used. OSPF can "tag" routes, and propagate these tags along with the routes.

An OSPF network can be broken up into smaller networks. A special area called the *backbone area* forms the core of the network, and other areas are connected to it. Inter-area routing goes via the backbone. All areas must connect to the backbone; if no direct connection is possible, a *virtual link* may be established.

Routers in the same broadcast domain or at each end of a point to point link form *adjacencies* when they have discovered each other. The routers elect a *designated router* (DR) and *backup designated router* (BDR) which act as hub to reduce traffic between routers. OSPF uses both unicast and multicast to send 'hello packets' and link state updates. Multicast addresses 224.0.0.5 and 224.0.0.6 are used. In contrast to RIP or BGP, OSPF does not use TCP or UDP but uses IP directly, using IP protocol 89.

BGP

The **Border Gateway Protocol (BGP)** is the core Internet routing protocol. It works by maintaining a table of IP networks or 'prefixes' which designate network reachability between autonomous systems (AS). BGP does not use technical metrics, but makes routing decisions based on network policies or rules.



```
12.34.567.89 - SecureCRT
-----
This is the Zebra BGP config script.
-----
Make a choice from the following list:
1) QUIT          3) Config_File  5) Stop          7) Disable_Boot
2) Previous_Menu 4) Start        6) Enable_Boot
#? █
```

3-25. BGP

BGP supports classless interdomain routing and uses route aggregation to decrease the size of routing tables. Since 1994, version four of the protocol has been in use on the Internet; all previous versions are considered obsolete.

BGP was created to replace the EGP routing protocol to allow fully decentralized routing in order to allow the removal of the NSFNET Internet backbone network. This allowed the Internet to become a truly decentralized system.

Very large private IP networks can also make use of BGP; an example would be the joining of a number of large Open Shortest Path First (OSPF) networks where OSPF by itself would not scale to size. Another reason to use BGP would be multihoming a network for better redundancy.

Most Internet users do not use BGP directly. However, since most Internet service providers must use BGP to establish routing between one another, it is one of the most important protocols of the Internet. Compare and contrast this with Signalling System 7, which is the inter-provider core call setup protocol on the PSTN.

Overview

This web-based configuration utility performs all of the necessary functions to configure the EdgeAccess UAD. This utility also allows a user to check the status of the UAD equipment and channels.



Figure 4-1. Web Manager Login

Accessing the UAD Configuration Tool

To access the administration tool:

1. Open a browser window.
2. In the address field, type the IP address of the UAD.
3. When prompted, enter the username (voip) and password (n/a) as set by mfg at time of shipment.
4. The UAD Web Configuration Network Interface screen will appear as shown in (Figure 4-1)
5. Click on each tab to display configuration options.

Network Configuration Tab

The Network Configuration Tab allows you to configure specific network settings, which allows configuration of Port Interfaces, Host Settings, Wireless AP, T1/E1, Traffic Control, Routes, MPLS, Counters, Dial Up, Frame Relay, Wireless, Routing and Serial Bridge. Simply click on the individual [links](#) under each tab to access the corresponding configuration options.

Network Interface Screen

The Network Interface Screen allows configuration of individual UAD ports. The network administrator should be able to provide the necessary addresses necessary to configure each port.

NOTE: Of the pvc0 and eth0 ports, only one can be configured LAN while the other WAN regardless of network configuration.

EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Network Interfaces | Host Settings | Wireless | T1/E1 | Traffic Control
Static Routes | MPLS Settings | Network Status | Network Counters

pvc0
lan

IP Address: 123.456.789.10
Netmask: 255.255.255.255
Gateway: none

Obtain IP Address automatically
 Use static IP Address

IP Address: 123.456.789.10
Netmask: 255.255.255.224
Gateway:

Disable this interface
Additional T1/E1 options on T1/E1 page.

eth0
wan

IP Address: 123.456.789.10
Netmask: 255.255.255.0
Gateway: 123.456.789.10

Obtain IP Address automatically
 Use static IP Address

IP Address: 123.456.789.10
Netmask: 255.255.255.0
Gateway: 123.456.789.10

Disable this interface
 Add this interface to Ethernet Bridge
 Serve DHCP on this interface

eth1
net1

wlan0
net2

Figure 4-2. Network Interface

Host Settings Screen

Each UAD must contain a unique Hostname. The Host Settings Link allows changes to the Hostname and to certain domain name settings.

EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Network Interfaces | Host Settings | Wireless | T1/E1 | Traffic Control
Static Routes | MPLS Settings | Network Status | Network Counters

Hostname

Hostname: pinsir
Domainname: edgeaccess.net

Domain Name Servers

Currently Active Domain Name Servers

Nameserver 1: 4.2.2.2
Nameserver 2: 4.2.2.1
Nameserver 3:

Configured Domain Name Servers

Nameserver 1: 4.2.2.2
Nameserver 2: 4.2.2.1
Nameserver 3:

Save All | Reboot Unit

Figure 4-3. Host Settings

Wireless Screen

In computer networking, a **wireless access point (WAP or AP)** is a device that connects wireless communication devices together to form a wireless network. The WAP usually connects to a wired network,

Figure 4-4. Wireless Screen

and can relay data between wireless devices and wired devices.

Provided the UAD has a wireless interface, it may also be configured as an access point via the [Network] Configuration Tab's [Wireless] Link. Wireless Encryption Protocol (WEP), a security protocol for wireless LANs may also be enabled via the Wireless Screen. If WEP is enabled, you must enter a key as an access point.

T1/E1 Screen

A T1 is framed to provide 24 logical 64Kbps channels and an E1, 30 logical channels respectively. Each channel is designed to carry a single digitized telephone call. Since telephone calls

Figure 4-5. T1/E1 Screen

are digitized at a rate of 64Kbps, we can send a call over a single DS-0. Therefore, a T1 provides 24 X 64Kbps in usable bandwidth. This equates to 1.536Mbps. The total bandwidth of a T1 is actually 1.544Mbps, which includes 8Kbps in overhead.

If the UAD is equipped with a T1/E1 combination network interface card, certain signaling settings will need to be configured via the [Network] Configuration Tab's [T1/E1] Link in order for the UAD to communicate effectively with the WAN.

Traffic Control Screen

Enabling Basic VoIP via the [Network] Tab, [Traffic Control] Screen establishes voice traffic as priority over data for the UAD.

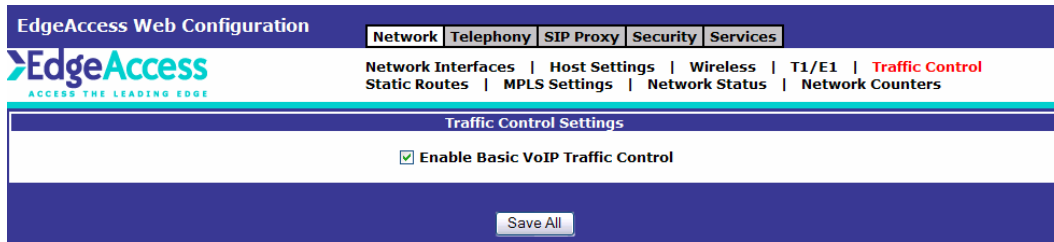


Figure 4-6. Traffic Control

Static Routes Screen

Static routes are special routes that the network administrator manually enters into the router configuration. You could build an entire network based on static routes. The problem with doing this is that when (not if!) a network failure occurs, the static route will not change without you performing the change. This isn't a good thing if the failure occurs during the middle of the night, or while you are on vacation.

This is why we've all heard the chant "Don't use static routes!" However, there are many places where static routes are essential to a smoothly operating network. Careful use and placement of static routes may actually improve the performance of your network, allowing you to conserve bandwidth for important business applications.

These settings may be done via the [Network] Configuration Tab's [Static Routes] Link.

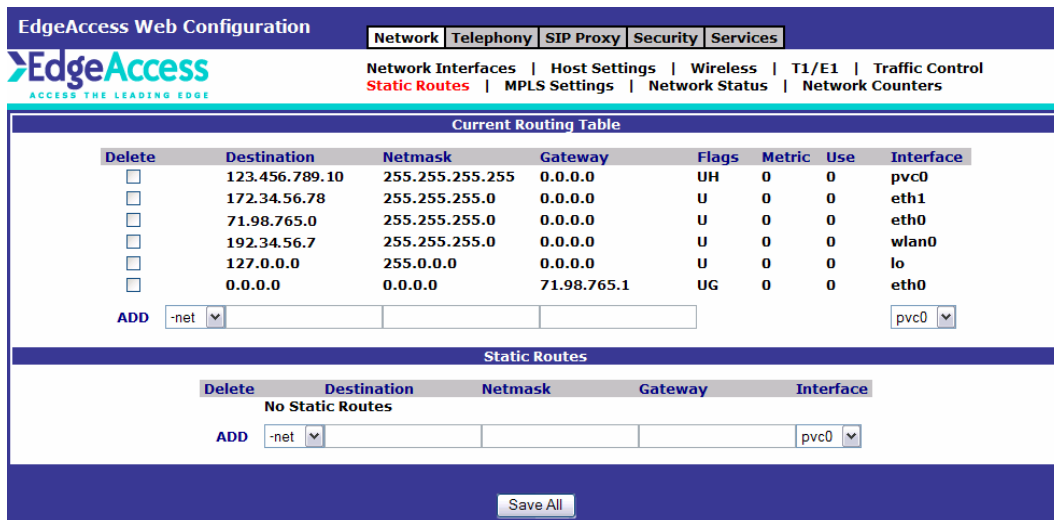


Figure 4-7. Static Routes

To add a route, enter the Destination, Gateway, Netmask and choose an Interface. Then click the [Save All] button.

MPLS Settings Screen

MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

From a QoS standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss.

When packets enter a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets.

The MPLS settings may be modified via the [Network] Configuration Tab's [MPLS Settings] Link.

EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Network Interfaces | Host Settings | Wireless | T1/E1 | Traffic Control
Static Routes | MPLS Settings | Network Status | Network Counters

Multi Protocol Label Switching (MPLS)
 Auto Start on Boot

Outbound LSP Setup
 Enable Outbound LSP
Interface: not_assigned
Nexthop IP Address: not_assigned
Outbound Label: 0

Inbound LSP Setup
 Enable Inbound LSP
Interface: not_assigned
Inbound Label Space: 0
Inbound Label: 0

Save All

Figure 4-8. MPLS Settings

Network Status Screen

Address and Hostname information of stations on the network may be found via The [Network] Configuration Tab's [Network Status] Link.

EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Network Interfaces | Host Settings | Wireless | T1/E1 | Traffic Control
Static Routes | MPLS Settings | Network Status | Network Counters

Stations on the Network

IP Address	MAC Address	DHCP Client	AP Client	Lease Start	Lease End	Hostname
71.98.765.1	00:80:12:31:35:71	<input type="checkbox"/>	<input type="checkbox"/>			

Refresh Network

Figure 4-9. Network Status

Network Counters Screen

To access the Counters option, click on the [Network] tab and then select the [Network Counters] link. This page displays what current traffic is taking place on the IP. This page will time out and need to be refreshed after a period of time.

EdgeAccess Web Configuration

Network | Telephone | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Network Interfaces | Host Settings | Wireless | T1/E1 | Traffic Control
Static Routes | MPLS Settings | Network Status | Network Counters

UAD Network Counters

This is a snapshot of the network counters.
To refresh counters you must refresh this page.

eth0

Link encap:Ethernet HWaddr 00:50:B7:F0:21:42
inet addr: 71.98.765.444 Bcast: 71.98.765.444 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:6767 errors:0 dropped:0 overruns:0 frame:0
TX packets:5826 errors:0 dropped:0 overruns:0 carrier:0
collisions:20 txqueuelen:1000
RX bytes:496249 (484.6 Kb) TX bytes:1073902 (1.0 Mb)
Interrupt:11 Base address:0xe400

eth1

Link encap:Ethernet HWaddr 00:50:B7:F0:21:41
inet addr: 172.34.56.78 Bcast:172.34.56.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2375 errors:0 dropped:0 overruns:0 frame:0
TX packets:2120 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:247032 (241.2 Kb) TX bytes:224924 (219.6 Kb)
Interrupt:5 Base address:0xe800

hdlc0

Link encap:Frame Relay Access Device
UP POINTOPOINT RUNNING NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:12 Base address:0xe000

pvc0

Link encap:Frame Relay DLCI HWaddr -3071
inet addr:206.113.125.35 P-t-P:206.113.125.34 Mask:255.255.255.255
UP POINTOPOINT NOARP MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)

wifi0

Link encap:Ethernet HWaddr 00:11:95:F2:01:A4
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:280773 errors:0 dropped:0 overruns:0 frame:49992
TX packets:15710 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:199
RX bytes:18182852 (17.3 Mb) TX bytes:17571349 (16.7 Mb)
Interrupt:11 Memory:d0820000-d0830000

wlan0

Link encap:Ethernet HWaddr 00:11:95:F2:01:A4
inet addr: 192.345.67.89 Bcast:192.345.67.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:9479 errors:0 dropped:0 overruns:0 frame:0
TX packets:12015 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:828792 (809.3 Kb) TX bytes:16773809 (15.9 Mb)

Wireless Settings

Figure 4-10. Network Counters

Telephony Configuration Tab

The Telephony Configuration Tab allows you to configure the telephony setting for the UAD. Simply click on the individual [links](#) under each tab to access the corresponding configuration options.

Status Screen

The Status screen provides port setting information as well as current software version.

Figure 4-11. Telephony Status

Channels Screen

Protocol selection, changes to connection type and bandwidth control and call feature settings may be done via the [Telephony] Configuration Tab's [Channel] Link. Fax settings may also be configured via this same screen. However, we recommend contacting EdgeAccess support for assistance in configuring the fax settings as selections may vary based on service providers.

Figure 4-12. Telephony Channels

To configure the Features Settings, edit the fields using the information below for reference.

Call Waiting -If selected, this feature alerts the user to a second incoming call while they are on the phone.

Caller ID Display -Select this box to enable Caller ID function.

Caller ID Blocking -Select this box to block phone number from being seen by called party.

Call Forwarding – Allows user choose which events cause a call to be forwarded. Forwarding Number Enter the telephone number of location where calls are to be forwarded.

Number of Rings – The number of times the phone rings before it is sent to the forwarding number.

Missed Call – Select this box and enter the email address desired to receive an email alert of a missed inbound call.

When you have made your changes, click on the [Save All] button.

VSP Client Screen

A service provider may manage its gatekeeper information via the [Telephony] Configuration Tab's [VSP Client] Link. Edit the fields using the information below for reference.

The screenshot shows the 'VSP Client' configuration page in the EdgeAccess Web Configuration interface. The page is divided into two main sections: 'VSP Port Configuration' and 'GateKeeper Registration'.

VSP Port Configuration:

Port	Value	Set to Default
Listening	5000	<input type="checkbox"/>
Sending	5000	<input type="checkbox"/>

Set Sending Port Same as Listening Port

Differentiated Services

Precedence
Critical/Emergency Call Processing

Type of Service (TOS)

- Minimize Delay
- Maximize Throughput
- Maximize Reliability
- Minimize Monetary Cost

GateKeeper Registration:

Gatekeeper Registration Enabled

Primary Gatekeeper: xx.gatekeeper.net

Backup Gatekeeper: xx2.gatekeeper.net

Firewall Pinhole and DA Trigger Features

Pinhole Feature Enabled

IP: not_assigned

Port: 5000

Interval (1/10 seconds): 10

DA Trigger Feature Enabled

IP:

Trigger Levels: 1

Ports:

Interval (1/10 seconds):

Save All

Figure 4-13. Telephony VSP Client

Listening Port - Enter the socket port # that the application will use to listen for voice packets.

SoftSwitch Registration - Check this box to enable user registration. When this box is checked, SoftSwitch and Backup SoftSwitch boxes will be editable.

Primary SoftSwitch -Enter primary SoftSwitch IP address.

Backup SoftSwitch -Enter backup SoftSwitch IP address.

When you have made your changes, click the [Save All] button.

SIP Client Configuration

SIP Client Settings may be modified via the [Telephony] Configuration Tab's [SIP Client] Link. Edit the fields using the information below for reference.

SIP Client Settings - General

SIP Listening Port: 5090
 RTP Port: 16000
 Retry Attempts: 3
 Retry Timer: 25
 SIP Expires: 500
 RTP Inactivity Timer: 120
 Hold Timer: 600
 Outbound Proxy: 192.34.56.78
 Outbound Proxy Port: 5060

Invites without SDP
 Inband G711 DTMF
 Answer Supervision
 Registrations Enabled
 Proxy Enabled
 No To: tag on Auth Invites

SIP Client Settings - User

Channel	URI	User	Auth Username	Auth Password	ProxyOrder
1	4550		line12abcstore25	••••••••	0
2	4551		line34abcstore25	••••••••	0
3	4552		line56abcstore25	••••••~•	0
4					
5					
6					
7					
8					

Differentiated Services

Precedence
 Critical/Emergency Call Processing

Type of Service (TOS)

Minimize Delay
 Maximize Throughput
 Maximize Reliability
 Minimize Monetary Cost

SIP Proxy List

Entry	Proxy Address	Sending Port
0	virtualproxy1.globalipx	5060
1		
2		
3		
4		
5		
6		
7		

Save All

Figure 4-14. Telephony SIP Client

SIP Transport – Select the desired transport type.

SIP Port – Enter the Port # for SIP call signaling.

RTP Port – Enter the Port # for RTP Stream Data.

Retry Attempts – Enter the # of retries for unanswered SIP messages.

SIP Expires – Enter the amount of time in seconds that the registration should last before expiring.

RTP Inactivity Timer – Enter the amount of time a call should hang up if no packets are received within the predetermined time limit.

Hold Timer – Enter the amount of time the system should hang up a call that has been placed on hold.

Proxy Address – Enter the IP address or Proxy name in which to register. This system is equipped to register to multiple SIP Proxies.

Proxy Order – Specify the order of the Proxies.

VPEP Client Configuration

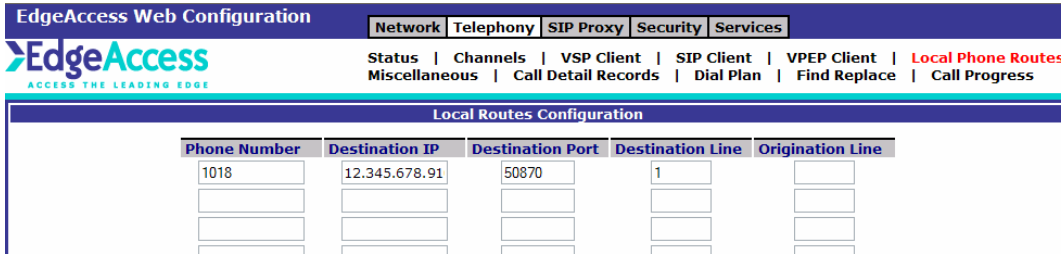
vPEP™ is a proprietary protocol designed to increase the performance and efficiency of satellite-based voice over internet protocol (VoIP) applications. vPEP™ takes advantage of several innovative optimization techniques to reduce the bandwidth utilization and speed data delivery over an IP network. This communication protocol is based on a Client/Server or Client/Client communication standard built to take advantage of the redundancies in the IP protocol, thus enhancing and accelerating the data transfers across links and at the same time remaining transparent to the end user. If UAD includes the VPEP™ Module, contact EdgeAccess support for configuration assistance. [BOB, DO WE HAVE A WAY TO TURN THIS ON/OFF CONSIDERING OUR CUSTOMERS ARE SUPPOSE TO PAY FOR VPEP?]

The screenshot shows the 'EdgeAccess Web Configuration' interface. At the top, there are navigation tabs for 'Network', 'Telephony', 'SIP Proxy', 'Security', and 'Services'. Below these are links for 'Status', 'Channels', 'VSP Client', 'SIP Client', 'VPEP Client', 'Local Phone Routes', 'Miscellaneous', 'Call Detail Records', 'Dial Plan', 'Find Replace', and 'Call Progress'. The main content area is divided into two columns: 'VPEP Features' and 'VPEP Control'. The 'VPEP Features' column contains three sections: 'VSP Options' with checkboxes for 'VSP VPEP Enabled' and 'VSP VPEP Symmetrical'; 'SIP Options' with checkboxes for 'SIP VPEP Enabled' and 'SIP VPEP Symmetrical'; and 'General Options' with checkboxes for 'Use VPEP Proxy' and 'Use IP Routing'. The 'VPEP Control' column contains three sections: 'Proxy Options' with input fields for 'Proxy Control Port', 'Proxy Control IP', and 'Proxy Voice IP'; 'Client Options' with an input field for 'Client Control Port' and a dropdown menu for 'Client Control Interface' currently set to 'eth0'. A 'Save All' button is located at the bottom center of the configuration area.

Figure 4-15. Telephony VPEP Client

Local Phone Routes

To access the Local Telephony Routing option, select the Telephony tab and then click on the Local Telephony Routing link. This option allows you to configure the local routing capabilities and routing phone numbers.



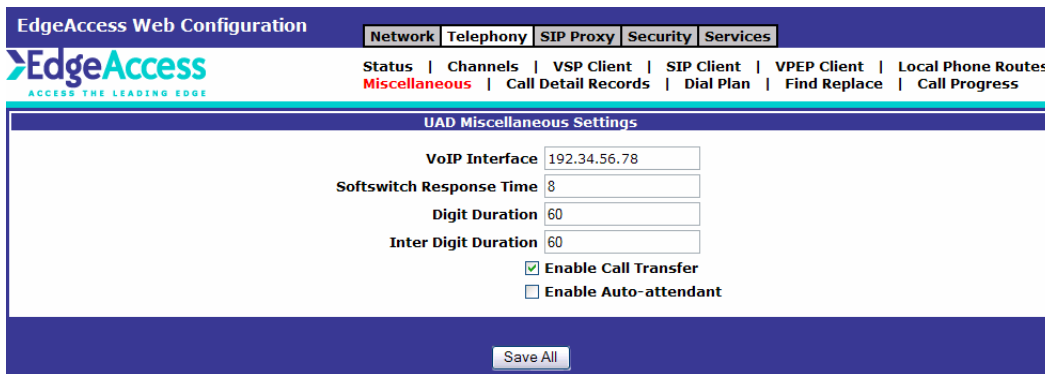
The screenshot shows the 'Local Routes Configuration' page in the EdgeAccess Web Configuration interface. The page has a navigation bar with tabs for Network, Telephony, SIP Proxy, Security, and Services. Under the Telephony tab, there are links for Status, Channels, VSP Client, SIP Client, VPEP Client, Local Phone Routes, Miscellaneous, Call Detail Records, Dial Plan, Find Replace, and Call Progress. The main content area is titled 'Local Routes Configuration' and contains a table with the following columns: Phone Number, Destination IP, Destination Port, Destination Line, and Origination Line. The first row of the table has the following values: 1018, 12.345.678.91, 50870, 1, and an empty field. Below the first row, there are three more rows of empty input fields for each column.

Phone Number	Destination IP	Destination Port	Destination Line	Origination Line
1018	12.345.678.91	50870	1	

Figure 4-16. Local Phone Routes

Miscellaneous

To access the Miscellaneous options, click on the Miscellaneous tab. From this tab you can set Log Rotation, Update, Status and Find Replace settings.



The screenshot shows the 'UAD Miscellaneous Settings' page in the EdgeAccess Web Configuration interface. The page has a navigation bar with tabs for Network, Telephony, SIP Proxy, Security, and Services. Under the Telephony tab, there are links for Status, Channels, VSP Client, SIP Client, VPEP Client, Local Phone Routes, Miscellaneous, Call Detail Records, Dial Plan, Find Replace, and Call Progress. The main content area is titled 'UAD Miscellaneous Settings' and contains the following settings:

- VoIP Interface: 192.34.56.78
- Softswitch Response Time: 8
- Digit Duration: 60
- Inter Digit Duration: 60
- Enable Call Transfer
- Enable Auto-attendant

At the bottom of the page, there is a 'Save All' button.

Figure 4-17. Miscellaneous

VOIP Interface – Select the Interface by typing WAN, LAN or the IP address that the application will use when calculating which address to register with the softswitch.

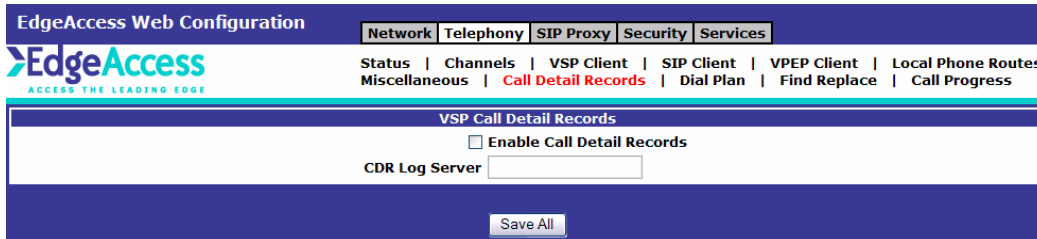
Softswitch Response Timeout – Enter the amount of time in seconds that the Softswitch response should timeout.

Digit Duration – Enter the amount of time in milliseconds that a DTMF tone will be played by the DSP when pumping digits out a phone line.

InterDigit Duration – Enter the amount of time in milliseconds for the time between DTMF digits when pumping digits out a phone line.

Call Detail Records

The call detail record (CDR) feature creates text records of call related data. The data recorded includes calling and called numbers, call origination/connect time, the time the call was disconnected, etc. The CDRs are collected in files for billing purposes. To log CDRs, simply check the 'Enable' box via the [Telephony] Configuration Tab's [Call Detail Records] and identify the IP address for the server where the records are to be stored.



EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Status | Channels | VSP Client | SIP Client | VPEP Client | Local Phone Routes
Miscellaneous | Call Detail Records | Dial Plan | Find Replace | Call Progress

VSP Call Detail Records

Enable Call Detail Records

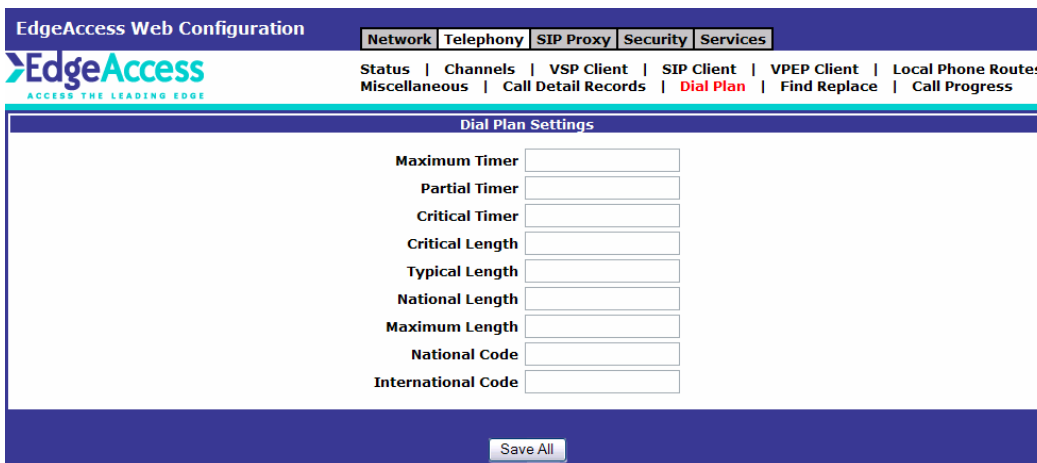
CDR Log Server

Save All

Figure 4-18. Call Detail Records

Dial Plan Configuration

To configure the Dial Settings on the UAD, edit the fields using the information below for reference.



EdgeAccess Web Configuration

Network | Telephony | SIP Proxy | Security | Services

EdgeAccess
ACCESS THE LEADING EDGE

Status | Channels | VSP Client | SIP Client | VPEP Client | Local Phone Routes
Miscellaneous | Call Detail Records | Dial Plan | Find Replace | Call Progress

Dial Plan Settings

Maximum Timer

Partial Timer

Critical Timer

Critical Length

Typical Length

National Length

Maximum Length

National Code

International Code

Save All

Figure 4-19. Dial Plan

Find Replace

To access the Find Replace option, click on the [Telephony] Configuration Tab's [Find Replace] Link. Use this option to replace digits for in and/or out dialing. This feature is beneficial when dialing into different dialing plans.

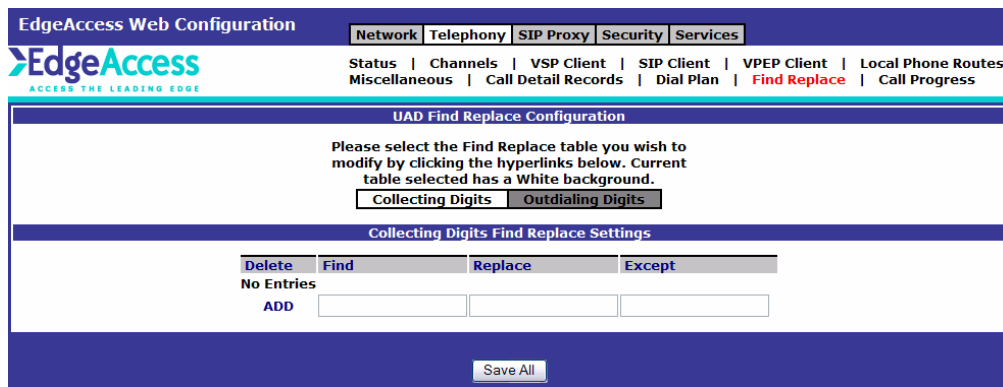


Figure 4-20. Find Replace

Collecting Digits – Click on the Collecting Digits button to change digits before the Softswitch lookup.

Outdialing Digits – Click on the Outdialing Digits button to change numbers received from Softswitch.

Find – Starting at the beginning of a string, enter digits to look for.

Replace – Starting at the beginning of a string, enter replacement digits.

Except – Enter any exceptions to the find and replace.

When you have entered your changes, click on the Commit Changes button.

Call Progress

To access the

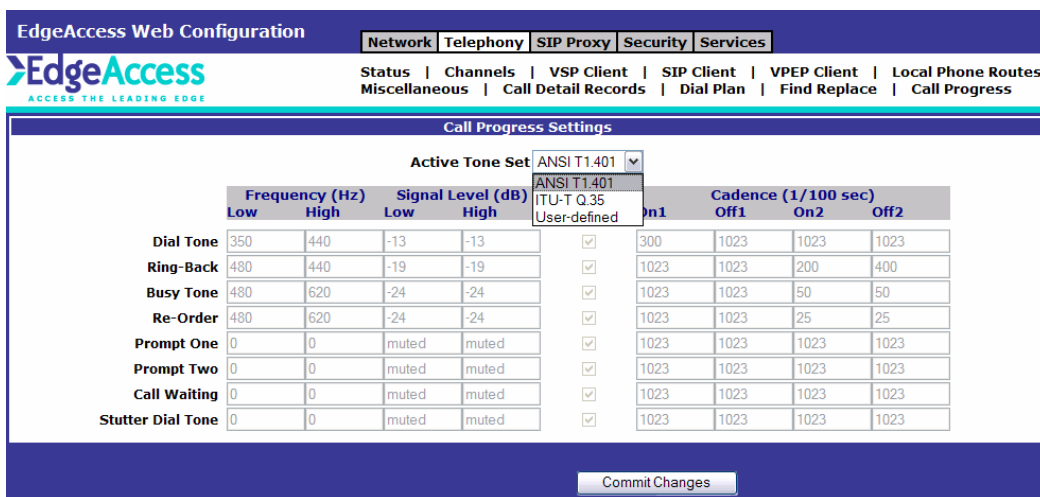
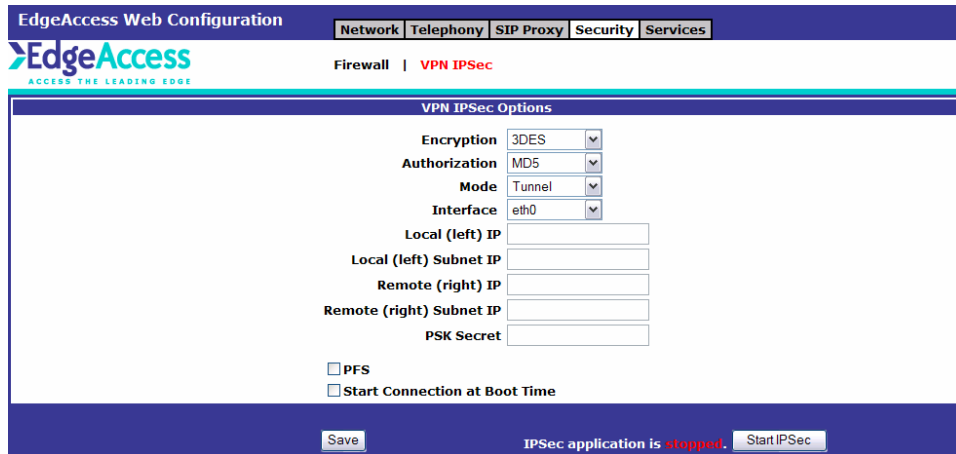


Figure 4-21. Call Progress

VPN

Changes may be made to the Firewall via the [Security] Configuration Tab's [VPN IPSec] Link. Edit the fields using the information below for reference.



The screenshot displays the EdgeAccess Web Configuration interface. At the top, there is a navigation bar with tabs for Network, Telephony, SIP Proxy, Security, and Services. The Security tab is active, and the VPN IPSec link is selected. The main content area is titled "VPN IPSec Options" and contains the following configuration fields:

- Encryption: 3DES
- Authorization: MD5
- Mode: Tunnel
- Interface: eth0
- Local (left) IP: [Empty text box]
- Local (left) Subnet IP: [Empty text box]
- Remote (right) IP: [Empty text box]
- Remote (right) Subnet IP: [Empty text box]
- PSK Secret: [Empty text box]

Below the fields, there are two checkboxes: PFS and Start Connection at Boot Time. At the bottom of the configuration area, there is a "Save" button and a status indicator that reads "IPSec application is stopped." with a "StartIPSec" button next to it.

Figure 4-21. VPN

[Space Intentionally Left Blank]

Services

DHCP Services

To access the DHCP option, select the Services tab and click on the DHCP Server link. This option allows you to configure the necessary parameters of the UAD.

Enter the required DHCP Server parameters and any optional parameters. When you have entered your changes, click on the Commit Changes button.

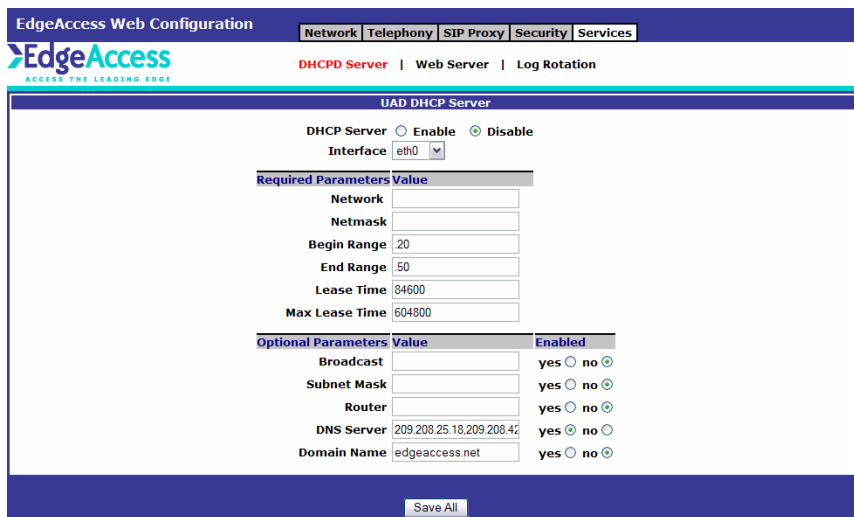


Figure 4-20. DHCP Server

WEB Server

To access the Web Server option, select the Services tab and click on the Web Server link. To enable Secure Socket Layer (SSL), click on the box.



Figure 4-21

When you have entered your changes, click the [Save All] button.

Log Rotation

To access the Web Server option, select the Services tab and click on the Web Server link.

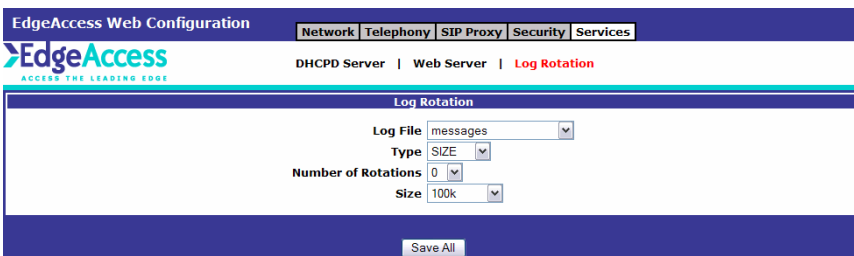


Figure 4-21

Legacy Configuration Reference

The following configuration screens may be inherent in older software releases. In order to become current, please contact EdgeAccess support to determine if the UAD is still eligible for an extended warranty program.

Updates

Depending upon the software release of the UAD, an [Update] link may be available for updating parameters for different software modules. Should that option be available

The screenshot shows the 'UAD Configuration Utility' interface. At the top, there are navigation tabs: 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. Below these are links for 'Log Rotation', 'Update', 'Status', and 'Find Replace'. The main content area is titled 'UAD Update' and contains a 'UAD Update Settings' dialog box. This dialog box has the following fields: 'Root File System' (checkbox), 'Edgebin' (checkbox), 'Kernel' (checkbox), 'Update Server' (text box with '5'), 'Directory' (text box), 'Revision' (text box), 'Username' (text box with '2'), and 'Password' (text box). At the bottom of the dialog is a 'Commit Changes' button. The bottom right of the main window has 'Help' and 'SiteMap' links.

Figure L-1. Update

Root File System – Select this box to update the Root File System Image.

Edgebin – Select this box to connect the Setup Manager to the FTP Server configured in the Update Parameters and Update the Maintenance, Script Files and Telephony Application.

Kernel – Select this box to connect the Setup Manager to the FTP Server configured in the Update Parameters and Update the Operating System Kernel File.

Update Server – Enter the IP address of the Update Server.

Directory – Enter the Directory Path for the Update Files.

Revision – Enter the Update Version.

Username – Enter the Username for the FTP Update Server.

Password – Enter the Password for the FTP Update Server.

When you have entered your changes, click on the Commit Changes button.

Dial UP

To access the Dial UP option, select the Network tab and then click the Dial Up link. This allows you to configure parameters necessary to connect to an ISP (Internet Service Provider).

Interfaces

Select whether you are using WAN or LAN interface.

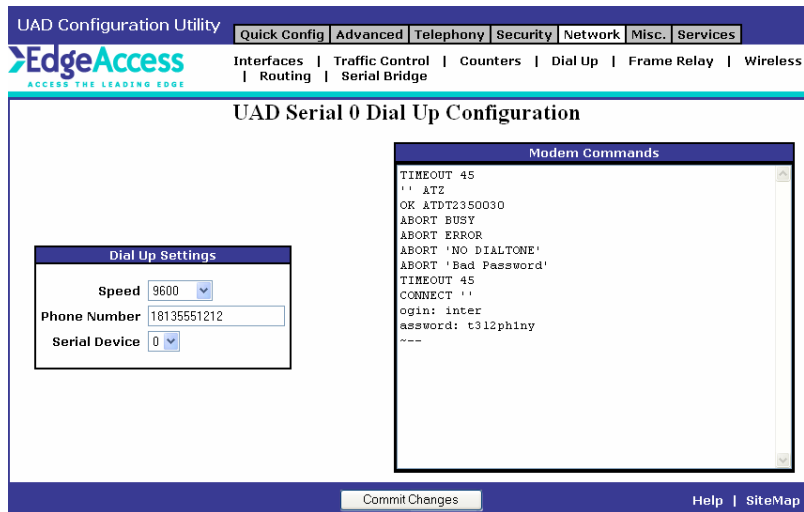


Figure L-2. Dial up

DNS Settings – The Domain Name System allows you to add and entry to the system.

Interface Configuration – Enter the IP Address, Netmask, Network Broadcast and Gateway information that applies to the interface you are using.

When you have made your changes, click Commit Changes button.

Serial Bridge

The Serial Bridge mode allows you to configure the UAD to communicate with wireless satellites modems to transmit GPS coordinates.

To access the Serial Bridge options, click on the Network tab and then select the Serial Bridge link.

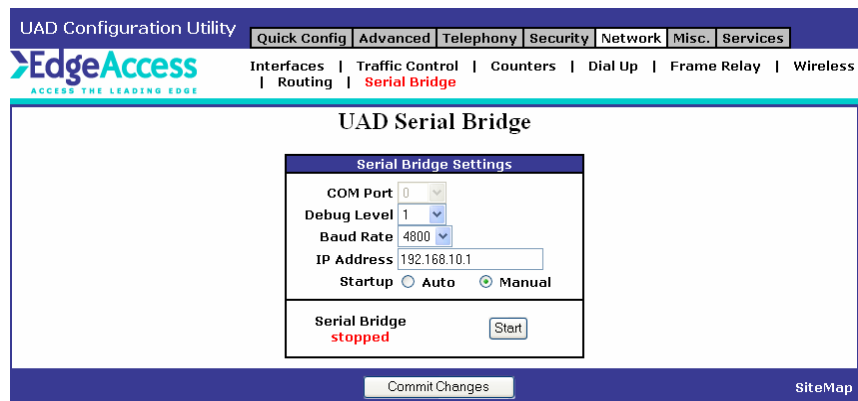


Figure L-3. Serial Bridge

Connectivity Configuration

To configure the Connectivity Settings on the UAD, edit the fields using the information below for reference.

Protocols – Select the Voice protocol for the UAD (VSP, SIP or MGCP).

SoftSwitch Lookup -Select this box if the UAD is going to be a part of a network where a SoftSwitch is being used.

Direct Connect -Select this box to enable Direct Connect to the UAD specified in the Remote Connection below.

Remote IP Address-When Direct Connect is selected, enter the remote IP that the local channel connects to when a call is received.

Remote Logical Telephony Port -When Direct Connect is selected, enter the logical port number (trunk) of the channel on the remote UAD. This port number associated with the Remote IP determines the call routing.

Remote IP Port -When Direct Connect is selected, enter the IP port number on which the remote UAD listens for VoIP packets.

DNIS (optional) -When Direct Connect is selected, you may enter a DNIS to outdial.

Assigned Number - Enter the Virtual phone number assignment for this port. May be an actual PSTN number depending on service provider.

Digits to Collect – Enter the number of digits that the IAD should accept before assuming that dialing is complete.

Voice Prompt Directory – Enter the subdirectory where the speech files (wave) are located. Use “default” when electing to use default files provided in the system. This feature is only available in G.723.1 coder.

Prefix Connect -Select this box to enable the prefix connect feature. When selected, the **Prefix Connect box** should contain the digit or string of digits used for out dialing. Typical use is for FXO lines, when you must dial a ‘9’ for an outside line.

Find/Replace Prefix – Select this box to enable the replacement of a string of digits for in and out dialing. This feature is often useful when dialing from a system and terminating into another system with a different dialing plan.

Advanced Configuration

To configure the Advanced Settings on the UAD, edit the fields using the information below for reference.

Input Gain – Enter the amount of input gain to apply to the signal received. This item is sometimes necessary to adjust the input volume when a poor connection is present.

DTMF Volume – Enter the desired dB level used for regenerating DTMF across the network.

DTMF Gain – Use this option along with the DTMF Volume setting to adjust the input gain.

Number of Blocks – Enter the number of frames the DSP should collect prior to sending interrupt.

Bypass Coder – When in Bypass mode, use to select active coder type.

When you have made your changes, click on the Commit Changes button.

Channel Configuration

Channel Settings

To configure the Telephony settings on an UAD, select a Channel from the **Channel Select** field.

Channel Enabled – Select this box to enable the port.

Logical Port # - Select a logical port number to be associated with this channel. The selection is similar to the trunking association of the channel.

Volume – Select the output volume to be associated with this port. This setting is usually necessary when individual channels need higher output levels or gain adjustment.

Coder Type – Select the speech coder to be used for transmission. *Note: The higher the speech rate, the more bandwidth used for voice transmission.*

Connection Type -Use this option to select whether connecting to a phone (FXS) or a phone line (FXO).

FXO Connection

To access the FXO Settings option, select the Telephony tab and then click on the **FXO link**. The FXO Connection Screen will be displayed as shown in (Figure 4-6).

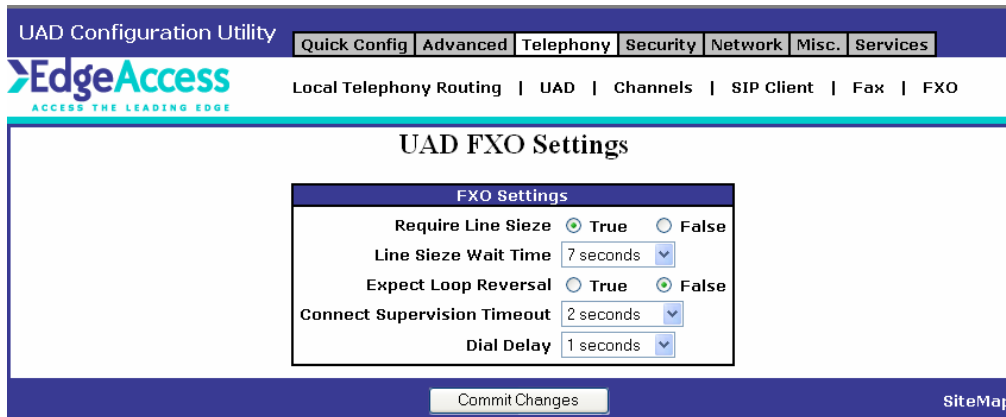


Figure L-4. FXO Settings

Require Line Seize

True – Line seize indication will be required before dialing. Enter the amount of time to wait for the line seize in the Line_Seize Wait Time field. If no line seize indication is received before wait time expires, call originator will be sent an error indication, and the call will be dropped.

False – Line seize indication is not required before dialing.

Expect Loop Reversal

True – Yes

False - No

Connect Supervision Timeout -If no indication is received positive or negative, the amount of time to wait before issuing connect signal to call originator.

Dial Delay - Enter amount of time to wait after line seize to ensure line is stable before dialing number.

Auto Attendant Extension – Type (1) to enable or (0) to disable the Auto Attendant function.

Call Transfer – Type (1) to enable or (0) to disable the Centrex-type Call Transfer function.

INDEX

A

Authorization Codes6

C

Call Barring.....6

Call Forwarding6, 55

Call Progress Detection.....5, 14, 60

Call Restriction6

Call Waiting6, 55

Caller ID.....6, 55

Classes.....35

Coder Type.....12, 67

Connect Supervision Timeout.....15, 68

Connection Type.....12, 54, 67

D

DHCP Client 8, 8, 23-24

DHCP Server 8, 18, 21-23, 33, 63

Direct Dial.....14, 18

DNIS13, 66

DTMF Gain.....67

DTMF Volume.....67

E

Encoding12

F

Fax.....5, 54

Filtering.....7

Filters35

Firewall4, 5, 7, 34, 61-62

Frame Relay.....

FXO.....4, 5, 12, 13, 15, 66-68

FXS5, 12, 16, 67

H

Hostname11, 20, 38, 48, 51

I

Input Gain67

Installation.....4, 11

IP Security.....42

L	
LAN Settings	10, 33
Line_Seize.....	15, 68
Listening Port.....	12, 56
Log CDR.....	13, 59
Logical Port.....	12, 13, 66-67
N	
NAT	4, 5, 7
Network.....	6, 48, 80
P	
Password	10, 11, 18, 38, 41, 47, 64, 69
PING	38
Port Map.....	34
Prefix Connect	13, 66
Q	
Qdisc	35, 36
S	
Security	61
Setup Manager	17-22, 24, 33, 40-42, 64
SIP.....	5, 6, 56, 57, 66
Softswitch Lookup.....	13, 60, 66
Softswitch Registration.....	12, 56
Static Routes	22, 33, 50
T	
Traffic Control	35, 36, 48, 50
U	
Update.....	40, 64
Utilities.....	38-39
W	
WAN Settings	20-31
Web Manager	17, 47