



Operations Manual

BlueBox 400 Universal Integrated Device (UAD)



BlueBox 400 (BB400)
Universal Access Device (UAD)
VOICE OVER IP TECHNOLOGIES

EdgeAccess, Inc.
5425 Beaumont Center Blvd, #918 • Tampa, FL 33634
Customer Support: support@edgeaccess.net

Table of Contents

Introduction	4
Quick Start	
Install UAD.....	8
Connecting Devices.....	15
Check Connections.....	15
Management Options	
Setup Manager	16
Web-Based Manager.....	17
Set Up Manager	
Setup Manager	18
Setup Menu	18
Hostname	20
WAN Menu	20
WAN DHCP Menu	24
WAN T1 Configuration Menu	27
LAN Menu.....	37
LAN DHCP Menu.....	37
Static Routes	38
Firewall Menu	39
Traffic Control	41
Miscellaneous Menu	44
Utilities Menu	48
MS VPN Client Menu.....	54
Update Menu	56
Wireless.....	61
IPSecurity	67
Web-Based Manager	
Web-Based Manager.....	75
Telephony Tab.....	76
Security Tab.....	85
Network Tab	86
Miscellaneous Tab.....	90
Services	94
Trouble Shooting BlueBox 400 UAD	
Monitoring via Telnet	96
UAD Debug Levels	96
Call Transfer	97
Index.....	99

Introduction

This guide provides users with operational procedures, which will be used when working with the EdgeAccess BlueBox 400 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.
- Chapter 5 covers basic troubleshooting techniques for the UAD.
- 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 BlueBox 400 UAD equipment

Technical Support

For complete technical support information, check our Web site at www.edgeaccess.com or call (340) 714-7573.

Overview

The EdgeAccess BlueBox 400 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

4 FXO, 4 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)
H.323*

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:

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 Linux 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 Linux 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

Use (Figure 1-1) for the following devices.

- The internal two pins in the UAD ports are FXS.
- 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.



Figure 1-1

Check the Connections

Use (Figure 1-2) for the following connections.

- Check the port LEDs to confirm the link status.
- 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 1-2

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 IP Telnet, 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.

Setup Manager

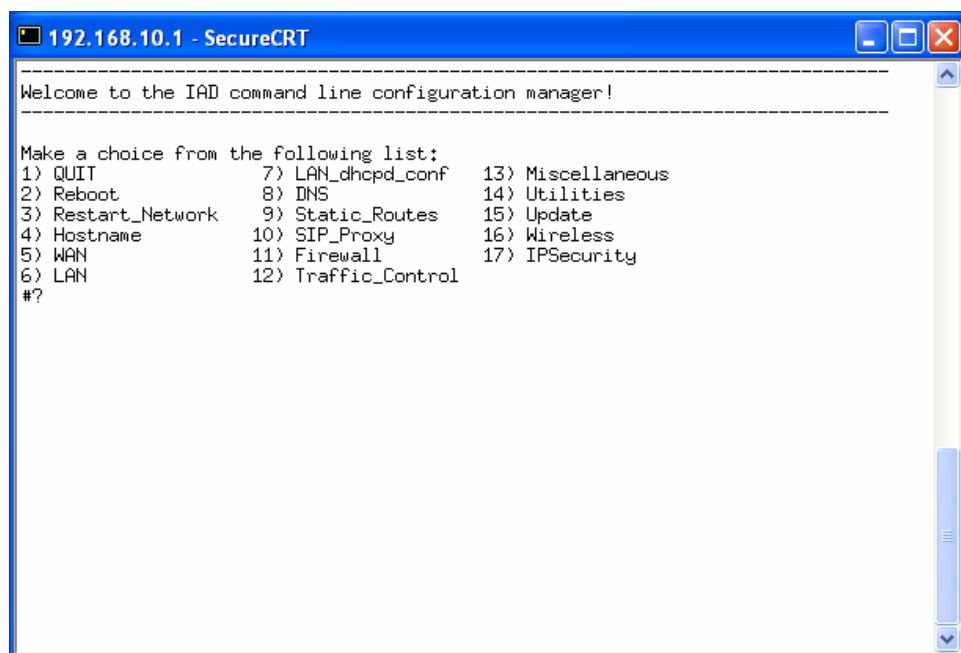


Figure 2 -1

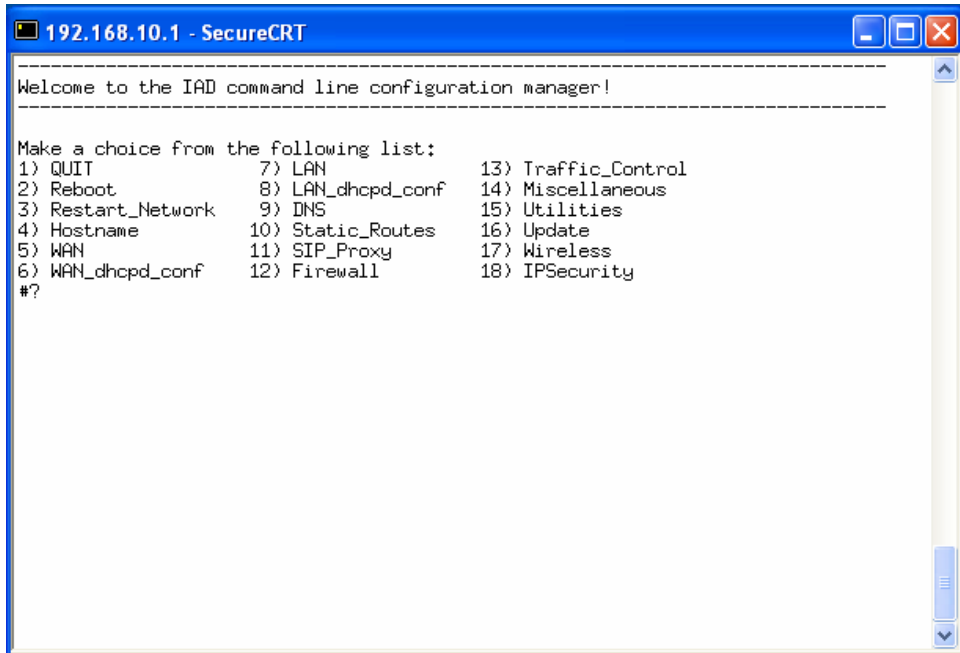


Figure 2 -2

Web-Based Manager

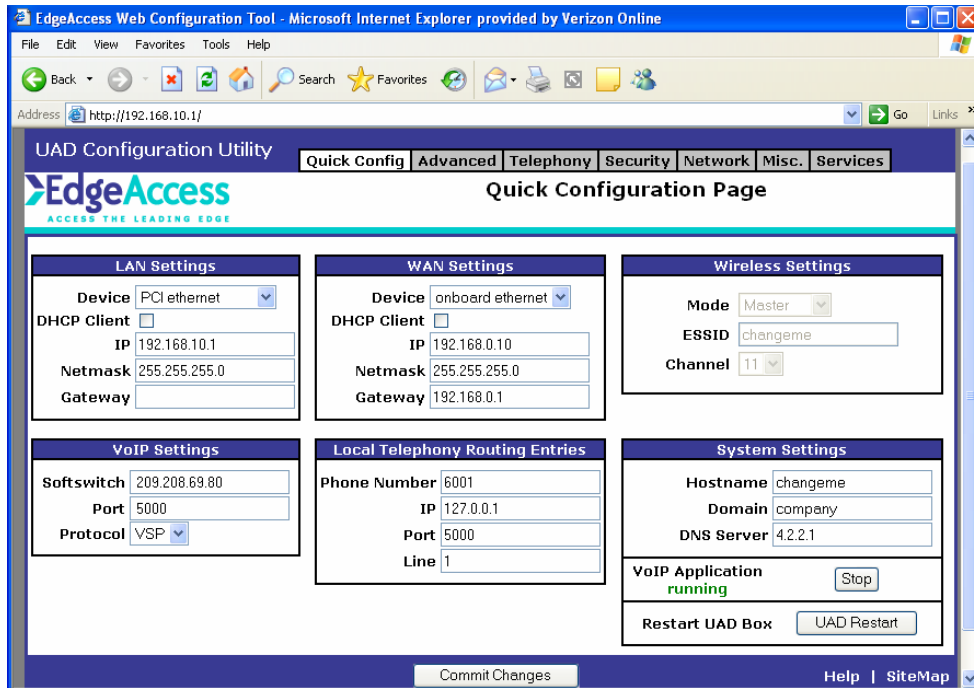


Figure 2 -3

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.

Please enter all Selections/Options by choosing the number that corresponds with your selection.

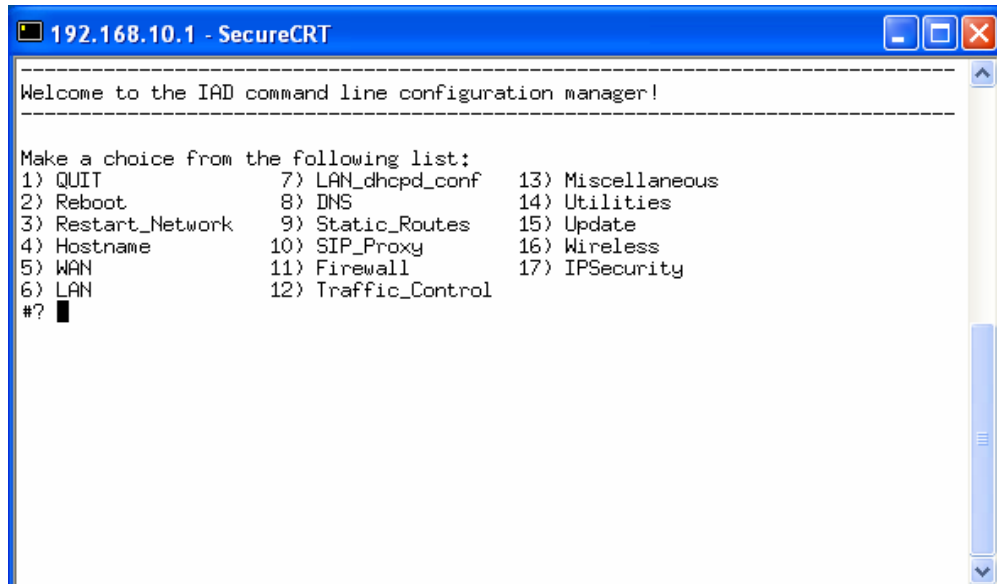


Figure 3-1

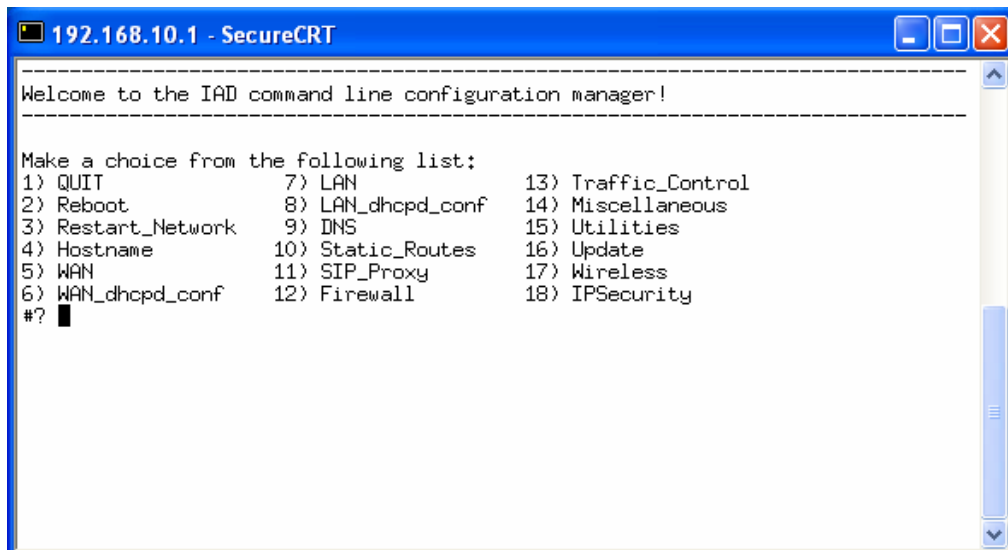


Figure 3-2

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.

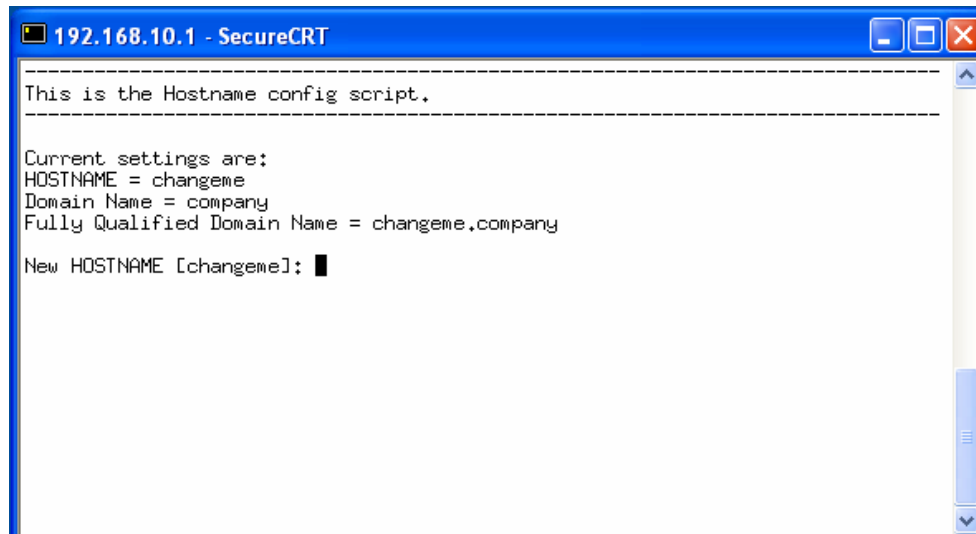


Figure 3-3

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]**.

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*).

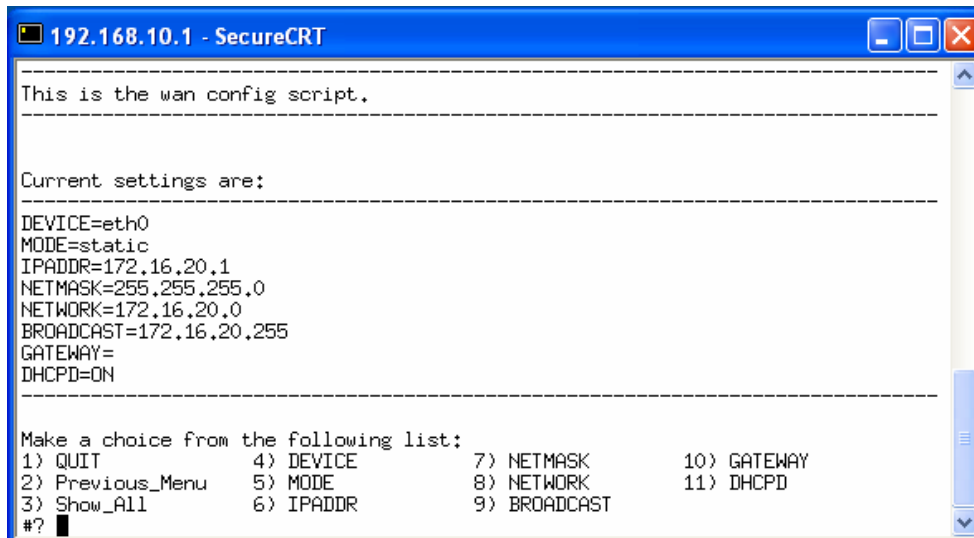


Figure 3-4

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 fall all network interfaces (*Figure 3-5*).

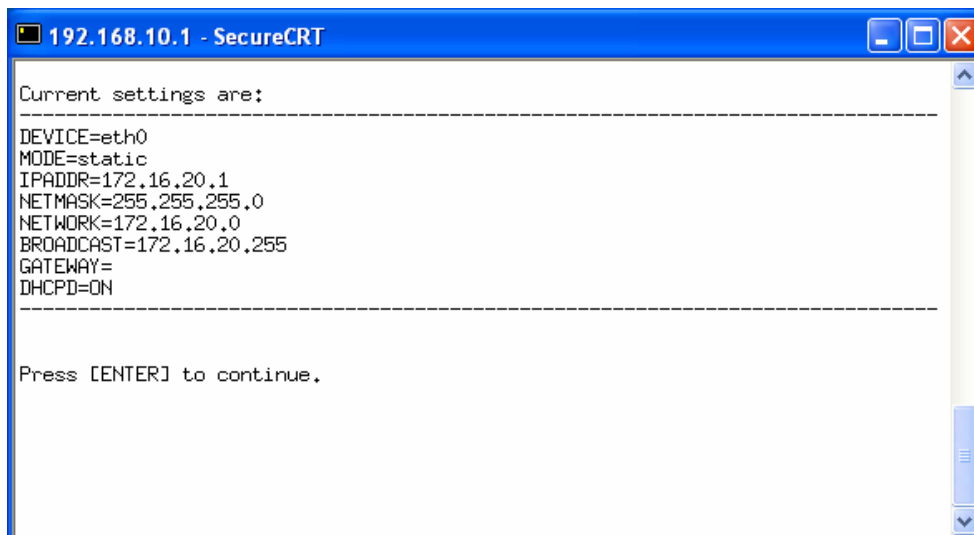


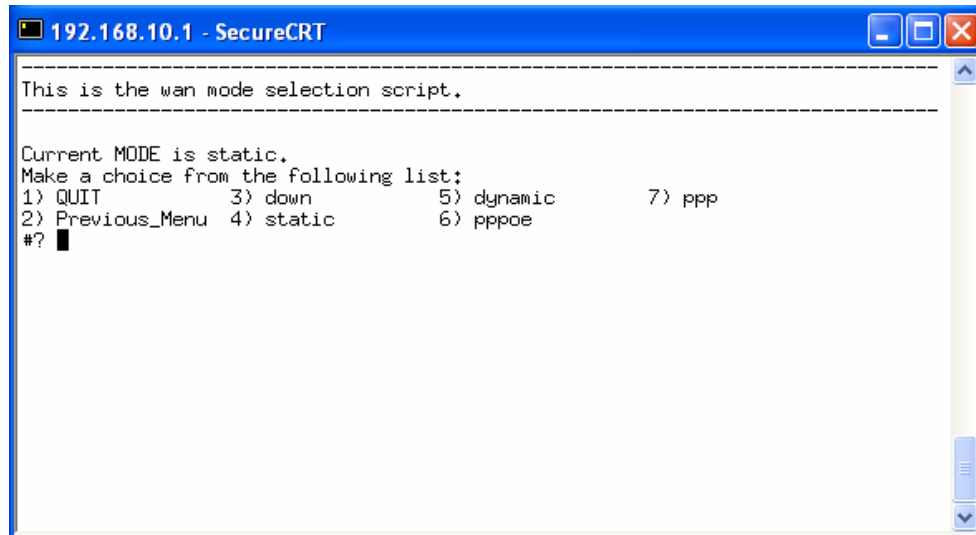
Figure: 3-5

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 (*Figure 3-6*).



```
192.168.10.1 - SecureCRT
-----
This is the wan mode selection script.
-----
Current MODE is static.
Make a choice from the following list:
1) QUIT          3) down          5) dynamic       7) ppp
2) Previous_Menu 4) static        6) pppoe
#? █
```

Figure 3-6

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.

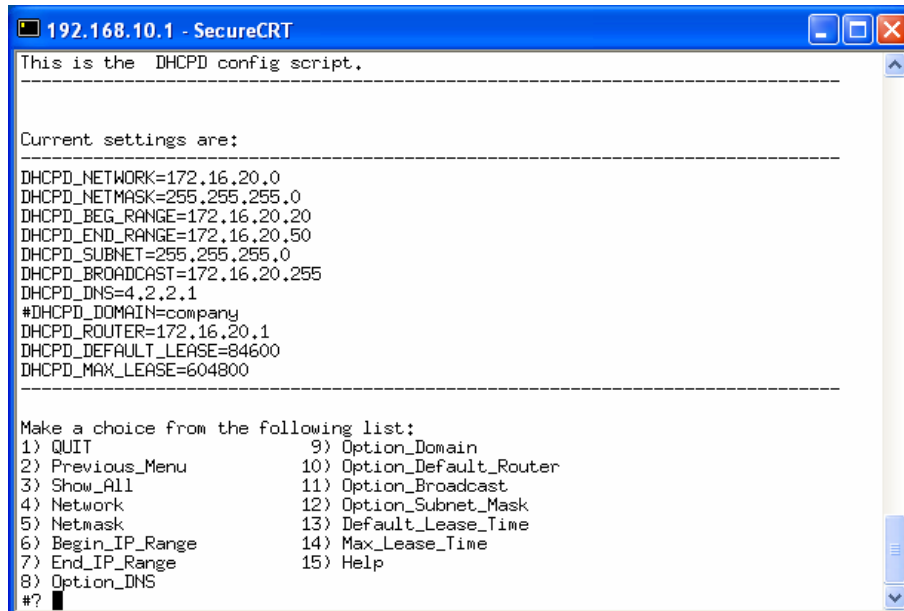
Wireless_AP

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 3-7) will be displayed. From this menu, the WAN DHCP Server parameters can be set.



```
192.168.10.1 - 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 3-7

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.

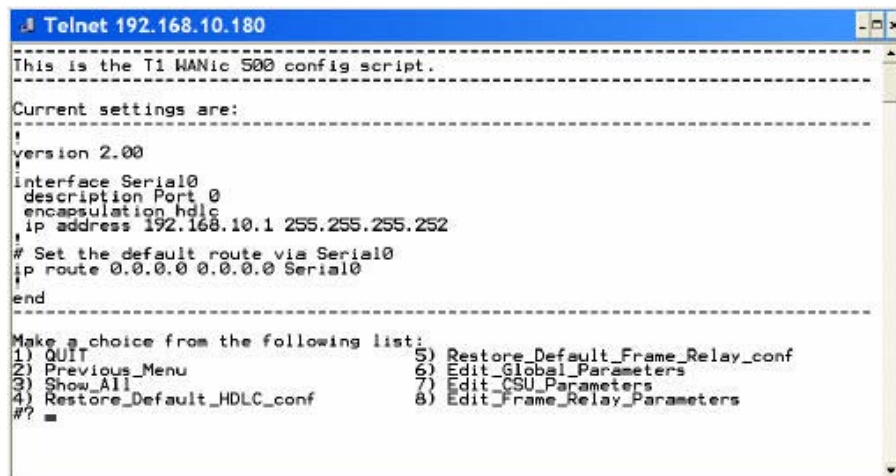
WAN_T1_conf

This option will only appear on the Main Menu, if the UAD has a T1 WAN Interface Card installed (*Figure 3-10*). 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 3-11*).



```
Telnet 192.168.10.180
-----
Welcome to the IAD command line configuration manager!
-----
Make a choice from the following list:
1) QUIT                7) Miscellaneous
2) Hostname           8) Utilities
3) WAN                9) Update
4) WAN_T1_conf       10) Wireless_Client
5) LAN                11) Wireless_Access_Point
6) Firewall          12) IPSecurity
#?
```

Figure 3-8



```
Telnet 192.168.10.180
-----
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
#? =
```

Figure 3-9

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*).



```
Telnet 192.168.10.93
-----
This is the T1 WANic 500 Global params config script.
-----
Current settings are:
-----
!
version 2.00
!
interface Serial0
description Port 0
encapsulation frame-relay ietf
ip address 192.168.10.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 Serial0
!
end
-----
Make a choice from the following list:
1) QUIT
2) Previous_Menu
3) Show_All
4) encapsulation
#? =
5) description
6) static_ip_address_and_route
7) remove_static_routes
8) Help
```

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*).

```
Telnet 192.168.10.93
-----
This is the T1 WANic 500 CSU params config script.
-----
Current settings are:
-----
!
version 2.00
interface Serial0
description Port 0
encapsulation frame-relay ietf
ip address 192.168.10.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 Serial0
end
-----
Make a choice from the following list:
1) QUIT          4) clock_source  7) lbo           10) egl
2) Previous_Menu 5) data_coding  8) linecode     11) ip_address
3) Show_All      6) framing      9) timeslots    12) Help
#? =
```

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*).

```
Telnet 192.168.10.93
-----
This is the T1 WANic 500 Frame-Relay params config script.
-----
Current settings are:
-----
|
|
| version 2.00
|
| interface Serial0
|   description Port 0
|   encapsulation frame-relay ietf
|   ip address 192.168.10.1 255.255.255.0
|
| ip route 0.0.0.0 0.0.0.0 Serial0
|
| end
|
|-----
|
| Make a choice from the following list:
| 1) QUIT                               5) Add_Subinterface
| 2) Previous_Menu                       6) Delete_Subinterface
| 3) Show_All                            7) Help
| 4) Edit_Master_Interface_Commands
| #?
|
```

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*).

```
Telnet 192.168.10.93
-----
This is the T1 WANic 500 Frame-Relay master interface config script.
-----
Current settings are:
-----
|
|
| version 2.00
|
| interface Serial0
|   description Port 0
|   encapsulation frame-relay ietf
|   ip address 192.168.10.1 255.255.255.0
|
| ip route 0.0.0.0 0.0.0.0 Serial0
|
| end
|
|-----
|
| Make a choice from the following list:
| 1) QUIT                               3) Show_All           5) mode
| 2) Previous_Menu                       4) lmi_type           6) Help
| #?
|
```

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 in the PCI interface, 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
```

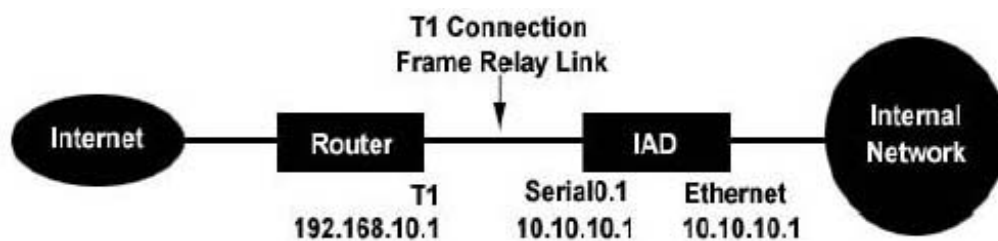
```

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:

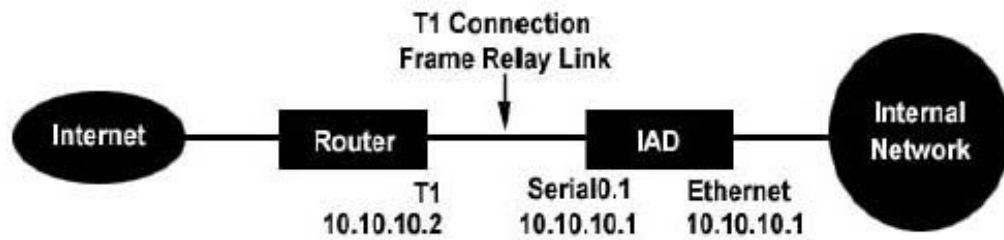
```

!
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:

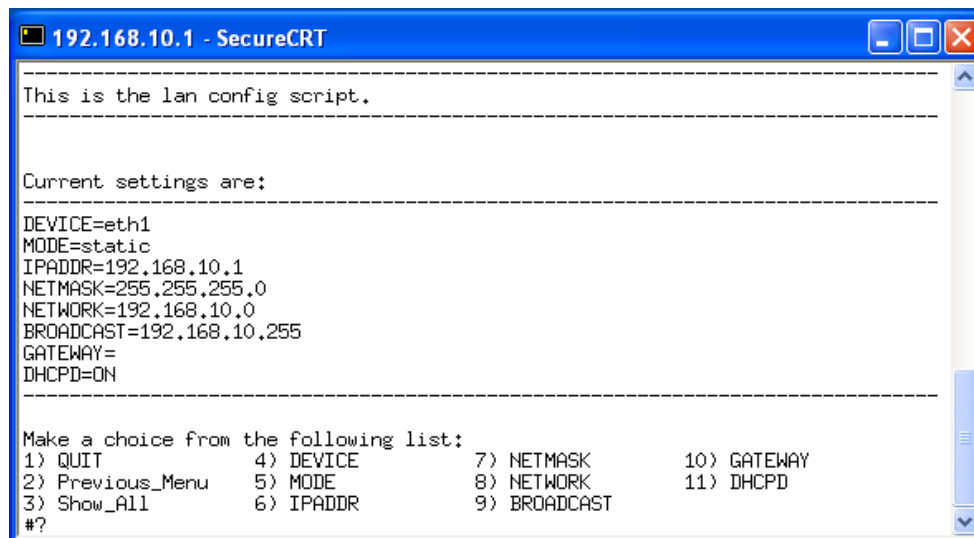
Main Menu > WAN_T1_CONF > Edit_HDLC_Parameters > IP_Address

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 (*Figure 3-14*).



```
192.168.10.1 - SecureCRT
-----
This is the lan config script.
-----
Current settings are:
-----
DEVICE=eth1
MODE=static
IPADDR=192.168.10.1
NETMASK=255.255.255.0
NETWORK=192.168.10.0
BROADCAST=192.168.10.255
GATEWAY=
DHCPD=ON
-----
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 3-14

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 shown in (*Figure 3-15*) will be displayed.

```

192.168.10.1 - SecureCRT
-----
This is the DHCPD config script.
-----
Current settings are:
-----
DHCPD_NETWORK=192.168.10.0
DHCPD_NETMASK=255.255.255.0
DHCPD_BEG_RANGE=192.168.10.20
DHCPD_END_RANGE=192.168.10.50
DHCPD_SUBNET=255.255.255.0
DHCPD_BROADCAST=192.168.10.255
DHCPD_DNS=4.2.2.1
#DHCPD_DOMAIN=company.com
DHCPD_ROUTER=192.168.10.1
DHCPD_DEFAULT_LEASE=84600
DHCPD_MAX_LEASE=604800
-----
Make a choice from the following list:
1) QUIT                9) Option_Domain
2) Previous_Menu      10) Option_Default_Router
3) Show_All           11) Option_Broadcast
4) Network            12) Option_Subnet_Mask
5) Netmask            13) Default_Lease_Time
6) Begin_IP_Range    14) Max_Lease_Time
7) End_IP_Range      15) Help
8) Option_DNS
#?

```

Figure 3-15

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 3-16).

```

192.168.10.1 - SecureCRT
-----
This is the IAD IP ROUTING table management script.
-----
Current routing table:
-----
Kernel IP routing table
Destination  Gateway      Genmask      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 3-16

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.

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 3-17*) will be displayed.

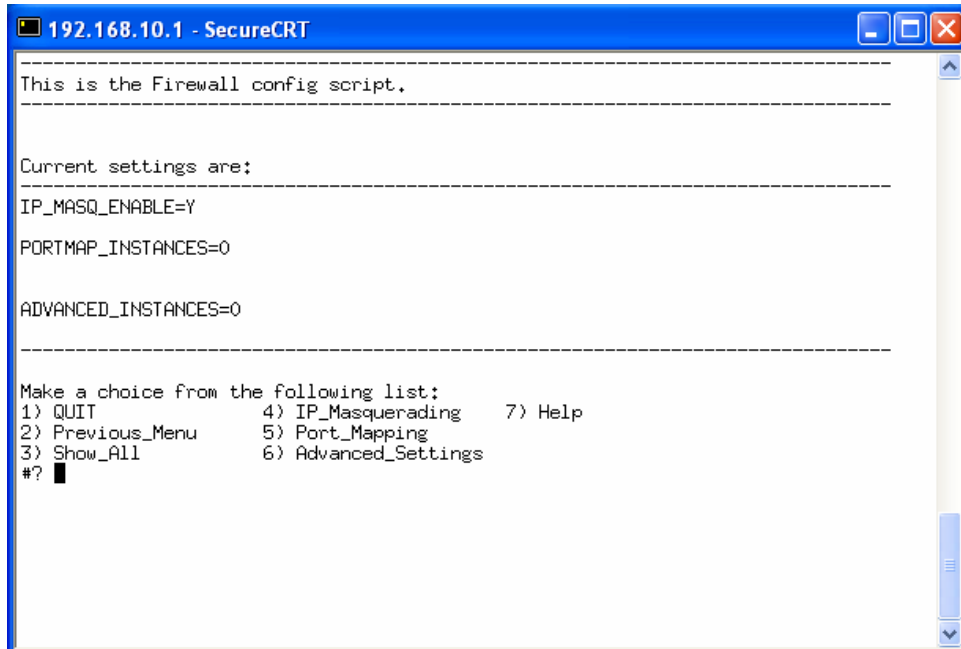
Port Mapping

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.

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 Linux with a real IP address as a gateway for non-connected machines with "fake" IP addresses. The Linux 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.

A screenshot of a SecureCRT terminal window titled "192.168.10.1 - SecureCRT". The terminal displays the following text:

```
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 3-17

IP_Masquerading

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

Port_Mapping

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 (*Figure 3-18*).

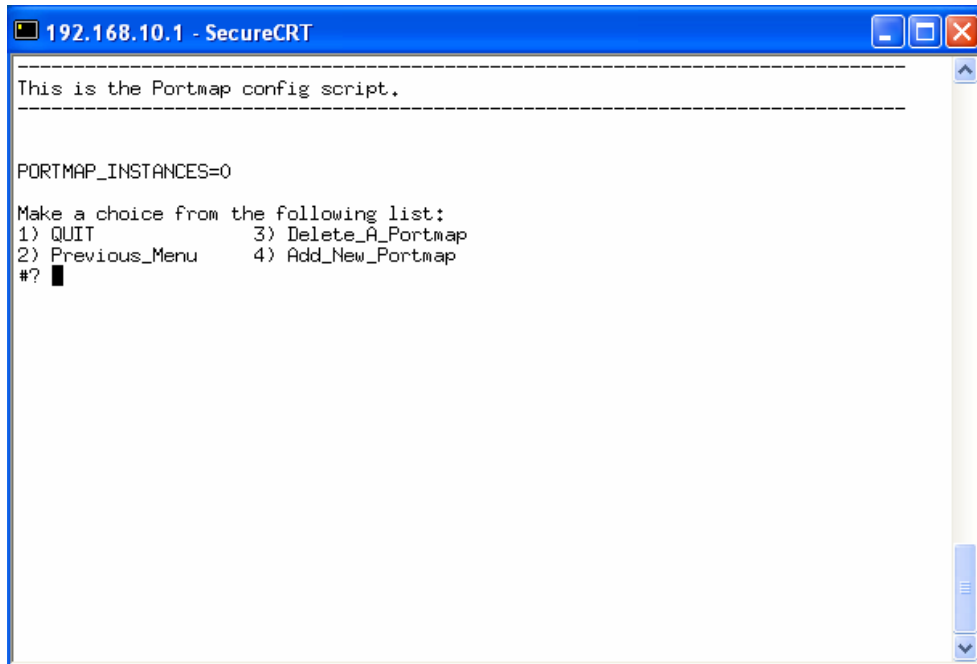


Figure 3-18

Advanced_Settings

When (Advanced_Settings) from the Firewall Configuration Menu is selected, the system will display the Advanced Settings Menu (*Figure 3-19*).

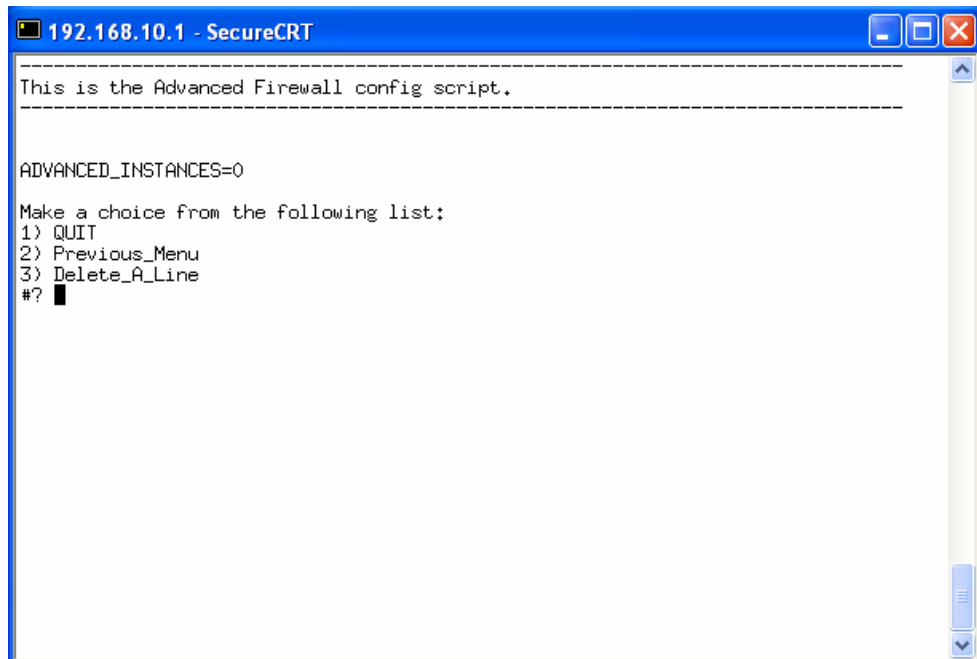


Figure 3-19

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 Linux kernel consists of the following components:

- queueing 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 3-20*) will be displayed.

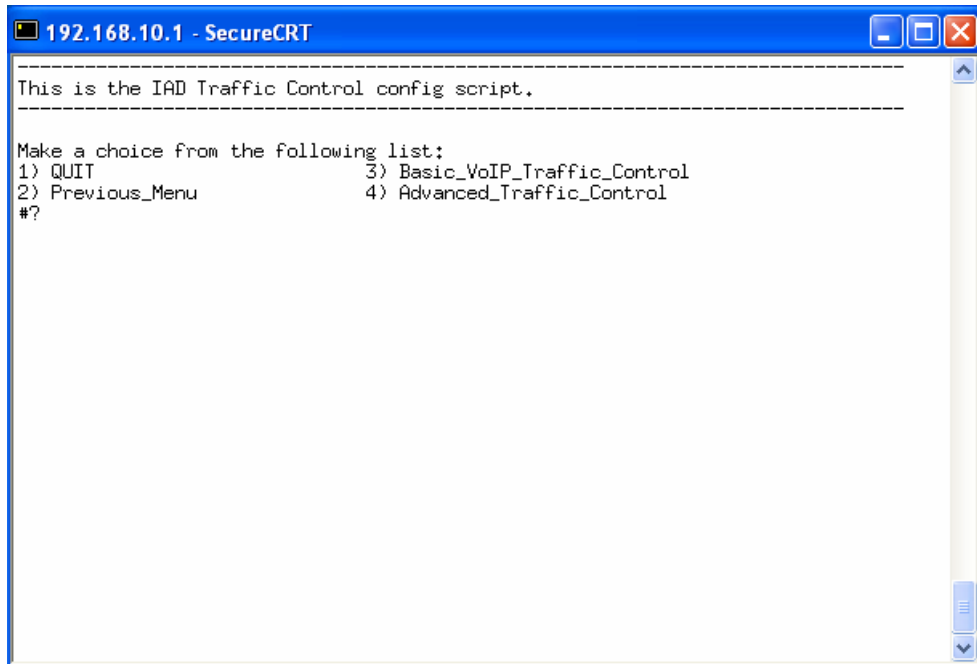


Figure 3-20

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

Stopt_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 (*Figure 3-21*).

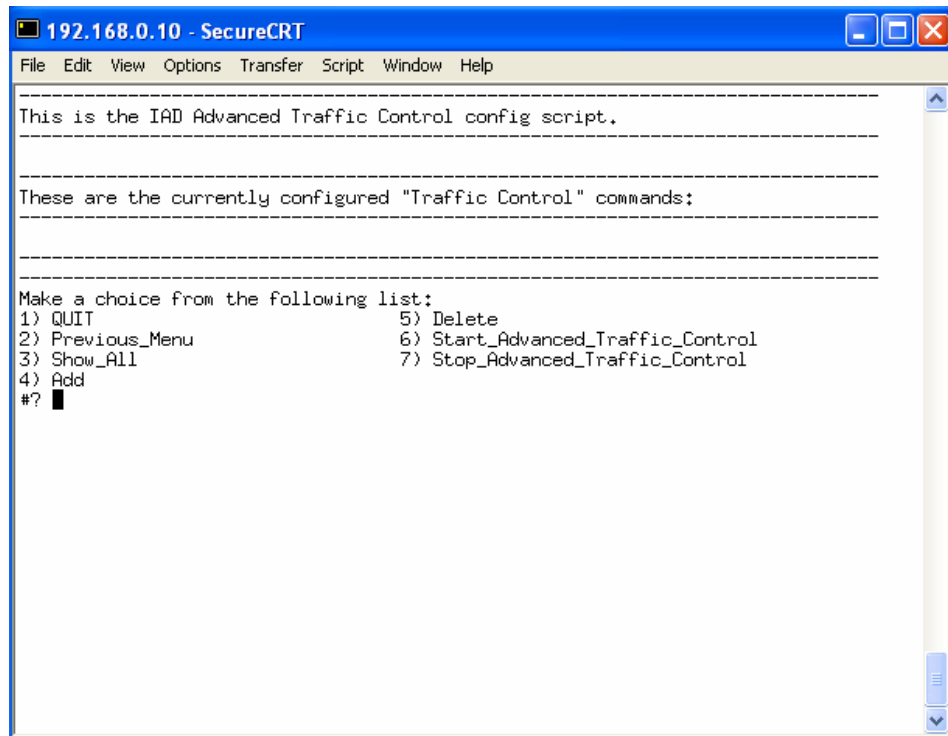


Figure 3-21

ADD

When (Add) from the Advanced Traffic Control Configuration Menu is selected, the system allows you to add Traffic Control Commands for a specific interface on the UAD (*Figure 3-22*).

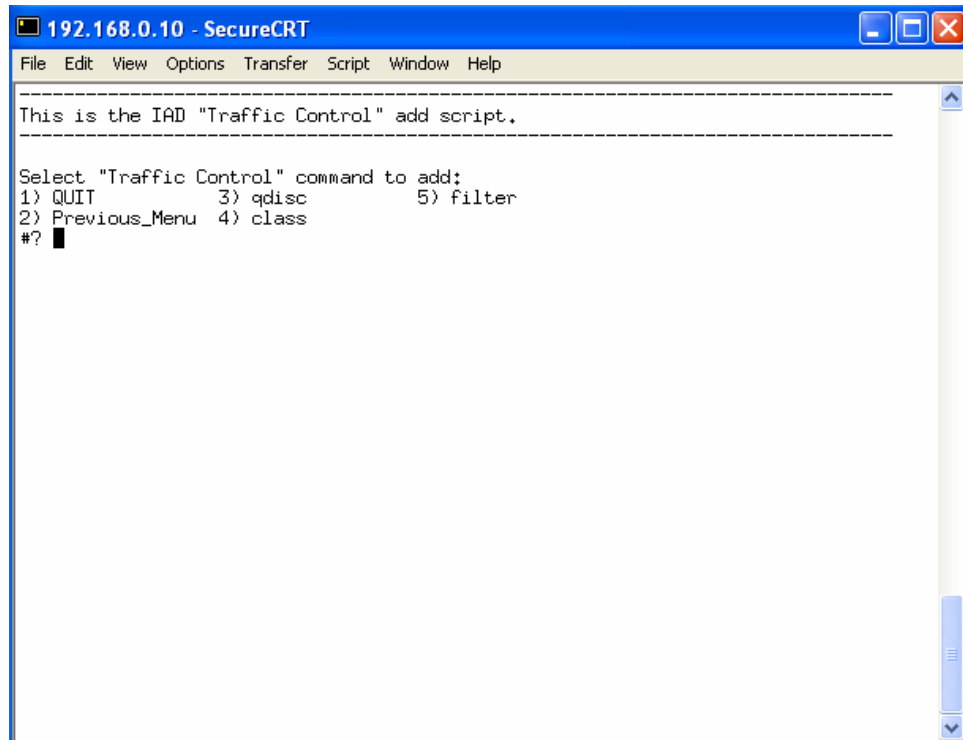


Figure 3-22

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.

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 3-23) will be displayed.

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

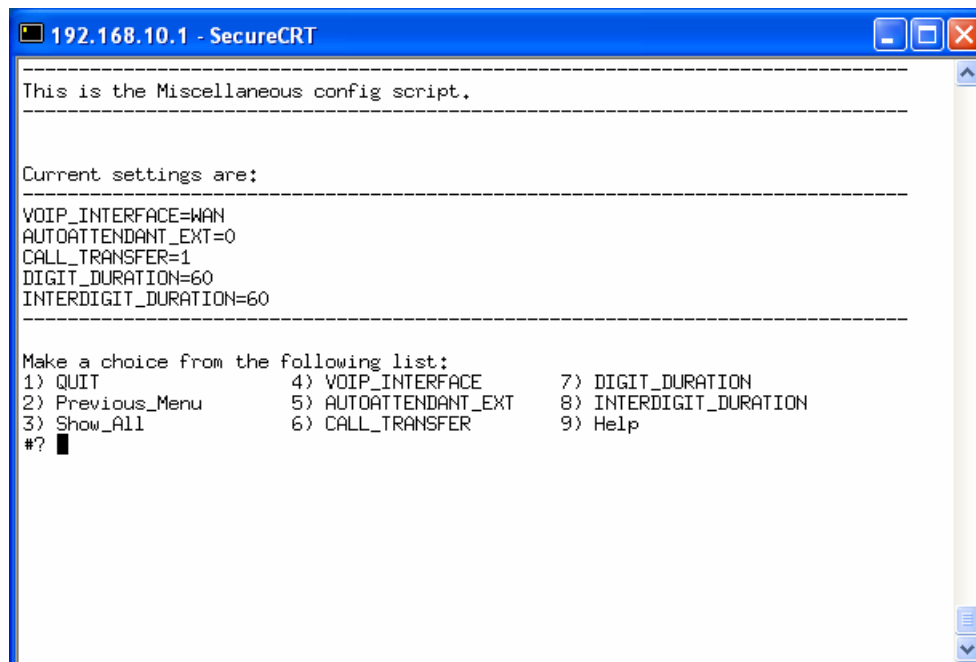
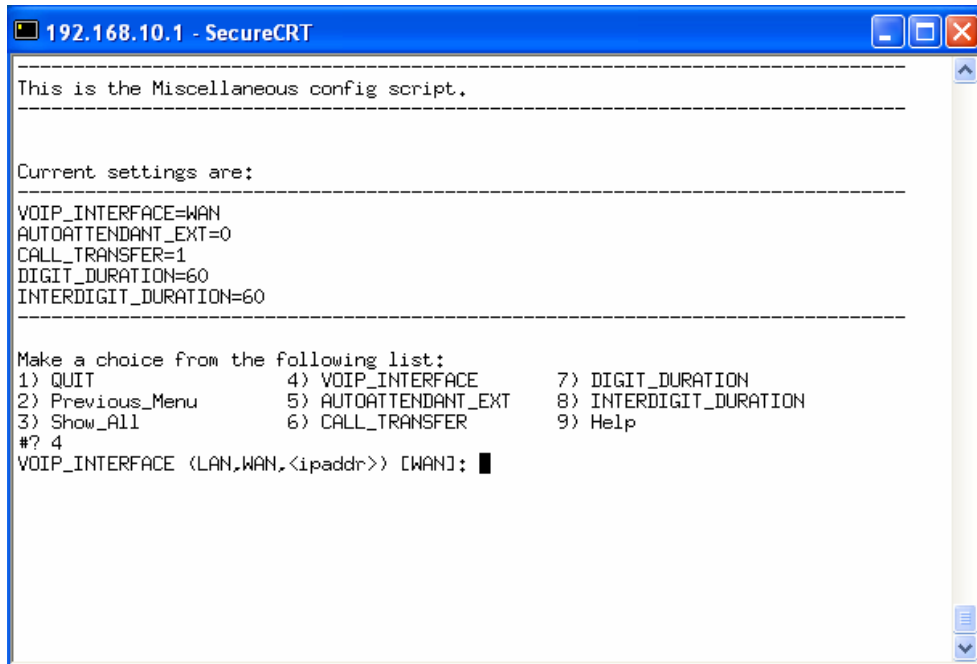


Figure 3-23

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 (Figure 3-24).

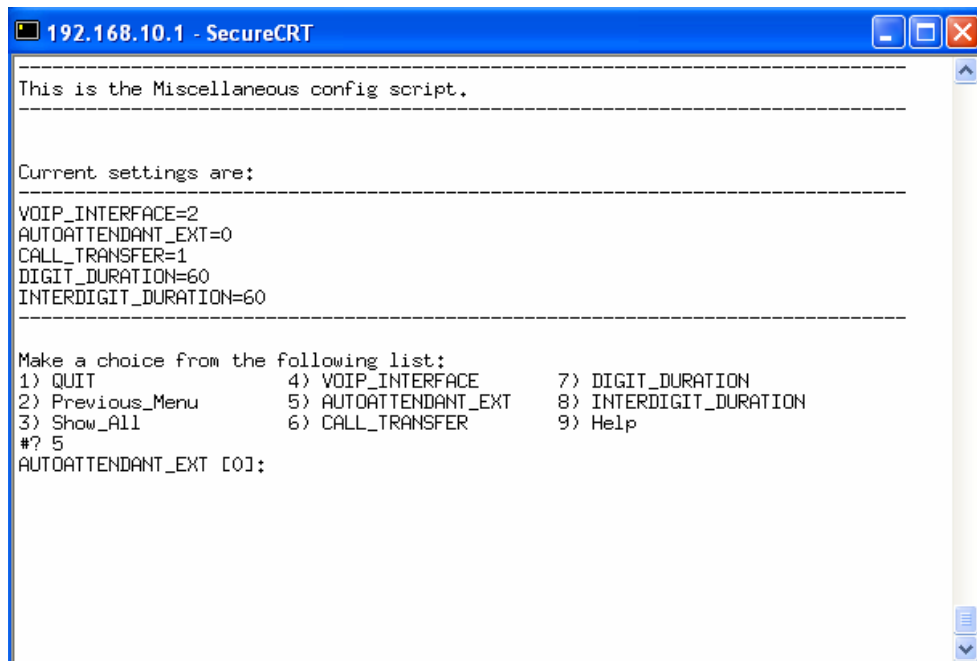


```
192.168.10.1 - SecureCRT
-----
This is the Miscellaneous config script.
-----
Current settings are:
-----
VOIP_INTERFACE=WAN
AUTOATTENDANT_EXT=0
CALL_TRANSFER=1
DIGIT_DURATION=60
INTERDIGIT_DURATION=60
-----
Make a choice from the following list:
1) QUIT                4) VOIP_INTERFACE      7) DIGIT_DURATION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

Figure 3-24

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 (*Figure 3-25*).

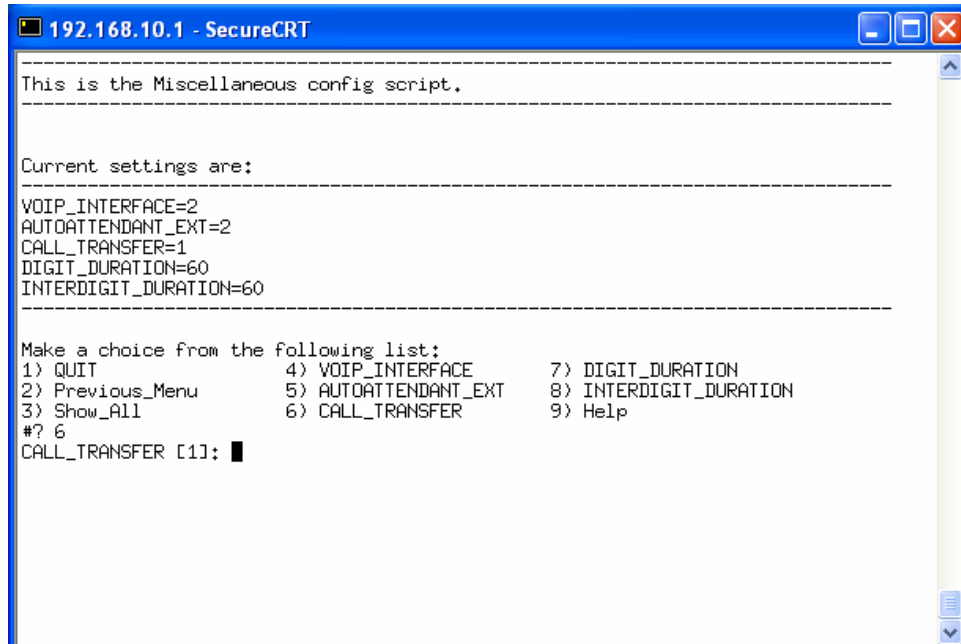


```
192.168.10.1 - SecureCRT
-----
This is the Miscellaneous config script.
-----
Current settings are:
-----
VOIP_INTERFACE=2
AUTOATTENDANT_EXT=0
CALL_TRANSFER=1
DIGIT_DURATION=60
INTERDIGIT_DURATION=60
-----
Make a choice from the following list:
1) QUIT                4) VOIP_INTERFACE      7) DIGIT_DURATION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

Figure 3-25

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 (*Figure 3-26*).



```
192.168.10.1 - SecureCRT
-----
This is the Miscellaneous config script.
-----
Current settings are:
-----
VOIP_INTERFACE=2
AUTOATTENDANT_EXT=2
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
#? 6
CALL_TRANSFER [1]: █
```

Figure 3-26

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 (*Figure 3-27*).

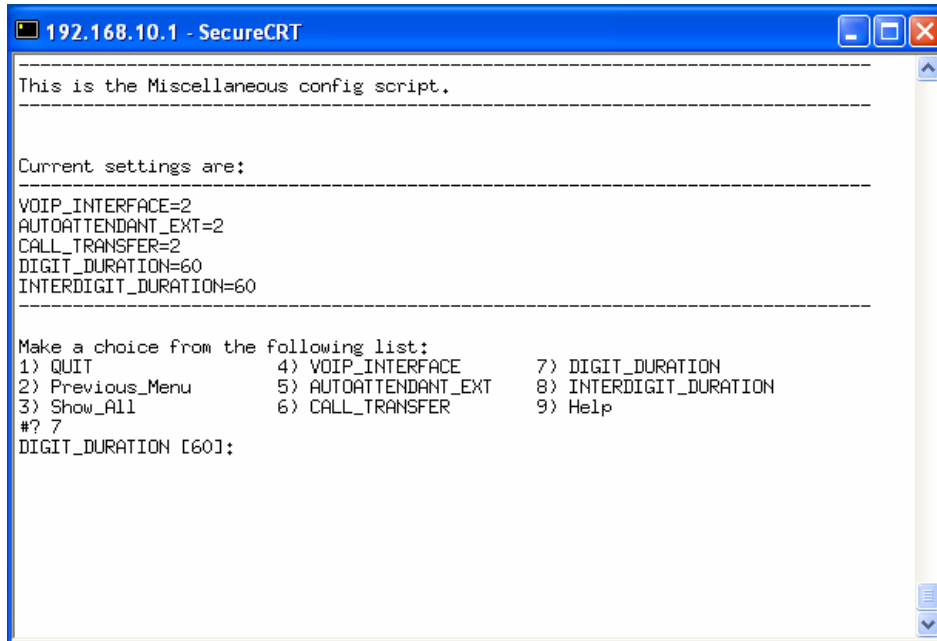


Figure 3-27

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 (Figure 3-28).

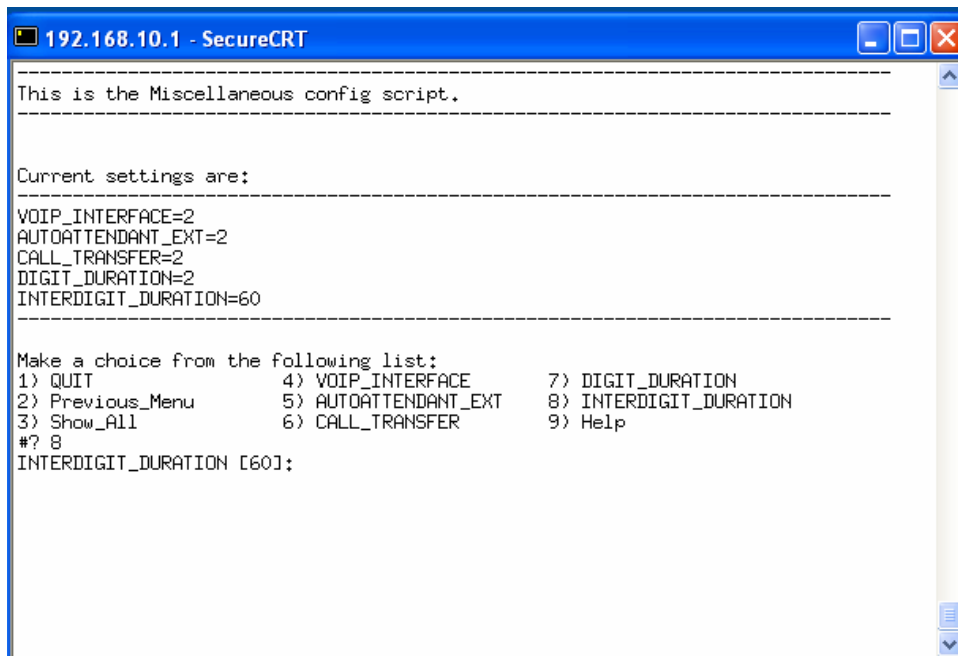


Figure 3-28

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 3-29) will be displayed.

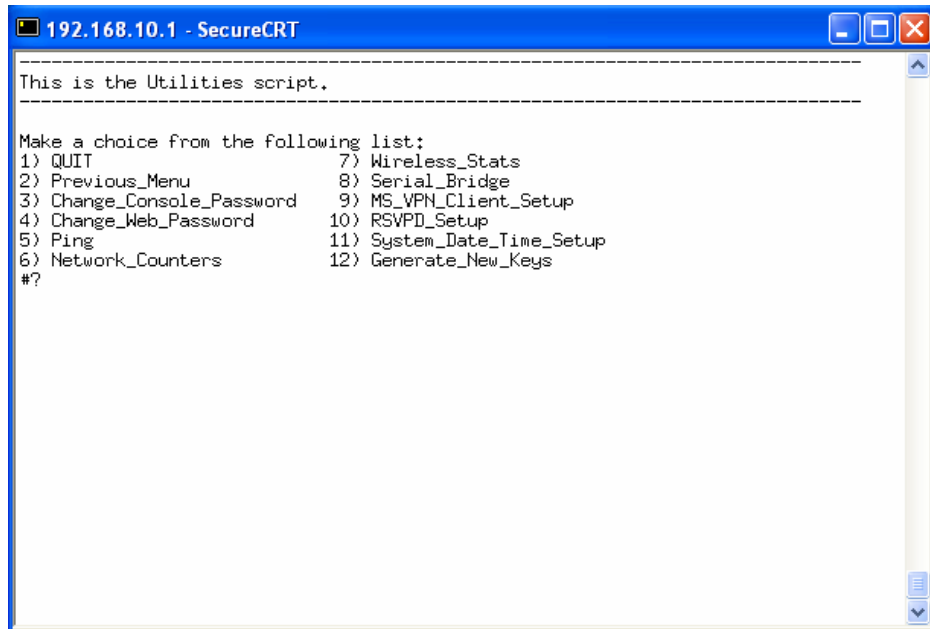


Figure 3-29

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 3-30).

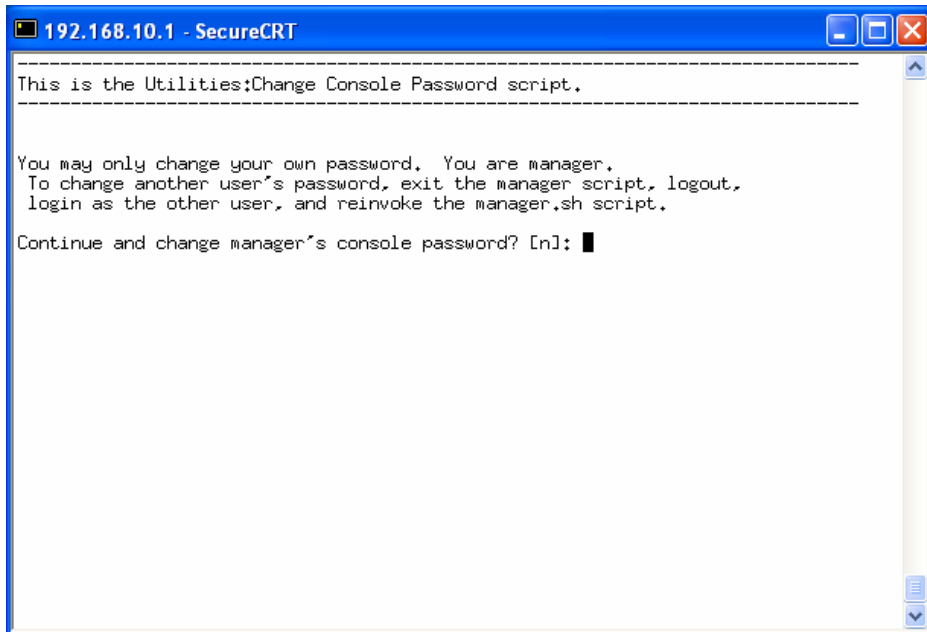


Figure 3-30

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 3-31).

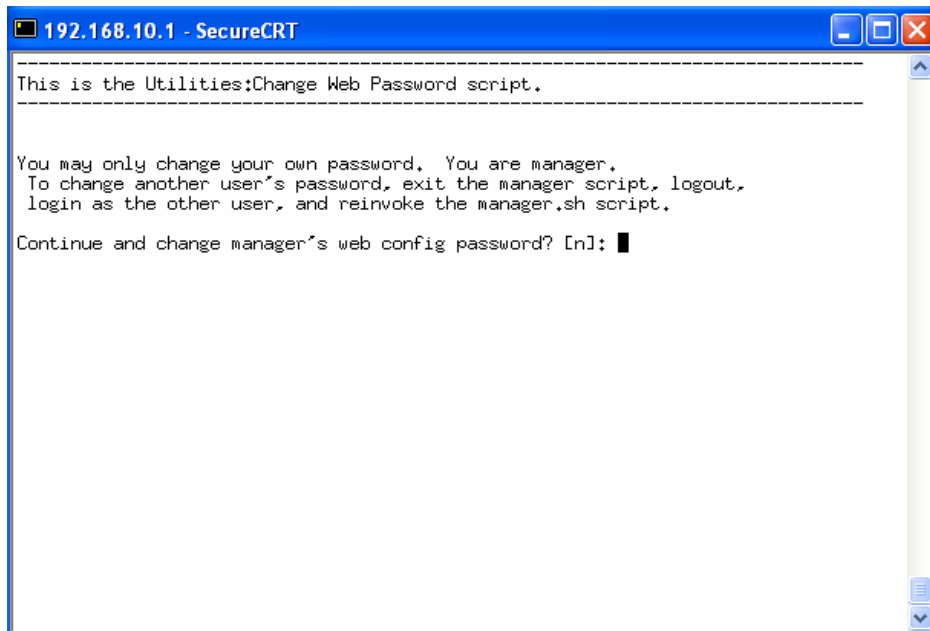


Figure 3-31

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 3-32*).

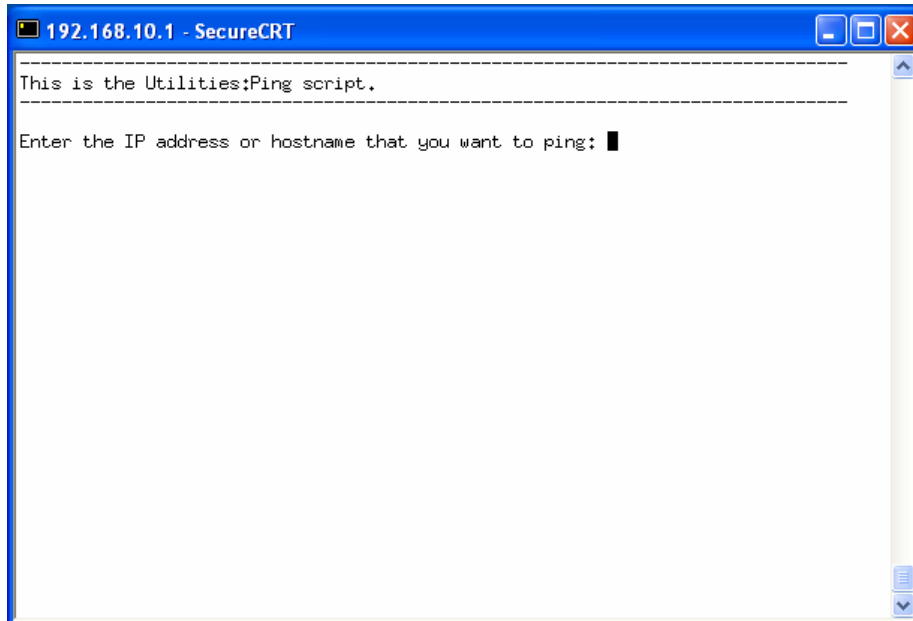


Figure 3-32

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 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 3-33*) shows you a successful Ping command and (*Figure 3-34*) 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: 192.168.10.1
-----
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 3-33

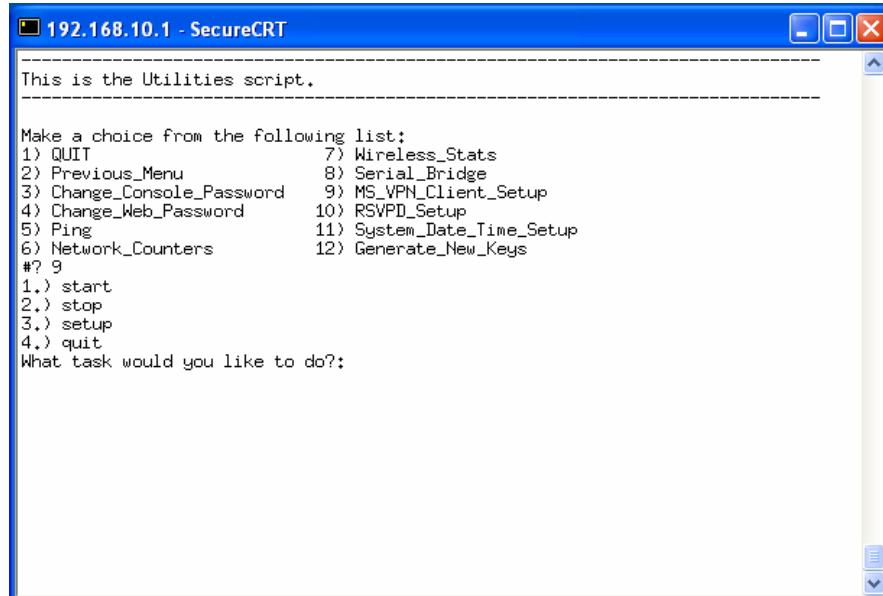
```
192.168.10.1 - SecureCRT
-----
This is the Utilities:Ping script.
-----
Enter the IP address or hostname that you want to ping: 192.168.11.1
-----
PING 192.168.11.1 (192.168.11.1): 56 octets data
sendto: Network is unreachable
ping: sent 64 octets to 192.168.11.1, ret=-1
sendto: Network is unreachable
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 3-34

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 (*Figure 3-35*).

A screenshot of a SecureCRT terminal window titled "192.168.10.1 - SecureCRT". The terminal displays a script that starts with "This is the Utilities script." followed by a dashed line. Below the line, it says "Make a choice from the following list:" and lists 12 numbered options: 1) QUIT, 2) Previous_Menu, 3) Change_Console_Password, 4) Change_Web_Password, 5) Ping, 6) Network_Counters, 7) Wireless_Stats, 8) Serial_Bridge, 9) MS_VPN_Client_Setup, 10) RSVPD_Setup, 11) System_Date_Time_Setup, and 12) Generate_New_Keys. Below the list, there is a sub-menu with options: 1.) start, 2.) stop, 3.) setup, and 4.) quit. The prompt "What task would you like to do?:" is at the bottom of the list.

```
192.168.10.1 - 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
#? 9
1.) start
2.) stop
3.) setup
4.) quit
What task would you like to do?:
```

Figure 3-35

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 (*Figure 3-36*).

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.

```
192.168.10.1 - 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
#? 9
1.) start
2.) stop
3.) setup
4.) quit
What task would you like to do?: 3
ls: /etc/pptp.d: No such file or directory
1.) Manage CHAP secrets
2.) Manage PAP secrets
3.) List PPTP Tunnels
4.) Add a NEW PPTP Tunnel
5.) Delete a PPTP Tunnel
6.) Configure resolv.conf
7.) Select a default tunnel
8.) Quit
?:
```

Figure 3-36

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

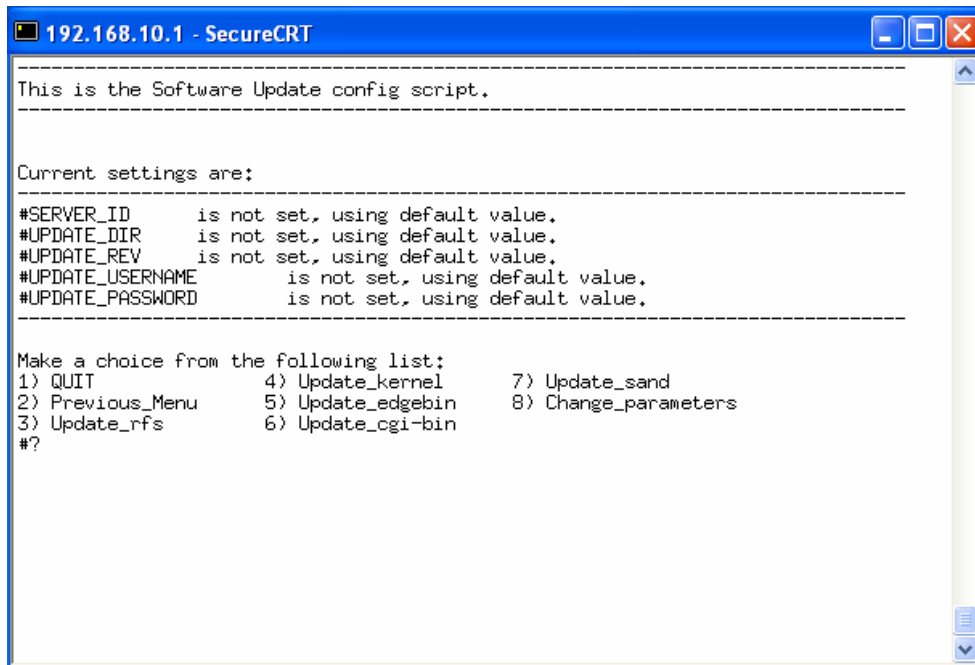
The (Select a default tunnel) option from the MS VPN Setup Menu allows you to select a default tunnel.

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

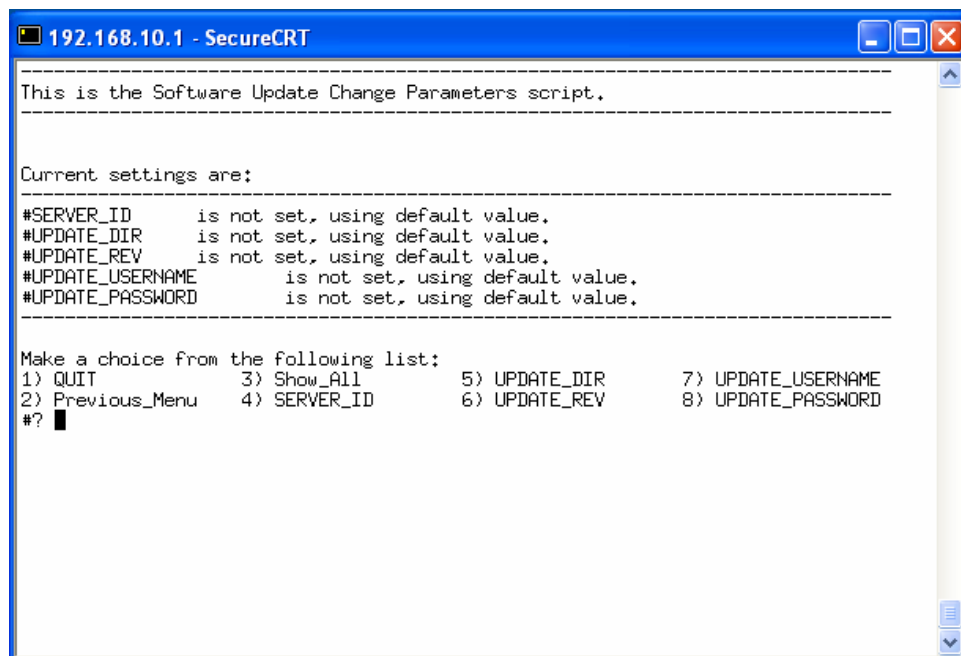
When (Update_kernel) from the Update Menu is selected, the Setup Manager will connect to the FTP Server configured in the Update Parameters and Update the Operating System Kernel File.

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 (Figure 3-38) will be displayed.



```
192.168.10.1 - SecureCRT
-----
This is the Software Update Change Parameters 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          3) Show_All      5) UPDATE_DIR    7) UPDATE_USERNAME
2) Previous_Menu 4) SERVER_ID     6) UPDATE_REV    8) UPDATE_PASSWORD
#? █
```

Figure 3-38

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 (Figure 3-39).

```
192.168.10.1 - SecureCRT
-----
This is the Software Update Change Parameters 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          3) Show_All      5) UPDATE_DIR    7) UPDATE_USERNAME
2) Previous_Menu 4) SERVER_ID     6) UPDATE_REV   8) UPDATE_PASSWORD
#? 4
SERVER_ID []:
```

Figure 3-39

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 (*Figure 3-40*).

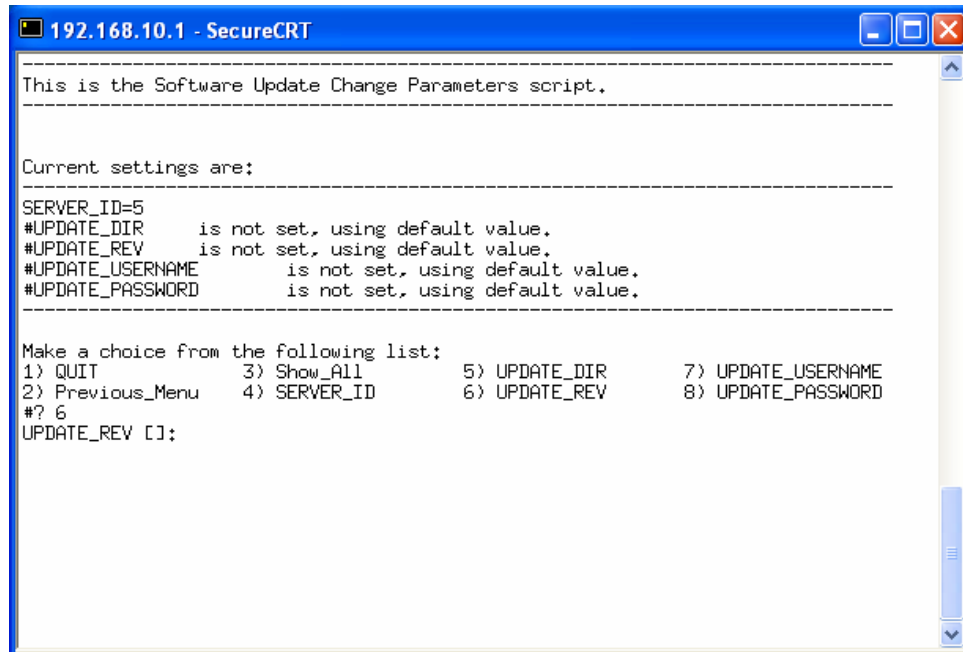
```
192.168.10.1 - SecureCRT
-----
This is the Software Update Change Parameters script.
-----
Current settings are:
-----
#SERVER_ID      is not set, using default value.
#UPDATE_DIR     is not set, using default value.
#UPDATE_REV     is not set, using default value.
#UPDATE_USERNAME is not set, using default value.
#UPDATE_PASSWORD is not set, using default value.
-----
Make a choice from the following list:
1) QUIT          3) Show_All      5) UPDATE_DIR    7) UPDATE_USERNAME
2) Previous_Menu 4) SERVER_ID     6) UPDATE_REV   8) UPDATE_PASSWORD
#? 4
SERVER_ID []: 5

/opt/iad/cfg/ftpupdate.cfg parameters updated.
Press [ENTER] to continue.█
```

Figure 3-40

UPDATE_REV

When (UPDATE_REV) from the Change Parameters Menu is selected, the Setup Manager will prompt you to enter the Update Version (*Figure 3-41*).



```
192.168.10.1 - SecureCRT
-----
This is the Software Update Change Parameters script.
-----
Current settings are:
-----
SERVER_ID=5
#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          3) Show_All      5) UPDATE_DIR      7) UPDATE_USERNAME
2) Previous_Menu 4) SERVER_ID     6) UPDATE_REV      8) UPDATE_PASSWORD
#? 6
UPDATE_REV []:
```

Figure 3-41

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 (*Figure 3-42*).

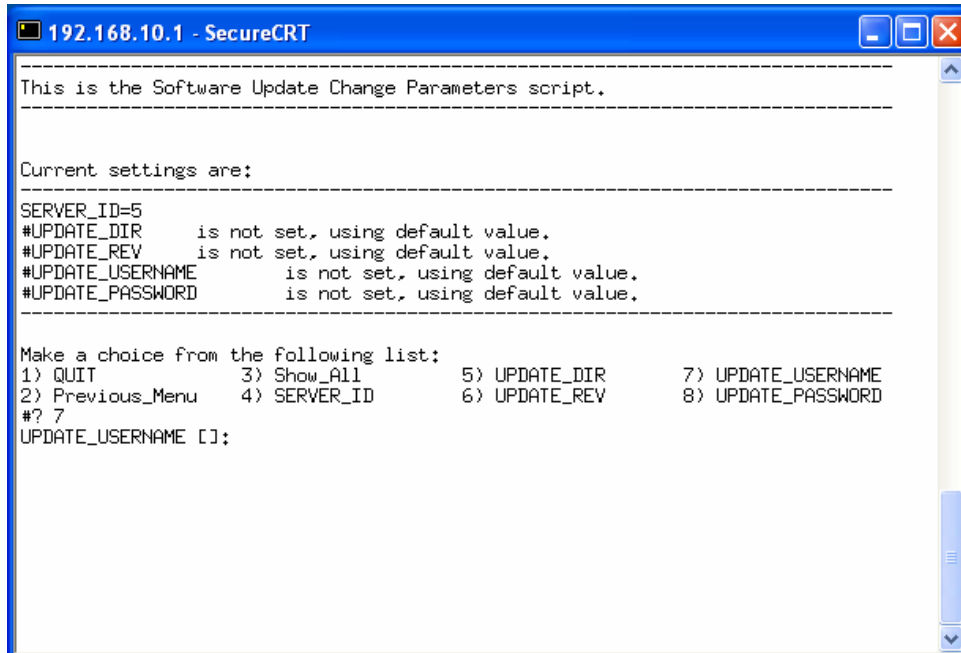


Figure 3-42

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 (*Figure 3-43*).

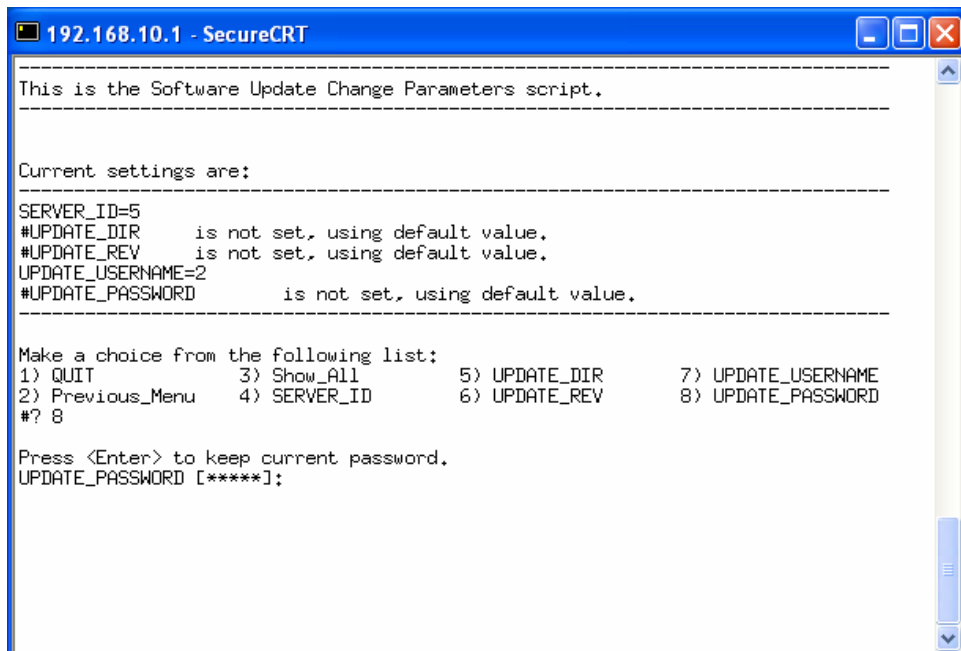
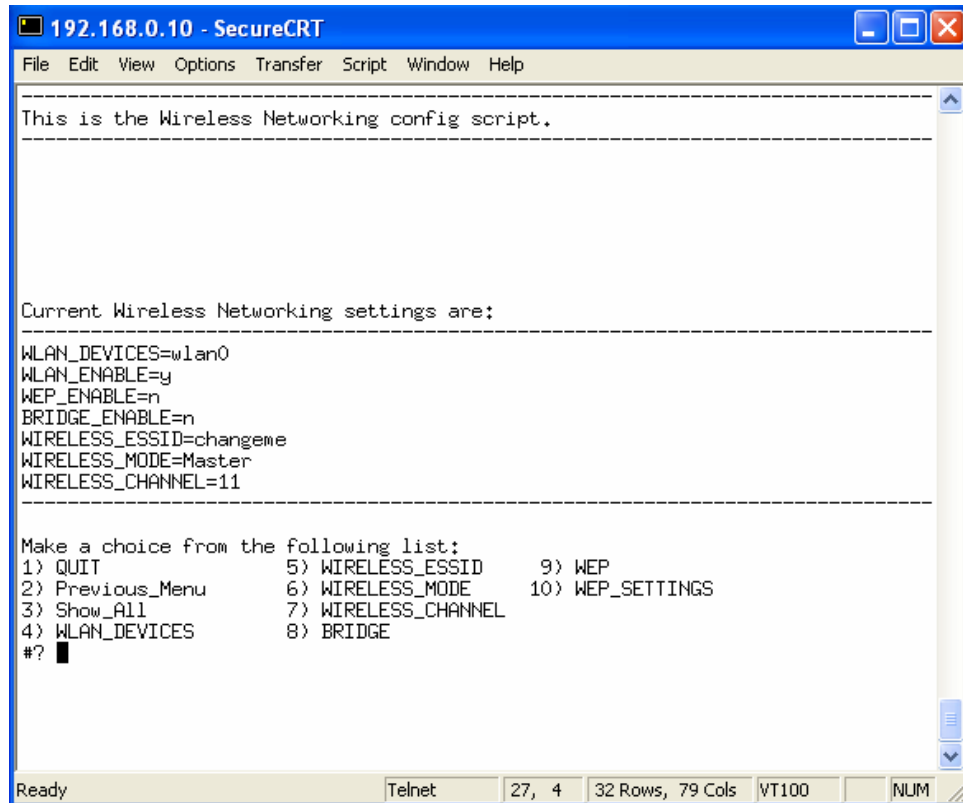


Figure 3-43

Wireless

The (Wireless) option from the Main Configuration Menu (*Figure 3-44*) allows you to configure the Wireless Client parameters for the UAD. The Setup manager will automatically display the parameters for the Wireless Client.

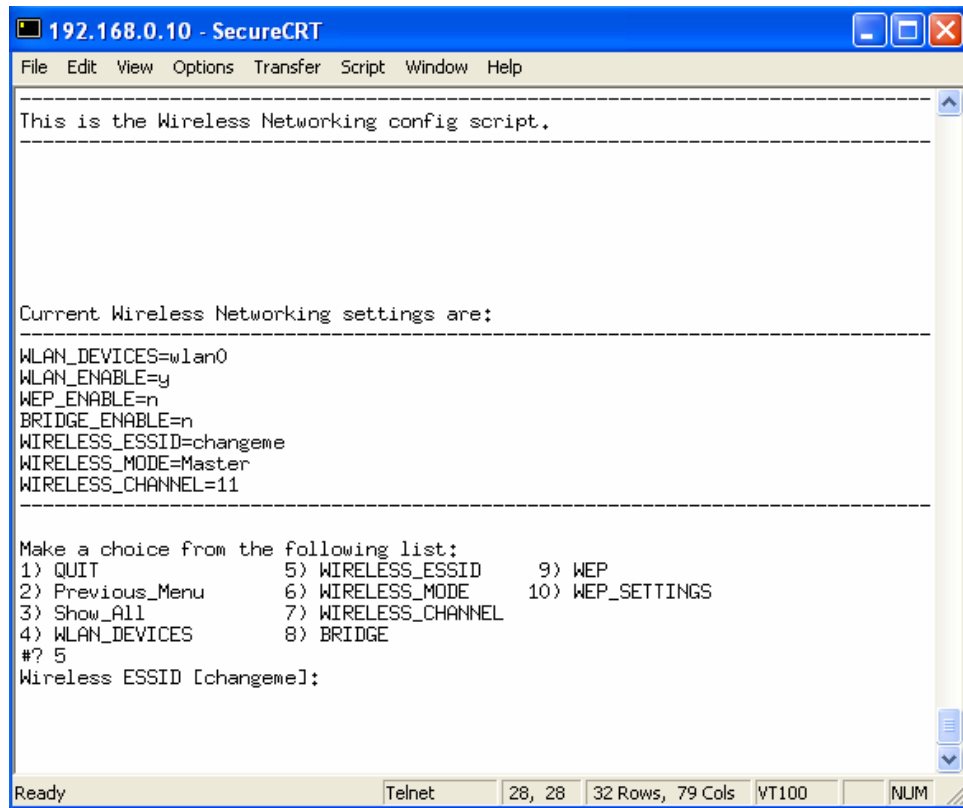


```
192.168.0.10 - SecureCRT
File Edit View Options Transfer Script Window Help
-----
This is the Wireless Networking config script.
-----
Current Wireless Networking settings are:
-----
WLAN_DEVICES=wlan0
WLAN_ENABLE=y
WEP_ENABLE=n
BRIDGE_ENABLE=n
WIRELESS_ESSID=changeme
WIRELESS_MODE=Master
WIRELESS_CHANNEL=11
-----
Make a choice from the following list:
1) QUIT                5) WIRELESS_ESSID    9) WEP
2) Previous_Menu      6) WIRELESS_MODE     10) WEP_SETTINGS
3) Show_All           7) WIRELESS_CHANNEL
4) WLAN_DEVICES       8) BRIDGE
#? █
```

Figure 3-44

Wireless_ESSID

The Wireless_ESSID option from the Wireless Client Menu (*Figure 3-45*) allows you to set the Extended Service Set ID for your Wireless Network. The ESSID is the identifying name of an 802.11b wireless network. By specifying the ESSID in your client setup is how to ensure you connect to your wireless network instead of another network by mistake.



```
192.168.0.10 - SecureCRT
File Edit View Options Transfer Script Window Help
-----
This is the Wireless Networking config script.
-----

Current Wireless Networking settings are:
-----
WLAN_DEVICES=wlan0
WLAN_ENABLE=y
WEP_ENABLE=n
BRIDGE_ENABLE=n
WIRELESS_ESSID=changeme
WIRELESS_MODE=Master
WIRELESS_CHANNEL=11
-----

Make a choice from the following list:
1) QUIT                5) WIRELESS_ESSID    9) WEP
2) Previous_Menu      6) WIRELESS_MODE    10) WEP_SETTINGS
3) Show_All           7) WIRELESS_CHANNEL
4) WLAN_DEVICES       8) BRIDGE
#? 5
Wireless ESSID [changeme]:
```

Figure 3-45

Wireless_Mode

The (Wireless Mode) option from the Wireless Menu (*Figure 3-46*) allows you to set the Wireless MODE by selecting Managed, Master, Ad-hoc or Use_Current_Mode.

In a wireless (specifically 802.11b) an Ad-hoc network is where all the wireless clients communicate directly to each other.

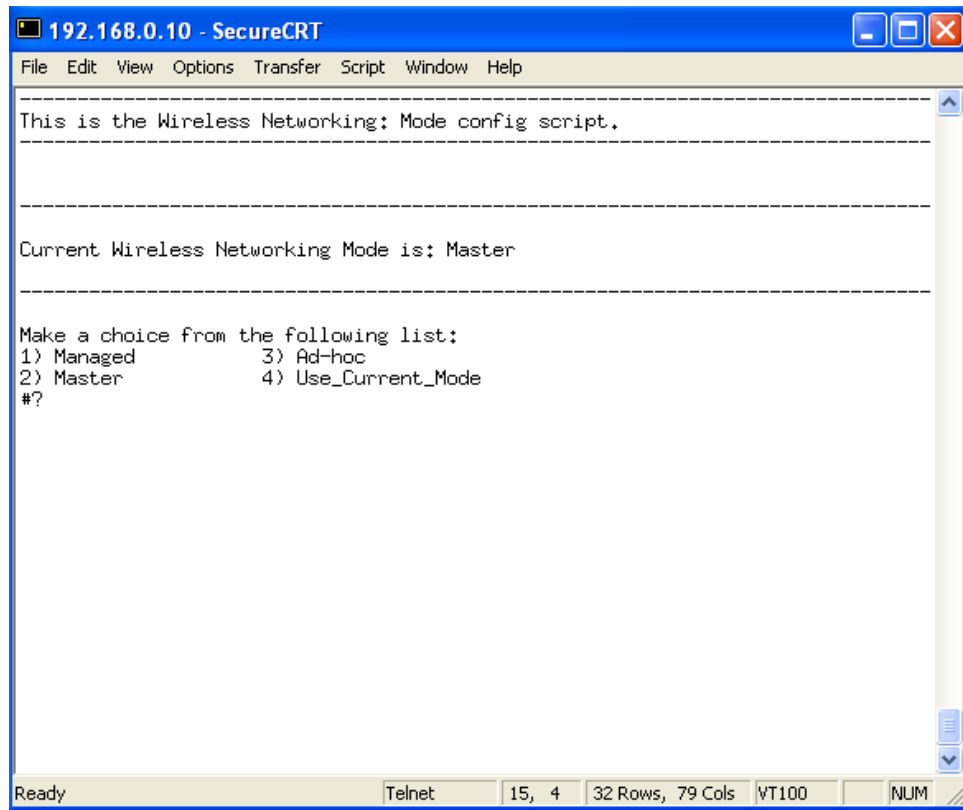


Figure 3-46

Wireless_Channel

The (Wireless_Channel) option from the Wireless Menu (*Figure 3-47*) allows you to select the number of channels desired.

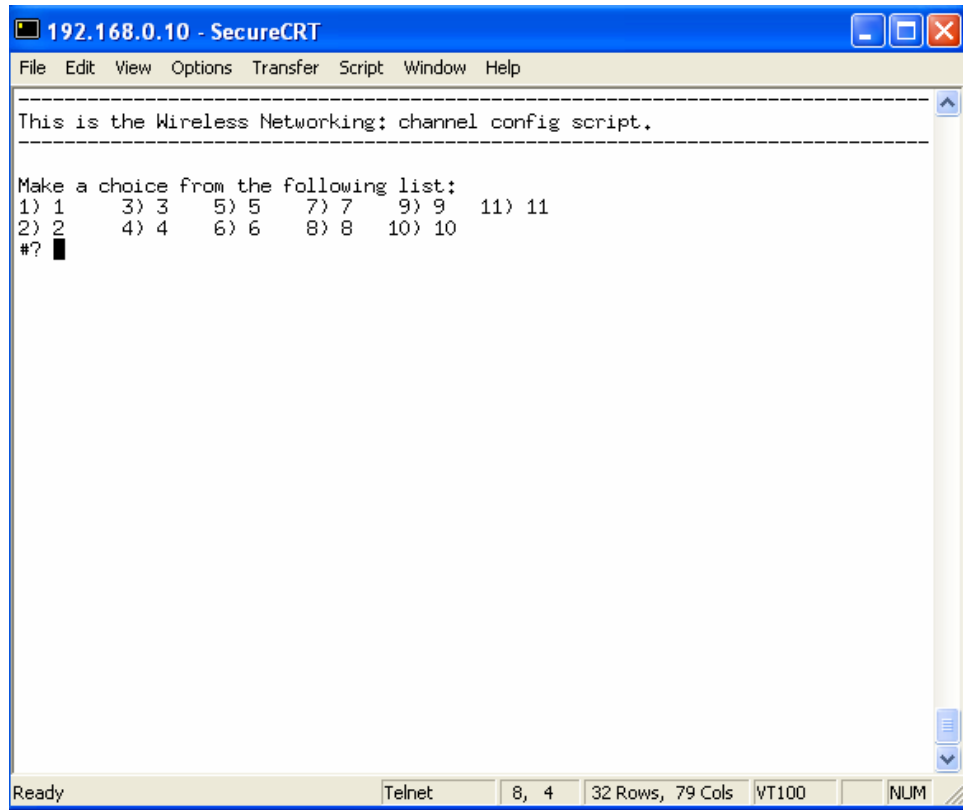


Figure 3-47

Bridge

The (Bridge) option from the Wireless Menu (*Figure 3-48*) allows you to enable or disable the Bridge command. Bridge means the Access point is transparent to the network. Both wired and wireless interfaces have the same IP address and all wired and wireless devices appear to be on the same subnet.

```
192.168.0.10 - SecureCRT
File Edit View Options Transfer Script Window Help
-----
This is the Wireless Networking config script.
-----

Current Wireless Networking settings are:
-----
WLAN_DEVICES=wlan0
WLAN_ENABLE=y
WEP_ENABLE=n
BRIDGE_ENABLE=n
WIRELESS_ESSID=changeme
WIRELESS_MODE=Master
WIRELESS_CHANNEL=1
-----

Make a choice from the following list:
1) QUIT                5) WIRELESS_ESSID    9) WEP
2) Previous_Menu      6) WIRELESS_MODE    10) WEP_SETTINGS
3) Show_All           7) WIRELESS_CHANNEL
4) WLAN_DEVICES       8) BRIDGE
#? 8

BRIDGE_ENABLE (y/n) [n]: █
```

Figure 3-48

WEP

The Wireless Encryption Protection (WEP) option (*Figure 3-49*) allows the user to enable the WEP feature by choosing to enable it upon boot-up or the user may enable at any given time. This option allows the user to individually enable or disable specific WEP keys.

```
192.168.0.10 - SecureCRT
File Edit View Options Transfer Script Window Help
Current Wireless Networking settings are:
-----
WLAN_DEVICES=wlan0
WLAN_ENABLE=y
WEP_ENABLE=y
BRIDGE_ENABLE=n
WIRELESS_ESSID=changeme
WIRELESS_MODE=Master
WIRELESS_CHANNEL=1
WIRELESS_ENC_KEY=restricted
-----

Make a choice from the following list:
1) QUIT                5) WIRELESS_ESSID      9) WEP
2) Previous_Menu      6) WIRELESS_MODE      10) WEP_SETTINGS
3) Show_All           7) WIRELESS_CHANNEL
4) WLAN_DEVICES       8) BRIDGE
#? 9
Enable WEP on boot-up? (y/n) [y]: y
Enable WEP Now? (y/n) [n]: y

Current Wireless WEP Options are:
-----
WEP Enabled: y
WEP Key [1]: off
WEP Key [2]: off
WEP Key [3]: off
WEP Key [4]: off
Active WEP Transmit Key: [1]

Open System Enabled: n

Ready Telnet 32, 42 32 Rows, 79 Cols VT100 NUM
```

Figure 3-49

WEP Settings

The (WEP_SETTINGS) option allows the user to configure WEP settings.

WEP_Keys – Selecting this option allows the user to set up the different WEP keys and choose an active key for the system.

OpenSystem_Enable – The user may select this feature to Open or Close the system to accept or reject non-encrypted packets (data).

```
192.168.0.10 - SecureCRT
File Edit View Options Transfer Script Window Help
-----
This is the Wireless Networking: WEP config script.
-----
Current Wireless WEP Options are:
-----
WEP Enabled: n
WEP Key [1]: off
WEP Key [2]: off
WEP Key [3]: off
WEP Key [4]: off
Active WEP Transmit Key: [1]

Open System Enabled: n
-----
Make a choice from the following list:
1) QUIT                3) WEP_Keys
2) Previous_Menu      4) OpenSystem_Enable
#?
```

Figure 3-50

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 3-51*).

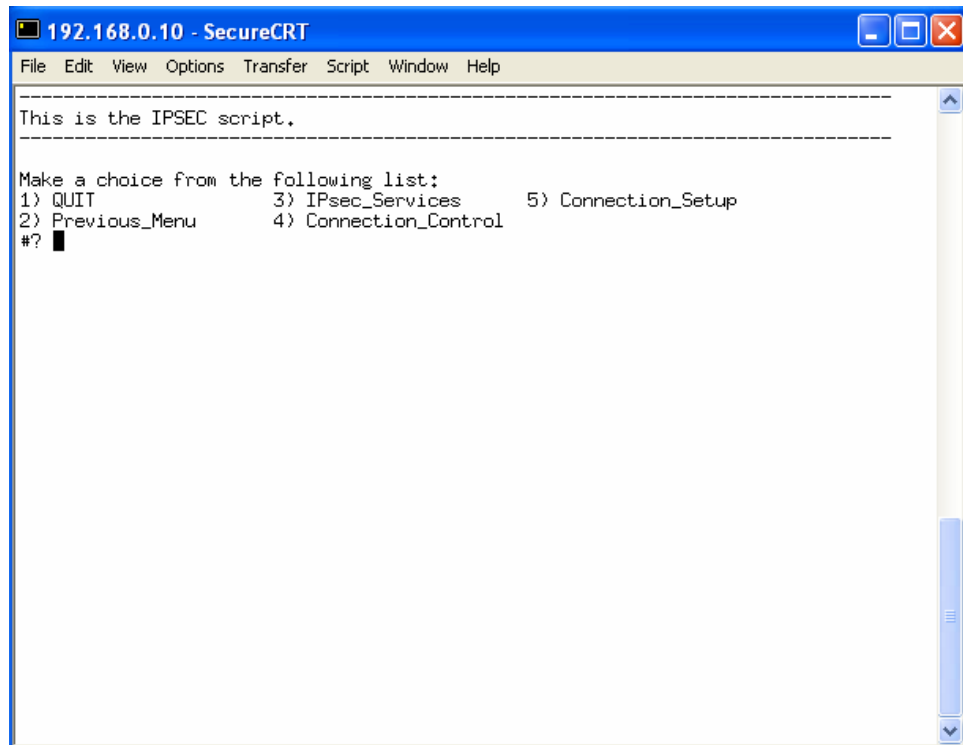


Figure 3-51

IPsec_Services

The (IPsec_Services) option from the IPSEC Menu allows you to control the IP Services for the UAD. The Setup Manager will automatically display the IP Services Control Menu (*Figure 3-52*).

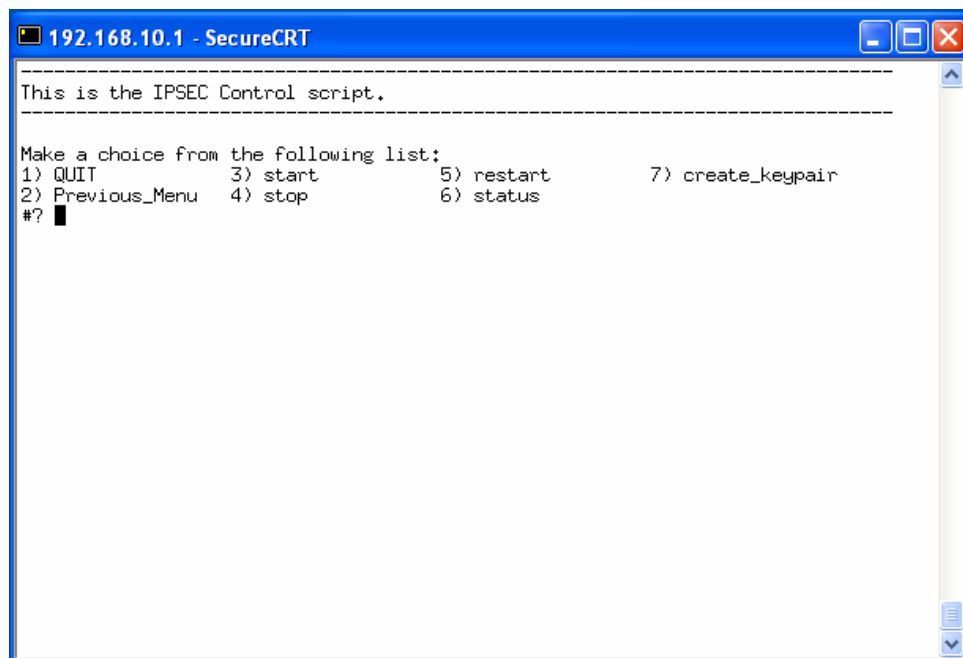


Figure 3-52

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

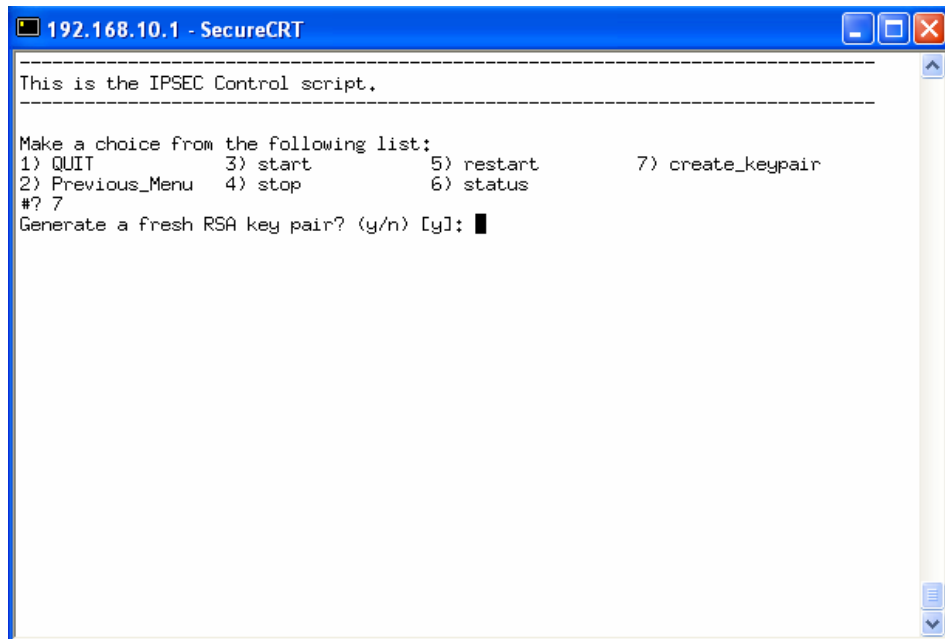
When (restart) from the IPsec_Services Control Menu is selected, the system will RESTART the IP Security Service on the UAD.

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.



```
192.168.10.1 - SecureCRT
-----
This is the IPSEC Control script.
-----
Make a choice from the following list:
1) QUIT          3) start        5) restart      7) create_keypair
2) Previous_Menu 4) stop         6) status
#? 7
Generate a fresh RSA key pair? (y/n) [y]:
```

Figure 3-53

Connection_Control

The (Connection_Control) option from the IPSEC Menu allows you to control the IPSEC Connection for the UAD. The Setup Manager will automatically display the Connection Control Menu (Figure 3-54).

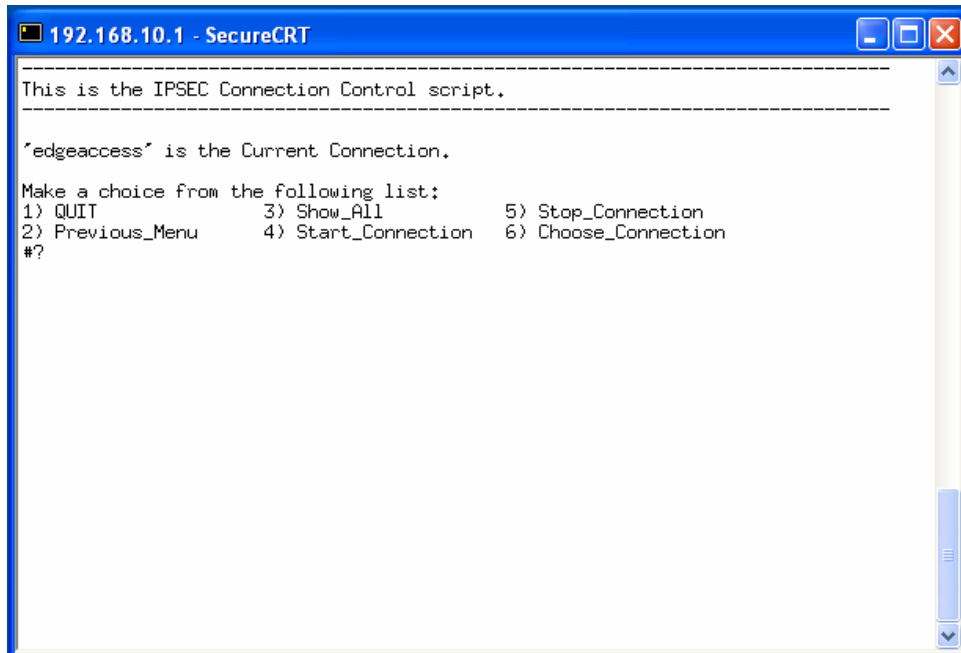


Figure 3-54

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 3-55) will be displayed.

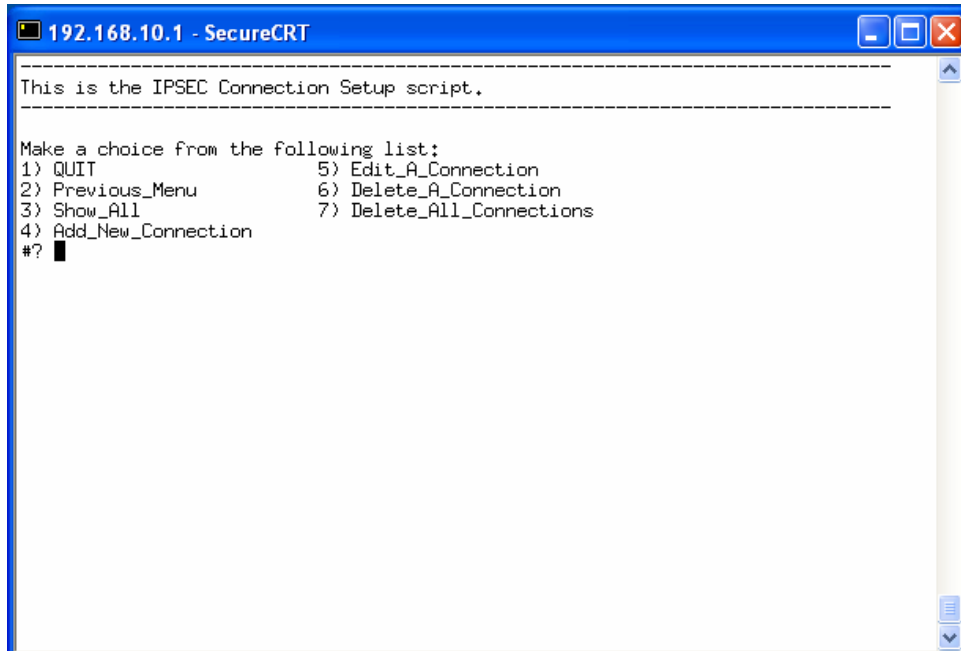


Figure 3-55

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 3-56) will be displayed.

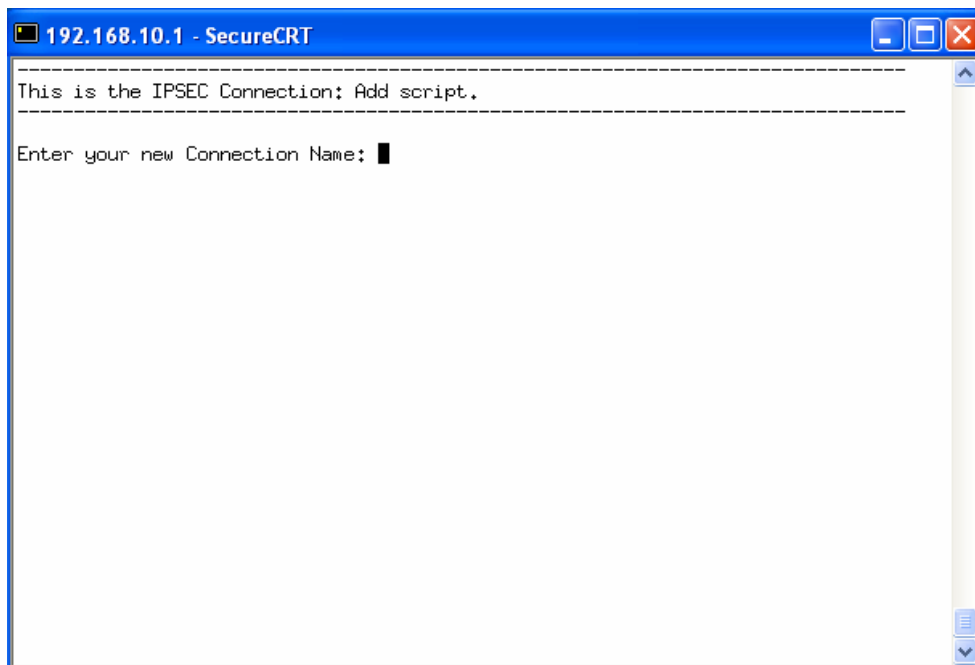


Figure 3-56

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 shown in (Figure 3-57) will be displayed.

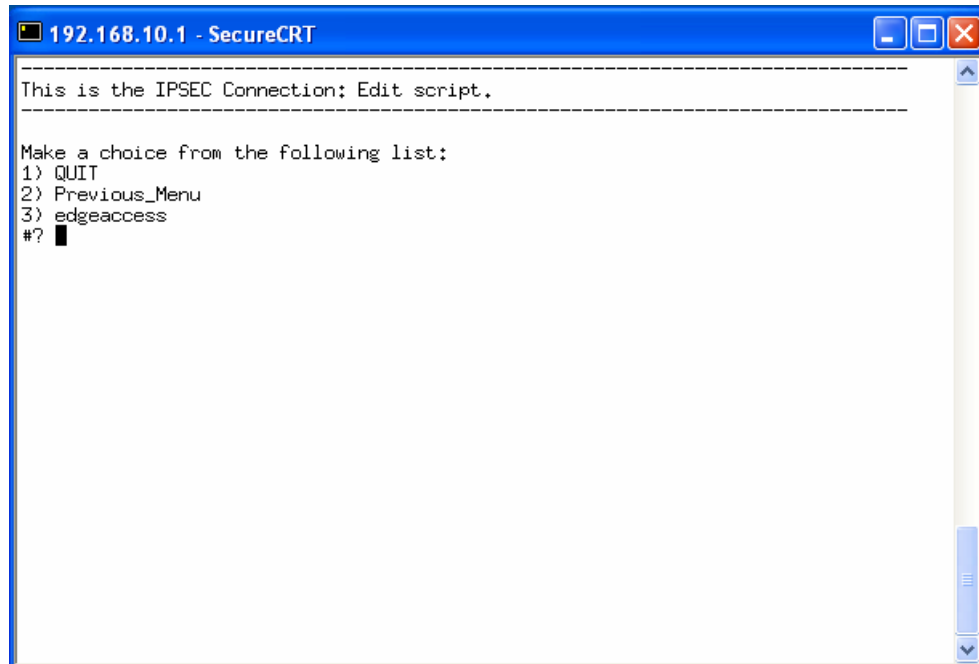


Figure 3-57

From the Edit_A_Connection option, select the IPsec Connection you want to edit. When you choose the IPsec Connection, the following menu (Figure 3-58) will be shown.

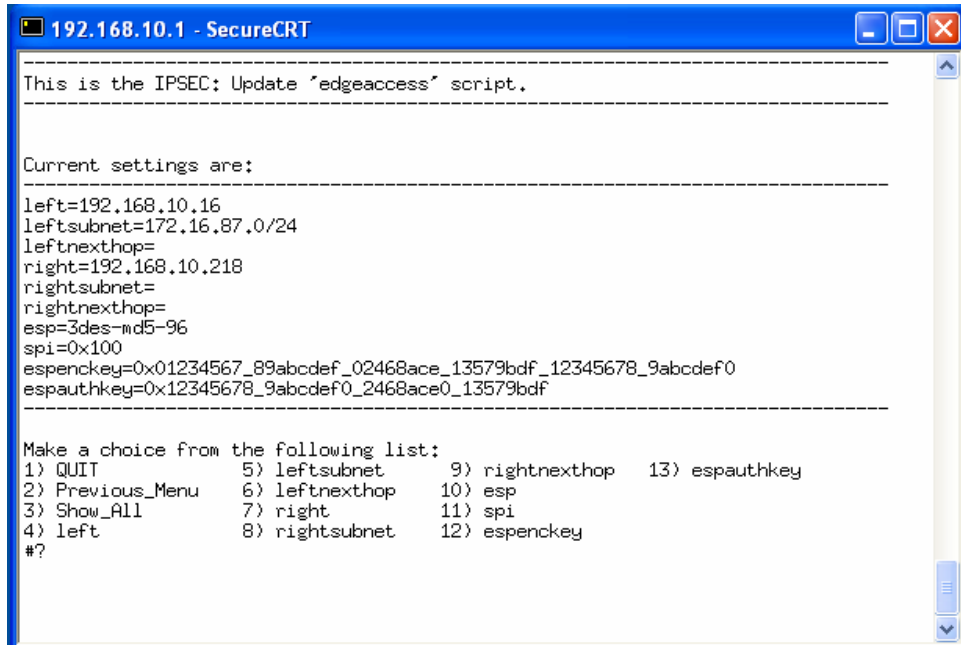


Figure 3-58

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.

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.

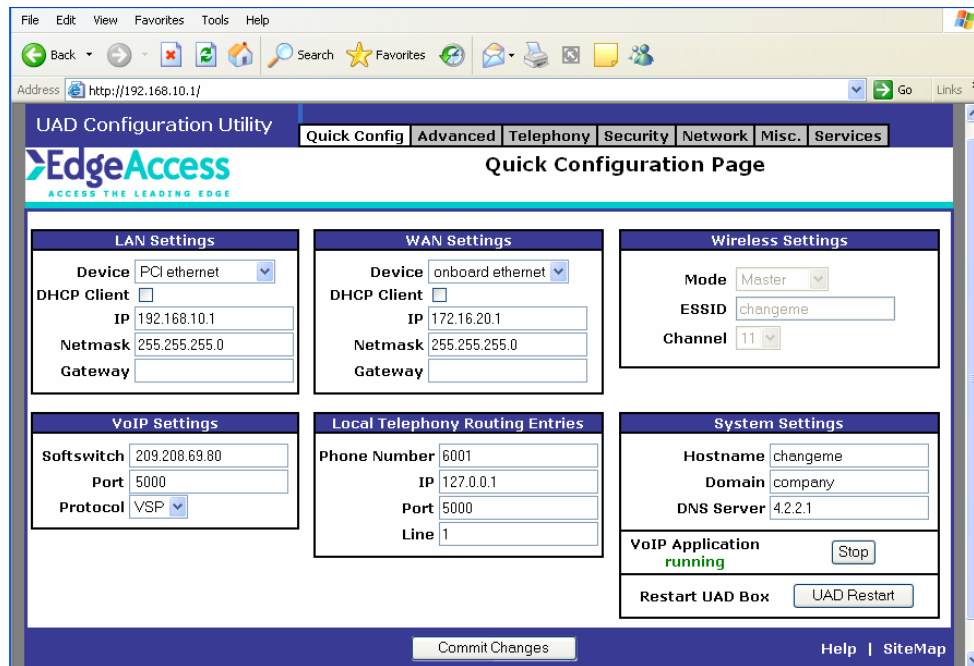


Figure 4-1

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 leave password blank, click Enter.
4. The UAD Configuration Main Menu will appear as shown in (Figure 4-1)
5. Click on each tab to display configuration options.

Telephony Configuration Tab

The Telephony Configuration Tab allows you to configure the telephony setting for the UAD.

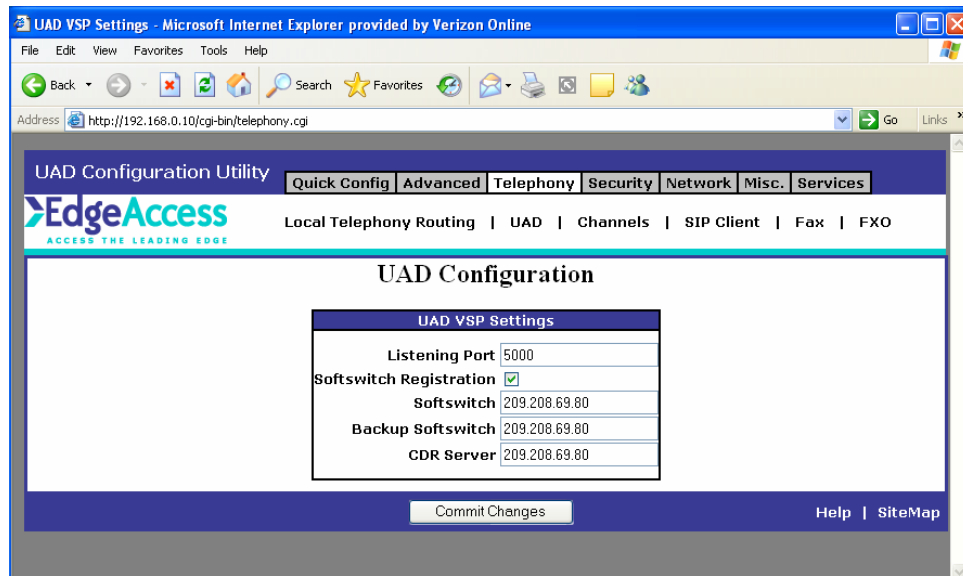


Figure 4-2

UAD Configuration

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.

CDR -Enter the IP address of the machine that will accept CDR.

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

Channel Configuration Tab

UAD Configuration Utility

Quick Config | Advanced | **Telephony** | Security | Network | Misc. | Services

EdgeAccess
ACCESS THE LEADING EDGE

Local Telephony Routing | UAD | Channels | SIP Client | Fax | FXO

Channel 1 Configuration

Channel Select: 1

Channel Settings	Connectivity Settings
<input checked="" type="checkbox"/> Channel Enabled Logical Port: 1 Volume: 0 db Codec: G.723.1 6.3 kbps	Telephone Protocols <input checked="" type="radio"/> VSP <input type="radio"/> SIP <input checked="" type="radio"/> Softswitch Lookup <input type="radio"/> Direct Connect
Frame Duration <input type="radio"/> 10ms <input type="radio"/> 20ms <input checked="" type="radio"/> 30ms	IP Address: 192.168.10.231 Logical Telephony Port: 5 IP Port: 5000 DNIS:
Connectivity Type <input type="radio"/> FXO <input checked="" type="radio"/> FXS	<input type="checkbox"/> Log Call Detail Records (CDR)
Dialing Settings Assigned Number: 1111111 Voice Prompt: default Directory: <input type="checkbox"/> Prefix Connect <input type="checkbox"/> Find/Replace <input checked="" type="checkbox"/> Pass Flash-Hook	Features Settings <input checked="" type="checkbox"/> Call Waiting <input checked="" type="checkbox"/> Caller ID Display <input type="checkbox"/> Caller ID Block
Advanced Settings Input Gain: 0 db DTMF Volume: 0 db DTMF Gain: 0 db Frames per Packet: 2	Call Forwarding <input checked="" type="radio"/> Off <input type="radio"/> All <input type="radio"/> Busy <input type="radio"/> Ring No Answer <input type="radio"/> Ring No Answer or Busy Forwarding Number: Number of Rings: 4
	Missed Call <input type="checkbox"/> E-mail on Missed Call E-mail Address:

Commit Changes SiteMap

Figure 4-4

Channel Settings

To configure the Telephony settings on an UAD, select a Channel from the **Channel Select** field (Figure 4-4).

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).

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.

Log CDR -Select this box enable “Call Detail Records”, logging to a central server as specified on the Telephony-UAD page.

Dial Configuration

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

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.

Features Configuration

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. To enable this feature click on the box.

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 Commit Changes button.

SIP Client

To access the SIP Configuration menu, click on the SIP Client tab. Edit the fields using the information below for reference.

UAD Configuration Utility

[Quick Config](#) | [Advanced](#) | [Telephony](#) | [Security](#) | [Network](#) | [Misc.](#) | [Services](#)

EdgeAccess

 Local Telephony Routing | UAD | Channels | **SIP Client** | Fax | FXO

UAD SIP Client

SIP Client Settings

SIP Transport UDP TCP

SIP Port

RTP Port

Retry Attempts

Retry Timer

SIP Expires

RTP Inactivity Timer

Hold Timer

Invites without SDP Enable Disable

Inband G711 DTMF Enable Disable

Answer Supervision Enable Disable

Registrations Enabled Enable Disable

Proxy Enabled Enable Disable

Entry	Proxy Address
0	<input type="text"/>
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
4	<input type="text"/>
5	<input type="text"/>
6	<input type="text"/>
7	<input type="text"/>

Channel	Username	Password	ProxyOrder
0	<input type="text" value="1111111"/>	<input type="text" value="1111111"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
1	<input type="text" value="2222222"/>	<input type="text" value="2222222"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
2	<input type="text" value="3333333"/>	<input type="text" value="3333333"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
3	<input type="text" value="4444444"/>	<input type="text" value="4444444"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4	<input type="text" value="5555555"/>	<input type="text" value="5555555"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
5	<input type="text" value="6666666"/>	<input type="text" value="6666666"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
6	<input type="text" value="7777777"/>	<input type="text" value="7777777"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
7	<input type="text" value="8888888"/>	<input type="text" value="8888888"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

[Help](#) | [SiteMap](#)

Figure 4-5

SIP Configuration:

Click on the SIP Client tab to change SIP configuration. Edit the fields using the information below for reference.

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 in which the Proxies are to be

Fax

The Fax option operates in two modes: Relay and Bypass Mode.

UAD Configuration Utility

Quick Config | Advanced | **Telephony** | Security | Network | Misc. | Services

EdgeAccess
ACCESS THE LEADING EDGE

Local Telephony Routing | UAD | Channels | SIP Client | Fax | **FXO**

UAD Fax Configuration

Fax Settings

Transfer: ByPass

ByPass NOB: 1 blocks

Volume: -9.5 bps

Max Rate: 14400 bps

Protocol: T38udp

ByPass Coder: G.711 64kbps

Jitter (0-400 msec): 400

Non Extend: Enable Disable

CID: Enable Disable

V34: Enable Disable

V32BIS: Enable Disable

V23: Enable Disable

V22BIS: Enable Disable

V21: Enable Disable

Bell: Enable Disable

ASN1: Enable Disable

HDLC: Enable Disable

ECM: Enable Disable

Negotiation

Retries: 3

Action: Go to Next Position

Image Transmission

Retries: 10

Action: Wait/Do Nothing

Post Transmission

Retries: 10

Action: Wait/Do Nothing

Commit Changes

Help | SiteMap

Figure 4-6

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.

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).

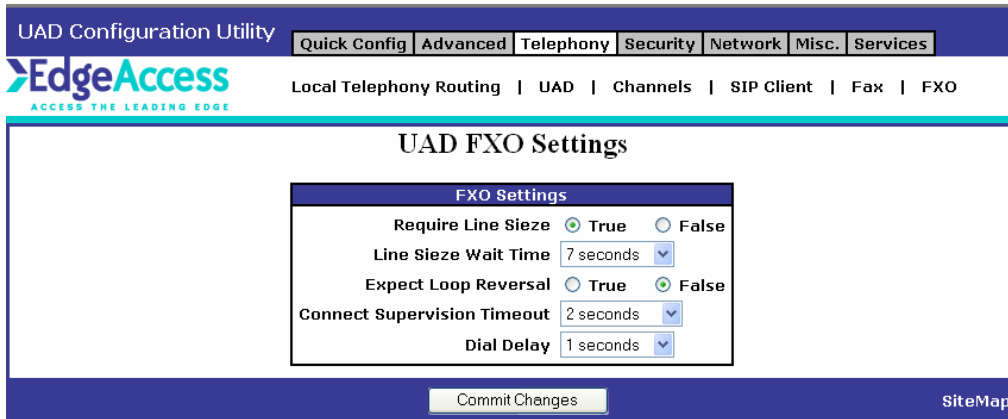


Figure 4-6

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.

Security

WEP

To access Wireless Encryption Protocol (WEP) option, click on the Security tab and then select the WEP link. Select to enable or disable the WEP setting. If enabled, you must enter a key as an access point.

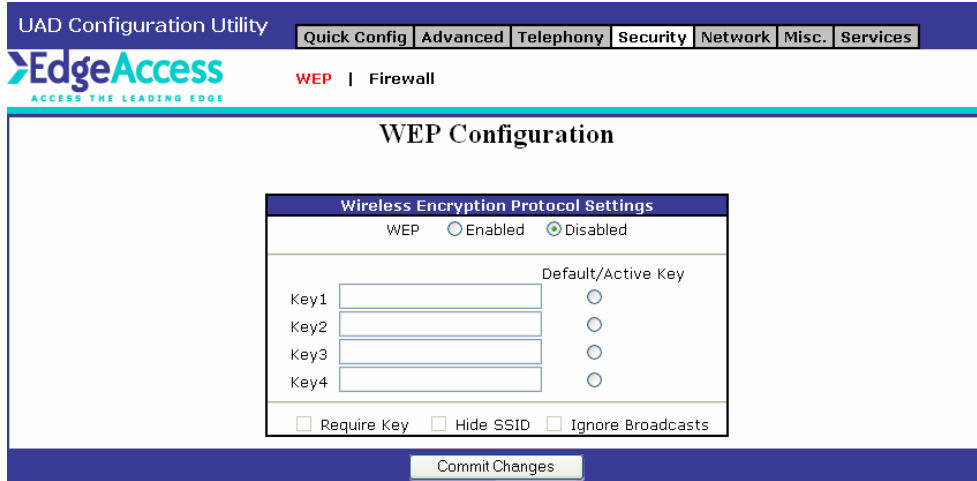


Figure 4-7

Firewall

To access the Firewall option, select on the Security tab and then click the Firewall link.

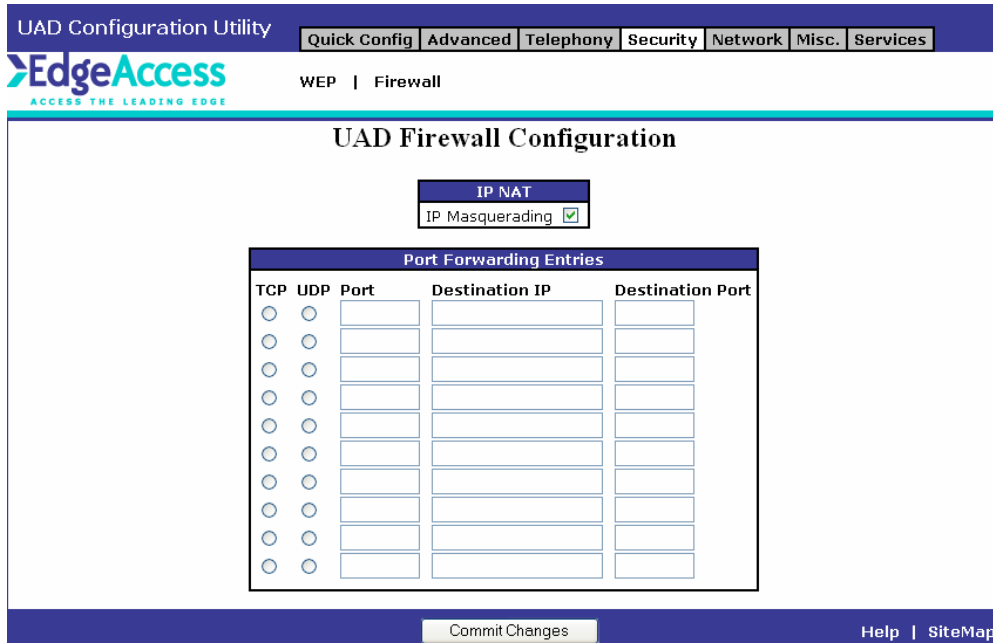


Figure 4-8

Enabling IP Masquerading – Select this box if you would like to enable IP Masquerading that allows Internet connection sharing with PCs on the LAN side of the UAD.

Protocol – Select the type of protocol that the Firewall should expect for messages to be mapped.

Port – Enter the Port where the messages will arrive on the Firewall.

Destination IP – Enter the IP address where the Firewall is to send messages.

Destination Port – Enter the Port Number where the Firewall is to send messages, even if the Port is the same as the Destination Port, enter it here.

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

Network

To configure the Network, select the Network Tab. This tab allows you to configure Interfaces, Traffic Control, Counters, Dial Up, Frame Relay, Wireless, Routing and Serial Bridge.

The screenshot shows the 'UAD Configuration Utility' interface. At the top, there are tabs for 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. The 'Network' tab is selected. Below the tabs, there are sub-tabs for 'Interfaces', 'Traffic Control', 'Counters', 'Dial Up', 'Frame Relay', 'Wireless', 'Routing', and 'Serial Bridge'. The 'Interfaces' sub-tab is active, showing the 'Interface wan Configuration' window. The 'Interface' dropdown is set to 'wan'. The 'Interface Config' section contains the following fields: Device (eth0), Mode (static), IP Address (192.168.0.10), Netmask (255.255.255.0), Network (192.168.0.0), Broadcast (192.168.0.255), and Gateway (192.168.0.1). To the left, the 'System DNS Settings' section has Primary DNS (4.2.2.1) and Secondary DNS (empty) fields. At the bottom, there is a 'Commit Changes' button and 'Help | SiteMap' links.

Figure 4-9

Interfaces

Select whether you are using WAN or LAN interface.

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.

Traffic Control

Traffic Control allows you to enable the Traffic Control commands for the UAD. To enable Traffic Control select the box. When you have made your changes, click on the Commit Changes button.



Figure 4-10

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).

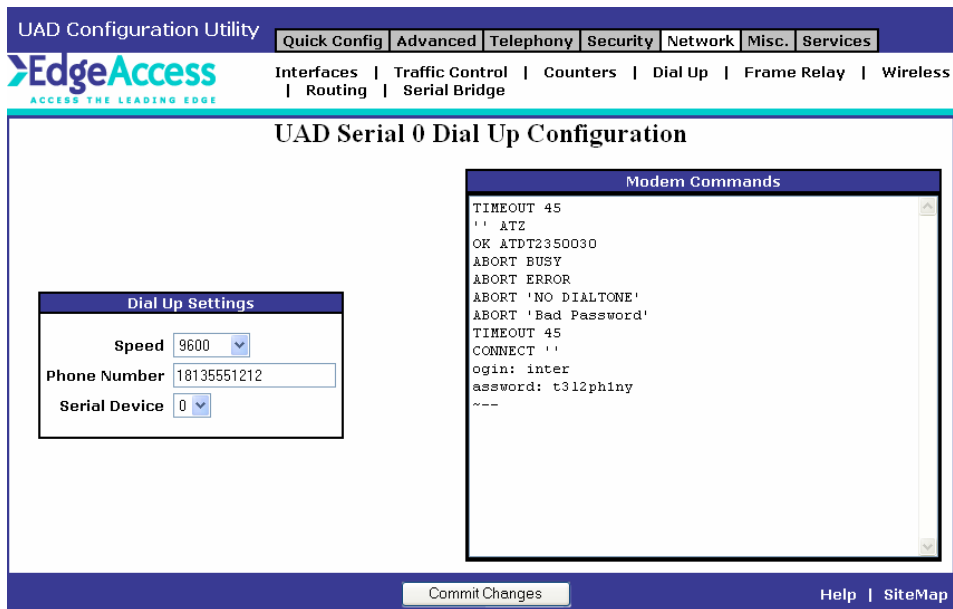


Figure 4-11

Counters

To access the Counters option, click on the Network tab and then select the 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.

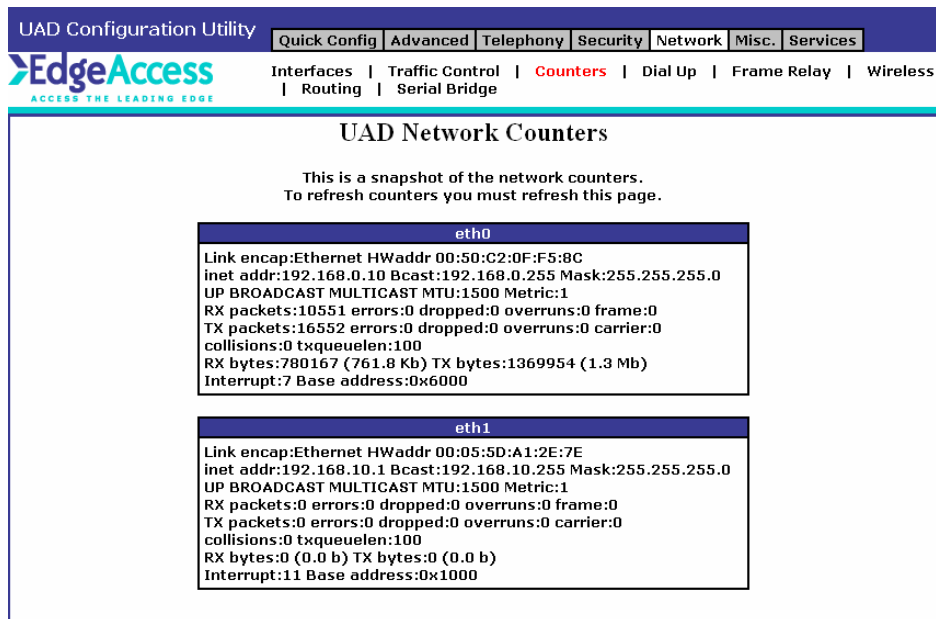


Figure 4-12

Frame Relay

To access the Frame Relay option, click on the Network tab and then select the Frame Relay link. This page allows you to setup the Frame Relay parameters for the T1 WAN or LAN interface on the UAD.

Interface – Choose the Interface that you are using.

Description – Specify a description for the serial interface.

IP Address – Enter the values for the Serial Interface IP address.

Netmask - Enter the values for the Serial Interface Netmask.

Encapsulation – Select the encapsulation type.

DLCI – Enter the number of channels to split to provide service.

Mode – Select the Mode for the T1 interface on the UAD by selecting DCE or DTE.

LMI Type – Select the Local Management Interface type for the T1 interface on the UAD. The LMI type is the protocol of how the data is transmitted.

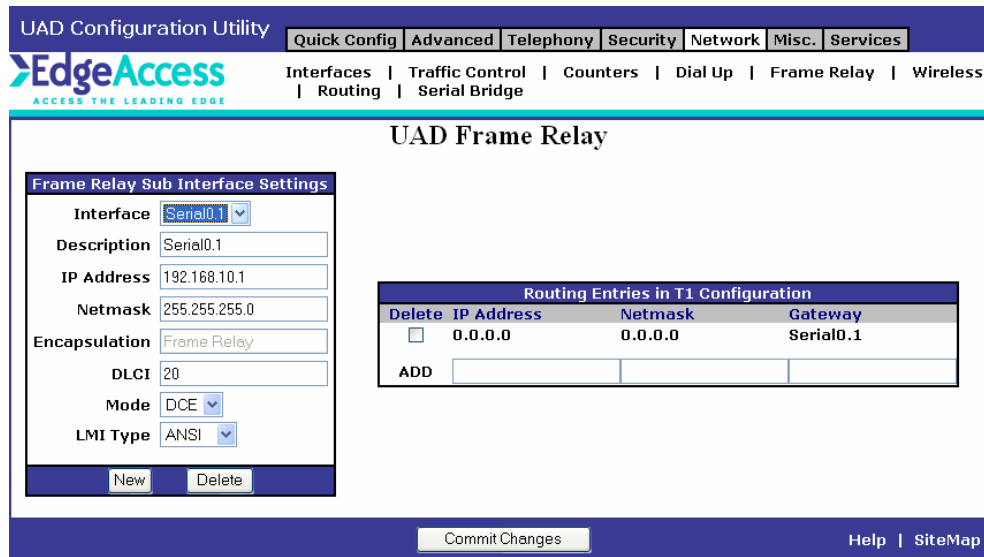


Figure 4-13

Routing Entries in T1 Configuration – To add routing entries, enter the values of the IP Address, Netmask and Gateway. To remove a routing entry, select the Delete box, enter the IP Address, Netmask and Gateway.

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

Wireless

The Wireless option allows the user to enable Wireless Access Point functionality by choosing on of the following modes: Master, Managed or Ad-Hoc. To access the Wireless option, select the Network tab and then click on the Wireless link.

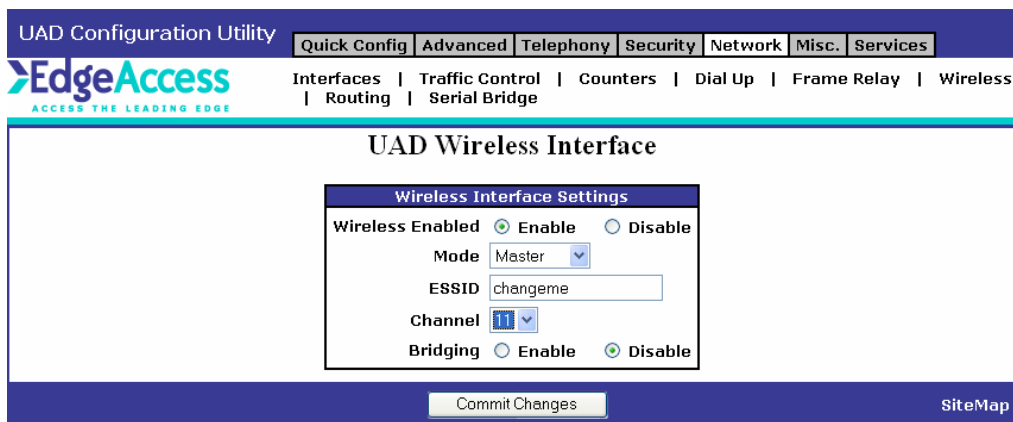


Figure 4-14

Wireless Enabled – To turn on or off the Wireless Access Point functionality, select Enable or Disable.

Mode – Select the Mode for the T1 interface on the UAD.

ESSID –

Channel – Select the number of channels.

Bridging – To turn on or off the Bridging feature, select Enable or Disable.

Click on the Commit Changes button.

Routing

To access the Routing option, click on the Network tab and then select the Routing link. This page allows you to setup the route information for the UAD.

The screenshot displays the 'UAD Routing' configuration page. At the top, there is a navigation bar with tabs for 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. Below this, there are sub-tabs for 'Interfaces', 'Traffic Control', 'Counters', 'Dial Up', 'Frame Relay', and 'Wireless', with 'Routing' selected under 'Interfaces'. The main content area is titled 'UAD Routing' and contains two tables. The first table, 'Current Routing Table', has columns: Delete (checkbox), Destination, Gateway, Netmask, Flags, Metric, Use, and Interface. It lists four routes: 192.168.0.0 (eth0), 192.168.10.0 (eth1), 127.0.0.0 (lo), and 0.0.0.0 (eth0). Below this table is an 'ADD' button and input fields for Destination, Gateway, Netmask, and Interface (set to eth0). The second table, 'Static Routes', has columns: Delete (checkbox), Destination, Netmask, Gateway, and Interface. It also has an 'ADD' button and input fields. At the bottom of the page is a 'Commit Changes' button and a 'Help | SiteMap' link.

Figure 4-15

To add a route, enter the Destination, Gateway, Netmask and choose and Interface. Then click the Commit Changes button.

To delete a route, enter the Destination, Gateway, Netmask and Interface. Then click the 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.

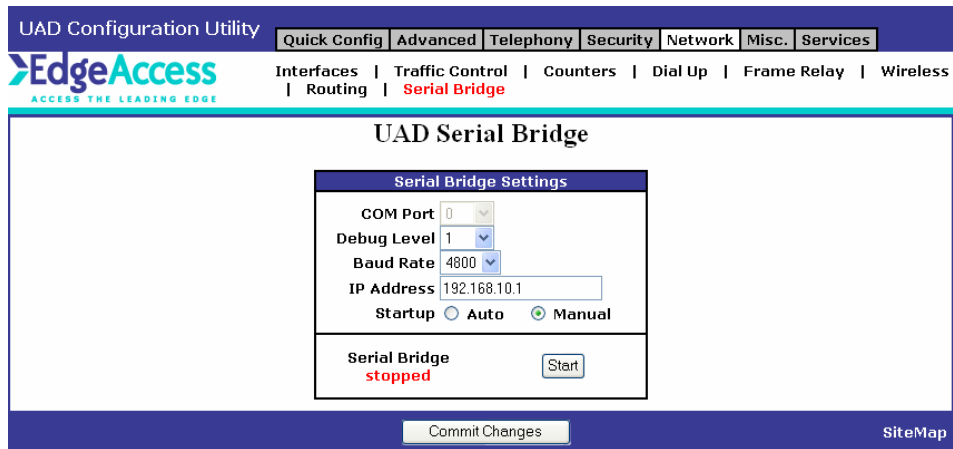


Figure 4-16

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

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.

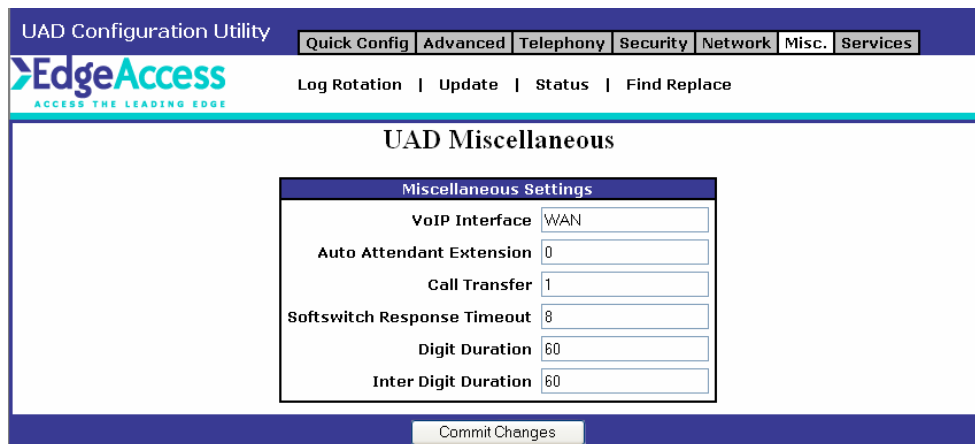


Figure 4-17

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.

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

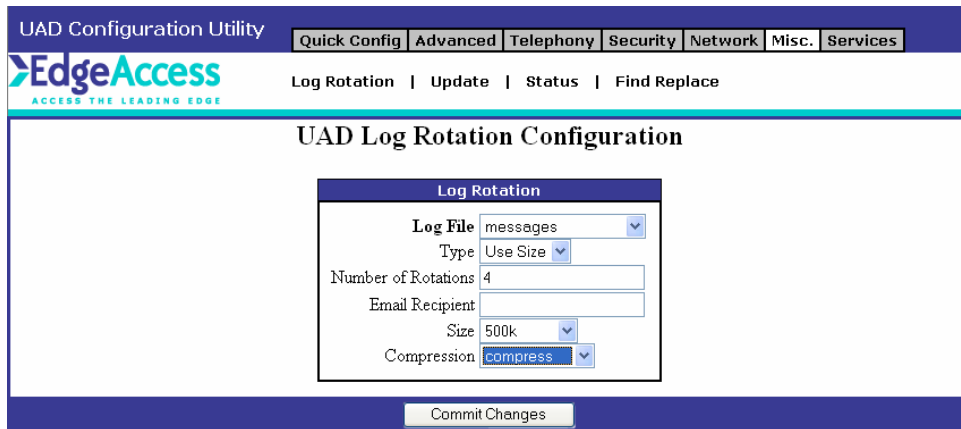
Call Transfer – Type (1) to enable or (0) to disable the Centrex-type Call Transfer function.

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.

Log Rotation

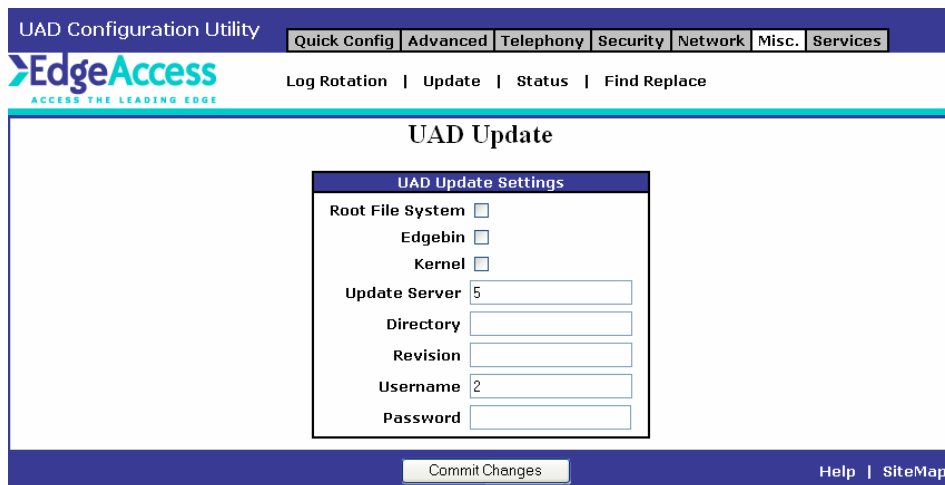


The screenshot shows the 'UAD Log Rotation Configuration' page in the UAD Configuration Utility. The page has a blue header with the 'EdgeAccess' logo and navigation tabs: 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. Below the header, there are links for 'Log Rotation', 'Update', 'Status', and 'Find Replace'. The main content area is titled 'UAD Log Rotation Configuration' and contains a form with the following fields: 'Log File' (dropdown menu set to 'messages'), 'Type' (dropdown menu set to 'Use Size'), 'Number of Rotations' (text input set to '4'), 'Email Recipient' (text input), 'Size' (dropdown menu set to '500k'), and 'Compression' (dropdown menu set to 'compress'). At the bottom of the form is a 'Commit Changes' button.

Figure 4-18

Update

To access the Update option, click on the Miscellaneous tab and select the Update link. This option allows you to set the Update parameters for the different software modules.



The screenshot shows the 'UAD Update' page in the UAD Configuration Utility. The page has a blue header with the 'EdgeAccess' logo and navigation tabs: 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. Below the header, there are links for 'Log Rotation', 'Update', 'Status', and 'Find Replace'. The main content area is titled 'UAD Update' and contains a form with the following fields: 'Root File System' (checkbox), 'Edgebin' (checkbox), 'Kernel' (checkbox), 'Update Server' (text input set to '5'), 'Directory' (text input), 'Revision' (text input), 'Username' (text input set to '?'), and 'Password' (text input). At the bottom of the form is a 'Commit Changes' button. In the bottom right corner of the page, there are links for 'Help' and 'SiteMap'.

Figure 4-19

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.

Status

To access the UAD Status option, click on the Miscellaneous tab and then select the Status link. The Status option displays the current settings for the UAD.

UAD Configuration Utility

Quick Config | Advanced | Telephony | Security | Network | Misc. | Services

EdgeAccess
ACCESS THE LEADING EDGE

Log Rotation | Update | **Status** | Find Replace

UAD Status

UAD Device Status
Number of Ports: 4
Software Version: 5.68 SIP&VSP
Application up since: Oct 18 2004 06:15:49
Current date/time: Oct 20 2004 19:06:22
Softswitch Registration: ON
Primary Softswitch: 209.208.69.80
Backup Softswitch: 209.208.69.80
Device: /dev/vhub0
FPGA Code: IAD41165
Type of Device: iad4 rev. 0 (4810x DSP) FXS only

Channel Status
Port[1] FXS - trunk[1], +()1111111 [STATE_IDLE]
Port[2] FXS - trunk[2], +()2222222 [STATE_IDLE]
Port[3] FXS - trunk[3], +()3333333 [STATE_IDLE]
Port[4] FXS - trunk[4], +()4444444 [STATE_IDLE]

Miscellaneous
DHCP Server: On
Traffic Control: Off
RFS Version: 2004-07-15.1616
Edgebin Version: 2004-07-15.1212
Application: Running
Hostname: lb_pain
IP Masquerading: On
Interfaces: eth0 eth1

SiteMap

Figure 4-20

Find Replace

To access the Find Replace option, click on the Miscellaneous tab and select the 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.

The screenshot shows the 'UAD Configuration Utility' interface. At the top, there is a navigation bar with tabs: 'Quick Config', 'Advanced', 'Telephony', 'Security', 'Network', 'Misc.', and 'Services'. Below the navigation bar is the 'EdgeAccess' logo and the text 'ACCESS THE LEADING EDGE'. To the right of the logo are links for 'Log Rotation', 'Update', 'Status', and 'Find Replace'. The main content area is titled 'UAD Find Replace' and contains the following text: 'Please select the Find Replace table you wish to modify by clicking the hyperlinks below. Current table selected has a White background.' Below this text are two buttons: 'Collecting Digits' (highlighted in white) and 'Outdialing Digits' (highlighted in grey). Below the buttons is a table titled 'Collecting Digits Find Replace Settings'. The table has four columns: 'Delete', 'Find', 'Replace', and 'Except'. The 'Find' column contains the text 'No Entries' and an 'ADD' button. Below the table is a 'Commit Changes' button and a 'SiteMap' link.

Figure 4-21

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.

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.

UAD Configuration Utility

Quick Config | Advanced | Telephony | Security | Network | Misc. | Services

EdgeAccess
ACCESS THE LEADING EDGE

DHCP Server | SIP Proxy | Web Server

UAD DHCP Server

DHCP Server Settings

DHCP Server Enable Disable

Interface

Required Parameters	Value
Network	<input type="text" value="192.168.0.0"/>
Netmask	<input type="text" value="255.255.255.0"/>
Begin Range	<input type="text" value="192.168.0.20"/>
End Range	<input type="text" value="192.168.0.50"/>
Lease Time	<input type="text" value="84600"/>
Max Lease Time	<input type="text" value="604800"/>

Optional Parameters	Value	Enabled
Broadcast	<input type="text" value="192.168.0.255"/>	yes <input checked="" type="radio"/> no <input type="radio"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	yes <input checked="" type="radio"/> no <input type="radio"/>
Router	<input type="text" value="192.168.0.10"/>	yes <input checked="" type="radio"/> no <input type="radio"/>
DNS Server	<input type="text" value="4.2.2.1"/>	yes <input checked="" type="radio"/> no <input type="radio"/>
Domain Name	<input type="text" value="company"/>	yes <input type="radio"/> no <input checked="" type="radio"/>

Commit Changes

Help | SiteMap

Figure 4-22

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

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.

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

UAD Configuration Utility

Quick Config | Advanced | Telephony | Security | Network | Misc. | Services

EdgeAccess
ACCESS THE LEADING EDGE

DHCP Server | SIP Proxy | Web Server

UAD Web Server

Web Server Settings

Use SSL

Commit Changes

SiteMap

Figure 4-23

Monitoring via Telnet or Hyper Terminal

1. You must have “**root**” user access to start or stop to VoIP application.
2. From a Windows – based machine, connect to the UAD by one of the two following methods:
 - A. **Telnet** (Click Start button then Click the Run button): Type telnet X.X.X.X (IP Address of UAD).
 - B. **Hyper Terminal** (Click Start button then Click the Run button): Type **hypertrm**, and type the name for the HyperTerminal session configured for the UAD.
3. Type “**voip**” for the username and press **[Enter]**, for the password press **[Enter]** (default is a black password).
4. Type “**su**” to login as “**root**” user and press **[Enter]**, for the password type “**default**” and press **[Enter]** (default password is “default”).
5. Type **vhubctl restart [debug level] &** this will restart the application in debug mode. (See debug levels section for more info).
6. To Stop the application type **vhubctl stop**.
7. To Start the application type **vhubctl start**.

**Note: If the application is stopped accidentally the UAD will NOT automatically start the application.*

UAD Debug Levels

To set the debug level type **vhubctl start ABCD**.

The debug values are described below:

A stands for miscellaneous messages that can be shown with the following values:

- 0 = do not show miscellaneous messages
- 1 = show line interrupts
- 3 = show digit related messages
- 7 = show other minutia messages

8 = show time related messages

B stands for gatekeeper messages that can be shown with the following values:

0 = do not show gatekeeper messages

1 = show gatekeeper message s cha n, type, and reply

3 = also show gatekeeper message contents

7 = also show gatekeeper message plus more

C stands for gateway messages that can be shown with the following values:

0 = do not show gateway messages

1 = show gateway message direction, chan, and type

3 = also show gateway message remote end

7 = also show gateway message contents

D stands for state changes that can be shown with the following values:

0 = do not show state changes or config messages

1 = show state changes

3 = also show configuration message code

7 = also show configuration message contents

Call Transfer

There are two different ways that you can transfer a telephone call:

1. Supervised.
2. Unsupervised.

Unsupervised:

1. Party A (transferee) calls Party B (transferor) blind transfer to Party C (transfer target).
 - a. A calls B and wants to be transferred to C.
 - b. B presses Flash and Gets a dial tone.
 - c. B dials *30 followed by the number or extension for C.
 - d. If transfer is successful (That is C picks up the phone...) all is good with the transferor that is B. If C is busy or not a valid phone number..., Party B gets a ring back and when B picks up talks with A again.

Supervised:

1. Party A calls B supervised transfer to C.
 - a. A calls B...A and B are talking.
 - b. B presses flash and dials the number (no *30) to reach C.
 - c. If C answers the phone and wants to talk to A then hang-up B and C, so A will be transferred to C.
 - d. If C does not want to talk to A B presses flash and B will be talking to A...C can hang-up and he won't be transferred.
 - e. If C does not pick up the phone or is busy when B tries to reach him, then if B presses flash he will be connected back to A... Or if B hangs up A will ring back B.

INDEX

A

Adding a New Port Map 40, 72

Authorization Codes..... 6

C

Call Barring 6

Call Detail Record 11

Call Forwarding..... 6, 80

Call Progress Detection 14

Call Restriction..... 6

Call Waiting..... 6, 80

Caller ID..... 6, 80

Classes 6, 42

Coder Type 11, 78

Connect Supervision Loop Reversal..... 14, 79

Connect Supervision Timeout..... 14, 79

Connection Type..... 11, 63, 64, 65, 79

D

Deleting a Port Map 40

DHCP Client 7, 18, 23

DHCP Server 7, 24, 94

Direct Dial	12, 79
DNIS	12, 79
DTMF Gain	80
DTMF Volume.....	80

E

Encoding.....	11
---------------	----

F

Fax.....	82
Filtering	6
Filters	42, 45
Firewall	6, 39, 74, 85
Frame Relay	31-36, 88
FXO	4, 5, 11, 13, 73, 74, 83
FXS.....	5, 11, 15, 73

H

HDLC	36
Hostname	10, 20, 52, 77

I

Input Gain	80
Installation.....	9
IP Security	67

L

LAN Settings.....	4, 6, 7, 8, 9, 10, 15, 16, 18, 37, 39, 46, 80
-------------------	---

Line _Seize	13, 84
Listening Port	11
Log CDR	12, 79
Logical Port	11, 78
N	
NAT	4, 5, 6, 7
Network	80
P	
Password	9, 10, 18, 50, 51, 60, 69, 85, 89
PING	52
Prefix Connect	13, 80
Proxy Server	6
Q	
Qdisc	42, 45
S	
Security	85
Setup Manager	16, 18, 20, 22, 24, 27, 37, 56, 57, 58, 59, 60, 61, 63, 85
SIP	81
Softswitch Lookup	6, 79
Softswitch Registration	11, 76
Static Routes	38

T

Toll Call 13

Traffic Control 42, 43, 87

U

Update 54

Utilities 50

V

Voice Prompt Directory 13

VoIP Interface 46

W

WAN Settings.....4, 7, 8, 16, 20, 22, 23, 24, 27, 46, 80, 83

Web Manager 17, 75