To log out of a phone, do the following:

1. Select User | Log out of group.
2. The display changes to:

```
Group log out
➡all
 Lancelot Capability
```

   The display shows the names of all the users who have temporarily logged into the phone as an operator or agent. If more than one user has logged into the phone, the phone displays "all" as the first selection.

3. Use the Up and Down buttons to select the individual you want to log out, or select "all" to log all users out of all groups, and press the Enter button.
4. The phone ceases to light the LED on the User button green continuously if there are no other additional users logged into the phone and no user is logged into an ACD group or operator group. When you use the headset, the same LED is lit continuously red.
5. If there were no ACD agents logged into the ZIP4x5, the display shows instead:

```
User log out
No user is logged in
```

   When you press any key, the phone displays the idle screen.

This function is used to log out of an operator or ACD group. When you use this function, the phone removes you from all groups that you have logged into. If you had logged into multiple groups, and you want to log out of one group but remain in one or more other groups, you must log back into the groups after executing this command.

7.4 Do Not Disturb (DND)

Press this button if you want to receive no calls. The phone lights the LED on the button continuously red. The display does not change. When you set DND, it has no effect on calls that you have in progress or calls that are on hold.

If you have configured any forwarding rules on the phone, setting DND overrides those rules. When this function is active and the ZIP4x5 receives a call it immediately rejects it. The phone does not make any sound, does not light any of the call appearance buttons, and does not change the display. If you press this button when you have one or more incoming calls, you will reject all incoming calls.

If your phone is idle,[1] the phone displays the number of calls that you have missed, for example:

```
Sales support
17 missed calls
Mon 26 Jan 04  20:31
```

1. See section 6.3.1 on page 50 for a definition of the idle state.

To remove the DND function, press the button again.

To call a person who had called you see section 9.7.5 on page 124.

7.5 Forward

7.5.1 Description

When the phone forwards a call, it redirects an incoming call to another destination (name or number). The destination can be another extension within the enterprise or an external number. You can turn on and off forwarding to instruct the phone to forward calls:

- unconditionally (all calls)
- if you do not answer the phone (on no answer)
- if you have an active call (when busy)

7.5.2 Unconditional

If you have configured the phone to forward calls unconditionally the phone does not announce that it is receiving an incoming call. It does not change the display or any LED. The phone immediately forwards the call to the destination that you have specified.

When the phone receives an incoming call, it does not accumulate this as a missed call.

7.5.3 On No Answer

If you have configured the phone to forward calls on no answer, the phone announces an incoming call in the usual manner. If you do not answer the call within ten seconds, the phone transfers the call to the destination that you have specified.

The phone counts the number of calls that it forwards on no answer as missed calls.

7.5.4 When Busy

If you have configured the phone to forward calls when busy, the phone announces an incoming call in the usual manner if you do not have an active call.

If you have an active call, the phone forwards the call to the destination that you have specified. In this case, an active call is one where you are in the middle of a conversation or when you have put a conversation on hold. That is, the phone has a call button whose LED is lit continuously green or orange, or flashing green or orange.

If the phone receives more than one incoming call, the phone will indicate there are incoming calls on multiple call appearances. As soon as you answer one of the calls, the phone is now busy and it immediately forwards the other calls to the destination that you have specified.

The phone counts the number of calls that it forwards when busy as missed calls.

7.5.5 Configuring

Press the Forward button.[1] The display changes to:

```
Forward
➡off
 all calls
 on no answer
 when busy
```

This example shows five rows, though in practice the display can show only three rows at once. As you press Up and Down, the display scrolls through the list of choices. Press the Enter button to select a choice or the Esc button to cancel.

When you make a selection other than *off*, the display changes to one of the following to prompt you to enter a name or number to which the calls should be redirected:

```
Forward
all calls
➡1704
```

```
Forward
on no answer
➡1066
```

```
Forward
when busy
➡1415
```

You can enter the name or number from the keypad as you would if you were making a call, or from a memory location.[2]

After you enter a name or number and press the Enter button, the phone lights the LED on the Fwd button continuously green. If you select *off*, the LED is turned off.

7.6 Park

The functionality of call park and call pickup are dependent on the phone system. You can park individual calls and conference calls. The following description is based on connecting your ZIP4x5 to a phone system that fully supports the park and pickup function.

1. You can access this feature through the menu, under settings. Pressing the Forward button is a short cut.
2. See section 9.7.3 on page 122 and section 9.7.4 on page 123 for a description of how to specify a memory location.

7.6.1 Individual Call

To park a call, ensure you are in active communication with the person. That is, the LED on the call appearance button is lit continuously green. Press the Park button. The ZIP4x5 transfers the call to the park server and appears to the other person as if the call has been placed on hold.[1] The person with whom you were talking hears music on hold supplied by the phone system.[2]

The system issues you a two digit number and the screen changes to:

```
Park on 37
Lancelot Capability
Brown
```

You must note the two digit number that the system issues to you (in the example above it is 37). The display remains unchanged until another action takes place.

The phone transfers control of the call to the phone system, turns off the LED on the call appearance button, turns the LED on the Park button continuously red, and sounds an audible double beep in the earpiece or speaker. You can place the phone on hook.

The phone continues to display the screen shown above, and continues to light the LED on the Park button, until you go on hook, press a call appearance button, or use another function or feature of the phone. If the phone receives an incoming call, it will retain the display for a minimum of two seconds.

The phone does not provide dial tone until you go on hook and off hook again or you press a call appearance button.

To retrieve the call use the Pickup function as described in section 7.7 on page 68.

7.6.2 Failure to Park an Individual Call

If the park is unsuccessful, the phone displays:

```
* Failure to park *
Lancelot Capability
Brown
```

The phone retains this display until you press a key, lift the handset, or replace the handset, after which it displays the screen that the phone was showing prior to you attempting to park the call. You remain connected to the other person.

You can try to park the call again, but if your attempts to park a call fail repeatedly, you should consult your system administrator.

1. See section 10.6.5 on page 176 for details how to configure the address of the park server.
2. See section 9.5.2 on page 116 for a description of the hold function.

7.6.3 Conference Call

When you park a conference call, the ZIP4x5 parks each of the calls that comprise the conference call sequentially. The phone system returns a two digit park number for each of the calls in your conference call. For example, if you had three parties in a conference call, the phone displays:

```
Park on 57 58 59
Conference call
```

The phone system normally issues sequential numbers for the park numbers, but this cannot be guaranteed.

When you park the conference call, the parties to the call hear music on hold and cannot communicate with one another until you pickup the call as described in section 7.7 on page 68.[1]

7.6.4 Failure to Park a Conference Call

If the park is unsuccessful, the phone displays XX instead of a park number:

```
Park on 57 XX 58
Conference call
* Failure to park *
```

The phone retains this display until you press a key, lift the handset, or replace the handset, after which it displays the screen that the phone was showing prior to you attempting to park the call. You remain connected to the party or parties that were not parked.

You can try to park the call again, but if your attempts to park a call fail repeatedly, you should consult your system administrator.

7.7 Pickup

The functionality of call park and call pickup are dependent on the phone system. You can pickup an individual call or a conference call that has been parked with the Park function as described in section 7.6 on page 66.

You can pickup a call that you parked yourself or that another person parked. You cannot pickup a call that was parked if the other party terminated the call while the call was parked.

1. This is different from placing the conference on hold as described in section 9.8.2 on page 127.

7.7.1 Individual Call

You can resume a conversation that has been previously put on hold with the Park function using any ZIP4x5 phone. Press the Pickup button. The phone lights the LED continuously red on the Park button and displays:

```
Pickup from
➡
```

Enter the two digit number for the parked call and press the Enter button or the # key. If you specify an invalid number (or if the party who was parked terminated the call in the mean time), the phone displays:

```
Pickup from
➡37
(36 is invalid)
```

If the phone is off hook, the phone will play the fast busy tone when you have entered an invalid number. You can enter a valid number or press the Esc button to exit the function.

Once the phone is connected to the parked call, the phone turns off the LED on the Pickup button and changes the display to the usual display of a call being connected, as described in section 9.3.5 on page 109.

If you forget the two digit number, call the operator for assistance. The operator may be able to assist you to find the number.

If you pickup a parked call that you had not intended to pickup, park the call again. Call the operator and tell the operator what has happened.

7.7.2 Conference Call

To pickup a conference call, you must pickup each of the calls that was parked. Therefore, you use the pickup function more than once to resume the conference.

1. Press the Pickup button.

   The phone lights the LED continuously red on the Park button and displays:

```
Pickup from
➡
```

2. Enter the two digit number for one of the parked calls and press the Enter button or the # key.

   You are now communicating with one of the people on the conference call.

3. Press the Conf key.

   The phone lights the first call appearance orange and selects a second call appearance.

4. Repeat from item 1 until you have picked up all members of the conference call.

If you try to pickup from an invalid number, the phone display indicates the error shown in the previous section.

7.8 Page

A page is an announcement sent to multiple people without those people needing to answer the phone. The phone plays the announcement through its speaker and you do not need to take the phone off hook to hear the announcement. If you have an active conversation (the LED on a call appearance button is lit continuously green or orange), the phone may or may not play the announcement depending on the settings chosen by the system administrator. The functionality of paging is dependent on the phone system.

To make a paging announcement, do the following:

1. If you have any active calls, put them on hold or terminate them.
2. If you have calls in progress on all four call appearances, you cannot page. Terminate at least one of the calls to make a call appearance available.
3. Either:
   a. Go off hook and press the Page button; or
   b. Press the Page button.
4. The ZIP4x5 accesses the phone system and changes the display to:

```
Page
Retrieving list
▇▇▇▇▇▇▇▇          01:17
```

   The phone shows a new bar every second and maintains the total time on the right of the third row of the display. Every 10 s the phone clears the bars and then starts to show them one by one again.[1]
5. If the phone encounters an error, it displays one of the screens shown in section 7.9 on page 71.
6. The phone lights the LED on the Page button continuously red.
7. The phone changes the display to:

```
Select paging group
➡Inside Sales
 Finance
```

   The phone displays a list of paging groups that you are allowed to page. This list is defined by the system administrator.
8. Use the Up and Down buttons or the Up and Down keys to select the group you want to page and press the Enter button.

1. The length of time taken to access the server depends on the number of paging groups and the activity on your network. This could be anywhere from a second to a minute.

The phone selects the lowest numbered call appearance and puts the phone into speaker mode.

9. The phone lights the LED on the Page button to flash red for 250 ms and off for 250 ms.
10. The phone changes the display to:

```
Paging
Inside Sales
                00:15
```

The phone indicates which group you are paging and shows a timer that increments to indicate the duration of the page.

11. Speak your paging announcement. The call control system relays it to all members of the paging group.
12. When you have finished the page, go on hook, press the call appearance button that was being used, or press the Page button.

7.9 Error Conditions

If the phone encounters an error while logging in a user, logging in an ACD agent, parking a call, or paging, it will display one of the following error messages.

1. In this section, the first line of the display of the screen images shows:

```
User log in
```

However, if the phone receives an error while you are logging into an ACD group, the screens will instead show:

```
Group log in
```

If you are parking a call, the screens will instead show:

```
Call park
```

If you are attempting to make a page, the screens will instead show:

```
Page
```

2. If communications with the phone system fail, the phone displays:

```
User log in
Error:
Network failure
```

3. If the phone system does not respond, the phone displays:

```
User log in
Error: Server not
responding
```

4. If the phone system has asked for authentication (user address and password), and you entered these incorrectly, the phone displays:

```
User log in
Error: Invalid
address or password
```

5. If the phone system does not support the function, the phone displays:

```
User log in
Error:Not
supported by server
```

6. When you press any key, the phone displays the idle screen.

Chapter 8

Firewalls, NATs, and VPNs

8.1 Introduction

Many employees work from home, using high speed Internet access via DSL or a cable modem. Home configurations often provide some protection against hackers, viruses, and other hazards by incorporating a small router that performs firewall and Network Address Translation (NAT) services. These routers may have Virtual Private Networking (VPN) capabilities to provide secure access to corporate LAN. Figure 8-1 displays a typical setup for a remote employee.

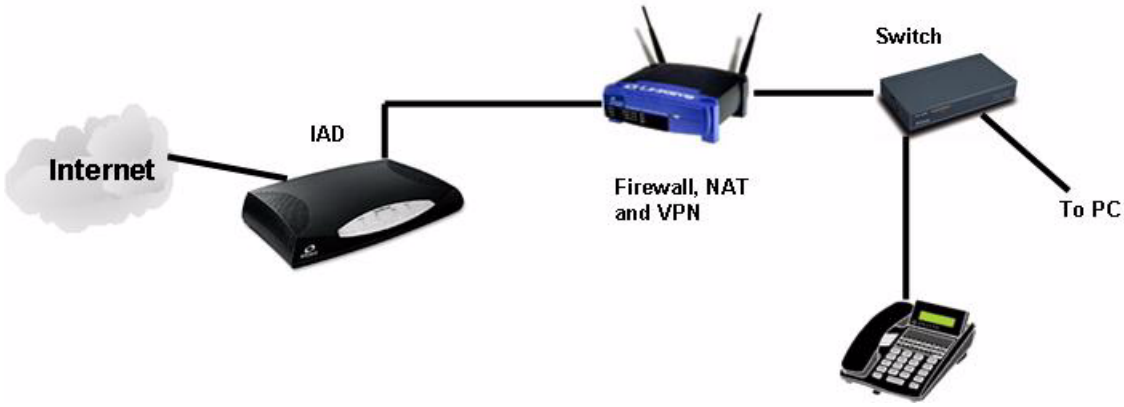

Figure 8-1 Typical home network for a telecommuter

One disadvantage of this approach is that the IT manager must support and configure this router. The ZIP4x5 offers a more efficient approach by providing Firewall, NAT, and VPN capabilities, in addition to normal phone features. This simplified configuration is shown in figure 8-2.

Figure 8-2 A Simplified Home Network using a ZIP4x5

Figure 8-3 depicts a network configuration that utilizes the ZIP4x5 operating as a remote router. A VPN tunnel is established or traversed when the ZIP4x5, or a device behind it, attempts to reach an IP address range at the headquarters. When the ZIP4x5, or devices behind it, attempt to contact other IP addresses, the ZIP4x5 routes the traffic through its firewall and NAT.

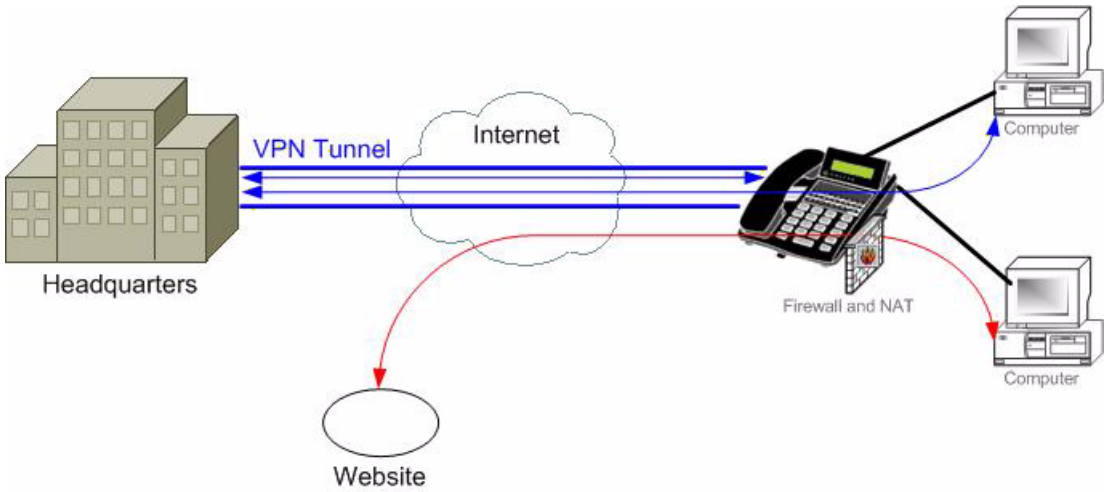

Figure 8-3 General network diagram

The ZIP4x5 provides two methods of setting up your remote network:

- **Configuration files** that are accessible through the corporate TFTP server. Configuration files are typically used by the network administrator to configure the ZIP4x5 before shipping the phone to the remote user. Appendix C, starting on page 197, describes the construction and use of configuration files.
- **Web Interface Configuration Utility** is accessible by entering the IP address of your ZIP4x5 on your internet browser. The remote user can modify individual configuration settings with this utility without returning the device to the administrator. Appendix D, starting on page 225, describes the Web Interface Configuration Utility.

This chapter describes the remote network functions available on the ZIP4x5 and provides a description of the configuration file statements and web interface configuration utility panels required to implement and configure these functions.

8.2 Enabling Remote Network Support

8.2.1 Network Mode Definitions

The ZIP4x5 defines two network configuration modes: normal network mode and remote network mode:

8.2.1.1 Normal Network Mode

When the ZIP4x5 is in *normal network mode*, it functions as a SIP device within a LAN. You can generate and accept calls with the phone, but it is not configured to act as remote network router. When booting the ZIP4x5 in normal network mode, the phone's network can be configured through the DHCP server or you can set a static IP address. Normal network mode supports a maximum of eight VLANs.

8.2.1.2 Remote Network Mode

When the ZIP4x5 is in remote mode, it performs router services between your LAN and a WAN, such as the internet. You can configure the phone to establish a VPN tunnel through the WAN with the corporate network and then provide corporate resources to the devices connected to the phone through its LAN. Remote network mode allows you to provide firewall services and act as a DHCP server for your LAN. Remote network mode supports two VLANs: one VLAN connects the ZIP4x5 to your LAN while the other VLAN connects the phone to the WAN.

8.2.2 Setting the Network Mode

You can set the network mode through the configuration file or the Web Interface

8.2.2.1 Configuration File

Mode and Remote Network VLAN instructions are firewall configuration commands. Firewall configuration commands must be listed in the file section that is headed by [FW]. The commands that configure the mode and the VLAN include:.

```
[FW]
mode=1
wan_vid=2
lan_vid=1
[VLAN_CONFIG]
mode=1
```

Figure 8-4 Configuration File Instructions that sets the Network mode.

mode: This instruction determines the network mode of the phone. Valid settings are 0 and 1:

- **To enable Normal Network Mode,** set mode = 0. All remote settings are disabled and the phone behaves as a normal SIP device.
- **To enable Remote Network Mode,** set mode = 1. All remote settings are enabled, including firewall, VPN, and router support between the WAN and your LAN.

  When mode=1, the following parameters must also be set:

  — ***wan_vid:*** This instruction establishes the VLAN ID for the WAN. Valid settings range from 1 to 4095; default value is 2. Within the VLAN configuration of the phone, wan_vid corresponds to VLAN A. The tag bits for the Phone, P1, P2, P2, and the LAN are TUUUE. (See section 10.6.4 on page 173 for information on tag bits).

— *lan_vid:* This instruction establishes the VLAN ID for the LAN. Valid settings range from 1 to 4095; default value is 1. You cannot set lan_vid to the same value as wan_vid. Within the VLAN configuration of the phone, lan_vid corresponds to VLAN B. The tag bits for the Phone, P1, P2, P2, and the LAN are TEEEU. (See section 10.6.4 on page 173 for information on tag bits).

— **Mode=1 (VLAN_CONFIG section):** When in remote network mode, the ZIP4x5 does not offer VLAN capabilities. This setting enables the LAN and WAN tag bit and ID settings. VLAN C through VLAN H are disableded when mode (firewall) = 1. Tag bits for each of these VLANs are set to TEEEE.

8.2.2.2 Web Interface

The Web Interface instruction that sets the network mode is *Enable Firewall, NAT, and VPN*, located on the Network Setup panel shown in figure 8-5. To access the Network Setup panel, select Protected Settings | Network Setup from the Home panel.

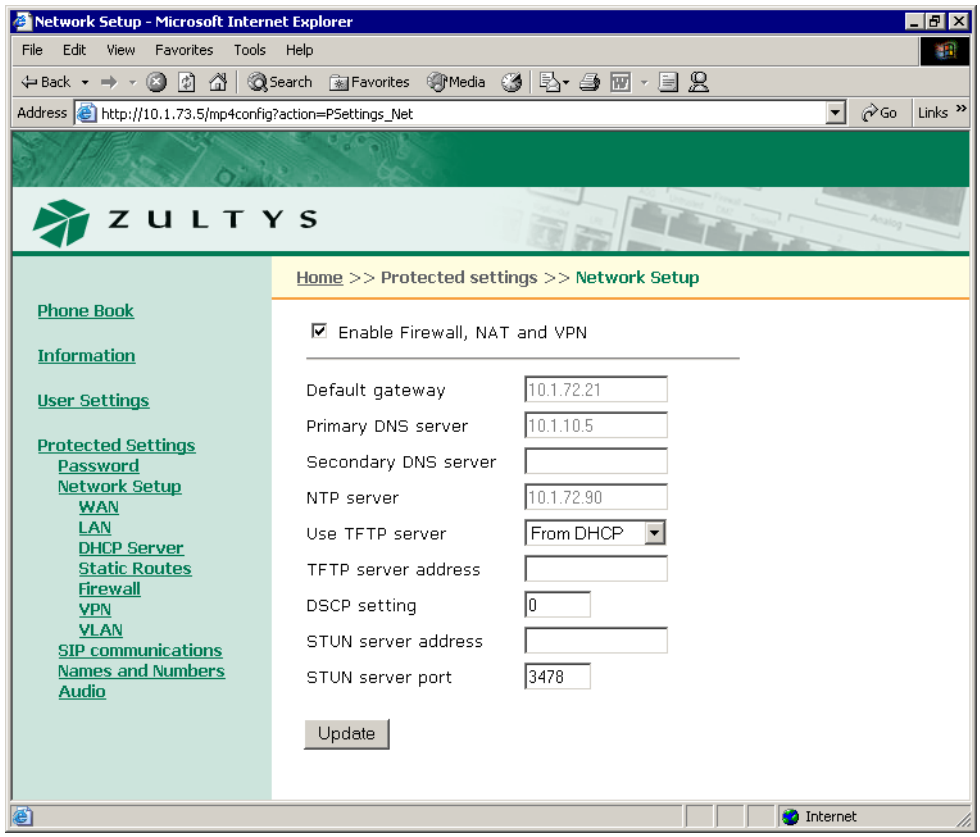

Figure 8-5 Web Interface panel – Network Setup

To enable **Normal Network mode**, verify that the *Enable Firewall, NAT, and VPN* is not checked.

To enable **Remote Network mode**, verify that *Enable Firewall, NAT, and VPN* is checked, then configure the LAN and WAN parameters located on the VLAN panel shown in figure 8-6. To access this panel, select Protected Settings | VLAN from the home panel. If the *Enable Firewall, NAT, and VPN* option on the Network Setup panel is not selected, the Web Interface displays the VLAN configuration panel for normal network mode.

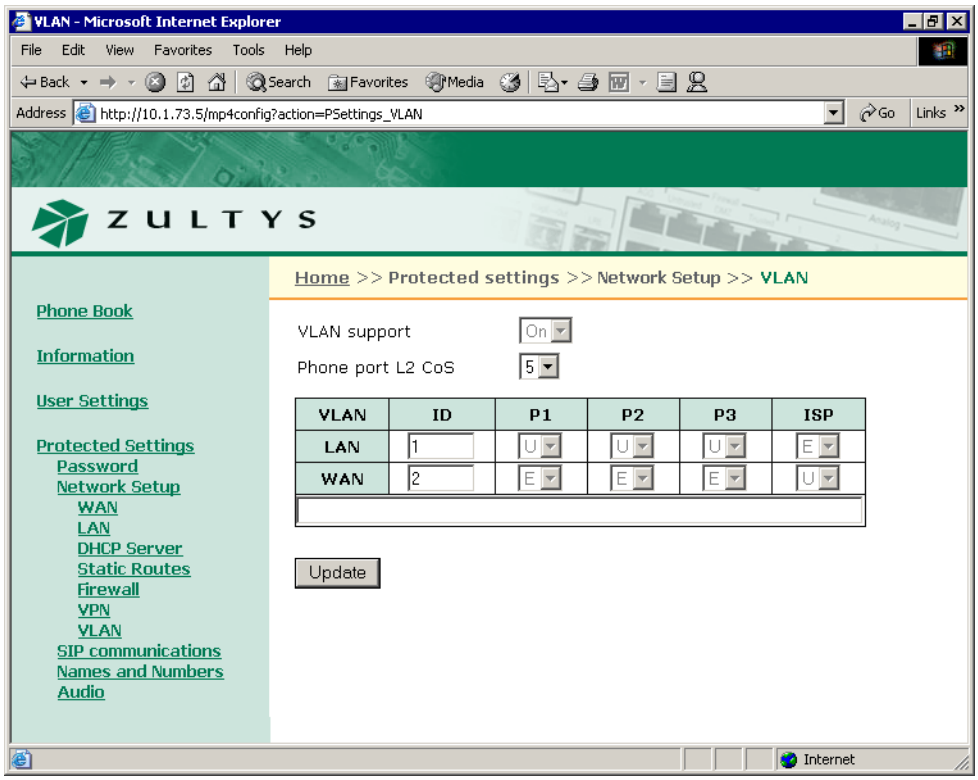

Figure 8-6 Web Interface Panel – VLAN, Remote Network mode

8.3 WAN Configuration

The ZIP4x5 provides three methods for configuring its interface settings to communicate with your WAN, normally through your ISP:

- act as a DHCP client to your ISP in order to receive and set your WAN configuration information
- use Point to Point Protocol over Ethernet (PPPoE) to access your account with your ISP
- enter Fixed IP Address settings as provided by your ISP

8.3.1 DHCP Client

When the ZIP4x5 acts as a DHCP client, you receive the WAN IP address, subnet mask, default gateway, and DNS server through the ISP's DHCP server.

8.3.1.1 Setting DHCP Mode through the Configuration File

Setting up the ZIP4x5 as a DHCP client requires two commands:

- In the NET_CONFIG file section, set use_dhcp to yes
- In the FW file section, turn off PPPoE by setting pppoe_mode to 0, then set wan_ip and wan_mask to dummy values. The ZIP4x5 replaces these values when it receives them from the DHCP server.

Figure 8-7 displays configuration file code that enables DHCP mode.

```
[NET_CONFIG]
use_dhcp=yes
[FW]
pppoe_mode=0
wan_ip=1.1.1.1
wan_mask=255.255.255.255
```

Figure 8-7 Configuration File Instructions to configure the ZIP4x5 as a DHCP client.

8.3.1.2 Setting DHCP Mode through the Web Interface

The Web Interface instruction that sets the WAN connection for DHCP mode is located on the WAN panel shown in figure 8-8. To access the WAN panel, select Protected Settings | Network Setup | WAN from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

To set the ZIP4x5 as a DHCP client, set *Connection type* to DHCP, enter dummy values for the WAN IP address and subnet mask, then press the ***Update*** button.

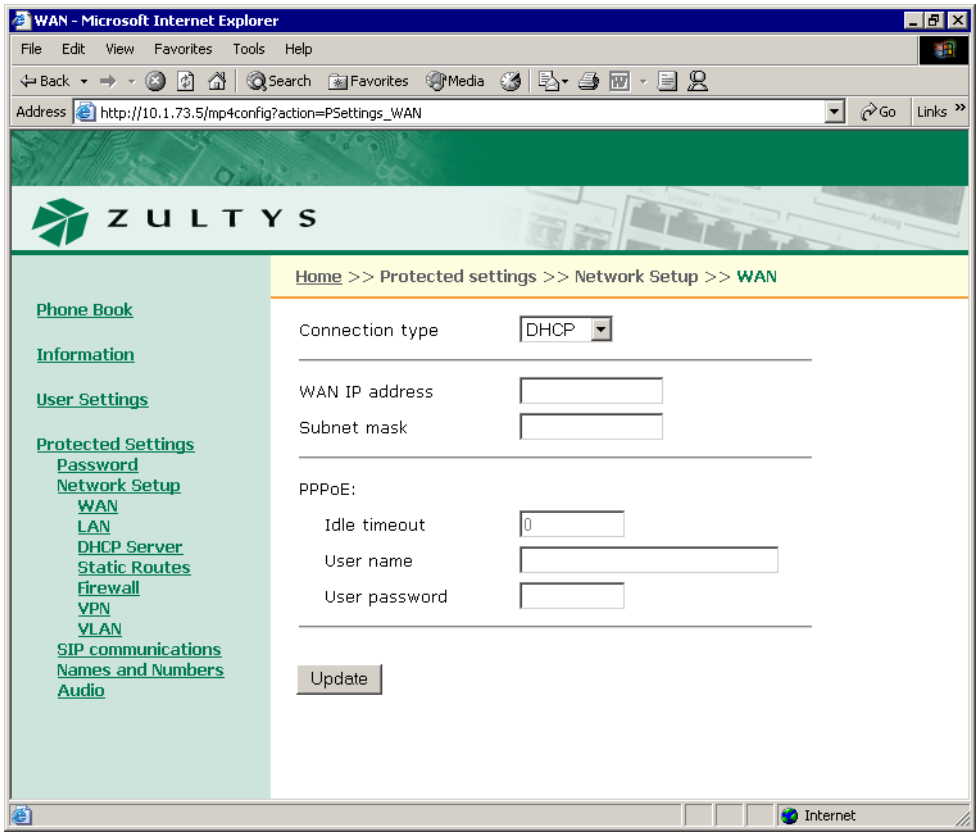

Figure 8-8 Web Interface WAN panel

8.3.2 PPPoE Mode

PPPoE is used by security conscious DSL service providers that require a username and password to establish a connection. A basic network diagram is shown in figure 8-9. The ZIP 4x5 replaces the *Router with PPPoE* and supplies a username and password to the PPPoE server at the ISP. The ZIP 4x5 discovers the PPPoE server through a broadcast mechanism and learns its IP address and other network settings from the ISP.

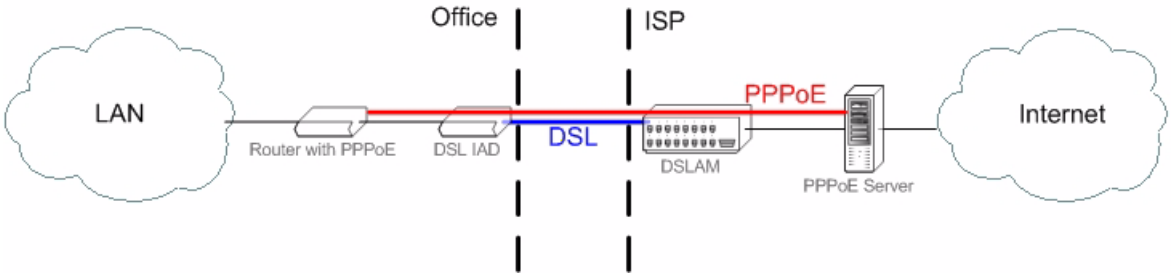

Figure 8-9 Using the ZIP 4x5 with PPPoE

8.3.2.1 Setting Up PPPoE through a Configuration File

Setting PPPoE Mode with the configuration file requires the following commands:

- In the NET_CONFIG file section, set ***use_dhcp*** to no
- In the FW file section, turn on PPPoE by setting ***pppoe_mode*** to 1, specify a user name (pppoe_user) and password (pppoe_pwd), then set wan_ip and wan_mask to dummy values. The ZIP 4x5 replaces these values when it receives them from the PPPoE server.

Figure 8-10 displays an example of code that enables PPPoE mode.

```
[NET_CONFIG]
use_dhcp=no
[FW]
pppoe=1
pppoe_user=dana_thomas_remote
pppoe_pwd=rdds43wa
wan_ip=1.1.1.1
wan_mask=255.255.255.255
```

Figure 8-10 Configuration File Instructions that enables PPPoE mode.

8.3.2.2 Setting PPPoE Mode through Web Interface

The Web Interface instruction that sets the WAN connection for PPPoE mode is located on the WAN panel shown in figure 8-8. To access the WAN panel, select Protected Settings | Network Setup | WAN from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

Set Connection type to PPPoE and specify the User Name and User Password in the PPPoE section of the panel. Enter dummy values for the WAN IP address and subnet mask, then press the Update button.

8.3.3 Fixed Address Mode

When you specify fixed IP address mode, you must configure the static WAN IP address, subnet mask, default gateway address, and primary DNS server address. You can also specify secondary and tertiary DNS server addresses along with NTP and TFTP server addresses. Your ISP provides these addresses to you.

8.3.3.1 Setting Up Fixed IP Addressing through a Configuration File

Setting Fixed IP Address Mode with the configuration file requires the following commands:

1. In the NET_CONFIG file section:
   - set use_dhcp to 0
   - set default_gateway to the IP address provided by your ISP
   - set primary_dns to the IP address provided by your ISP
   - set secondary_dns to the IP address provided by your ISP (optional)
2. In the FW file section:
   - set pppoe_mode to 0
   - set wan_IP to the fixed public IP address provided by the ISP
   - set wan_mask to the subnet mask for the WAN interface; this is also provided by the ISP.

Figure 8-11 displays an example of code that sets Fixed IP Address mode.

```
[NET_CONFIG]
use_dhcp=no
default_gateway=147.139.10.3
primary_dns=147.139.15.0
[FW]
pppoe_mode=0
wan_ip=147.139.20.5
wan_mask=255.255.255.0
```

Figure 8-11 Configuration File Instructions that sets the Network mode.

8.3.3.2 Setting Fixed IP Addressing through the Web Interface

The Web Interface instruction that sets the WAN connection for Fixed Address mode is located on the WAN panel shown in figure 8-9. To access the WAN panel, select Protected Settings | Network Setup | WAN from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

Set Connection type to ***Fixed IP*** and specify the User Name and User Password. Then press the Update button. Then return to the Network Setup panel (figure 8-5) and enter the IP address for the default gateway, and the DNS servers.

8.4 LAN Configuration

Configuring the LAN connection to your ZIP4x5 requires the assignment of a static IP address to the LAN network. You can also configure the ZIP4x5 as a DHCP server for the devices located on your LAN.

8.4.1 Setting the IP Address

Setting the IP Address requires the valid IP Address and subnet mask that accesses your LAN.

8.4.1.1 Setting the IP Address through the Configuration File

Setting the IP Address for the LAN requires the following commands in the NET_CONFIG file section:

- set IP_addr to the IP address for the LAN
- set subnet_mask to the subnet mask of the LAN

Figure 8-12 displays an example of code that sets Fixed IP Address mode.

```
[NET_CONFIG]
ip_addr=172.16.16.1
subnet_mask=255.255.128.0
```

Figure 8-12 Configuration File Instructions that sets the Network mode.

8.4.1.2 Setting the IP Address through the Web Interface

The Web Interface instructions that sets the LAN IP address and subnet mask is located on the LAN panel shown in figure 8-13. To access the LAN panel, select Protected Settings | Network Setup | LAN from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

8.4.2 Configuring the ZIP4x5 as a DHCP Server

Setting up the ZIP4x5 as a DHCP server provides a resource for devices on your LAN to obtain dynamic IP addresses and network configuration parameters, as shown in figure 8-14. The following data is provided by the ZIP4x5 DHCP server:

Dynamic IP Addresses: The dynamic addresses that the ZIP4x5 DHCP server provides should belong to the private address spaces defined in RFC 1918:

— 10.0.0.0 - 10.255.255.255 (10/8 prefix)

— 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)

— 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

Lease Duration. This specifies the period that client PCs can maintain their dynamic IP address without renewing their lease.

DNS Server: Specifies the address of the DNS server accessible to the LAN. The ZIP4x5 DHCP Server can provide up to three server addresses.

Domain Name: Specifies the domain name of the LAN.

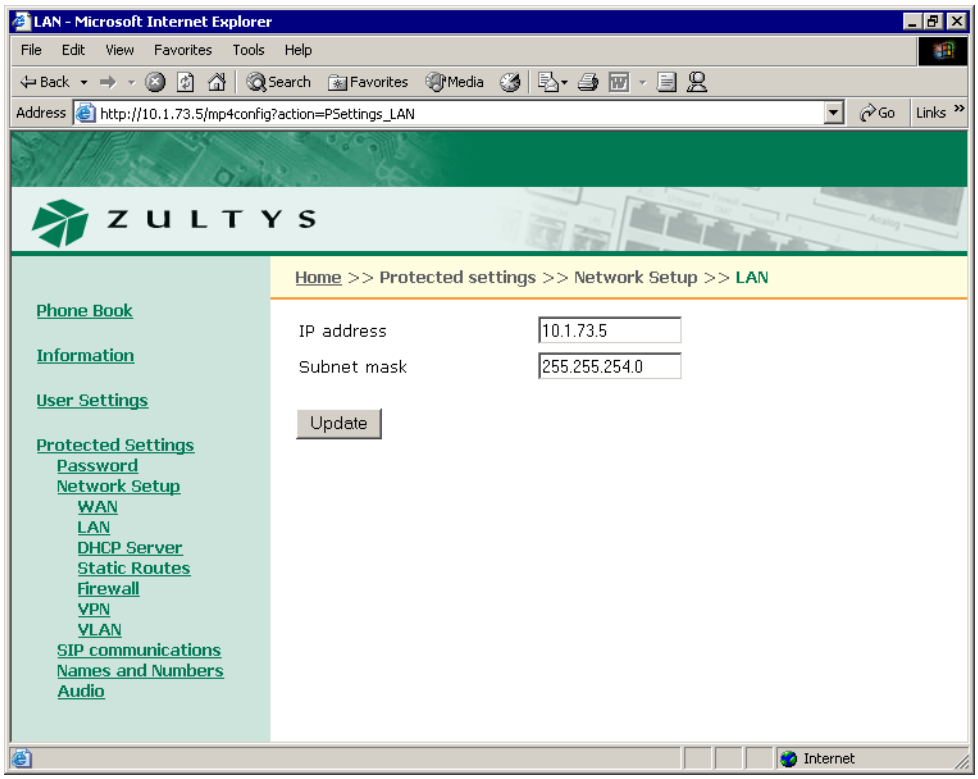

Figure 8-13 Web Interface LAN panel

Figure 8-14 ZIP4x5 as a DHCP Server

NTP Server: Specifies the IP address of the NTP server. The ZIP4x5 DHCP Server can provide up to three server addresses.

TFTP Server: Specifies the IP address of the TFTP server that is accessible to the devices on your LAN.

8.4.2.1 Configuring the ZIP4x5 as a DHCP Server from the Configuration File

Setting up the ZIP4x5 as a DHCP server requires that the phone is not configured as a DHCP client in the WAN Configuration, as explained in section 8.3.1. DHCP configuration requires the following commands in the DHCP_SRV file section:

- **mode:** Set mode to 1 to enable DHCP server functions. Set mode to 0 to disable DHCP server functions.
- **start_ip:** specifies the starting address of the DHCP scope. This begins the list of IP addresses that the DHCP assigns to requesting devices.
- **end_ip:** specifies the ending address of the DHCP scope.
- **o_mask:** specifies the subnet mask for the DHCP scope.
- **lease_secs:** specifies the IP Address lease duration, in seconds
- **o_router:** specifies the IP address of the default gateway
- **o_dns1:** specifies the IP address of the primary DNS server
- **o_dns2:** specifies the IP address of the secondary DNS server
- **o_dns3:** specifies the IP address of the tertiary DNS server
- **o_domain:** specifies the default domain name
- **o_ntp1:** specifies the IP address of the primary NTP server
- **o_ntp2:** specifies the IP address of the secondary NTP server
- **o_ntp3:** specifies the IP address of the tertiary NTP server
- **o_tftp:** specifies the IP address of the TFTP server

Figure 8-15 displays an example of code that configures the ZIP4x5 as a DHCP server.

```
[DHCP_SRV]
mode=1
start_ip=10.0.0.0
end_ip=10.0.0.255
o_mask=255.255.255.0
lease_secs=3600
o_router=10.1.32.5
o_dns1=10.1.15.4
o_domain=zultys.com
o_ntp1=10.1.18.2
o_tftp=10.1.11.224
```

Figure 8-15 Configuration File Instructions that configures the ZIP4x5 as a DHCP server.

8.4.2.2 Configuring the ZIP4x5 as a DHCP Server from the Web Interface

To access the DHCP Web Interface panel, shown in figure 8-16, select Protected Settings | Network Setup | DHCP Server from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel. Parameter descriptions are listed in the order that they appear on the web interface panel.

DHCP server mode. Set this parameter to Enabled to configure the ZIP4x5 as a DHCP server. Set this parameter to Disabled to disable server functions.

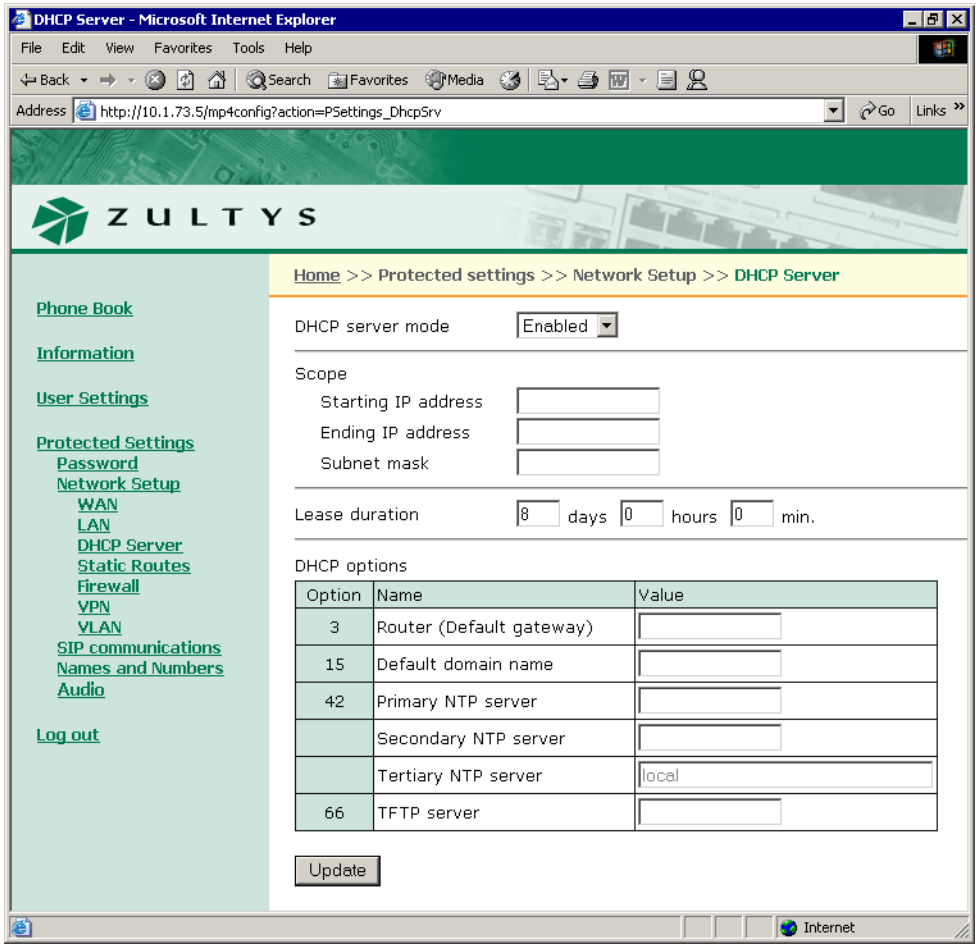

Figure 8-16 Web Interface DHCP Server panel

Starting IP address. This parameter specifies the starting address of the DHCP scope. This begins the list of IP addresses that the DHCP assigns to requesting devices.

Ending IP address. This parameter specifies the ending address of the DHCP scope.

Subnet mask. This parameter specifies the subnet mask for the DHCP scope.

Lease duration. This parameter specifies the IP Address lease duration.

DHCP options. These data entry boxes configure the IP addresses that the ZIP4x5 returns to its client devices.

8.5 Firewall

The firewall defines the attributes of the data packets that the ZIP4x5 allows passage through to the LAN and WAN.

8.5.1 Component Description

The ZIP4x5 firewall comprises the following two components: The LAN filters and the WAN filters.

8.5.1.1 LAN Filters

The LAN filters determine the packets that the firewall prohibits from being sent from the LAN to the WAN. By default, the ZIP4x5 grants full access to the WAN (internet) for packets originating from LAN devices.

Each LAN filter statement comprises a set of filters. Each filter is made up of the following components:

- **name:** This parameter is the firewall label.
- **protocol:** This parameter specifies the protocol of the packets that are prohibited from passing through the firewall.
- **address:** This parameter specifies the source IP address of the packets that are prohibited from passing through the firewall.
- **port:** This parameter specifies the port number of the packets that are prohibited from (LAN firewall) passing through the firewall.

Firewall filters are prioritized such that packets are evaluated against them in sequential order. You can also enable or disable individual filters.

8.5.1.2 WAN Filters

WAN filters determine the packets that the firewall allows to pass from the WAN to the LAN. The firewall also allows packets into the LAN that are direct responses to data originally sent from the LAN. By default, the ZIP4x5 denies access to the LAN for all packets originating from the WAN (internet).

Each WAN filter statement comprises a set of filters. Each filter is made up of the following components:

- **name:** This parameter is the firewall label.
- **protocol:** This parameter specifies the protocol of the packets that are allowed to pass through the firewall.
- **address:** This parameter specifies the IP address of the LAN device that will receive the packets that match the protocol and port listed by this filter.
- **port:** This parameter specifies the port number of the packets that are allowed to pass through the firewall.

Firewall filters are prioritized such that packets are evaluated against them in sequential order. You can also enable or disable individual filters.

Figure 8-17 displays a sample network with the ZIP4x5 functioning as a firewall.

8.5.2 Setting Up Firewalls through a Configuration File

The FW section of the configuration file provides two firewall statements: lan_filters and wan_filters. The syntax of each statement follows:

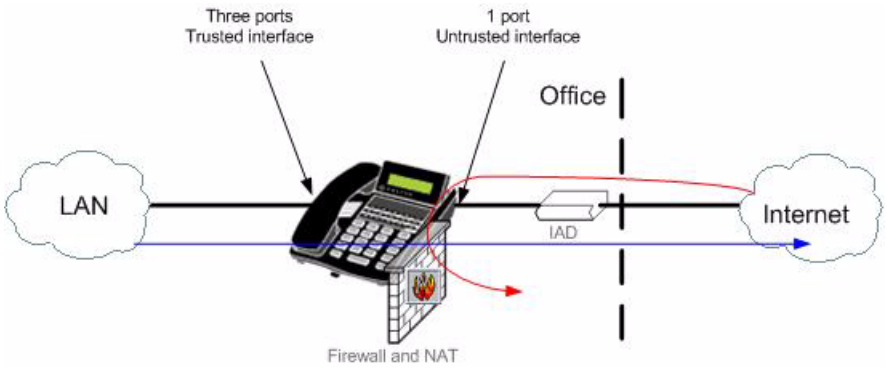

Figure 8-17 ZIP4x5 Firewall

lan_filter = l_filter_1 | l_filter_2 | l_filter_3 |... |l_filter_n such that:

l_filter_x specifies an individual filter such that:

l_filter_x= l_name_x#l_prot_x#l_addr_x#l_port_x#l_active_x

l_name_x is the label

l_prot_x is the protocol of the data packet targeted by the filter

valid entries are tcp, udp, icmp, all

l_addr_x is the origin IP address of data packets targeted by the filter

address range is specified by address/prefix notation

example syntax is 10.10.10.0/24

l_port_x is the origin port of targeted data packets

valid for only udp and tcp protocols

multiple ports specified by colon – 10:12 indicates 10-12

l_active_x indicates the activity status of the filter

0 - filter is not used; 1 - filter is used

wan_filter = w_filter_1 | w_filter_2 | w_filter_3 |... |w_filter_n such that:

w_filter_x specifies an individual filter such that:

w_filter_x= w_name_x#w_prot_x#w_addr_x#w_port_x#w_active_x

w_name_x is the label

w_prot_x is the protocol of the data packet targeted by the filter

valid entries are tcp, udp, icmp, all

w_addr_x is the origin IP address of data packets targeted by the filter

parameter can only specify a single address

example syntax is 10.10.10.0

w_port_x is the origin port of targeted data packets

valid for only udp and tcp protocols

parameter can only specify a single port

w_active_x indicates the activity status of the filter

0 - filter is not used; 1 - filter is used

Figure 8-18 displays the section of a configuration file that creates a firewall.

```
[FW]
lan_filters=NoWebAccessForBill#tcp#172.16.16.20#80:82#1
wan_filters=AcceptFTP#tcp#172.16.16.54#21#1|AcceptSomeTelnet#172.16.16.45#23#
1
```

Figure 8-18 Configuration File Instructions that configures a Firewall

8.5.3 Setting the Firewalls through the Web Interface

The Web Interface instructions that configure the firewall is located on the Firewall panel shown in figure 8-19. To access the Firewall panel, select Protected Settings | Network Setup | Firewall from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

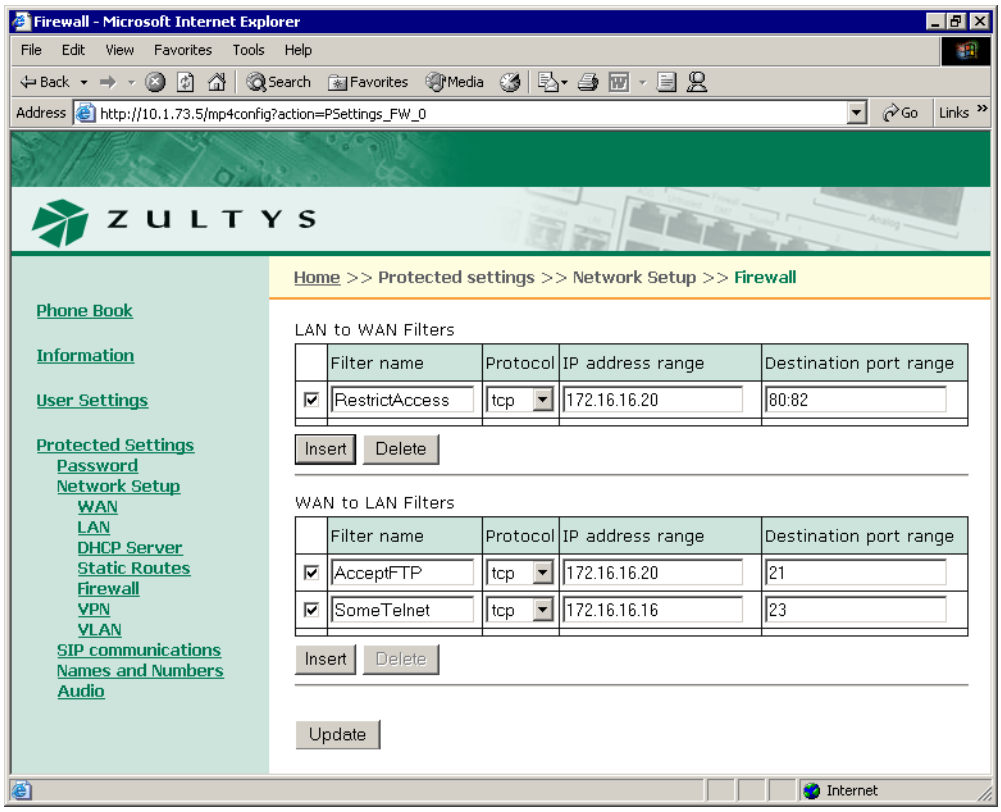

Figure 8-19 Web Interface Firewall panel

8.6 Static Routes

Static routes allow you to specify a gateway for communicating with a device at a given IP address.

8.6.1 Setting Up Static Routes through a Configuration File

The FW section of the configuration file provides a static route statement that allows you to establish multiple static routes:

static_route = $route_1$ | $route_2$ | $route_3$ |... |$route_n$ where:

$route_x$ specifies an individual static route with the following syntax:

$route_x$ = $address_x$#$subnet_x$#$gateway_x$

$address_x$ is the IP address of the remote network

$subnet_x$ is subnet mask of the remote network

$gateway_x$ is the IP address that must be used to reach the target.

```
[FW]
static_routes=210.1.0.0#255.255.252.0#172.3.1.8|10.5.0.0#255.255.240.0#172.16
.16.20
```

Figure 8-20 Configuration File Instructions that configures Static Routes

8.6.2 Setting the Firewalls through the Web Interface

The Web Interface instruction that sets the static routes is located on the Static Routes panel shown in figure 8-21. To access this panel, select Protected Settings | Network Setup | Static Routes from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

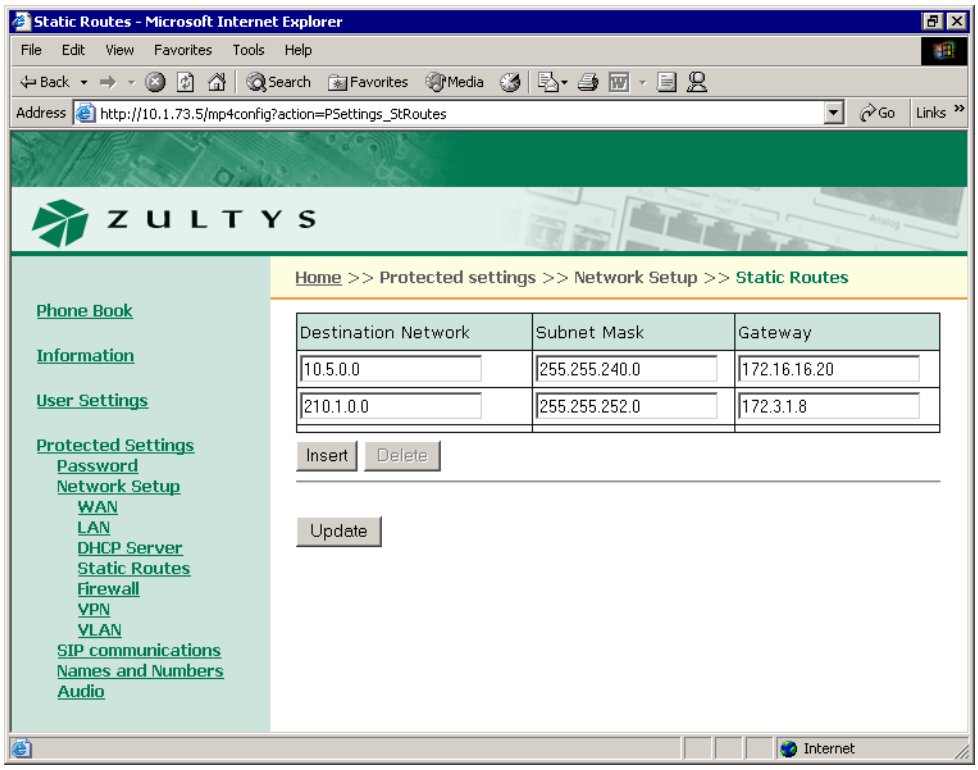

Figure 8-21 Web Interface Static Route panel

Each row specifies one static route:

- **Destination Network:** This parameter is the IP address of the device(s) at the route's end.
- **Subnet Mask:** This parameter is the subnet mask of the device(s) at the route's end.
- **Gateway:** This parameter specifies the IP address of the device that must be accessed to reach the target device.

8.7 Virtual Private Networks (VPN)

8.7.1 Description

A virtual private network (VPN) uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN maintains privacy through security procedures and tunneling protocols that encrypt data at the sending end and decrypt it at the receiving end. An additional level of security can be added by also encrypting the originating and receiving network addresses.

VPN connections link local area networks. The traffic that flows between these networks passes through shared resources such as routers, switches, and other network equipment that make up the public wide area network (WAN). VPN communications are secured through an IP Security (IPsec) tunnel.

Figure 8-22 shows an example of a VPN tunnel between a small office and its corporate headquarters.

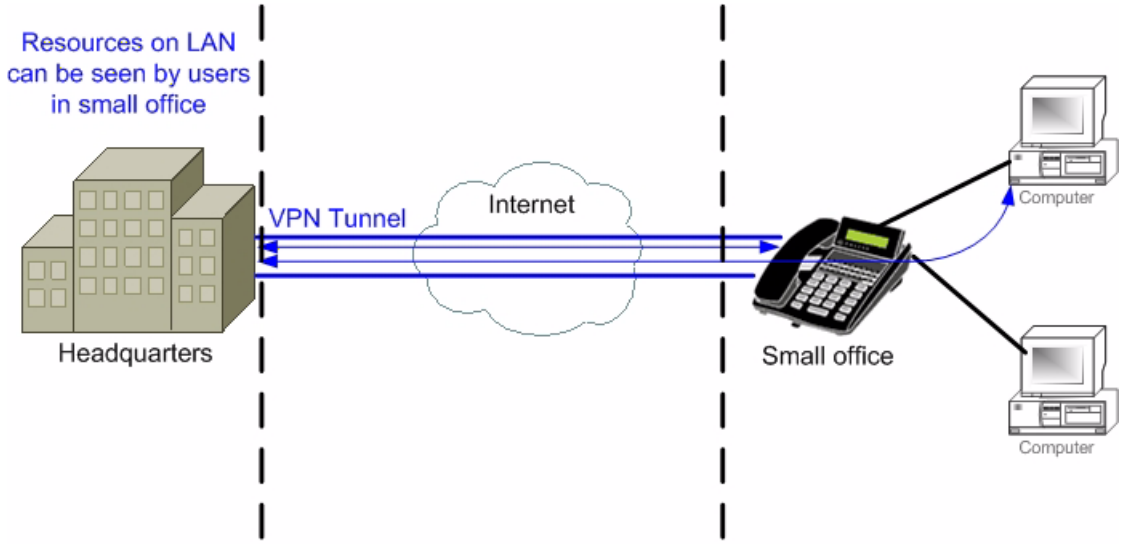

Figure 8-22 VPN tunnel between a small office and a corporate headquarters

8.7.1.1 IP Security (IPsec)

Internet Protocol Security (IPsec) is a framework for a set of protocols that secures network communications at the packet processing layer. IPsec is useful for implementing VPNs and for remote user access through dial-up connections to private networks. IPsec handles security arrangements without requiring changes to individual user computers.

IPsec protocols define the following VPN attributes:

Packet Encapsulation Mode: The packet encapsulation mode determines the structure of the IP packet that is sent through the VPN. The ZIP4x5 uses Tunnel Mode, where the original IP packet is encapsulated within another IP payload, with a new header appended to it.

Authentication and Encryption: These protocols determine the method of authenticating and encrypting packets that are sent through the VPN.

Key Management Method: Key management refers to the means that keys are distributed to VPN participants. The ZIP4x5 supports AutoKey IKE and Manual Keys:

- AutoKey IKE uses the Internet Key Exchange (IKE) protocol to automatically generate and negotiate keys.
- In Manual Key mode, administrators on both ends of the tunnel configure all security parameters. While this is a viable technique for small static networks, key management over configurations across great distances pose security issues. Manual key mode is sometimes necessary with ISPs having firewalls that do not allow passage of connections in IKE mode.

8.7.2 Establishing a VPN using AutoKey IKE

AutoKey IKE utilizes *Tunnel Negotiation* to synchronize the methods and parameters that the VPN participants will use to secure communications through an IPsec tunnel. Two negotiation phases are required to establish an AutoKey IKE IPSec tunnel and agree upon the Security Association (SA) parameters. An SA is a unidirectional agreement between the participants regarding the methods and parameters that will secure tunnel communications.

Phase 1. The participants establish a secure channel for negotiating the Security Associations.

Phase 2. The participants negotiate the Security Associations for encrypting and authenticating the ensuing data exchanges.

8.7.2.1 Phase 1

Phase 1 of an AutoKey IKE tunnel negotiation consists of the exchange of proposals for how to authenticate and secure the channel. The participants exchange proposals for the following security services:

Authentication algorithms. The ZIP4x5 supports sha1 and md5.

Encryption algorithms. The ZIP4x5 supports 3des, des, blowfish, cast128.

A Diffie-Hellman Group. The Diffie-Hellman (DH) exchange is used to generate new keys. **The ZIP4x5 uses DH Group 2 for all Phase 1 negotiations.**

Preshared Key. A Preshared key is a key used for encryption and decryption that must be possessed by both participants before initiating communication. The maximum length of the preshared key is 128 characters.

Key Lifetime. The ZIP4x5 supports a phase 1 key lifetime of 28,800 seconds. This parameter cannot be altered.

A successful Phase 1 negotiation concludes when both ends of the tunnel agree to accept at least one set of the Phase 1 security parameters. The ZIP4x5 offers three phase 1 negotiation modes:

Main Mode. This mode features three two-way exchanges that protect the identities of the participants. Main mode is difficult to efficiently use when a VPN peer uses its identity as part of the authentication process.

Aggressive Mode. This mode features two exchanges (three messages) in which the identities of the participants are exchanged in the clear.

Base Mode. This mode features four messages where the initiator sends authentication data along with the key exchange payload; this allows the responder to verify the senders identity before responding with a key exchange payload.

8.7.2.2 Phase 2

After the participants establish a secure and authenticated channel, they proceed through Phase 2 to negotiate the Security Associations for securing data to be passed through the IPSec tunnel.

In a process that is similar to Phase 1, the participants exchange proposals to determine the security parameters. Phase 2 proposals include an authentication algorithm, an encryption algorithm, and can specify a Diffie-Hellman group to implement Perfect Forward Secrecy.

Authentication algorithms. The ZIP4x5 supports hmac_md5 and hmac_sha1.

Encryption algorithms. The ZIP4x5 supports rijndael and 3des.

Perfect Forward Secrecy. Perfect Forward Secrecy (PFS) is a method for deriving Phase 2 keys independently from the preceding keys. When PFS is not implemented, the Phase 1 proposal creates the key from which all Phase 2 keys are derived. The originating key can generate Phase 2 keys with a minimum of CPU processing. If an unauthorized party gains access to the originating key, all successive encryption keys are compromised. PFS addresses this security risk by forcing a new Diffie-Hellman key exchange for each Phase 2 tunnel. Although using PFS is more secure, enabling PFS may require more time to perform the rekeying procedure. **When PFS is enabled, the ZIP4x5 uses DH Group 2 for all Phase 2 negotiations.**

8.7.3 Establishing a VPN using Manual Keys

Manual keys require the agreement of VPN security parameters and keys by the network administrators prior to the establishment of the VPN. The ZIP4x5 supports the following Manual Key parameters:

- ***authentication algorithms*** – The ZIP4x5 supports hmac_md5 and hmac_sha1.
- ***encryption algorithms*** – The ZIP4x5 supports rijndael and 3des
- ***encryption key*** – This parameter specifies the encryption key. Each VPN participant must enter the same key. It is recommended that the length of the key be at least 16 bytes.
- ***authorization key*** – This parameter specifies the authorization key. Each VPN participant must enter the same key. It is recommended that the length of the key be at least 16 bytes.

- ***security parameter index*** – The Security Parameter Index is a data field that identifies the Security Association. It must be exactly 8 hex digits. Each VPN participant defines an inbound and outbound SPI; the inbound SPI of the local end must match the outbound SPI at the remote end.

8.7.4 Setting Up VPNs through a Configuration File

Establishing a VPN with a configuration file requires the following commands in the Firewall file section.

8.7.4.1 Commands for AutoKey IKE Mode and Manual Key mode

ipsec_mode. This command enables VPN support and specifies the key management method that your VPNs use:

— ipsec_mode=0 VPN mode is disabled

— ipsec_mode=1 VPN mode is enabled and uses autokey IKE

— ipsec_mode=2 VPN mode is enabled and uses manual keys

remote_lan_net. This command specifies the IP address of the remote LAN. Address format is net/prefix.

remote_wan_ip. This command specifies the IP address of the remote VPN gateway.

encrypt_algo. This parameter specifies the encryption algorithm for data transfer (manual) or phase 2 negotiations (AutoKey). Valid settings include rijndael and 3des.

auth_algo. This parameter specifies the authentication algorithm for data transfer (manual) or phase 2 negotiations (AutoKey). Valid settings include hmac_md5 and hmac_sha1.

8.7.4.2 Commands for AutoKey IKE Mode

p1_encrypt_algo. This command specifies the phase 1 negotiation algorithm. Valid settings include 3des, des, blowfish, and cast128.

p1_hash_algo. This command specifies the phase 1 negotiation hash algorithm. Valid settings include sha1 and mds.

p1_mode. This specifies the phase 1 mode. Valid settings include main, aggressive, and base.

psk. This command specifies the preshared key.

pf_secrecy. This command specifies the method for deriving phase 2 keys:

— pf_secrecy=0 off

— pf_secrecy=1 perfect forward secrecy is used to derive phase 2 keys.

key_lifetime. This command specifies the period that a key is valid. After the lifetime expires, the key must be renegotiated. Valid settings include x hour, x min, x sec.

my_ident. This parameter specifies the user IP address and is valid only if p1=aggressive.

8.7.4.3 Commands for Manual Keys Mode

encrypt_key. The parameter specifies the encryption key used in manual key mode. Valid setting must be double-quoted character string or a series of hexadecimal digits preceded by '0x'. This parameter is valid only if ipsec_ mode=2.

authkey. This parameter specifies the authorization key when in manual key mode. Valid setting must be double-quoted character string or a series of hexadecimal digits preceded by '0x'. This parameter is valid only if ipsec_ mode=2.

inbound_spi. This specifies the Security Parameter Index which is a field used to identify the Security Association. It must be exactly 8 hex digits. The inbound SPI at the local end must match the outgoing SPI at the remote end. Valid only if ipsec_mode=2.

outbound_spi. This specifies the Security Parameter Index which is a field used to identify the Security Association. It must be exactly 8 hex digits. The inbound SPI at the remote end must match the outbound SPI at the local end. Valid only if ipsec_mode=2.

Figure 8-23 displays an example of code that establishes a VPN tunnel.

```
[FW]
ipsec_mode=1
remote_lan_net=172.16.0.0/20
remote_wan_ip=180.1.0.50
p1_encrypt_algo=rijndael
p1_hash_algo=sha1
p1_mode=aggressive
psk=JUNK
pf_secrecy=0
key_lifetime=1 hour
encrypt_algo=3des
auth_algo=hmac_md5
my_indent="user_name@zultys.com"
```

Figure 8-23 Configuration File Instructions that establishes and AutoKey IKE VPN.

8.7.5 Establishing a VPN through the Web Interface

The Web Interface instruction that sets the Virtual Private Network is located on the VPN panel shown in figure 8-24. To access the VPN panel, select Protected Settings | Network Setup | VPN from the Home panel. The *Enable Firewall, NAT, and VPN* option on the Network Setup panel must be selected to view this panel.

Parameter descriptions are listed in order of appearance on the panel.

8.7.5.1 General Parameter Descriptions

Enabled / Disabled: Select **Enabled** to establish a VPN from your ZIP4x5.

Remote IP network. This command specifies the IP address of the remote LAN. Address format is net/prefix.

Remote IP network gateway. This command specifies the IP address of the remote VPN gateway.

Encryption. This parameter specifies the encryption algorithm for data transfer (manual) or phase 2 negotiations (AutoKey). Valid settings include aes and 3des.

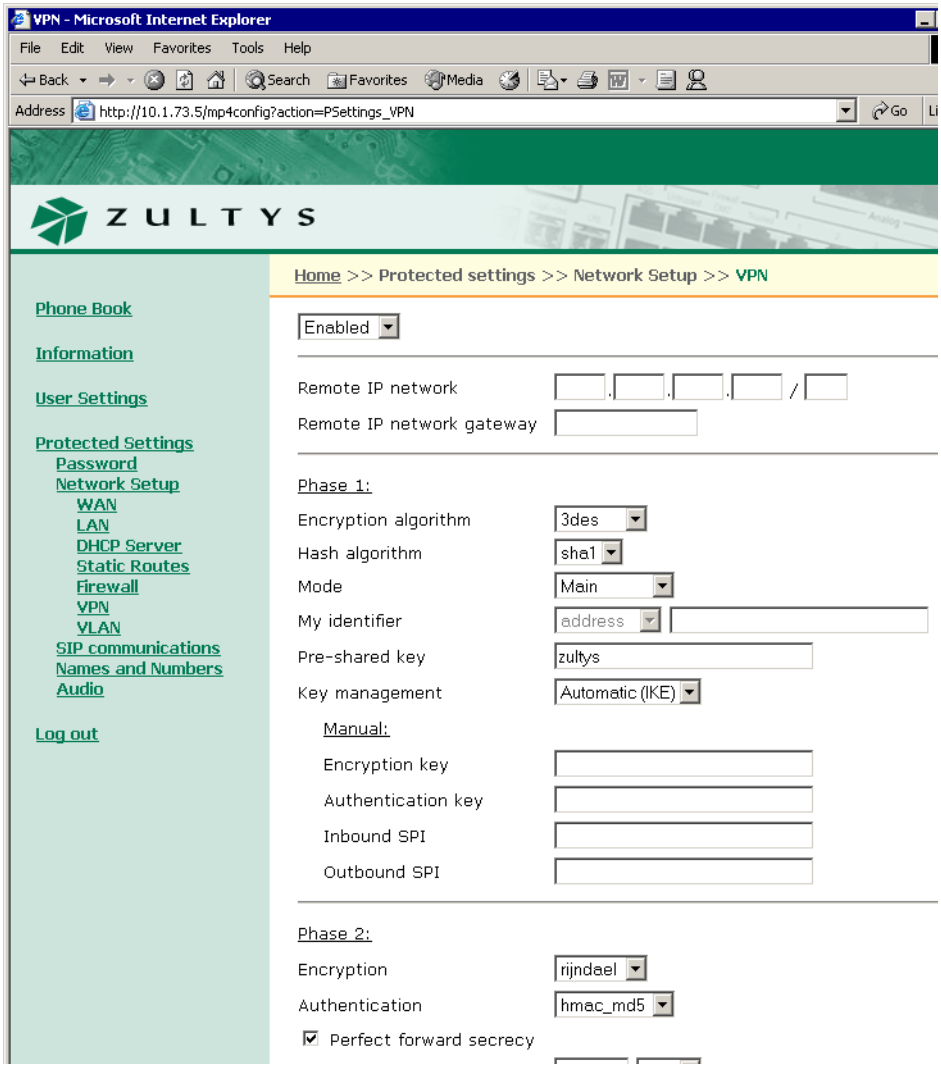

Figure 8-24 Web Interface VPN panel

Authentication. This parameter specifies the authentication algorithm for data transfer (manual) or phase 2 negotiations (AutoKey). Valid settings include md5 and sha1.

Key Management. This parameter specifies the key management method. Valid settings are Automatic IKE and Manual.

8.7.5.2 Automatic Parameter Descriptions

Perfect Forward Secrecy. This command specifies the method for deriving phase 2 keys:

— pf_secrecy=0 off

— pf_secrecy=1 perfect forward secrecy is used to derive phase 2 keys.

When pfs is enabled, the ZIP4x5 uses DH Group 2 for all phase 2 negotiations.

Pre-shared key. This parameter specifies the preshared key.

Key Lifetime. This command specifies the period that a key remains valid. After the lifetime expires, the key must be renegotiated. Valid settings includes 12 hours, 3600 seconds, and 30 minutes.

8.7.5.3 Manual Parameter Descriptions

Encryption key. This parameter specifies the encryption key used in manual key mode. Valid setting is either a double-quoted character string or a series of hexadecimal digits preceded by '0x'.

Authentication key. This parameter specifies the authorization key when in manual key mode. Valid setting is either a double-quoted character string or a series of hexadecimal digits preceded by '0x'.

Inbound SPI. This specifies the Security Parameter Index, which is a field that identifies the Security Association. It must be exactly 8 hex digits. The inbound SPI at the local end must match the outgoing SPI at the remote end.

Outbound SPI. This specifies the Security Parameter Index, which is a field that identifies the Security Association. It must be exactly 8 hex digits. The inbound SPI at the remote end must match the outbound SPI at the local end.

8.7.5.4 Phase 1 Settings Descriptions

Encryption Algorithm. This command specifies the phase 1 negotiation algorithm. Valid settings include 3des, des, blowfish, and cast128.

Hash Algorithm. This command specifies the phase 1 negotiation hash algorithm. Valid settings include sha1 and mds.

Mode. This command specifies the phase 1 mode. Valid settings include main, aggressive, and base.

User FQDN. This parameter specifies the user IP address and is valid only if p1=aggressive. Valid setting is a fully qualified domain name.

Chapter 9

Using the Phone

9.1 Going Off Hook and On Hook

You can use the handset, headset, or speaker for any call and easily switch between them – even during the same call. Subsequent sections detail the processes for making and terminating a call. This section briefly describes how to select between the three audio paths.

9.1.1 Using the Handset, Headset, and Speaker

To use the handset, pick it up. When you have finished using it, replace it in the cradle.

To use the headset, press the Hook button. When you have finished using it, press the Hook button again. When the headset is active, the phone lights the LED on the Hook button continuously red. When the headset is inactive, the phone turns off the LED.

You can also use a Bluetooth wireless headset with your ZIP4x5. To activate Bluetooth mode, select Menu | User Settings | Bluetooth | Enable, then press the Enter button. Section 10.5.7 on page 155 describes the process of detecting available Bluetooth headsets and pairing a Bluetooth headset with your phone.

To initiate a call with a Bluetooth headset that is paired with your phone, turn on the headset. The display shows the following Bluetooth icon when Bluetooth is enabled and the phone is able to communicate with your headset:

```
ZIP 4x5 SIP Phone
                  Ω
Fri 23 Apr 04   14:24
```

If Bluetooth is enabled, but the phone is not paired with a headset or cannot sense the headset to which it is paired, it will display the Bluetooth icon with a dash in the middle of the headset:

```
ZIP 4x5 SIP Phone
                  Ω
Fri 23 Apr 04   14:24
```

To use the speaker, press and release the Speaker key. When you have finished using it, press the key again. When the speaker is active, the phone lights the LED on the Speaker key continuously red. When the speaker is inactive, the phone turns off the LED.

9.1.2 Off Hook

The term *off hook* means that you do one of the following:

- pick up the handset
- press the Hook button so that it is active (LED is lit continuously red)
- press the Speaker key so that the speaker is active (LED is lit continuously red)

The phone is said to be off hook when you have done any one of these things.

9.1.3 On Hook

The term *on hook* means that you do all of the following:

- replace the handset in the cradle
- press the Hook button so that it is inactive (LED is off)
- press the Speaker key so that the speaker is inactive (LED is off)

The phone is said to be on hook when all of these conditions are met.

9.1.4 Switching Between the Handset, Headset, and Speaker

If you are using the handset and want to:

- use the headset, press the Hook button and replace the handset in the cradle
- use the speaker, press the speaker key and replace the handset in the cradle

If you are using the headset and want to:

- use the handset, pick up the handset
- use the speaker, press the speaker key

If you are using the speaker and want to:

- use the handset, pick up the handset
- use the headset, press the Hook button

9.1.5 Disconnecting the Handset or Headset

9.1.5.1 Handset

The phone cannot detect whether a handset is connected or not. Therefore if you connect or disconnect a handset during a call, the phone does not change its state.

9.1.5.2 Headset

Before a Call. If you connect a headset to the headset jack before making a call, you can use it to make or receive subsequent calls.

During a Call. If you are using a headset and unplug it during a call, the phone continues to send the sound to the headset jack. You cannot hear the other person and he or she cannot hear you. To resume the conversation, plug the headset back into the plug, lift the handset, or press the Speaker button.

If you connect a headset to the headset jack during a call, and the Hook button was inactive, then when you subsequently press the Hook button you can use the headset. If the Hook button was active when you inserted the headset you cannot use it during the current call.

9.2 Making a Call

To make a call, you normally want the phone to be in the idle state (see section 6.3.1 on page 50). You can obtain dial tone before you dial, or you can make a call without hearing a dial tone.[1]

Section 9.2.1 on page 99 and section 9.2.2 on page 101 describe how to dial a number. You can also make a call by dialling a SIP address as described in section 9.2.6 on page 102.

You can make a call by dialling from memory (the phone book) as described in section 9.7.5 on page 124, or by dialling from the list of recent calls as described in section 9.7.5 on page 124.

You can directly call from one ZIP4x5 to another without the aid of a call control system, as described in section 9.2.9 on page 105

Important This type of phone is different from phones that have been in common use for the past 100 years. On those older phones, as you press a button to dial a digit, the phone transmits the digit to the telephone exchange. On the ZIP4x5, the phone sends all the digits as a complete message and you therefore need to inform the phone when you have entered all the digits. The phone then assembles the complete message and sends it to the SIP server.

9.2.1 Dialling a Number After You Get Dial Tone

1. Do one of the following:

a. Take the phone off hook.[2]

- If all four call appearances are in use, nothing happens.
- If there is a free call appearance, the phone selects the lowest numbered call appearance that is free. The phone flashes the LED on that call appearance button green for 250 ms and off for 750 ms.[3] This indicates the call appearance has been reserved but is not yet in use.
- The phone provides dial tone to the handset, headset, or speaker as appropriate.[4]

b. Press one of the call appearance buttons that has its LED turned off.

1. It is not necessary to receive a dial tone. If the phone is connected to the switch, you can make a call. This is similar to the way you use a PC. If it is connected to the network, you can access the network – you do not require any audible feedback prior to accessing the network.
2. See section 9.1.2 on page 98 for a definition of off hook.
3. A summary of the meanings of the LEDs for the call appearance buttons is given in appendix B on page 193.
4. The tone that you hear is generated by the phone. You select that to match the tone commonly in use in your country. Section 10.5.10 on page 160 describes how you select the country where you live.

- The phone reserves the call appearance and indicates this by flashing the LED on that call appearance button green for 250 ms and off for 750 ms.
- The phone selects speaker mode and provides dial tone to the speaker.

2. The phone shows:

```
1. Call
```

The number on the first row is the call appearance that has been reserved for this call.

3. Enter the digits.[1]

- As you enter the digits, the phone displays the digits, for example:

```
1. Call
40883280
```

- The phone plays the DTMF digits to the handset, headset, or speaker as appropriate while you type them.
- The phone flashes the LED on the call appearance button fast, which is a prompt for you to press it.

4. When you have finished entering all the digits, do one of the following:

a. Press the # key.[2]

b. Press the call appearance button that is flashing green.[3]

c. Wait three seconds, after which time the phone assumes that you have entered all the digits.

5. The phone will play the DTMF digit for the # key.

6. The phone will send the dialled digits. It plays no sound while it does this.

7. The phone will change the display to (for example):

```
1. Calling
4083280450
```

The first line of the display shows the call appearance that is being used for the call.

8. The phone indicates the call appearance that is being used by changing the flashing for the LED on the call appearance button. The LED will be lit for 750 ms and flash off for 250 ms.

1. At this point, you can dial from a memory location in the phone book. When you do so, you don't need to enter any digits or do any of the items listed in step 4. See section 9.7.3 on page 122 for details.
2. If you want to send a # digit as part of the dialled name or number, see section 9.2.3 on page 101.
3. If you press any other call appearance button, the phone will clear the display and assume you want to make a new call.

9. While the call is proceeding, the phone plays ringback tone. This may be generated by the phone according to the country selection that you have made.
10. When the call is established (the called party has answered) the phone lights the LED on the call appearance button green continuously.

9.2.2 Dialling a Number without Dial Tone

You can make a call without having to hear a dial tone or the digits being dialled. You can do this while the phone is in the calculator mode. This mode is called "hot key dialling".

1. Enter the digits. The phone shows the digits on the screen. As you enter the digits the phone does not play the DTMF sounds for the digits.
2. Do one of the following:
   a. Pick up the handset. The phone selects the lowest number call appearance that is available and sends the digits.
   b. Press the Hook button. The phone selects the lowest number call appearance that is available, sends the digits, and routes the sound to the headset.
   c. Press the Speaker key. The phone selects the lowest number call appearance that is available, sends the digits, and puts the phone into speaker mode.
   d. Press one of the call appearance buttons. The phone sends the digits and puts the phone into speaker mode.
   e. Press the # key. The phone selects the lowest numbered call appearance that is available, sends the digits, and puts the phone into speaker mode. The phone does not play the DTMF digit for the # key.

You can also dial directly from the phone book without a dial tone as described in section 9.7.3 on page 122.

9.2.3 Sending a # as Part of the Number

When you are entering a number and you press the # key the phone interprets that as the end of the number and sends the number to the switch without the #. If you need to send a # as part of the string, press the Func key. The phone changes the top row of the display to show:

```
1. Call      Func:abc
```

The keys now allow you to enter letters as well as numbers. This is more fully described in section 9.2.6 on page 102. Press the * key twice to display characters that you can select. Use the right arrow on the volume key to highlight the # character, then press the * key again. Finally, press the Func key so that the keys enter only numbers again.

9.2.4 Dialling When in Calculator Mode

You can keep the phone normally in calculator mode as described in section 9.9.9 on page 132 and still be able to make and receive calls. When you want to make a call, you can do so with or without a dial tone.

If you want to dial a SIP address, you must exit calculator mode first.

1. Do one of the following:
   a. Lift the handset or press the Hook button.
   b. Press one of the call appearance buttons that is not lit.
2. The phone exits calculator mode, reserves a call appearance, and provides dial tone.
3. Dial the number or address as described in section 9.2.1 on page 99.

When you terminate the call, the phone returns to calculator mode if there is no activity on any of the call appearances (all LEDs on these buttons are off). When the phone resumes the calculator mode, the phone displays the state of any calculation that you had started.

9.2.5 Making a Call While Accessing the Menu

If you are accessing the menu and want to make a call, you can do so only by getting dial tone first. That is, you must go off hook or select a free call appearance as described in section 9.2.1 on page 99. When the call terminates the phone resumes access to the menu exactly as it was prior to the call. The phone automatically exits the menu function 60 s after the end of the call if you do not press any keys or buttons.

If you are accessing the phone book, and have used the search function to locate a name, number, or address, then when you go off hook or select a call appearance, the phone calls that contact and exits the menu function.

9.2.6 Dialling Using a SIP Address

9.2.6.1 Purpose

When you dial using a SIP address, you don't need to know a person's phone number. This is a good method of making a call if the person's address has been created logically. You can use any of the schemes described in section 9.2.1 on page 99 or section 9.2.2 on page 101. If the phone is in calculator mode see section 9.2.4 on page 101 for how to make the call.

A SIP address is normally written as:

SIP:name@domain

For example:

SIP:john.doe@zultys.com

With the ZIP4x5, you must not write "SIP:" because the phone will automatically insert that for you. Also, when you call an address that is within the same domain as your phone, you do not need to enter the domain name.

9.2.6.2 Entering an Address

To dial using a SIP address, you must take the phone out of calculator mode. See section 9.9.8 on page 132 for details. It is easier to enter an address in this manner without first selecting a call appearance or obtaining dial tone. When you have selected a call appearance, the phone times out between you entering characters and sends the characters. This time-out might be too short when creating an alphanumeric address.

To enter an alphanumeric address instead of a numeric address, press the Func key once. The display shows **Func:abc** on the top row. The function key in this mode locks the use of the keys so that you do not need to repeatedly press the Func key.

The digit keys 2 to 9 allow you to type the letters of the alphabet that are displayed on those keys. When you press a key, it selects the first character. If you quickly press the key again, it selects the second letter and so on. When you repeatedly press the key, the phone selects the next character in sequence, then the number of the key, then it scrolls back to the first letter.

To scroll through the list of characters, press the key within 800 ms of the last press. If you take longer than this, the cursor position moves to the right and when you next press the key you will select the first letter in the list. If you want to select a character from the same key to be the next character you enter, you can wait or you can press the right arrow on the volume key.

To select upper case characters instead of lower case characters, press the # key. The display shows **Func:ABC** on the top row. To return to selecting lower case characters, press the # key again. The arrow on that key reminds you the key is used to shift between upper and lower case characters.

The maximum length of a SIP address is defined to be 256 characters. However, the ZIP4x5 will allow you only to enter 64 characters. Once you reach that limit, the phone will not accept more characters.

9.2.6.3 Character Mapping on Numeric Keys

This is a list of the characters selected by repeatedly pressing the various keys:

1. ~, -, _, !, 1

2. a, b, c, 2; or A, B, C, 2

3. d, e, f, 3; or D, E, F, 3

4. g, h, i, 4; or G, H, I, 4

5. j, k, l, 5; or J, K, L, 5

6. m, n, o, 6; or M, N, O, 6

7. p, q, r, s, 7; or P, Q, R, S, 7

8. t, u, v, 8; or T, U, V, 8

9. w, x, y, z, 9; or W, X, Y, Z, 9

0. @, space, 0

****.*** * then selection

9.2.6.4 Using the * Key

When you press the * key, the ZIP4x5 selects the * which can be sent as a part of a dialled number, either by SIP or as a DTMF digit. If you press the * key twice within 800 ms, you can select from many different symbols. The phone changes the display to:

```
Select character:
.,:;-_#*()' "@&%/\<>~
+÷=±µ°?!§$€¥
```

The cursor is at the dot character. Use the left and right arrows on the volume key or the Up and Down buttons to move the cursor. Press the Esc button to exit this mode. When the cursor is highlighting the character you want to select press any other key. The phone places the character you selected in place of the * that it originally displayed.[1]

You can enter a dot (period or full stop) quickly by pressing the * key three times.

9.2.6.5 Exiting Alphanumeric mode

You can put the phone out of the alphanumeric mode by pressing Func at any time. This will allow you to easily enter digits that may be part of the address. You can return the phone to alphanumeric mode by pressing the Func key again.

9.2.6.6 Display

The process for making a call to a SIP address, and what the LCD shows during the process, are similar to that described in section 9.2.1 on page 99 and section 9.2.2 on page 101 for dialling a number. When you are entering the address, the display shows:

```
Call:       Func:abc
john.doe@z
```

9.2.6.7 Editing the Address

Use the volume key as described in section 9.2.7 on page 104.

9.2.6.8 Sending the Address

To send the address (and initiate the call), lift the handset, press the hook button, press the speaker key, or press a call button. If you did one of these prior to entering the address, press the # key twice or wait three seconds.

9.2.6.9 LEDs

The LEDs operate as they do when you enter a numeric phone number.

9.2.7 Editing a Number

You can edit a number or SIP address that you have entered by using the volume keys.

When you press the right arrow, the cursor moves forward through the digits. If the cursor was at the last digit, the phone places the cursor at the first digit.

When you press the left arrow, the phone deletes the character *to the left* of the cursor.[2] If you press the left arrow when the cursor is at the first character, the phone moves the cursor to the position after the last character (and it therefore does not delete any character).

1. You cannot use some of these characters as part of an address. The SIP address is formulated based on the same rules as an email address.
2. This is equivalent to the backspace action on a computer's keyboard.

For example, suppose you want to dial the number 12345, but instead you enter:

```
1245
```

You can either press the left arrow twice, to get:

```
12
```

Then enter 345. Or, press the right arrow three times so that the cursor is at the 4. Then enter 3. The digit three is inserted before the digit 4.

9.2.8 Dialling an Invalid Destination

When you initiate the call, the phone performs a simple check on the number or address that you entered. If this is invalid, the phone displays:

```
1. Invalid address
408€32
```

The phone retains this display for three seconds before returning to whatever was displayed prior to your initiating the call (usually the idle display). If you had selected a call appearance, it will become idle after five seconds.

9.2.9 Making a Call Without a SIP Proxy

The ZIP4x5 is intended for use with a telephone system but it is possible to use it without one. You might do this if you have two phones either directly connected or isolated on a network. To make the call, you must know the IP address of the phone you want to call or the other device must have an FQDN that your ZIP4x5 can resolve with a DNS server.

To make a call directly to the other device, ensure that:

- your phone has a unique IP address
- your phone has not registered with a SIP registrar
- you know the IP address and device ID of the phone you want to contact

The following instructions contain many steps, some of which may not be applicable, depending on the configuration of the phone prior to your using it:

1. Log into the phone using the password as described in section 10.6.1 on page 165.
2. Disable DHCP, set a static IP address, subnet mask and default gateway, as described in section 10.6.2 on page 166.[1]
3. Remove the address of the TFTP server and the address of the SIP outbound proxy, as described in section 10.6.2 on page 166.

1. It is not a requirement that the phones have a static IP address. However, if you use DHCP, the phone may receive a new IP address after its lease expires. You will have to find out this new IP address before you can make a call to that phone.

4. Assign a unique device ID to the phone and remove the domain name as described in section 10.6.5 on page 176.
5. Repeat these steps for the other phone.
6. Connect the phones so that they can be accessed over the LAN.
7. Create a call from one phone to the other using the method outlined in section 9.2.6 on page 102, but address the other phone by its device ID and IP address:

```
1. Call      Func:abc
<device ID>@<IP
address>
```

For example, if the two phones have device IDs of East and West, you might make a call from East to West by typing:

```
1. Call      Func:abc
West@10.1.13.17
```

If the other phone has an FQDN, you might enter:

```
1. Call      Func:abc
West@Zultys.West.com
```

8. If you want to repeatedly make calls in this manner, enter the address into a memory location, as described in section 10.2.2 on page 135. Dial the number from memory as described in section 9.7.3 on page 122.

9.3 Call Proceeding and Call Answered

9.3.1 Calling

When you have started to make a call, the display changes to:

```
1. Calling
4083280450
                 0:17
```

The display shows the call appearance that is in use for this call and the number or address being called. The display indicates the time (minutes and seconds) since you started the call and reflects the time that you have been waiting for the call to connect.

The phone displays the called number on the second line. In the unlikely event that the number is greater than 20 digits, the ZIP4x5 displays the rest of the number on the third line.

If the number that you have dialled is in your phone book, the ZIP4x5 displays the name of the called party instead of the phone number. It will display the name on the second and third lines. Where possible, the ZIP4x5 will split the name at a space character. For example:

```
1. Calling
Zultys Technologies
                 0:17
```

or:

```
1. Calling
Lancelot Capability
Brown            0:17
```

The phone will continue to use this name instead of the number for future displays during this call.

If you have dialled the person using a SIP address, the phone will display this instead of a number. It will try to break the name at a period (full stop), “at” symbol, or other punctuation.

The LED on the call appearance button flashes green for 750 ms and off for 250 ms.

You will hear nothing during this phase of the call.

9.3.2 Ringback

9.3.2.1 ZIP4x5 to SIP Phone Calls or ZIP4x5 to ISDN Calls

When you make a call to another SIP phone, the ringback that you hear will be generated by your phone. The tones will be those that you have selected for the country.[1]

If you are making a call to the PSTN, the SIP to PSTN gateway normally opens the communication path so that you hear the sound coming from the network. Therefore, if you are calling a different country you will hear the ringback tone from that country. This tone may be different from that used in your country.

The LED on the call appearance button continues to flash green for 750 ms and off for 250 ms. The display changes to:

```
1. Ringing
4083280450
                 0:32
```

The timer continues to show the time since you initiated the call.

1. See section 10.5.10 on page 160 for details on how you select the country.

9.3.2.2 ZIP4x5 to CAS Calls

If you are connected to the PSTN using T1 CAS circuits, your SIP to PSTN gateway may not know the status of the connection. It may open the speech path even though there is no ringback. The LED on the call appearance button will then be lit solidly green.

The phone behaves as if the call has been established as described in section 9.5 on page 115. Because the speech path is open, you may hear busy tone although the phone indicates that you are connected.

9.3.3 Far End Busy

If the person you are calling is busy, the phone either plays the busy tone for your country or the busy tone that is generated by the phone network at the far end. This depends whether your server has indication that the called party is busy or not. If your server is aware the called party is busy, your phone flashes the LED on the call appearance button green for 750 ms and red for 250 ms. The display changes to:

```
1. Far end busy
4083280450
                0:28
```

The phone stops the timer as soon as it receives notification that the called party is busy. The phone maintains this state until you go on hook.

9.3.4 Network Busy

If the network is busy, the phone either plays the fast busy tone (congestion tone) for your country or the fast busy tone that is generated by the phone network at the far end. This depends whether your server can detect whether or not the network is busy. If it is aware the network is busy, your phone flashes the LED on the call appearance button green and red for 250 ms each color.

The ZIP4x5 displays this message if the number you are calling does not exist or is not available.

The display changes to:

```
1. Network busy
4083280450
                0:23
```

The phone stops the timer as soon as it receives notification that the network is busy.

The phone maintains this state until you go on hook.

9.3.5 Call Answered

9.3.5.1 Expanded Display

When the called party answers, the phone makes the LED for the call appearance to be lit continuously green and changes the display to:

```
1. Connected
4083280450
             00:00:45
```

or

```
1. Connected
Lancelot Capability
Brown        00:00:45
```

The display shows the duration of the call in hours, minutes, and seconds. The phone starts this timer from zero when it is made aware that the phone is connected. Depending on the system and the protocol used to complete the call, the phone may believe the call is connected but the called person has not yet answered the call.

If you want to display the date and time, use the Up or Down buttons to show the call appearance summary.[1]

You can toggle the phone to the compressed display mode by pressing the Enter button.[2]

9.3.5.2 Call Appearance Summary

This summary display is part of the expanded display. Press Up or Down to scroll through the expanded displays. At the end of the list, the display changes to:

```
1. Cnct   2. Idle
3. Idle   4. Idle
Sun 31 Aug 02  20:32
```

The display shows the state of each call appearance as follows:

- **Idle.** Call appearance not in use.
- **Call.** Calling.
- **FrRn.** The far end (called party) is ringing.
- **Cnct.** Connected.
- **Busy.** Far end busy.
- **NwBz.** Network busy

1. Do not press the Func key or Menu button before pressing the Up and Down buttons.
2. Do not press the Func key or Menu button before pressing the Enter button.

- **Ring.** There is an incoming call.
- **Hold.** You have placed the call (individual or conference call) on hold.
- **Conf.** The person is part of a conference call.
- **Trns.** You are in the middle of transferring the call.
- **Rejc.** Call to another phone was rejected.

You can toggle the phone to the compressed display mode by pressing the Enter button.

9.3.5.3 Compressed Display

When the phone displays the data in the compressed mode, the LED remains unchanged at solid green while the display changes to:

```
1. 4083280450  00:45

Sun 31 Aug 02  20:32
```

or:

```
1. Lancelot C  00:45

Sun 31 Aug 02  20:32
```

On the top row, the phone displays:

- the call appearance for this call (1 to 4)
- the number you called (or the SIP address of the person you called) or the name of the person if the name exists in the phone book
- a timer that indicates the duration of the call

The phone truncates the number (or name) that you have called to 12 characters so that it can display the duration of the call. The phone leaves a minimum of two spaces between the end of the phone number and the timer.

The timer shows the call time in minutes and seconds until the call length has reached an hour. It then displays the time in hours and minutes.

The phone displays the current time and date just as it does in the idle state.[1]

You can toggle the phone to the expanded display mode by pressing the Enter button.[2]

1. See section 6.3.1 on page 50 for the description of the idle state.
2. Do not press the Func key or Menu button before pressing the Enter button.

9.3.6 Network Failure

If the phone sends a message to the SIP server that the SIP server does not answer, the phone displays:

```
Unable to
communicate with
SIP device
```

The phone makes the handset, headset, and speaker quiet and displays the message until you attempt to make another call or perform another task on the phone.

You should contact the administrator of the system if you see this message.

9.4 Receiving a Call

9.4.1 Alerting

When you receive a call, the phone flashes the LED of the call appearance button. The LED flashes on for 250 ms and off for 250 ms.

The phone plays a ringing tone on the speaker if you have no active calls and you have adjusted the volume to be greater than zero. If you set the volume to zero, the ZIP4x5 plays no ring sound.

The phone plays one ring tone for calls that originate from outside the enterprise and another for those that originate inside the enterprise. You select the sound that is played using the menu as described in section 10.5.5 on page 149. You adjust the volume as described in section 6.2.1.3 on page 49.

9.4.2 Before You Answer

9.4.2.1 Expanded Display

When the phone is in the expanded display mode it shows on the display:

```
1. To <called name>
<caller's name, 1>
<caller's name, 2>
```

The phone shows the call appearance and the name of the called person, truncated to 14 characters. This name is taken from the SIP message and not from the name you have programmed into the phone. The phone shows this information because the phone could be shared by multiple people or another person might have redirected his or her calls to your phone.

The phone displays the name of the caller, again taken from the SIP message. The ZIP4x5 will try to break the name at a space character to neatly fit onto the two lines, or at a period (full stop), “at” symbol, or other punctuation if the name is a SIP address.

The phone shows in each case, the display name from the SIP message if it is present, otherwise it displays the user portion of the SIP URI.

For example, the phone might show:

```
1. To Garden Cottage
Lancelot Capability
Brown
```

If the SIP header had a number, the ZIP4x5 tries to match the number with numbers you have entered into the phone book.[1] If the phone finds a match, it displays the name associated with that number in the phone book instead of the number itself. If the SIP header did not have a name or number for the caller, it will show the SIP address of the caller.

You can toggle the phone to the compressed display mode by pressing the Enter button.

9.4.2.2 Compressed Display

When the phone is in the compressed display mode it shows on the display:

```
1. Lancelot Capabili

Sun 31 Aug 02  20:3
```

The phone truncates the caller's name or address to 17 characters. You can toggle the phone to the expanded display mode by pressing the Enter button.

9.4.3 Receiving Multiple Calls and Call Waiting

If you receive multiple calls, the phone flashes the LEDs on the call appearance buttons for each incoming call.

If you have an active call (a call appearance button is lit continuously green or continuously orange), the phone plays a short beep in the currently selected audio path. You can select the tone that is played as described in section 10.5.5 on page 149.

If you have one or more calls on hold, and you have placed the phone on hook, the phone plays the ringing tone you selected on the speaker.

9.4.3.1 Expanded Display

The display shows the first call that was received. To view the details of other calls, press the Up and Down buttons.[2] The display changes, for example:

```
1. To Garden Cottage
Lancelot Capability
Brown
```

1. The phone book is covered in detail in section 10.2 on page 133.
2. Do not press the Func key or Menu button before pressing the Up or Down buttons.

Press Down:

```
2. To Garden Cottage
Lord Blenheim
```

Press Down:

```
3. To Garden Cottage
Oxford Stone Masons
```

Press Down:

```
1. Ring   2. Ring
3. Ring   4. Idle
Tue 10 Feb 04  18:47
```

This example is for the case when there are three incoming calls. The meaning of the abbreviations on the fourth display is described in section 9.3.5.2 on page 109.

You can toggle the phone to the compressed display mode by pressing the Enter button.

9.4.3.2 Compressed Display

The display shows information for multiple calls. You can scroll the display by pressing the Up and Down buttons:

```
1. Lancelot Capabili
2. Lord Blenheim
3. Oxford stone Maso
```

Press Down:

```
2. Lord Blenheim
3. Oxford Stone Maso
Tue 10 Feb 04  13:24
```

Press Down:

```
3. Oxford stone Maso
Tue 10 Feb 04  13:242
1. Lancelot Capabili
```

The phone truncates the caller's name or address to 17 characters. When you press the Up and Down buttons, the rows of text denoting the call appearances scroll along with the date and time.

You can toggle the phone to the expanded display mode by pressing the Enter button. When you do so, the phone displays the details of the caller that was on the top row of the compressed display.