N4100

Wireless N HotSpot Gateway

User's Guide

Default Login Details

IP Address	192.168.1.1
User Name	admin
Password	1234

Version 1.0
Edition 1, 11/2010

ZyXEL

www.zyxel.com

About This User's Guide

Intended Audience

This manual is intended for people who want to configure the N4100 using the web configurator.

Related Documentation

- Quick Start Guide

  The Quick Start Guide is designed to help you get your N4100 up and running right away. It contains information on setting up your network and configuring for Internet access.

- Support Disc

  Refer to the included CD for support documents.

Documentation Feedback

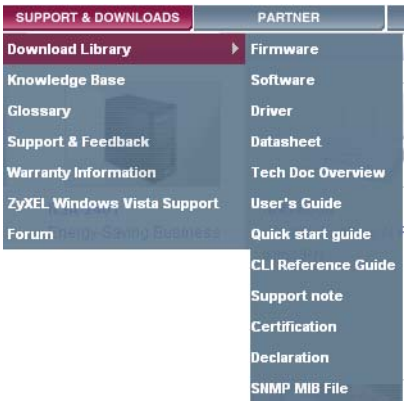
Send your comments, questions or suggestions to: techwriters@zyxel.com.tw

Thank you!

The Technical Writing Team, ZyXEL Communications Corp.,
6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 30099, Taiwan.

Need More Help?

More help is available at www.zyxel.com.



- Download Library

  Search for the latest product updates and documentation from this link. Read the Tech Doc Overview to find out how to efficiently use the documentation in order to better understand how to use your product.

- Knowledge Base

  If you have a specific question about your product, the answer may be here. This is a collection of answers to previously asked questions about ZyXEL products.

- Forum

  This contains discussions on ZyXEL products. Learn from others who use ZyXEL products and share your experiences as well.

Customer Support

Should problems arise that cannot be solved by the methods listed above, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

See http://www.zyxel.com/web/contact_us.php for contact information. Please have the following information ready when you contact an office.

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this User's Guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- This product may be referred to as the "N4100", the "device" or the "system" in this User's Guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A key stroke is denoted by square brackets and uppercase text, for example, [ENTER] means the "enter" or "return" key on your keyboard.
- "Enter" means for you to type one or more characters and then press the [ENTER] key. "Select" or "choose" means for you to use one of the predefined choices.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Maintenance > Log > Log Setting** means you first click **Maintenance** in the navigation panel, then the **Log** sub menu and finally the **Log Setting** tab to get to that screen.
- Units of measurement may denote the "metric" value or the "scientific" value. For example, "k" for kilo may denote "1000" or "1024", "M" for mega may denote "1000000" or "1048576" and so on.
- "e.g.," is a shorthand for "for instance", and "i.e.," means "that is" or "in other words".

Icons Used in Figures

Figures in this User's Guide may use the following generic icons. The N4100 icon is not an exact representation of your device.

N4100 	Computer 	Notebook computer 
Server 	Modem 	Firewall 
Telephone 	Switch 	Router 

Safety Warnings

- Do NOT use this product near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. ONLY qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Use ONLY an appropriate power adaptor or cord for your device.
- Connect the power adaptor or cord to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe).
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Do NOT use the device if the power adaptor or cord is damaged as it might cause electrocution.
- If the power adaptor or cord is damaged, remove it from the device and the power source.
- Do NOT attempt to repair the power adaptor or cord. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Do NOT obstruct the device ventilation slots, as insufficient airflow may harm your device.
- Antenna Warning! This device meets ETSI and FCC certification requirements when using the included antenna(s). Only use the included antenna(s).
- If you wall mount your device, make sure that no electrical lines, gas or water pipes will be damaged.

Your product is marked with this symbol, which is known as the WEEE mark. WEEE stands for Waste Electronics and Electrical Equipment. It means that used electrical and electronic products should not be mixed with general waste. Used electrical and electronic equipment should be treated separately.

Contents Overview

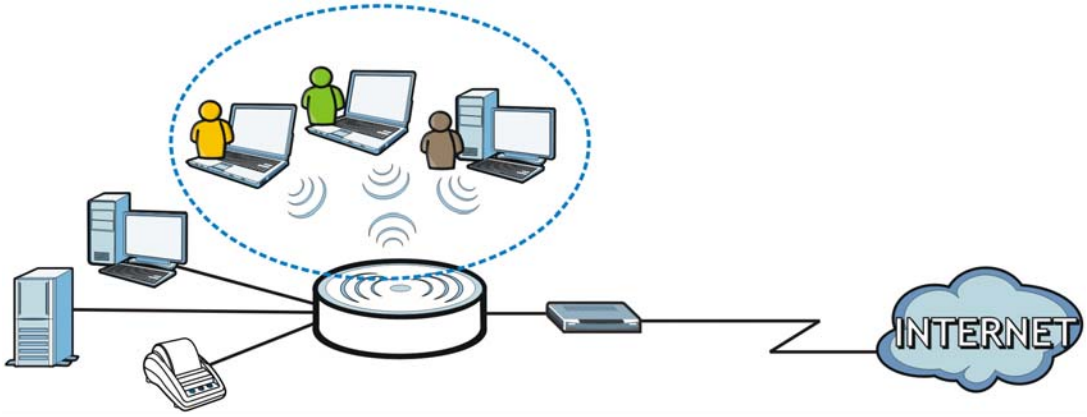
Table of Contents

PART I
User's Guide

1 Introduction

1.1 Overview

The N4100 combines an IEEE 802.11n wireless access point, router, 4-port switch and service gateway in one box. If you have a "statement printer", you can connect it directly to the N4100, allowing you to easily print subscriber statements. The N4100 is ideal for offices, coffee shops, libraries, hotels and airport terminals catering to subscribers that seek Internet access. You should have an Internet account already set up and have been given usernames, passwords etc. required for Internet access.



1.2 Managing the N4100

Use the N4100's built-in Web Configurator to manage it. You can connect to it using a web browser such as Firefox 2.0 (and higher) or Internet Explorer 6 (and higher). The web configurator gives you access to all the available settings for this product. For details on connecting to it, see the Quick Start Guide.

1.3 Good Habits for Managing the N4100

Do the following things regularly to make the N4100 more secure and to manage the N4100 more effectively.

- Change the password. Use a password that's not easy to guess and that consists of different types of characters, such as numbers and letters.
- Write down the password and put it in a safe place.
- Back up the configuration (and make sure you know how to restore it). Restoring an earlier working configuration may be useful if the device becomes unstable or even crashes. If you forget your password, you will have to reset the N4100 to its factory default settings. If you backed up an earlier configuration file, you would not have to totally re-configure the N4100. You could simply restore your last configuration.

1.4 Applications for the N4100

Here are some example uses for which the N4100 is well suited.

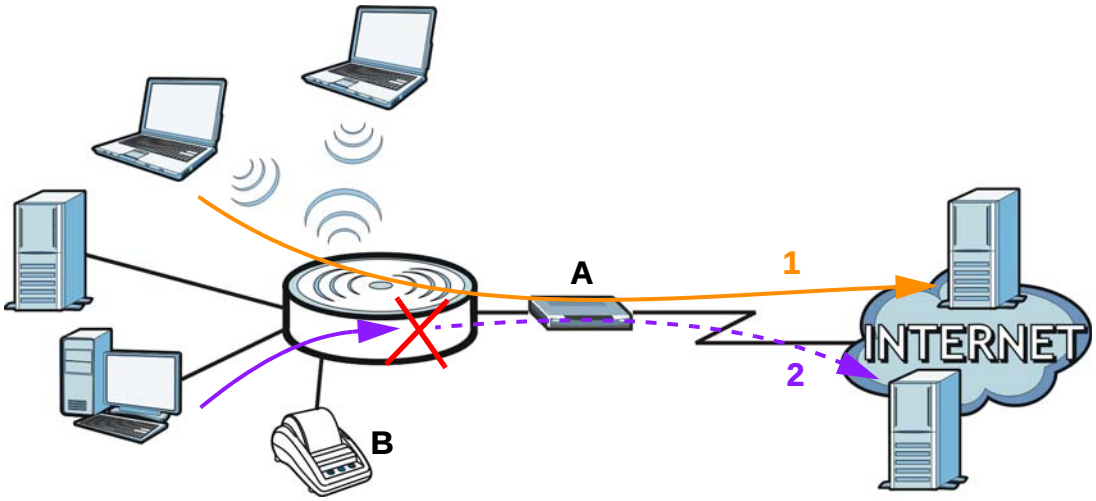
1.4.1 Internet Access

With a broadband modem or router (A), the N4100 allows the attached computers to enjoy high speed Internet access. Computers can connect to the ZyXEL Device's LAN ports (or wirelessly).

In public areas, such as a hotel or coffee shop, the N4100 provides high speed Internet access to subscribers with account billing and authentication, which can be done using a statement printer (B) and local subscriber database.

You can also configure filtering on the N4100 for secure Internet access. Use filtering to block access to specific IP addresses or web sites. For example, you could block subscriber access to pornographic or gambling web sites (2).

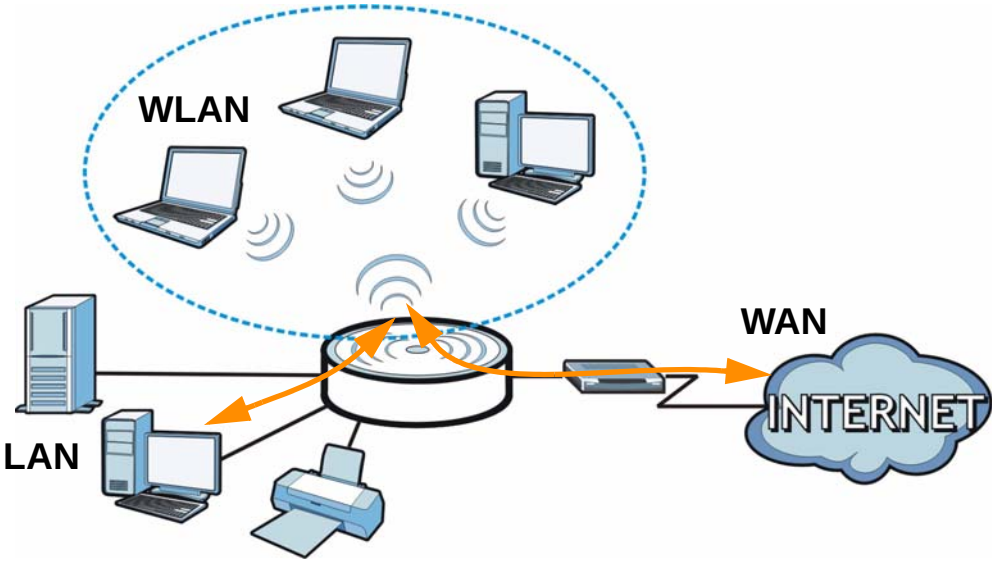
Figure 1 Internet Access Applicarion



1.4.2 Wireless Connection

By default, the wireless LAN (WLAN) is enabled on the N4100. IEEE 802.11b/g/n compliant clients can wirelessly connect to the N4100 to access network resources. The N4100 functions as an access point (AP) to bridge the wired and the wireless network allowing wireless stations to access the Internet through the N4100.

Figure 2 Wireless Connection Application



1.5 Restoring Factory Defaults

You can erase the current configuration and restore factory defaults using either the web configurator or the **RESET** button at the back of the device.

The web configurator allows you to reset the system but retain subscriber account information. See Chapter 29 on page 225 for more information.

If you forget your password or cannot access the web configurator, you will need to use the **RESET** button to reload the factory-default configuration file. This means that you will lose all of your custom configuration, including the local subscriber database, and the administrator password will be reset to “1234”.

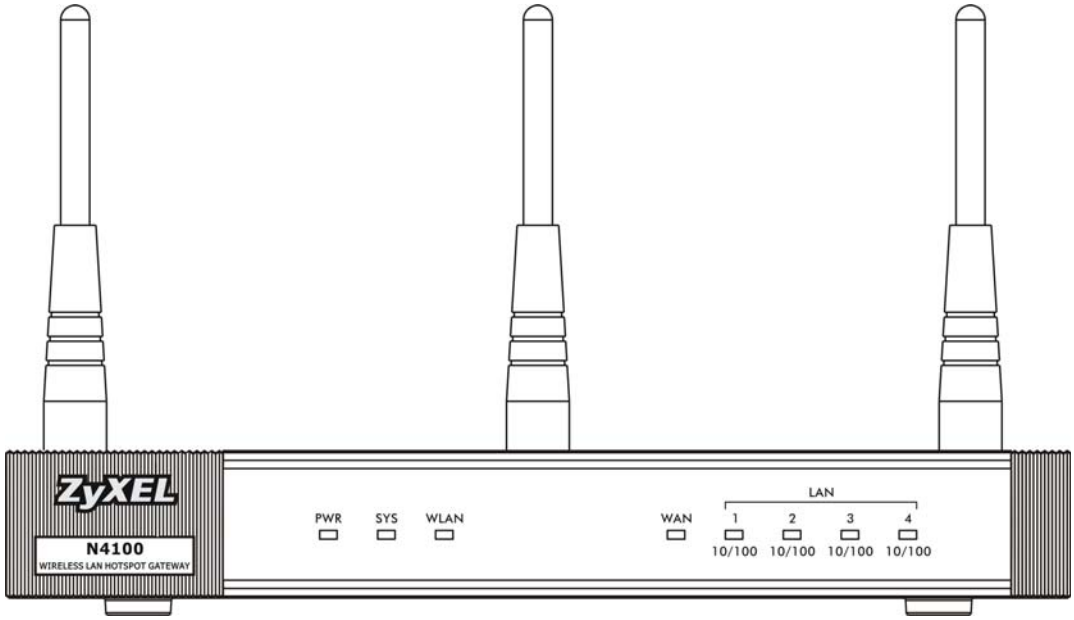
1.5.1 Using the Reset Button

1. Make sure the **POWER** LED is on (not blinking).
2. To set the device back to the factory default settings, use a pointed object to press the **RESET** button once or until the **PWR** LED begins to blink and then release it. When the **PWR** LED begins to blink, the defaults have been restored and the device restarts.

1.6 LEDs (Lights)

The following graphic displays the labels of the LEDs.

Figure 3 LEDs on the Front Panel



None of the LEDs are on if the N4100 is not receiving power.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The N4100 is receiving power.
		Off	The N4100 is not receiving power.
SYS	Green	On	The N4100 is ready and running.
		Off	The N4100 is not ready or has failed.
WLAN	Green	On	The wireless network is activated.
		Blinking	The N4100 is communicating with other wireless clients.
		Off	The wireless network is not activated.
WAN	Green	On	The N4100 has an Ethernet connection with another device (such as a broadband modem) through this port.
		Blinking	The N4100 is sending/receiving data through this port.
		Off	The N4100 does not have an Ethernet connection through this port.

Table 1 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
LAN 1~4	Green	On	The N4100 has an Ethernet connection with another device (such as a computer) through this port.
		Blinking	The N4100 is sending/receiving data through this port.
		Off	The N4100 does not have an Ethernet connection through this port.

Refer to the Quick Start Guide for information on hardware connections.

2

The Web Configurator

2.1 Overview

The web configurator is an HTML-based management interface that allows easy device setup and management via Internet browser. Use Internet Explorer 6.0 and later or Firefox 2.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in Windows XP SP (Service Pack) 2.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

See Appendix B on page 291 if you need to make sure these functions are allowed in Internet Explorer.

2.1.1 Accessing the Web Configurator

Note: The N4100 allows only one web configurator session at a time.

1. Make sure your N4100 hardware is properly connected (refer to the Quick Start Guide for details on this).
2. Launch your web browser.

3 Launch your web browser and type the WAN or LAN IP address of the N4100 as the web address (it is recommended that you connect your computer to the LAN and use the LAN IP address for initial configuration). **192.168.1.1** is the default IP address for the LAN port.

If you are using a different port number (between 8000 and 8099) for the web server, you must also append the port number to the LAN IP address separated with a colon ":", for example, http://192.168.1.1:8080.

Figure 4 N4100's IP Address

4 A password screen displays. Enter your user name and password. The default administrator user name is **admin** and the default password is **1234**. Click **Login**.

Note: The user name and password are case sensitive.

Figure 5 Password Screen

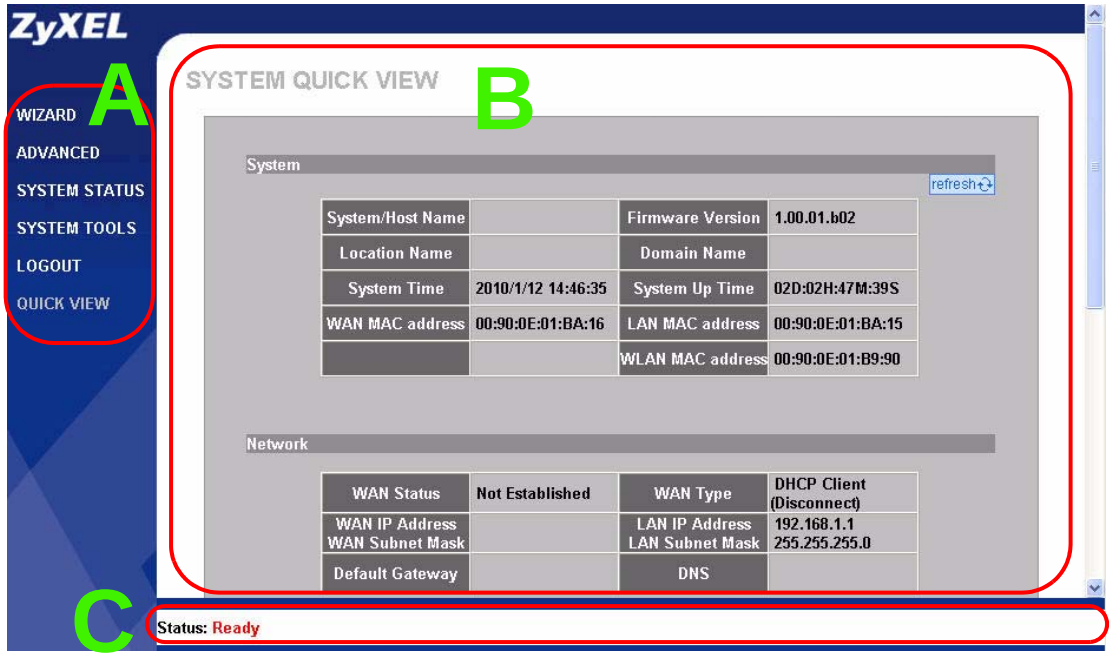
5 You should see the first screen of the Wizard setup. Refer to the Quick Start Guide for more information on configuring the Wizard setup screens.

Note: For security reasons, the N4100 automatically logs you out if there is no activity for longer than five minutes after you log in. If this happens, simply log back in again. You can change the time period in the **ADVANCED > SERVER** screen's **Administrator Idle-Timeout** field.

2.2 Web Configurator Main Screen

The main screen is divided into these parts:

Figure 6 Main Screen



- **A** - navigation panel
- **B** - main window
- **C** - status bar

2.2.1 Navigation Panel

Use the menu items on the navigation panel to open screens to configure N4100 features. The following tables describe each menu item.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
WIZARD		Use these screens for initial configuration including WAN and wireless setup, subscriber authentication, billing profile, account generating, statement printout, and system password and time.
ADVANCED		
SYSTEM		Use this screen to configure your device's name, change your N4100's time and date, configure from which IP address(es) users can manage the N4100, enable NAT and other system-related general settings.
WAN/LAN		Use this screen to set the LAN IP address, and configure the WAN settings on the N4100 for Internet access.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
SERVER	Server	Use this screen to set the embedded web server, the LAN DHCP server and specify the e-mail server for e-mail redirection.
	Static DHCP Table	Use this screen to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.
AUTHENTICATION		Use this screen to set up subscriber authentication on the N4100.
RADIUS		Use this screen to configure the N4100 to use an external RADIUS server.
BILLING		Use this screen to set up subscriber billing.
ACCOUNTING		Use this screen to set up and manage subscriber accounts.
CREDIT CARD		Use this screen to set the N4100 to handle credit card transactions.
KEYPAD		Use this screen to set up the optional keypad for a statement printer.
CUSTOMIZATION	Login Page	Use this screen to customize the subscriber login screen.
	Logo	Use this screen to upload your logo file.
	Information Windows	Use this screen to customize the information window on the subscriber's computer after a successful login.
	Account Printout	Use this screen to customize the account printout.
	Credit Card	Use this screen to customize the subscriber credit card billing interface.
PASS THROUGH		Use this screen to specify devices that can have traffic pass through the N4100.
FILTERING		Use this screen to block subscriber access to a list of destinations.
SHARE		Use this screen to allow logged-in subscribers to share devices on the LAN.
PORTAL PAGE		Use this screen to set the first web site to which a subscriber is redirected after logging in successfully.
ADVERTISEMENT		Use this screen to set advertisement links.
WALLED GARDEN		Use this screen to create walled garden web sites.
DDNS		This screen allows you to use a static hostname alias for a dynamic IP address.
LAN DEVICES		Use this screen to configure port mapping to make LAN devices behind the N4100 visible to the outside world.
SYSLOG	Syslog	Use this screen to configure the syslog server information. You can also set it to e-mail the logs to you.
	Log Settings	Use this screen to select which logs your N4100 is to send and the schedule for when the N4100 is to send the logs.
SESSION TRACE		Use this screen to configure the N4100 to record details about subscriber Internet access and to where the N4100 sends logs of the session traces.

Table 2 Navigation Panel Summary

LINK	TAB	FUNCTION
SECURE REMOTE		Use this screen to allow the N4100 to send RADIUS packets, syslogs and log e-mails through a PPTP VPN tunnel.
SNMP		Use this screen to to configure your N4100's settings for Simple Network Management Protocol (SNMP) management.
BANDWIDTH		Use this screen to limit the amount of upstream and downstream bandwidth each user can use.
WIRELESS		Use this screen to configure the wireless LAN settings, WLAN authentication/security settings.
ACCOUNT GENERATOR		Use this screen to use the N4100 with one or more account generators (statement printers).
LICENSING	Registration	Use this screen to register your N4100 with myZyXEL.com.
	Service	Use this screen to upgrade a service and update your service subscription status.
SYSTEM STATUS		
SYSTEM		This screen shows the current state of the N4100.
ACCOUNT LIST		This screen shows the subscriber account list.
ACCOUNT LOG		This screen shows information on the N4100's subscriber account logs.
CURRENT USER		This screen shows a list of subscribers currently logged on to the N4100 for Internet access.
DHCP CLIENT		This screen shows current DHCP client information of all network clients using the DHCP server on the N4100.
SESSION LIST		This screen shows incoming and outgoing packet information.
LAN DEVICES		This screen shows the status of LAN devices configured in the **ADVANCED > LAN DEVICES** screen.
SYSTEM TOOLS		
CONFIGURATION		Use this screen to backup and restore your device's configuration (settings) or reset the factory default settings.
FIRMWARE	Manual Firmware Upgrade	Use this screen to manually upload firmware to your device.
	Scheduled Firmware Upgrade	Use this screen to automatically download the latest firmware from a TFTP server.
SYSTEM ACCOUNT		Use this screen to configure your N4100's login user names and passwords.
SSL CERTIFICATE		Use this screen to download a CA registered certificate from a computer connected to the N4100.
PING COMMAND		Use this screen to test the Internet connection.
RESTART		This screen allows you to reboot the N4100 without turning the power off.
LOGOUT		Click this link to log out of the web configurator.
QUICK VIEW		Use this screen to view key system status information.

2.2.2 Main Window

The main window displays information and configuration fields. It is discussed in the rest of this document.

2.2.3 Status Bar

Check the status bar when you click **Apply** or **OK** to verify that the configuration has been updated.

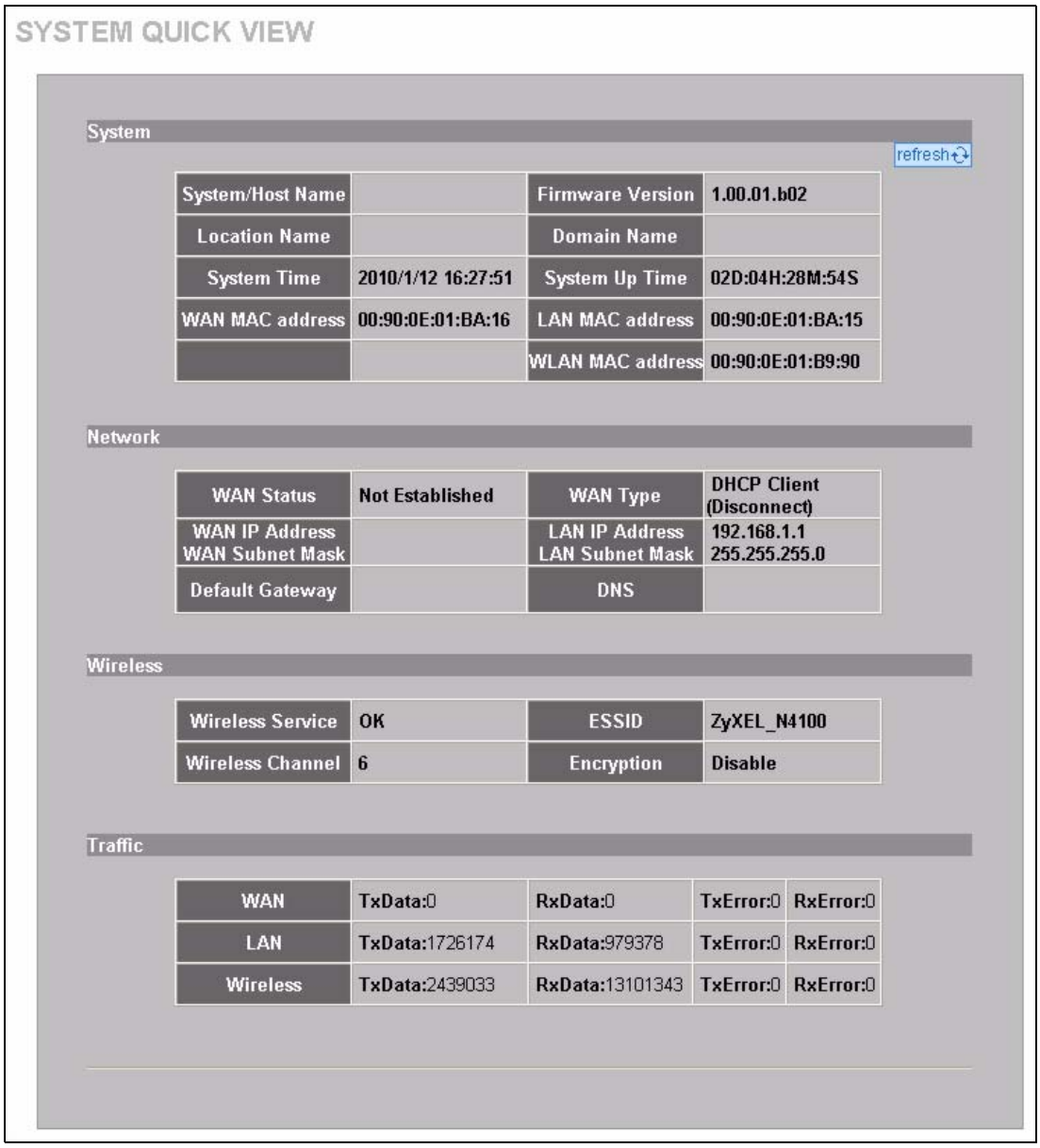
2.2.4 Wizard Setup Screens

The Wizard setup screens display when you first access the N4100. Refer to the Quick Start Guide for information on how to configure the Wizard setup screens.

2.2.5 System Quick View Screen

click **QUICK VIEW** to display the following screen. This screen displays key system status information.

Figure 7 Quick View



The following table describes the labels in this screen.

Table 3 Quick View

LABEL	DESCRIPTION
System	
Refresh	Click **Refresh** to update this screen.

Table 3 Quick View

LABEL	DESCRIPTION
System/Host Name	This field displays the description name of the N4100 for identification purposes.
Firmware Version	This field displays the version of the firmware on the N4100.
Location Name	This field displays the device's geographical location.
Domain Name	This field displays the domain name of the N4100.
System Time	This field displays the N4100's current time.
System Up Time	This field displays the how long the N4100 has been operating since it was last started.
WAN MAC Address	This field displays the MAC address of the N4100 on the WAN.
LAN MAC Address	This field displays the MAC address of the N4100 on the LAN.
WLAN MAC Address	This field displays the MAC address of the N4100 on the wireless LAN.
Network	
WAN Status	This field displays the status of the N4100's connection to the Internet (**Established** or **Not Established**).
WAN Type	This field displays the DHCP mode of the WAN port and whether the WAN port is connected to an Ethernet device. It displays **DHCP Client**, **Static IP Setting**, **PPPoE**, or **PPTP**.
WAN IP Address WAN Subnet Mask	This field displays the IP address and the subnet mask of the WAN port on the N4100.
LAN IP Address LAN Subnet Mask	This field displays the IP address and the subnet mask of the LAN port on the N4100.
Default Gateway	This field displays the IP address of the default gateway of the WAN port on the N4100.
DNS	This field displays the IP address of the DNS server that the N4100 is using.
Wireless	
Wireless Service	This field displays the status of the N4100's wireless LAN.
ESSID	This field displays the N4100's Extended Service Set IDentity.
Wireless Channel	This field displays the channel that the N4100 is using.
Encryption	This field displays the type of data encryption that the N4100 is using. **WEP**, **WPA** or **WPA2** displays if N4100 is using WEP, WPA or WPA2 data encryption correspondingly. **Disable** displays if the N4100 is not using data encryption.
Traffic	
WAN	This field displays traffic statistics for the N4100's WAN connection.
LAN	This field displays traffic statistics for the N4100's LAN connection.
Wireless	This field displays traffic statistics for the N4100's wireless LAN connection.

3

Tutorials

3.1 Overview

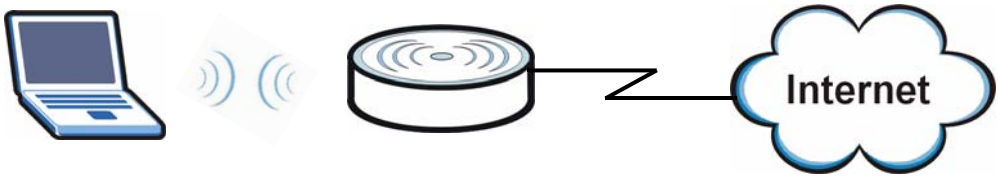
This chapter describes:

- how to set up a wireless network (Section 3.2 on page 35).
- how to generate a subscriber account (Section 3.3 on page 38).
- how to log in as a subscriber (Section 3.4 on page 42).
- how to print reports using SP300E (Section 3.5 on page 42).
- how to access the N4100 using DDNS (Section 3.6 on page 49).
- how to remotely access or manage the device behind the N4100 (Section 3.7 on page 51)
- how to set up and enable SSL security on the N4100 (Section 3.8 on page 52)

Note: The tutorials featured in this chapter require a basic understanding of connecting to and using the Web Configurator on your N4100. For details, see the included Quick Start Guide. For field descriptions of individual screens, see the related technical reference in this User's Guide.

3.2 Wireless Network Setup

The N4100 is connected to a broadband modem with Internet access. Thomas wants to set up a wireless network so that the users can use their notebooks or computers to wirelessly access the Internet through the N4100. In this wireless network, the N4100 serves as an access point (AP), and the notebook with a wireless network card or USB/PCI adapter is the wireless client. The wireless client can access the Internet through the AP.



Thomas has to configure the wireless network settings on the N4100. Then users can set up a wireless network using manual configuration (Section 3.2.2 on page 37).

3.2.1 Configuring the N4100 Wireless Network Settings

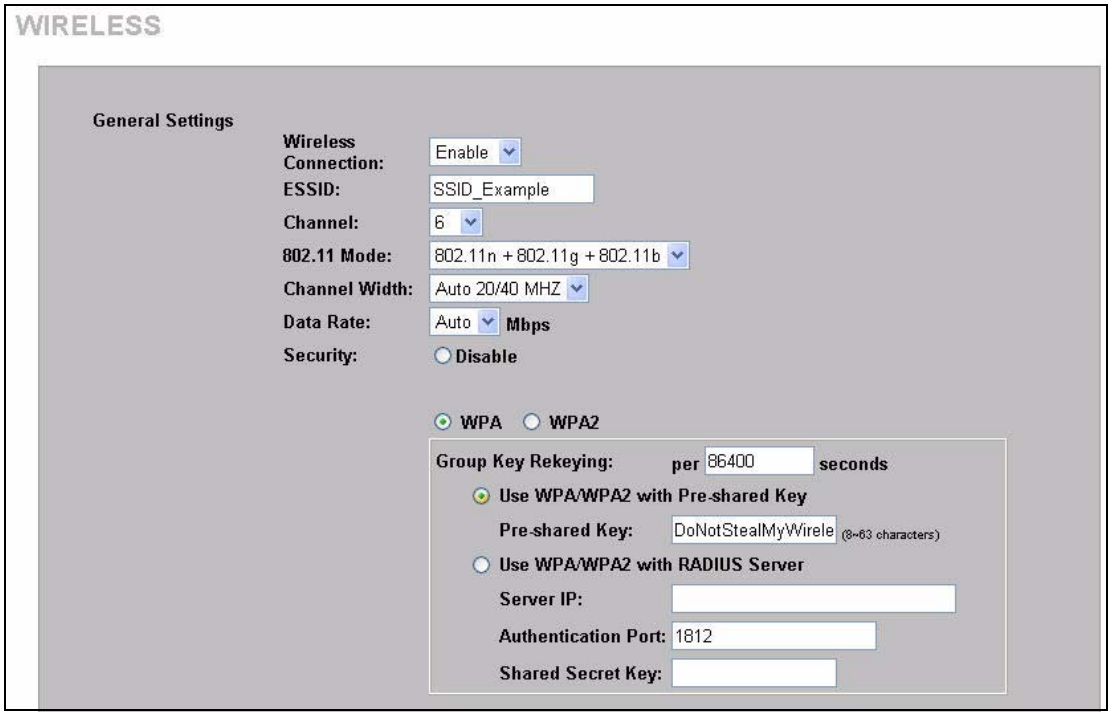
This example uses the following parameters to set up a wireless network.

SSID	SSID_Example
Security Mode	WPA-PSK
Pre-Shared Key	DoNotStealMyWirelessNetwork
802.11 Mode	IEEE 802.11b/g/n (Mixed)

Follow the steps below to configure the wireless settings on the N4100.

Note: To see the current SSID, go to the **SYSTEM STATUS > SYSTEM** or the **System Quick View** screen.

1 Open the **ADVANCED > WIRELESS** screen in the N4100's web configurator. Configure the screen using the provided parameters (see page 36).



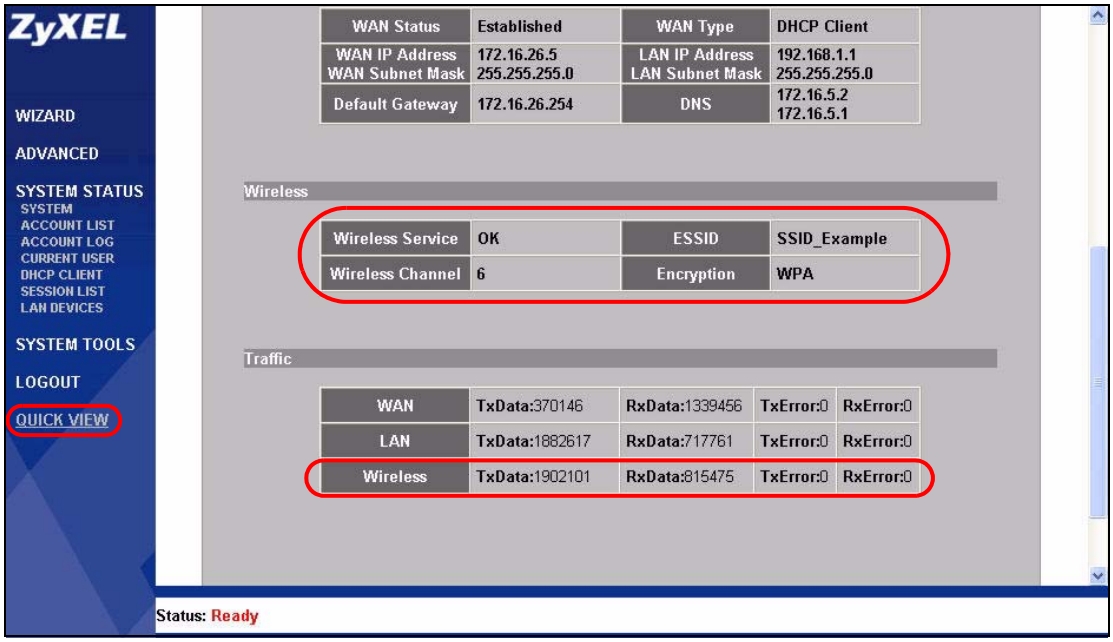
2 Make sure **Enable** is selected in the **Wireless Connection** field.

3 Enter "SSID_Example" as the ESSID and select a channel which is not used by another AP.

4 Select **802.11n + 802.11g + 802.11b** in the **802.11 Mode** field.

5 Set security mode to **WPA**, select the **Use WPA/WPA2 with Pre-shared Key** option and enter “DoNotStealMyWirelessNetwork” in the **Pre-shared Key** field. Click **Apply**.

6 Click **QUICK VIEW** to open the **System Quick View** screen. Verify your wireless and wireless security settings and check if the WLAN connection is up.



7 The user can now use the notebook’s wireless client to search for the N4100 (see Section 3.2.2 on page 37).

3.2.2 Connecting to the N4100 Wirelessly

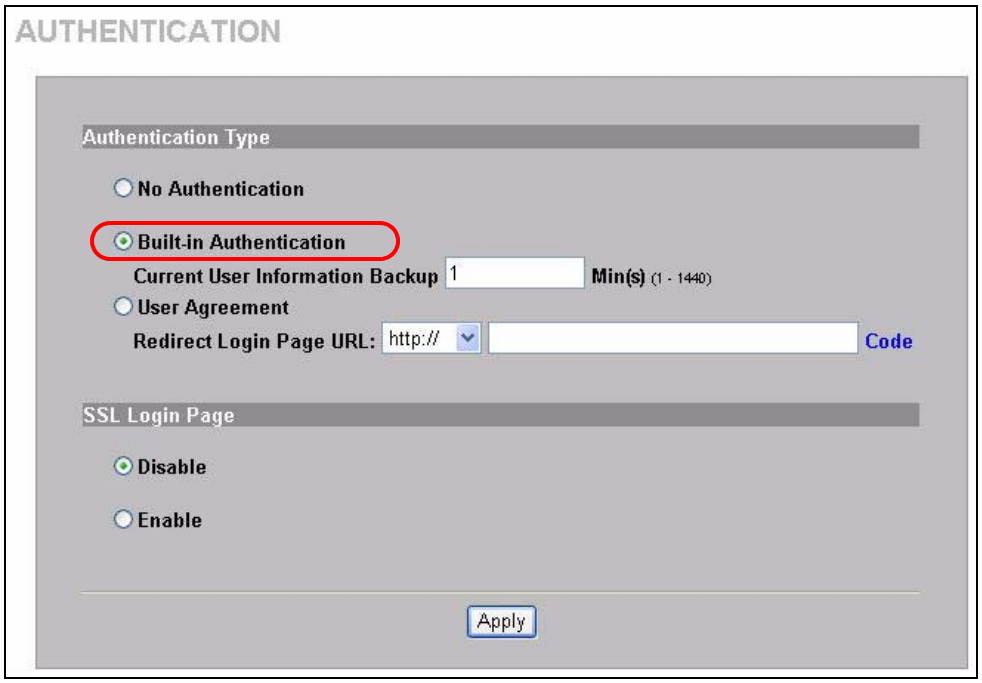
Use the wireless adapter’s utility installed on the notebook to search for the “SSID_Example” SSID. Then enter the “DoNotStealMyWirelessNetwork” pre-shared key to establish an wireless Internet connection.

Note: The N4100 supports IEEE 802.11b, IEEE 802.11g and IEEE 802.11n wireless clients. Make sure that your notebook or computer’s wireless adapter supports one of these standards.

3.3 Subscriber Authentication and Account Generation

There are two ways to automatically create subscriber accounts: using the **Account Generator Panel** screen in the web configurator or using a statement printer. You can also create accounts on an accounting server (RADIUS). See the RADIUS documentation for how to create accounts manually.

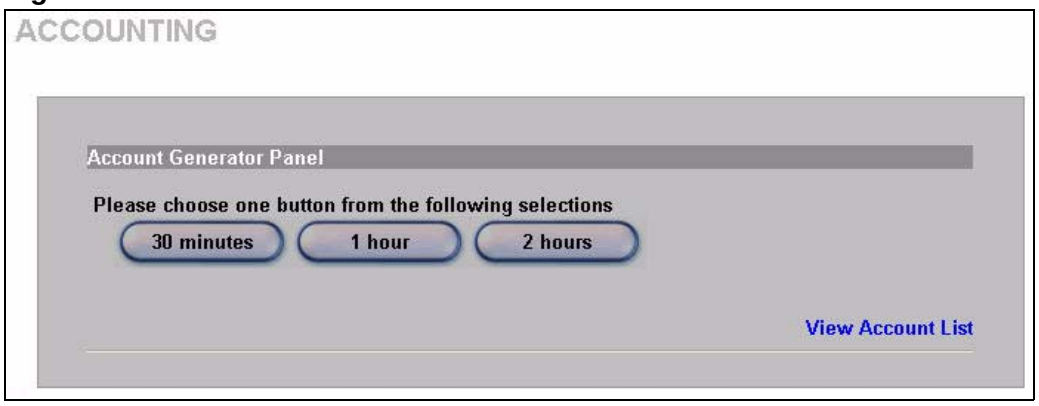
Note: You must set the authentication type to **Built-in Authentication** in the **ADVANCED > AUTHENTICATION** screen before you can create a subscriber account using the local subscriber database.



3.3.1 Creating Accounts in the Web Configurator

To automatically create subscriber accounts, click **Preview/Operate** in the **ADVANCED > ACCOUNTING** screen to display the **Account Generator Panel** screen shown next.

Figure 8 Account Generator Panel



Note: These button settings also apply to the buttons on a statement printer.

Click a button to generate an account based on the settings you configure for the button in the **ADVANCED > ACCOUNTING** screen. A window displays showing a printout preview of the account generated.

The following figure shows an example. Close this window when you are finished viewing it.

Figure 9 Web-based Account Generator Printout Preview Example

Figure 10 Web-based PC-connected Printout Preview Example

3.3.2 Using a Statement Printer to Create Accounts and Print Subscriber Statements

Follow the steps below to setup and create subscriber accounts and print subscriber statements using an external statement printer.

1 Make sure that the printer is connected to the appropriate power and the N4100, and that there is printing paper in the statement printer. Refer to the printer's User's Guide for details.

2 Press the button on the statement printer. The N4100 generates a dynamic account and the printer prints the subscriber's statement. Refer to Figure 9 on page 40 for a printout example.

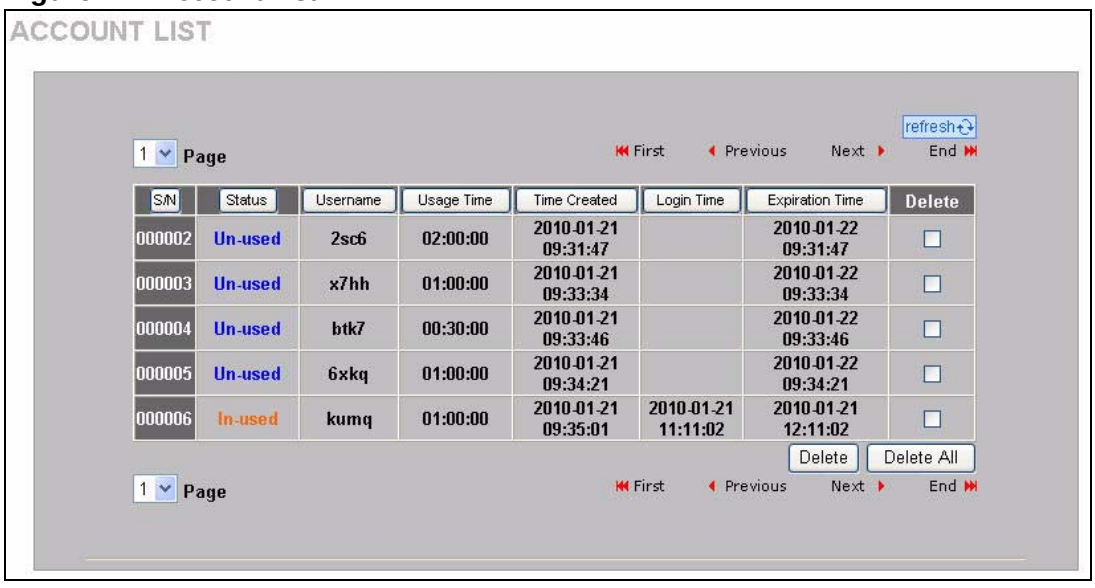
Refer to Chapter 13 on page 119 for how to configure the printout page.

3.3.3 Viewing the Account List

Do one of the following to view the account list.

- From the **Account Generator Panel** screen, (refer to Figure 8 on page 39) click **View Account List**.
- From the **SYSTEM STATUS** sub-menus, click **ACCOUNT LIST**.

Figure 11 Account List



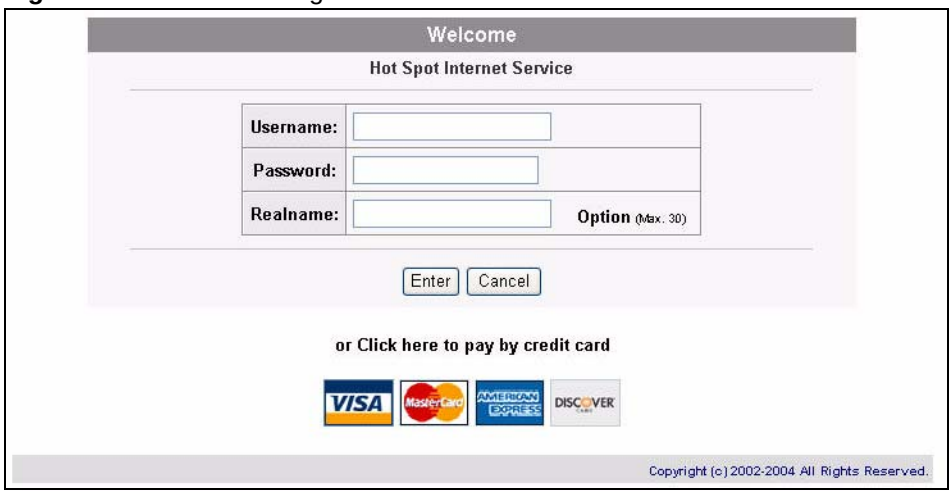
See Section 28.3 on page 216 for explanation of the account list screen. Refer to Section 3.4 on page 42 for more information on logging in as a subscriber.

3.4 Subscriber Login

To log in as a subscriber, enter a web site address such as www.zyxel.com in a web browser.

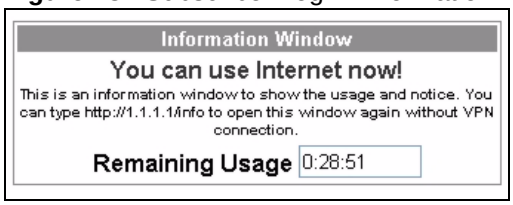
If user authentication is activated, the login screen displays prompting you to enter the user name and password. A standard subscriber login screen (with the credit card function) is shown in the figure below.

Figure 12 Subscriber Login Screen



Enter a user name and password and click Enter. Depending on the settings in the N4100, either the specified web page or an advertisement web page displays. An Information Window screen also displays showing the amount of time remaining on the account for Internet access.

Figure 13 Subscriber Login: Information Window



3.5 Report Printing Using the SP300E

This section shows you how to print reports using the SP300E. See the SP300E User's Guide for details on how to set up the SP300E.

3.5.1 Reports Overview

The SP300E allows you to print status reports about the subscriber accounts and general N4100 system information. Simply press a key combination on the SP300E to print a report instantly without accessing the web configurator.

The following lists the reports that you can print using the SP300E.

- Daily account summary
- Monthly account summary
- System status
- Network statistics

3.5.2 Key Combinations

The following table lists the key combination to print each report.

Note: You must press the key combination on the SP300E within five seconds to print.

Table 4 Report Printing Key Combinations

REPORT TYPE	KEY COMBINATION
Daily Account Summary	A B C A A
Monthly Account Summary	A B C B B
System Status	A B C C C
Network Statistics	A B C A B

The following sections describe each report printout in detail.

3.5.3 Daily Account Summary

The daily account report lists the accounts printed during the current day, the current day's total number of accounts and the total charge. It covers the accounts that have been printed during the current day starting from midnight (not the past 24 hours). For example, if you press the daily account key combination on 2010/1/1 at 20:00:00, the daily account report includes the accounts created on 2010/1/1 between 00:00:01 and 19:59:59.

Key combination: A B C A A

The following figure shows an example. “B” stands for the button that was pressed to generate the account. “UN” stands for the units of Internet access that were purchased.

Figure 14 Daily Account Example

```
          Daily Account
  ---------------------------
            2010/1/1

  S/N   Username  B  UN  Price
  ---------------------------
  000002 p2m6pf52 1  1   1.00
  000003 s4pcms28 1  2   2.00
  ---------------------------
       TOTAL ACCOUNTS: 2
      TOTAL PRICE: $ 3.00
  ---------------------------
       2010/1/1  20:00:11
            ---End---
```

3.5.4 Monthly Account Summary

The monthly account report lists the accounts printed during the current month, the current month’s total number of accounts and the total charge. It covers the accounts that have been printed during the current month starting from midnight of the first day of the current month (not the past one month period). For example, if you press the monthly account key combination on 2010/1/17 at 20:00:00, the monthly account report includes the accounts created from 2010/1/1 at 00:00:01 to 2010/1/17 at 19:59:59.

Key combination: A B C B B

The following figure shows an example. “B” stands for the button that was pressed to generate the account. “UN” stands for the units of Internet access that were purchased.

Figure 15 Monthly Account Example

```
        Monthly Account
----------------------------
          2010/1/1

S/N   Username  B  UN  Price
----------------------------
 000002 p2m6pf52 1  1   1.00
 000003 s4pcms28 1  2   2.00
 000004 7ufm7z22 2  1   2.00
 000005 qm5fxn95 3  2   6.00

----------------------------
      TOTAL ACCOUNTS: 4
    TOTAL PRICE: $ 11.00
----------------------------
     2010/1/17  20:00:11
          ---End---
```

3.5.5 Account Report Notes

The daily or monthly account report holds up to 2000 entries. If there are more than 2000 accounts created in the same month or same day, the account report’s calculations only include the latest 2000.

For example, if 2030 accounts (each priced at $1) have been created from 2010/1/1 00:00:00 to 2010/1/31 19:59:59, the monthly account report includes the latest 2000 accounts, so the total would be $2,000 instead of $2,030.

Use the **SYSTEM STATUS > ACCOUNT LOG** screen to see the accounts generated on another day or month (up to 2000 entries total).

3.5.6 System Status

This report shows the current system information such as the host name and WAN IP address.

Key combination: A B C C C

The following figure shows an example.

Figure 16 System Status Example

```
        System Status
---------------------------
      ITEM DESCRIPTION
---------------------------
      WAST ESTABLISHED
        WSTA Success
    SYST 02D:02H:42M:46S
---------------------------
        HOST MyDevice
     FRMW v1.00(ZB.2)CO
            WFRM
          BTRM 1.01
             LOCA
   WAMA 00-90-0E-00-4A-29
   LAMA 00-90-0E-00-4A-28
          WATP DHCP
       WAIP 172.21.2.67
       WASM 255.255.0.0
      WAGW 172.21.0.254
       PDNS 172.20.0.63
       SDNS 172.20.0.27
       DHCP DHCP SERVER
        DHSP 10.59.1.2
       DHEP 10.59.1.254
          DHLT 1440
        EMAIL /PORT25
---------------------------
     2010/1/28 11:24:42
          ---End---
```

The following table describes the labels in this report.

Table 5 System Status

LABEL	DESCRIPTION
WAST	This field displays the WAN connection status.
WSTA	This field displays the status of the N4100's wireless LAN.
SYST	This field displays the time since the system was last restarted.
HOST	This field displays the description name of the N4100 for identification purposes.
FRMW	This field displays the version of the firmware on the N4100.
WFRM	This field displays the version of the (internal) wireless adapter firmware on the N4100.
BTRM	This field displays the version of the bootrom.
WAMA	This field displays the MAC address of the N4100 on the WAN.
LAMA	This field displays the MAC address of the N4100 on the LAN.

Table 5 System Status (continued)

LABEL	DESCRIPTION
WATP	This field displays the mode of the WAN port.
WAIP	This field displays the IP address of the WAN port on the N4100.
WASM	This field displays the subnet mask of the WAN port on the N4100.
WAGW	This field displays the IP address of the default gateway of the WAN port on the N4100.
PDNS	This field displays the IP address of the primary DNS server.
SDNS	This field displays the IP address of the secondary DNS server.
DHCP	This field displays the DHCP mode (**DHCP Server**, **Relay** or **DHCP Disable**) on the LAN.
DHSP	If the **DHCP** field is **DHCP Server**, this field displays the first of the continuous addresses in the IP address pool. If the **DHCP** field is **DHCP Relay**, this field displays the DHCP server IP address.
DHEP	This field is visible when the **DHCP** is **DHCP Server**. This field displays the end of the continuous addresses in the IP address pool.
DHLT	This field is visible when the **DHCP** is **DHCP Server**. This field displays the time (in minutes) a DHCP client is allowed to use an assigned IP address.
EMAIL	The field displays e-mail server port number.
SSID	This field displays the N4100's Extended Service Set IDentity.
WCHA	This field displays the channel that the N4100 is using.
WSEC	This field displays whether the N4100's wireless security is turned on or off.

3.5.7 Network Statistics

This report shows the network statistics on the N4100.

Key combination: A B C A B

The following figure shows an example.

Figure 17 Network Statistics Example

```
          Network
----------------------------
      ITEM DESCRIPTION
----------------------------
      WAST ESTABLISHED
        WSTA Success
    SYST 02D:02H:42M:46S
----------------------------
          WATD 37
         WARD 4816
          WATE 0
          WARE 0
         LATD 1768
         LARD 4616
          LATE 0
          LARE 0
----------------------------
     2010/1/28 15:24:42
         ---End---
```

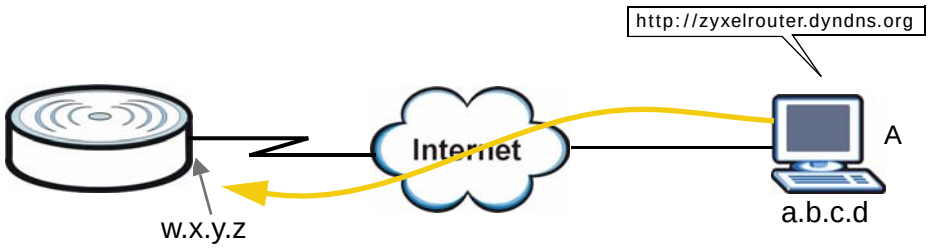
The following table describes the labels in this report.

Table 6 Network Statistics

LABEL	DESCRIPTION
WAST	This field displays the WAN connection status.
WSTA	This field displays the wireless LAN status.
SYST	This field displays the time since the system was last restarted.
WATD	This field displays the number of packets transmitted on the WAN.
WARD	This field displays the number of packets received on the WAN.
WATE	This field displays the number of error packets transmitted on the WAN.
WARE	This field displays the number of error packets received on the WAN.
LATD	This field displays the number of packets transmitted on the LAN.
LARD	This field displays the number of packets received on the LAN.
LATE	This field displays the number of error packets transmitted on the LAN.
LARE	This field displays the number of error packets received on the LAN.

3.6 Using DDNS to access the N4100

If you connect your N4100 to the Internet and it uses a dynamic WAN IP address, it is inconvenient for you to manage the device from the Internet. The N4100's WAN IP address changes dynamically. Dynamic DNS (DDNS) allows you to access the N4100 using a domain name.



To use this feature, you have to apply for DDNS service at www.dyndns.org.

This tutorial shows you how to:

- Registering a DDNS Account on www.dyndns.org
- Configuring DDNS on Your N4100
- Testing the DDNS Setting

Note: If you have a private WAN IP address, then you cannot use DDNS.

3.6.1 Registering a DDNS Account on www.dyndns.org

1. Open a browser and type **http://www.dyndns.org**.
2. Apply for a user account. This tutorial uses **UserName1** and **12345** as the username and password.
3. Log into www.dyndns.org using your account.
4. Add a new DDNS host name. This tutorial uses the following settings as an example.
   - Hostname: **zyxelrouter.dyndns.org**
   - Service Type: **Host with IP address**
   - IP Address: Enter the WAN IP address that your N4100 is currently using. You can find the IP address on the N4100's Web Configurator **Status** page.

   Then you will need to configure the same account and host name on the N4100 later.

3.6.2 Configuring DDNS on Your N4100

1 Log into the N4100's web configurator.

2 Configure the following settings in the **ADVANCED > DDNS** screen.

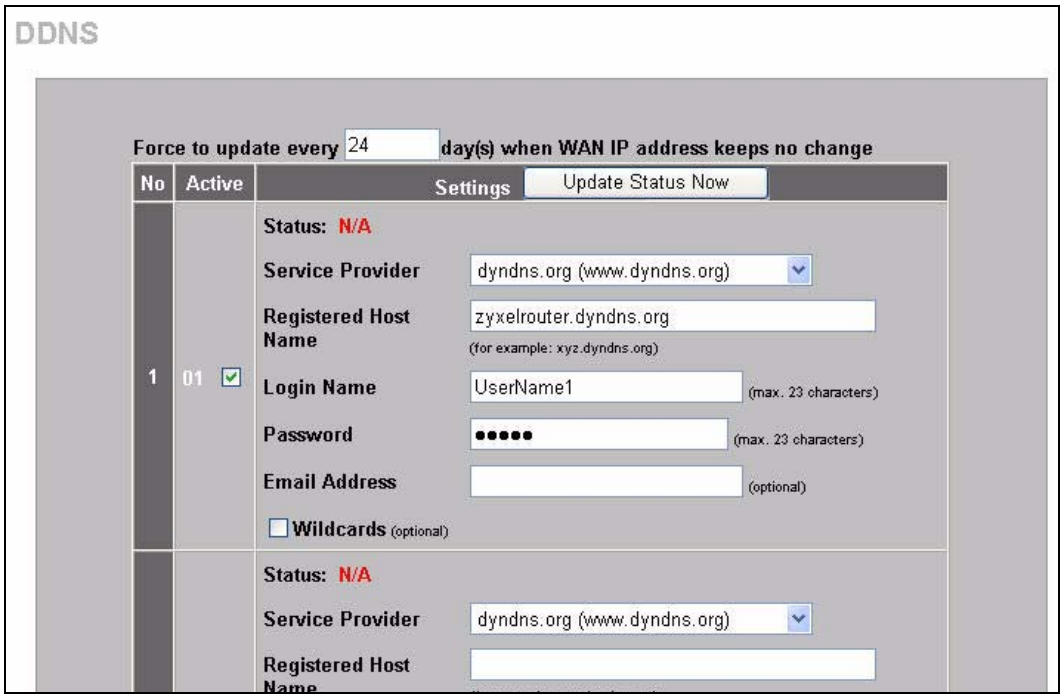
2a Select the **Active** check box of the first entry.

2b Select **dyndns.org** as the service provider name.

2c Type **zyxelrouter.dyndns.org** in the **Host Name** field.

2d Enter the user name (**UserName1** for example) and password (**12345** for example).

2e Click **Apply**.



3.6.3 Testing the DDNS Setting

Now you should be able to access the N4100 from the Internet. To test this:

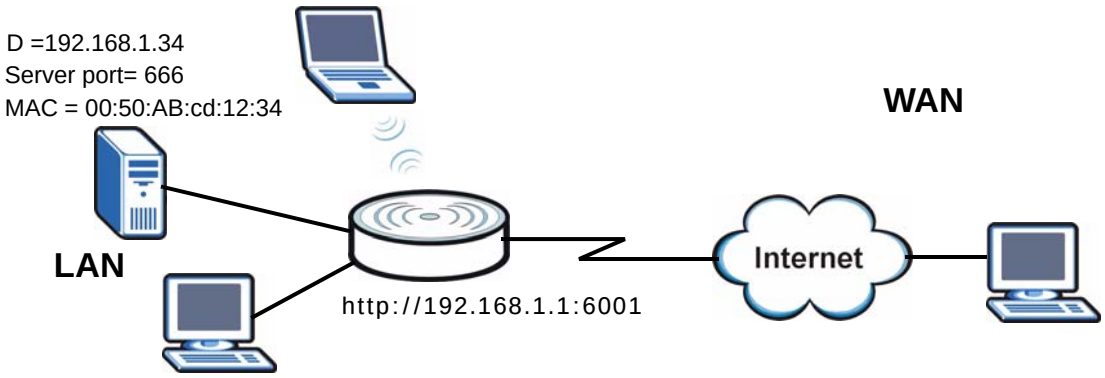
1 Open a web browser on the computer (using the IP address **a.b.c.d**) that is connected to the Internet.

2 Type **http://zyxelrouter.dyndns.org** and press [Enter].

3 The N4100's login page should appear. You can then log into the N4100 and manage it.

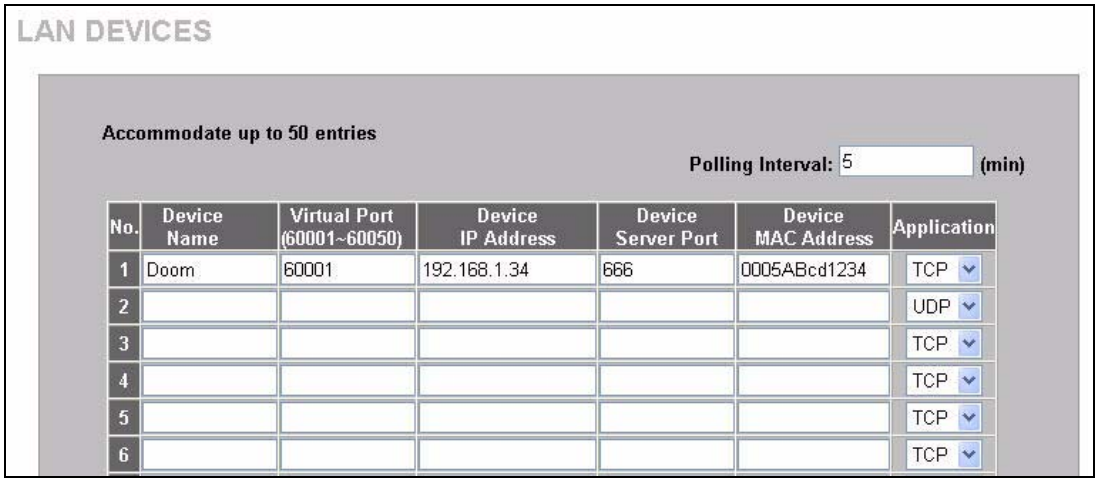
3.7 Accessing the Devices on the LAN from the WAN

Thomas manages a Doom server on a computer behind the N4100. In order for players on the Internet to communicate with the Doom server, Thomas needs to configure the port settings and IP address on the N4100. Traffic should be forwarded to server port 666 of the Doom server computer which has an IP address of 192.168.1.34.

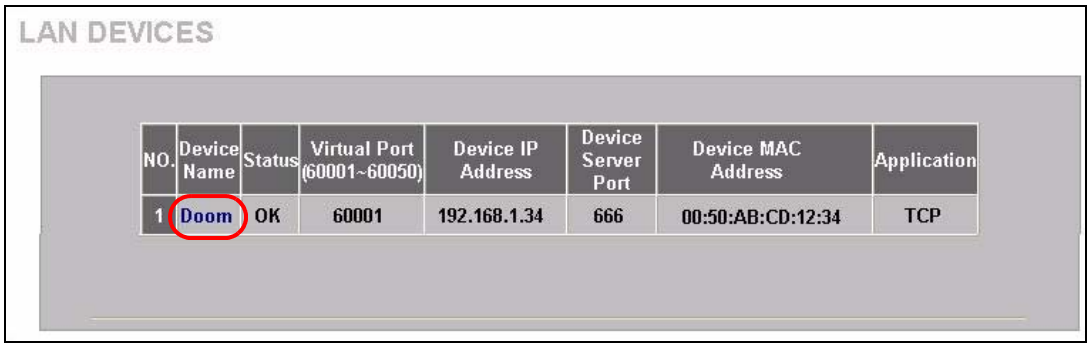


1 Click **ADVANCED > LAN DEVICES** to open the **LAN Devices** screen.

2 Configure the screen as follows and click **Apply**. Port 666 traffic will be forwarded to the computer with IP address 192.168.1.34 and MAC address 00:50:AB:cd:12:34. Virtual port 60001 on the N4100 is mapped to server port 666 on the computer.



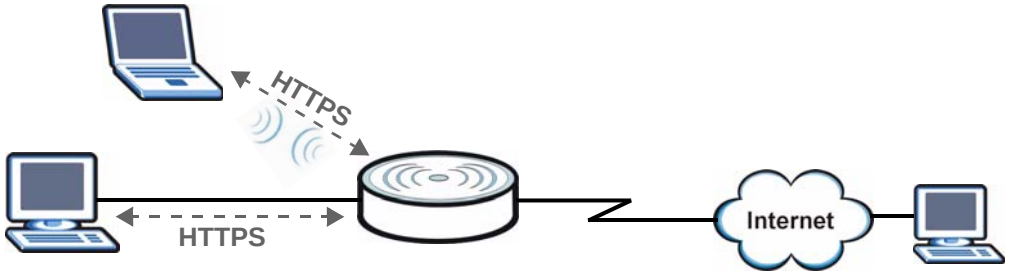
3 Players on the Internet then can have access to Thomas' Doom server.
You can also remotely access the Doom server's web-based management interface by entering http://192.168.1.1:60001 or clicking the device name in the **SYSTEM STATUS > LAN DEVICES** screen.



4 If you want to manage the Doom server using the N4100's dynamic domain name and the virtual port, http://www.domainname.com:60001 for example, see Section 3.6 on page 49 for how to configure the N4100's DDNS settings.

3.8 Using SSL Security for Connections between the N4100 and your Computer

When you connect to N4100 for management or Internet access, you can use SSL to protect data transfer between the N4100 and the web browser on your computer.

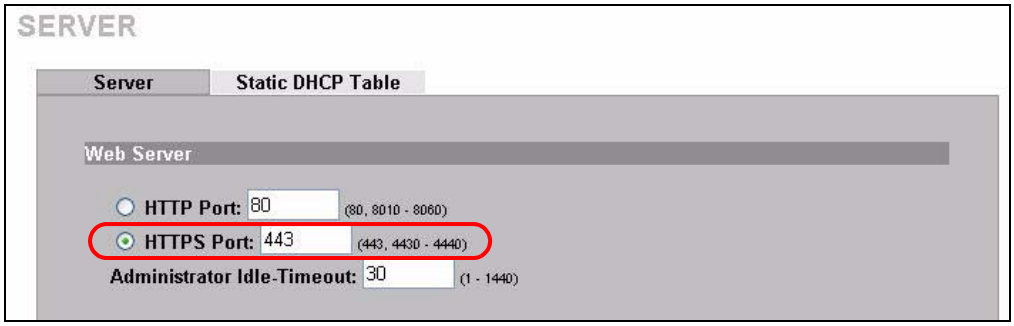


3.8.1 Activating SSL Security for Management Connections

Follow the steps below to activate the SSL security for management connections to the web configurator on the N4100.

1 Click **ADVANCED** > **SERVER**. Select **HTTPS** under **Web Server**.

Figure 18 ADVANCED > SERVER: Enable SSL (HTTPS) Security



2 Click **Apply** to save the changes and restart the N4100 when prompted. See Section 3.8.2 on page 53 for details on how to install the SSL security certificate in order to access the web configurator through a secure connection.

3.8.2 Viewing and Installing the SSL Security Certificate

After you enable and activate the SSL security on the N4100, you can access the web configurator through a secure connection.

Follow the steps below to view and install the default SSL security certificate on your computer.

1 Access the N4100. A **Security Alert** window displays.

Figure 19 Installing the SSL Security Certificate: Security Alert

2 Click **View Certificate** to display the **Certificate** window as shown.

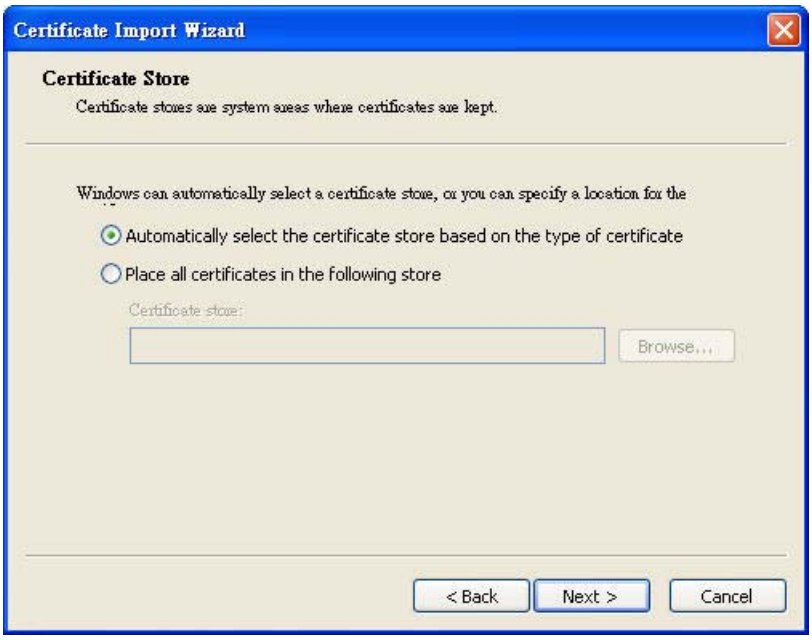
Figure 20 Installing the SSL Security Certificate: View Certificate

3 Click **Install Certificate** to install the certificate to your computer. A **Certificate Import Wizard** window displays. Click **Next**.

Figure 21 Installing the SSL Security Certificate: Certificate Import Wizard

4 Accept the default or specify the location to store the certificate. Click **Next**.

Figure 22 Certificate Import Wizard: Location

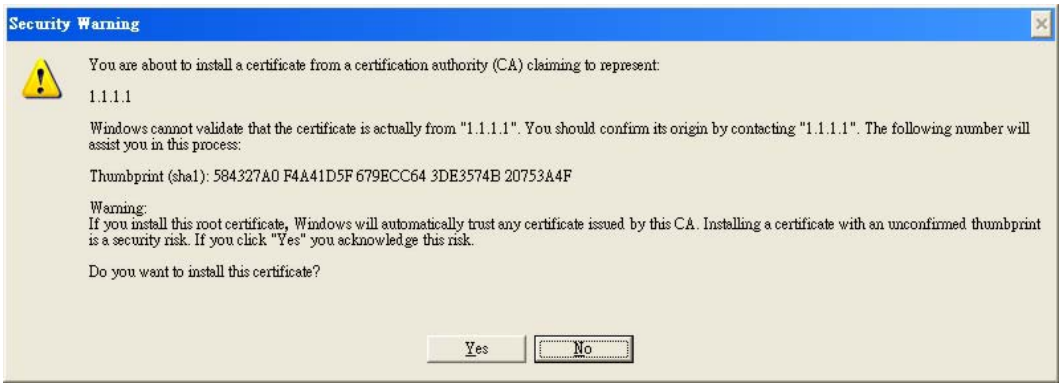


5 Click **Finish** to import the certificate.

Figure 23 Certificate Import Wizard: Finish

6 A **Security Warning** window displays as shown. Click **Yes** to store the certificate to the computer.

Figure 24 Security Warning

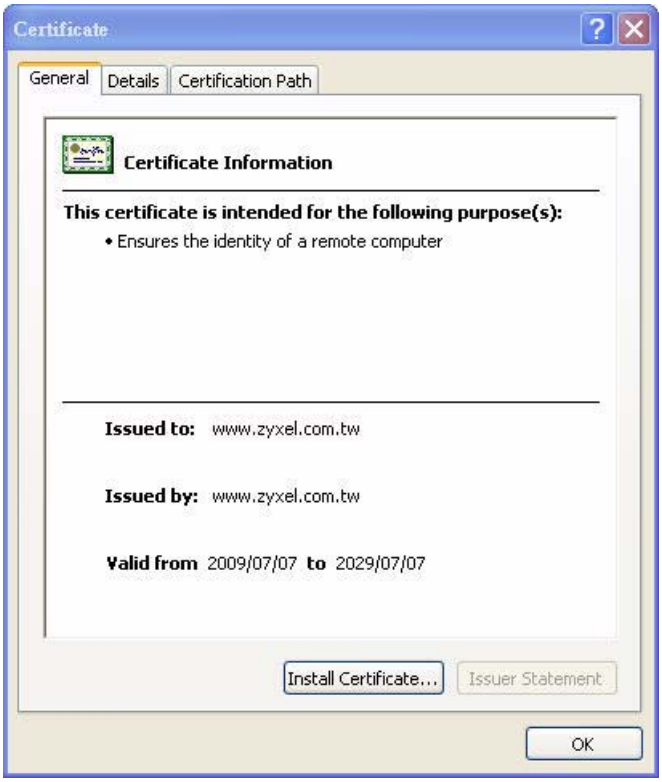


7 When the certificate is saved successfully, a **Certificate Import Wizard** window displays. Click **OK**.

Figure 25 Certificate Import Wizard

8 A **Certificate** window displays details.

Figure 26 Certificate Details



9 Click **OK** in the **Certificate** window to return to the **Security Alert** window as shown. Notice that the first item in the list changed to inform you that the certificate is from a trusted host. Click **Yes** to proceed to the login screen in secure mode.

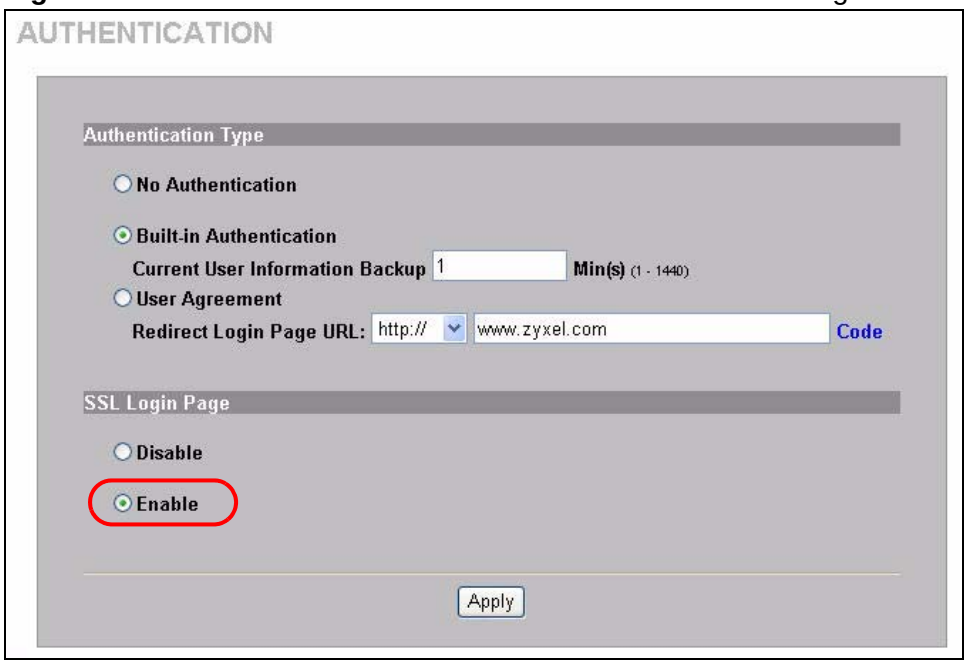
Figure 27 Security Alert: Trusted

3.8.3 Activating SSL Security for Subscriber Logins

Follow the steps below to activate the SSL security for subscriber login connections to the N4100. When a user accesses the subscriber login screen, the user name and password are protected before being sent to the N4100.

1 Click **ADVANCED > AUTHENTICATION** and select the **Enable** in the **SSL Login Page** field

Figure 28 ADVANCED > AUTHENTICATION: Activate SSL Login



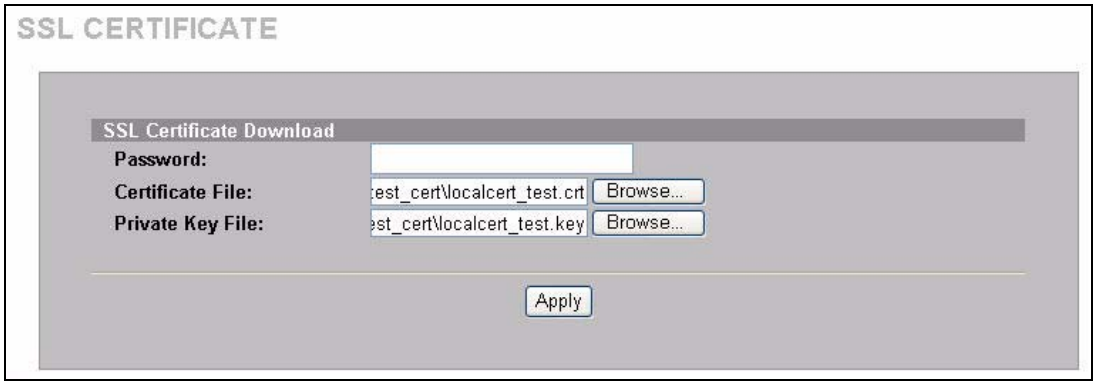
2 Click **Apply** to save the changes.

3.8.4 Using a New Certificate for SSL Security

If you don't want to use the default SSL security certificate generated by the system, you can save a CA-registered certificate and the private key on your computer and then download them to the N4100.

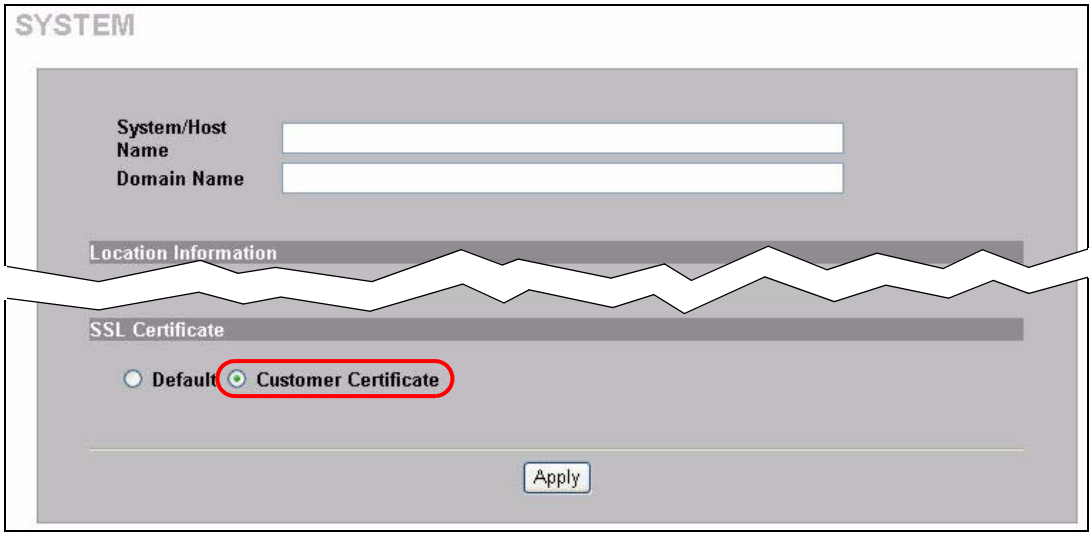
1 Click **SYSTEM TOOLS > SSL CERTIFICATE**.

2 Locate the certificate and private key files on your computer and click **Apply** to transfer the files to the N4100.



3 Click **Advanced > SYSTEM**.

4 Select **Customer Certificate** under **SSL Certificate** to have the N4100 use the certificate you downloaded for secure connections. Click **Apply**.



PART II
Technical Reference

4

System Setup

4.1 Overview

This chapter describes the **System** setup screen.

4.1.1 What You Can Do in this Chapter

Use the **System** screen (Section 4.2 on page 64) to configure administrative and system-related general settings for your N4100. You can also use this screen to change your N4100's time and date based on your local time zone.

4.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

System Name

The System Name is for identification purposes. However, because some ISPs check this name you should enter your computer's "Computer Name". Find the system name of your Windows computer by following one of the steps below.

- In Windows 2000, click **Start** > **Settings** > **Control Panel** and then double-click **System**. Click the **Network Identification** tab and then the **Properties** button. Note the entry for the **Computer name** field and enter it as the **System Name**.
- In Windows XP, click **Start** > **My Computer** > **View system information** and then click the **Computer Name** tab. Note the entry in the **Full computer name** field and enter it as the N4100 **System Name**.

Domain Name

This is a network address that identifies the owner of a network connection. For example, in the network address “www.zyxel.com/support/files”, the domain name is “www.zyxel.com”.

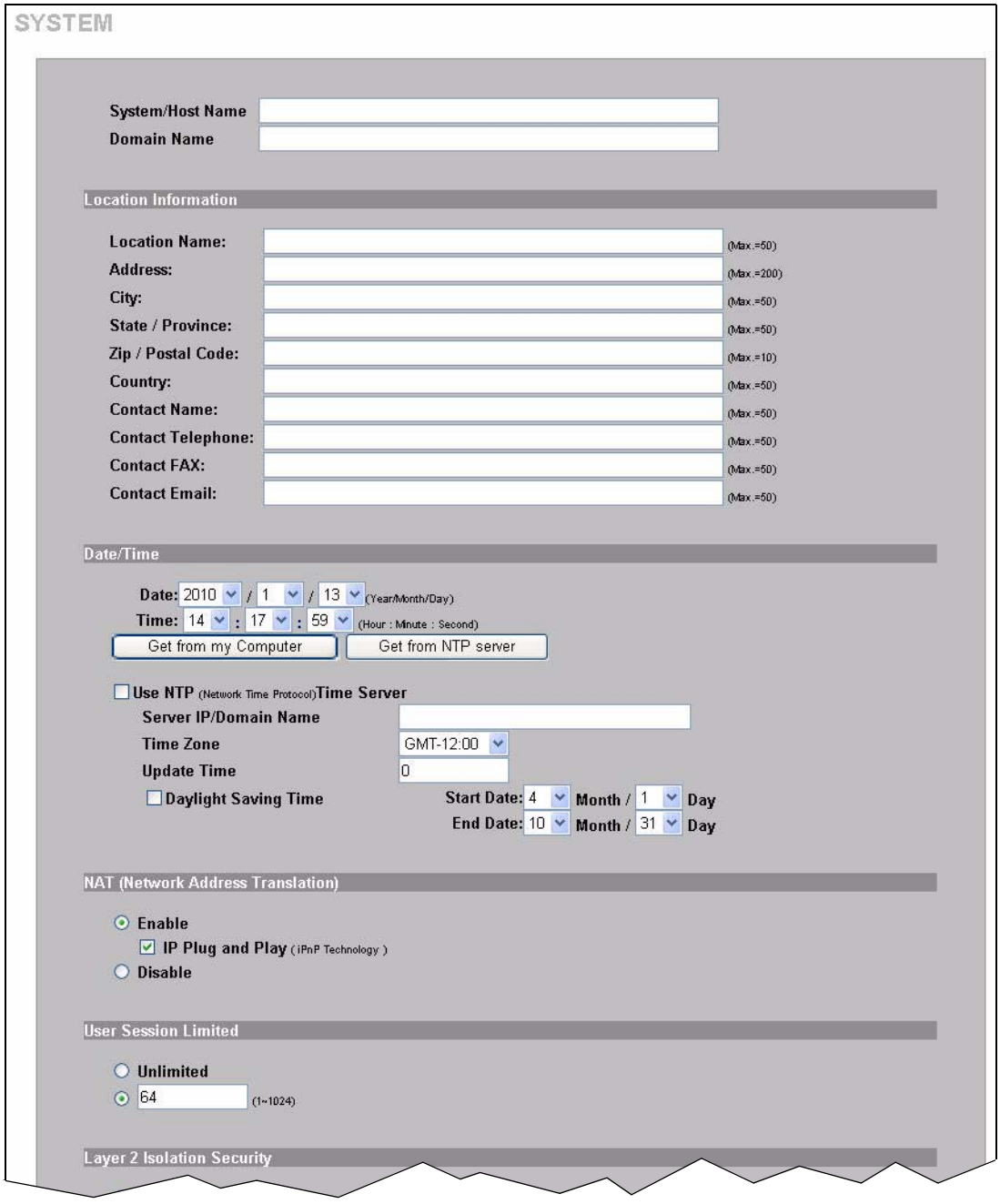
The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by a DHCP server is used. While

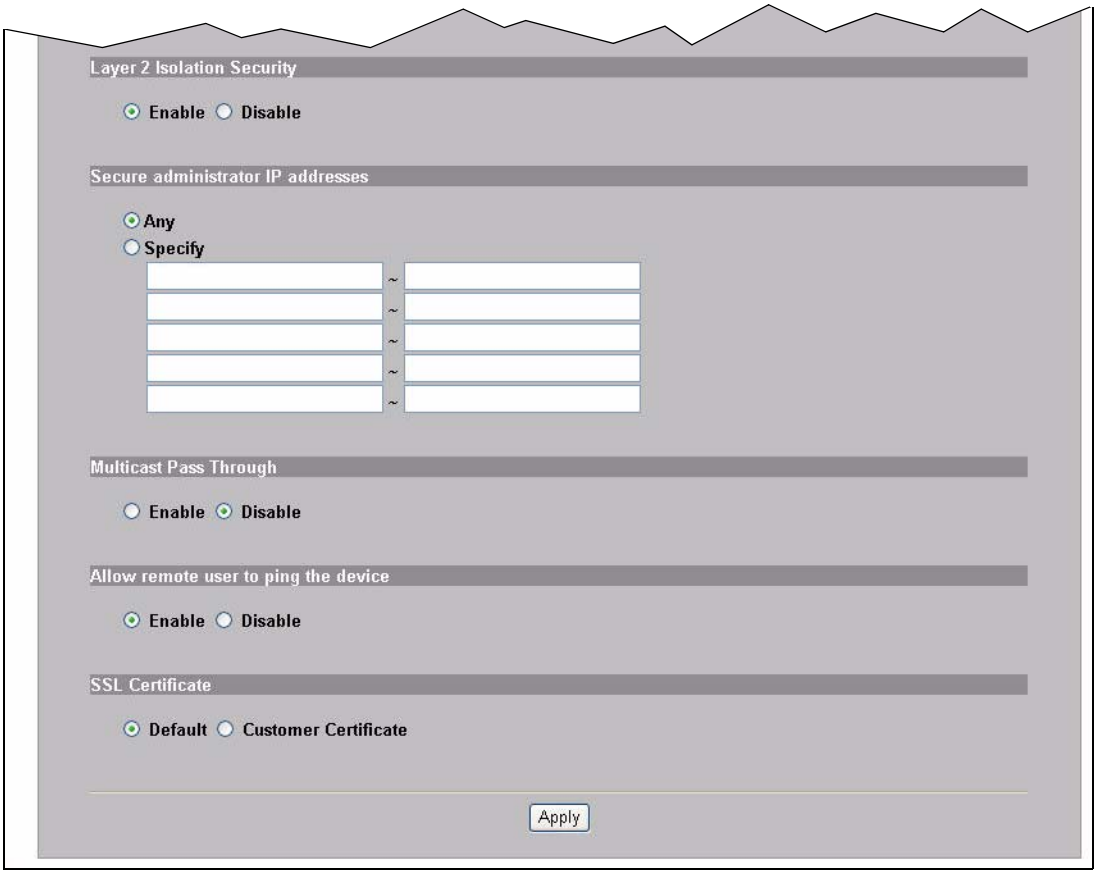
you must enter the host name (System Name), the domain name can be assigned from the N4100 via DHCP.

4.2 The System Screen

Click **ADVANCED > SYSTEM** to open this screen.

Figure 29 ADVANCED > SYSTEM





The following table describes the labels in this screen.

Table 7 ADVANCED > SYSTEM

LABEL	DESCRIPTION
System/Host Name	Enter a descriptive name for identification purposes. It is recommended you enter your computer's "Computer name" in this field. This name can be up to 50 alphanumeric characters long. Spaces, dashes "-" and underscores "_" are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the N4100 may obtain a domain name from a DHCP server. The domain name entered by you is given priority over the DHCP server assigned domain name.
Location Information	
Location Name	Enter the device's geographical location.
Address	Enter the street address of the device's location.
City	Enter the city of the device's location.
State/Province	Enter the state or province of the device's location.
ZIP/ Postal Code	Enter the zip code or postal code for the device's location.

Table 7 ADVANCED > SYSTEM (continued)

LABEL	DESCRIPTION
Country	Enter the country of the device's location.
Contact Name	Enter the name of the person responsible for this device.
Contact Telephone	Enter the telephone number of the person responsible for this device.
Contact FAX	Enter the fax number of the person responsible for this device.
Contact Email	Enter the e-mail address of the person responsible for this device.
Date/Time	Set the system date and time by selecting the appropriate choices from the drop-down list boxes.
Get from my Computer	Click this button to set the time and date on the N4100 to be the same as the management computer.
Get from NTP server	Click this button to set the N4100 to get time and date information from a specified NTP (Network Time Protocol) time server.
Use NTP (Network Time Protocol) Time Server	Select this check box to allow the N4100 to get time and date information from an NTP (Network Time Protocol) time server.
Server IP/ Domain Name	Enter the IP address or URL of your time server. Check with your ISP/ network administrator if you are unsure of this information.
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Update Time	Enter a number to determine how often the N4100 uses the NTP server to update the time and date.
Daylight Saving Time	Select this option if you use daylight savings time. Daylight saving is a period from late spring to fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
Start Date	Select the month and day that your daylight-savings time starts on if you selected **Daylight Saving Time**.
End Date	Select the month and day that your daylight-savings time ends on if you selected **Daylight Saving Time**.
NAT (Network Address Translation)	Enable NAT to have the N4100 translate Internet protocol addresses used within one network (for example a private IP address used in a local network) to a different IP address known within another network (for example a public IP address used on the Internet). See Chapter 19 on page 163 for more on NAT.
IP Plug and Play (iPnP Technology)	Select this option to activate the iPnP feature. This allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, even when the IP addresses of the computer and the N4100 are not in the same subnet. When you disable the iPnP feature, only computers with dynamic IP addresses or static IP addresses in the same subnet as the N4100's LAN IP address can connect to the N4100 or access the Internet through the N4100.

Table 7 ADVANCED > SYSTEM (continued)

LABEL	DESCRIPTION
User Session Limited	Select **Unlimited** to not place any restriction on the number of sessions that each user connected to the N4100 can use. Select the other radio button and type a number (from 1 to 1024) if you want to specify how many sessions each user connected to the N4100 can use.
Layer 2 Isolation Security	If you activate NAT, select **Enable** in this field to prevent communication between subscribers. This is the default selection. Select **Disable**, to deactivate layer 2 security and allow communication between subscribers.
Secure administrator IP addresses	Select **Any** to use any computer to access the web configurator on the N4100. Select **Specify** and then enter the IP address(es) or ranges of IP addresses of the computer(s) that are allowed to log in to configure the N4100. The addresses can be on the LAN or the WAN.
Multicast Pass Through	Select **Enable** to allow multicast traffic to pass through the N4100. This may affect your network performance. Select **Disable** to prevent any multicast traffic from passing through the N4100. This is the default setting.
Allow remote user to ping the device	This feature affects the security of the N4100's WAN port. Ping (Packet INternet Groper) is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. Select **Enable** to have the N4100 respond to incoming Ping requests from the WAN. This is less secure since someone on the Internet can see that the N4100 is there by pinging it. Select **Disable** to have the N4100 not respond to incoming Ping requests from the WAN. This is more secure since someone on the Internet cannot see that the N4100 is there by pinging it.
SSL Certificate	Secure Socket Layer (SSL) security allows you to create secure connections between the N4100 and the management or subscriber computer(s). Select **Default** to use the default system-generated SSL certificate. Select **Customer Certificate** to use a certificate obtained from a certificate authority. Refer to Chapter 31 on page 243 for more information.
Apply	Click **Apply** to save your changes back to the N4100.

4.3 Technical Reference

The following section contains additional technical information about the N4100 features described in this chapter.

4.3.1 iPnP ZyXEL Implementation

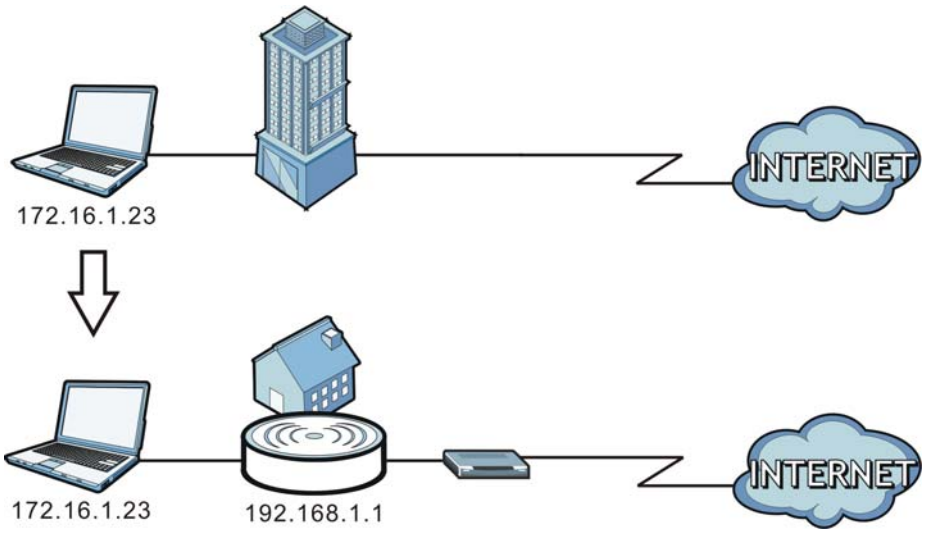
Traditionally, you must set the IP addresses and the subnet masks of a computer and the N4100 to be in the same subnet to allow the computer to access the Internet (through the N4100). In cases where your computer is required to use a static IP address in another network, you may need to manually configure the network settings of the computer every time you want to access the Internet via the N4100.

With the iPnP feature and NAT enabled, the N4100 allows a computer to access the Internet without changing the network settings (such as IP address and subnet mask) of the computer, when the IP addresses of the computer and the N4100 are not in the same subnet.

Whether a computer is set to use a dynamic or static (fixed) IP address, you can simply connect the computer to the N4100 and access the Internet.

The following figure depicts a scenario where a computer is set to use a static private IP address in the corporate environment. In a residential house where a N4100 is installed, you can still use the computer to access the Internet without changing the network settings, even when the IP addresses of the computer and the N4100 are not in the same subnet.

Figure 30 iPnP Example



The iPnP feature does not apply to a computer using either a dynamic IP address or a static IP address that is in the same subnet as the N4100's IP address.

Note: You *must* enable NAT to use the iPnP feature.

4.3.2 How iPnP Works

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network. IP routing table is defined on IP Ethernet devices (the N4100) to decide which hop to use, to help forward data along to its specified destination.

The following lists out the steps taken, when a computer tries to access the Internet for the first time through the N4100.

1 When a computer (which is in a different subnet) first attempts to access the Internet, it sends packets to its default gateway (which is not the N4100) by looking at the MAC address in its ARP table.

2 When the computer cannot locate the default gateway, an ARP request is broadcast on the LAN.

3 The N4100 receives the ARP request and replies to the computer with its own MAC address.

4 The computer updates the MAC address for the default gateway to the ARP table. Once the ARP table is updated, the computer is able to access the Internet through the N4100.

5 When the N4100 receives packets from the computer, it creates an entry in the IP routing table so it can properly forward packets intended for the computer.

After all the routing information is updated, the computer can access the N4100 and the Internet as if it is in the same subnet as the N4100.

5

WAN/LAN

5.1 Overview

A Local Area Network (LAN) is a shared communication system to which many computers are attached. A LAN is a computer network limited to the immediate area, usually the same building or floor of a building.

A WAN (Wide Area Network) is an outside connection to another network or the Internet. It connects your private networks, such as a LAN, and other networks, so that a computer in one location can communicate with computers in other locations.

5.1.1 What You Can Do in this Chapter

Use the **WAN / LAN** screen (Section 5.2 on page 73) to set the LAN IP address and subnet mask of your N4100, and configure the WAN settings on the N4100 for Internet access.

5.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

IP Address

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number. This is known as an Internet Protocol address.

Subnet Mask

The subnet mask specifies the network number portion of an IP address. Your N4100 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the N4100 unless you are instructed to do otherwise.

DHCP

DHCP (Dynamic Host Configuration Protocol) allows clients to obtain TCP/IP configuration at start-up from a server.

DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

There are two ways that an ISP disseminates the DNS server addresses.

- The ISP tells you the DNS server addresses, usually in the form of an information sheet, when you sign up. If your ISP gives you DNS server addresses, enter them in the **DNS Server** fields.
- Some ISPs choose to disseminate the DNS server addresses using the DNS server extensions of IPCP (IP Control Protocol) after the connection is up. If your ISP did not give you explicit DNS servers, chances are the DNS servers are conveyed through IPCP negotiation.

Encapsulation Method

Encapsulation is used to include data from an upper layer protocol into a lower layer protocol. To set up a WAN connection to the Internet, you need to use the same encapsulation method used by your ISP (Internet Service Provider). If your ISP offers a dial-up Internet connection using PPPoE (PPP over Ethernet) or PPTP (Point-to-Point Tunneling Protocol), they should also provide a username and password (and service name) for user authentication.

WAN IP Address

The WAN IP address is an IP address for the N4100, which makes it accessible from an outside network. It is used by the N4100 to communicate with other devices in other networks. It can be static (fixed) or dynamically assigned by the ISP each time the N4100 tries to access the Internet.

If your ISP assigns you a static WAN IP address, they should also assign you the subnet mask and DNS server IP address(es) (and a PPTP server IP address if you use the PPTP encapsulation method).

Maximum Transmission Unit

A maximum transmission unit (MTU) is the largest size packet or frame, specified in octets (eight-bit bytes) that can be sent in a packet- or frame-based network. The Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission. Too large an MTU size may mean

retransmissions if the packet encounters a router that can't handle that large a packet. Too small an MTU size means relatively more header overhead and more acknowledgements that have to be sent and handled.

Maximum Segment Size

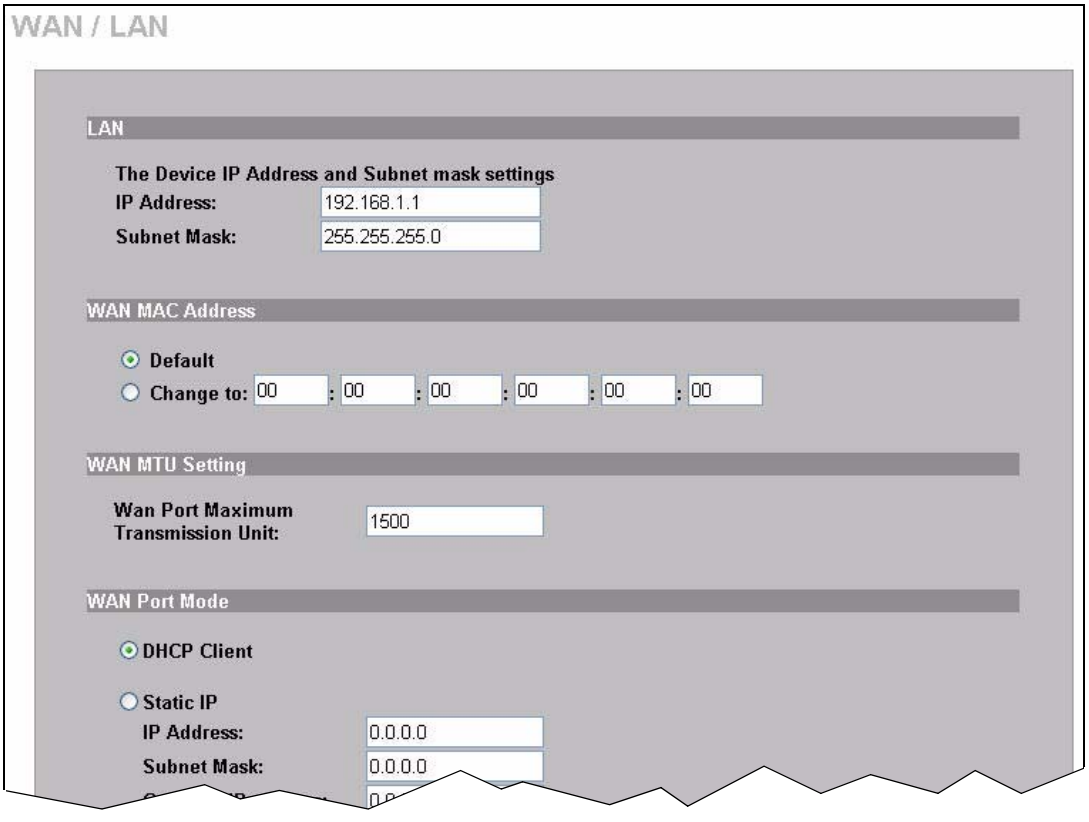
The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU).

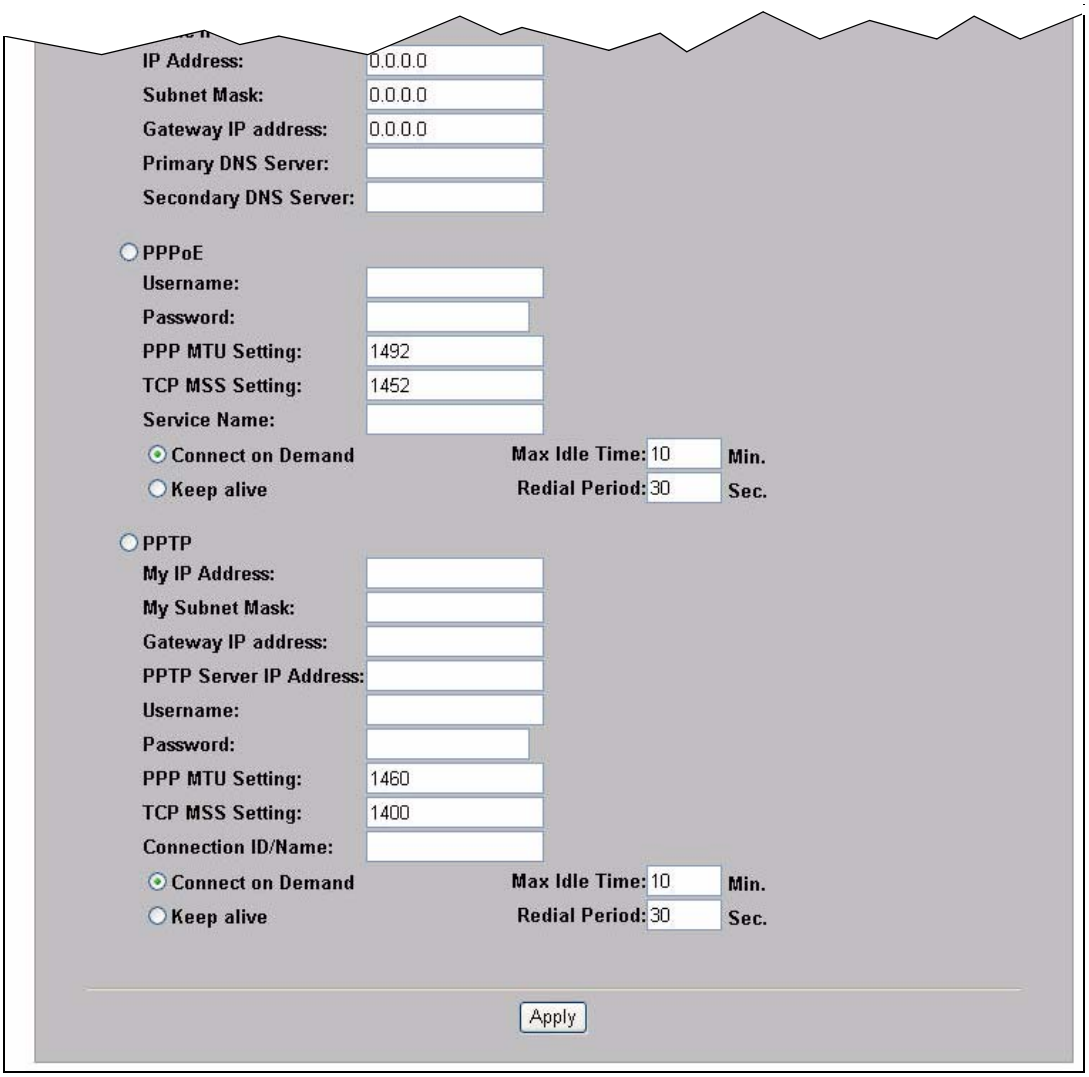
5.2 The WAN/LAN Screen

The N4100's LAN IP address is 192.168.1.1 with subnet mask of 255.255.255.0. The DHCP server is enabled on the LAN with a 253 client IP address pool starting from 192.168.1.2. You can change the DHCP settings in the **Server** screen.

Use this screen to configure the WAN and LAN settings on the N4100. Click **ADVANCED > WAN/LAN** to open this screen.

Figure 31 ADVANCED > WAN/LAN





The following table describes the labels in this screen.

Table 8 ADVANCED > WAN/LAN

LABEL	DESCRIPTION
LAN	
IP Address	Enter the LAN IP address of the N4100 in dotted decimal notation. The default is **192.168.1.1**.
Subnet Mask	Enter the LAN subnet mask in dotted decimal notation. The default is **255.255.255.0**.
WAN MAC Address	Select **Default** to use the factory assigned MAC address. If your ISP requires MAC address authentication, select **Change to** and enter the MAC address of a computer on the LAN in the fields provided.
WAN MTU Setting	

Table 8 ADVANCED > WAN/LAN

LABEL	DESCRIPTION
Wan Port Maximum Transmission Unit	Enter the MTU (Maximum Transfer Unit) size for the WAN interface when you select **DHCP Client** or **Static IP**.
WAN Port Mode	
DHCP Client	Select this option to set the N4100 to act as a DHCP client on the WAN. The N4100 obtains TCP/IP information (IP address, DNS server information, etc.) from a DHCP server. This is the default setting.
Static IP	Select this option to set the N4100 to use a static (or fixed) IP address.
IP Address	Enter the static IP address in dotted decimal notation.
Subnet Mask	Enter the subnet mask in dotted decimal notation.
Gateway IP address	Enter the IP address of the default gateway device. The gateway is a router or switch on the same network segment as the N4100. The gateway helps forward packets to their destinations. Leave this field as **0.0.0.0** if you do not know it.
Primary/ Secondary DNS Server	Enter the IP addresses of the primary and/or secondary DNS servers.
PPPoE	Select this option to activate **PPPoE** support. Refer to Section 5.3 on page 76 for more information.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size for PPPoE traffic.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Service Name	Enter the name of your PPPoE service.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the N4100 will attempt to bring up the connection after the redial period.
PPTP	Select this option to activate **PPTP** support. Refer to Section 5.3 on page 76 for more information.
My IP Address	Enter the IP address assigned to you.
My Subnet Mask	Enter the subnet mask assigned to you.
Gateway IP address	Enter the IP address of the gateway device.

Table 8 ADVANCED > WAN/LAN

LABEL	DESCRIPTION
PPTP Server IP Address	Enter the IP address of your ISP's PPTP server.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the MTU (Maximum Transfer Unit) size for PPTP traffic.
TCP MSS Setting	Enter the MSS (Maximum Segment Size) size.
Connection ID/Name	Enter your identification name of the PPTP server assigned to you by the ISP.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the **Max Idle Time** field. This is the default setting with an idle timeout of **10** minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the **Redial Period** field. When disconnected, the N4100 will attempt to bring up the connection after the redial period.
Apply	Click **Apply** to save your changes back to the N4100.

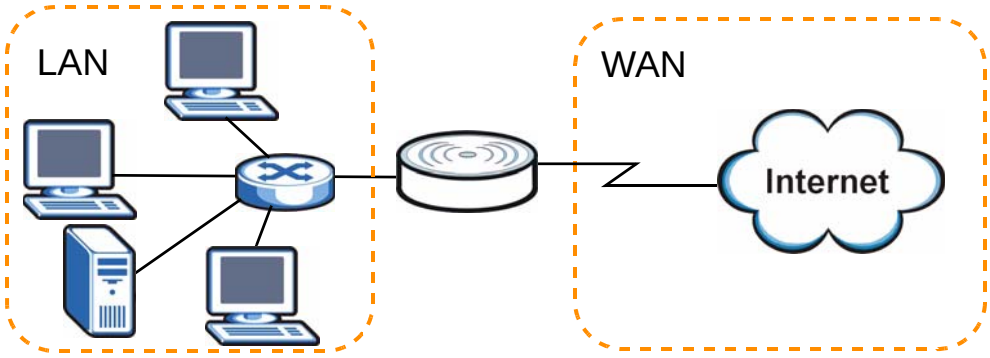
5.3 Technical Reference

The following section contains additional technical information about the N4100 features described in this chapter.

LANs, WANs and the N4100

The actual physical connection determines whether the N4100 ports are LAN or WAN ports. There are two separate IP networks, one inside the LAN network and the other outside the WAN network as shown next.

Figure 32 LAN and WAN IP Addresses



IP Address and Subnet Mask

Similar to the way houses on a street share a common street name, so too do computers on a LAN share one common network number.

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0 and you must enable the Network Address Translation (NAT) feature of the N4100. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

Once you have decided on the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your N4100, but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your N4100 will compute the subnet mask automatically based on the IP address that

you entered. You don't need to change the subnet mask computed by the N4100 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Note: Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, “Address Allocation for Private Internets” and RFC 1466, “Guidelines for Management of IP Address Space”.

PPP over Ethernet

The N4100 supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example RADIUS).

One of the benefits of PPPoE is the ability to let you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

Operationally, PPPoE saves significant effort for both you and the ISP or carrier, as it requires no specific configuration of the broadband modem at the customer site.

By implementing PPPoE directly on the N4100 (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the N4100 does that part of the task.

PPTP Encapsulation

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using TCP/IP-based networks.

PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet.

6 Server

6.1 Overview

This chapter describes how to configure the **Server** screens.

6.1.1 What You Can Do in this Chapter

- Use the **Server** screen (Section 4.2 on page 64) to set the embedded web server, the LAN DHCP server and specify the e-mail server for e-mail redirection on the N4100.
- Use the **Static DHCP Table** screen (Section 6.3 on page 86) to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

6.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

WWW (HTTP and HTTPS)

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

It relies upon certificates, public keys, and private keys (see Chapter 31 on page 243 for more information).

HTTPS on the N4100 is used so that you may securely access the N4100 using the web configurator. The SSL protocol specifies that the SSL server (the N4100) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the N4100), whereas the SSL client only should authenticate itself when the SSL server requires it to do so (select **Enable** in the **ADVANCED > AUTHENTICATION** screen to authenticate client certificates). If

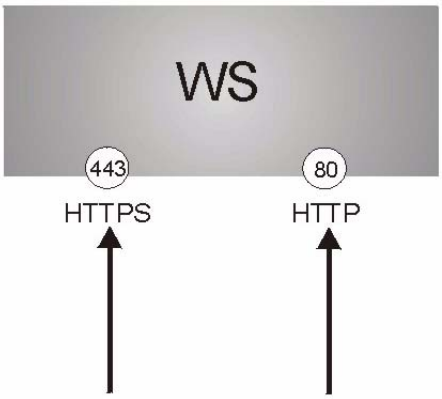
selected, the SSL-client must send the N4100 a certificate. You must apply for a certificate for the browser from a CA.

Please refer to the following figure.

1 HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the N4100's WS (web server).

2 HTTP connection requests from a web browser go to port 80 (by default) on the N4100's WS (web server).

Figure 33 HTTPS Implementation



DHCP Setup

DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients to obtain TCP/IP configuration at start-up from a server.

This N4100 has a built-in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

You can configure the N4100 as a DHCP server or disable it. When configured as a server, the N4100 provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured.

You can also configure the N4100 to relay client DHCP requests to a DHCP server and the server's responses back to the clients.

DNS Server Addresses

DNS (Domain Name System) maps a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it. The DNS

server addresses you enter when you set up DHCP are passed to the client machines along with the assigned IP address and subnet mask.

DNS Relay

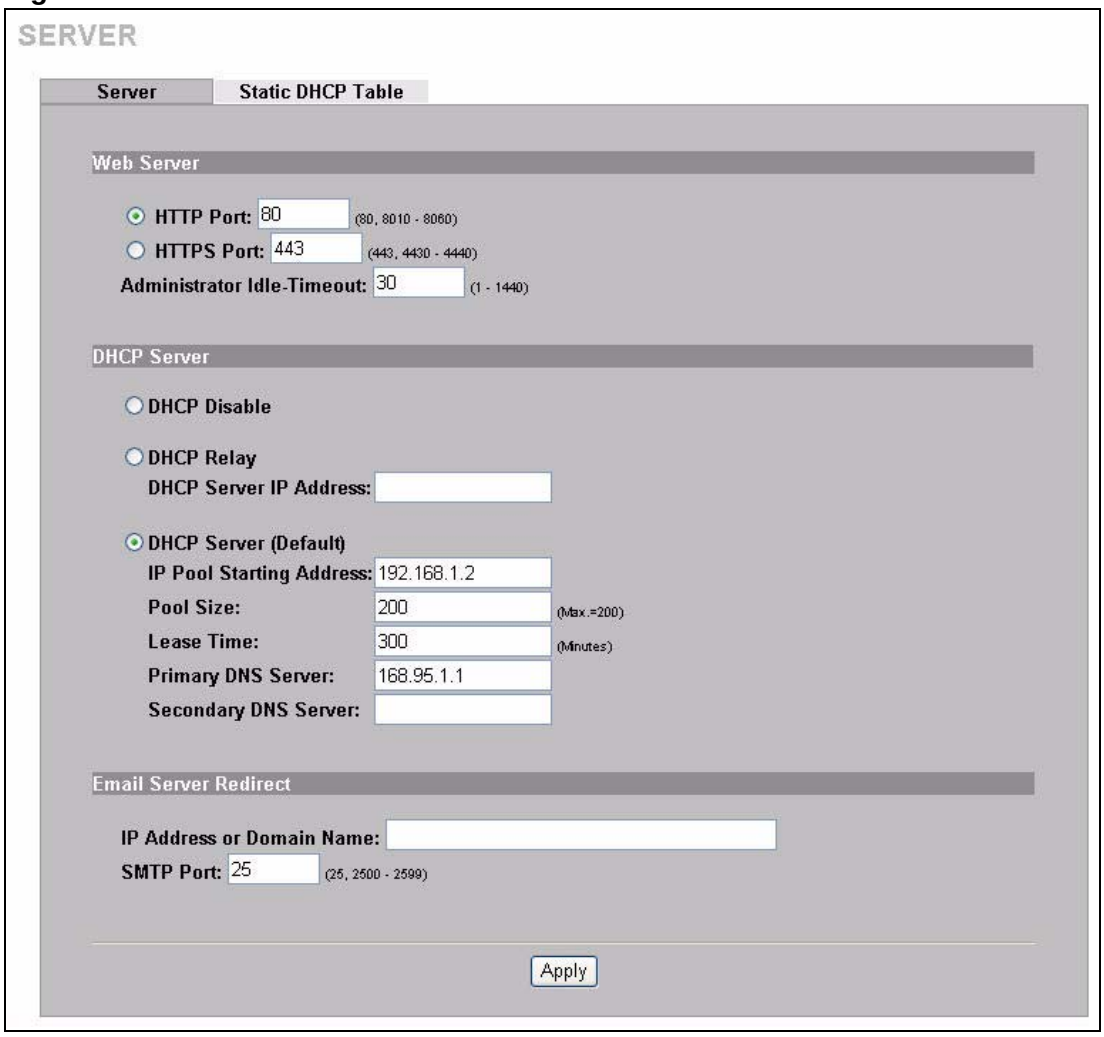
The N4100 supports the IPCP (IP Control Protocol) DNS server extensions through the DNS proxy feature. When this feature is enabled, the N4100 tells the DHCP clients that it itself is the DNS server. When a computer sends a DNS query to the N4100, the N4100 acts as a DNS proxy and forwards the query to the real DNS server learned through IPCP and relays the response back to the computer.

Please note that DNS proxy works only when the ISP uses the IPCP DNS server extensions. It does not mean you can leave the DNS servers out of the DHCP setup under all circumstances. If your ISP gives you explicit DNS servers, make sure that you enter their IP addresses in the DNS server fields.

6.2 The Server Screen

Click **ADVANCED > SERVER** to open this screen.

Figure 34 ADVANCED > SERVER



The following table describes the labels in this screen.

Table 9 ADVANCED > SERVER

LABEL	DESCRIPTION
Web Server	
HTTP Port	Select this radio button if you want to access the N4100 using unsecured HTTP. Specify the port number of the embedded web server on the N4100 for accessing the web configurator. The default port number is **80**. Changing the port number helps protect the N4100's web configurator from hacker attacks. Enter a number between 8010 and 8060 to access the web configurator behind a NAT-enabled network. If you enter a number between 8010 and 8060, you need to append the port number to the **WAN** or **LAN** port IP address to access the web configurator. For example, if you enter "8010" as the web server port number, then you must enter "http://192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address.
HTTPS Port	Select this radio button if you want to access the N4100 using secure HTTPS. Secure Socket Layer (SSL) security allows you to create secure connections between the N4100 and the management computer(s). Refer to Chapter 31 on page 243 for more information. Specify the port number of the embedded web server on the N4100 for accessing the web configurator. The default port number is **443**. Changing the port number helps protect the N4100's web configurator from hacker attacks. Enter a number between 4430 and 4440 to access the web configurator behind a NAT-enabled network. If you enter a number between 4430 and 4440, you need to append the port number to the **WAN** or **LAN** port IP address to access the web configurator. For example, if you enter "4430" as the web server port number, then you must enter "https://192.168.1.1:4430" where 192.168.1.1 is the WAN or LAN port IP address.
Administrator Idle-Timeout	Type how many minutes a management session can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. A value of "0" means a management session never times out, no matter how long it has been left idle (not recommended).
DHCP Server	Select the DHCP mode on the LAN.
DHCP Disable	Select this option to disable DHCP server on the LAN.
DHCP Relay	Use this if you have a DHCP server (either a computer or another router) and you want that DHCP server to also assign network information (IP address, DNS information etc.) to the devices that connect to the N4100. Select this option to set the N4100 to forward network configuration requests to a DHCP server. Then configure the **DHCP Server IP Address** field.

Table 9 ADVANCED > SERVER

LABEL	DESCRIPTION
DHCP Server IP Address	If you select **DHCP Relay**, enter the IP address of a DHCP server (on the WAN).
DHCP Server (Default)	Select this option to set the N4100 to assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the **LAN** port(s). This is the default setting.
IP Pool Starting Address	Enter the first of the continuous addresses in the IP address pool.
DHCP Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 1024.
Lease Time	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Primary/ Secondary DNS Server	Enter the IP address of the DNS server(s) in the **Primary DNS IP Address** and/or **Secondary DNS IP Address** fields. Note: You *must* specify a DNS server.
E-mail Server Redirect	
IP Address or Domain Name	Specify the IP address or the domain name of the e-mail server to which the N4100 forwards e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
Apply	Click **Apply** to save your changes back to the N4100.

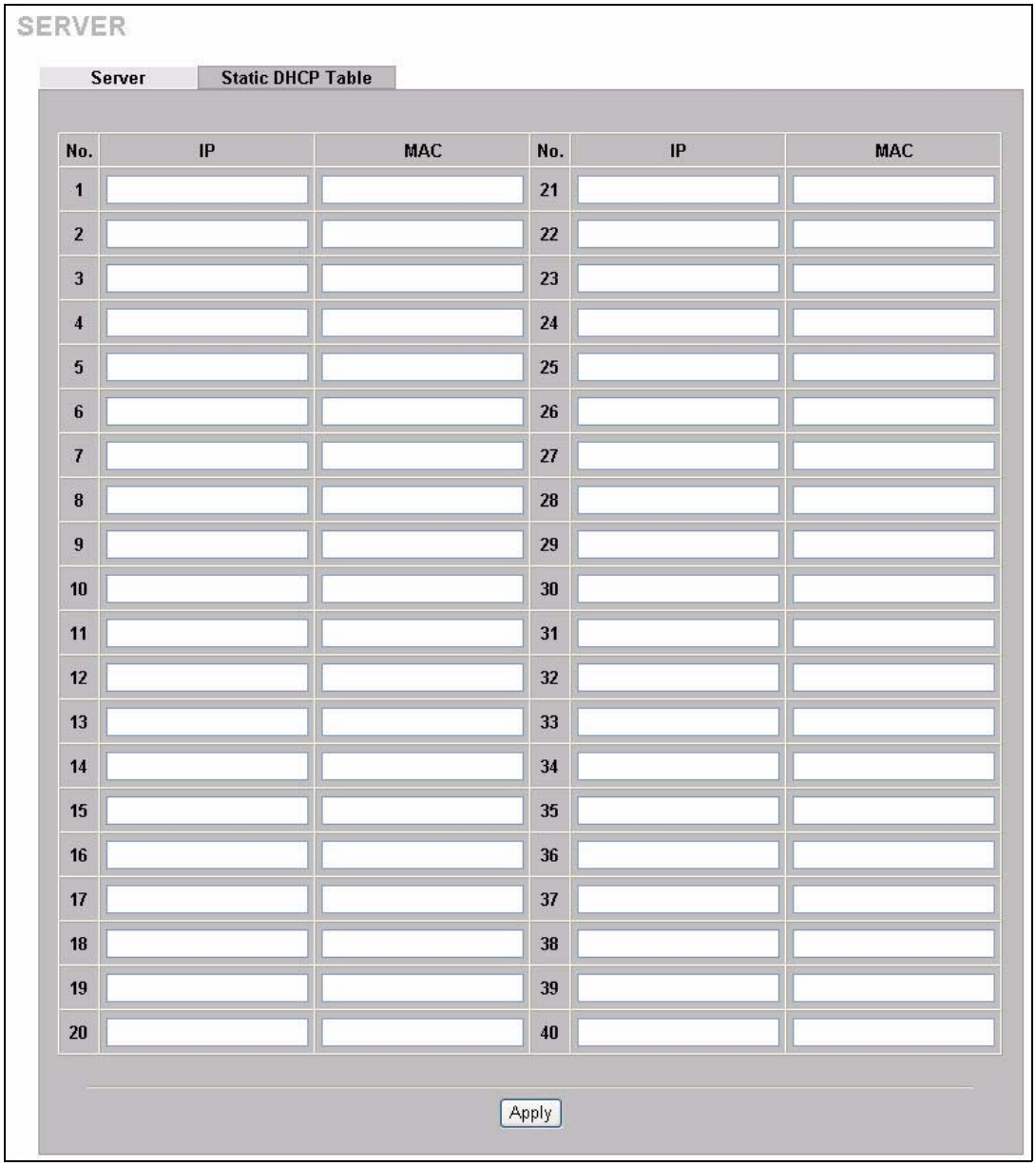
6.3 The Static DHCP Table Screen

This table allows you to assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.

Click **Network > LAN > Static DHCP Table** to open the following screen. Use this screen to change your N4100's static DHCP settings.

Figure 35 ADVANCED > SERVER > Static DHCP Table



The following table describes the labels in this screen.

Table 10 ADVANCED > SERVER > Static DHCP Table

LABEL	DESCRIPTION
No.	This is the index number of the entry.
IP Address	Enter the IP address that you want to assign to the computer on your LAN with the MAC address that you will also specify.

Table 10 ADVANCED > SERVER > Static DHCP Table

LABEL	DESCRIPTION
MAC Address	Enter the MAC address of a computer on your LAN.
Apply	Click **Apply** to save your changes back to the N4100.

7

Authentication

7.1 Overview

You can use the built-in subscriber database to manage the subscribers. The N4100 also provides a built-in billing mechanism to set up accounting information without using accounting software or an accounting server (such as RADIUS).

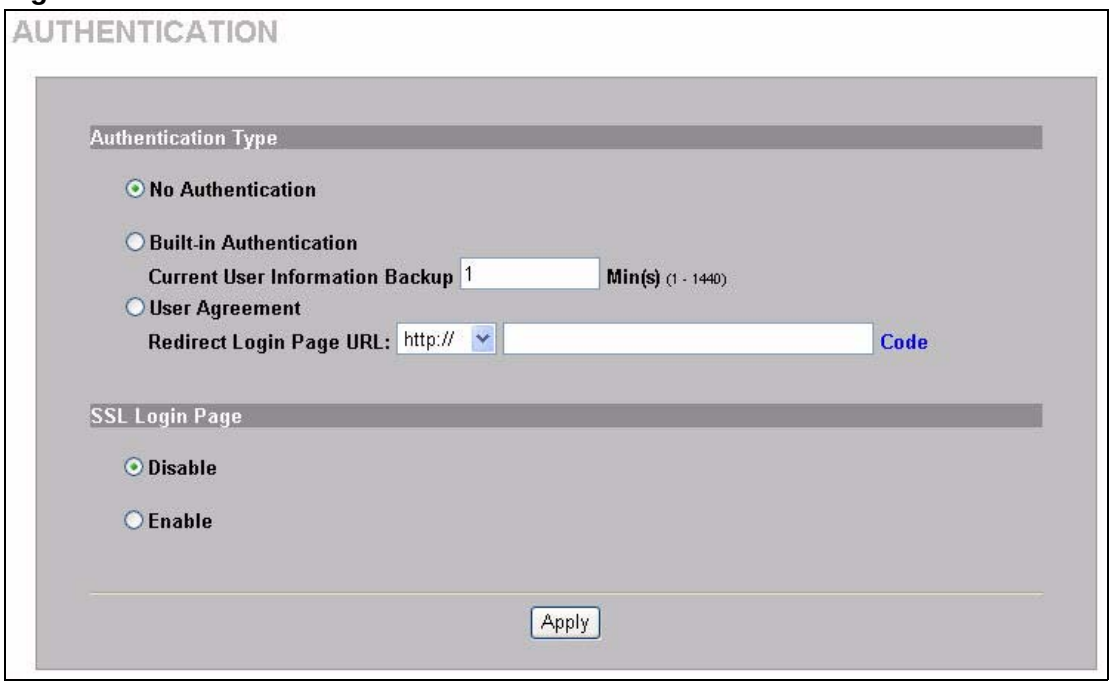
7.1.1 What You Can Do in this Chapter

Use the **Authentication** screen (Section 4.2 on page 64) to set up subscriber authentication on the N4100.

7.2 The Authentication Screen

Click **ADVANCED > AUTHENTICATION** to open this screen.

Figure 36 ADVANCED > AUTHENTICATION



The following table describes the labels in this screen.

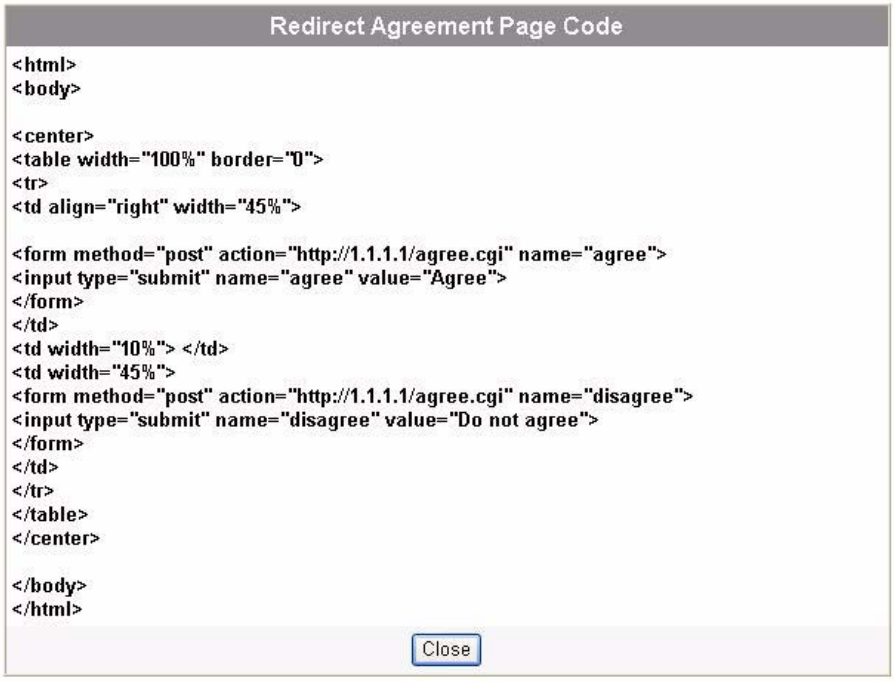
Table 11 ADVANCED > AUTHENTICATION

LABEL	DESCRIPTION
No Authentication	Select this option to disable subscriber authentication. Subscribers can access the Internet without entering user names and passwords. This is the default setting.
Built-in Authentication	Select this option to authenticate the subscribers using the local subscriber database. When you select this option, you *must* also configure the **Accounting** screen.
Current User Information Backup	The system provides automatic backup of account information and status. Use this field to set the number of minutes between backups. The default value is 1 minute. The valid range is 1 to 1440. If you create a subscriber account and the N4100 restarts before backing up the account information, the subscriber account will not be saved. You will need to create a new account for the subscriber.
User Agreement	Select **User Agreement** to redirect a subscriber to an Internet service usage agreement page before accessing the Internet.
Redirect Login Page URL	Specify the URL of the user agreement page in the field provided. Click **Code** to display the HTML source code of a default sample page. The user agreement page must include the HTML source code in the default sample page in order for the user agreement page to send the subscribers' agreement or disagreement to the N4100. Use up to 350 ASCII characters.
SSL Login Page	Select **Enable** to activate SSL security upon accessing the subscriber login screen so that the subscribers' user names and passwords are encrypted before being transmitted to the N4100. This applies when you select **Built-in Authentication** or **User Agreement**. Select **Disable** to de-activate SSL security for the subscriber login screen. Refer to Chapter 31 on page 243 for more information.
Apply	Click **Apply** to save your changes back to the N4100.

Click the **Code** link to display the HTML source code of a default sample page (shown next). The user agreement page must include the HTML source code in the

default sample page in order for the user agreement page to send the subscribers' agreement or disagreement to the N4100.

Figure 37 ADVANCED > AUTHENTICATION > Code



8

RADIUS

8.1 Overview

You can use an external RADIUS (Remote Authentication Dial-In User Service) server to authenticate the subscriber connections and keep track of accounting information.

RADIUS is based on a client-sever model that supports authentication, authorization and accounting. This system is the client and the server is the external RADIUS server.

RADIUS is a simple package exchange in which the N4100 acts as a message relay between the subscribers and the RADIUS server to establish a connection. When you enable RADIUS authentication, the N4100 uses RADIUS protocol (RFC 2865, 2866) to send subscriber authentication information to the external RADIUS server.

When you use an external RADIUS server for accounting, you can use either accumulation or time to finish accounting. See Chapter 9 on page 99 for information on accumulation and time to finish accounting.

8.1.1 What You Can Do in this Chapter

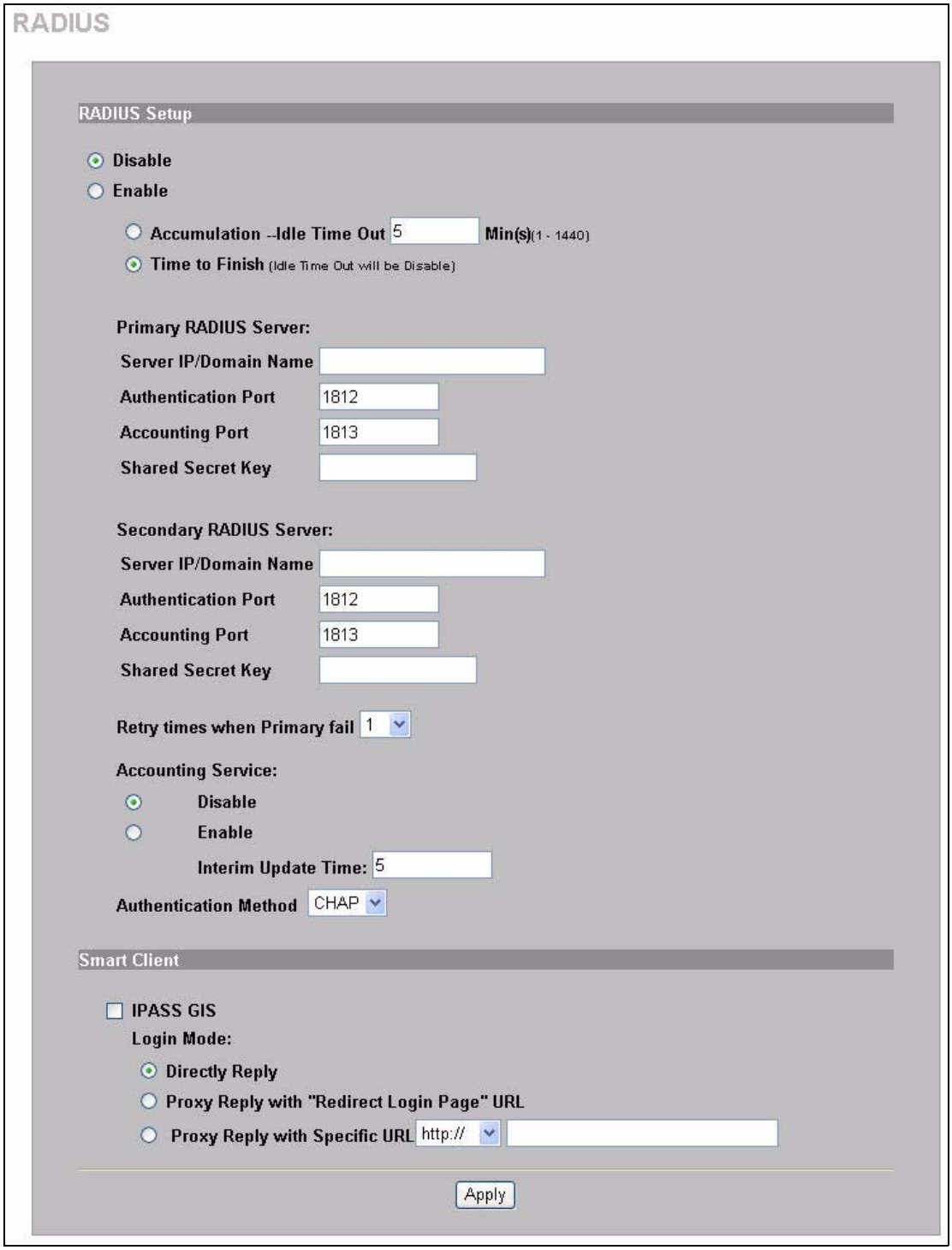
Use the **RADIUS** screen (Section 4.2 on page 64) to configure the N4100 to use an external RADIUS server.

8.2 The RADIUS Screen

Click **ADVANCED > RADIUS** to open this screen.

Note: You must set the authentication type to **Built-in Authentication** in the **ADVANCED > AUTHENTICATION** screen before you can save and apply any changes you do in the **RADIUS** screen.

Figure 38 ADVANCED > RADIUS



The following table describes the labels in this screen.

Table 12 ADVANCED > RADIUS

LABEL	DESCRIPTION
RADIUS Setup	Select **Disable** if you will not use an external RADIUS server to authenticate subscribers. Select **Enable** to use an external RADIUS server to authenticate subscribers. You may also use an external RADIUS server to perform accounting for the subscriber accounts. Note: Disabling authentication in the **AUTHENTICATION** screen also disables authentication via an external RADIUS server, regardless of what you set here.
Accumulation	Select this option to allow each subscriber multiple re-login until the time allocated is used up. This applies to subscribers that are authenticated by the RADIUS server; the setting in the **BILLING** screen applies to subscribers that are authenticated by the built-in authentication. You must also enable the accounting service below.
Idle Time Out	The N4100 automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is **5** minutes.
Time to Finish	Select this option to allow each subscriber a one-time login. Once the subscriber logs in, the system starts counting down the pre-defined usage even if the subscriber stops the Internet access before the time period is finished. If a subscriber disconnects and reconnects before the allocated time expires, the subscriber does not have to enter the user name and password to access the Internet again. This applies to subscribers that are authenticated by the RADIUS server; the setting in the **BILLING** screen applies to subscribers that are authenticated by the built-in authentication. You must also enable the accounting service below.
Primary RADIUS Server	
Server IP/ Domain Name	Enter the IP address or the domain name of the RADIUS server.
Authentication Port	Enter the port number that the RADIUS server uses for authentication. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Accounting Port	Enter the port number that the RADIUS server uses for accounting. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.

Table 12 ADVANCED > RADIUS

LABEL	DESCRIPTION
Shared Secret Key	Enter a password (up to 64 characters) as the key to be shared between the RADIUS server and the N4100. The key is not sent over the network. This key must be the same on the RADIUS server and the N4100.
Secondary RADIUS Server	
Server IP/ Domain Name	Enter the IP address or the domain name of the RADIUS server.
Authentication Port	Enter the port number that the RADIUS server uses for authentication. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Accounting Port	Enter the port number that the RADIUS server uses for accounting. You only need to change this value from the default if your network administrator gave you a specific port number to use. The allowed numbers are from 0 to 65535.
Shared Secret Key	Enter a password (up to 64 characters) as the key to be shared between the RADIUS server and the N4100. The key is not sent over the network. This key must be the same on the RADIUS server and the N4100.
Retry times when Primary fail	At times the N4100 may not be able to use the primary RADIUS server. Select the number of times the N4100 should reattempt to use the primary RADIUS server before attempting to use the secondary RADIUS server. This also sets how many times the N4100 will attempt to use the secondary RADIUS server. For example, you set this field to 3. If the N4100 does not get a response from the primary RADIUS server, it tries again up to three times. If there is no response, the N4100 tries the secondary RADIUS server up to three times. If there is also no response from the secondary RADIUS server, the N4100 stops attempting to authenticate the subscriber. The subscriber will see a message that says the RADIUS server was not found.
Accounting Service	Select **Disable** if you will not use an external RADIUS server to perform accounting for the wireless client accounts. Select **Enable** to use an external RADIUS server to perform accounting for the wireless client accounts.
Interim Update Time	Specify the time interval for how often the N4100 is to send a subscriber status update to the RADIUS server.
Authentication Method	Enter the authentication protocol that the RADIUS server uses. **PAP** (Password Authentication Protocol) requires users to enter a password before accessing a secure system. The user's name and password are sent over the wire to a server where they are compared with a database of user account names and passwords. **CHAP** (Challenge Handshake Authentication Protocol) avoids sending passwords over the wire by using a challenge/response technique.

Table 12 ADVANCED > RADIUS

LABEL	DESCRIPTION
IPASS GIS	The iPass company provides connectivity services for mobile Internet users. Select this check box to have the N4100 use the iPass Generic Interface Specification (GIS) method to authenticate iPass clients. Your external RADIUS servers must be Wi-Fi based Wireless Internet Service Provider roaming (WISPr) compliant in order to authenticate iPass clients.
Login Mode	When using iPass GIS, your ISP will provide you with login mode information. Select **Directly Reply**, **Proxy Reply with "Redirect Login Page" URL** or **Proxy Reply with Specific URL** (and enter a URL of up to 350 ASCII characters in the field provided). The login mode information for the iPass GIS connection. (Provided by your ISP).
Apply	Click **Apply** to save your changes back to the N4100.

9

Billing

9.1 Overview

You can use the built-in billing function to setup billing profiles. A billing profile describes how to charge subscribers.

9.1.1 What You Can Do in this Chapter

Use the **Billing** screen (Section 9.2 on page 100) to set up subscriber billing on the N4100.

9.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

Accumulation Accounting Method

The accumulation accounting method allows multiple re-logins until the allocated time period or until the subscriber account is expired. The N4100 accounts the time that the subscriber is logged in for Internet access.

Time-to-finish Accounting Method

The time-to-finish accounting method is good for one-time logins. Once a subscriber logs in, the N4100 stores the MAC address of the subscriber's computer for the duration of the time allocated. Thus the subscriber does not have to enter the user name and password again for re-login within the allocated time.

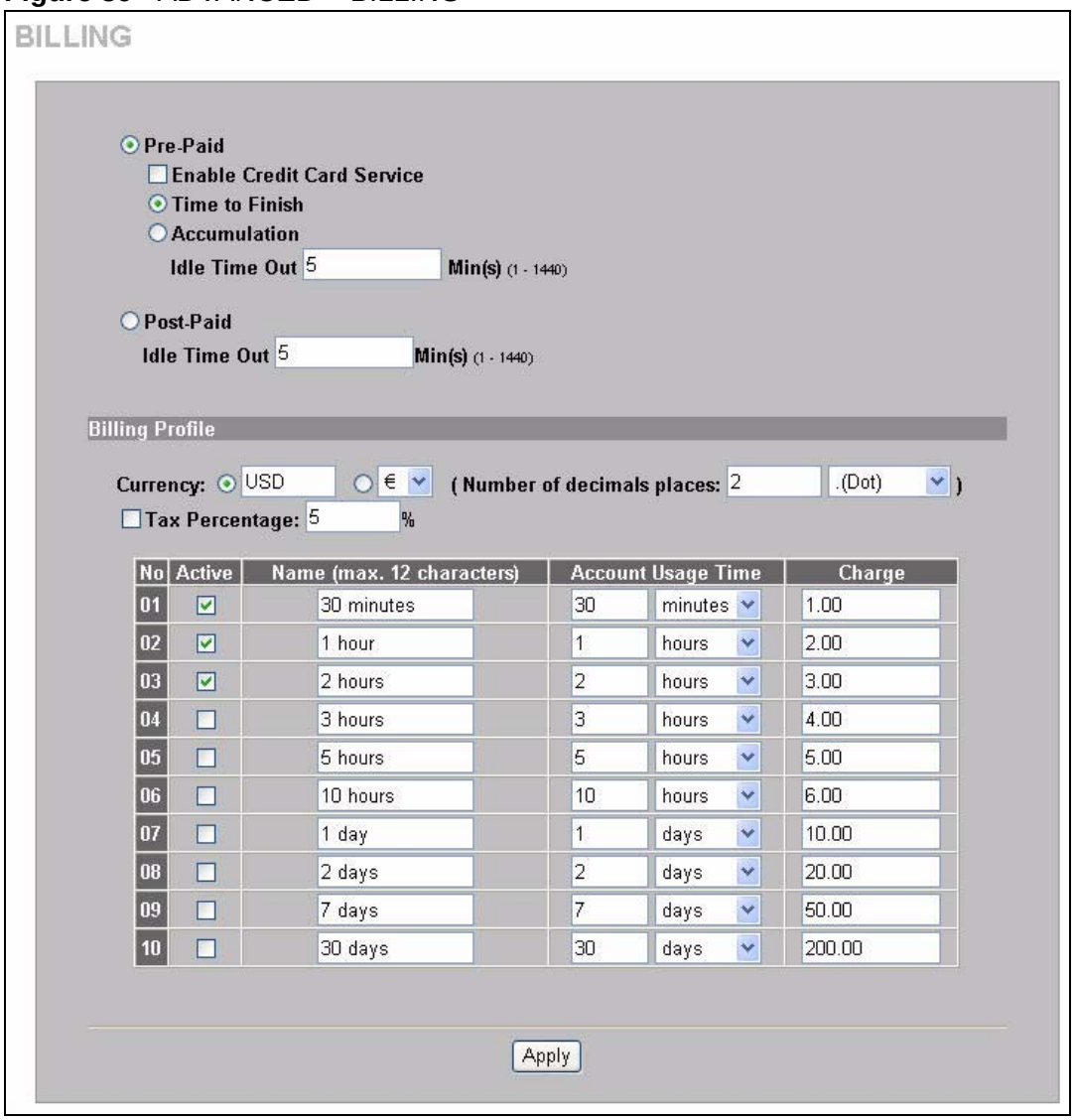
Once activated, the subscriber account is valid until the allocated time is reached even if the subscriber disconnects Internet access for a certain period within the allocated time. For example, Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects his Internet access to go to a 20-minute meeting. After the meeting, he only has 20 minutes left on his account.

9.2 The Billing Screen

Click **ADVANCED > BILLING** to open this screen.

Note: If you change the billing mode, the system erases all accounts and disconnects all on-line subscribers.

Figure 39 ADVANCED > BILLING



The following table describes the labels in this screen.

Table 13 ADVANCED > BILLING

LABEL	DESCRIPTION
Pre-Paid	Enable this option to allow the subscribers to access the Internet for a pre-defined time period.
Enable Credit Card Service	Enable the credit card service to authorize, process, and manage credit transactions directly through the Internet. Before you enable credit card service, make sure that your credit service is configured to work and the currency is American dollars. You must convert all prices on your billing page into American dollars (U.S. dollars). See Chapter 11 on page 109 for details. You must also configure your credit card service information in the **ADVANCED > CREDIT CARD** screen if you want to allow the subscribers to use credit cards to purchase Internet usage time.
Time to Finish	Select this option to allow each subscriber a one-time login. Once the subscriber logs in, the system starts counting down the pre-defined usage even if the subscriber stops the Internet access before the time period is finished. If a subscriber disconnects and reconnects before the allocated time expires, the subscriber does not have to enter the user name and password to access the Internet again.
Accumulation	Select this option to allow each subscriber multiple re-login until the time allocated is used up.
Idle Time Out	The N4100 automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is **5** minutes.
Post-Paid	A subscriber can access the Internet without a pre-defined usage time. The printout only shows the username and password. The hot spot operator can also use the optional keypad to terminate an account. You must use an optional keypad with the three-button printer in order to use the post-paid function. See Chapter 12 on page 113 for how to configure the keypad settings.
Idle Time Out	The N4100 automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is **5** minutes.
Currency	Enter the appropriate currency unit or currency symbol.
Number of decimals places	Define the number of decimal places (up to 3) to be used for billing. You can also select whether you would like to use a period (.) or a comma (,) for the decimal point.
Tax Percentage	Select this check box to charge sales tax for the account. Enter the tax rate (a 5% sales tax is entered as 5).
No.	The index numbers of the billing profiles.
Active	Select the check box, to activate the billing profile or clear the check box to deactivate the billing profile.

Table 13 ADVANCED > BILLING

LABEL	DESCRIPTION
Name	Enter a name (up to 12 characters) for the billing profile.
Account Usage Time	Use these fields to set the duration of the billing period. When this period expires, the subscriber's access will be stopped. Select a time period (**minutes**, **hours**, or **days**) and enter the time unit in the field provided to define each "profile's" maximum Internet access time.
Charge	Define each profile's price, up to 999999, per time unit (configured in the **Account Usage Time** field).
Apply	Click **Apply** to save your changes back to the N4100.

10

Accounting

10.1 Overview

Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list. Accounts are automatically generated either by pressing a button on a connected exclusive printer or using the web configurator (the **Account Generator Panel** screen).

10.1.1 What You Can Do in this Chapter

Use the **Accounting** screen (Section 10.2 on page 104) to set up and manage subscriber accounts.

10.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

Discount Price Plan

You can configure a custom discount pricing plan. This is useful for providing reduced rates for purchases of longer periods of time. You can charge higher rates per unit at lower levels (fewer units purchased) and lower rates per unit at higher levels (more units purchased).

The discount price plan only works when the hot spot operator does the billing through a statement printer or the web-based account generator panel. The discount price plan does not apply to subscribers purchasing access time online with a credit card.

Charge by Levels

The discount price plan gives you the option to charge by levels. This allows you to charge the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the total purchase reaches.

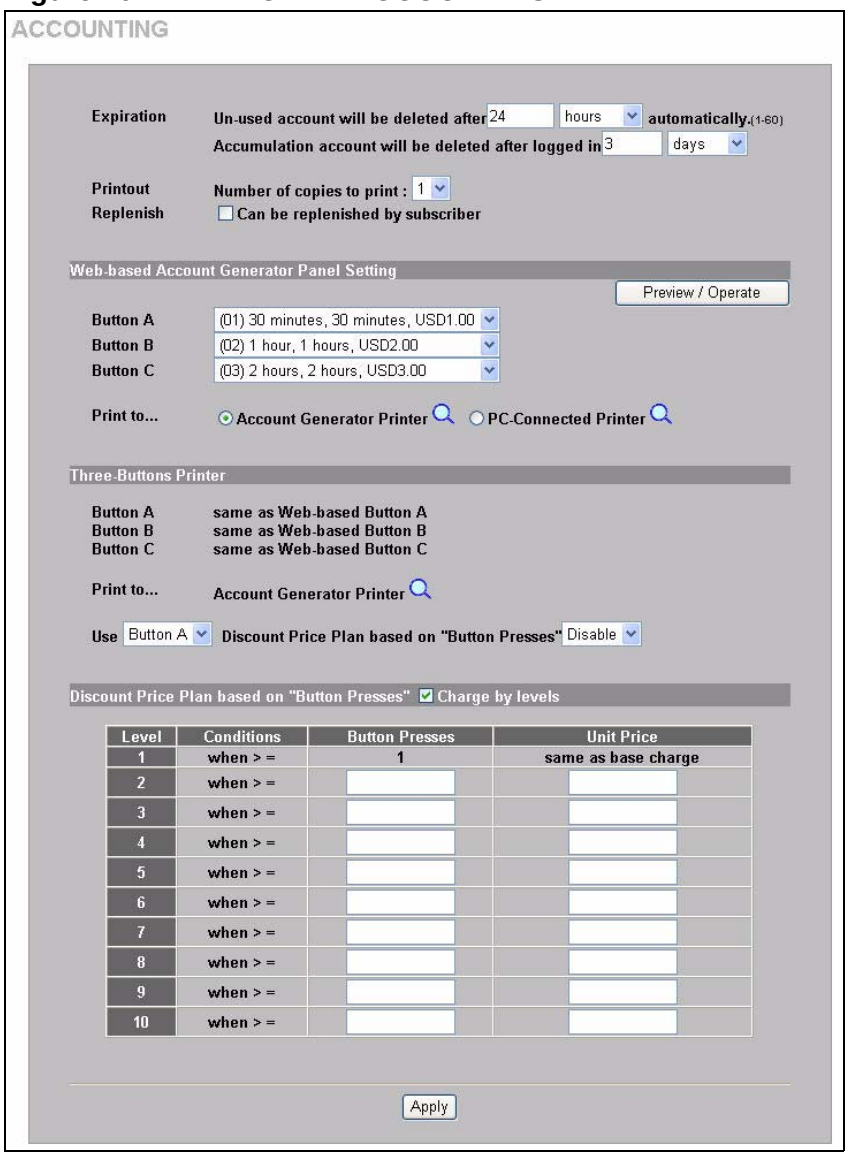
Otherwise you can disable the charge by level function and charge all of the time units only at the highest (least expensive) level that the total purchase reaches.

See Section 10.2.1 on page 106 for an example of the charge by levels accounting function.

10.2 The Accounting Screen

Click **ADVANCED > ACCOUNTING** to open this screen.

Figure 40 ADVANCED > ACCOUNTING



The following table describes the labels in this screen.

Table 14 ADVANCED > ACCOUNTING

LABEL	DESCRIPTION
Expiration	
Un-used account will be deleted after ~ automatically	Enter the number and select a time unit from the drop-down list box to specify how long to wait before the N4100 deletes an account that has not been used. This is for use with time to finish accounting.
Accumulation account will be deleted after logged in	Enter the number and select a time unit from the drop-down list box to specify how long to wait before the N4100 deletes an idle account. This is for use with accumulation accounting.
Printout	
Number of copies to print	Select how many copies of subscriber statements you want to print (1 is the default).
Replenish	
Can be replenished by subscriber	Select the check box to allow subscribers to purchase additional time units for their accounts before the accounts expire.
Web-based Account Generator Panel Setting	
Preview/ Operate	Click **Preview / Operate** to open the **Account Generator Panel** (see Section 3.3.1 on page 39 for more information).
Button A~C	Each button represents a billing profile that defines maximum Internet access time and charge per time unit. The buttons correspond to the buttons displayed in the **Account Generator Panel**. Select a billing profile from the list box for each button.
Print to...	Select **Account Generator Printer** if you want to print the account information using a statement printer connected to the N4100 via Ethernet. Select **PC-Connected Printer** if you want to print the account information using a printer connected to a network computer. Click the magnifying glass icon to display a print preview.
Three-Buttons Printer	Use this section with a three-button statement printer.
Button A~C	These buttons correspond to the **Web-based Account Generator Panel** section's buttons A~C. Each button represents a billing profile that defines maximum Internet access time and charge per time unit.
Print to...	Select **Account Generator Printer** if you want to print the account information using a statement printer connected to the N4100 via Ethernet. Click the magnifying glass icon to display a print preview.

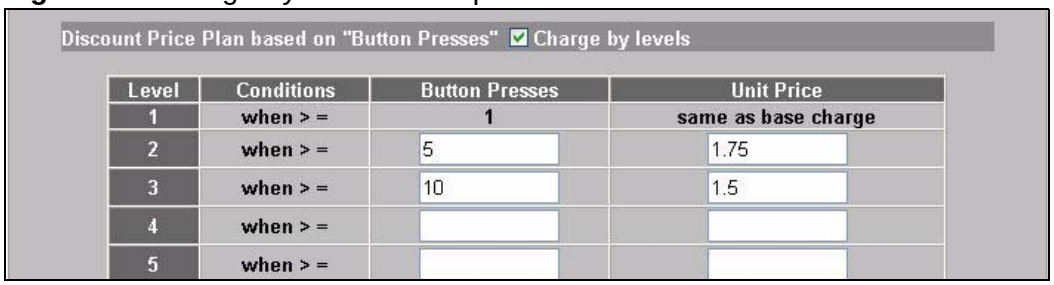
Table 14 ADVANCED > ACCOUNTING

LABEL	DESCRIPTION
Use ~ Discount Price Plan based on "Button Presses"	Select a button from the drop-down list box to assign the base charge and select **Enable** to activate the discount price plan.
Discount Price Plan based on "Button Presses"	
Charge by levels	Disable the charge by level function to charge all of the subscriber's time units only at the highest level (least expensive) that their total number of button presses reaches. Enable the charge by levels function to charge the subscriber the rates at each successive level from the first level (least expensive) to the highest level (least expensive) that their total number of button presses reaches.
Level	These are the read-only level numbers of the discount charges.
Conditions	A discount level takes effect whenever the button selected in the **Three button Printer Setting** section is pressed more than or the same number of times as the number displayed in the **Button Presses** field.
Button Presses	Enter the number of times the button must be pressed to equal that discount level.
Unit Price	Enter each level's charge per time unit.
Apply	Click **Apply** to save your changes back to the N4100.

10.2.1 Charge By Levels Example

This is an example of how charge by levels accounting works. The discount price plan allows you to make the unit price lower as the subscriber purchases more (meaning a higher number of button pushes). The Unit Price for level 1 is always the same as the base charge ($2.00 for this example). The following screen has discount price level 2 set to $1.75 and level 3 set to $1.50. Taxes are not included in this example.

Figure 41 Charge By Levels Example



A subscriber purchases 11 units. Without charge by levels accounting, the total would be the number of button presses (11) multiplied by the unit price for the

level that the number of button presses matches. In this case it would be 11x $1.50 for a total of $16.50 (excluding tax).

With charge by levels accounting, you charge the subscriber the rate at each successive level from the first level (most expensive per unit) to the highest level (least expensive per unit) that the purchase reaches. In this example, the N4100 would charge as follows:

Table 15 Charge By Levels Example

The base charge ($2.00) per unit for button presses 1-4.	($2.00 x 4= $8.00)
The level 2, unit price ($1.75) per unit for button presses 5-9.	($1.75 x 5= $8.75)
The level 3, unit price ($1.50) per unit for button presses 10-11.	($1.50 x 2= $3.00)
For a total of:	$19.75 (excluding tax)

11

Credit Card

11.1 Overview

The N4100 allows you to use a credit card service to authorize, process, and manage credit card transactions directly through the Internet. You must register with one of the supported credit card service (see Figure 42 on page 110) before you can configure the N4100 to handle credit card transactions.

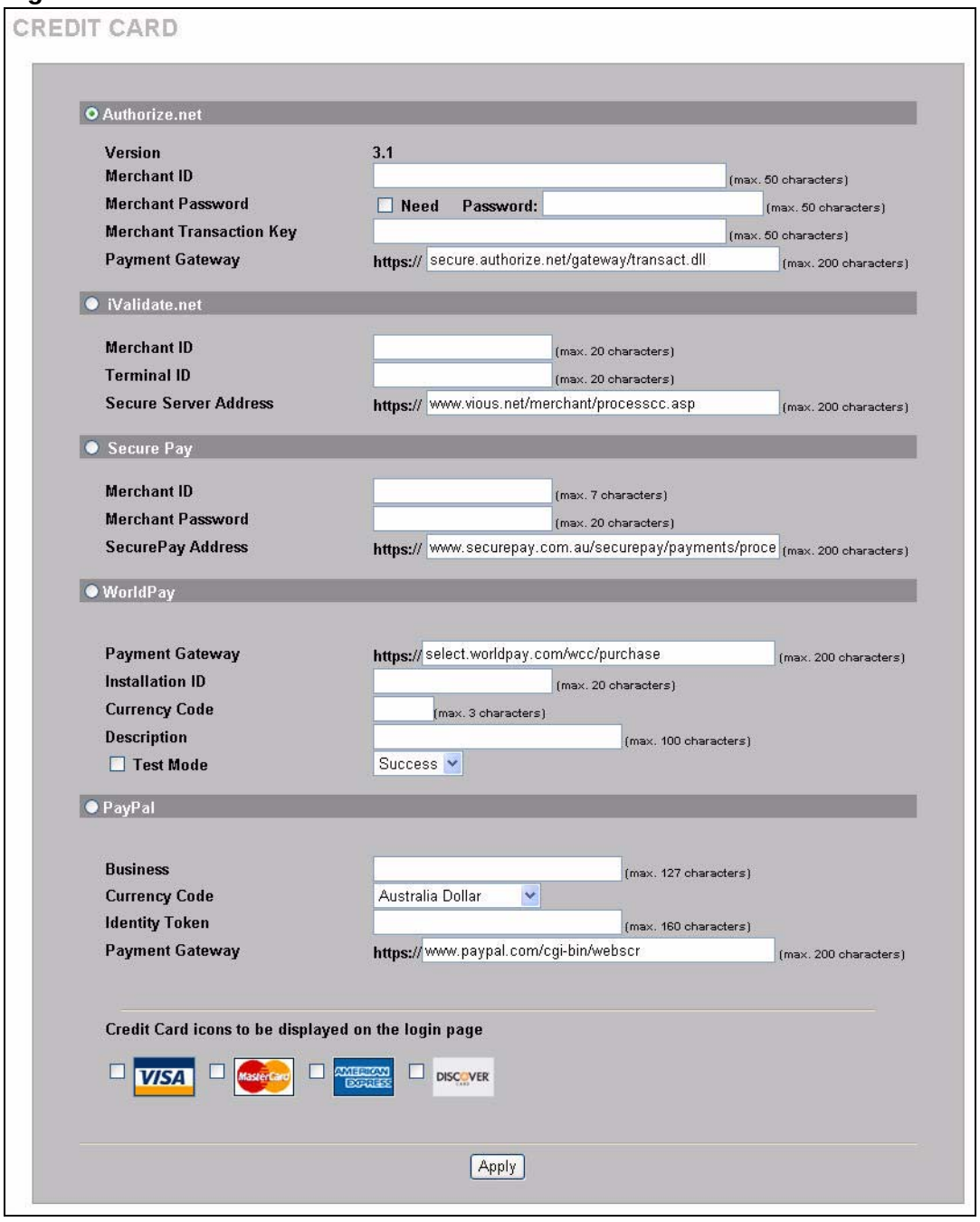
11.1.1 What You Can Do in this Chapter

Use the **Credit Card** screen (Section 11.2 on page 110) to set the N4100 to handle credit card transactions.

11.2 The Credit Card Screen

Click **ADVANCED > CREDIT CARD** to open this screen.

Figure 42 ADVANCED > CREDIT CARD



The following table describes the labels in this screen.

Table 16 ADVANCED > CREDIT CARD

LABEL	DESCRIPTION
Authorize.net	Select this radio button if you use Authorize.net to authorize credit card payments.
Version	This is the (read-only) software version of the Authorize.net payment Gateway.
Merchant ID	Enter the IDentification number that you received from Authorize.net.
Merchant Password Need	Select this if you have to provide a password to Authorize.net.
Password	Enter the password you have to provide to Authorize.net.
Merchant Transaction Key	Enter the transaction key exactly as you received it from Authorize.net. The transaction key is similar to a password. The Authorize.net gateway uses the transaction key to authenticate transactions.
Payment Gateway	Enter the address of the Authorize.net gateway.
iValidate.net	Select this radio button if you use iValidate.net to authorize credit card payments.
Merchant ID	Enter the IDentification number that you received from iValidate.net.
Terminal ID	Enter the Device Identification Number that you received from your merchant provider.
Secure Server Address	Enter the address of the iValidate.net secure server.
Secure Pay	Select this radio button if you use SecurePay to authorize credit card payments.
Merchant ID	Enter the IDentification number that you received from Authorize.net.
Merchant Password Need	Enter the password you have to provide to SecurePay.
SecurePay Address	Enter the address of the SecurePay gateway.
WorldPay	Select this radio button if you use WorldPay to authorize credit card payments.
Payment Gateway	Enter the address of the WorldPay gateway provided to you by WorldPay after applying for your WorldPay account.
Installation ID	Enter the installation ID provided to you by WorldPay after successfully applying for your WorldPay account.
Currency Code	Enter the currency in which payments are made. The available currencies depend on your agreement with WorldPay.
Description	Enter the description of each purchase. This description appears on the customer's receipt.
Test Mode	Check this box if you want to evaluate the way WorldPay is used without actually transferring funds. There are two test modes, **Success** and **Fail**. In **Success** test mode, transactions are submitted as if the bank authorized the transaction. In **Fail** test mode, transactions are submitted as if the bank declined authorization.

Table 16 ADVANCED > CREDIT CARD

LABEL	DESCRIPTION
PayPal	Select this radio button if you use PayPal to authorize credit card payments.
Business	Enter the business name on your PayPal account.
Currency Code	Select the currency in which payments are made. The available currencies depend on your agreement with PayPal.
Identity Token	Enter the ID token provided to you by PayPal after successfully applying for your PayPal account.
Payment Gateway	Enter the address of the PayPal gateway provided to you by PayPal after applying for your PayPal account.
Credit Card icons to be displayed on the login page	Select the check box(es) of the credit card icon(s) that you want the N4100 to display on the subscriber login page.
Apply	Click **Apply** to save your changes back to the N4100.

12 Keypad

12.1 Overview

You can use an optional PS/2 numeric keypad with a statement printer. Use this screen to define functions for the keys.

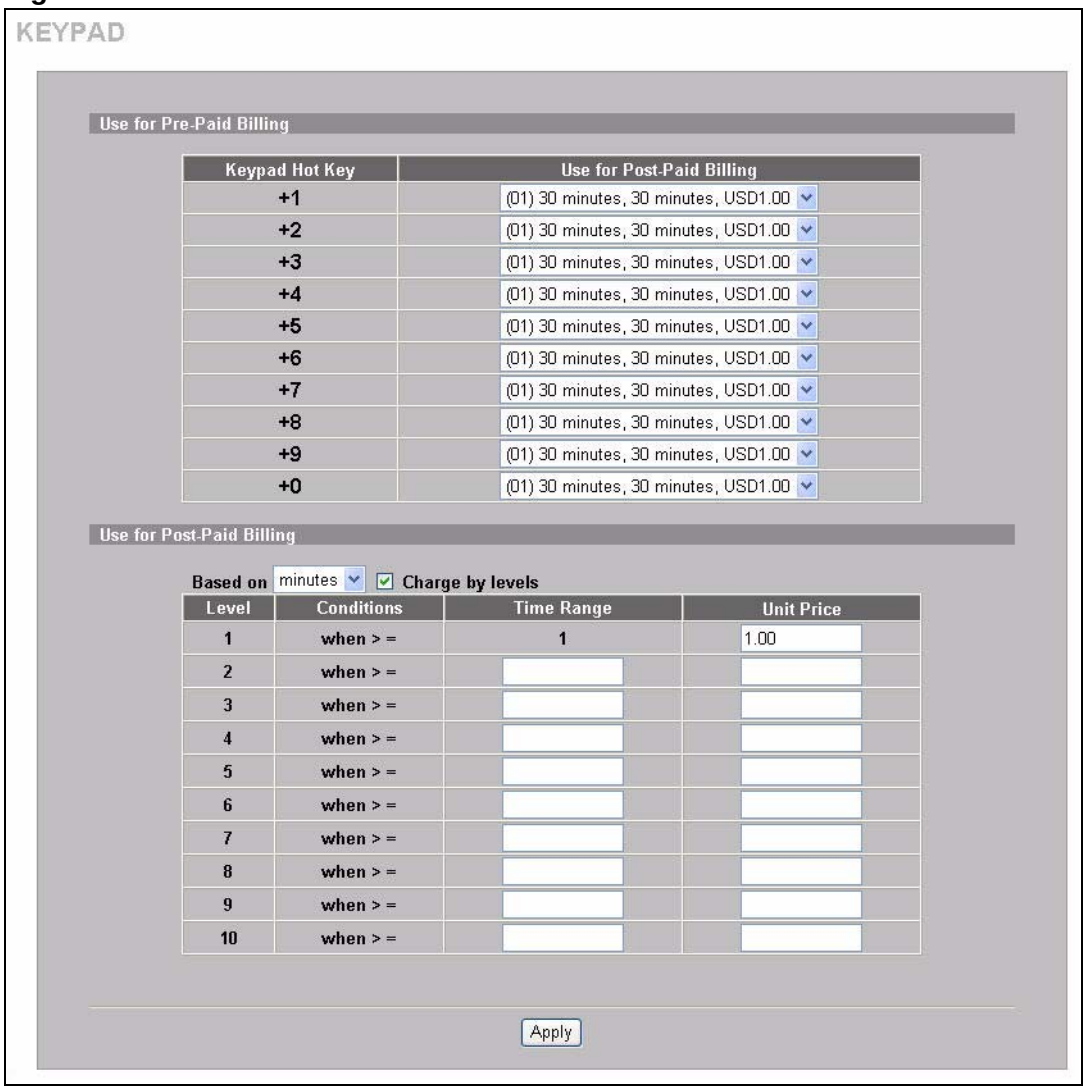
12.1.1 What You Can Do in this Chapter

Use the **Keypad** screen (Section 12.2 on page 114) to set up the optional keypad for a statement printer.

12.2 The Keypad Screen

Click **ADVANCED > KEYPAD** to open this screen.

Figure 43 ADVANCED > KEYPAD



The following table describes the labels in this screen.

Table 17 ADVANCED > KEYPAD

LABEL	DESCRIPTION
Use for Pre-Paid Billing	The system provides ten user definable hot keys through the use of the + Key plus the 1 through 0 keys across the top of the keypad.
Keypad Hot Key	+1~+0 This is the combination hot key for a keypad application.
Use for Post-Paid Billing	Select the billing profile that you want to assign to the combination hot key. Use the **Billing** screen to configure and activate billing profiles. Only active billing profiles display here for you to choose from.

Table 17 ADVANCED > KEYPAD

LABEL	DESCRIPTION
Use for Post-Paid Billing	Use the following fields to define the basic charge levels and rates for accounts.
Base on	Select the billing time unit from the drop-down list box.
Charge by levels	Use this field to enable or disable the charge by levels function. See Chapter 10 on page 103 for details on the charge by levels function.
Level	These are the read-only level numbers of the charges.
Conditions	Charges may vary by subscription time. A charge level takes effect when the amount of time the subscriber has used is bigger than or the same as the number displayed in the **Time Range** field.
Time Range	Enter the number of time units (defined in the **Base on** field) for this charge level.
Unit Price	Enter each level's charge per time unit.
Apply	Click **Apply** to save your changes back to the N4100.

12.3 Keypad Configuration Examples

These sections explain how to configure the N4100 for use with a PS/2 keypad.

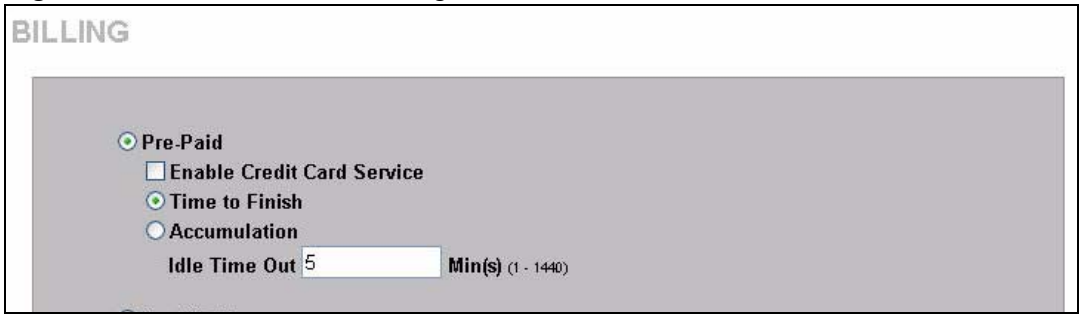
12.3.1 Keypad with Pre-Paid Billing Example

The following is an example of how to configure the N4100 to use a PS/2 keypad for pre-paid billing.

1 Click **ADVANCED > BILLING**.

2 Select **Pre-Paid** and click **Apply**.

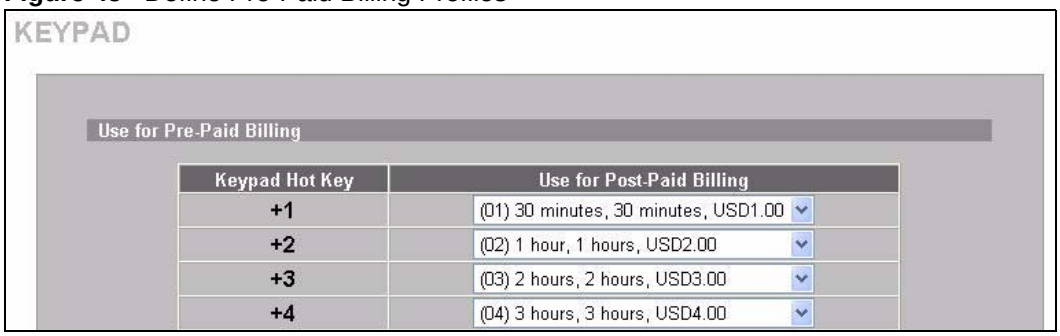
Figure 44 Select Pre-Paid Billing



3 Click **ADVANCED > KEYPAD**.

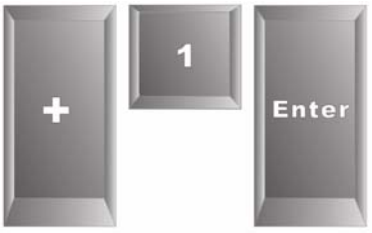
4 Define your pre-paid billing profiles and click **Apply**.

Figure 45 Define Pre-Paid Billing Profiles



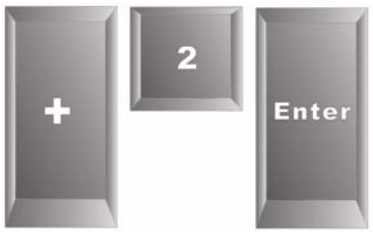
5 Use the keypad to create subscriber accounts. Press the keypad hot key and then [ENTER] to generate a new subscriber account and print the account information.

Figure 46 Billing Profiles 1 and 2 Examples



The first billing profile
(01) 30 minutes, 30 minutes, USD1.00

```
Welcome!
----------------------------------------
Hotspot Internet Service
----------------------------------------
Username:b4e55f35
Password:xz6g6n82
Billing:Time to Finish
Service:30 minutes
Unit:1
Usage Time:00:30:00
Total:USD 1.00
Tax:USD 0.00
Grand Total:USD 1.00
----------------------------------------
ESSID:ZyXEL
----------------------------------------
2010/01/22 16:40:58
S/N:000001
Please activate your account before
2010/01/23 04:40:58
----------------------------------------
Thank you very much !
```



The second billing profile
(02) 1 hour, 1 hours, USD2.00

```
Welcome!
----------------------------------------
Hotspot Internet Service
----------------------------------------
Username:7spct858
Password:jic7rp55
Billing:Time to Finish
Service:1 hour
Unit:1
Usage Time:01:00:00
Total:USD 2.00
Tax:USD 0.00
Grand Total:USD 2.00
----------------------------------------
ESSID:ZyXEL
----------------------------------------
2010/01/22 16:58:04
S/N:000001
Please activate your account before
2010/01/23 04:58:04
----------------------------------------
Thank you very much !
```

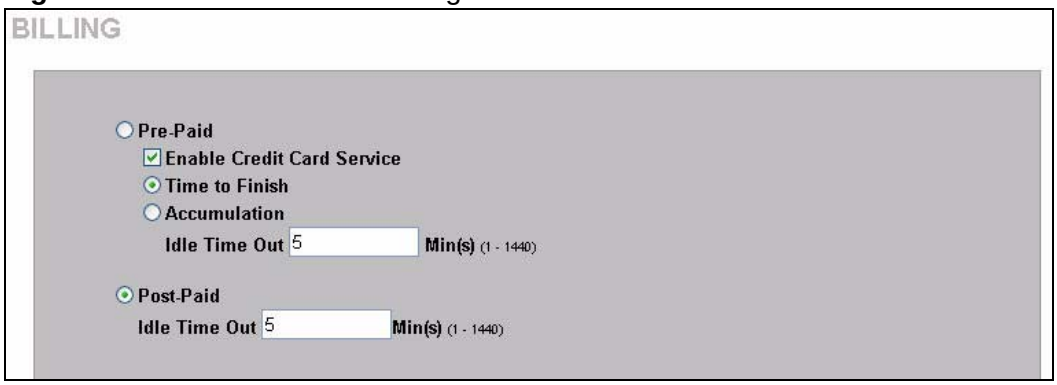
12.3.2 Keypad with Post-Paid Billing Example

The following is an example of how to configure the N4100 to use a PS/2 keypad for post-paid billing.

1 Click **ADVANCED > BILLING**.

2 Select **Post-Paid** and click **Apply**.

Figure 47 Select Post-Paid Billing



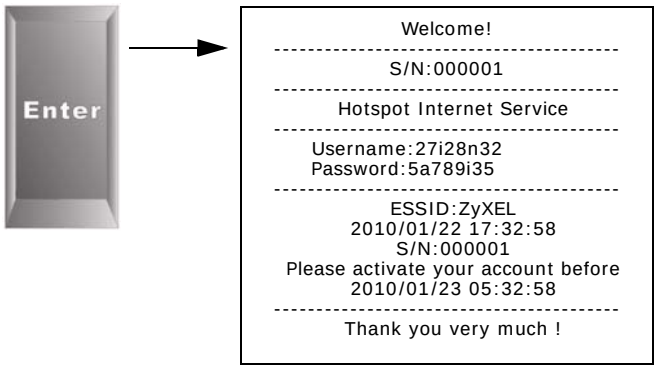
3 Click **ADVANCED > KEYPAD**.

4 Define your post-paid billing plan and click **Apply**.

Figure 48 Define Post-Paid Billing Plan

5 Use the keypad to create subscriber accounts. Press [ENTER] to generate a new subscriber account and print the account's information. The account information includes a serial number, password and the time the account was created.

Figure 49 Post-Paid Account Printout Example



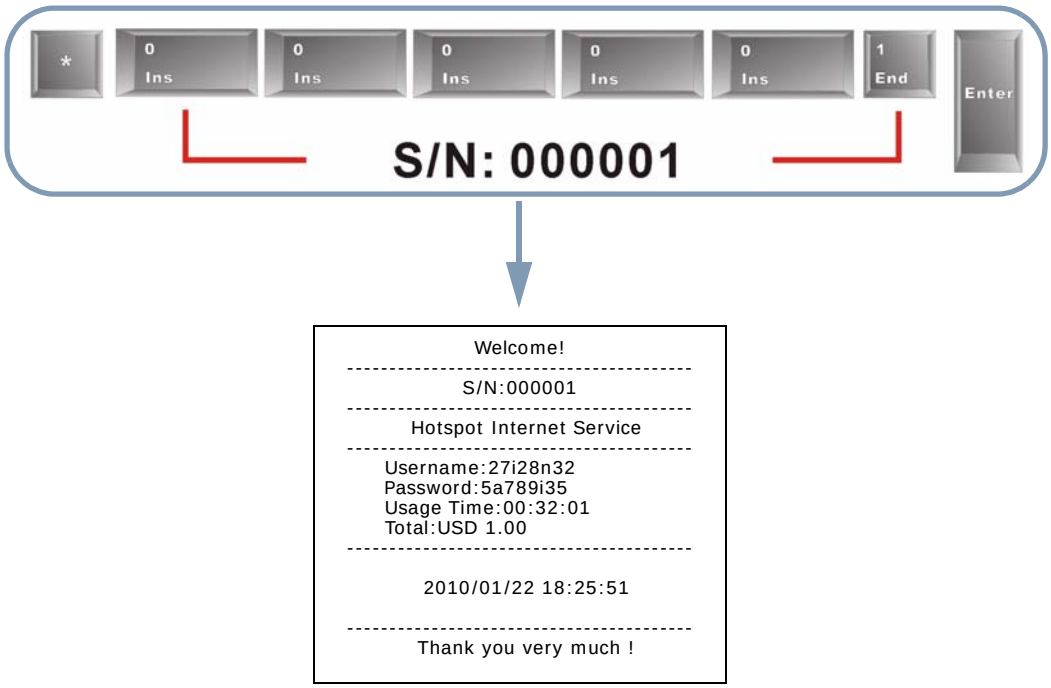
6 When a subscriber is done using the Internet service, press the following to print a bill.

*

Serial number

[ENTER]

Figure 50 Post-Paid Account Bill Printout Example



13

Customization

13.1 Overview

Use these screens to tailor what displays on the subscriber interface. You can configure the subscriber login screen, which logo displays; an information window, the account printouts and the credit card billing interface.

13.1.1 What You Can Do in this Chapter

- Use the **Login Page** screen (Section 13.2 on page 120) to customize the subscriber login screen.
- Use the **Logo** screen (Section 13.3 on page 127) to upload your logo file.
- Use the **Information Windows** screen (Section 13.4 on page 128) to customize the information window on the subscriber's computer after a successful login.
- Use the **Account Printout** screen (Section 13.5 on page 129) to customize the account printout.
- Use the **Credit Card** screen (Section 13.6 on page 134) to customize the subscriber credit card billing interface.

13.1.2 What You Need to Know

The following terms and concepts may help as you read through the chapter.

Login Page

When subscriber authentication is activated in the **Authentication** screen, the subscriber login screen is the first screen that all subscribers see when trying to access the Internet. You can configure walled garden web addresses for web sites that all subscribers are allowed to access without logging in (refer to Chapter 17 on page 153).

Information Windows

You can set the N4100 to display an information window after a subscriber has successfully logged in. This information window shows the amount of time a subscriber has used or the time the subscriber still has to access the Internet.

The subscriber information window varies depending on the account type and billing configuration you set on the N4100.

The information window displays the amount of time used for Internet access on a super subscriber account. With other types of account, the information window displays the amount of time a subscriber still has to use for Internet access.

When you set the system to allow accounts to be replenished, the information window displays a Replenish button.

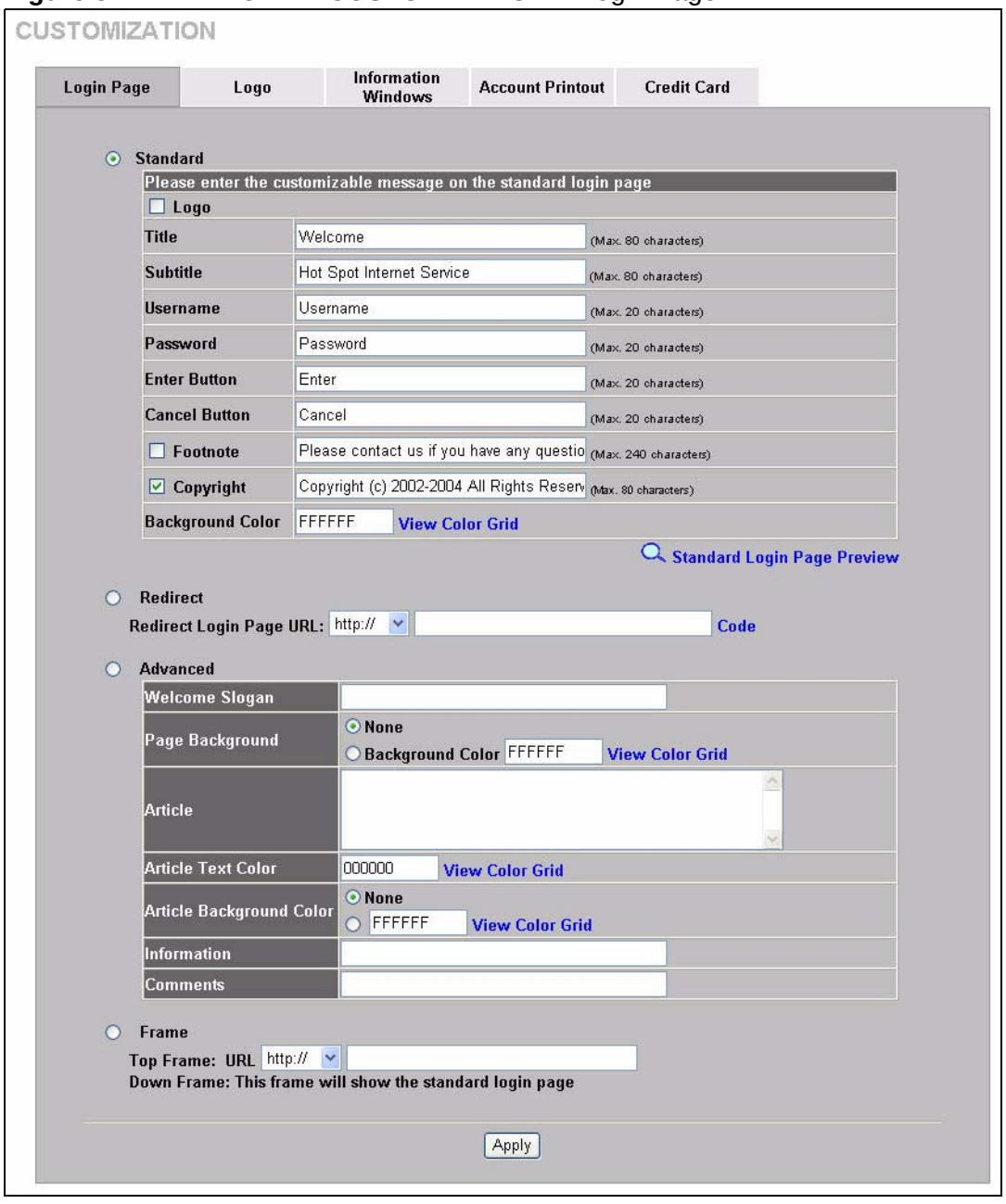
When you set the billing type to accumulation, the information window displays a Logout button.

13.2 The Login Page Screen

Click **ADVANCED > CUSTOMIZATION > Login Page** to open this screen.

The N4100 provides different formats in which you can customize the login screen: **Standard**, **Redirect**, **Advanced** and **Frame**.

Figure 51 ADVANCED > CUSTOMIZATION > Login Page



13.2.1 Standard

Select the **Standard** option to use the N4100's pre-configured, default simple login screen.

Figure 52 ADVANCED > CUSTOMIZATION > Login Page: Standard

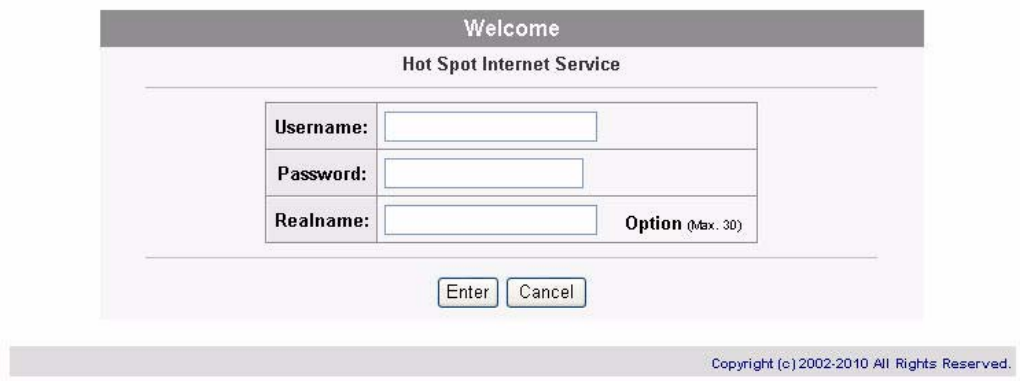
The following table describes the related labels.

Table 18 ADVANCED > CUSTOMIZATION > Login Page: Standard

LABEL	DESCRIPTION
Standard	Select this option to set the N4100 to display the standard subscriber login screen.
Logo	Select this check box to display your logo on the subscriber login screen. See Section 13.3 on page 127 for how to upload a logo file.
Title	Enter the title name (up to 80 characters) on the subscriber login page.
Subtitle	Enter the subtitle name (up to 80 characters) on the subscriber login screen.
Username	Enter the name of the **Username** field on the subscriber login screen.
Password	Enter the name of the **Password** field on the subscriber login screen.
Enter Button	Enter the name for the **Enter** button on the subscriber login screen.
Cancel Button	Enter the name for the **Cancel** button on the subscriber login screen.
Footnote	Select the check box to add a footnote to the subscriber login page. Enter the footnote (up to 240 characters) in the field provided.
Copyright	Select the check box to add copyright information to the bottom of the subscriber login page. Enter the copyright information (up to 80characters) in the field provided.
Background Color	Enter a hexadecimal number to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Standard Login Page Preview	Click this link to preview the standard login screen in a new browser window.

The following figure shows an example of what a subscriber sees when logging in.

Figure 53 Subscriber Login Page Example: Standard



13.2.2 Redirect

You can set the N4100 to redirect the subscribers to another login screen. This allows you to use your own customized login screen that you have created with a website-design tool. This gives you the ability to use a company login page and/or add multimedia features such as flash.

Select the **Redirect** option in the **Login Page** screen.

Figure 54 ADVANCED > CUSTOMIZATION > Login Page: Redirect

The following table describes the related labels.

Table 19 ADVANCED > CUSTOMIZATION > Login Page: Redirect

LABEL	DESCRIPTION
Redirect	Select this option to direct the subscriber to another login screen.
Redirect Login Page URL	Specify the web site address to which the N4100 directs the subscribers for logins. The web site must be on the WAN. You can use up to 350 ASCII characters.
Code	Click **Code** to display the source code of the web page you specify. The redirect subscriber login screen must include the HTML source code in the default sample page in order for the subscriber login screen to send the subscribers' usernames and passwords to the N4100.

Figure 55 ADVANCED > CUSTOMIZATION > Login Page: Redirect > Code

Redirect Login Page Code

If you need the credit card icons to be displayed on your customized login page, please integrate the sample code with below image links.
Size: 54 x 35 pixels
1.VISA: http://1.1.1.1:8080/card_visa.gif
2.Master Card: http://1.1.1.1:8080/card_master.gif
3.American Express: http://1.1.1.1:8080/card_ae.gif
4.Discover: http://1.1.1.1:8080/card_discover.gif

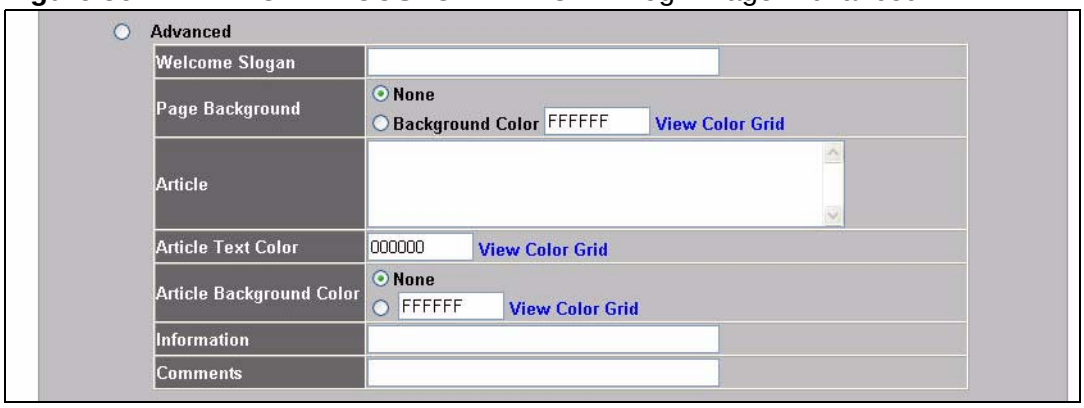
```
<html>
<body style="font-family: Arial" bgcolor="#FFFFFF">
<form method="post" action="http://1.1.1.1/login.cgi" name="apply">
<div align="center">
<table cellSpacing="0" cellPadding="0" width="50%" borderColorLight="#8e8e8e"
border="1">
<tr>
<td align="center" width="100%" bgColor="#8e8e8e" height="24">
<font face="Arial, Helvetica, sans-serif" size="2" color="#FFFFFF"><b>Welcome</b></font>
</td>
</tr>
<tr>
<td align="center"> <table cellSpacing="0" cellPadding="4" width="100%"
bgColor="#FFFFFF" border="0"> <tr>
<td align="right" width="35%" style="font-family: Arial, Helvetica, sans-serif; font-size: 12pt">
<font color="#000000" size="2"><b>Username:</b></font>
</td>
<td width="65%">
<input type="text" name="username" size="25">
</td>
</tr>
<tr>
<td align="right" width="35%" style="font-family: Arial, Helvetica, sans-serif; font-size: 12pt">
<font color="#000000" size="2"><b>Password:</b></font>
</td>
<td width="65%">
<input type="password" name="password" size="25">
</td>
</tr>
<tr>
<td align="right" width="35%" style="font-family: Arial, Helvetica, sans-serif; font-size: 12pt">
<font color="#000000" size="2"><b>Realname:</b></font>
</td>
<td width="65%">
<input type="text" name="realname" size="25">
<font color="#000000" size="2"><b>Option</b></font>
<font color="#000000" size="1"> (Max. 30)</font>
</td>
</tr>
<tr>
<td align="center" width="100%" style="font-family: Arial; font-size: 12pt" bgcolor="#F7F7F7"
colspan="2">
<input type="submit" name="apply" value="Enter" style="font-family: Arial">
<input type="reset" name="clear" value="Clear" style="font-family: Arial">
</td>
</tr>
</table>
</td>
</tr>
</table>
</div>
<div align="center">
<table border="0" width="100%" cellspacing="0" cellpadding="0">
<tr>
<td align="center" width="100%" height="30">
<font color="#000000" size="2">
<a href="https://1.1.1.1/creditcard.cgi"><b>or Click here to pay by credit card</b></a>
<font></td>
</tr>
</table>
</div>
</form>
</body>
</html>
```

Close

13.2.3 Advanced

Select the **Advanced** option to customize a login screen where you can create a welcome slogan and add advertising information.

Figure 56 ADVANCED > CUSTOMIZATION > Login Page: Advanced



The following table describes the related labels.

Table 20 ADVANCED > CUSTOMIZATION > Login Page: Advanced

LABEL	DESCRIPTION
Advanced	Select this option to set the N4100 to display the advanced subscriber login screen.
Welcome Slogan	Enter a welcome message (up to 80 characters long) in the text box provided.
Page Background	Select **None** to set the background color of the login screen to white (the default). Select **Background Color** to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 1024 characters long) in the text box. This is useful for advertisements or announcements.
Article Text Color	Set the color of the article text block background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Article Background Color	Select **None** to set the article background color of the login screen to white (the default). Select the other radio button to set the color of the login screen's article background to the color specified, for example, enter '000000' for black. Click **View Color Grid** to display a list of web-friendly colors and corresponding hexadecimal values.
Information	Enter information such address and telephone or fax numbers in the text box provided. Up to 80 characters allowed.
Comments	Enter any comments (up to 80 characters long) in the text box provided.

Figure 57 Subscriber Login Page Example: Advanced

13.2.4 Frame

The **Frame** login screen splits the login screen into two frames: top and bottom. You can specify a web site to be displayed in the top frame with the user name and password prompt displayed in the bottom frame. The frame login screen is useful for you to link to a web site (such as the company web site) as your welcome screen. In addition, you can externally design a web page with images and/or advanced multimedia features.

Select the **Frame** option in the **Login Page** screen.

Figure 58 ADVANCED > CUSTOMIZATION > Login Page: Frame

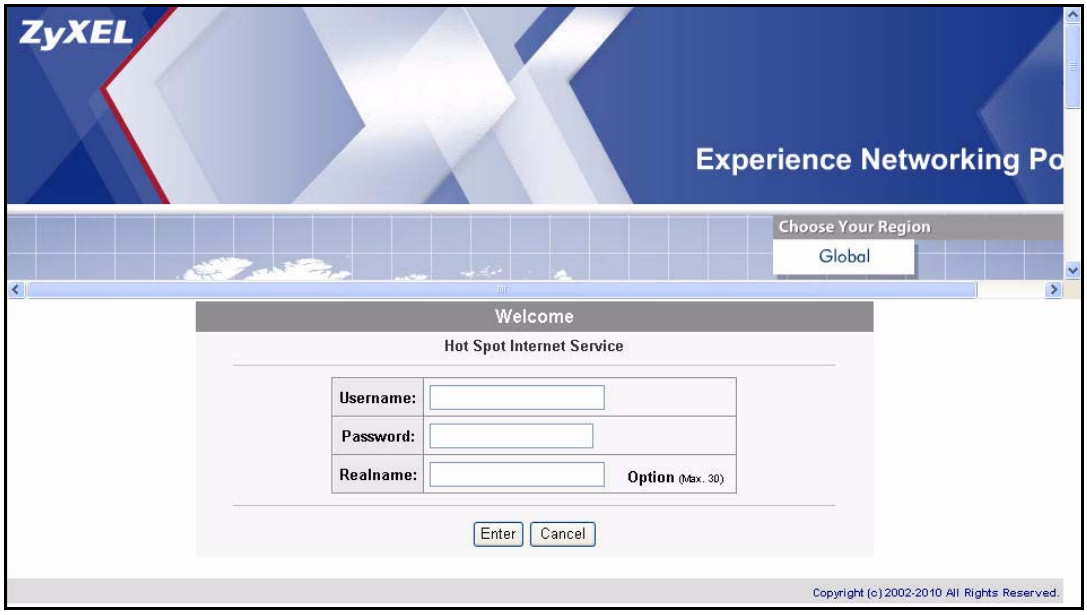
The following table describes the related labels.

Table 21 ADVANCED > CUSTOMIZATION > Login Page: Frame

LABEL	DESCRIPTION
Frame	Select this option to configure and set the N4100 to display the subscriber login screen in two frames.
Top Frame	Enter a web site address in the **URL Link** field, for example, http://www.zyxel.com. You can use up to 350 ASCII characters.
Down Frame	The bottom frame displays the standard subscriber login page.

The following figure shows a framed subscriber login screen example.

Figure 59 Subscriber Login Page Example: Frame

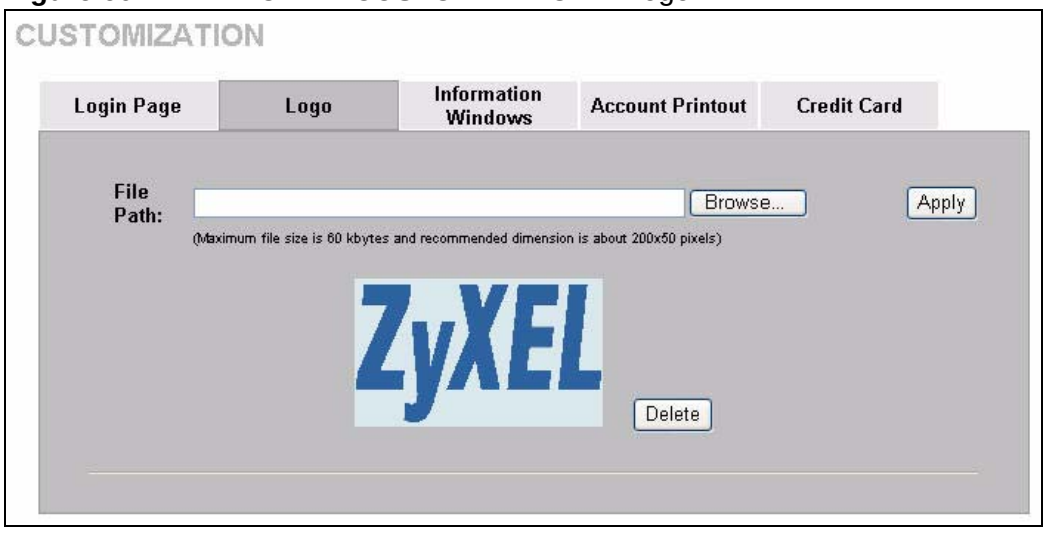


13.3 The Logo Screen

This function allows you to upload a file containing your logo. The logo can be shown on the standard login page and the account printout when printing with a network-connected printer.

To upload your logo file, click **ADVANCED > CUSTOMIZATION > Logo** to open this screen.

Figure 60 ADVANCED > CUSTOMIZATION > Logo



The following table describes the labels in this screen.

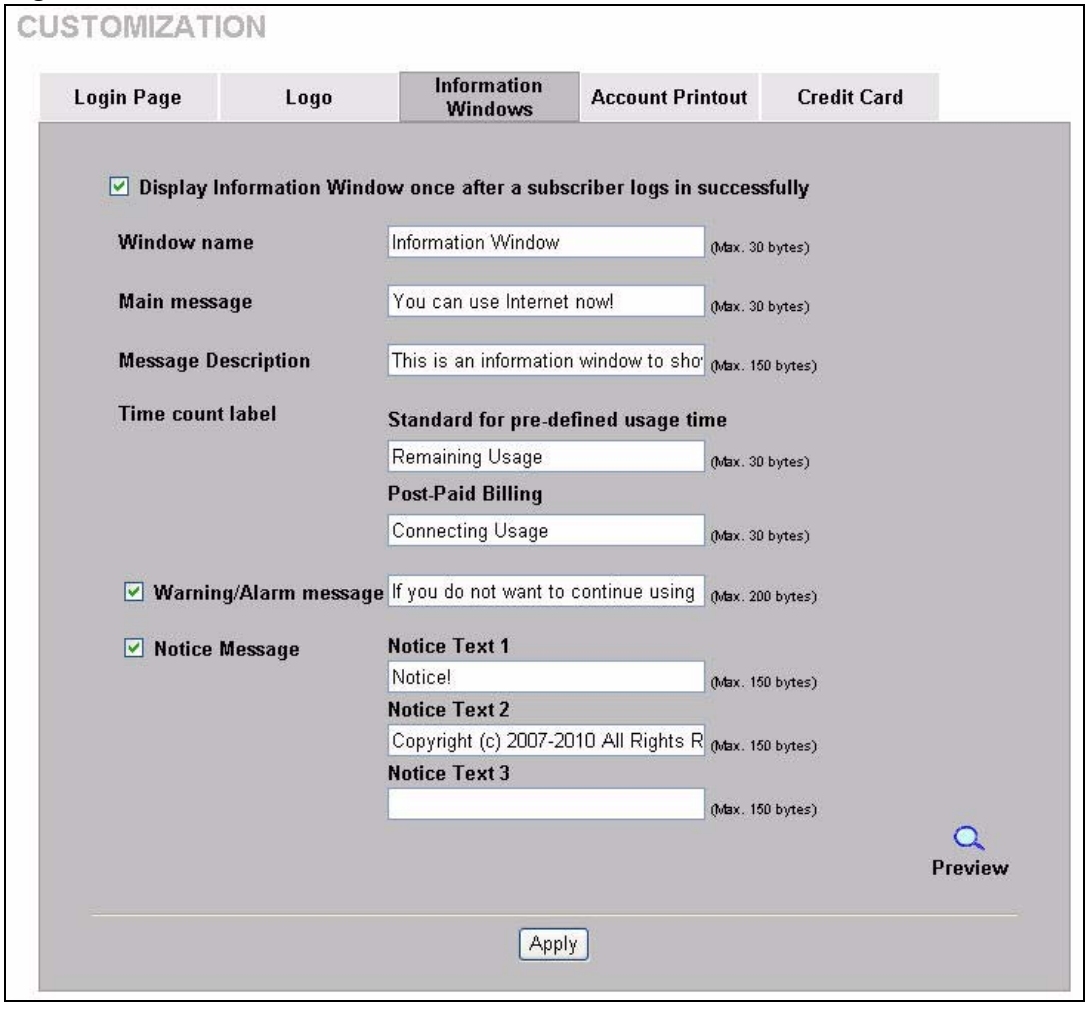
Table 22 ADVANCED > CUSTOMIZATION > Logo

LABEL	DESCRIPTION
File Path	Enter the file path name of the logo file or click **Browse** to search for it.
Apply	Click **Apply** to upload your logo file to the N4100.
Delete	Click **Delete** to remove the logo you uploaded.

13.4 The Information Windows Screen

To upload your logo file, click **ADVANCED > CUSTOMIZATION > Information Windows** to open this screen.

Figure 61 ADVANCED > CUSTOMIZATION > Information Windows



The following table describes the labels in this screen.

Table 23 ADVANCED > CUSTOMIZATION > Information Windows

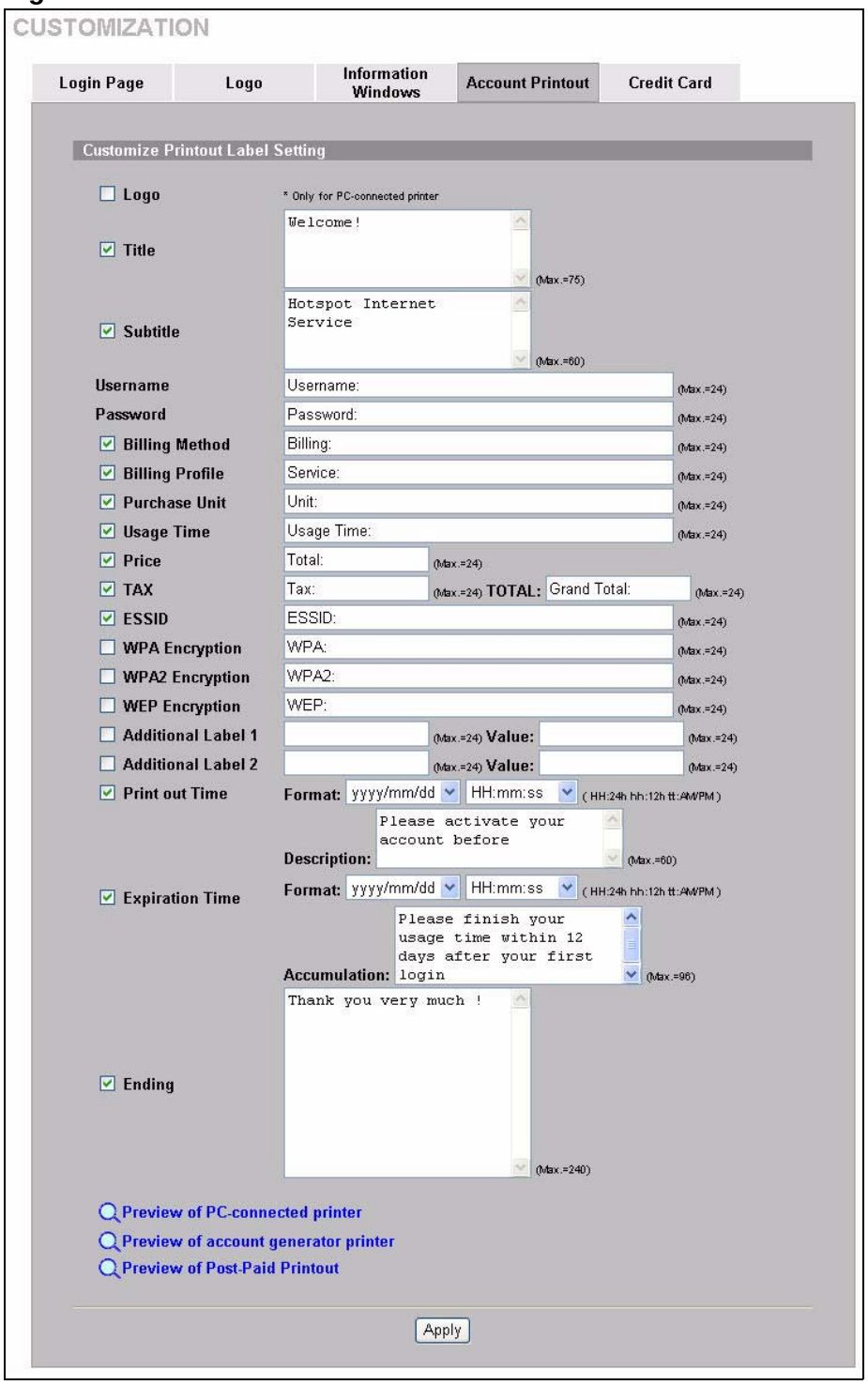
LABEL	DESCRIPTION
Display Information Window once after a subscriber logs in successfully	Select this check box to display the information window on the subscriber's computer after a successful login.
Window name	Enter a descriptive name (up to 30 characters) as the title of the window.
Main message	Enter a short message (up to 30 characters).
Message Description	Enter a short description about the information window.
Time count label	**Standard for pre-defined usage time** -Enter the label for the field displaying the remaining time. This field displays when the N4100 is set to use pre-paid billing. **Post-Paid Billing** -Enter the label for the field displaying the amount of time used. This field displays when the N4100 is set to use post-paid billing.
Warning/ Alarm Message	Select this check box to display the warning message that you enter in the text box provided.
Notice Message	Select this check box to display any additional message(s) that you enter in the text box(es) provided. You can specify up to three additional messages (such as discount information) in the information window.
Preview	Click **Preview** to display a preview of the information window.
Apply	Click **Apply** to save your changes back to the N4100.

13.5 The Account Printout Screen

After you have created the subscriber accounts, you can print out the account information.

To customize the account printout, click **ADVANCED > CUSTOMIZATION > Account Printout** to display the screen as shown.

Figure 62 ADVANCED > CUSTOMIZATION > Account Printout



The following table describes the labels in this screen.

Table 24 ADVANCED > CUSTOMIZATION > Account Printout

LABEL	DESCRIPTION
Logo	Select this check box to print your logo on the account statement when you use a network-connected printer. See Section 13.3 on page 127 for how to upload a logo file.
Title	Select this check box and enter a title for the printout. You can enter up to 75 printable English, French, Italian, German and/or Spanish characters.
Subtitle	Select this check box and enter a subtitle for the printout. You can enter up to 60 printable English, French, Italian, German and/or Spanish characters.
Username	Enter the label name for the field displaying the account username.
Password	Enter the label name for the field displaying the account password.
Billing Method	Select this check box and enter the label name for the field displaying the method for billing.
Billing Profile	Select this check box and enter the label name for the field displaying the name for the billing profile used.
Purchase Unit	Select this check box and enter the label name for the field displaying the number of time units purchased.
Usage Time	Select this check box and enter the label name for the field displaying the amount of time an account is allowed for Internet access.
Price	Select this check box and enter the label name to display the specified label name for the field displaying the price.
TAX	Select this check box and enter a label name for the field displaying the tax.
TOTAL	Enter a label name for the field displaying the sum of the price and the tax.
ESSID	Select this check box and enter a label name for the field displaying the wireless LAN's Extended Service Set Identifier (**ESSID**).
WPA Encryption	Select this check box and enter a label name for the field displaying the Wi-Fi Protected Access (**WPA Encryption**) key. This field displays on the account statement when the N4100 is using WPA data encryption with a pre-shared key.
WPA2 Encryption	Select this check box and enter a label name for the field displaying the Wi-Fi Protected Access 2 (**WPA2 Encryption**) key. This field displays on the account statement when the N4100 is using WPA data encryption with a pre-shared key.
WEP Encryption	Select this check box and enter a label name for the field displaying the Wired Equivalent Privacy (**WEP Encryption**) key. This field displays on the account statement when the N4100 is using WEP data encryption.
Additional Label 1 and 2	Select this check box and enter a label name to display the specified label name(s) for the field(s) displaying any additional information.
Value	Type any additional information that you want to display.
Print out Time	Select this check box to display the time an account is printed out. Select date and time formats from the drop-down list boxes.

Table 24 ADVANCED > CUSTOMIZATION > Account Printout

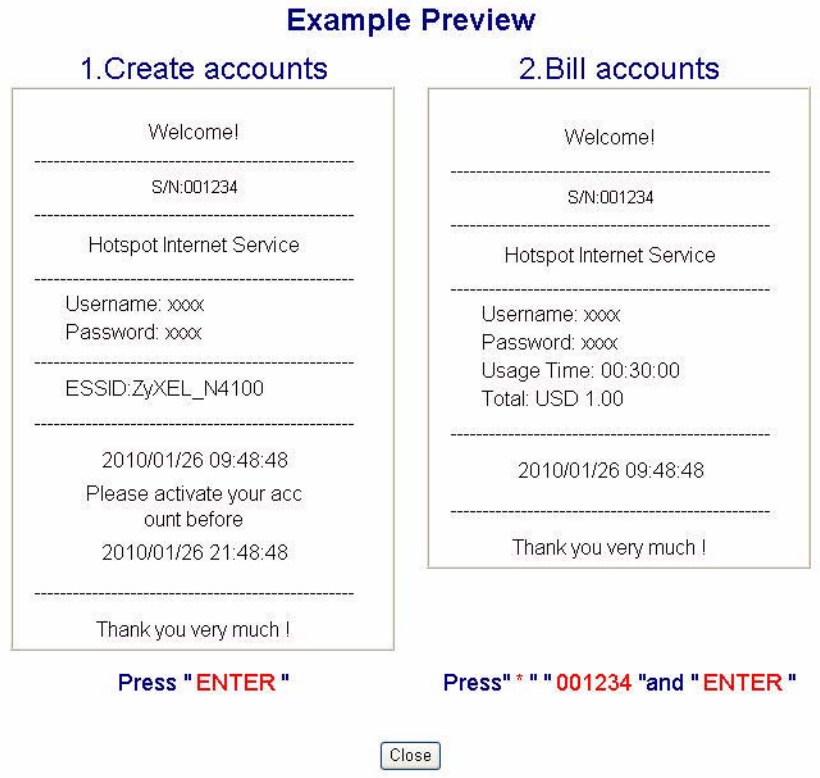
LABEL	DESCRIPTION
Description	Enter an explanation for the subscriber about the deadline for activating the account. You can enter up to 60 printable English, French, Italian, German and/or Spanish characters.
Expiration Time	Select this check box to display the time an account expires. Enter an explanation for the subscriber about the account's expiration. Select date and time formats from the drop-down list boxes.
Accumulation	This message displays in the account printout when you set the N4100 to use accumulation billing. Enter an explanation for the subscriber about the deadline for using the purchased time. You can enter up to 96 printable English, French, Italian, German and/or Spanish characters.
Ending	Select this check box to display a message at the end of the printout. Enter the message in the text box provided. You can enter up to 240 printable English, French, Italian, German and/or Spanish characters.
Preview of PC-connected printer	Click **Apply** to save your changes and then click this link to display a preview of an account printout, as it would print on a printer connected to a network computer.
Preview of account generator printer	Click this link to display a preview of an account printout, as it would print on an external account generator printer (or the statement printer).
Preview of Post-Paid Printout	Click this link to display a preview of a post-paid account printout.
Apply	Click **Apply** to save your changes back to the N4100.

The following figures show account printout examples.

Figure 63 Preview of PC-connected Printer Example

Figure 64 Preview of Account Generator Printer Example

Figure 65 Preview of Post-Paid Printout Example



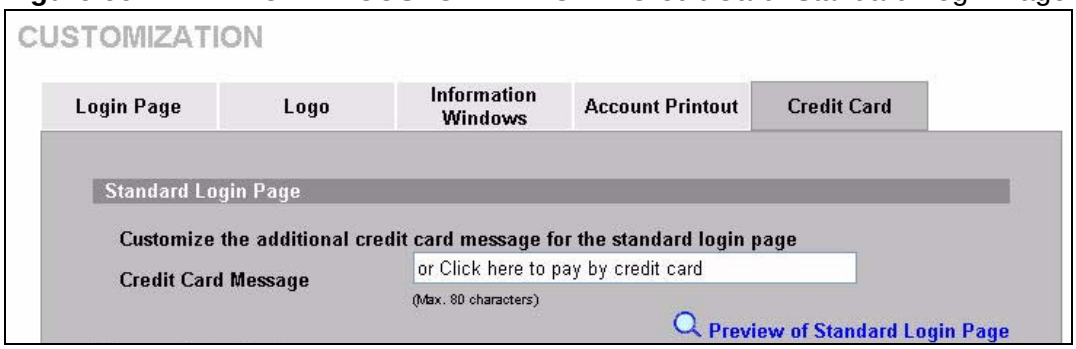
13.6 The Credit Card Screen

When you configure the N4100 to use credit card billing, you can use this page to customize the subscriber billing interface. Click **ADVANCED > CUSTOMIZATION > Credit Card** to display the screen as shown.

13.6.1 Credit Card Standard Login Page

Use this section to customize the credit card message that displays on the standard login page.

Figure 66 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page



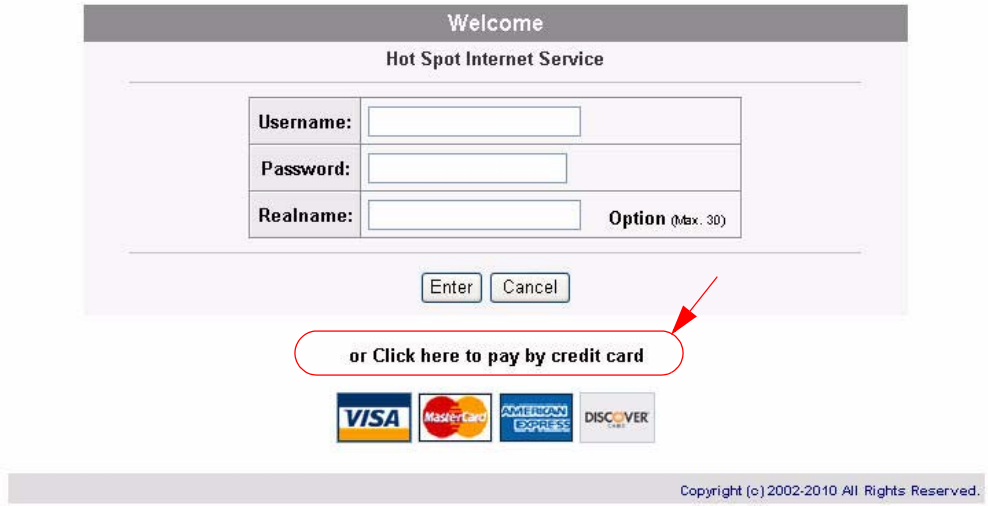
The following table describes the labels in this screen.

Table 25 ADVANCED > CUSTOMIZATION > Credit Card: Standard Login Page

LABEL	DESCRIPTION
Credit Card Message	Enter the credit card message that you want to display on the standard login page. The message you configure here only displays on the standard login page when you configure and enable credit card service.
Preview of Standard Login Page	Click this link to display a preview of the standard login page.

The following figure shows an example of the standard login page with the credit card option.

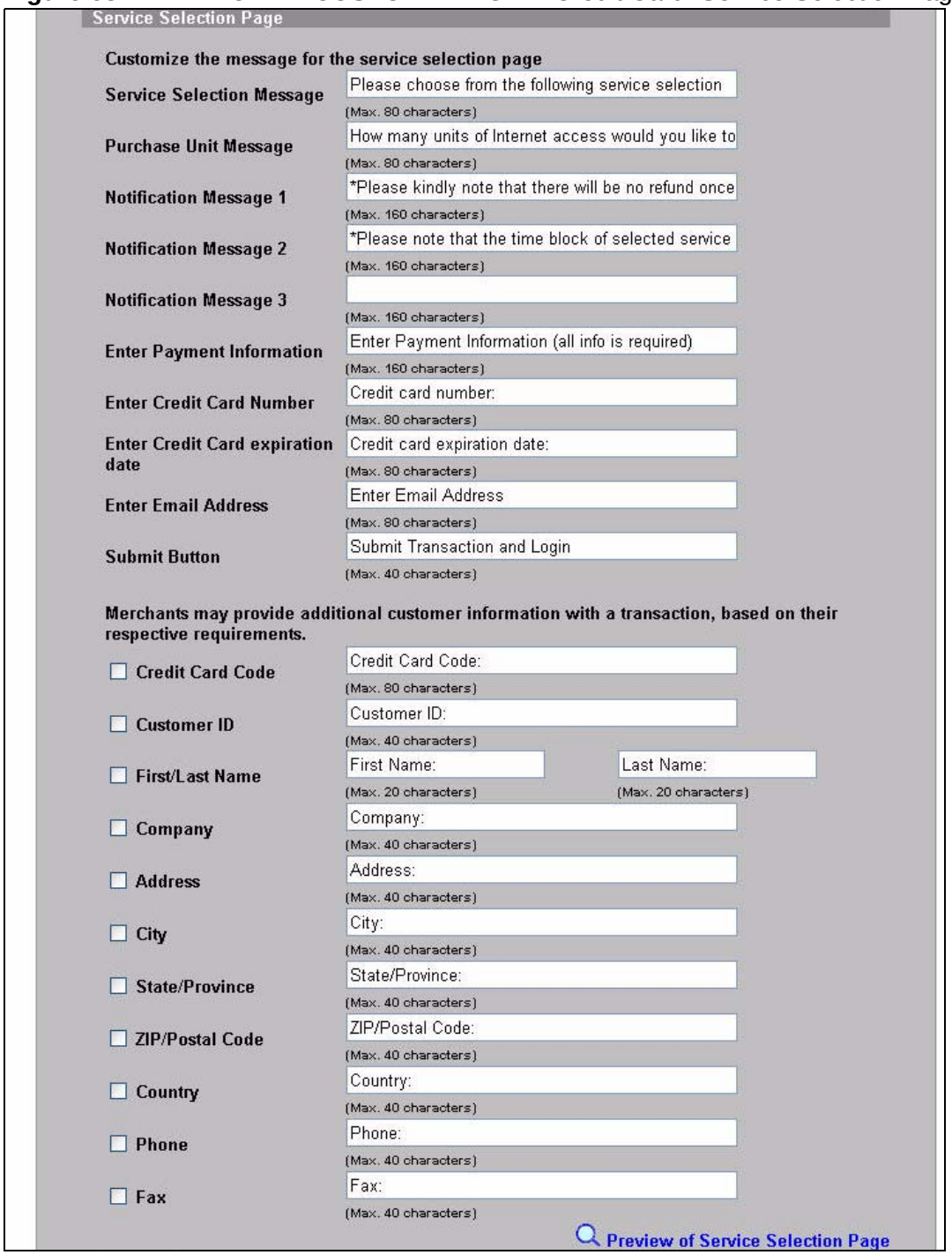
Figure 67 Credit Card Standard Login Page Example



13.6.2 Credit Card Service Selection Page

Use this section to customize the credit card billing interface that displays on the subscriber's screen.

Figure 68 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page



The following table describes the labels in this screen.

Table 26 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page

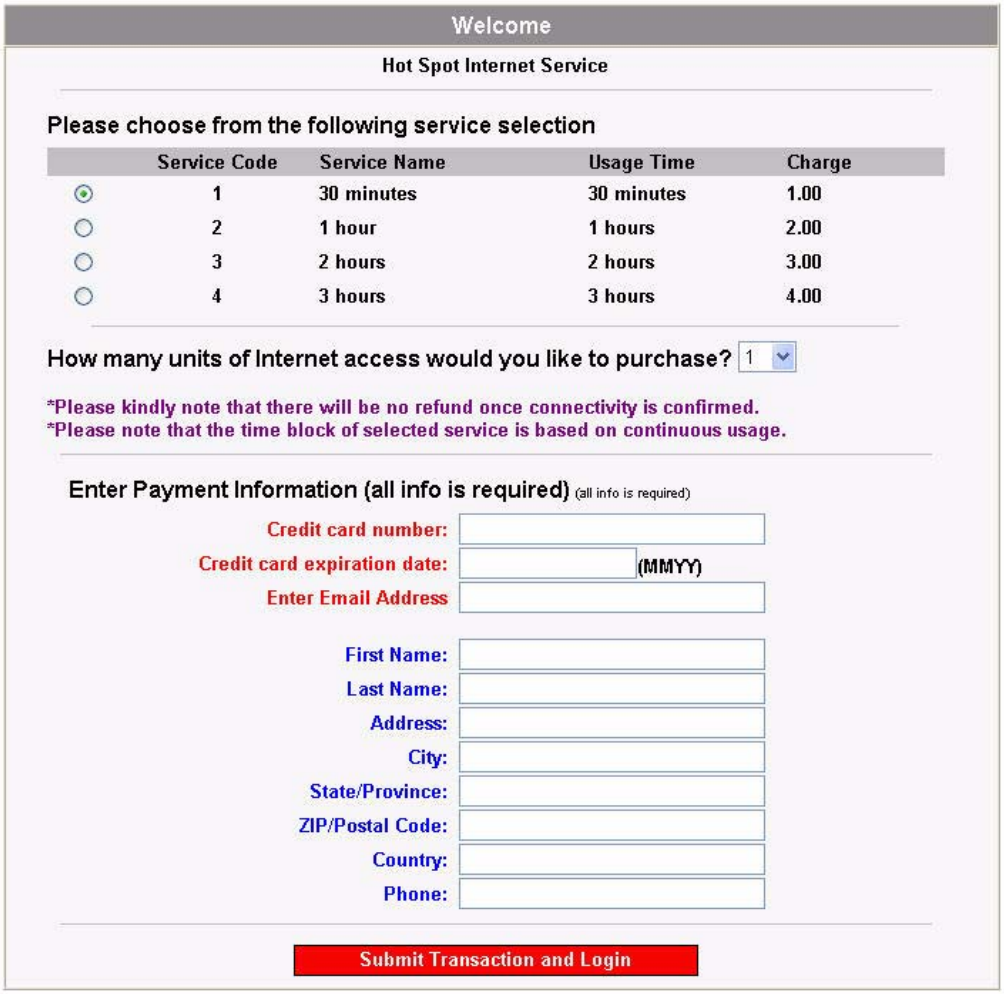
LABEL	DESCRIPTION
Service Selection Message	Enter a message to instruct the subscribers to select a billing profile. Use the Billing screen to configure and activate billing profiles. Only active billing profiles display on the subscriber's screen.
Purchase Unit Message	Enter a message to instruct the subscribers to select the number of time units to purchase.
Notification Message (1-3)	Enter an additional message(s) regarding the purchase of Internet access. For example, you may enter a refund policy.
Enter Payment Information	Enter a message to instruct the subscribers to provide the required payment information.
Enter Credit Card Number	Enter a label name for the field where the subscriber enters the credit card number.
Enter Credit Card expiration date	Enter a label name for the field where the subscriber enters the credit card's expiration date.
Enter Email Address	Enter a label name for the field where the subscriber enters an e-mail address.
Submit Button	Enter a label name for the button the subscriber clicks to submit the transaction information.
Optional Information	You may select check boxes to display additional fields on the credit card billing interface that displays on the subscriber's screen.
Credit Card Code	Credit cards have an authorization code on the back. Select this check box if you want the screen to display a credit card authorization code field. Enter the label name for the field that requests the subscriber's credit card authorization code.
Customer ID	Select this check box if you want the screen to display a customer ID field. A customer with an Authorize.net-issued ID can enter it in the field. Enter the label name for the field that requests the subscriber's ID.
First/Last Name	Select this check box if you want the screen to display the first and last name fields. Enter the label names for the fields that request the subscriber's first and last name.
Company	Select this check box if you want the screen to display a company field. Enter the label name for the field that requests the name of the subscriber's company.
Address	Select this check box if you want the screen to display an address field. Enter the label name for the field that requests the subscriber's address.
City	Select this check box if you want the screen to display a city field. Enter the label name for the field that requests the name of the city where the subscriber lives.
State/Province	Select this check box if you want the screen to display a state or province field. Enter the label name for the field that requests the subscriber's state or province.
ZIP/ Postal Code	Select this check box if you want the screen to display a zip or postal code field. Enter the label name for the field that requests the subscriber's zip or postal code.

Table 26 ADVANCED > CUSTOMIZATION > Credit Card: Service Selection Page

LABEL	DESCRIPTION
Country	Select this check box if you want the screen to display a country field. Enter the label name for the field that requests the subscriber's country.
Phone	Select this check box if you want the screen to display a phone number field. Enter the label name for the field that requests the subscriber's phone number.
Fax	Select this check box if you want the screen to display a fax number field. Enter the label name for the field that requests the subscriber's fax number.
Preview of Service Selection Page	Click this link to display a preview of the credit card service selection page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card service selection page.

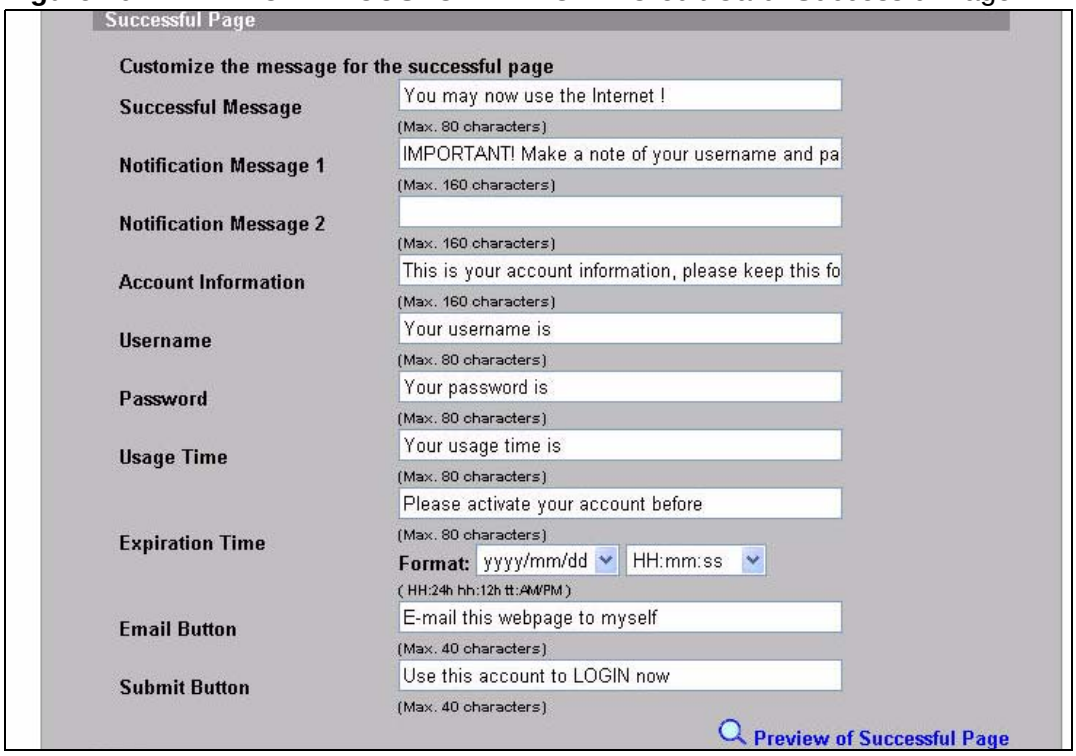
Figure 69 Credit Card Service Selection Page Preview



13.6.3 Credit Card Successful Page

Use this section to customize the page that displays on the subscriber's screen if an attempt to use a credit card is successful.

Figure 70 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page



The following table describes the labels in this screen.

Table 27 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page

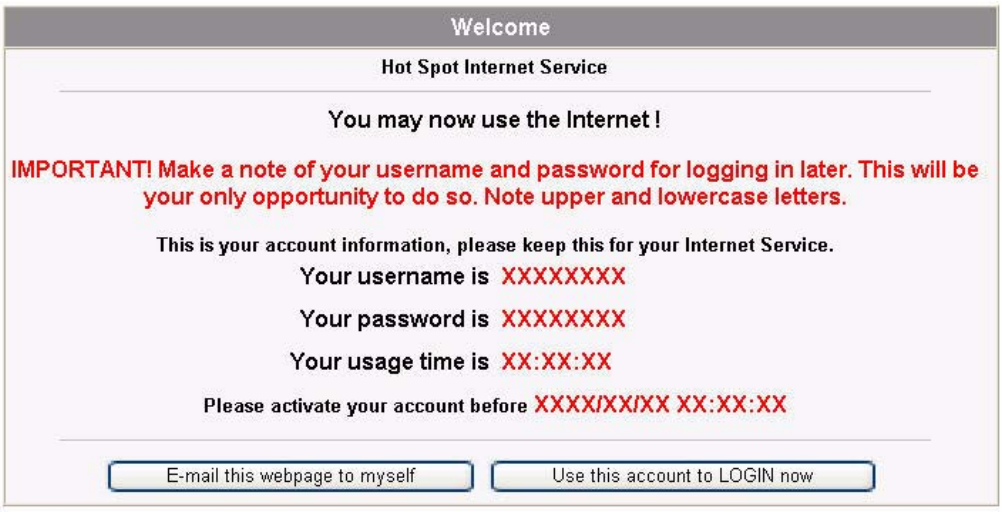
LABEL	DESCRIPTION
Successful Message	Enter a message to tell the subscriber that the online credit card transaction was successful.
Notification Message (1-2)	Enter an additional message(s) regarding the subscriber's use of the purchased Internet access.
Account Information	Enter a message to tell the subscriber about the account information in the following fields.
Username	Enter a label name for the field that displays the subscriber's user name.
Password	Enter a label name for the field that displays the subscriber's password.
Usage Time	Enter a label name for the field that displays the subscriber's purchased period of Internet access.
Expiration Time	Enter the label name for the field displaying when the account expires. Select date and time formats from the **Format** drop-down list boxes.
Email Button	Enter a label name for the button the subscriber can click to send a copy of the account information to the subscriber's e-mail account.

Table 27 ADVANCED > CUSTOMIZATION > Credit Card: Successful Page

LABEL	DESCRIPTION
Submit Button	Enter a label name for the button the subscriber clicks to log into the account.
Preview of Successful Page	Click this link to display a preview of the credit card transaction successful page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card transaction successful page.

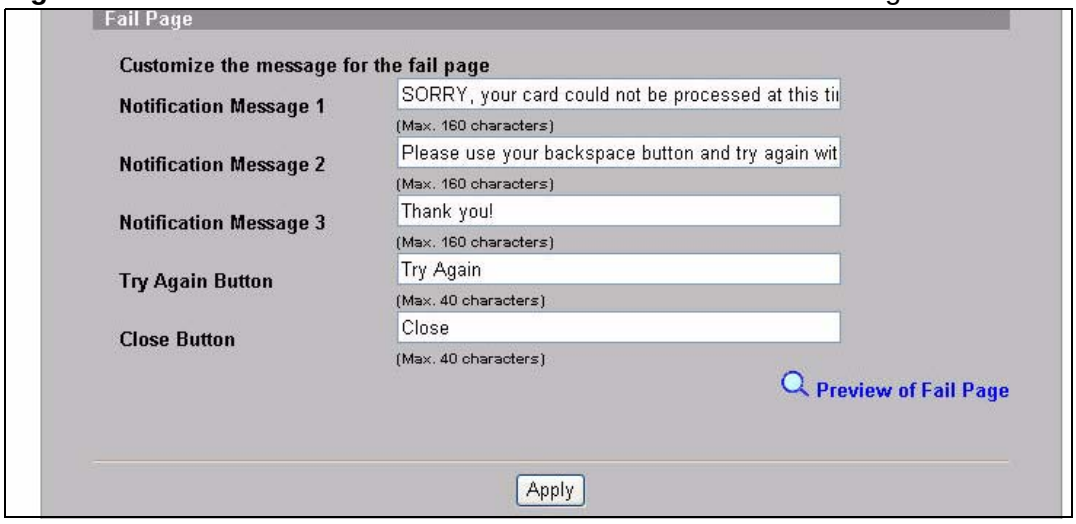
Figure 71 Credit Card Successful Page Preview



13.6.4 Credit Card Fail Page

Use this section to customize the page that displays on the subscriber's screen if an attempt to use a credit card fails.

Figure 72 ADVANCED > CUSTOMIZATION > Credit Card: Fail Page



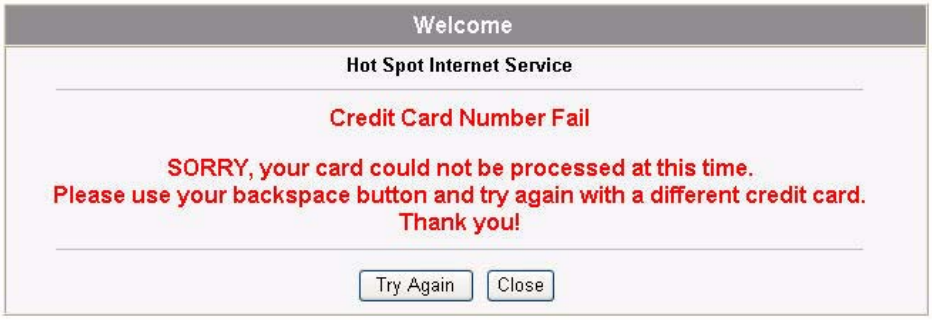
The following table describes the labels in this screen.

Table 28 ADVANCED > CUSTOMIZATION > Credit Card: Fail Page

LABEL	DESCRIPTION
Notification Message (1-3)	Enter a message(s) to tell the subscriber that the online credit card transaction failed and how to try again.
Try Again Button	Enter a label name for the button that takes the subscriber back to the credit card service selection page.
Cancel Button	Enter a label name for the button that the subscriber can use to stop attempting to make a credit card transaction and close the credit card interface.
Preview of Fail Page	Click this link to display a preview of the credit card transaction failed page that will display on the subscriber's screen.

The following figure shows an example preview of the credit card transaction failed page.

Figure 73 Credit Card Failed Page Preview



14

Pass Through

14.1 Overview

You can set up two types of pass through on the N4100: by device or by web site address.

You can set the N4100 to allow specific computers on the LAN (based on the IP or MAC address) to access the Internet without prompting for a user name and password. This feature is useful, for example, if you want to set up computers to provide free Internet access in the VIP room or for sponsors in events.

To allow global access to web sites, specify the web site address (by IP address or URL) that any user can access without logging in. This is similar to the walled garden feature, but without displaying the web site link(s) in the subscriber login screen. You have to inform the users about which web sites they can access for free.

14.1.1 What You Can Do in this Chapter

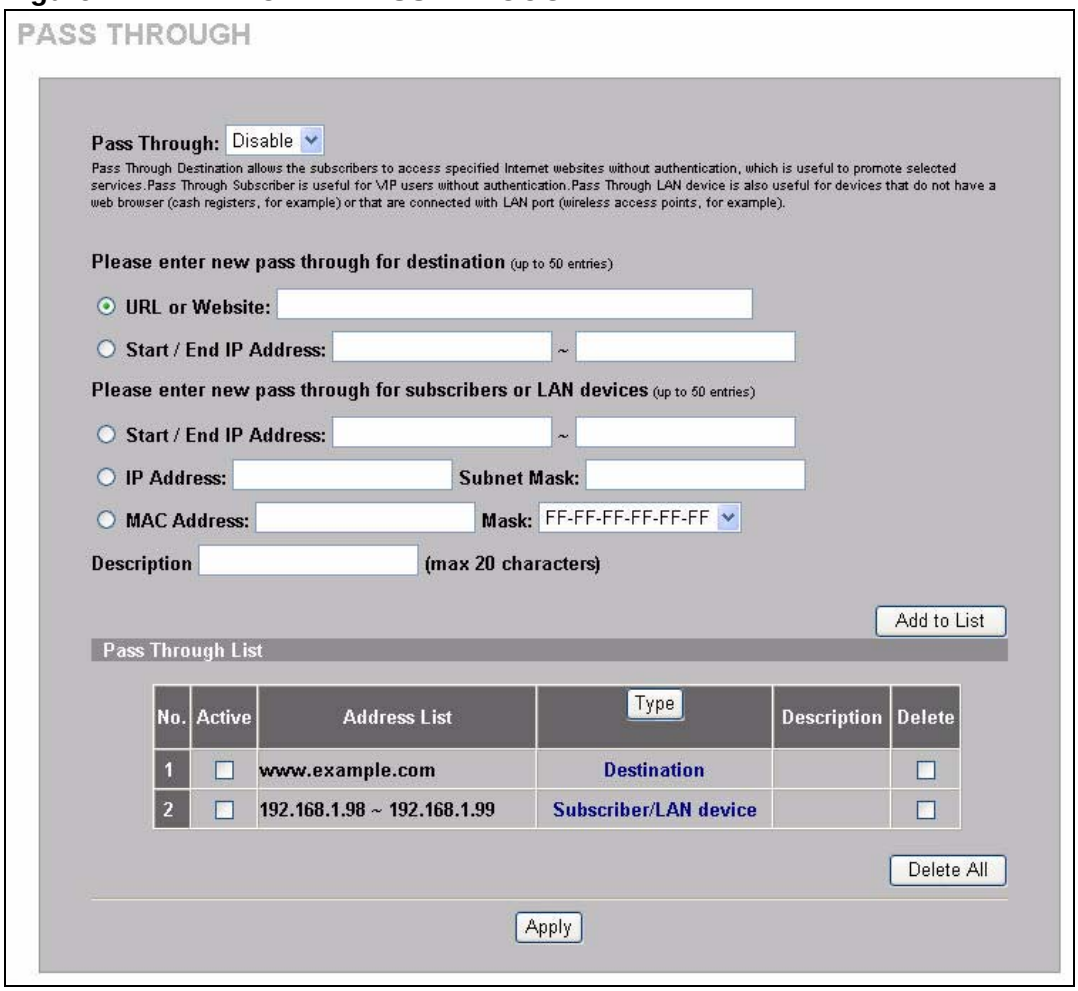
Use the **Pass Through** screen (Section 13.2 on page 120) to specify devices that can have traffic pass through the N4100.

14.2 The Pass Through Screen

Click **ADVANCED > PASS THROUGH** to open this screen.

Note: Pass through has priority over filtering.

Figure 74 ADVANCED > PASS THROUGH



The following table describes the labels in this screen.

Table 29 ADVANCED > PASS THROUGH

LABEL	DESCRIPTION
Pass Through	Enable pass through to allow all users to access specific web sites (or IP addresses) and/or allow packets from specific computers to go through the N4100 without prompting for a user name and password.
Please enter new pass through for destination (up to 50 entries) The destinations should be on the WAN.	
URL or Website	Select this option to allow users to access a website without entering a user name or password. Enter the URL (up to 350 ASCII characters) of the web site to which you want to allow access.
Start / End IP Address	Select this option to allow users to access a range of IP addresses without entering a user name or password. Enter the beginning and ending IP addresses in dotted decimal notation.

Table 29 ADVANCED > PASS THROUGH

LABEL	DESCRIPTION
Please enter new pass through for subscribers or LAN devices (up to 50 entries)	
Start / End IP Address	Select this option to allow packets from computers with a specific range of IP addresses to pass through the N4100 without entering a user name and password. Enter the beginning and ending IP addresses IP addresses in dotted decimal notation, for example, 192.168.1.10.
IP Address	Select this option to allow packets from a computer with a specific IP address to pass through the N4100 without entering a user name and password. You can specify a range of IP addresses on a network by specifying an IP address here and a subnet mask in the **Subnet Mask** field. Enter the IP address in dotted decimal notation, for example, 192.168.1.10.
Subnet Mask	Enter the subnet mask of the IP address that you entered in the **IP Address** field.
MAC Address	Select this option to allow packets from a computer with a specific MAC address to pass through the N4100 without entering a user name and password. Enter the MAC address of a computer (in 6 hexadecimal pairs separated by a hyphen "-", for example, 00-50-BA-8D-22-96).
Mask	Enter the subnet mask of the MAC address that you entered in the **MAC Address** field.
Description	Enter a descriptive name of up to 20 ASCII characters for this entry.
Add to List	Click this button to add the pass through entry you configured to the **Pass Through List**.
Pass Through List	This table displays the device and web site address entries that you have set up on the N4100.
No.	This read-only field displays the index number of a pass through entry.
Active	Select this check box to turn on this pass through entry and allow access without a user name and password. Clear this check box to turn off this pass through entry and block access without a user name and password.
Address List	This read-only field displays the address(es) of a pass through entry.
Type	This read-only field displays "Destination" for a pass through entry based on a destination URL or IP address. The field displays "Subscriber/LAN device" for a pass through entry based on a LAN device or a subscriber's computer. Click the column heading to sort the pass through entries by type (**Destination** or **Subscriber/LAN device**).
Description	This read-only field displays the name of a pass through entry.
Delete	Select this check box(es) and click **Apply** to remove the pass through entry.
Delete All	Click this button to remove all of the pass-through entries.
Apply	Click **Apply** to save your changes back to the N4100.

15

Filtering

15.1 Overview

Filtering allows you to block subscriber access to a list of destinations. This lets you block access to specific Internet websites or IP addresses. An example of what this would be useful for is blocking access to sites where subscribers would use large amounts of bandwidth for large file downloads or file sharing.

15.1.1 What You Can Do in this Chapter

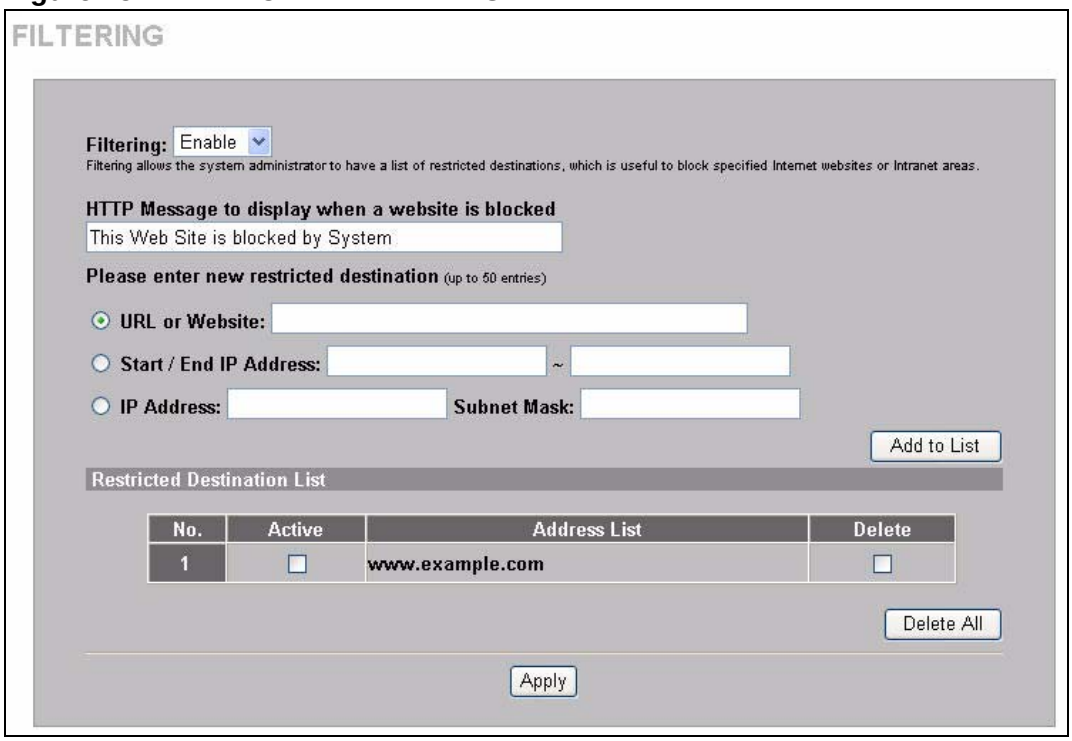
Use the **Filtering** screen (Section 15.2 on page 147) to configure the N4100's filter function.

15.2 The Filtering Screen

To configure filtering on the N4100, click **ADVANCED > FILTERING** to open this screen.

Note: Pass through has priority over filtering.

Figure 75 ADVANCED > FILTERING



The following table describes the labels in this screen.

Table 30 ADVANCED > FILTERING

LABEL	DESCRIPTION
Filtering	Enable filtering to block subscriber access to specified Internet websites or IP addresses.
HTTP Message to display when a website is blocked	Enter a message to display on the subscriber's screen when the system blocks access to a website. The default message is "This Web Site is blocked by System".
Please enter new restricted destination (up to 50 entries)	Use these fields to add to the list of forbidden destinations.
URL or Website	Enter the full URL of the website to which you want to block subscriber access for example, "http://www.example.com". You can use up to 350 ASCII characters.
Start / End IP Address	Enter the beginning and ending IP addresses of a range of IP addresses to which you want to block subscriber access.
IP Address	Enter an IP address to which you want to block subscriber access.
Subnet Mask	Enter the subnet mask of the IP address to which you want to block subscriber access.
Add to List	Click this button to add a new entry to the list of restricted destinations.

Table 30 ADVANCED > FILTERING

LABEL	DESCRIPTION
Restricted Destination List	This table lists Internet destinations to which the system is to block subscriber access.
No.	This is the index number of a destination entry.
Active	Select this check box to block subscriber access to this destination.
Address List	This field displays the destination address(s).
Delete	Select this(ese) check box(es) and click **Apply** to remove the destination entry.
Delete All	Click this button to remove all of the destination entries.
Apply	Click **Apply** to save your changes back to the N4100.

16 Share

16.1 Overview

The share function allows logged-in subscribers to share devices on the LAN. This is useful for allowing subscribers to use printers or servers.

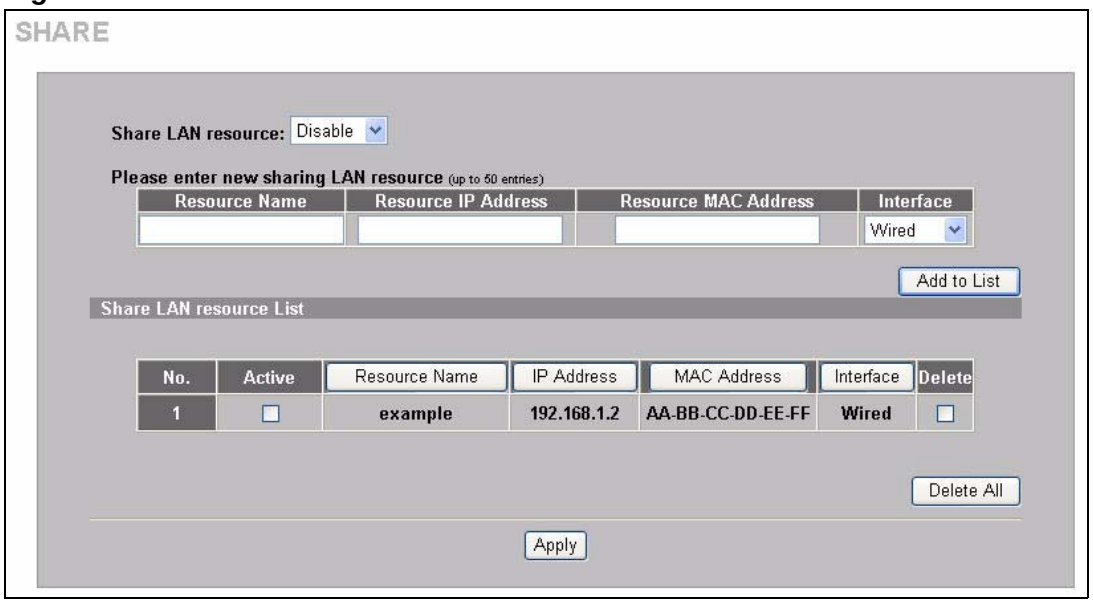
16.1.1 What You Can Do in this Chapter

Use the **Share** screen (Section 16.2 on page 151) to configure the N4100 for the sharing of network devices.

16.2 The Share Screen

To configure sharing on the N4100, click **ADVANCED > SHARE** to open this screen.

Figure 76 ADVANCED > SHARE



The following table describes the labels in this screen.

Table 31 ADVANCED > SHARE

LABEL	DESCRIPTION
Share LAN resource	Enable the sharing of LAN resources to allow logged-in subscribers to access specific devices on the LAN. Disable the sharing of LAN resources to block logged-in subscribers from accessing devices on the LAN.
Resource Name	Enter the LAN device's name (up to 50 ASCII characters).
Resource IP Address	Enter the IP address of the LAN device.
Resource MAC Address	Enter the MAC address of the LAN device.
Interface	Select the N4100's interface to which the LAN device is connected.
Add to List	Click this button to add the LAN device information to the list below.
Share LAN resource List	
No.	The index number of share LAN device.
Active	Select or clear this check box to enable or disable the sharing of access to the LAN device.
Resource Name	This field displays the LAN device's name. Click the column heading to sort the entries by resource name.
IP Address	This field displays the IP address of the LAN device. Click the column heading to sort the entries by IP address.
MAC Address	This field displays the MAC address of the LAN device. Click the column heading to sort the entries by MAC address.
Interface	This field displays to which of the N4100's interfaces the LAN device is connected. Click the column heading to sort the entries by interface.
Delete	Select a check box(es) and click **Apply** to delete the share device entry(ies).
Delete All	Click this button to remove all of the share device entries.
Apply	Click **Apply** to save your changes back to the N4100.

17

Portal Page, Advertisement Links and Walled Garden

17.1 Overview

When you enable subscriber authentication in the **ADVANCED > AUTHENTICATION** screen, you can set the N4100 to redirect a subscriber to a portal web site, display advertisement links or activate the walled garden feature for generating on-line advertising revenue.

17.1.1 What You Can Do in this Chapter

- Use the **Portal Page** screen (Section 17.2 on page 154) to set a portal web site.
- Use the **Advertisement** screen (Section 17.3 on page 155) to set advertisement links.
- Use the **Walled Garden** screen (Section 17.4 on page 156) to create walled garden web sites.

17.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

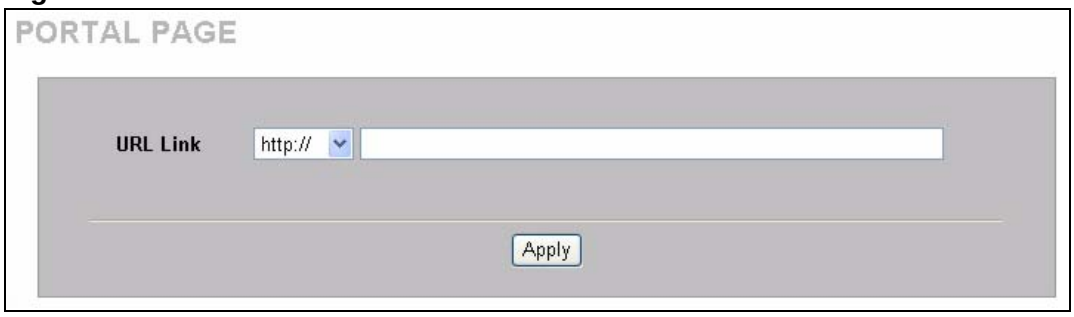
Portal Page

A portal page is the first web site to which a subscriber is redirected after logging in successfully. The super user account also gets redirected to the portal page. Users are also redirected to this web site if you set up the N4100 to not require authentication or to require the acceptance of a user agreement before allowing Internet access. If you do not specify a portal web site, the subscriber will be directed to the intended web site specified.

17.2 The Portal Page Screen

Click **ADVANCED > PORTAL PAGE** to open this screen.

Figure 77 ADVANCED > PORTAL PAGE



The following table describes the labels in this screen.

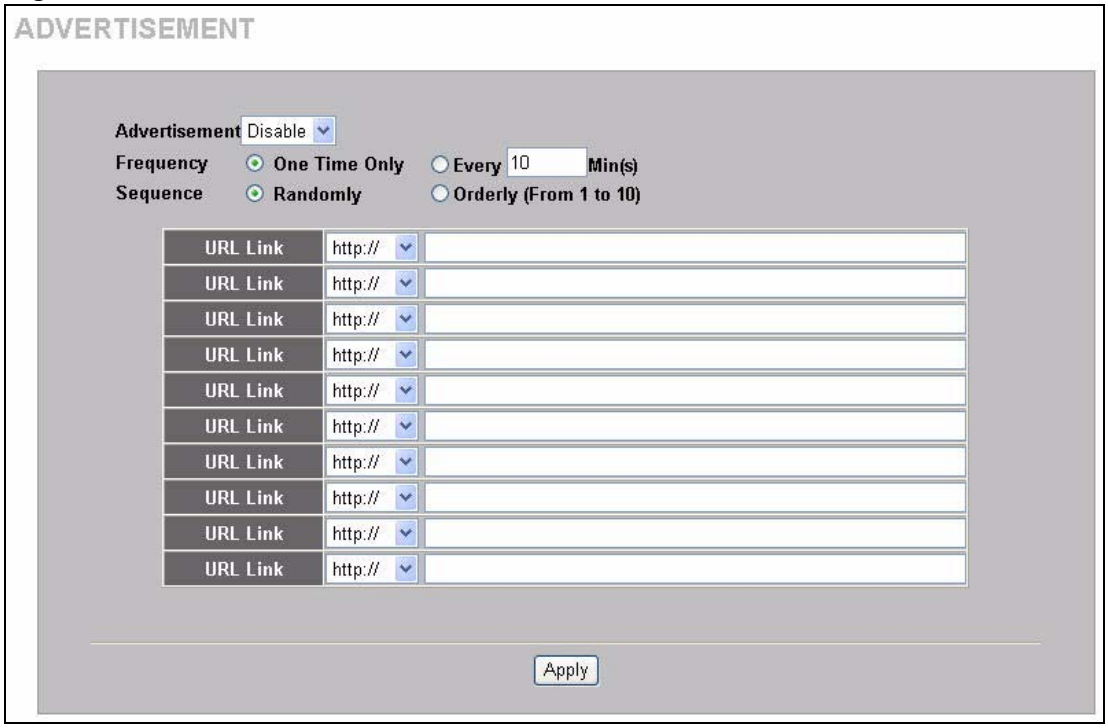
Table 32 ADVANCED > PORTAL PAGE

LABEL	DESCRIPTION
URL Link	Enter the web site address of a portal page. You can use up to 350 ASCII characters.
Apply	Click **Apply** to save your changes back to the N4100.

17.3 The Advertisement Screen

You can set the N4100 to display an advertisement web page as the first web page whenever the subscriber connects to the Internet. Click **ADVANCED > ADVERTISEMENT** to open this screen.

Figure 78 ADVANCED > ADVERTISEMENT



The following table describes the labels in this screen.

Table 33 ADVANCED > ADVERTISEMENT

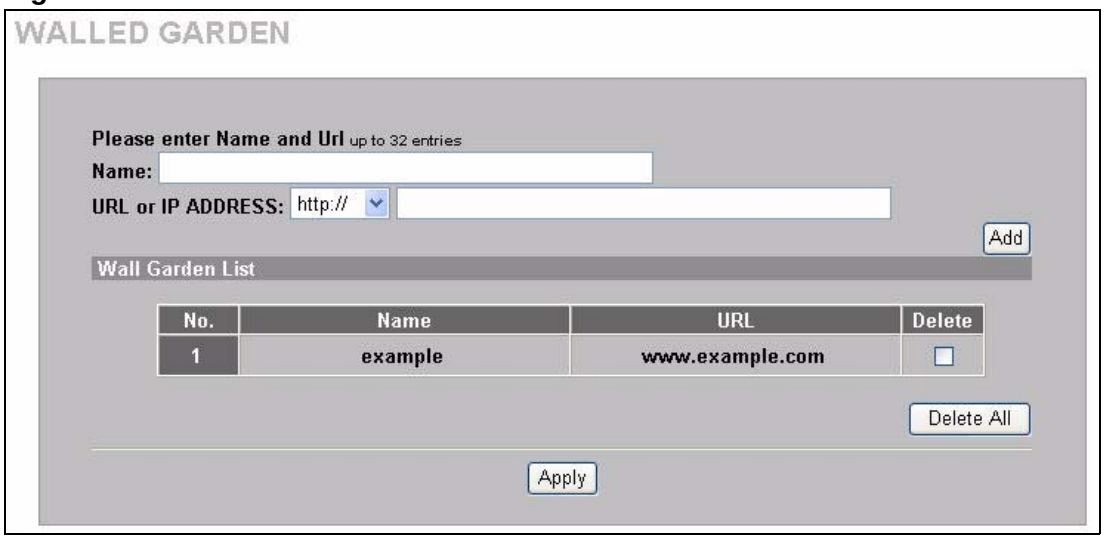
LABEL	DESCRIPTION
Advertisement	Select **Enable** to display advertisement web links. otherwise, select **Disable** to turn off this feature.
Frequency	Select **One Time Only** to display an advertisement web link in an active browser window once after a subscriber logs in successfully. Select **Every ... Min(s)** to display an advertisement web link in an active browser window once every time period specified (in minutes) after a subscriber logs in successfully.
Sequence	Select **Randomly** to display the advertisement links in random order, one at a time. Select **Orderly** to display the advertisement links in the order that you configure them.
URL Link	Enter the web site URLs in the fields provided. For example, “http:// www.zyxel.com”. You can use up to 350 ASCII characters.
Apply	Click **Apply** to save your changes back to the N4100.

17.4 The Walled Garden Screen

A subscriber must log in before the N4100 allows the subscriber access to the Internet. However, with a walled garden, you can define one or more web site addresses that all subscribers can access without logging in. These can be used for advertisements for example.

Click **ADVANCED > WALLED GARDEN** to open this screen.

Figure 79 ADVANCED > WALLED GARDEN



The following table describes the labels in this screen.

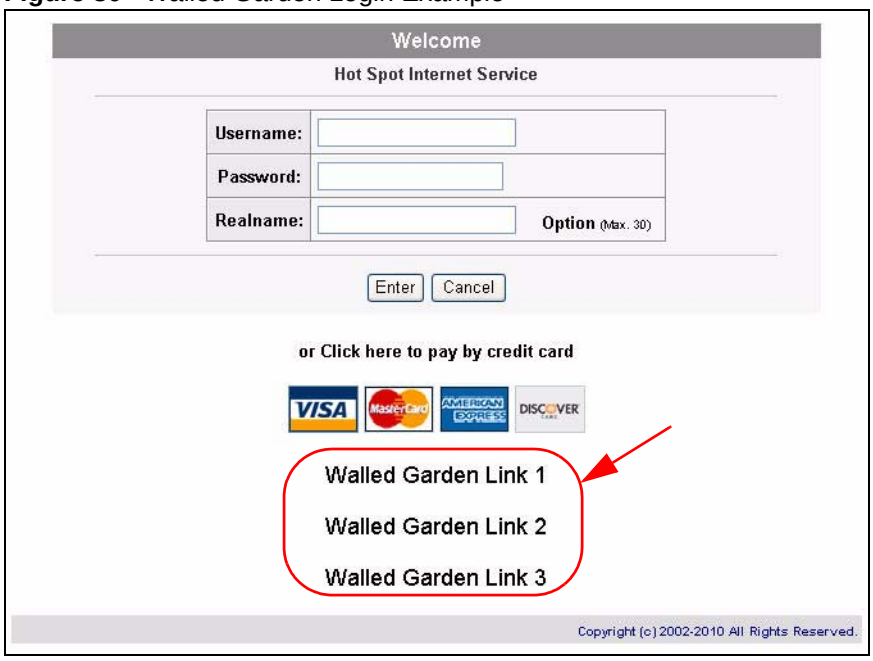
Table 34 ADVANCED > WALLED GARDEN

LABEL	DESCRIPTION
Name	Enter a descriptive name (up to 80 characters) for the walled garden link to be displayed in the web browser.
URL or IP Address	Enter the web site URL (up to 350 ASCII characters) or IP address. For example, “http://www.zyxel.com”.
Add to List	Click this button to append your entry to the list below.
Delete	Select the check boxes of entries that you want to remove and click **Apply** to remove them.
Delete All	Click this button to remove all of the walled garden links.
Apply	Click **Apply** to save your changes back to the N4100.

17.4.1 Walled Garden Login Example

The following figure shows the subscriber login screen with three walled garden links. The links are named **Walled Garden Link 1** through **3** for demonstration purposes.

Figure 80 Walled Garden Login Example



18 DDNS

18.1 Overview

DDNS (Dynamic Domain Name System) allows you to update your dynamic IP address with one or many dynamic DNS services so that anyone can contact you (in NetMeeting, CU-SeeMe or other services). This is for cases where the ISP gives the N4100 a dynamic IP address but you still want to use a domain name. You can also access your FTP server or Web site on your own computer using a domain name (for example, myhost.dhs.org, where myhost is a name of your choice), which will never change instead of using an IP address that changes each time you reconnect.

Note: You must go to the Dynamic DNS service provider's website and register a user account and a domain name before you can use the Dynamic DNS service with your N4100.

The Dynamic DNS service provider will give you a password or key.

Note: If you have a private WAN IP address, then you cannot use Dynamic DNS.

18.1.1 What You Can Do in this Chapter

Use the **DDNS** screen (Section 18.2 on page 160) to set the N4100 to use DDNS.

18.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

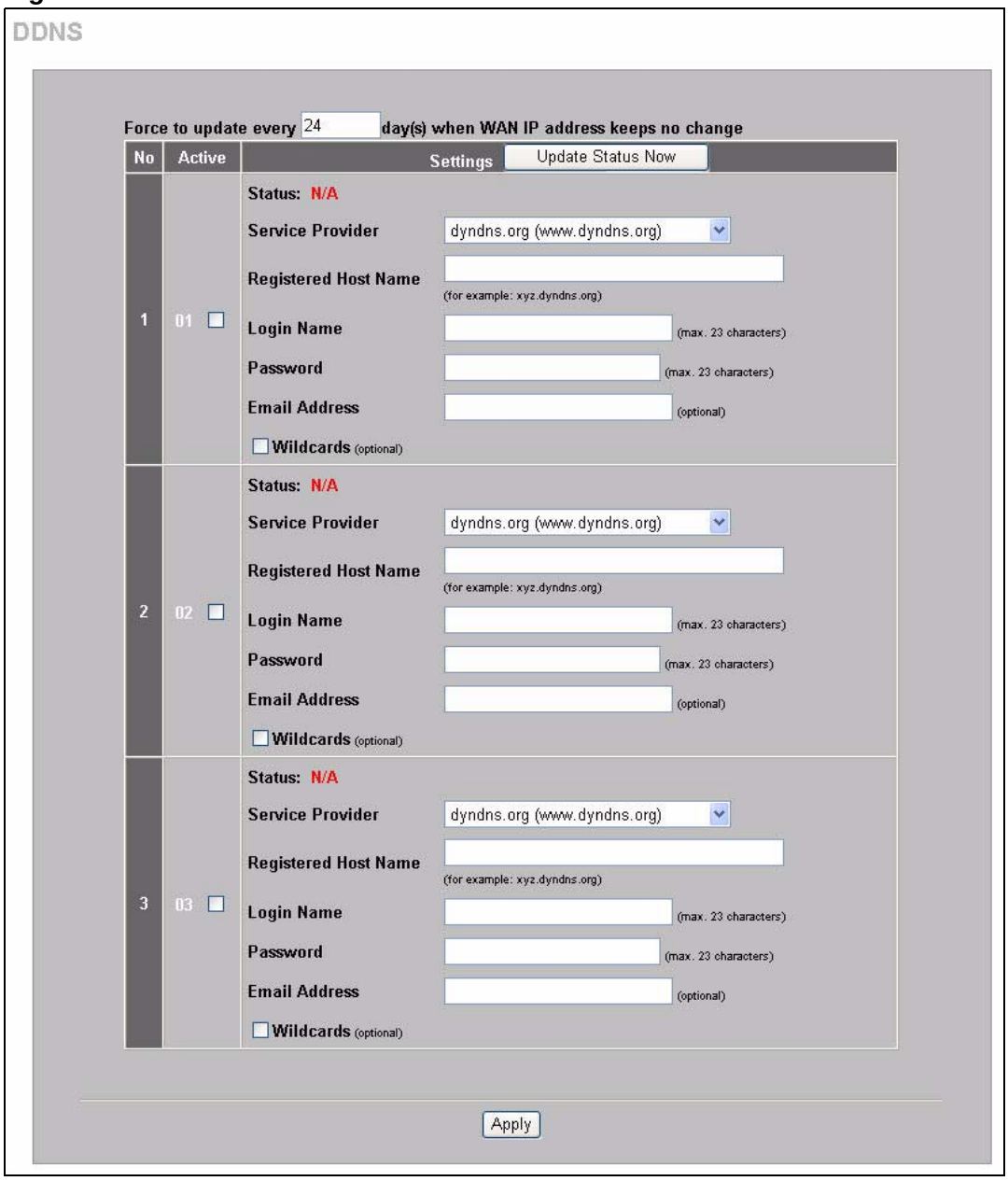
DYNDNS Wildcard

Enabling the wildcard feature for your host causes *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org. This feature is useful if you want to be able to use, for example, www.yourhost.dyndns.org and still reach your hostname.

18.2 The DDNS Screen

Click **ADVANCED > DDNS** to open this screen.

Figure 81 ADVANCED > DDNS



The following table describes the labels in this screen.

Table 35 ADVANCED > DDNS

LABEL	DESCRIPTION
Force to update every ~day(s) when WAN IP address keeps no change	Enter a number in the field to set the force update interval (in days). This sets how often the N4100 updates the DDNS server with the N4100's WAN IP address when the N4100's WAN IP address stays the same.
No	This is the index number of a DDNS account.
Active	Select or clear the check box to enable or disable the DDNS record.
Update Status Now	Click the **Update Status Now** button to have the N4100 update the DDNS server with the N4100's WAN IP address.
Settings	Enter the DDNS server account information in the fields below.
Status	This field displays **N/A** when the DDNS client service is not installed. This field displays the time of the latest update (in YY/MM/DD HH:MM:SS format) and the current state of the DDNS Client. This field displays **Updated Successfully** when the DDNS client service is installed and running. This field displays **Update Fail** when the DDNS client service is installed, but the service is not running.
Service Provider	Select the name of your Dynamic DNS service provider.
Registered Host Name	Enter the host name in the field provided.
Login Name	Enter the user name for the above **Registered Host Name**. The Dynamic DNS service provider assigns you this user name.
Password	Enter the password for the above **Login Name**. The Dynamic DNS service provider assigns you this password.
Email Address	Enter your e-mail address. The DDNS server e-mails you important information once your Internet Name has been successfully registered.
Wildcards (optional)	Select the check box to enable DYNDNS Wildcard.
Apply	Click **Apply** to save your changes back to the N4100.

19

LAN Devices

19.1 Overview

NAT (Network Address Translation - NAT, RFC 1631) is the translation of the IP address of a host in a packet. For example, the source address of an outgoing packet, used within one network is changed to a different IP address known within another network.

Traditionally, when you have a device (for example, a switch) on a LAN using NAT, you cannot access the device from the WAN since the LAN device is assigned a private IP address.

Your N4100 is a NAT-enabled device that makes your whole inside network appear as a single computer to the outside world.

This chapter describes how you can remotely access devices on the LAN through the N4100.

19.1.1 What You Can Do in this Chapter

Use the **LAN Devices** screen (Section 19.2 on page 164) to configure port mapping on the N4100.

19.1.2 What You Need to Know

The following terms and concepts may help as you read through this chapter.

Port Mapping

To make LAN devices behind the N4100 visible to the outside world, you configure a mapping between a virtual port on the N4100 and a server port on a LAN device. A virtual port is a port on the N4100 that appears as a physical port to the attached devices. A server port defines a server to which all specified requests are forwarded.

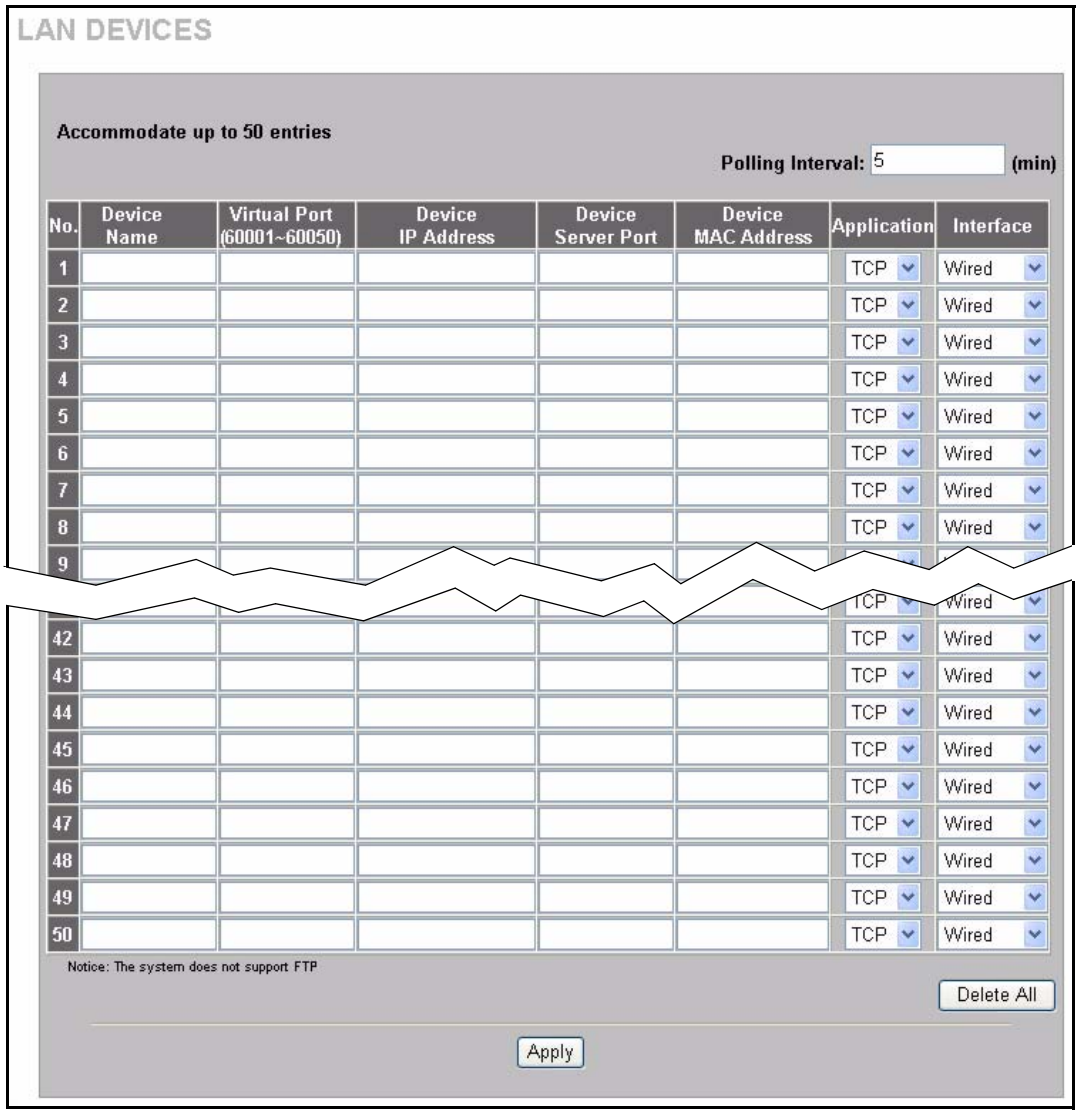
In addition, centralized LAN device management is possible through the N4100 using port mapping. You can access the management interface on the LAN device remotely provided that the LAN device has allowed remote management.

19.2 The LAN Devices Screen

Click **ADVANCED > LAN DEVICES** to open this screen.

Note: You can configure port mapping for up to 50 LAN devices on the N4100.

Figure 82 ADVANCED > LAN DEVICES



The following table describes the labels in this screen.

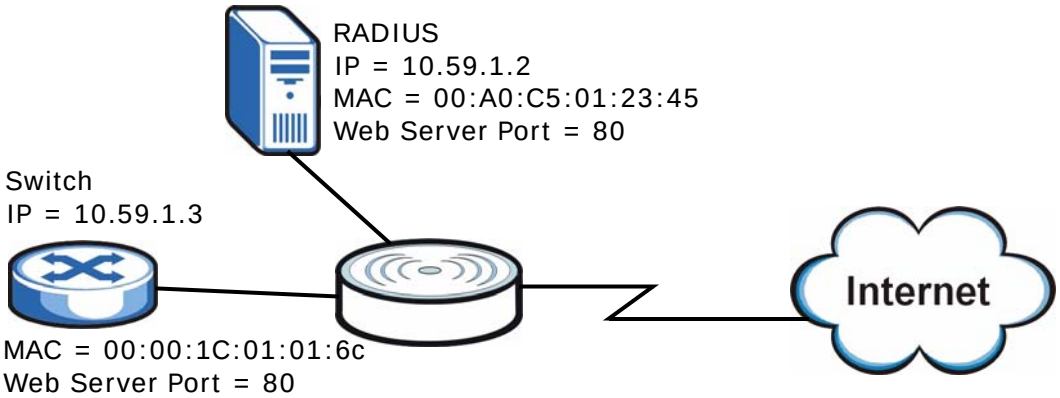
Table 36 ADVANCED > LAN DEVICES

LABEL	DESCRIPTION
Polling Interval	Specify the time interval (in minutes) between the N4100's probes for device availability.
No.	This read-only field displays the index number of an entry.
Device Name	Enter the name (up to 20 characters) of the LAN device for identification purposes.
Virtual Port	Enter a unique port number between 60001 and 60050 to map to the port number in the **Server Port** field.
Device IP Address	Enter the IP address of a LAN device in dotted decimal notation. For example, 192.168.1.40.
Device Server Port	Enter the port number for a service (for example, 80 for HTTP) on the LAN device.
MAC Address	Enter the MAC address of the LAN device in hexadecimal notation in 6 hexadecimal pairs, for example, 0050BA8D2296. Make sure you enter the correct MAC address.
Application	Select an application type from the drop-down list box. Choose from **TCP** or **UDP**. Only requests for the selected application type are forwarded to the specified server port on the LAN device.
Interface	Select the N4100's interface to which the LAN device is connected.
Delete All	Click **Delete All** to clear all entries. To delete a single entry, erase the contents in that entry.
Apply	Click **Apply** to save your changes back to the N4100.

19.2.1 LAN Device Management Example

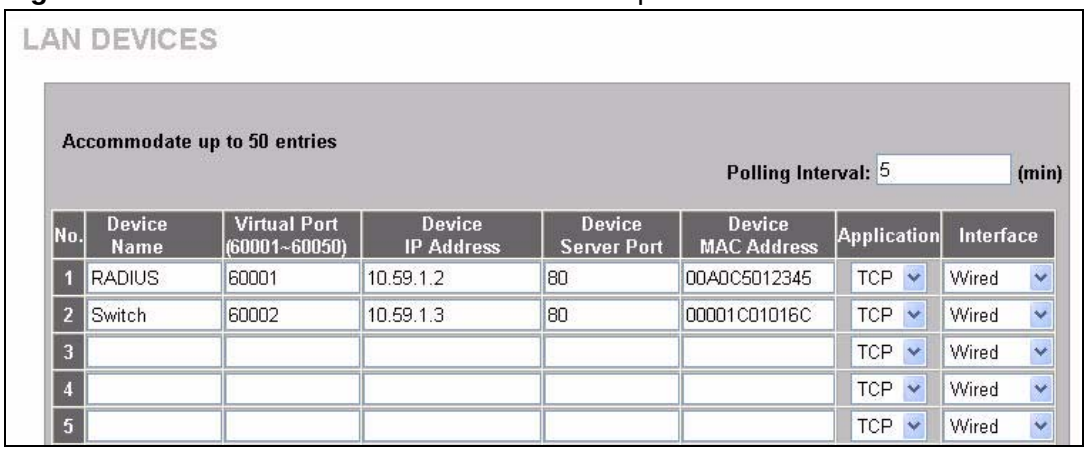
In this example, there is a manageable switch and a mail server behind the N4100 and you want to be able to remotely access the web-based management interfaces on the manageable switch and RADIUS server over the Internet.

Figure 83 LAN Device Remote Management Example



You map virtual port 60001 on the N4100 to the web server port on the RADIUS server and 60002 to the web server port on the manageable switch.

Figure 84 ADVANCED > LAN DEVICES: Example



To access the web-based management interface, enter the WAN IP address of your N4100 and the virtual port number of the LAN device separated by a colon. In this example, to access the RADIUS server, enter “http:// 192.168.1.1:60001” where 192.168.1.1 is the WAN IP address of the N4100. The login screen of the LAN device management interface should display.

You can also access the LAN device by entering the domain name provided that the N4100 has a domain name (or a dynamic domain name). Enter the domain name and the virtual port number separated by a colon, for example, http:// www.domainName:60001.

You can also access the LAN devices through the N4100 web configurator, refer to Section 28.8.1 on page 224 for more information.

20 Syslog

20.1 Overview

This chapter contains information about configuring syslog settings on the N4100.

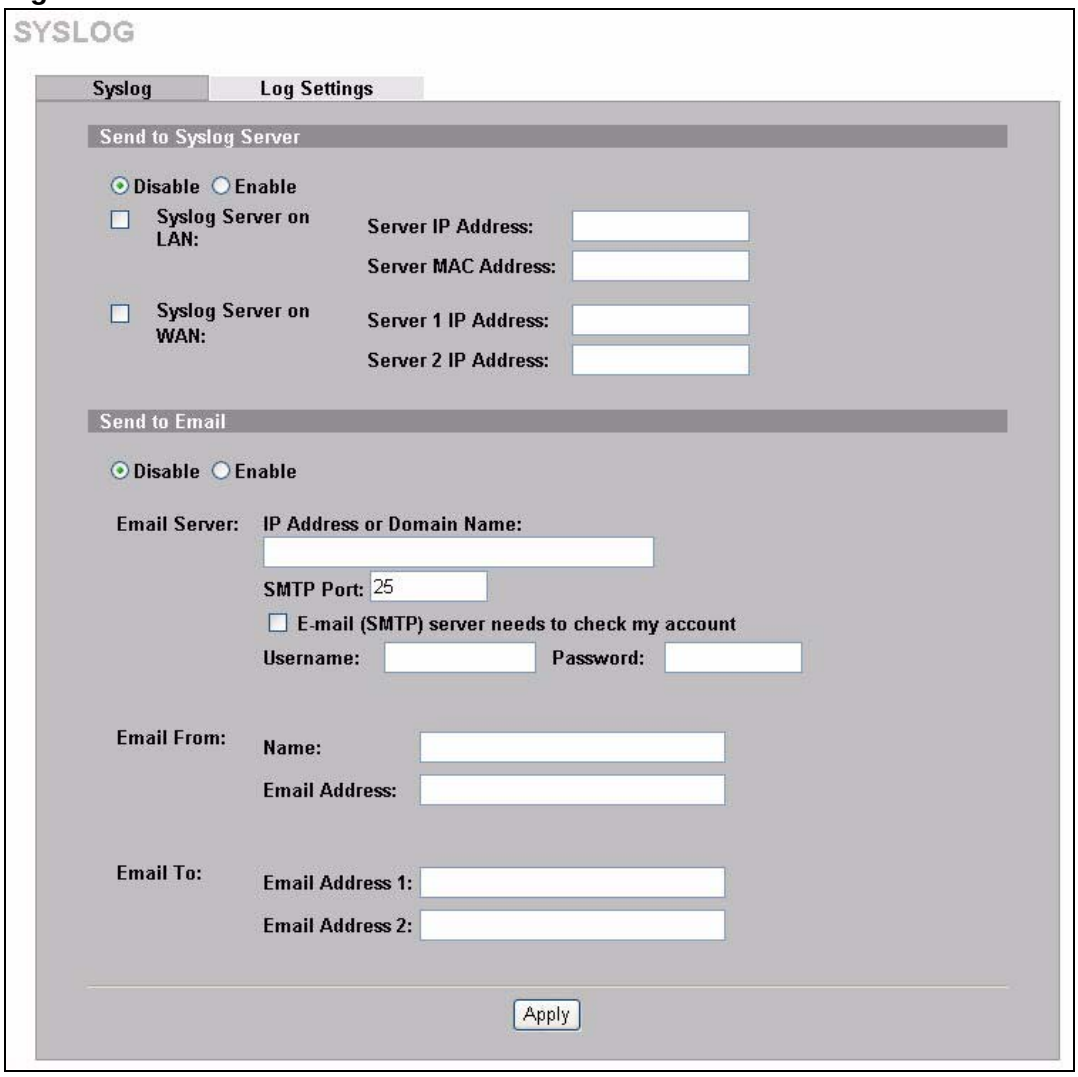
20.1.1 What You Can Do in this Chapter

- Use the **Syslog** screen (Section 20.2 on page 168) to configure to where the N4100 is to send logs.
- Use the **Log Settings** screen (Section 20.3 on page 170) to configure which logs the N4100 is to send and the schedule for when the N4100 is to send the logs.

20.2 The Syslog Screen

Click **ADVANCED > SYSLOG** to open this screen.

Figure 85 ADVANCED > SYSLOG



The following table describes the labels in this screen.

Table 37 ADVANCED > SYSLOG

LABEL	DESCRIPTION
Send to Syslog Server	Select **Enable** to activate the syslog function. Select **Disable** to de-activate the syslog function.
Syslog Server on LAN	Select this check box to specify a syslog server on the LAN.
Server IP Address	Enter the IP address (in dotted decimal notation) of the syslog server on the LAN.

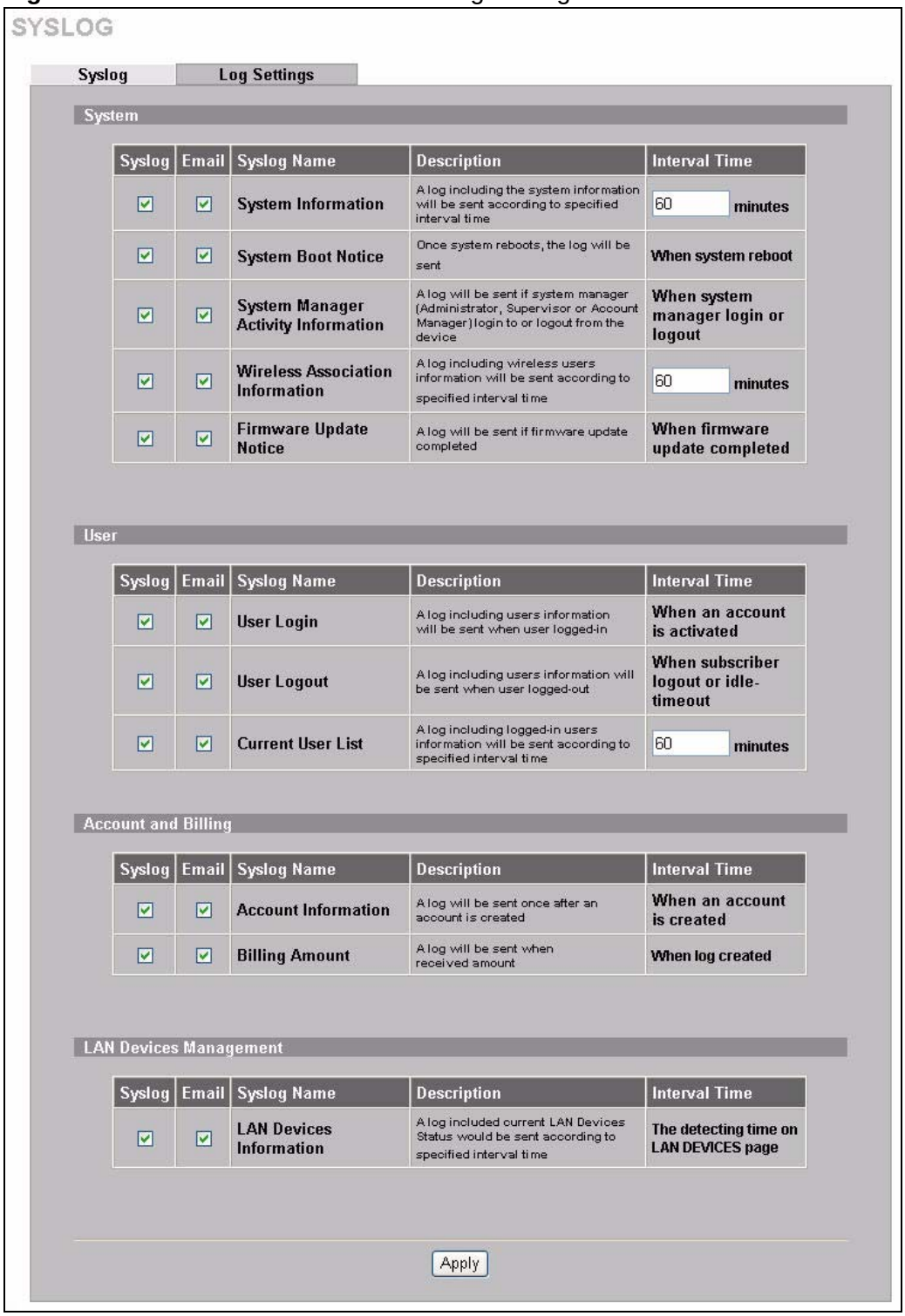
Table 37 ADVANCED > SYSLOG

LABEL	DESCRIPTION
Server MAC Address	Enter the MAC address of the syslog server on the LAN.
Syslog Server on WAN	Select this check box to specify a syslog server on the WAN.
Server 1 IP Address	Enter the IP address of the first syslog server on the WAN in dotted decimal notation.
Server 2 IP Address	Enter the IP address of the second syslog server on the WAN in dotted decimal notation.
Send to Email	Select **Enable** to have the N4100 send syslog messages to the e-mail account that you specify. Select **Disable** to not have the N4100 send syslog e-mail messages.
Email Server	
IP Address or Domain Name	Enter the IP address or domain name of the mail server for the e-mail addresses specified below. If this field is left blank, the syslog will not be sent via e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
E-mail (SMTP) server needs to check my account	Select this check box if your SMTP server requires user name and password authentication before accepting e-mail. Your network administrator, SMTP server provider or ISP should supply the username and password.
Username	Enter the username for the SMTP server.
Password	Enter the password for the SMTP server.
Email From	
Name	Type a name that you want to be in the “message from” field of the log e-mail message that the N4100 sends.
Email Address	Enter your e-mail address. This is the address others use to send e-mail to **Email Address 1**/**Email Address 2**.
Email To	
Email Address 1,2	Enter your first and second e-mail addresses to which the N4100 is to send the syslog e-mails. If you leave these fields blank, logs will not be sent via e-mail.
Apply	Click **Apply** to save your changes back to the N4100.

20.3 The Log Settings Screen

Click **ADVANCED > SYSLOG > Log Settings** to open this screen.

Figure 86 ADVANCED > SYSLOG > Log Settings



The following table describes the labels in this screen.

Table 38 ADVANCED > SYSLOG > Log Settings

LABEL	DESCRIPTION
Syslog	Select this check box to send this log information to your syslog server.
Email	Select this check box to send log information to the e-mail address specified in the **Syslog** screen.
Syslog Name	This field displays the name (or type) of the syslog. Select the check box(es) to send the syslog.
Description	This field displays a short description about the syslog.
Interval Time	This field displays how often the N4100 sends the syslog. If available, enter the number of minutes the N4100 waits between sending the syslog.
Apply	Click **Apply** to save your changes back to the N4100.

The following table describes the syslog formats.

Table 39 Log Formats

SYSLOG NAME	FORMAT	CREATED
System Information	**Id** <MAC Address> **System Uptime** <0 days 00h:04m:00s> **Location Name** <Location Name> **WAN** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError> **LAN** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError> **Wireless** <FrameTxOK| FrameRxOK| FrameTxError| FrameRxError>	Each time interval specified (between 1 and 10080 minutes).
System Boot Notice	**Id** <MAC Address> **System Up**	Each time the device reboots, when system reboot
System Manager Activity Information	**Id** <MAC Address> **System Account Activity Information** <Username, User IP, Status> Where: Username = Administrator | Supervisor | Accounting Operator User IP = IP Address Status = Login | Logout | Idle Time Out	Each time when a system manager logs in or logs out.
Wireless Association Information	**Id** <MAC Address> **Wireless Association Information** <Number of associated users, Start Number, End number) (Signal strength, Signal quality, Connection speed, MAC address>(...)(...)(...)	Each time interval specified (between 1 and 10080 minutes).

Table 39 Log Formats (continued)

SYSLOG NAME	FORMAT	CREATED
Logged-in Users	**Id** <MAC Address> **Logged-in Users** <Type, Number of logged-in users, Start Number, End number> Username, User IP, User MAC, Interface, Login time, RxData count, TxData count)(…)(…) Where: Type: Dynamic | Super | User agreement If the type of Logged-in user is Super Subscriber or User agreement, Username will be "********".	Each time interval specified (between 1 and 10080 minutes).
Account Created	**Id** <Mac Address> **Account Create** <Type, S/N, Username, Unit, Account usage time, Billing profile information> Where: Type: TimeToFinish | Accumulation | PostPaid Billing profile information = index, name Account usage time: 00:59:59 (example)	When an account is created.
Account Activated	**Id** <Mac Address> **Account Activate** < Username, User IP, User MAC, Interface >	When a subscriber account is activated.
Subscriber Trace	**Id** <MAC Address> **Subscriber Trace** <Type, Event, S/N, Username, User IP, User MAC, Interface, Login time, Logout time, Usage Time, Time Left, RxData count, TxData count) Where: Type: TimeToFinish | Accumulation | PostPaid | Super Event: Finished | Replenished | Logout | Idle-Timeout | Account Expired | Deleted If the type of Subscriber Trace is Super, the Username will be "********", and S/N will be "******". Usage time: 00:59:59 (example)	When a subscriber logs out.
User Agreement	(**Id**, Mac Address) (**User Agreement**, Type, User IP, User MAC) Where: Type: Agree | Do not agree	When "user agreement" is enabled.

Table 39 Log Formats (continued)

SYSLOG NAME	FORMAT	CREATED
Billing Log	**Id** <Mac Address> **Billing Log** <, Type, S/N, Username, Billing profile information, Units, Usage time, Bill, Payment> Where: Type: TimeToFinish | Accumulation | PostPaid Billing profile name: [Name] Usage time: “00:59:59” (example) Billing profile information = index, name Payment: Cash | Credit Card “Credit Card” does not support “PostPaid”. If Type is “PostPaid”, the billing profile information and Units will be “*”.	When a billing log is created
LAN Devices Information	**Id** <MAC Address> **LAN Devices Information** <Number of devices, Start Number, End number> **Device name** <status> [additional information]	Each time interval specified (between 1 and 10080 minutes).
LAN Devices Alarm	**Id** <MAC Address> **LAN Device Alarm** <Device name, FAIL>	When the N4100 cannot connect to an attached LAN device.

Table 40 Subscriber Trace Relationship

TYPE	EVENT	TIME LEFT
TimeToFinish	Finished	00:00:00
TimeToFinish	Replenished	00:12:00 to S/Nxxxxxx
TimeToFinish	Deleted	00:12:00
Accumulation	Finished	00:00:00
Accumulation	Replenished	00:12:00 to S/Nxxxxxx
Accumulation	Logout	00:48:00
Accumulation	Idle-Timeout	00:48:00
Accumulation	Deleted	00:48:00
Accumulation	Account Expired	00:48:00
PostPaid	Logout	******
PostPaid	Idle-Timeout	******
PostPaid	Deleted	******
PostPaid	Finished	******
PostPaid	Account Expired	******

Table 40 Subscriber Trace Relationship

TYPE	EVENT	TIME LEFT
Super	Idle-Timeout	******
Super	Deleted	******

21

Session Trace

21.1 Overview

You can set the N4100 to send session information of subscribers accessing the Internet. The N4100 records the session information and stores it temporary. Once the session trace information reaches 50 records or the specified time period is reached, the N4100 sends the session information to the specified TFTP server, e-mail address and/or syslog server.

21.1.1 What You Can Do in this Chapter

Use the **Session Trace** screen (Section 21.2 on page 176) to configure the N4100 to record details about subscriber Internet access and to where the N4100 sends logs of the session traces.

21.2 The Session Trace Screen

Click **ADVANCED > SESSION TRACE** to open this screen.

Figure 87 ADVANCED > SESSION TRACE

The following table describes the labels in this screen.

Table 41 ADVANCED > SESSION TRACE

LABEL	DESCRIPTION
Session Trace	Enable the session trace feature to record the destination IP address, destination port, source IP address, source MAC address and source port of every subscriber session. The N4100 sends the collected information in a text file to the destination(es) that you specify below. Disable the session trace feature to not record and send details about the Internet access activity of your subscribers.
Send Session Trace log file every~ minutes.	Enter the time interval (minutes) for how often you want the N4100 to send the session trace log file. Note: The N4100 will also automatically send the log file whenever the log has 50 entries. The N4100 clears the session trace record after sending a log file.
Send to TFTP Server	
Enable	Select the check box to have the N4100 send the session trace log file to the TFTP server that you specify.
Primary TFTP Server IP Address	Enter the IP address of the first TFTP server in dotted decimal notation.
Secondary TFTP Server IP Address	Enter the IP address of the second TFTP server in dotted decimal notation.
Send to E-mail Server	
Enable	Select the check box to have the N4100 send the session trace log file to the e-mail account that you specify.
Email Server	
IP Address or Domain Name	Enter the IP address or domain name of the mail server for the e-mail addresses specified below. If this field is left blank, the syslog will not be sent via e-mail.
SMTP Port	Enter the port number (25, or between 2500 and 2599) for the mail server. The default is **25**.
Enable E-mail (SMTP) server needs to check my account	Select this check box if your SMTP server requires user name and password authentication before accepting e-mail. Your network administrator, SMTP server provider or ISP should supply the username and password.
Username	Enter the username for the SMTP server.
Password	Enter the password for the SMTP server.
Email From	
Name	Type a name that you want to be in the “message from” field of the log e-mail message that the N4100 sends.

Table 41 ADVANCED > SESSION TRACE

LABEL	DESCRIPTION
Email Address	Enter your e-mail address. This is the address others use to send e-mail to **Email Address 1**/**Email Address 2**.
Email To	
Email Address 1,2	Enter your first and second e-mail addresses to which the N4100 is to send the syslog e-mails. If you leave these fields blank, logs will not be sent via e-mail.
Send to Syslog Server	
Enable	Select the check box to have the N4100 send the session trace log file to the syslog server that you specify in the **Syslog** screen.
Apply	Click **Apply** to save your changes back to the N4100.

21.3 Session Trace Filename Convention

The subscriber session information is stored a plain text file with a “txt” filename extension. The general structure of the filename is <hostname>DDMMYYHHMMSS.txt. For example, “MIS221004131543.txt” is the file name of a session information file created at 13:15:43 PM on October 22, 2004 on a N4100 with a hostname of “MIS”.

You can view the subscriber session trace information using any text editor. The following figure shows an example of the session information file the N4100 sends to a TFTP server.

Figure 88 Session Trace Information Example

```
Host Name User Name   Date    SourceIP      SourceMac    SourcePort DestIP       DestPor
MyDevice 79mv9r33  16Aug05165501 192.168.1.2   000FFE1E4AE0 2101   66.102.7.147   80
MyDevice 79mv9r33  16Aug05165517 192.168.1.2   000FFE1E4AE0 2104   168.95.1.1     53
MyDevice 79mv9r33  16Aug05165517 192.168.1.2   000FFE1E4AE0 2105   69.44.58.78    80
```

The following table describes the fields in a session information file.

Table 42 Session Trace File Fields

LABEL	DESCRIPTION
Host Name	This is the host (or system) name of the N4100.
User Name	This is the subscriber account username. This field is empty if you disable authentication in the **Authentication** screen (see Chapter 7 on page 89 for more information).
Date	This is the date and time the N4100 creates a session trace record.
SourceIP	This is the IP address of the subscriber.
SourceMac	This is the MAC address of the subscriber’s computer.

Table 42 Session Trace File Fields

LABEL	DESCRIPTION
SourcePort	This is the source port number of the subscriber.
DestIP	This is the destination IP address the subscriber accesses.
DestPort	This is the destination port number for this session.

22

Secure Remote

22.1 Overview

This chapter shows you how to configure settings to use the N4100's VPN PPTP client for a secure connection to a remote site or back end system.

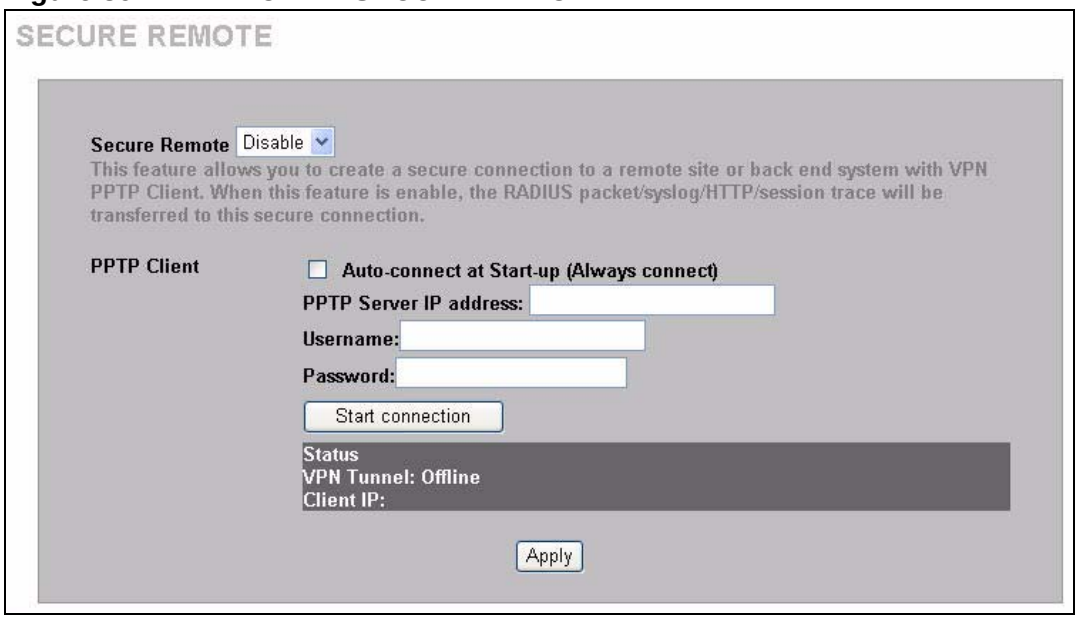
22.1.1 What You Can Do in this Chapter

Use the **Secure Remote** screen (Section 22.2 on page 181) to allow the N4100 to send RADIUS packets, syslogs and log e-mails through a PPTP VPN tunnel.

22.2 The Secure Remote Screen

Click **ADVANCED > SECURE REMOTE** to open this screen.

Figure 89 ADVANCED > SECURE REMOTE



The following table describes the labels in this screen.

Table 43 ADVANCED > SECURE REMOTE

LABEL	DESCRIPTION
Secure Remote	Select **Enable** to have the N4100 send RADIUS packets, syslogs and log e-mails through a PPTP VPN tunnel.
Auto-connect at Start-up (Always connect)	Turn this on to have the N4100 automatically establish this connection after it turns on.
PPTP Server IP address	Enter the IP address of the PPTP server to which the N4100 will make the secure connection.
Username	Enter the user name exactly as it was provided by the ISP or network administrator. The user name can be up to 80 alphanumeric characters and is case-sensitive.
Password	Enter the password exactly as it was provided by the ISP or network administrator. The password can be up to 80 alphanumeric characters and is case-sensitive.
Start/Stop Connection	Click this button to initiate or cancel the PPTP connection.
Status	
VPN Tunnel	This field displays whether or not the PPTP connection is currently up.
Client IP	This is the IP address that the PPTP server assigned to the N4100 for the VPN connection.
Apply	Click **Apply** to save your changes back to the N4100.

23

SNMP

23.1 Overview

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. Your N4100 supports SNMP agent functionality, which allows a manager station to manage and monitor the N4100 through the network.

An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed device (the N4100). An agent translates the local management information from the managed switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/managed objects that define each piece of information to be collected about a switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request/response protocol based on the manager/agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 44 SNMP Commands

COMMAND	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

23.1.1 SNMP Traps

The N4100 will send traps to the SNMP manager when any one of the following events occurs:

Table 45 SNMP Traps

TRAP NAME	DESCRIPTION
sysReboot	A trap is sent after booting (power on).

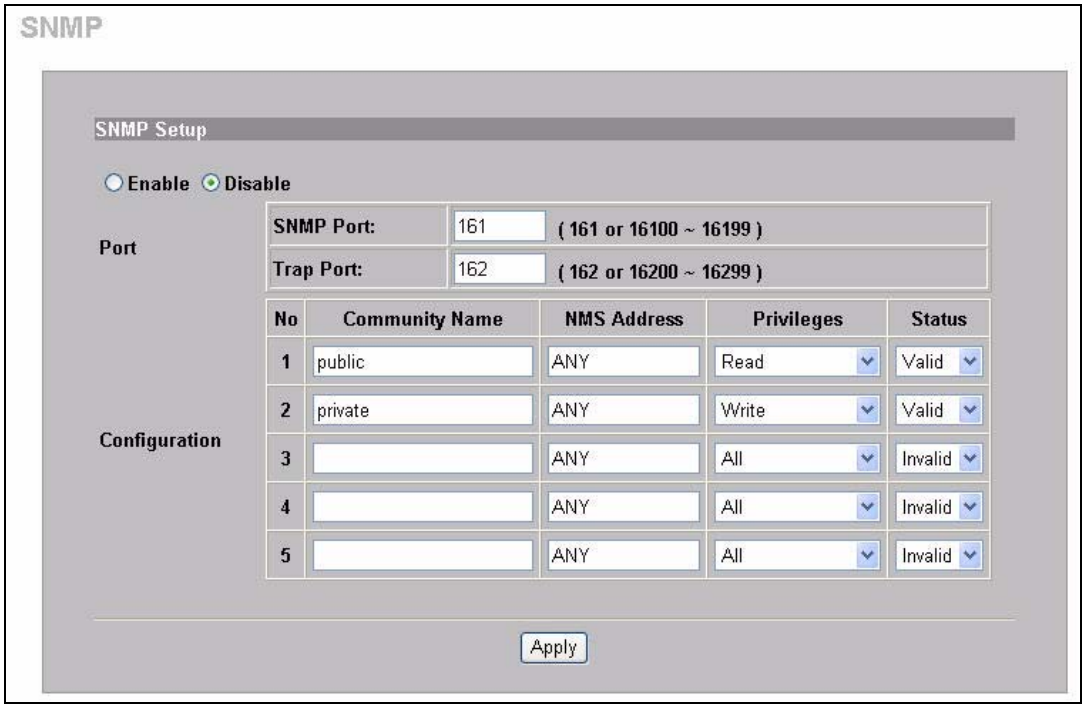
23.1.2 What You Can Do in this Chapter

Use the **SNMP** screen (Section 23.2 on page 184) to configure your SNMP settings.

23.2 The SNMP Screen

Click **ADVANCED > SNMP** to open this screen.

Figure 90 ADVANCED > SNMP



The following table describes the fields in this screen.

Table 46 ADVANCED > SNMP

LABEL	DESCRIPTION
SNMP Setup	Select **Enable** to allow a manager station to manage and monitor the N4100 through the network via SNMP. Otherwise, select **Disable**.
Port	
SNMP Port	Enter the N4100's port number to which the manager station sends requests.
Trap Port	Enter the port number on which the manager station listens for SNMP traps and information from the N4100.
Configuration	
No	This is the index number of the entry.
Community Name	Enter the password for the incoming Get, GetNext or Set requests from the management station. The default community for read-only access is **public** and the default community for read-write access is **private**.
NMS Address	Enter the IP address of the Network Management System (NMS) that controls and monitors the managed device (N4100). **ANY** means any computer that connects to the N4100 can request SNMP information and/or receive traps from the N4100.
Privileges	Select the privilege level of the password. **Read** means the password is for read-only (Get or GetNext) access. **Write** means the password is for read-write (Get/GetNext and Set) access. **Trap Recipient** means the password is for accepting SNMP traps from the N4100. **All** means the password has all the above permissions.
Status	Select whether this password is valid or not.
Apply	Click this button to save your changes back to the N4100.

24

Bandwidth

24.1 Overview

You can set the N4100 to limit the amount of bandwidth each user can use. This prevents one user from consuming a disproportionately large amount of bandwidth and helps ensure that every user gets their fair share. If there is a lot of unused bandwidth, however, this feature is not necessary and slows down users who could use the extra bandwidth to upload or download large amounts of information more quickly.

The N4100 separates bandwidth into upstream bandwidth and downstream bandwidth. Upstream bandwidth is used when users send information to the WAN, and downstream bandwidth is used when users receive information from the WAN. This distinction is helpful when you might want to set limits one way but not the other. For example, if your users download a lot of MP3 files, you might set a limit on downstream bandwidth but not set a limit on upstream bandwidth. In other situations, however, you might put the same limit on upstream and downstream bandwidth.

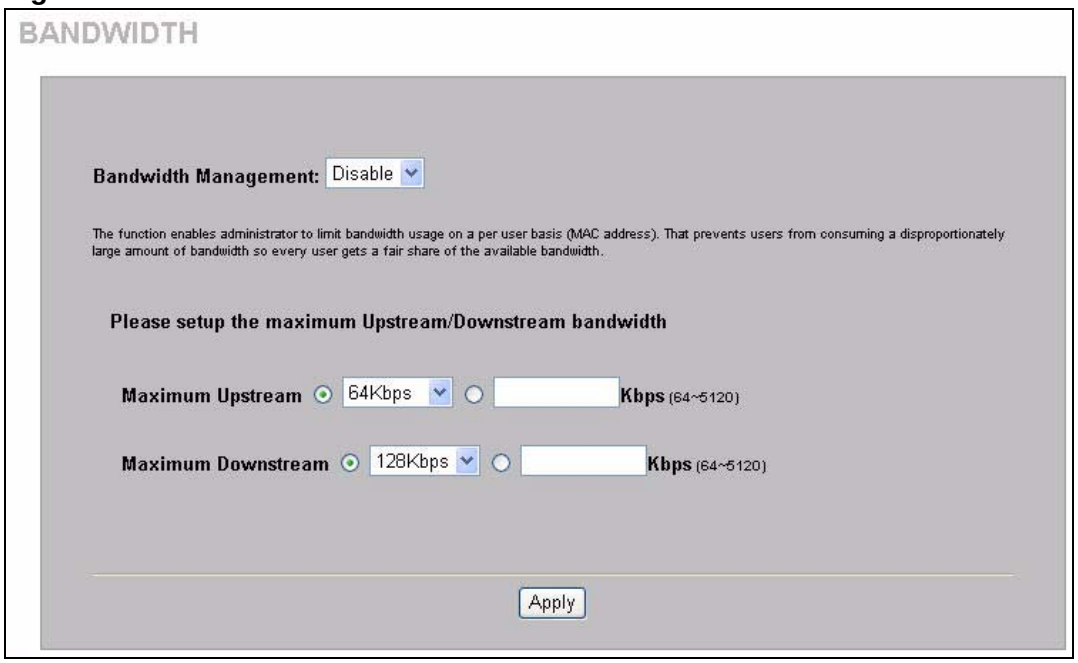
24.1.1 What You Can Do in this Chapter

Use the **Bandwidth** screen (Section 24.2 on page 188) to configure the N4100 to limit the amount of upstream and downstream bandwidth each user can use.

24.2 The Bandwidth Screen

Click **ADVANCED > BANDWIDTH** to open this screen.

Figure 91 ADVANCED > BANDWIDTH



The following table describes the fields in this screen.

Table 47 ADVANCED > BANDWIDTH

LABEL	DESCRIPTION
Bandwidth Management	Select **Enable** to turn on bandwidth management. If you select **Disable**, each user gets as much bandwidth as possible until the available bandwidth is gone.
Maximum Upstream	Select the maximum amount of upstream (outbound) bandwidth or enter a specific amount of bandwidth in Kbps that any user can have.
Maximum Downstream	Select the maximum amount of downstream (inbound) bandwidth or enter a specific amount of bandwidth in Kbps that any user can have.
Apply	Click this button to save your changes back to the N4100.

25

Wireless LAN

25.1 Overview

This chapter describes how to turn the wireless connection on or off, configure a name, wireless channel and security for the wireless network.

See Section 25.5 on page 198 for advanced technical information on wireless networks.

25.1.1 What You Can Do in this Chapter

Use the **Wireless** screen (Section 25.4 on page 192) to configure wireless LAN settings on the N4100.

25.2 What You Need to Know

Wireless Basics

"Wireless" is essentially radio communication. In the same way that walkie-talkie radios send and receive information over the airwaves, wireless networking devices exchange information with one another. A wireless networking device is just like a radio that lets your computer exchange information with radios attached to other computers. Like walkie-talkies, most wireless networking devices operate at radio frequency bands that are open to the public and do not require a license to use. However, wireless networking is different from that of most traditional radio communications in that there a number of wireless networking standards available with different methods of data encryption.

Wireless Network Construction

Wireless networks consist of wireless clients, access points and bridges.

- A wireless client is a radio connected to a user's computer.

- An access point is a radio with a wired connection to a network, which can connect with numerous wireless clients and let them access the network.
- A bridge is a radio that relays communications between access points and wireless clients, extending a network's range.

Traditionally, a wireless network operates in one of two ways.

- An "infrastructure" type of network has one or more access points and one or more wireless clients. The wireless clients connect to the access points.
- An "ad-hoc" type of network is one in which there is no access point. Wireless clients connect to one another in order to exchange information.

Network Names

Each network must have a name, referred to as the SSID - "Service Set IDentifier". The "service set" is the network, so the "service set identifier" is the network's name. This helps you identify your wireless network when wireless networks' coverage areas overlap and you have a variety of networks to choose from.

Radio Channels

In the radio spectrum, there are certain frequency bands allocated for unlicensed, civilian use. For the purposes of wireless networking, these bands are divided into numerous channels. This allows a variety of networks to exist in the same place without interfering with one another. When you create a network, you must select a channel to use.

Since the available unlicensed spectrum varies from one country to another, the number of available channels also varies.

Wireless Security

By their nature, radio communications are simple to intercept. For wireless data networks, this means that anyone within range of a wireless network without security can not only read the data passing over the airwaves, but also join the network. Once an unauthorized person has access to the network she/he can either steal information or introduce malware (malicious software) intended to compromise the network. For these reasons, a variety of security systems have been developed to ensure that only authorized people can use a wireless data network, or understand the data carried on it.

These security standards do two things. First, they authenticate. This means that only people presenting the right credentials (often a username and password, or a "key" phrase) can access the network. Second, they encrypt. This means that the information sent over the air is encoded. Only people with the code key can

understand the information, and only people who have been authenticated are given the code key.

These security standards vary in effectiveness. Some can be broken, such as the old Wired Equivalent Privacy (WEP). Using WEP is better than using no security at all, but it will not keep a determined attacker out. Other security standards are secure in themselves but can be broken if a user does not use them properly. For example, the WPA-PSK security standard is perfectly secure if you use a long key which is difficult for an attacker's software to guess - for example, a twenty-letter long string of apparently random numbers and letters - but it is not very secure if you use a short key which is very easy to guess.

Because of the damage that can be done by a malicious attacker, it's not just people who have sensitive information on their network who should use security. Everybody who uses any wireless network should ensure that effective security is in place.

A good way to come up with effective security keys, passwords and so on is to use obscure information that you personally will easily remember, and to enter it in a way that appears random and does not include real words. For example, if your mother owns a 1970 Dodge Challenger and her favorite movie is Vanishing Point (which you know was made in 1971) you could use "70dodchal71vanpoi" as your security key.

Signal Problems

Because wireless networks are radio networks, their signals are subject to limitations of distance, interference and absorption.

Problems with distance occur when the two radios are too far apart. Problems with interference occur when other radio waves interrupt the data signal. Interference may come from other radio transmissions, such as military or air traffic control communications, or from machines that are coincidental emitters such as electric motors or microwaves. Problems with absorption occur when physical objects (such as thick walls) are between the two radios, muffling the signal.

25.3 Before You Begin

Before you start using these screens, ask yourself the following questions. See Section 25.2 on page 189 if some of the terms used here do not make sense to you.

- What wireless standards do the other wireless devices support (IEEE 802.11g, for example)? What is the most appropriate standard to use?

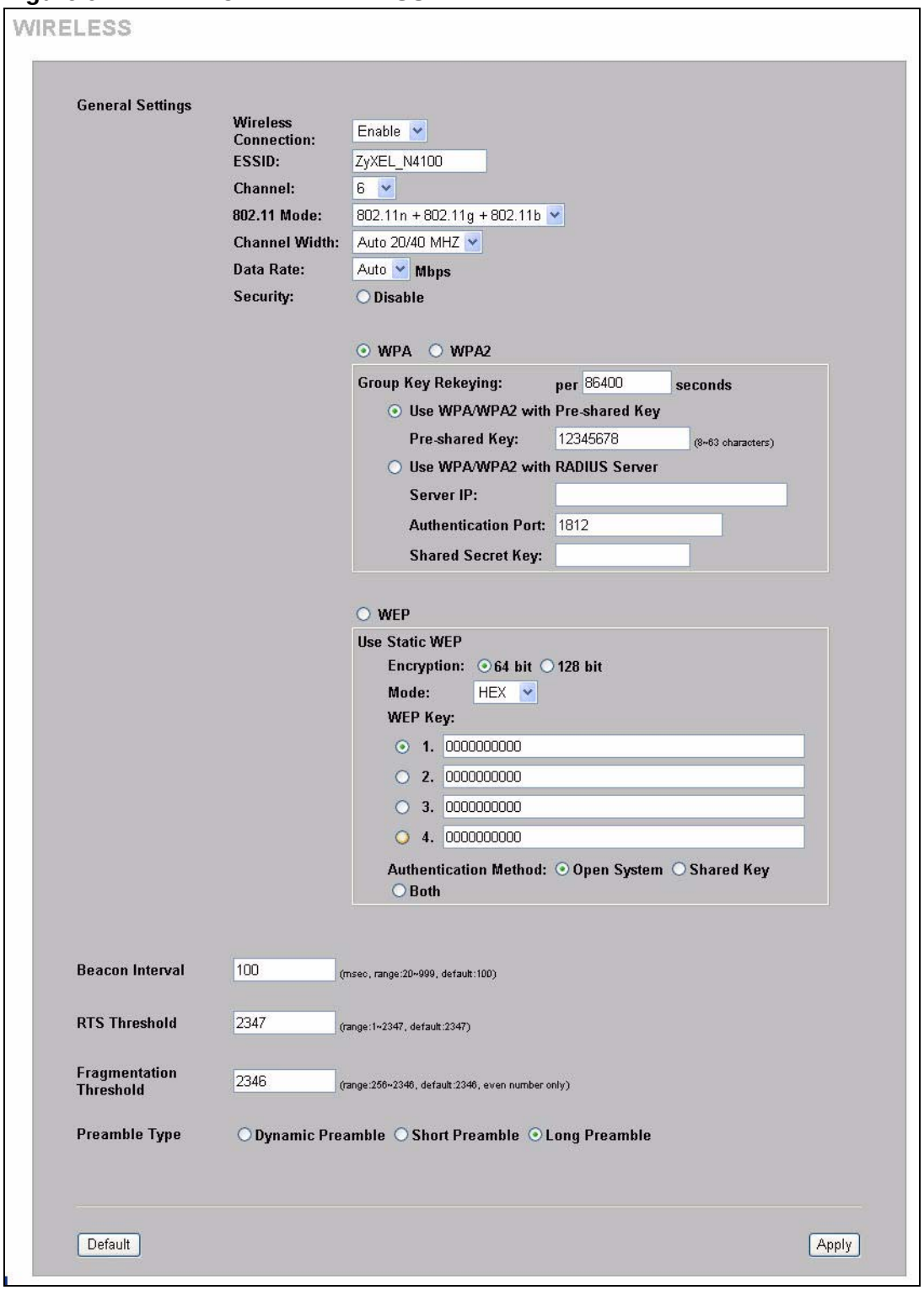
- What security options do the other wireless devices support (WPA-PSK, for example)? What is the best one to use?
- What advanced options do you want to configure, if any? If you want to configure advanced options, ensure that you know precisely what you want to do. If you do not want to configure advanced options, leave them alone.

25.4 The Wireless Screen

Note: If you are configuring the N4100 from a computer connected to the wireless LAN and you change the N4100's SSID or security settings, you will lose your wireless connection when you press **Apply** to confirm. You must then change the wireless settings of your computer to match the N4100's new settings.

Click **ADVANCED > WIRELESS** to open this screen.

Figure 92 ADVANCED > WIRELESS



The following table describes the fields in this screen.

Table 48 ADVANCED > WIRELESS

LABEL	DESCRIPTION
Wireless Connection	Select **Enable** to activate wireless LAN.
ESSID	The Extended Service Set IDentity (ESSID) identifies the service set with which a wireless device is associated. Wireless devices associating to the access point (AP) must have the same ESSID. Enter a descriptive name (up to 32 printable 7-bit ASCII characters) for the wireless LAN.
Channel	Select a channel/operating frequency from the drop-down list box depending on your particular region.
802.11 Mode	Select **802.11b only** to only allow IEEE 802.11b compliant WLAN devices to associate with the N4100. Select **802.11g only** to allow IEEE 802.11g compliant WLAN devices to associate with the N4100. IEEE 802.11b compliant WLAN devices can associate with the N4100 only when they use the short preamble type. Select **802.11n only** to only allow IEEE 802.11n compliant WLAN devices to associate with the N4100. This can increase transmission rates, although IEEE 802.11b or IEEE 802.11g clients will not be able to connect to the N4100. Select **802.11g + 802.11b** to allow either IEEE 802.11g or IEEE 802.11b compliant WLAN devices to associate with the N4100. The N4100 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select **802.11n + 802.11g** to allow either IEEE 802.11n or IEEE 802.11g compliant WLAN devices to associate with the N4100. The N4100 adjusts the transmission rate automatically according to the wireless standard supported by the wireless devices. Select **802.11n + 802.11g + 802.11b** to allow both IEEE802.11b, IEEE802.11g and IEEE802.11n compliant WLAN devices to associate with the N4100. The transmission rate of your N4100 might be reduced.

Table 48 ADVANCED > WIRELESS (continued)

LABEL	DESCRIPTION
Channel Width	Select whether the N4100 uses a wireless channel width of **Auto 20/40 MHz** or **20 MHz**. A standard 20MHz channel offers transfer speeds of up to 150Mbps whereas a 40MHz channel uses two standard channels and offers speeds of up to 300 Mbps. 40MHz (channel bonding or dual channel) bonds two adjacent radio channels to increase throughput. The wireless clients must also support 40 MHz. It is often better to use the 20 MHz setting in a location where the environment hinders the wireless signal. It is recommended that you select **Auto 20/40 MHz**. This allows the N4100 to adjust the channel bandwidth depending on network conditions. Select **20 MHz** if you want to lessen radio interference with other wireless devices in your neighborhood or the wireless clients do not support channel bonding. This field is available only when you set the **802.11 Mode** to **802.11n only**, **802.11n + 802.11g** or **802.11n + 802.11g + 802.11b**.
Data Rate	Select a transmission rate at which wireless clients can always connect to the N4100.
Security	Select **Disable** to allow wireless devices to communicate with the N4100 without any data encryption. Select **WPA** (Wi-Fi Protected Access) to have the N4100 perform user authentication and data encryption. WPA's data encryption is stronger than WEP. Select **WPA2** (Wi-Fi Protected Access 2) to have the N4100 perform user authentication and data encryption. WPA2's data encryption is stronger than WPA and WEP. Select **WEP** (Wired Equivalent Privacy to have the N4100 encrypt data frames before transmitting them over the wireless network. Select the check box to enable WEP data encryption. Then configure the WEP keys.
WPA/WPA2	
Group Key Rekeying	The **Group Key Rekeying** field sets how often the AP (if using **WPA**(**2**)**-PSK** key management) or RADIUS server (if using **WPA**(**2**) key management) sends a new group key out to all clients.
Use WPA/WPA2 with Pre-shared Key	Select this radio button to use a pre-shared key for WPA or WPA2.
Pre-shared Key	Type a pre-shared key from 8 to 63 case-sensitive ASCII characters (including spaces and symbols).
Use WPA/WPA2 with RADIUS Server	Select this radio button to use a RADIUS server to authenticate the wireless clients.
Server IP	Enter the external authentication server's IP address (in dotted decimal notation).

Table 48 ADVANCED > WIRELESS (continued)

LABEL	DESCRIPTION
Authentication Port	You need not change this value unless your network administrator instructs you to do so with additional information.
Shared Secret Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the N4100. The key is not sent over the network. This key must be the same on the external authentication server and the N4100.
WEP	
Encryption	Select **64-bit** or **128-bit** for the WEP key length.
Mode	Select the type of input mode from the drop-down list box. Choices are **HEX** and **ASCII**. Select **ASCII** to enter the WEP keys as ASCII characters. Select **HEX** to enter the WEP keys as hexadecimal characters.
WEP Key 1 ... 4	Enter the WEP keys in the fields provided and select a key as the default key to use. If you select **64 bit** in the **WEP Encryption** field. Enter either 10 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example 11AA22BB33) for HEX key type or Enter 5 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example MyKey) for ASCII key type. If you select **128 bit** in the **WEP Encryption** field, Enter either 26 hexadecimal digits in the range of “A-F”, “a-f” and “0-9” (for example, 00112233445566778899AABBCC) for HEX key type or Enter 13 printable ASCII characters (case sensitive) ranging from “a-z”, “A-Z” and “0-9” (for example, MyKey12345678) for ASCII key type. The values for the WEP keys must be set up exactly the same on all wireless devices in the same wireless LAN. ASCII WEP keys are case sensitive.

Table 48 ADVANCED > WIRELESS (continued)

LABEL	DESCRIPTION
Authentication mode	There are two types of WEP authentication namely, **Open System** and **Shared Key**. **Open system** is implemented for ease-of-use and when security is not an issue. The wireless client and the AP or peer computer do not share a secret key. Thus the wireless clients can associate with any AP or peer computer and listen to any transmitted data that is not encrypted. **Shared key** mode involves a shared secret key to authenticate the wireless client to the AP or peer computer. This requires you to enable the wireless LAN security and use same settings on both the wireless client and the AP or peer computer. Select **Shared Key** to have the N4100 authenticate only those wireless clients that use **Shared Key** mode and have the correct WEP key. Select **Open System** to have the N4100 allow association with wireless clients that use **Open System** mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. Select **Both** to have the N4100 allow association with wireless clients that use **Open System** mode. Data transfer is encrypted as long as the wireless client has the correct WEP key for encryption. The N4100 authenticates wireless clients using **Shared Key** mode that have the correct WEP key.
Beacon Interval	Set the number of milliseconds that should pass between sending out a beacon. Enter a time period between 20 and 999. The default is **100**.
RTS Threshold	Enter a value between 1 and 2347 to enable an RTS/CTS handshake to avoid retransmitting due to hidden nodes.
Fragmentation Threshold	Enter a value between 256 and 2346 to enable a fragmentation threshold. This sets the maximum size of data fragments that can be sent. Use a low setting if there is a great deal of radio interference.
Preamble Type	Preamble is used to signal that data is coming to the receiver. Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11b compliant wireless devices support long preamble, but not all support short preamble. Select **Long Preamble** if you are unsure what preamble mode the wireless clients support, and to provide more reliable communications in busy wireless networks. Select **Short Preamble** if you are sure the wireless clients support it, and to provide more efficient communications. Select **Dynamic Preamble** to have the N4100 automatically use short preamble when wireless clients support it, otherwise the N4100 uses long preamble.
Default	Click this button to load the factory default wireless LAN settings.
Apply	Click this button to save your changes back to the N4100.

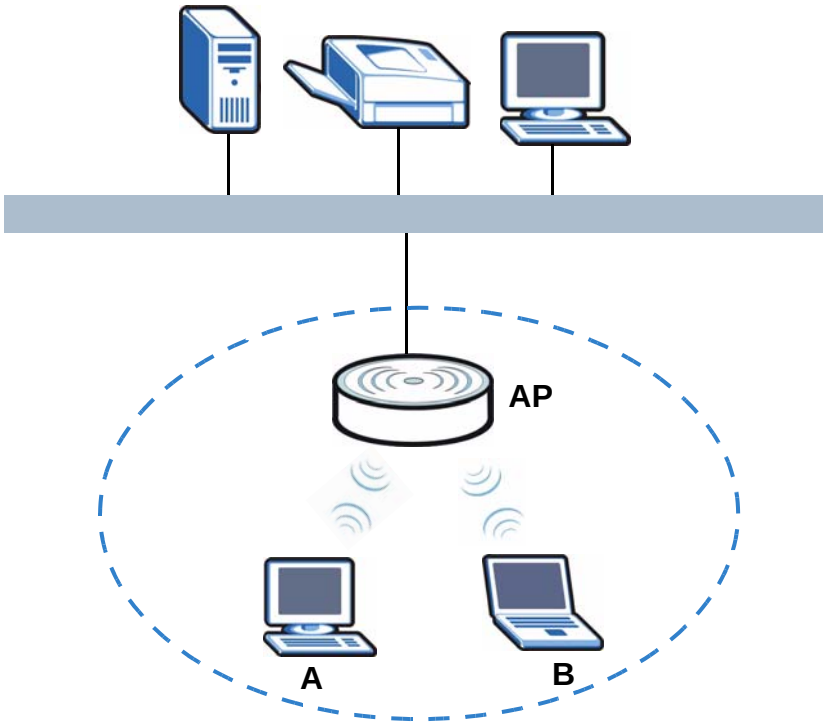
25.5 Technical Reference

This section discusses wireless LANs in depth. For more information, see the appendix.

25.5.1 Wireless Network Overview

The following figure provides an example of a wireless network.

Figure 93 Example of a Wireless Network



The wireless network is the part in the blue circle. In this wireless network, devices **A** and **B** use the access point (**AP**) to interact with the other devices (such as the printer) or with the Internet. Your N4100 is the AP.

Every wireless network must follow these basic guidelines.

- Every device in the same wireless network must use the same SSID.

  The SSID is the name of the wireless network. It stands for Service Set IDentifier.
- If two wireless networks overlap, they should use a different channel.

  Like radio stations or television channels, each wireless network uses a specific channel, or frequency, to send and receive information.

- Every device in the same wireless network must use security compatible with the AP.

  Security stops unauthorized devices from using the wireless network. It can also protect the information that is sent in the wireless network.

25.5.2 Additional Wireless Terms

The following table describes some wireless network terms and acronyms used in the N4100's Web Configurator.

Table 49 Additional Wireless Terms

TERM	DESCRIPTION
RTS/CTS Threshold	In a wireless network which covers a large area, wireless devices are sometimes not aware of each other's presence. This may cause them to send information to the AP at the same time and result in information colliding and not getting through. By setting this value lower than the default value, the wireless devices must sometimes get permission to send information to the N4100. The lower the value, the more often the devices must get permission. If this value is greater than the fragmentation threshold value (see below), then wireless devices never have to get permission to send information to the N4100.
Preamble	A preamble affects the timing in your wireless network. There are two preamble modes: long and short. If a device uses a different preamble mode than the N4100 does, it cannot communicate with the N4100.
Authentication	The process of verifying whether a wireless device is allowed to use the wireless network.
Fragmentation Threshold	A small fragmentation threshold is recommended for busy networks, while a larger threshold provides faster performance if the network is not very busy.

25.5.3 Wireless Security Overview

The following sections introduce different types of wireless security you can set up in the wireless network.

25.5.3.1 SSID

Normally, the N4100 acts like a beacon and regularly broadcasts the SSID in the area. You can hide the SSID instead, in which case the N4100 does not broadcast the SSID. In addition, you should change the default SSID to something that is difficult to guess.

This type of security is fairly weak, however, because there are ways for unauthorized wireless devices to get the SSID. In addition, unauthorized wireless devices can still see the information that is sent in the wireless network.

25.5.3.2 User Authentication

Authentication is the process of verifying whether a wireless device is allowed to use the wireless network. You can make every user log in to the wireless network before they can use it. However, every device in the wireless network has to support IEEE 802.1x to do this.

For wireless networks, you can store the user names and passwords for each user in a RADIUS server. This is a server used in businesses more than in homes. If you do not have a RADIUS server, you cannot set up user names and passwords for your users.

Unauthorized wireless devices can still see the information that is sent in the wireless network, even if they cannot use the wireless network. Furthermore, there are ways for unauthorized wireless users to get a valid user name and password. Then, they can use that user name and password to use the wireless network.

25.5.3.3 Encryption

Wireless networks can use encryption to protect the information that is sent in the wireless network. Encryption is like a secret code. If you do not know the secret code, you cannot understand the message.

The types of encryption you can choose depend on the type of authentication. (See Section 25.5.3.2 on page 200 for information about this.)

Table 50 Types of Encryption for Each Type of Authentication

	NO AUTHENTICATION	RADIUS SERVER
Weakest	No Security	
↕	Static WEP	
	WPA-PSK	WPA
Strongest	WPA2-PSK	WPA2

For example, if the wireless network has a RADIUS server, you can choose WPA or WPA2. If users do not log in to the wireless network, you can choose no encryption, static WEP, WPA-PSK, or WPA2-PSK.

Usually, you should set up the strongest encryption that every device in the wireless network supports. For example, suppose you have a wireless network with the N4100 and you do not have a RADIUS server. Therefore, there is no

authentication. Suppose the wireless network has two devices. Device A only supports WEP, and device B supports WEP and WPA. Therefore, you should set up static WEP in the wireless network.

Note: It is recommended that wireless networks use WPA-PSK, WPA, or stronger encryption. The other types of encryption are better than none at all, but it is still possible for unauthorized wireless devices to figure out the original information pretty quickly.

Many types of encryption use a key to protect the information in the wireless network. The longer the key, the stronger the encryption. Every device in the wireless network must have the same key.

26

Account Generator

26.1 Overview

This chapter shows you how to configure settings for the account generator (also known as the statement printer or “exclusive printer”).

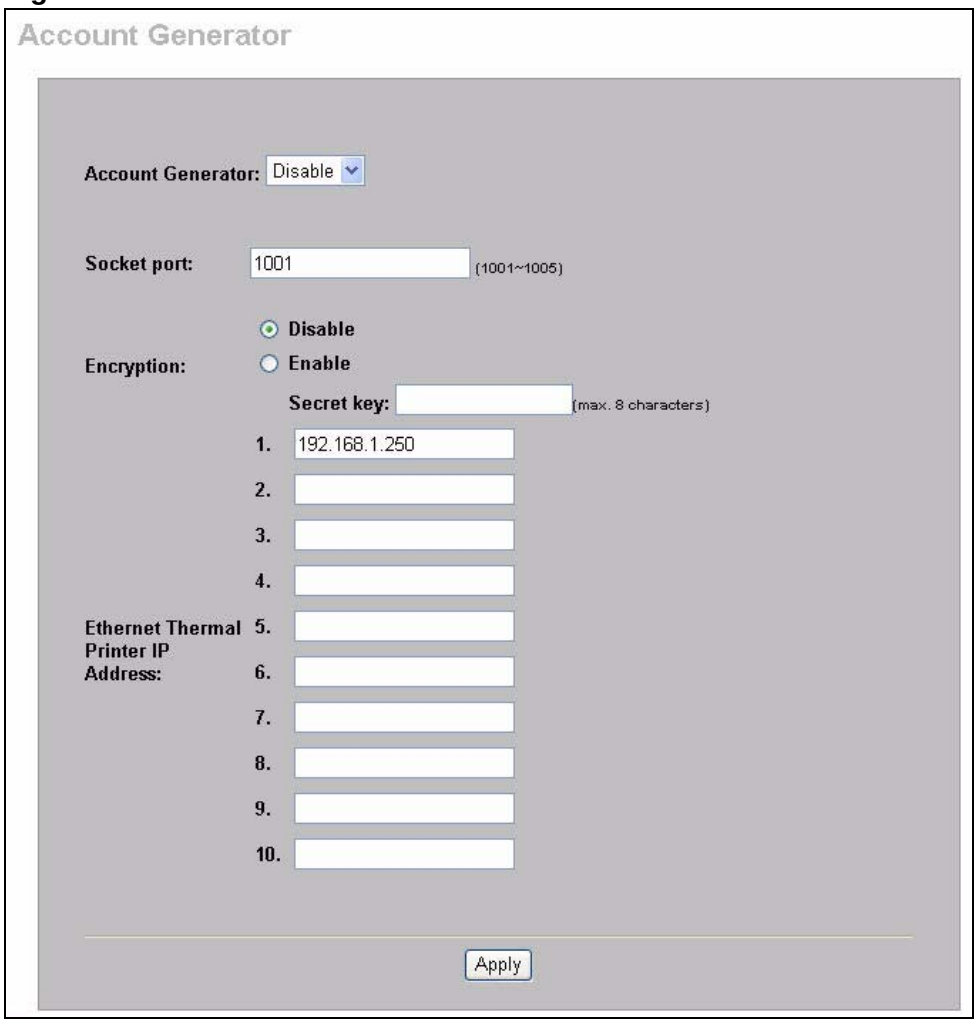
26.1.1 What You Can Do in this Chapter

Use the **Account Generator** screen (Section 26.2 on page 204) to configure the settings for using the N4100 with one or more account generators (statement printers).

26.2 The Account Generator Screen

Click **ADVANCED > ACCOUNT GENERATOR** to open this screen.

Figure 94 ADVANCED > ACCOUNT GENERATOR



The following table describes the fields in this screen.

Table 51 ADVANCED > ACCOUNT GENERATOR

LABEL	DESCRIPTION
Account Generator	Select **Enable** to use an account generator (statement printer) to generate subscriber accounts and print subscriber statements.
Socket port	This is the port number that your account generator (statement printer) uses. If you change this, make sure you also change it in the printer, see the printer's user's guide for how to do this.

Table 51 ADVANCED > ACCOUNT GENERATOR (continued)

LABEL	DESCRIPTION
Encryption	Turn on the encryption to encode the data that the N4100 sends to the statement printer(s). When you use the encryption, the data is unreadable to anyone that does not know the secret key. This protects against people stealing account information or creating illegitimate accounts. To use encryption, you must also configure the secret key in the following field and on the statement printer(s).
Secret key	When you use encryption, enter a code here. You can use up to 8 ASCII characters. You must also configure the same code as the secret key on the statement printer(s).
Ethernet Thermal Printer IP Address	This is the IP address that a statement printer uses. If you change this, make sure you also change it in the printer, see the printer's user's guide for how to do this. You can use multiple statement printers with the N4100. Each device on your network (including statement printers) must have a unique IP address. The port number however can be the same for more than one device.
Apply	Click this button to save your changes back to the N4100.

27

Licensing

27.1 Overview

This chapter shows you how to register your N4100 at myZyXEL.com and extend a service with your iCard's PIN number. At the time of writing, the N4100 can use the concurrent user upgrade service to extend the maximum number of the LAN/WLAN users that can connect to the N4100 at one time.

myZyXEL.com is ZyXEL's online services center where you can register your N4100 and manage subscription services available for the N4100.

Note: You need to create an account before you can register your device and activate the services at myZyXEL.com.

You can directly create a myZyXEL.com account and register your N4100 using the **Registration** screen. Alternatively, go to http://www.myZyXEL.com with the N4100's serial number and LAN MAC address to register it. Refer to the web site's on-line help for details. Check the sticker on the device's rear panel to see the N4100's serial number and LAN MAC address.

Note: To activate a service on a N4100, you need to access myZyXEL.com via that N4100.

27.1.1 What You Can Do in this Chapter

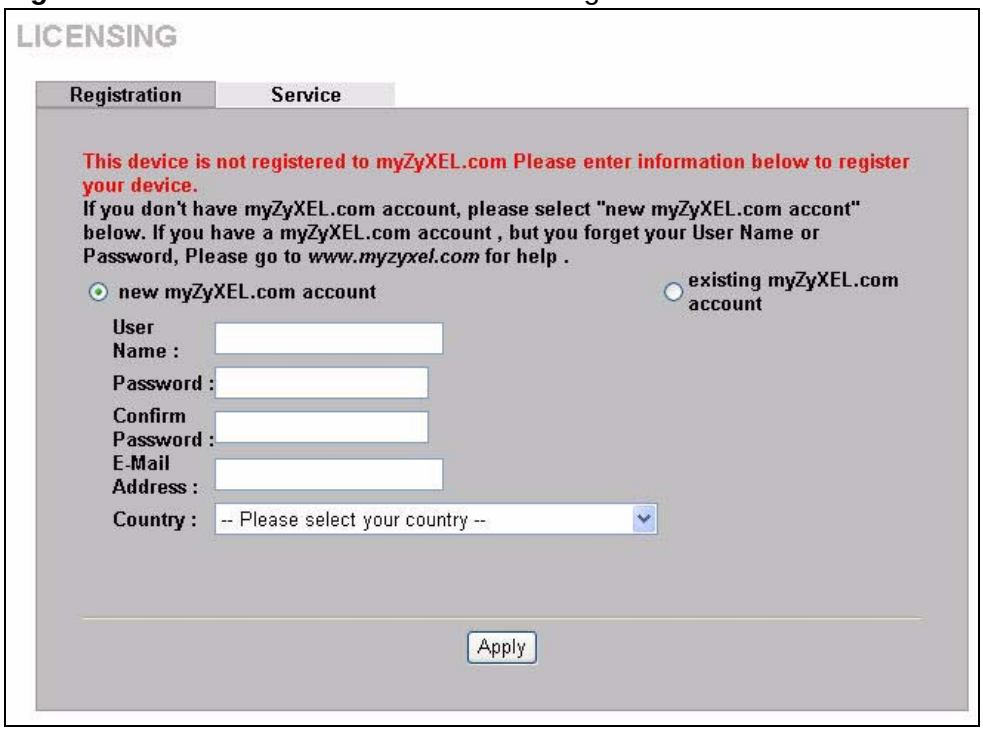
- Use the **Registration** screen (Section 26.2 on page 204) to register your N4100 with myZyXEL.com.
- Use the **Service** screen (Section 26.2 on page 204) to view the license status or enter your iCard's PIN number (license key) to upgrade a service subscription.

27.2 The Registration Screen

Click **ADVANCED > LICENSING > Registration** to open this screen.

Note: If the N4100 is registered already, this screen is read-only. Use the **Service** screen to upgrade a service and update your service subscription status.

Figure 95 ADVANCED > LICENSING > Registration



The following table describes the fields in this screen.

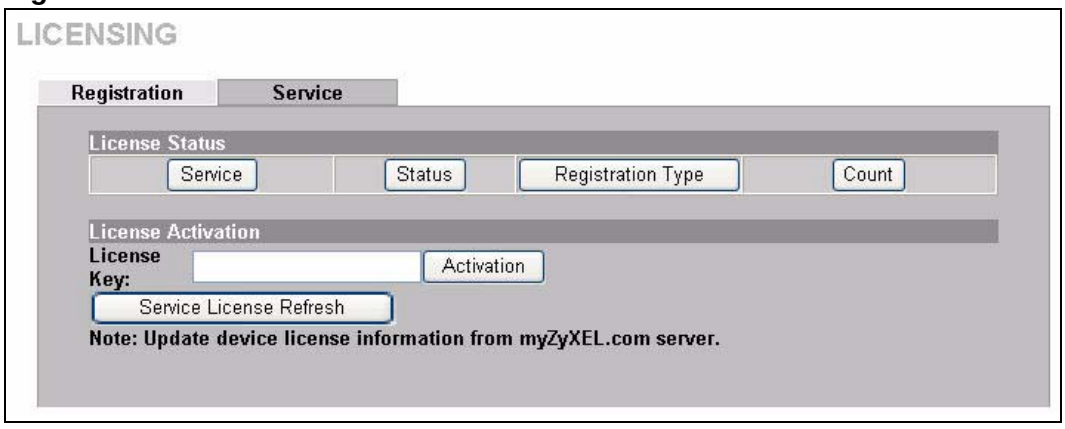
Table 52 ADVANCED > LICENSING > Registration

LABEL	DESCRIPTION
New myZyXEL.com account	If you haven't created an account at myZyXEL.com, select this option and configure the following fields to create an account and register your N4100.
Existing myZyXEL.com account	If you already have an account at myZyXEL.com, select this option and enter your user name and password in the fields below to register your N4100.
User Name	Enter a user name for your myZyXEL.com account. The name should be from six to 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Password	Enter a password of between six and 20 alphanumeric characters (and the underscore). Spaces are not allowed.
Confirm Password	Enter the password again for confirmation.
E-Mail Address	Enter your e-mail address. You can use up to 80 alphanumeric characters (periods and the underscore are also allowed) without spaces.
Country	Select your country from the drop-down box list.
Apply	Click this button to save your changes back to the N4100.

27.3 The Service Screen

Click **ADVANCED > LICENSING > Service** to open this screen.

Figure 96 ADVANCED > LICENSING > Service



The following table describes the fields in this screen.

Table 53 ADVANCED > LICENSING > Service

LABEL	DESCRIPTION
License Status	
Service	This field displays the service name available on the N4100.
Status	This field displays **Licensed** when the N4100 is registered and a service is activated.
Registration Type	This field displays **Standard** when the N4100 is registered and a service is activated.
Count	This field displays the current maximum number of wired and wireless users that may connect to the N4100 at the same time.
License Activation	
License Key	Enter your iCard's PIN number and click **Activation** to extend the concurrent user number from 100 (default) to 200. To upgrade the service, you need to buy an iCard or e-iCard (specific to the service supported by your N4100) and enter the PIN number to extend the service.
Service License Refresh	If you restore the N4100 to the default configuration or upload a different configuration file after you register, click this button to update service license information.

28

System Status

28.1 Overview

This chapter describes the **System Status** screens.

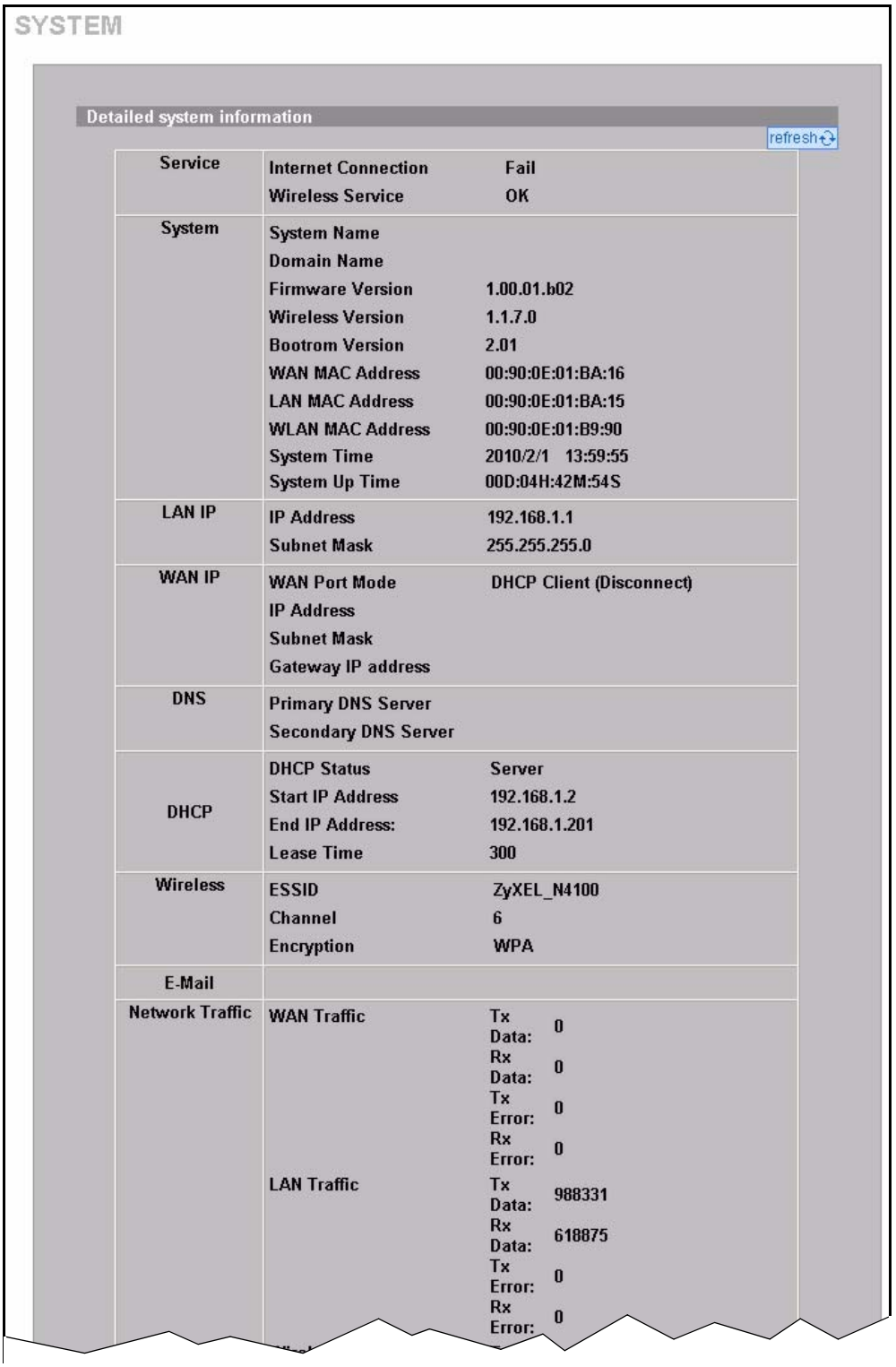
28.1.1 What You Can Do in this Chapter

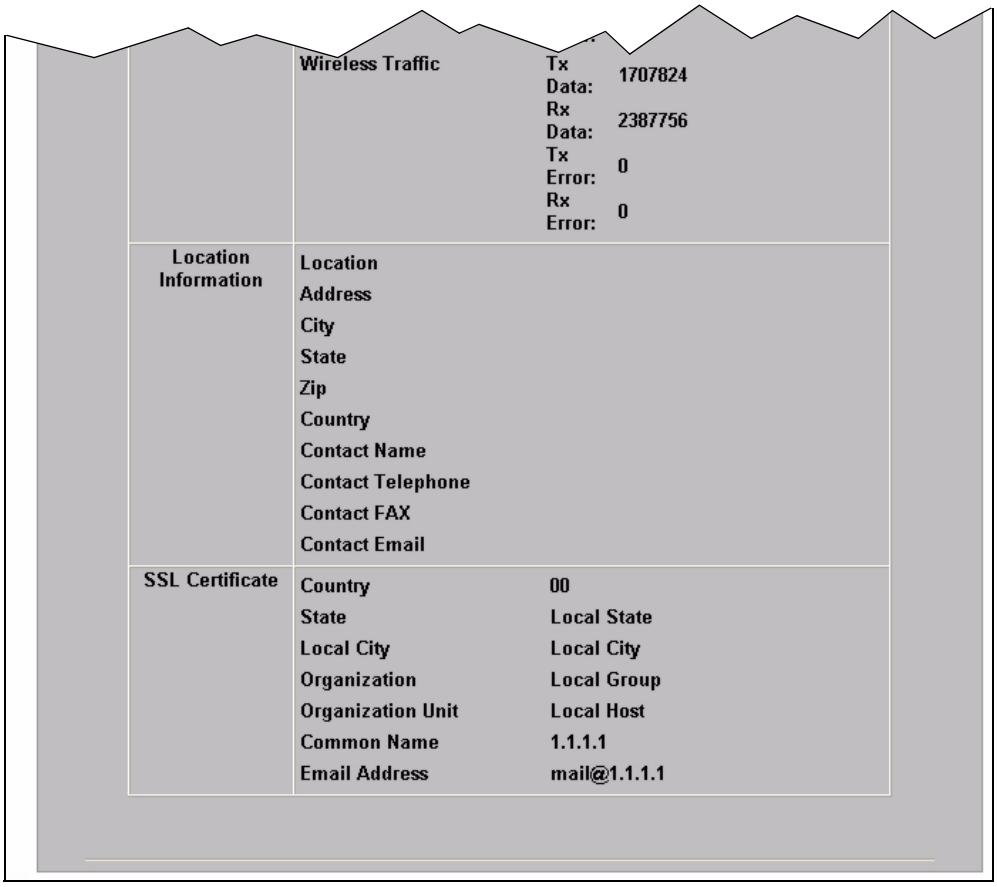
- Use the **System** screen (Section 28.2 on page 212) to view the current state of the N4100.
- Use the **Account List** screen (Section 28.3 on page 216) to view the subscriber account list.
- Use the **Account Log** screen (Section 28.4 on page 218) to display information on the N4100's subscriber account logs.
- Use the **Current User** screen (Section 28.5 on page 220) to display a list of subscribers currently logged on to the N4100 for Internet access.
- Use the **DHCP Client** screen (Section 28.6 on page 221) to view current DHCP client information of all network clients using the DHCP server on the N4100.
- Use the **Session List** screen (Section 28.7 on page 222) to display a list of incoming and outgoing packet information.
- Use the **LAN Devices** screen (Section 28.8 on page 223) to display the status of LAN devices configured in the **ADVANCED > LAN DEVICES** screen.

28.2 The System Screen

Click **SYSTEM STATUS > SYSTEM** to open this screen.

Figure 97 SYSTEM STATUS > SYSTEM





The following table describes the labels in this screen.

Table 54 SYSTEM STATUS > SYSTEM

LABEL	DESCRIPTION
Service	
Internet Connection	This field displays the status of the N4100's connection to the Internet.
Wireless Service	This field displays the status of the N4100's wireless LAN.
System	
System Name	This field displays the description name of the N4100 for identification purposes.
Domain Name	This field displays the domain name of the N4100.
Firmware Version	This field displays the version of the firmware on the N4100.
Wireless Version	This field displays the version of the wireless features on the N4100.
Bootrom Version	This field displays the version of the bootbase in the N4100.

Table 54 SYSTEM STATUS > SYSTEM (continued)

LABEL	DESCRIPTION
WAN MAC Address	This field displays the MAC address of the N4100 on the WAN.
LAN MAC Address	This field displays the MAC address of the N4100 on the LAN.
WLAN MAC Address	This field displays the MAC address of the N4100 on the WLAN.
System Time	This field displays the N4100's current time.
System Up Time	This field displays the how long the N4100 has been operating since it was last started.
LAN IP	
IP Address	This field displays the IP address of the LAN port on the N4100.
Subnet Mask	This field displays the subnet mask of the LAN port on the N4100.
WAN IP	
WAN Port Mode	This field displays the DHCP mode of the WAN port. It displays **DHCP Client**, **Static IP Setting**, **PPPoE** or **PPTP**.
IP Address	This field displays the IP address of the WAN port on the N4100.
Subnet Mask	This field displays the subnet mask of the WAN port on the N4100.
Gateway IP address	This field displays the IP address of the default gateway of the WAN port on the N4100.
DNS	
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
DHCP	
DHCP Status	This field displays the DHCP mode on the LAN.
Start IP Address	This field displays the first of the continuous addresses in the IP address pool.
End IP Address	This field displays the last of the continuous addresses in the IP address pool.
Lease Time	This field displays the time period (in minutes between 1 and 71582788) during which a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Wireless	
ESSID	This field displays the N4100's Extended Service Set IDentity.
Channel	This field displays the channel that the N4100 is using.
Encryption	This field displays the type of data encryption that the N4100 is using. **WEP** displays if the N4100 is using WEP data encryption. **WPA** displays if N4100 is using WPA data encryption. **WPA2** displays if N4100 is using WPA2 data encryption. **Disable** displays if the N4100 is not using data encryption.
E-mail	This field displays the IP address or the domain name of the SMTP server.

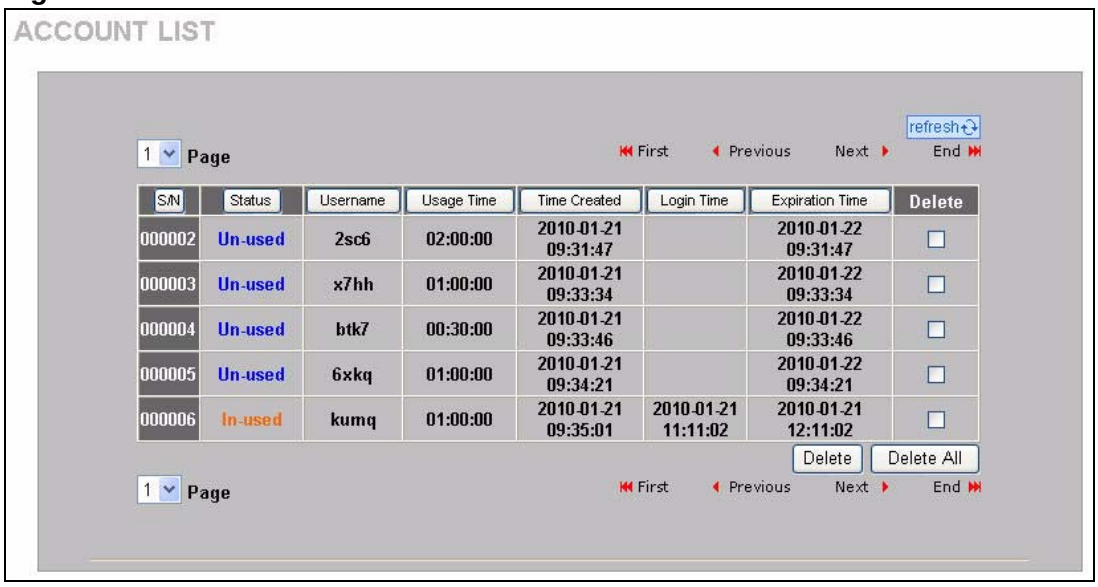
Table 54 SYSTEM STATUS > SYSTEM (continued)

LABEL	DESCRIPTION
Network Traffic	
WAN Traffic	This field displays traffic statistics for the N4100's WAN connection.
LAN Traffic	This field displays traffic statistics for the N4100's LAN connection.
Wireless Traffic	This field displays traffic statistics for the N4100's wireless LAN connection.
Location Information	
Location	This field displays the device's geographical location.
Address	This field displays the street address of the device's location.
City	This field displays the city of the device's location.
State	This field displays the state or province of the device's location.
ZIP	This field displays the zip code or postal code for the device's location.
Country	This field displays the country of the device's location.
Contact Name	This field displays the name of the person responsible for this device.
Contact Telephone	This field displays the telephone number of the person responsible for this device.
Contact FAX	This field displays the fax number of the person responsible for this device.
Contact Email	This field displays the e-mail address of the person responsible for this device.
SSL Certificate	
Country	This field displays the two-letter abbreviation of your country.
State	This field displays the name of the state or province where your organization is located.
Local City	This field displays the name of the city your organization is located.
Organization	This field displays the name of your organization.
Origination Unit	This field displays additional information about your organization.
Common Name	This field displays the fully qualified domain name of your web server.
Email Address	This field displays your e-mail address.

28.3 The Account List Screen

Click **SYSTEM STATUS > ACCOUNT LIST** to open this screen.

Figure 98 SYSTEM STATUS > ACCOUNT LIST



The following table describes the labels in this screen.

Table 55 SYSTEM STATUS > ACCOUNT LIST

LABEL	DESCRIPTION
refresh	Click **refresh** to update this screen.
S/N	This field displays the serial number of an account. The maximum number of subscriber account entries is 512. Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time (specified in the **ADVANCED > ACCOUNTING** screen), the account is deleted from the account list.
Status	This field displays **In-used** when the account is currently in use. Otherwise it displays **Un-used**.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.
Time Created	This field displays when the account was created (in yyyy/mm/dd hh/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd hh/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.

Table 55 SYSTEM STATUS > ACCOUNT LIST (continued)

LABEL	DESCRIPTION
Expiration Time	This field displays when the subscriber's account becomes invalid (in yyyy/mm/dd hh/mm/ss format). When the subscriber has already logged into the account, this field displays the time until which the subscriber can continue to use the account to access the Internet. This field displays the time that the account expires if the subscriber does not log into it. Click the heading to sort the entries in ascending or descending order based on this column.
Delete	Select the **Delete** check box(es) next to individual accounts and click **Delete** to remove the selected accounts.
Delete All	Click **Delete All** to remove all accounts.
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.

28.4 The Account Log Screen

Click **SYSTEM STATUS > ACCOUNT LOG** to open this screen. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries if applicable.

Figure 99 SYSTEM STATUS > ACCOUNT LOG

The following table describes the labels in this screen.

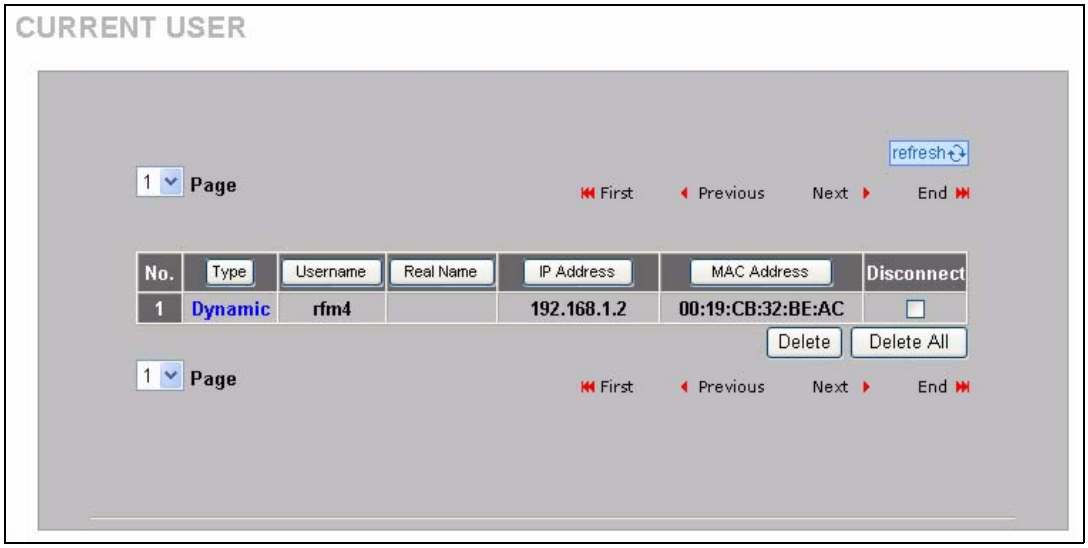
Table 56 SYSTEM STATUS > ACCOUNT LOG

LABEL	DESCRIPTION
Export	Click **Export** to save the log to a computer.
Clear Log	Click **Clear Log** to remove all of the log entries from the N4100's memory and this screen.
Refresh	Click **Refresh** to update this screen.
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.
S/N	This field displays the index number of an entry. The maximum number of user account entries is 512.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Time Created	This field displays when the account was created (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Login Time	This field displays when the subscriber logged in to use the account (in yyyy/mm/dd HH/mm/ss format). Click the heading to sort the entries in ascending or descending order based on this column.
Usage Time	This field displays the amount of time the subscriber has purchased. Click the heading to sort the entries in ascending or descending order based on this column.
Charge	This field displays the total cost of the subscriber's account.
Payment Info	This field displays the subscriber's method of payment cash or credit.
Status	This field displays **IN-Used** when the account is currently in use. Otherwise it displays **Un-used**. This field displays **Finished** when a subscriber uses up the time allocated to an account. This field displays **Expired** when a subscriber does not log into the account and the account has reached expiration. This field displays **Delete** when a subscriber's account is removed from the account list before it expires. This field displays **Replenished** and the serial number of the subscriber's account when a subscriber has purchased additional time units for the account.

28.5 The Current User Screen

Click **SYSTEM STATUS > CURRENT USER** to open this screen. Click a column heading to sort the entries if applicable.

Figure 100 SYSTEM STATUS > CURRENT USER



The following table describes the labels in this screen.

Table 57 SYSTEM STATUS > CURRENT USER

LABEL	DESCRIPTION
Refresh	Click **Refresh** to update this screen.
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.
No.	This field displays the index number of the entry.
Type	This field displays the type of account that the user has. **Dynamic** means the account is created automatically using a statement printer or web configurator. **No-Auth** means subscriber authentication is disabled on the N4100. The **Username** and **Real Name** fields are not available. **Super User** means the account is a super subscriber system account. Any one logs in using this account can access the Internet for free. See Chapter 30 on page 239 for more information. **RADIUS** means the account is created on an accounting server (RADIUS).

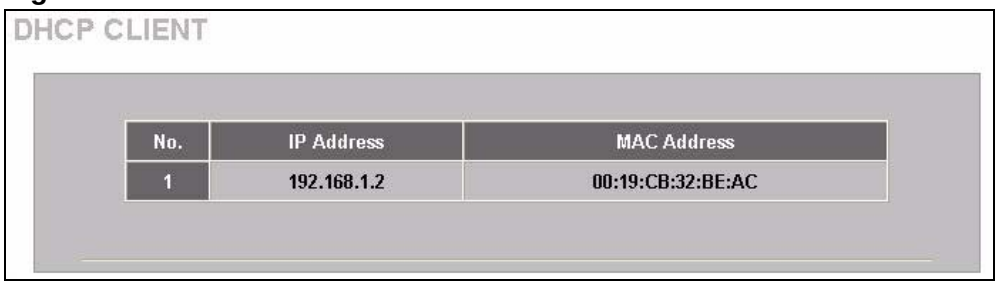
Table 57 SYSTEM STATUS > CURRENT USER (continued)

LABEL	DESCRIPTION
Username	This field is displayed only if any subscribers are using the system. This field displays the username currently used by the account.
Real Name	This field displays the descriptive name entered by the user when he or she logs into the account.
IP Address	This field displays the IP address of a subscriber's computer.
MAC Address	This field displays the MAC address of the computer that is logged in using the account.
Disconnect	This field is displayed only if any subscribers are using the system. Select this(ese) check box(es) and click **Delete** to terminate the selected subscriber connection.
Delete All	Click this button to terminate all subscriber connections.

28.6 The DHCP Client Screen

Click **SYSTEM STATUS > DHCP CLIENT** to open this screen.

Figure 101 SYSTEM STATUS > DHCP CLIENT



The following table describes the labels in this screen.

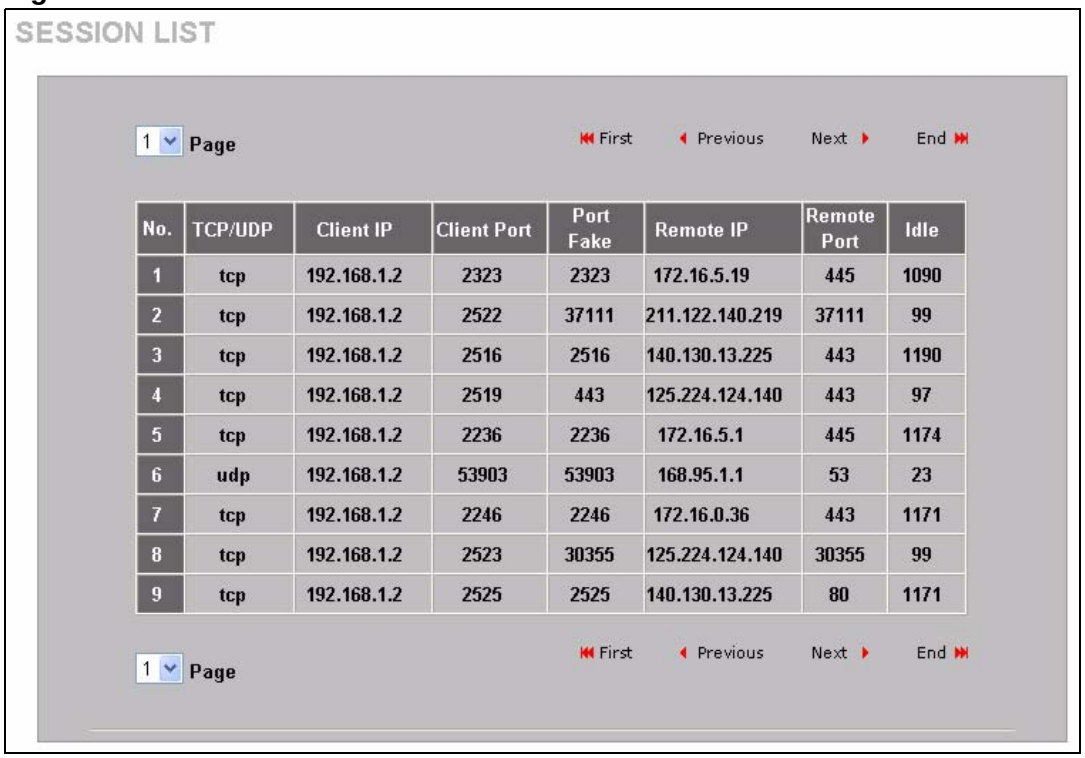
Table 58 SYSTEM STATUS > DHCP CLIENT

LABEL	DESCRIPTION
No.	This field displays the index number of the entry.
IP Address	This field displays the IP address assigned to the client computer.
MAC Address	This field displays the MAC address of the client computer. The MAC (Media Access Control) or Ethernet address on a LAN (Local Area Network) is unique to your computer (six pairs of hexadecimal characters). A network interface card such as an Ethernet adapter has a hardwired address that is assigned at the factory. This address follows an industry standard that ensures no other adapter has a similar address.

28.7 The Session List Screen

Click **SYSTEM STATUS > SESSION LIST** to open this screen.

Figure 102 SYSTEM STATUS > SESSION LIST



The following table describes the labels in this screen.

Table 59 SYSTEM STATUS > SESSION LIST

LABEL	DESCRIPTION
Page	Select a page number from the drop-down list box to display the selected page.
First	Click **First** to go to the first page.
Previous	Click **Previous** to return to the previous page.
Next	Click **Next** to go to the next page.
End	Click **End** to go to the last page.
No.	This field displays the index number of an entry.
TCP/UDP	This field displays the type of traffic (**TCP** or **UDP**).
Client IP	This field displays the IP address of the client computer.
Client Port	This field displays the port number through which the client computer transmits the traffic.
Port Fake	This field displays the NAT port to and from which the N4100 maps the session's traffic.
Remote IP	This field displays the IP address of a remote device the client computer accesses.

Table 59 SYSTEM STATUS > SESSION LIST (continued)

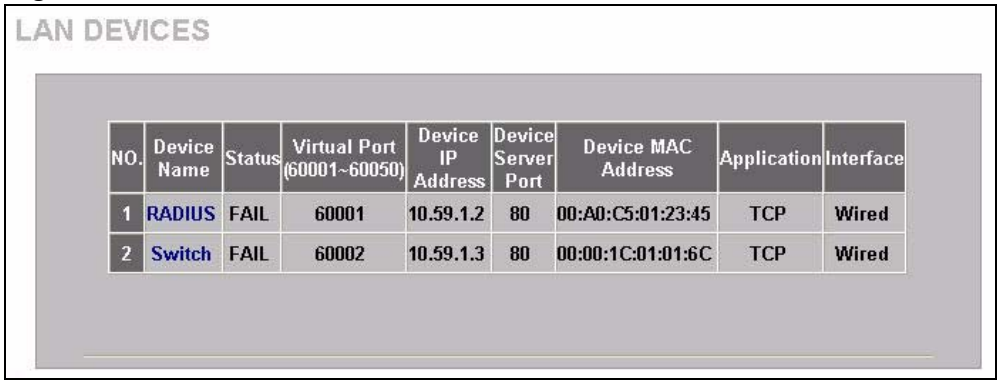
LABEL	DESCRIPTION
Remote Port	This field displays the port number of a remote device the client computer accesses.
Idle	This field displays how many seconds are left before the session times out if there is no more traffic. The N4100 automatically times out idle TCP sessions after 5 minutes (300 seconds). The N4100 automatically times out idle UDP sessions after 1 minute (60 seconds).

28.8 The LAN Devices Screen

The **SYSTEM STATUS > LAN DEVICES** screen displays the status of LAN devices configured in the **ADVANCED > LAN DEVICES** screen (refer to Chapter 19 on page 163).

Click **SYSTEM STATUS > LAN DEVICES** to open this screen. This screen automatically updates every minute.

Figure 103 SYSTEM STATUS > LAN DEVICES



The following table describes the labels in this screen.

Table 60 SYSTEM STATUS > LAN DEVICES

LABEL	DESCRIPTION
NO.	This field displays the index number.
Device Name	This field displays the name of the LAN device. Click the device name to access the LAN device if the **Status** field is **OK**.
Status	This field displays the current status of the LAN device. It displays **OK** when the LAN device is turned on and working properly. Otherwise it displays **FAIL**.
Virtual Port (60001-60050)	This field displays the virtual port number.
Device IP Address	This field displays the IP address of the LAN device.

Table 60 SYSTEM STATUS > LAN DEVICES (continued)

LABEL	DESCRIPTION
Device Server Port	This field displays the server port number of the LAN device.
Device MAC Address	This field displays the MAC address of the LAN device.
Application	This field displays the type of application packet that is forwarded to the LAN device.
Interface	This field displays to which interface on the N4100 the LAN device is connected.

28.8.1 Accessing a LAN Device

Before you can access a LAN device behind the N4100, the following requirements must be met.

- The LAN device has a web-based management interface and it is enabled.
- You have set up the virtual port mapping to the LAN device server port in the **ADVANCED > LAN DEVICES** screen.
- The LAN device status is **OK** in the **SYSTEM STATUS > LAN DEVICES** screen.

There are two methods to access the LAN device: directly or through the web configurator.

1 To access the LAN device through the web configurator, open the **SYSTEM STATUS > LAN DEVICES** screen and click the device name. A new Internet browser should display showing the login screen of the LAN device management interface.

2 To directly access the LAN device, enter the WAN IP address of your N4100 and the virtual port number of the LAN device separated by a colon. For example, enter “http:// 192.168.1.1:60001” where 192.168.1.1 is the WAN IP address of the N4100. The login screen of the LAN device management interface should display.

29

Configuration and Firmware

29.1 Overview

This chapter explains how to manage configuration files and upload new firmware.

Use the instructions in this chapter to change the device's configuration file or upgrade its firmware. After you configure your device, you can backup the configuration file to a computer. That way if you later misconfigure the device, you can upload the backed up configuration file to return to your previous settings. You can alternately upload the factory default configuration file if you want to return the device to the original default settings. The firmware determines the device's available features and functionality.

29.1.1 Some Warnings

The following are some friendly reminders about your device:

Do NOT turn off the N4100 while a firmware upload is in progress!

Only use firmware for your device's specific model.

29.1.2 What You Can Do in this Chapter

- Use the **Firmware** screen (Section 29.3 on page 232) to upload firmware to your N4100.
- Use the **Configuration** screen (Section 29.2 on page 226) to backup and restore device configurations. You can also reset your device settings back to the factory default.

29.1.3 What You Need To Know

Filename Conventions

The configuration file (often called the romfile) contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. It has a

“cfg” filename extension. Once you have customized the N4100's settings, they can be saved back to your computer under a filename of your choosing.

The system firmware has a “bin” filename extension. Find this firmware at www.zyxel.com. With many FTP clients, the filenames are similar to those seen next.

29.2 The Configuration Screen

You can use the web configurator to perform configuration file backup and restore. Backing up the configuration allows you to back up (save) the device’s current configuration to a file. Once your device is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

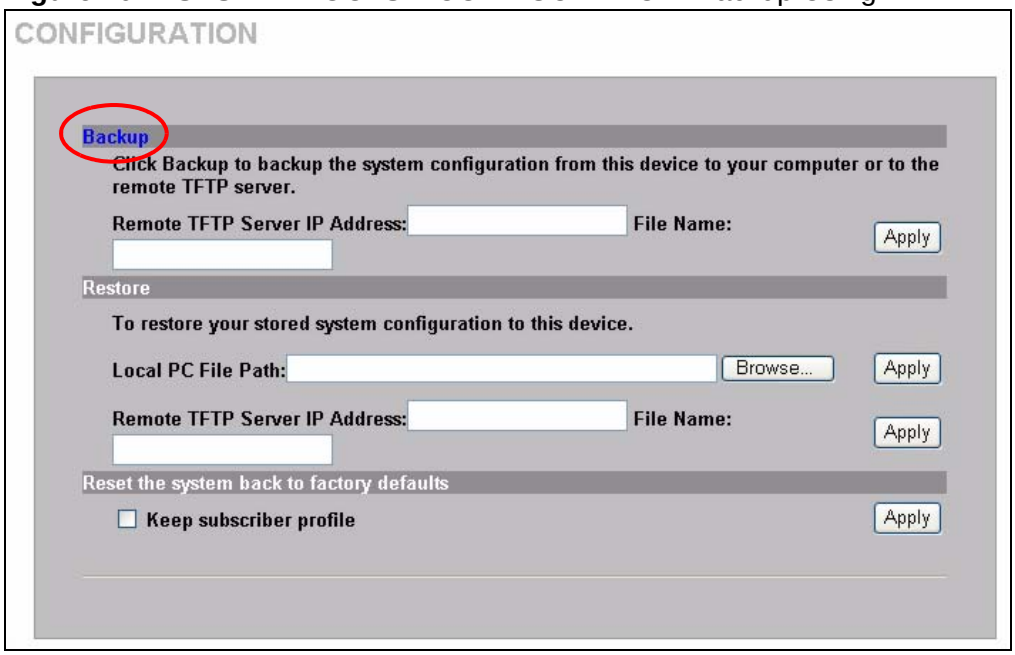
WARNING!
DO NOT INTERRUPT THE FILE TRANSFER PROCESS AS THIS MAY PERMANENTLY DAMAGE YOUR DEVICE.

29.2.1 Backup Configuration Using HTTP

Use the following procedure to use HTTP to back up the device’s current configuration to a file on your computer.

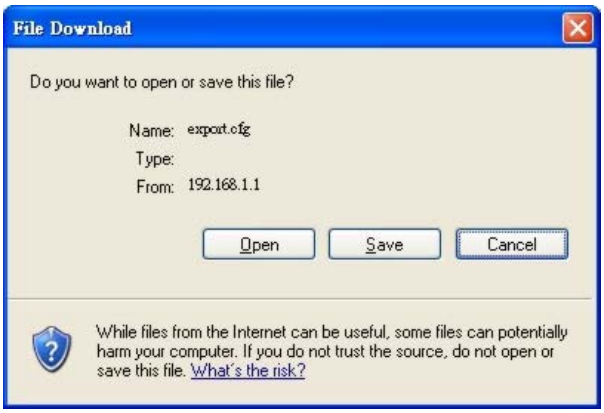
1 Click **SYSTEM TOOLS > CONFIGURATION**. A screen displays as shown next. Click **Backup**.

Figure 104 SYSTEM TOOLS > CONFIGURATION: Backup Using HTTP



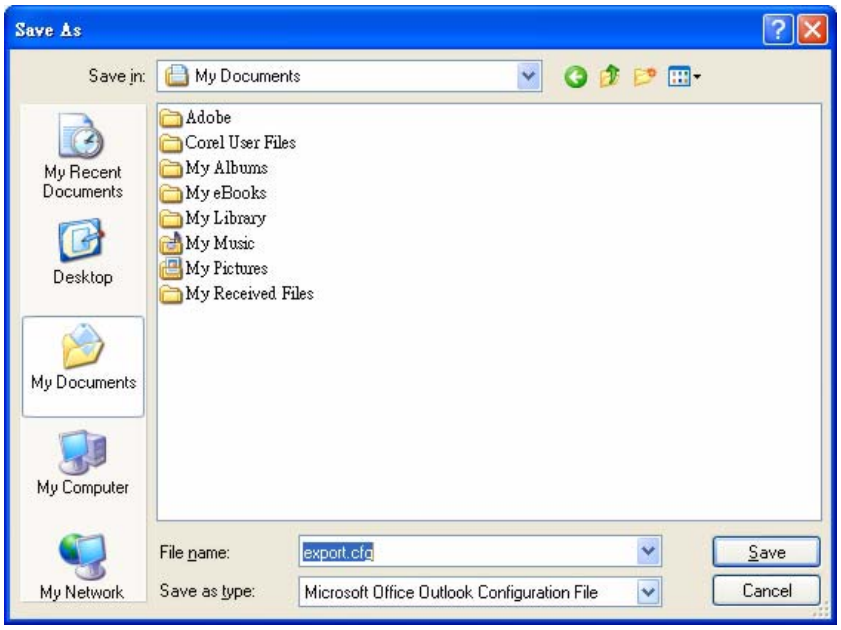
2 A **File Download** window displays as shown next. Click **Save**.

Figure 105 Configuration Backup: File Download



3 A **Save As** window displays.

Figure 106 Configuration Backup: Save As



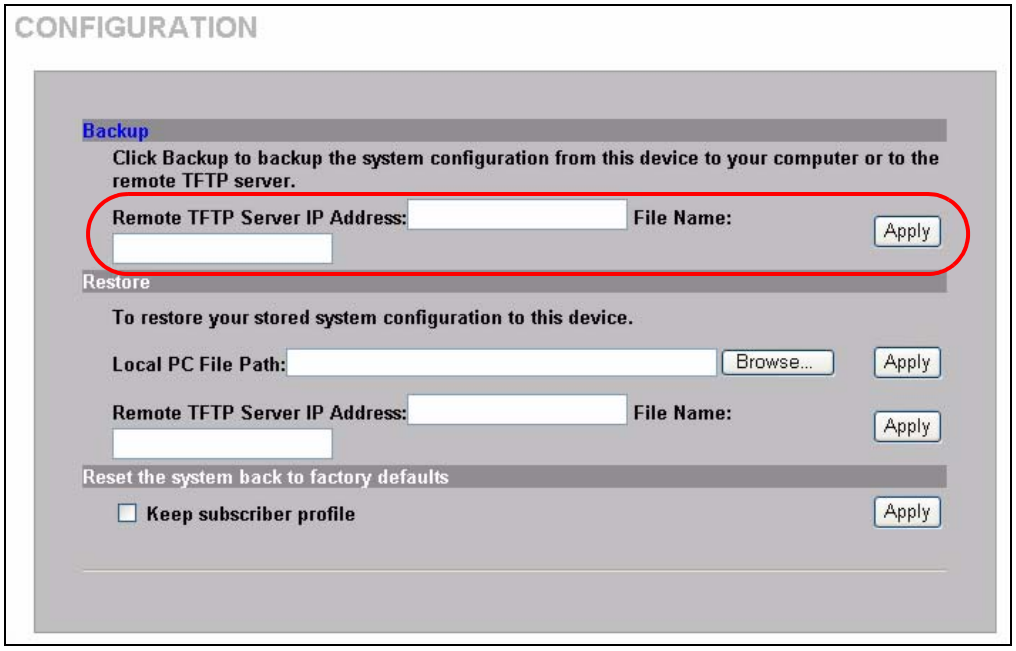
4 Specify the file name and/or location and click **Save** to start the backup process.

29.2.2 Backup Configuration Using TFTP

Use the following procedure to use TFTP to back up the device's current configuration to a file on a TFTP server.

1 Click **SYSTEM TOOLS** > **CONFIGURATION**. A screen displays as shown next.

Figure 107 SYSTEM TOOLS > CONFIGURATION: Backup Using TFTP



2 Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.

3 Specify a file name for the configuration backup in the **File Name** field.

4 Click **Apply**. When the file transfer process is complete, a screen displays as follows.

Figure 108 Configuration Backup: Using TFTP Successful

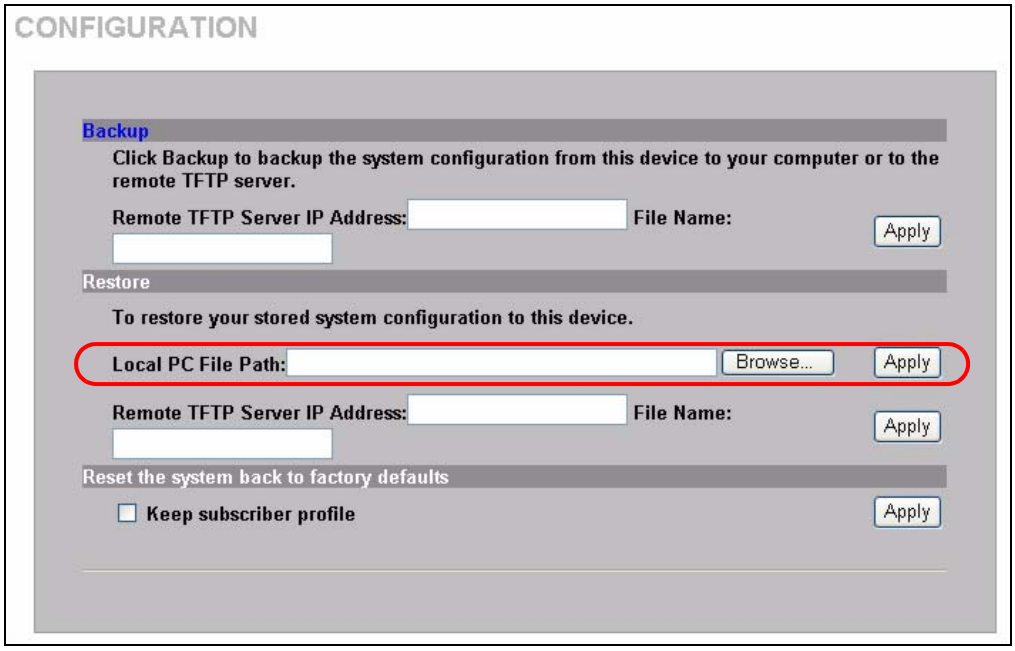
29.2.3 Restore Configuration Using HTTP

This section shows you how to upload a new or previously saved configuration file from your computer to your N4100.

Note: This function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

1 Click **SYSTEM TOOLS** > **CONFIGURATION**. A screen displays as shown next.

Figure 109 SYSTEM TOOLS > CONFIGURATION: Restore Using HTTP



2 Specify the location and filename of a configuration file in the **Local PC File Path** field or click **Browse**.

3 Click **Apply** to start the configuration restore process. The N4100 automatically restarts after the restoration process is complete.

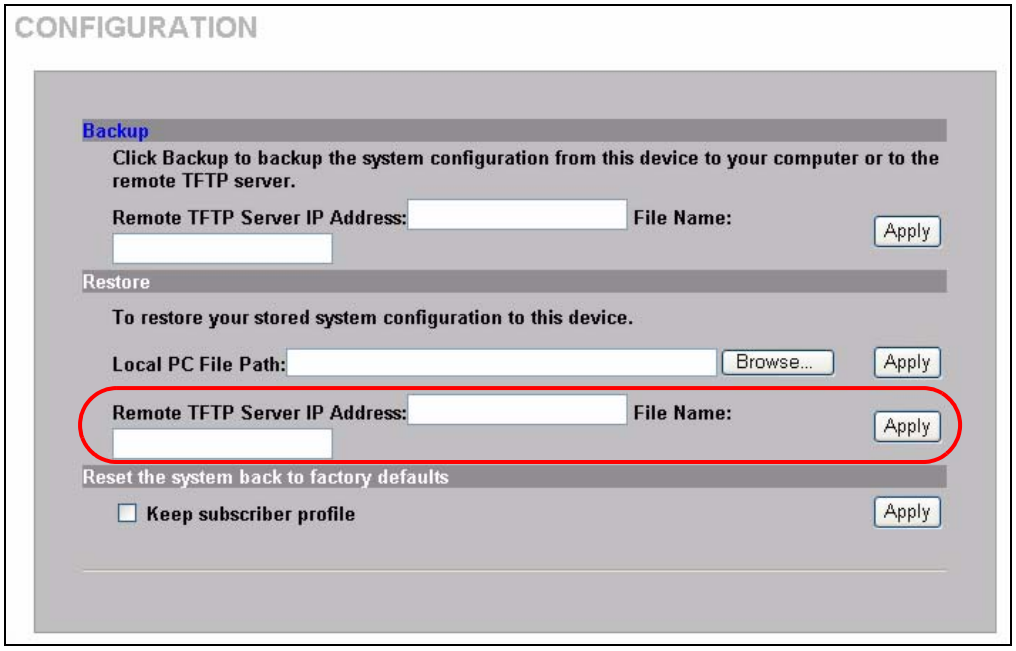
29.2.4 Restore Configuration Using TFTP

This section shows you how to upload a new or previously saved configuration file from a TFTP server to your N4100.

Note: This function erases the current configuration before restoring a previous back up configuration; please do not attempt to restore unless you have a backup configuration file stored on disk.

1 Click **SYSTEM TOOLS** > **CONFIGURATION**. A screen displays as shown next.

Figure 110 SYSTEM TOOLS > CONFIGURATION: Restore Using TFTP



2 Enter the IP address of the TFTP server in dotted decimal notation in the **Remote TFTP Server IP Address** field.

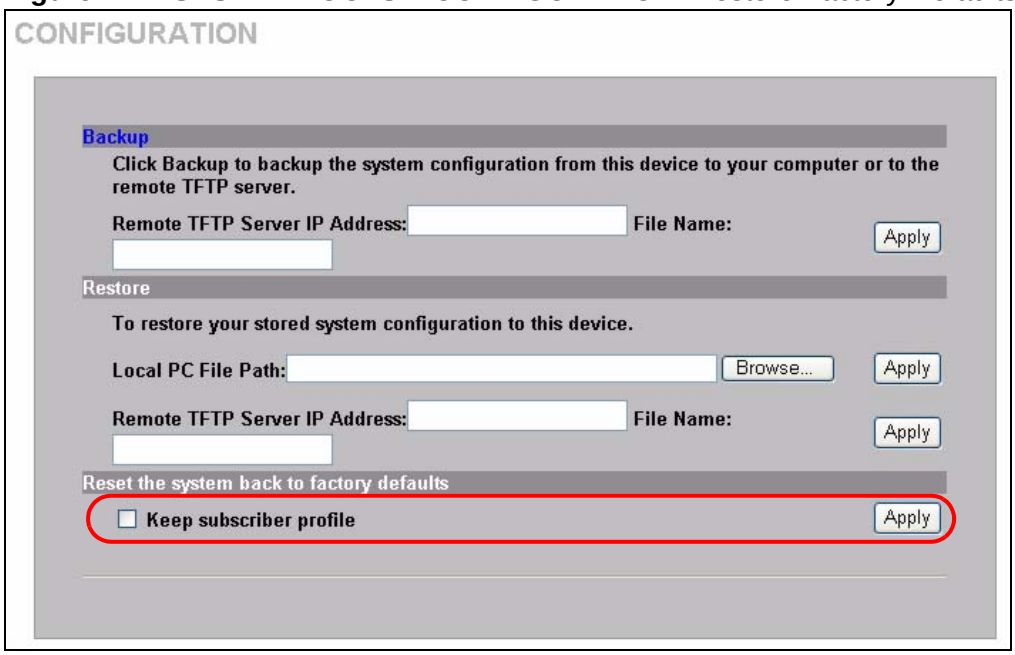
3 Specify the file name of the configuration file in the **File Name** field.

4 Click **Apply** to start the configuration restore process. The N4100 automatically restarts after the restoration process is complete.

29.2.5 Restore Factory Defaults

To reset the N4100 back to the factory defaults, click **SYSTEM TOOLS > CONFIGURATION** to display the screen as shown next.

Figure 111 SYSTEM TOOLS > CONFIGURATION: Restore Factory-Defaults



The following table describes the labels in this screen.

Table 61 SYSTEM TOOLS > CONFIGURATION: Restore Factory-Defaults

LABEL	DESCRIPTION
Reset the system back to factory defaults	
Keep subscriber profile	Select this option to reset the system configuration back to the factory default but retain subscriber account information. All other custom configuration is erased.
Apply	Click **Apply** to reset system configuration back to the factory defaults.

29.3 The Firmware Screen

There are two ways to upgrade firmware to the N4100: manually or scheduled.

To manually upgrade the firmware, you have to download the latest firmware first from www.zyxel.com and then upload it to the N4100. You can upload it to the N4100 using the Web Configurator or using a TFTP server.

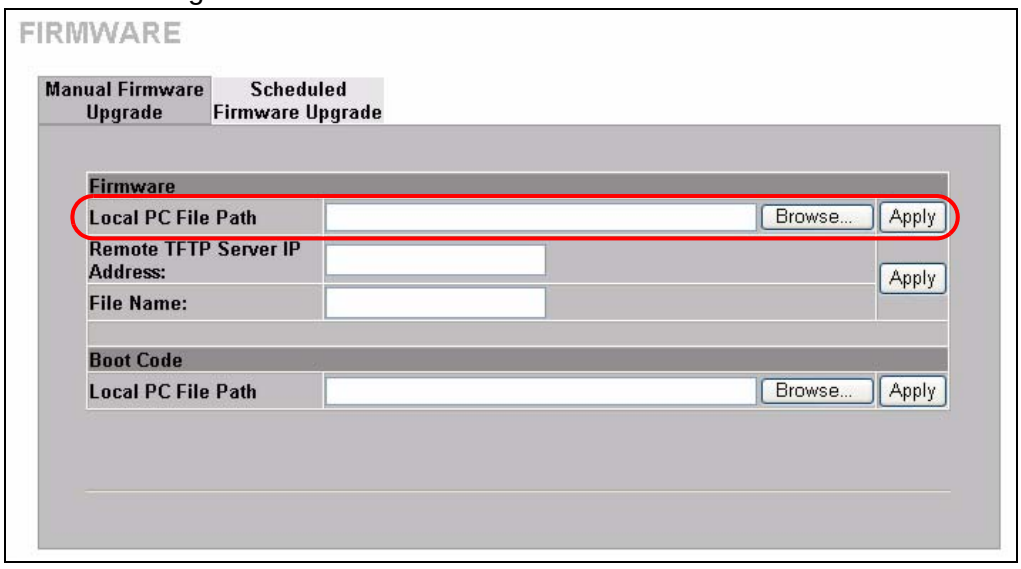
With scheduled firmware upgraded, you need to set up a TFTP server where the N4100 can automatically download the latest firmware at the specified time.

29.3.1 Manual Firmware Upgrade Using the Web Configurator

Follow the steps below to upload the firmware using the web configurator.

1 Click **SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 112 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Using the Web Configurator

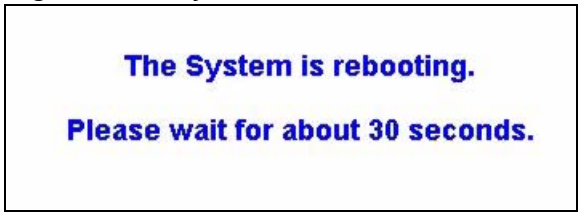


2 Specify the name of the firmware file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The firmware must be a binary file and should have a .bin extension.

3 When the file transfer is completed successfully, a restart message displays and the N4100 automatically restarts.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

Figure 113 System Restart



4 After the N4100 finishes restarting, access the web configurator again. Check the firmware version number in the **System Quick View** screen.

Note: When the N4100 restarts, all connections terminate. Subscribers need to log in again.

29.3.2 Manual Firmware Upgrade via TFTP Server

Use the following procedure to use TFTP to upload the firmware from a TFTP server to the N4100.

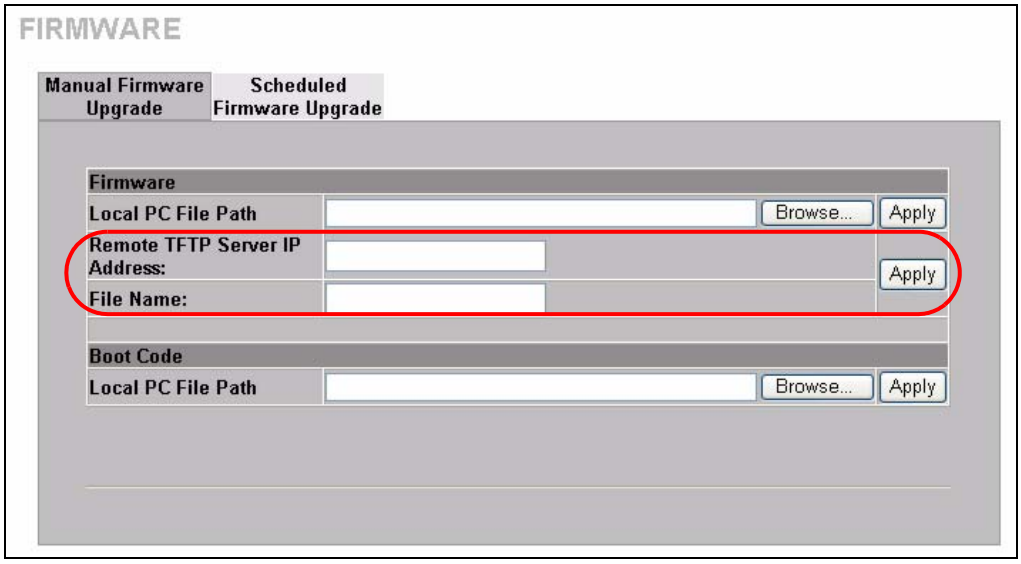
1 Download the latest firmware from www.zyxel.com and store it in a TFTP server. Unzip the file if it is zipped.

2 Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the documentation that comes with your TFTP server program for instructions.

3 Access the web configurator. Refer to the section on accessing the web configurator for instructions.

4 Click **SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 114 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: via TFTP Server



5 Specify the IP address of the TFTP server in the **Remote TFTP Server IP Address** field.

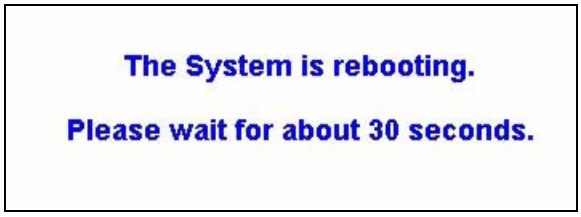
6 Specify the name of the firmware file in the **File Name** field.

7 Click **Apply** to start the file transfer process.

8 When the file transfer is completed successfully, a restart message displays and the N4100 automatically restarts.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

Figure 115 System Restart



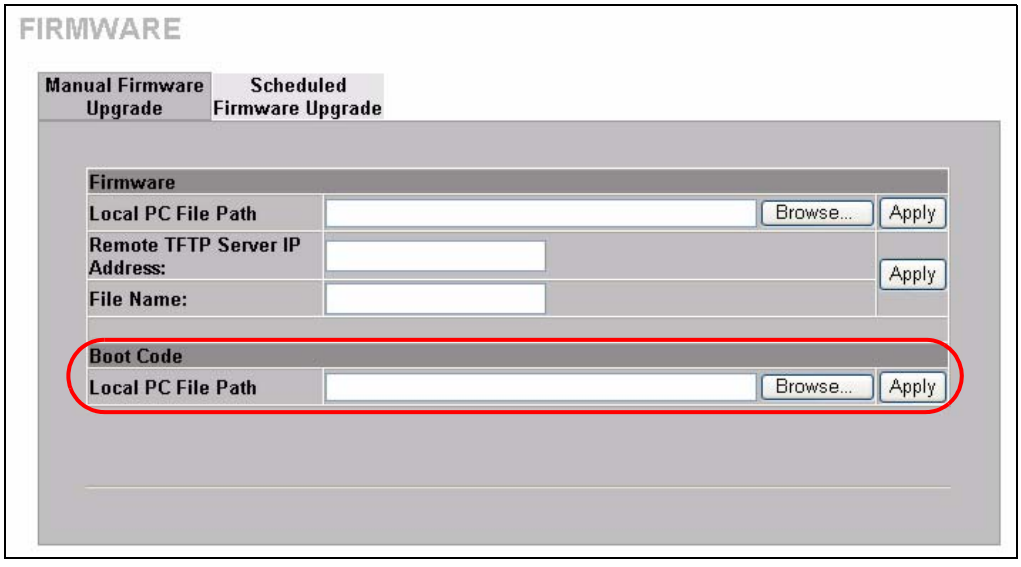
9 After the N4100 finishes restarting, access the web configurator again. Check the firmware version number in the **System Quick View** screen.

29.3.3 Manual Boot Code Upgrade Using the Web Configurator

Follow the steps below to upload the boot code using the web configurator.

1 Click **SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade** to display the screen as shown.

Figure 116 SYSTEM TOOLS > FIRMWARE > Manual Firmware Upgrade: Boot Code Upgrade Using the Web Configurator

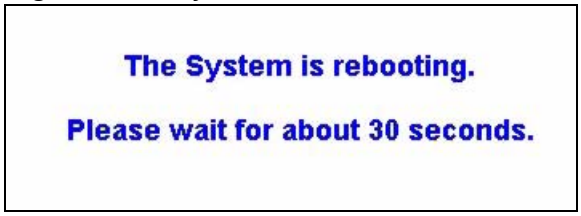


2 Specify the name of the boot code file in the **Local PC File Path** field or click **Browse** to locate the file and click **Apply** to start the file transfer process. The boot code must be a binary file and should have a .rom extension.

3 When the file transfer is completed successfully, a restart message displays and the N4100 automatically restarts.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

Figure 117 System Restart



4 After the N4100 finishes restarting, access the web configurator again. Check the Boot ROM version number in the **System Quick View** screen.

Note: When the N4100 restarts, all connections terminate. Subscribers need to log in again.

29.3.4 Scheduled Firmware Upgrade

Click **SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade** to display the screen as shown.

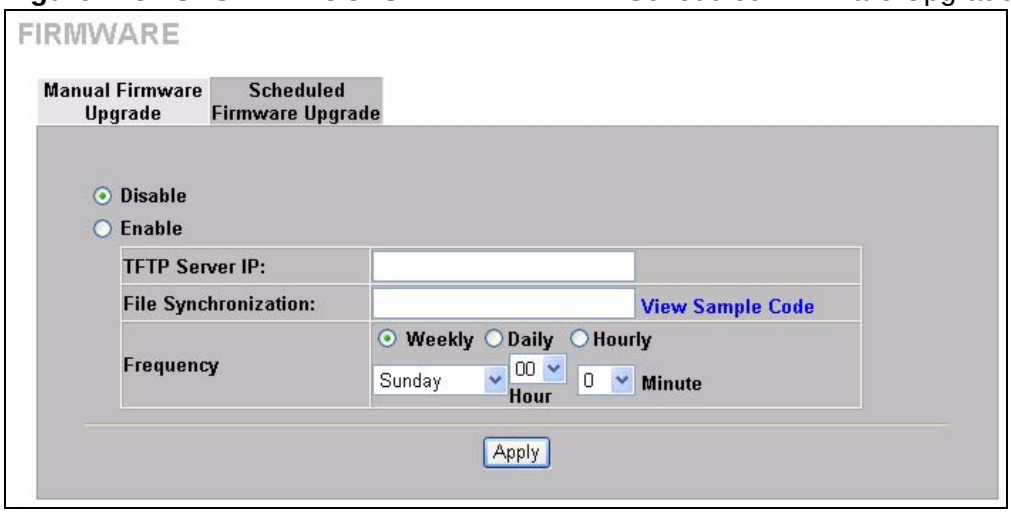
Configure the screen to automatically download the latest firmware from a TFTP server.

Note: Make sure that the TFTP server has the firmware and synchronization check file before you configure for scheduled firmware upgrades.

Make sure that you check new features or functionality enhancements in new firmware releases before you put the firmware on the TFTP server.

WARNING!
Do not interrupt the file upload process as this may PERMANENTLY damage the device.

Figure 118 SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade



Note: When the N4100 restarts, all connections terminate. Subscribers need to log in again.

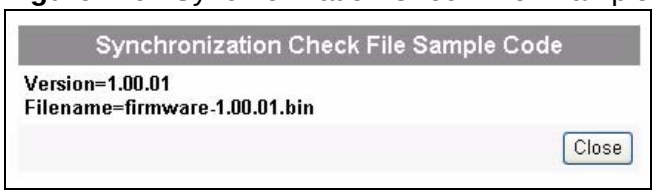
The following table describes the labels in this screen.

Table 62 SYSTEM TOOLS > FIRMWARE > Scheduled Firmware Upgrade

LABEL	DESCRIPTION
Disable Enable	Select **Disable** or **Enable** to turn the scheduled firmware upgrade function on or off (disabled by default).
TFTP Server IP	Type the IP address of the TFTP server from which the N4100 can download new firmware files.
File Synchronization	A synchronization check file is a .txt file containing the latest firmware filename and version number on the TFTP server. Enter the name of the check file.
View Sample File	Click **View Sample File** to see an example synchronization check file.
Frequency	Set how often (**Weekly**, **Daily** or **Hourly**) you want to have the N4100 check for new firmware and upgrade to new firmware if available (default **Weekly**). Then select the day (applies only when you select **Weekly**), the hour (applies when you select **Daily** or **Hourly**) and the minute that you want the N4100 to do the check and upload.
Apply	Click **Apply** to save your changes back to the N4100.

The following figure shows an example of a check file's content.

Figure 119 Synchronization Check File Example



30

System Account

30.1 Overview

There are four system accounts that you can use to log in to the N4100: administrator, account operator, supervisor and super subscriber.

The administrator account allows you full access to all system configurations. The default administrator user name is “admin” and the default password is “1234”.

The account operator account is used for proprietary subscriber account management only. No system configuration is allowed. This account is useful for front desk personnel (such as in a hotel) for setting up subscriber accounts without tampering with the system configuration. The account operator default user name and password are “account”.

With the supervisor account, you can only view the system status and change the supervisor account password. This account is useful for allowing a manager to view the device’s status and lists of accounts and logged in subscribers without changing the system configuration. The default supervisor account user name and password is “supervisor”.

Use the super subscriber account to test the Internet connection between the N4100 and the ISP. The N4100 does not impose time limitations or charges on this account. Thus, anyone who logs in with this account is able to gain Internet access for free. The default super subscriber user name and password are “super”.

Note: You can only log in using the super subscriber account in the subscriber login screen.

30.1.1 What You Can Do in this Chapter

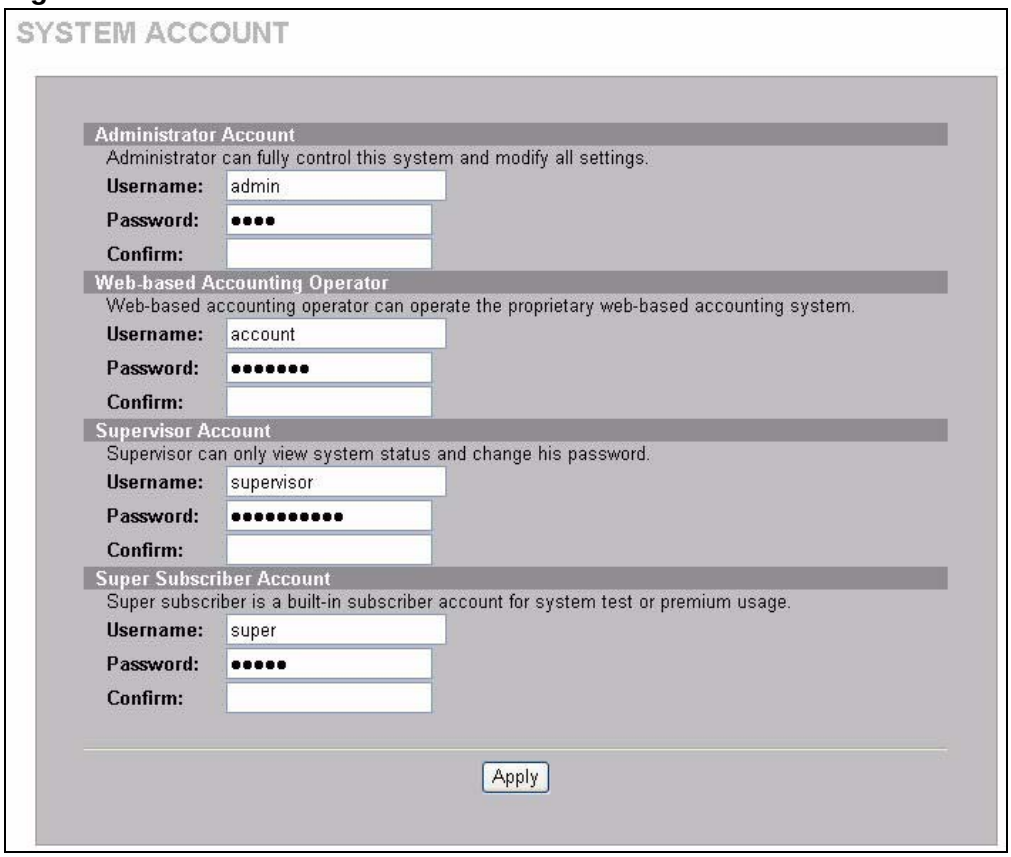
Use the **System Account** screen (Section 30.2 on page 240) to change system login account user names and passwords.

30.2 The System Account Screen

Note: It is recommended you change the account passwords.

Click **SYSTEM TOOLS > SYSTEM ACCOUNT** to open the screen shown next.

Figure 120 SYSTEM TOOLS > SYSTEM ACCOUNT



The following table describes the fields in this screen.

Table 63 SYSTEM TOOLS > SYSTEM ACCOUNT

LABEL	DESCRIPTION
Administrator Account	
Username	Enter the user name for the administrative account. The default is **admin**.
Password	Enter a new administrative account password.
Confirm	Enter the new administrator password again for confirmation.
Web-based Accounting Operator	
Username	Enter the user name for the account manager account. The default is **account**.
Password	Enter a new account manager password.

Table 63 SYSTEM TOOLS > SYSTEM ACCOUNT (continued)

LABEL	DESCRIPTION
Confirm	Enter the new account manager password again for confirmation.
Supervisor Account	
Username	Enter the user name for the supervisor account. The default is **supervisor**.
Password	Enter a new supervisor password.
Confirm	Enter the new supervisor password again for confirmation.
Super Subscriber Account	You can only log in using the super subscriber account in the subscriber login screen.
Username	Enter the user name for the super subscriber account. The default is **super**.
Password	Enter a new super subscriber account password.
Confirm	Enter the new super subscriber account password again for confirmation.
Apply	Click **Apply** to save your changes back to the N4100.

31

SSL Certificate

31.1 Overview

SSL (Secure Socket Layer) security is a standard Internet protocol for secure communications that uses a combination of certificate-based authentication and public-key encryption. SSL protects data transfer between the web configurator on the N4100 and the web browser on a connected computer.

With SSL security activated, data (such as user name and password) transferred between the N4100 and the computer is protected when you access the N4100 using a web browser that supports SSL.

See Section 3.8 on page 52 for how to setup and enable Secure Socket Layer (SSL) security on the N4100.

31.1.1 What You Can Do in this Chapter

Use the **SSL Certificate** screen (Section 31.2 on page 243) to download a CA registered certificate from a computer connected to the N4100.

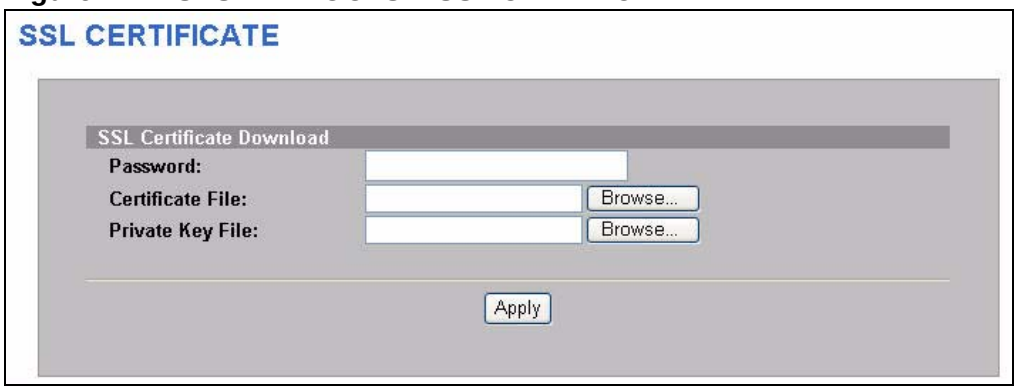
31.2 The SSL Certificate Screen

You can register for a certificate from a CA (Certificate Authority). A CA issues digital certificates and guarantees the identity of the certificate owner.

Note: You must save the certificate and private key files from the CA on a computer that is connected to the N4100.

Click **SYSTEM TOOLS > SSL CERTIFICATE** to open the screen shown next.

Figure 121 SYSTEM TOOLS > SSL CERTIFICATE



The following table describes the fields in this screen.

Table 64 SYSTEM TOOLS > SSL CERTIFICATE

LABEL	DESCRIPTION
Password	Enter the private key password from the CA. Make sure you enter it exactly as the CA provides.
Certificate File	Specify the name and/or location of the file containing the certificate. Or click **Browse** to locate the file.
Private Key File	Specify the name and/or location of the file containing the private key, Or click **Browse** to locate the file.
Apply	Click **Apply** to transfer the certificate and private key files from the computer to the N4100.

Note: See Chapter 4 on page 63 for how to set the N4100 to use the certificate that you download.

32

Ping Command

32.1 Overview

This chapter shows how to use the ping function to check the N4100's network connection.

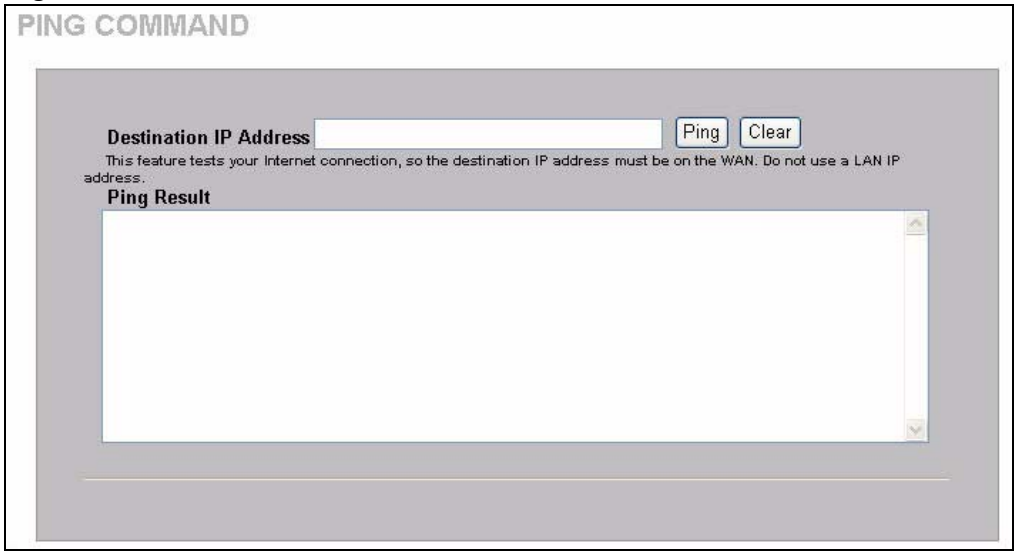
32.1.1 What You Can Do in this Chapter

Use the **Ping Command** screen (Section 32.2 on page 245) to test the Internet connection.

32.2 The Ping Command Screen

Click **SYSTEM TOOLS > PING COMMAND** to open the screen shown next.

Figure 122 SYSTEM TOOLS > PING COMMAND



The following table describes the fields in this screen.

Table 65 SYSTEM TOOLS > PING COMMAND

LABEL	DESCRIPTION
Destination IP Address	Type the IP address of a device on the WAN that you want to ping in order to test the Internet connection. This feature tests your Internet connection, so the destination IP address must be on the WAN. Do not use a LAN IP address.
Ping	Click this button to have the device ping the IP address.
Clear	Click this button to clear the ping results in the multi-line text box.
Ping Result	This multi-line text box displays the results of the ping.

33

Restart

33.1 Overview

This chapter covers how to use the **Restart** screen.

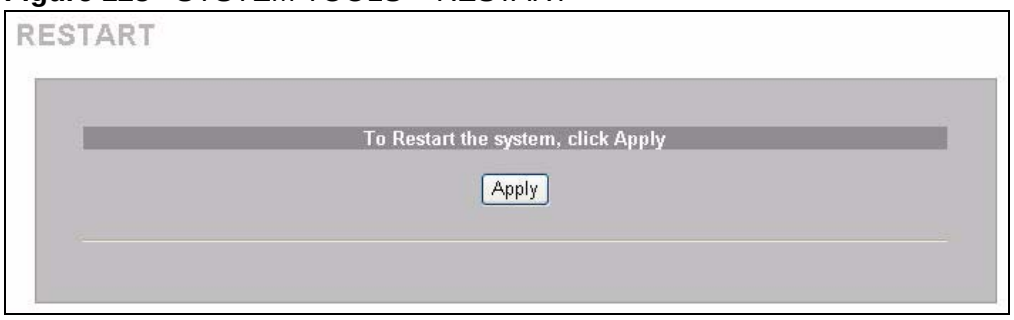
33.1.1 What You Can Do in this Chapter

Use the **Restart** screen (Section 33.2 on page 247) to reboot the N4100.

33.2 The Restart Screen

Click **SYSTEM TOOLS > RESTART** to open the screen shown next. Click **Apply** to have the N4100 reboot. This does not affect the N4100's configuration.

Figure 123 SYSTEM TOOLS > RESTART



34

Troubleshooting

34.1 Overview

This chapter offers some suggestions to solve problems you might encounter. The potential problems are divided into the following categories.

- Power, Hardware Connections, and LEDs
- N4100 Access and Login
- Internet Access
- Wireless LAN Troubleshooting

34.2 Power, Hardware Connections, and LEDs

The N4100 does not turn on. None of the LEDs turn on.

1. Make sure the N4100 is turned on.
2. Make sure you are using the power adaptor or cord included with the N4100.
3. Make sure the power adaptor or cord is connected to the N4100 and plugged in to an appropriate power source. Make sure the power source is turned on.
4. Turn the N4100 off and on.
5. If the problem continues, contact the vendor.

One of the LEDs does not behave as expected.

1. Make sure you understand the normal behavior of the LED. See Section 1.6 on page 25.
2. Check the hardware connections. See the Quick Start Guide.
3. Inspect your cables for damage. Contact the vendor to replace any damaged cables.
4. Turn the N4100 off and on.
5. If the problem continues, contact the vendor.

34.3 N4100 Access and Login

I forgot the IP address for the N4100.

1. The default IP address is 192.168.1.1.
2. If you changed the IP address and have forgotten it, you might get the IP address of the N4100 by looking up the IP address of the default gateway for your computer. To do this in most Windows computers, click **Start > Run**, enter **cmd**, and then enter **ipconfig**. The IP address of the **Default Gateway** might be the IP address of the N4100 (it depends on the network), so enter this IP address in your Internet browser.
3. If this does not work, you have to reset the device to its factory defaults. See Section 1.5 on page 24.

I cannot see or access the **Login** screen in the web configurator.

1. Make sure you are using the correct IP address.
   - The default IP address is 192.168.1.1.
   - If you changed the IP address, use the new IP address.

- If you changed the IP address and have forgotten it, see the troubleshooting suggestions for I forgot the IP address for the N4100.

2 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide.

3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled. See Appendix B on page 291.

4 Reset the device to its factory defaults, and try to access the N4100 with the default IP address. See Section 1.5 on page 24.

5 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

I can see the **Login** screen, but I cannot log in to the N4100.

1 Make sure you have entered the user name and password correctly. The default administrator user name is **admin**. These fields are case-sensitive, so make sure [Caps Lock] is not on.

2 You cannot log in to the web configurator while someone is using Telnet to access the N4100. Log out of the N4100 in the other session, or ask the person who is logged in to log out.

3 Turn the N4100 off and on.

4 If this does not work, you have to reset the device to its factory defaults. See Section 34.2 on page 249.

34.4 Internet Access

I cannot access the Internet.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 25.

2 Make sure you entered your ISP account information correctly in the WAN screen. These fields are case-sensitive, so make sure [Caps Lock] is not on.

3 Disconnect all the cables from your device, and follow the directions in the Quick Start Guide again.

4 If the problem continues, contact your ISP.

I cannot access the Internet anymore. I had access to the Internet (with the N4100), but my Internet connection is not available anymore.

1 Check the hardware connections, and make sure the LEDs are behaving as expected. See the Quick Start Guide and Section 1.6 on page 25.

2 Turn the N4100 off and on.

3 If the problem continues, contact your ISP.

The Internet connection is slow or intermittent.

1 There might be a lot of traffic on the network. Look at the LEDs, and check Section 1.6 on page 25. If the N4100 is sending or receiving a lot of information, try closing some programs that use the Internet, especially peer-to-peer applications.

2 If you are accessing the Internet wirelessly, check the signal strength. If the signal strength is low, try moving your computer closer to the N4100 if possible, and look around to see if there are any devices that might be interfering with the wireless network (for example, microwaves, other wireless networks, and so on).

3 Turn the N4100 off and on.

4 If the problem continues, contact the network administrator or vendor, or try one of the advanced suggestions.

34.5 Wireless LAN Troubleshooting

I cannot access the N4100 or ping any computer from the WLAN.

1 Make sure the wireless LAN is enabled on the N4100.

2 Make sure the wireless adapter on the wireless station is working properly.

3 Make sure the wireless adapter installed on your computer is IEEE 802.11 compatible and supports the same wireless standard as the N4100.

4 Make sure your computer (with a wireless adapter installed) is within the transmission range of the N4100.

5 Check that both the N4100 and your wireless station are using the same wireless and wireless security settings.

6 Check if MAC Filter is configured to deny wireless access to certain MAC addresses to the N4100. See Chapter 8 on page 69 in the User's Guide for more information.

35

Product Specifications

The following tables summarize the N4100's hardware and firmware features.

Firmware Specifications

Table 66 Firmware Specifications

IP Plug and Play (iPnP technology)	Zero Configuration IP Plug and Play Internet Access
Networking Functions	NAT Various WAN connections (Static IP/DHCP Client/PPPoE/PPTP) DHCP Server HTTP Proxy Server NTP (Network Time Protocol) support
User Authentication and Accounting	Supports up to 100 concurrent users Web-based Authentication Idle-timeout Control
Security and Firewall	Layer 2 Isolation SSL Login Page and Administration VPN (IPSec/PPTP/L2TP) Pass through Custom SSL Certificate Administration Access Control

Table 66 Firmware Specifications

Management	Web-based management tool TFTP/HTTP firmware upgrade Scheduled firmware upgrade Backup/Restore Configuration file SNMP MIBII supported LAN devices Management LAN devices Status Monitor Session List Syslog Default printer (SP300E) support
Marketing Cooperation	Pass through IP/MAC/URL Custom Login Page Login Page Redirect Advertisement URL link Walled garden Portal page redirection

Hardware Specifications

Table 67 Hardware Specifications

Network Specification	IEE802.3 10BaseT Ethernet IEE802.3u 100BaseTX Fast Ethernet IEE802.11b/g/n Wireless LAN ANSI/IEEE 802.3 NWay auto-negotiation
Compatibility	Can communicate with Wi-Fi certificated wireless adapters
Connectors	4 LAN Ports and One WAN Port 10/100BaseTX with auto MDI/MDI-X
Wireless Operation Range	Open Space: 100~300m Indoors: 35~100m
Wireless Data Rate	Up to 300 Mbps for IEEE 802.11n with auto fallback to IEEE 802.11g or IEEE 802.11b
Encryption	WEP 64/128, WPA, WPA2

Table 67 Hardware Specifications

External Antenna	Three 2dBi (Max) Dual detachable diversity antennas with reverse SMA connectors
Power Requirement	External Power Adapter Input: 100-240 VAC, 50/60 Hz, 0.5 A Output: 12 VDC, 1.5A
Dimensions	Size: 212.5 (L) x 138.5(W) x 52.0(H) mm Net Weight: 508g
Environment Conditions	Operating Temperature:0 to 50°C Storage Temperature: -20 to 60°C Humidity: Max. 95% non-condensing
Mounting	Desktop Wall mounted
LED Indicators	One **PWR** LED One **SYS** LED One **WLAN** Link/Activity LED One **WAN** Link/Activity LED Four **LAN** Link/Activity LEDs

Certifications

Table 68 Certifications

Certifications	FCC part 15 Class B CE / R&TTE C-Tick IC RSS-210

The following list, which is not exhaustive, illustrates the standards supported in the N4100.

Table 69 Standards Supported

STANDARD	DESCRIPTION
RFC 1058	RIP-1 (Routing Information Protocol)
RFC 1112	IGMP v1
RFC 1305	Network Time Protocol (NTP version 3)

Table 69 Standards Supported (continued)

STANDARD	DESCRIPTION
RFC 1631	IP Network Address Translator (NAT)
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1723	RIP-2 (Routing Information Protocol)
RFC 2236	Internet Group Management Protocol, Version 2.
RFC 2516	A Method for Transmitting PPP Over Ethernet (PPPoE)
RFC 2766	Network Address Translation - Protocol
IEEE 802.1D	Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges
IEEE 802.1x	Port Based Network Access Control.
Microsoft PPTP	MS PPTP (Microsoft's implementation of Point to Point Tunneling Protocol)

RJ-45 Ethernet Ports

The following table describes the types of network cable used for the different connection speeds.

Note: Make sure the Ethernet cable length between connections does not exceed 100 meters (328 feet).

Table 70 Network Cable Types

SPEED	NETWORK CABLE TYPE
10 Base-TX	100Ω 2-pair UTP/STP Category 3, 4 or 5
100 Base-TX	100Ω 2-pair UTP/STP Category 5

WAN Port

The following figure and table describe the Ethernet cable pin assignments for the WAN port.

Figure 124 WAN Port Cable Pin Assignments

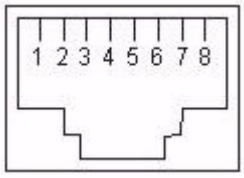


Table 71 WAN Port Cable Pin Assignments

PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
1	Output Transmit Data +	TD+
2	Output Transmit Data -	TD-
3	Input Transmit Data +	RD+
4	Unused	N/U
5	Unused	N/U
6	Input Transmit Data -	RD-
7	Unused	N/U
8	Unused	N/U

Make sure that the Ethernet cable connection between the N4100 and the switch or router conforms to the following pin assignments.

Table 72 WAN Port Cable Pin Assignments

ETHERNET DEVICE (SWITCH/HUB/ROUTER ETC.)		N4100	
1	RD+	1	TD+
2	RD-	2	TD-
3	TD+	3	RD+
6	TD-	6	RD-

LAN Ports

The following figure and table describe the Ethernet cable pin assignments for the LAN port.

Figure 125 LAN Port Cable Pin Assignments

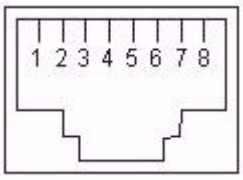


Table 73 LAN Port Cable Pin Assignments

PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
1	Input Transmit Data +	RD+
2	Input Transmit Data -	RD-

Table 73 LAN Port Cable Pin Assignments

PIN NO	RJ-45 SIGNAL ASSIGNMENT	DESIGNATION
3	Output Transmit Data +	TD+
4	Unused	N/U
5	Unused	N/U
6	Output Transmit Data -	TD-
7	Unused	N/U
8	Unused	N/U

Make sure that the Ethernet cable connection between the ZyAIR and a computer or switch uplink port conforms to the following pin assignments.

Table 74 LAN Port Cable Pin Assignments

ETHERNET DEVICE (COMPUTER/ UPLINK PORT)		N4100	
1	TD+	1	RD+
2	TD-	2	RD-
3	RD+	3	TD+
6	RD-	6	TD-

CONSOLE Port

The N4100 does not currently use this port.

Antenna Connector Type

The N4100 is equipped with reverse polarity SMA jacks.

Antenna Specifications

2.4 GHz wireless antennas with reverse polarity SMA plugs are included.

A

Setting Up Your Computer's IP Address

Note: Your specific N4100 may not support all of the operating systems described in this appendix. See the product specifications for more information about which operating systems are supported.

This appendix shows you how to configure the IP settings on your computer in order for it to be able to communicate with the other devices on your network. Windows Vista/XP/2000, Mac OS 9/OS X, and all versions of UNIX/LINUX include the software components you need to use TCP/IP on your computer.

If you manually assign IP information instead of using a dynamic IP, make sure that your network's computers have IP addresses that place them in the same subnet.

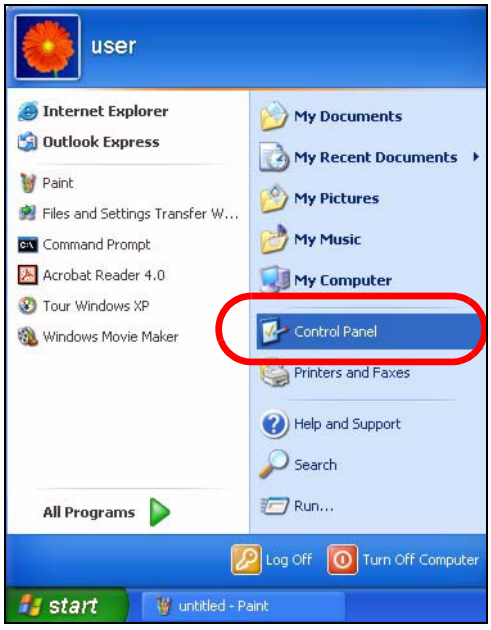
In this appendix, you can set up an IP address for:

Windows XP/NT/2000

The following example uses the default Windows XP display theme but can also apply to Windows 2000 and Windows NT.

1 Click **Start** > **Control Panel**.

Figure 126 Windows XP: Start Menu

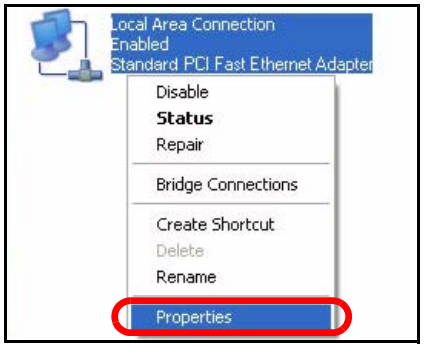


2 In the **Control Panel**, click the **Network Connections** icon.

Figure 127 Windows XP: Control Panel

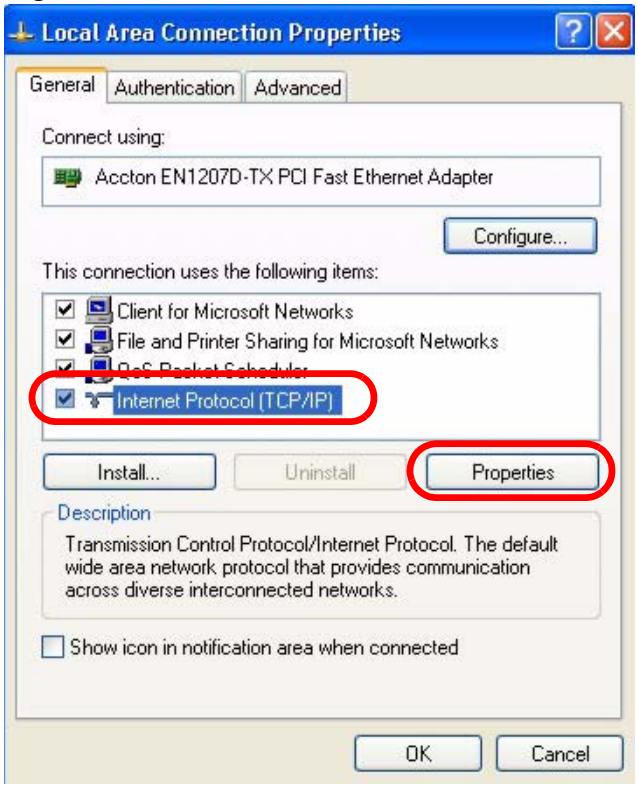
3 Right-click **Local Area Connection** and then select **Properties**.

Figure 128 Windows XP: Control Panel > Network Connections > Properties



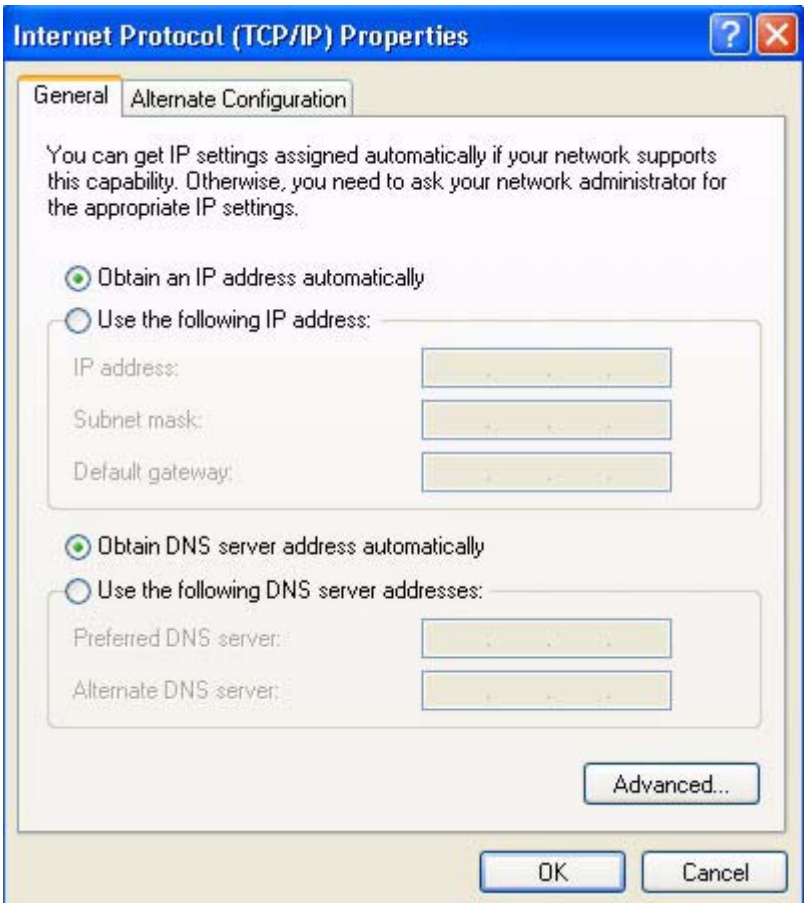
4 On the **General** tab, select **Internet Protocol (TCP/IP)** and then click **Properties**.

Figure 129 Windows XP: Local Area Connection Properties



5 The **Internet Protocol TCP/IP Properties** window opens.

Figure 130 Windows XP: Internet Protocol (TCP/IP) Properties



6 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.

7 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

8 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

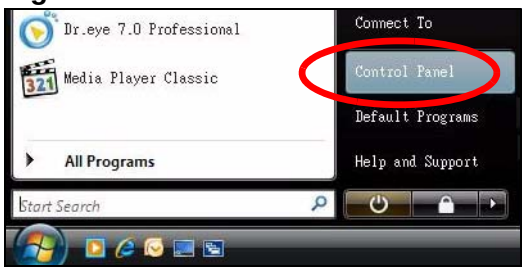
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows Vista

This section shows screens from Windows Vista Professional.

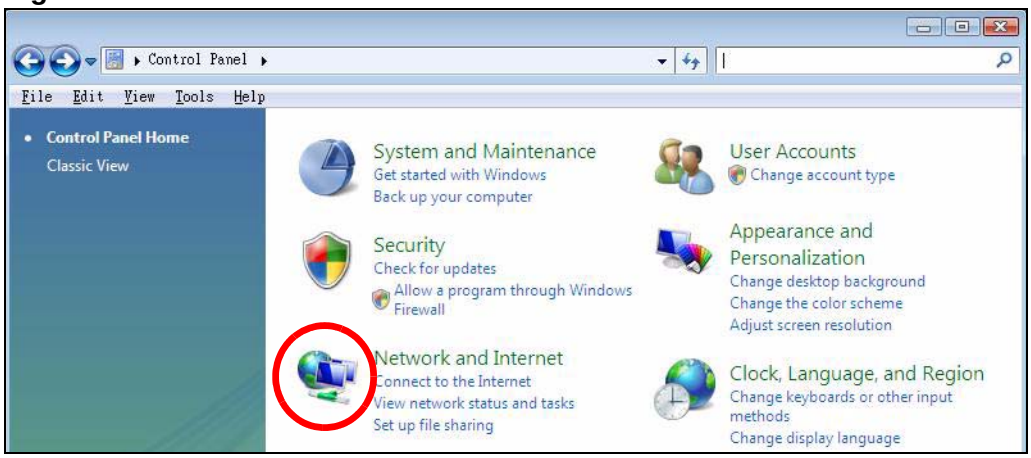
1 Click **Start** > **Control Panel**.

Figure 131 Windows Vista: Start Menu



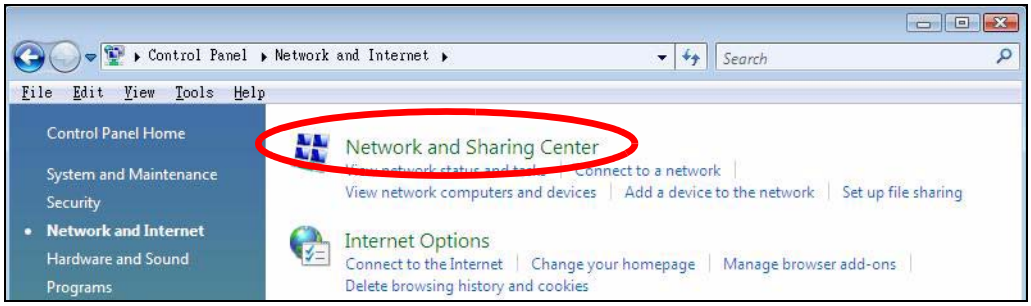
2 In the **Control Panel**, click the **Network and Internet** icon.

Figure 132 Windows Vista: Control Panel



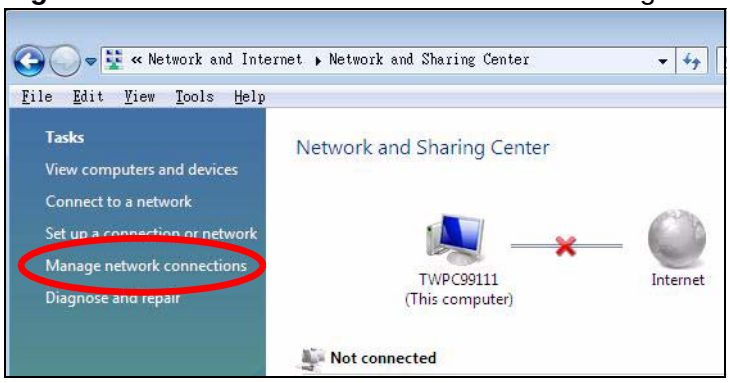
3 Click the **Network and Sharing Center** icon.

Figure 133 Windows Vista: Network And Internet



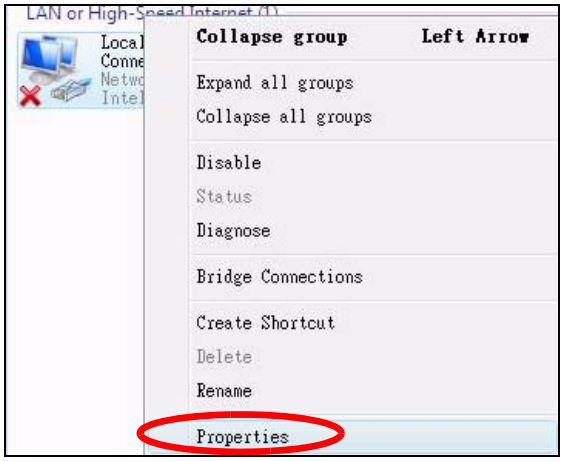
4 Click **Manage network connections**.

Figure 134 Windows Vista: Network and Sharing Center



5 Right-click **Local Area Connection** and then select **Properties**.

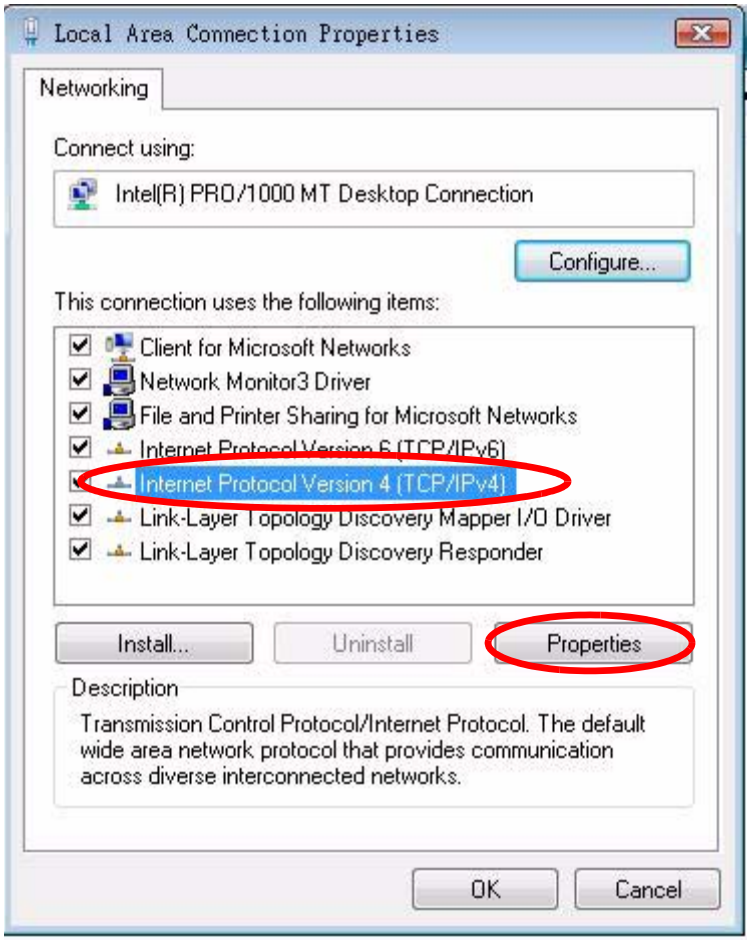
Figure 135 Windows Vista: Network and Sharing Center



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

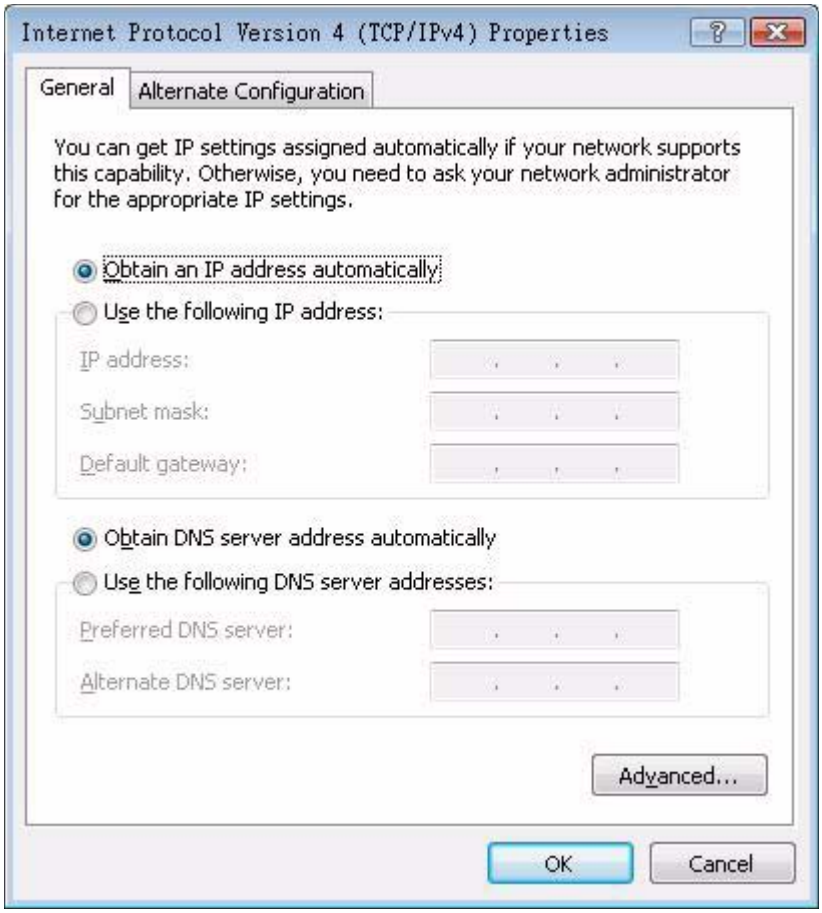
6 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 136 Windows Vista: Local Area Connection Properties



7 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 137 Windows Vista: Internet Protocol Version 4 (TCP/IPv4) Properties



8 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided.Click **Advanced**.

9 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

10 Click **OK** to close the **Local Area Connection Properties** window.

Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

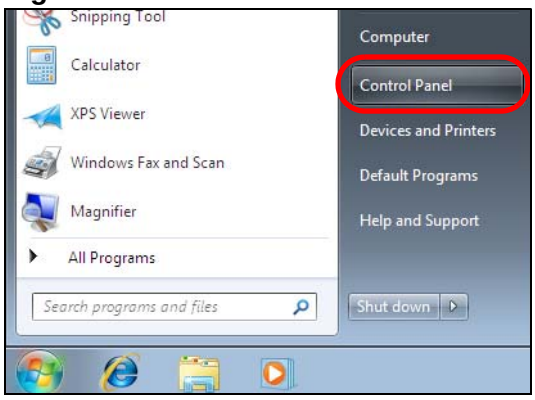
You can also go to **Start > Control Panel > Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab to view your IP address and connection information.

Windows 7

This section shows screens from Windows 7 Enterprise.

1 Click **Start** > **Control Panel**.

Figure 138 Windows 7: Start Menu

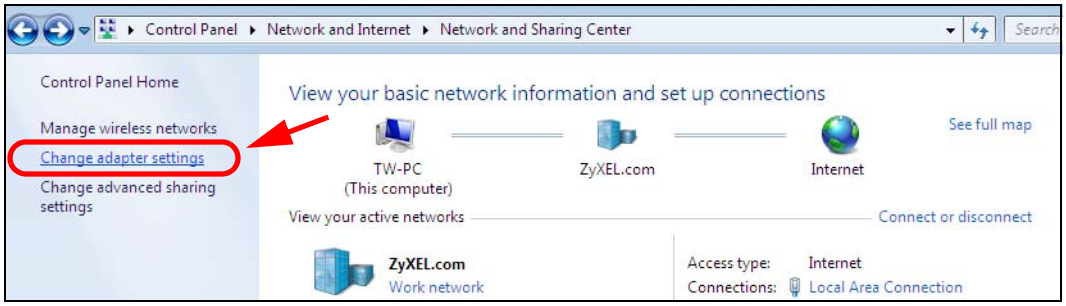


2 In the **Control Panel**, click **View network status and tasks** under the **Network and Internet** category.

Figure 139 Windows 7: Control Panel

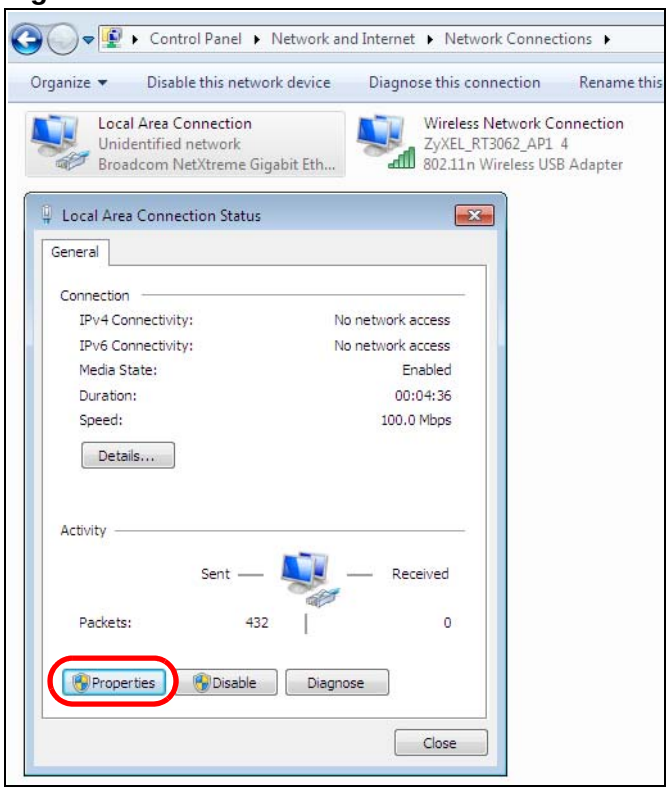
3 Click **Change adapter settings**.

Figure 140 Windows 7: Network And Sharing Center



4 Double click **Local Area Connection** and then select **Properties**.

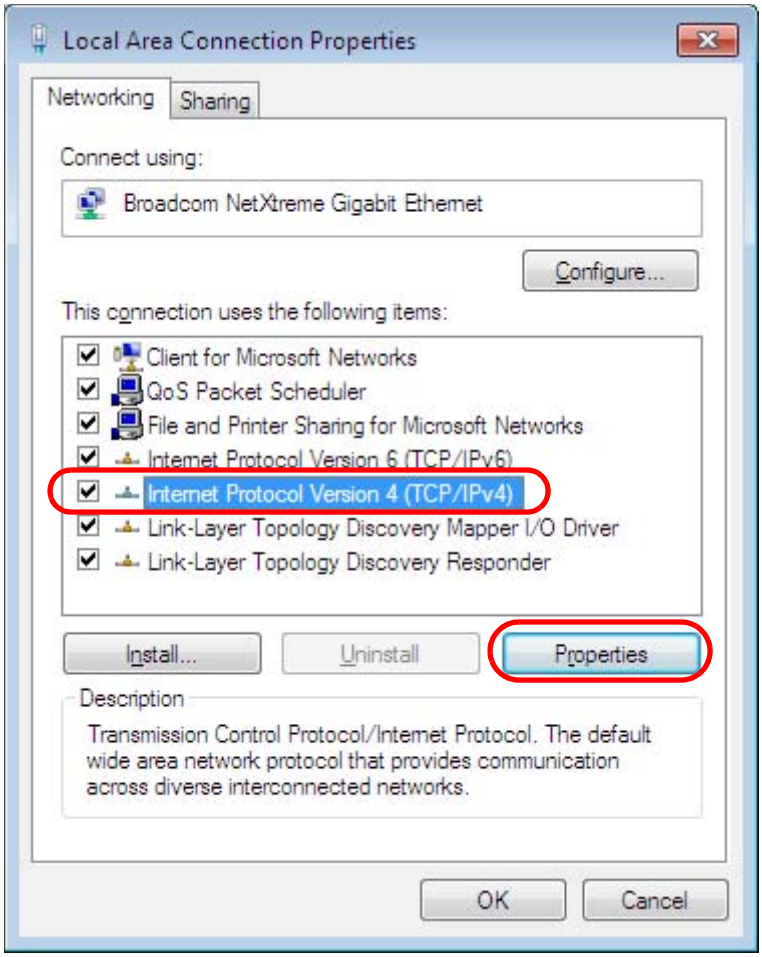
Figure 141 Windows 7: Local Area Connection Status



Note: During this procedure, click **Continue** whenever Windows displays a screen saying that it needs your permission to continue.

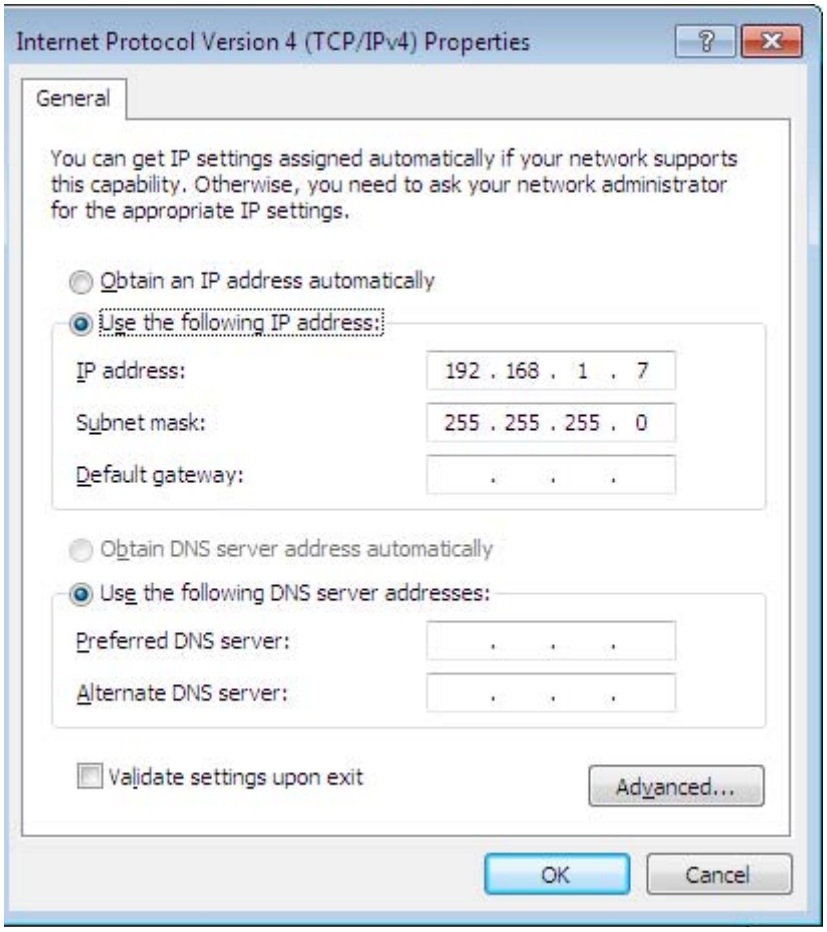
5 Select **Internet Protocol Version 4 (TCP/IPv4)** and then select **Properties**.

Figure 142 Windows 7: Local Area Connection Properties



6 The **Internet Protocol Version 4 (TCP/IPv4) Properties** window opens.

Figure 143 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties



7 Select **Obtain an IP address automatically** if your network administrator or ISP assigns your IP address dynamically.

Select **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields if you have a static IP address that was assigned to you by your network administrator or ISP. You may also have to enter a **Preferred DNS server** and an **Alternate DNS server,** if that information was provided. Click **Advanced** if you want to configure advanced settings for IP, DNS and WINS.

8 Click **OK** to close the **Internet Protocol (TCP/IP) Properties** window.

9 Click **OK** to close the **Local Area Connection Properties** window.

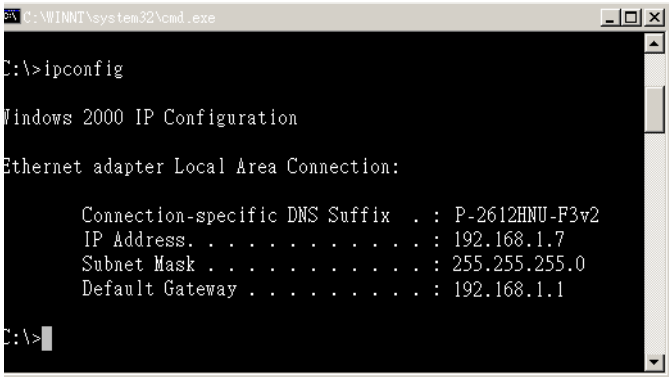
Verifying Settings

1 Click **Start** > **All Programs** > **Accessories** > **Command Prompt**.

2 In the **Command Prompt** window, type "ipconfig" and then press [ENTER].

3 The IP settings are displayed as follows.

Figure 144 Windows 7: Internet Protocol Version 4 (TCP/IPv4) Properties

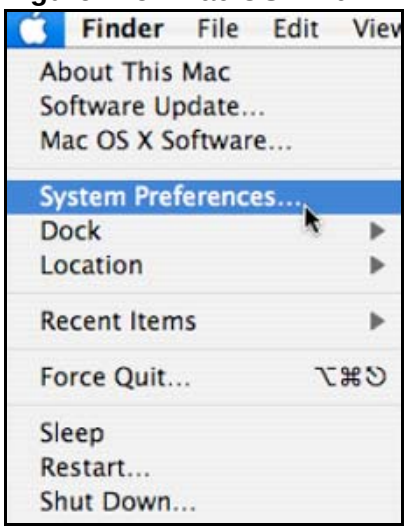


Mac OS X: 10.3 and 10.4

The screens in this section are from Mac OS X 10.4 but can also apply to 10.3.

1 Click **Apple** > **System Preferences**.

Figure 145 Mac OS X 10.4: Apple Menu

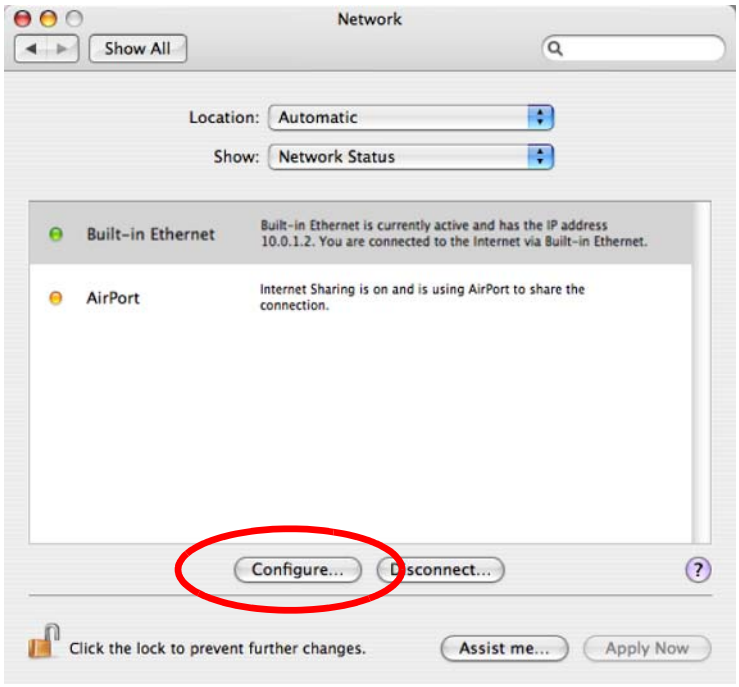


2 In the **System Preferences** window, click the **Network** icon.

Figure 146 Mac OS X 10.4: System Preferences

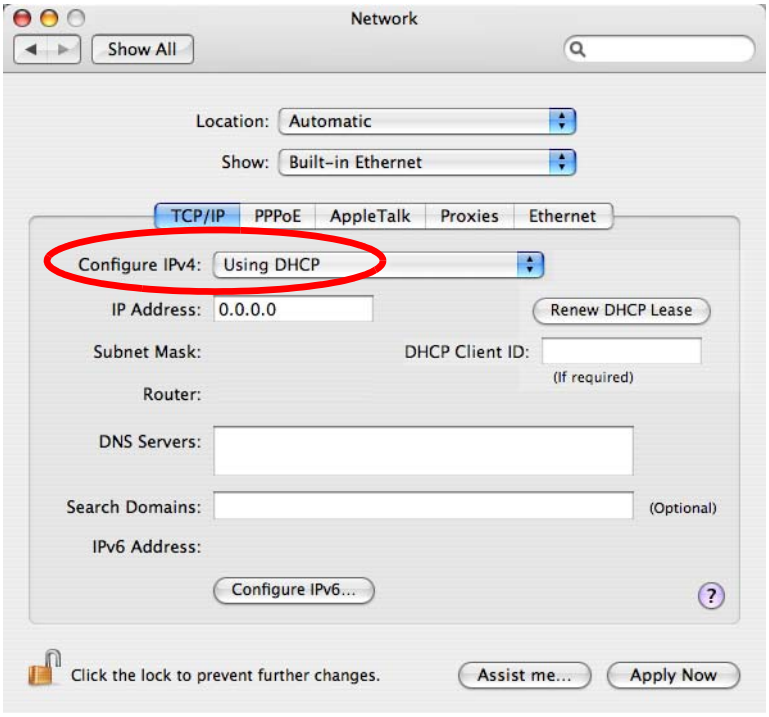
3 When the **Network** preferences pane opens, select **Built-in Ethernet** from the network connection type list, and then click **Configure.**

Figure 147 Mac OS X 10.4: Network Preferences



4 For dynamically assigned settings, select **Using DHCP** from the **Configure IPv4** list in the **TCP/IP** tab.

Figure 148 Mac OS X 10.4: Network Preferences > TCP/IP Tab.

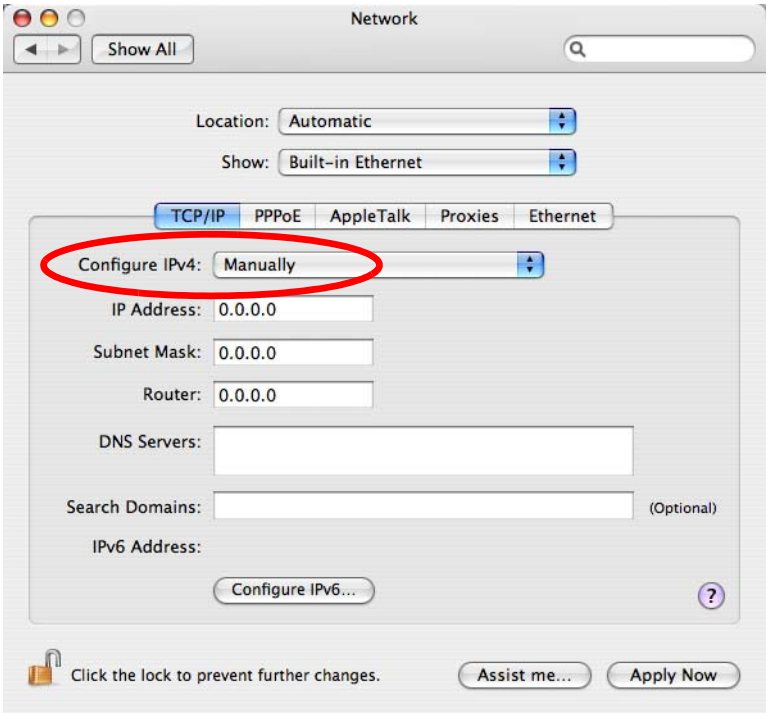


5 For statically assigned settings, do the following:

- From the **Configure IPv4** list, select **Manually**.
- In the **IP Address** field, type your IP address.
- In the **Subnet Mask** field, type your subnet mask.

- In the **Router** field, type the IP address of your device.

Figure 149 Mac OS X 10.4: Network Preferences > Ethernet

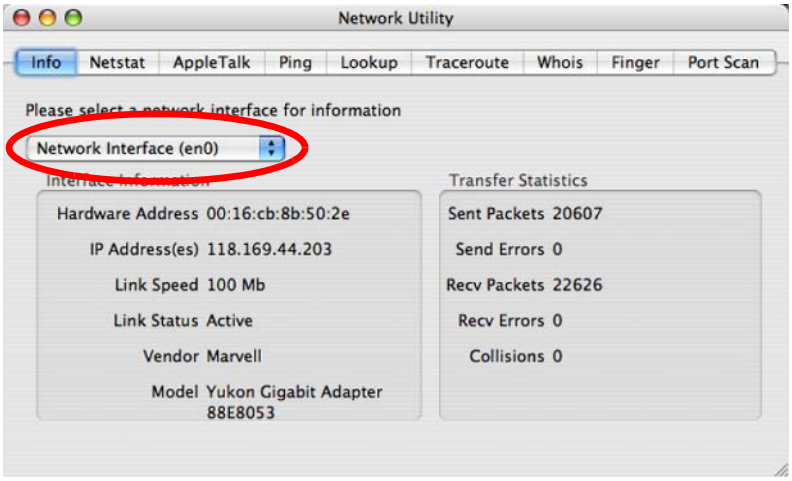


6 Click **Apply Now** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network Interface** from the **Info** tab.

Figure 150 Mac OS X 10.4: Network Utility

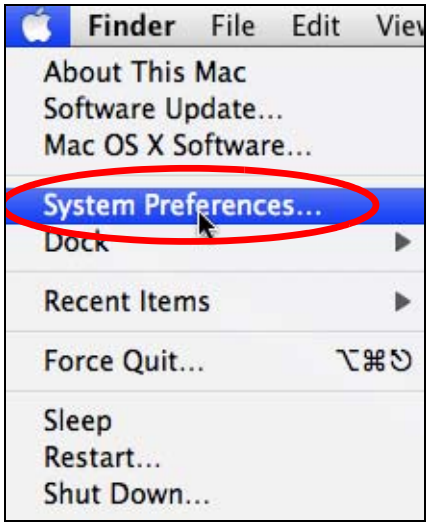


Mac OS X: 10.5 and 10.6

The screens in this section are from Mac OS X 10.5 but can also apply to 10.6.

1 Click **Apple** > **System Preferences**.

Figure 151 Mac OS X 10.5: Apple Menu

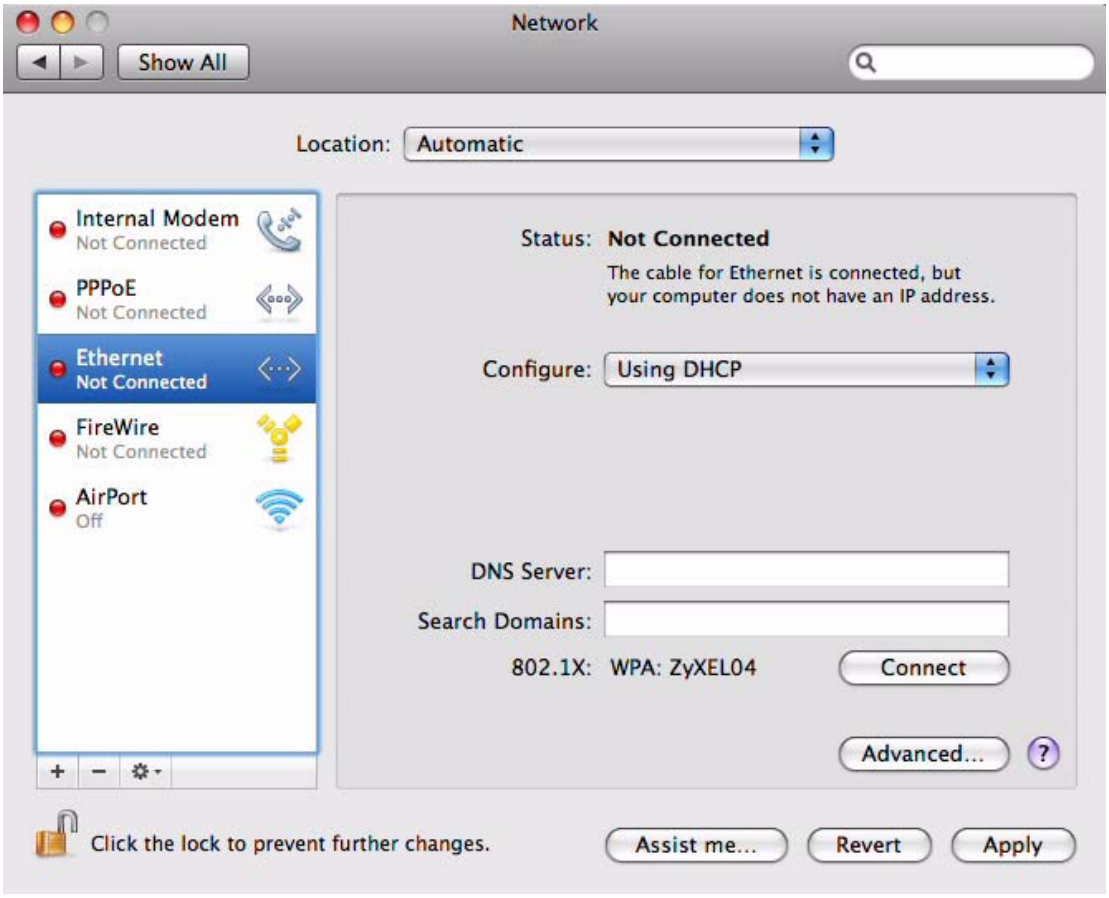


2 In **System Preferences**, click the **Network** icon.

Figure 152 Mac OS X 10.5: Systems Preferences

3 When the **Network** preferences pane opens, select **Ethernet** from the list of available connection types.

Figure 153 Mac OS X 10.5: Network Preferences > Ethernet



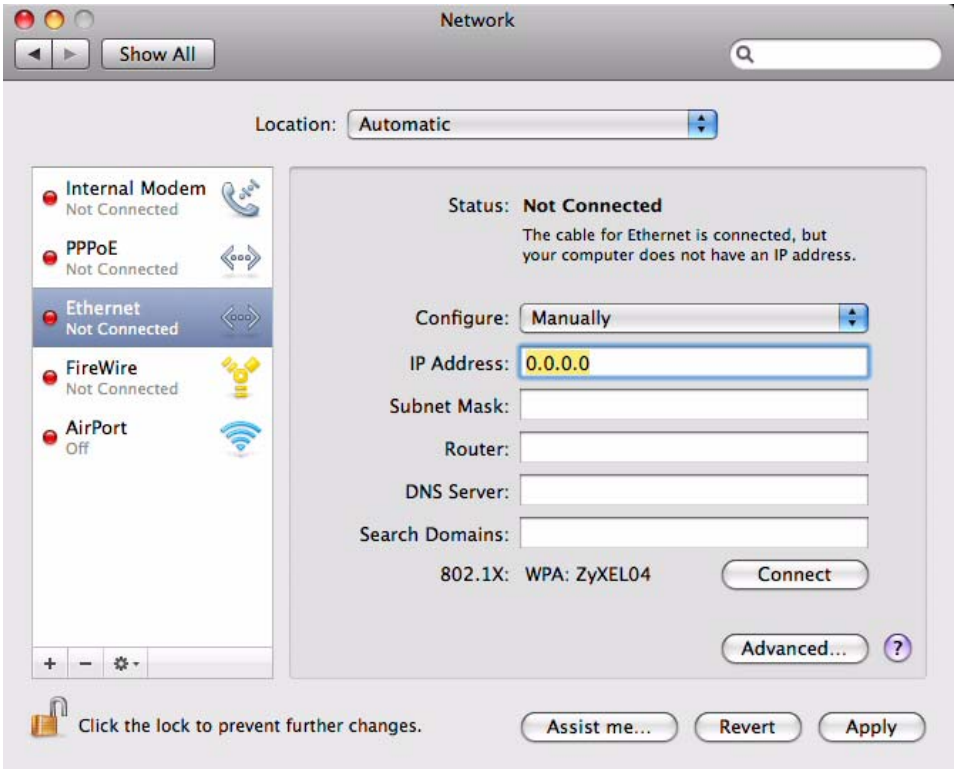
4 From the **Configure** list, select **Using DHCP** for dynamically assigned settings.

5 For statically assigned settings, do the following:

- From the **Configure** list, select **Manually**.
- In the **IP Address** field, enter your IP address.
- In the **Subnet Mask** field, enter your subnet mask.

- In the **Router** field, enter the IP address of your N4100.

Figure 154 Mac OS X 10.5: Network Preferences > Ethernet

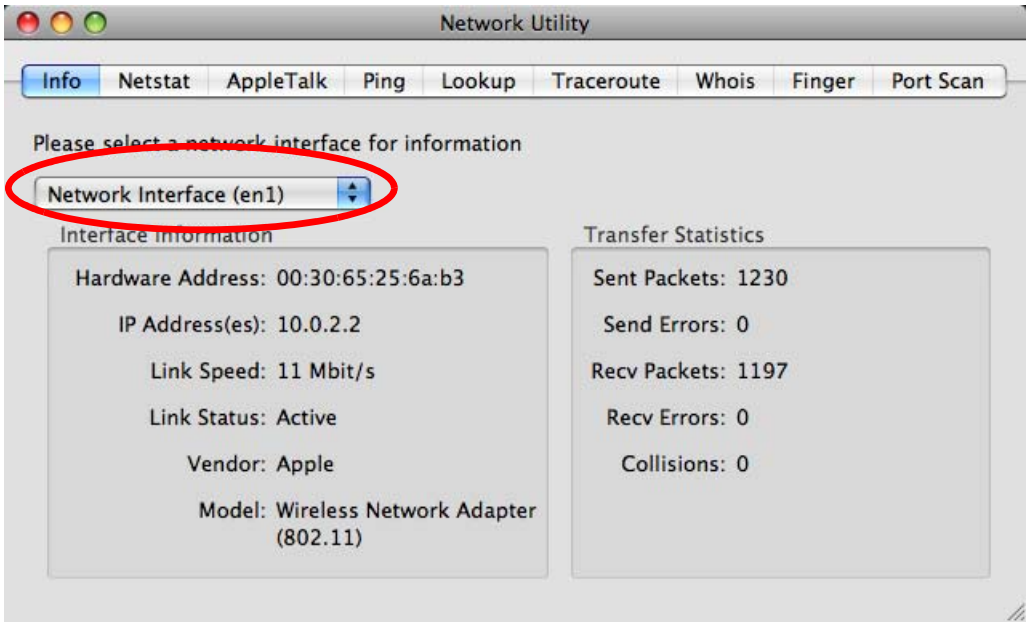


6 Click **Apply** and close the window.

Verifying Settings

Check your TCP/IP properties by clicking **Applications > Utilities > Network Utilities**, and then selecting the appropriate **Network interface** from the **Info** tab.

Figure 155 Mac OS X 10.5: Network Utility



Linux: Ubuntu 8 (GNOME)

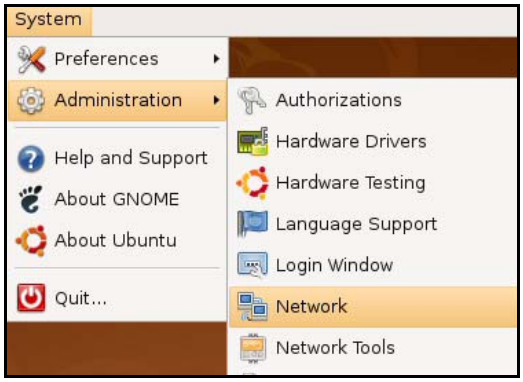
This section shows you how to configure your computer's TCP/IP settings in the GNU Object Model Environment (GNOME) using the Ubuntu 8 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default Ubuntu 8 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in GNOME:

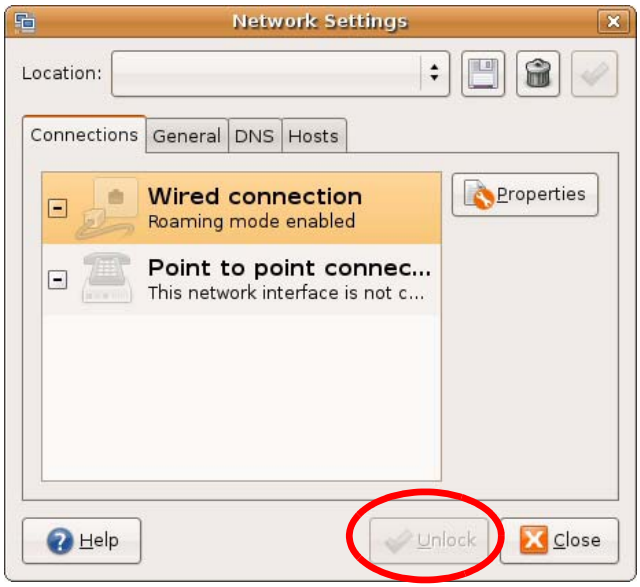
1 Click **System > Administration > Network**.

Figure 156 Ubuntu 8: System > Administration Menu



2 When the **Network Settings** window opens, click **Unlock** to open the **Authenticate** window. (By default, the **Unlock** button is greyed out until clicked.) You cannot make changes to your configuration unless you first enter your admin password.

Figure 157 Ubuntu 8: Network Settings > Connections



3 In the **Authenticate** window, enter your admin account name and password then click the **Authenticate** button.

Figure 158 Ubuntu 8: Administrator Account Authentication

4 In the **Network Settings** window, select the connection that you want to configure, then click **Properties**.

Figure 159 Ubuntu 8: Network Settings > Connections

5 The **Properties** dialog box opens.

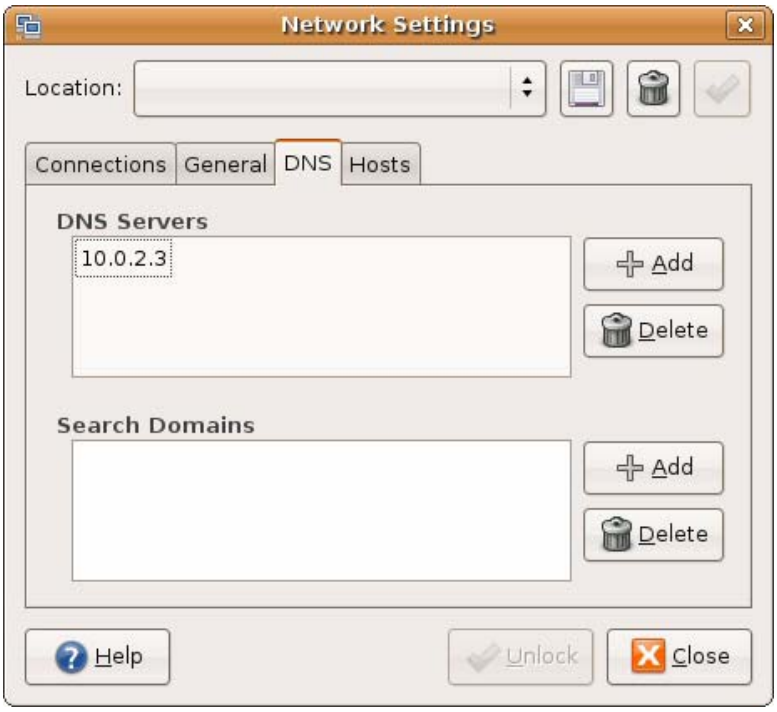
Figure 160 Ubuntu 8: Network Settings > Properties

- In the **Configuration** list, select **Automatic Configuration (DHCP)** if you have a dynamic IP address.
- In the **Configuration** list, select **Static IP address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Gateway address** fields.

6 Click **OK** to save the changes and close the **Properties** dialog box and return to the **Network Settings** screen.

7 If you know your DNS server IP address(es), click the **DNS** tab in the **Network Settings** window and then enter the DNS server information in the fields provided.

Figure 161 Ubuntu 8: Network Settings > DNS



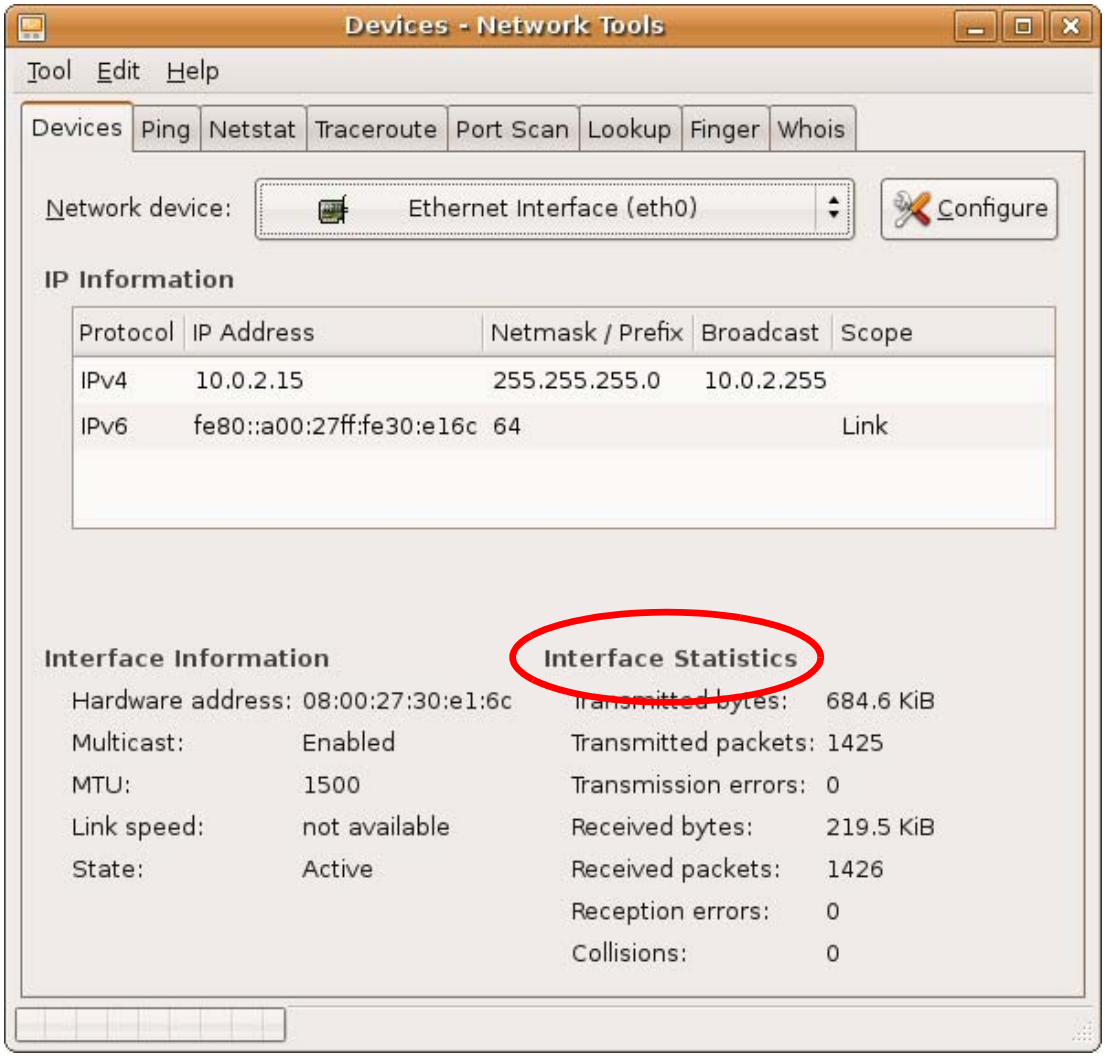
8 Click the **Close** button to apply the changes.

Verifying Settings

Check your TCP/IP properties by clicking **System > Administration > Network Tools**, and then selecting the appropriate **Network device** from the **Devices**

tab. The **Interface Statistics** column shows data if your connection is working properly.

Figure 162 Ubuntu 8: Network Tools



Linux: openSUSE 10.3 (KDE)

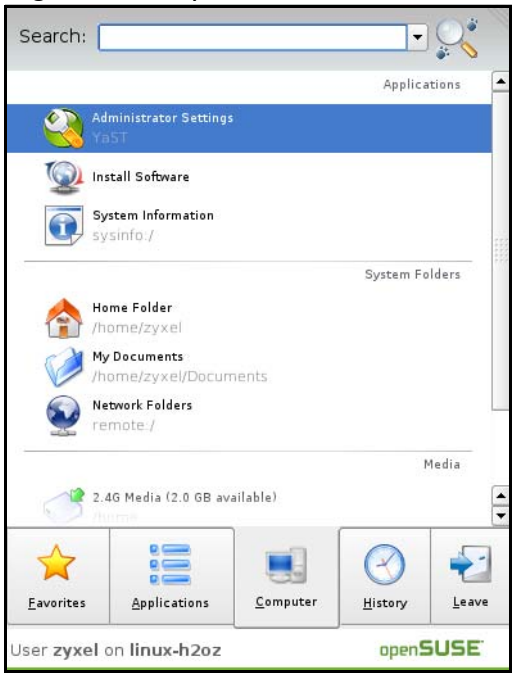
This section shows you how to configure your computer's TCP/IP settings in the K Desktop Environment (KDE) using the openSUSE 10.3 Linux distribution. The procedure, screens and file locations may vary depending on your specific distribution, release version, and individual configuration. The following screens use the default openSUSE 10.3 installation.

Note: Make sure you are logged in as the root administrator.

Follow the steps below to configure your computer IP address in the KDE:

1 Click **K Menu > Computer > Administrator Settings (YaST)**.

Figure 163 openSUSE 10.3: K Menu > Computer Menu

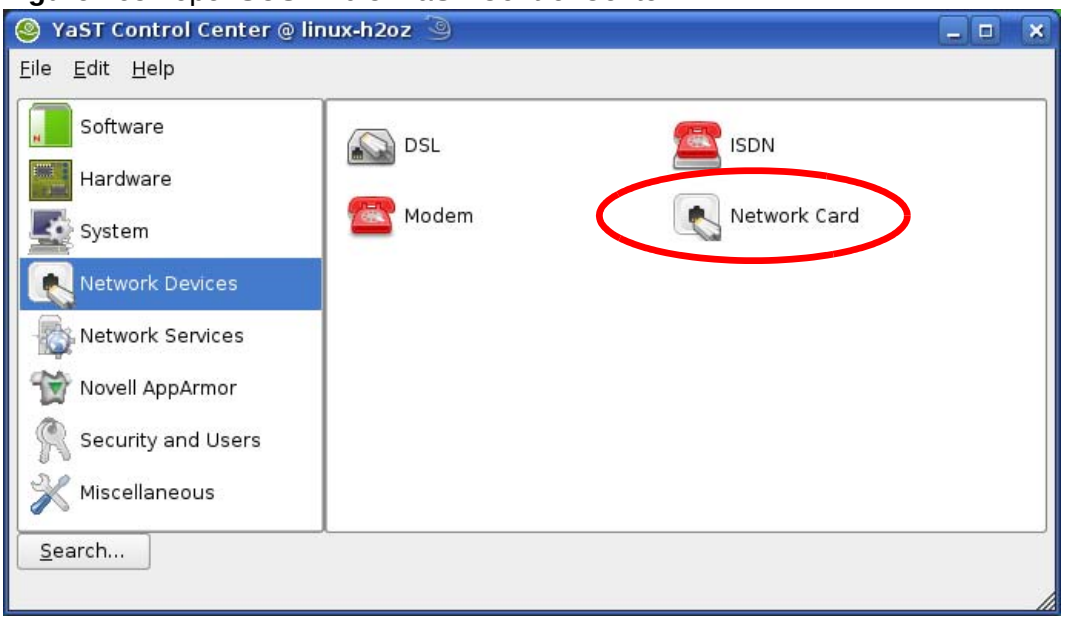


2 When the **Run as Root - KDE su** dialog opens, enter the admin password and click **OK**.

Figure 164 openSUSE 10.3: K Menu > Computer Menu

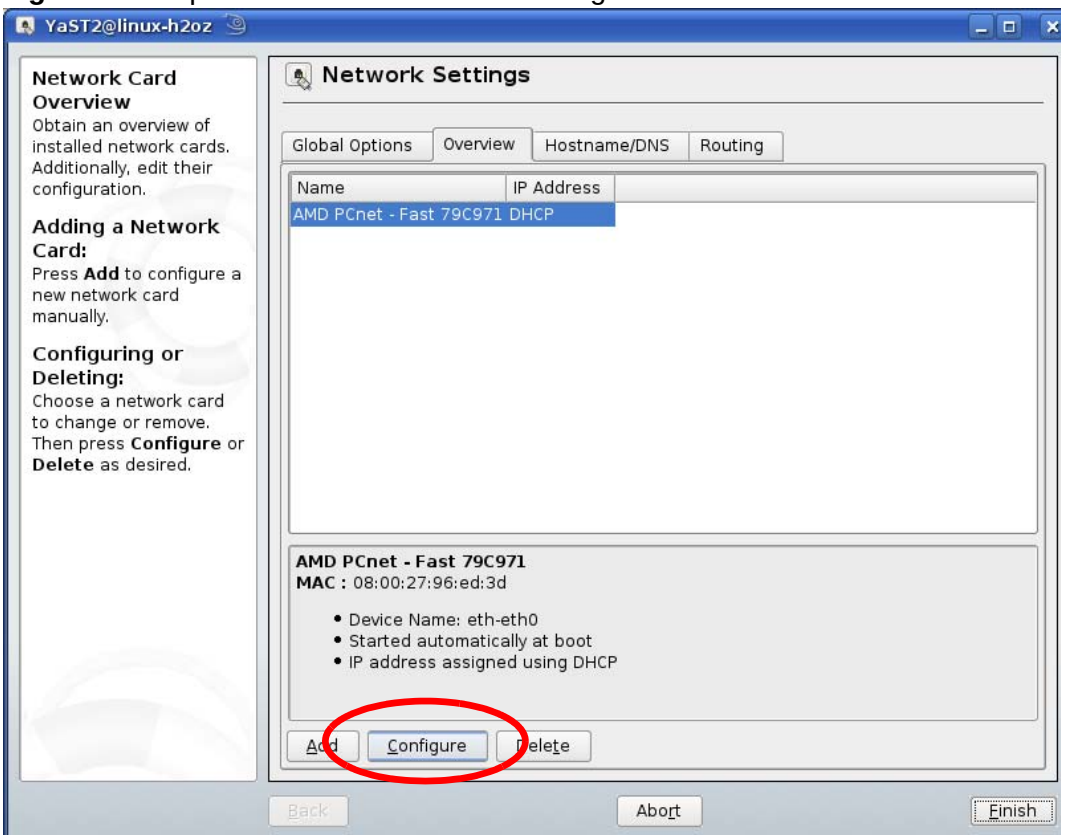
3 When the **YaST Control Center** window opens, select **Network Devices** and then click the **Network Card** icon.

Figure 165 openSUSE 10.3: YaST Control Center



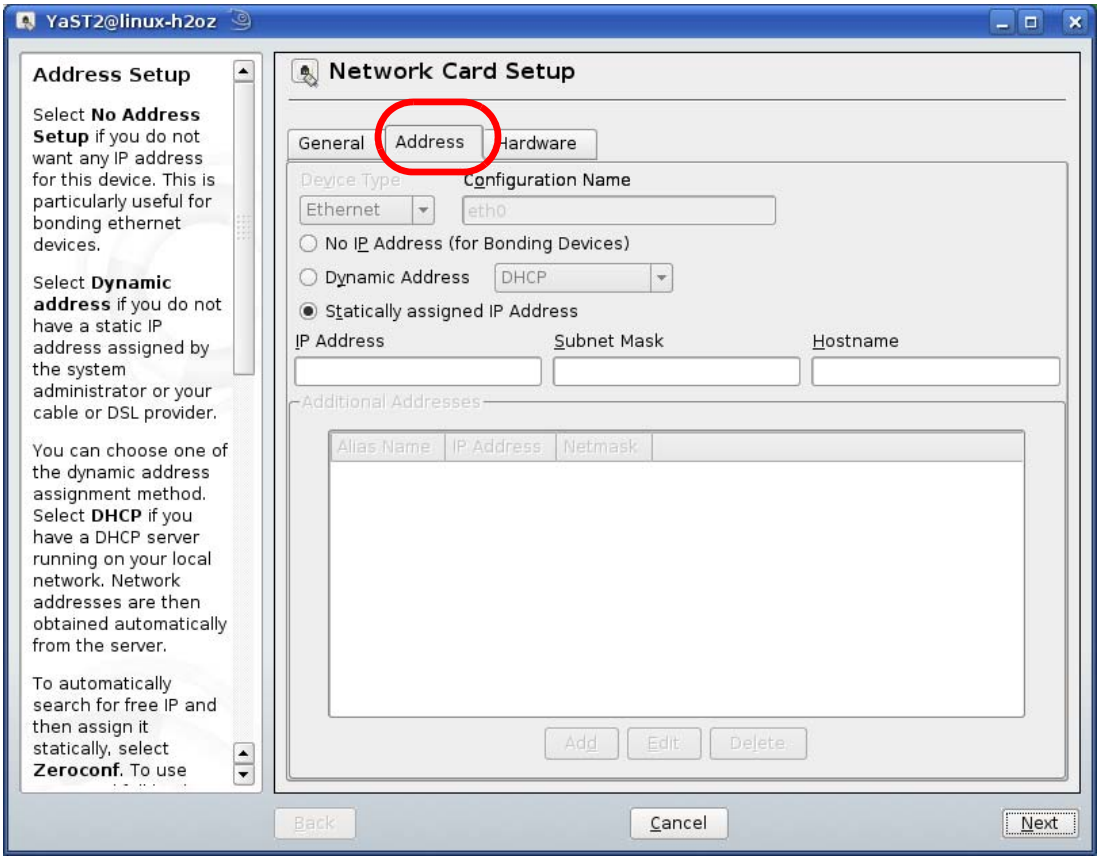
4 When the **Network Settings** window opens, click the **Overview** tab, select the appropriate connection **Name** from the list, and then click the **Configure** button.

Figure 166 openSUSE 10.3: Network Settings



5 When the **Network Card Setup** window opens, click the **Address** tab

Figure 167 openSUSE 10.3: Network Card Setup



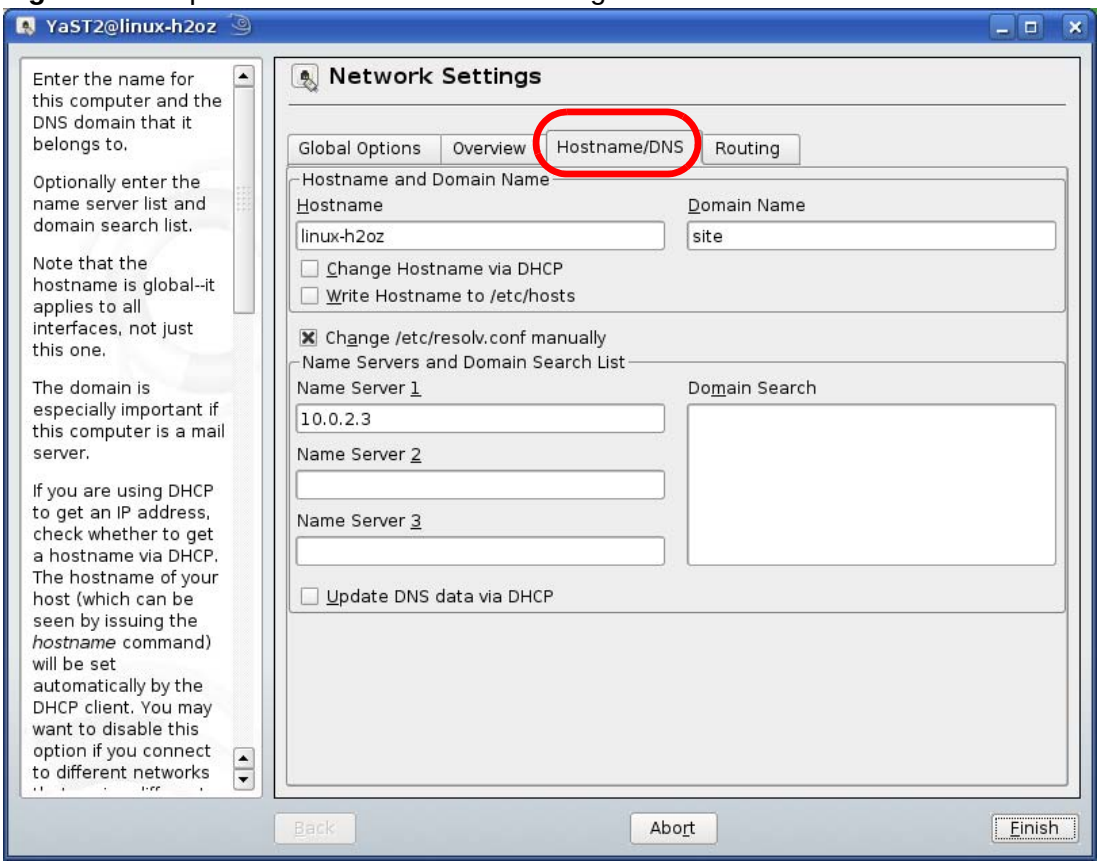
6 Select **Dynamic Address (DHCP)** if you have a dynamic IP address.

Select **Statically assigned IP Address** if you have a static IP address. Fill in the **IP address**, **Subnet mask**, and **Hostname** fields.

7 Click **Next** to save the changes and close the **Network Card Setup** window.

8 If you know your DNS server IP address(es), click the **Hostname/DNS** tab in **Network Settings** and then enter the DNS server information in the fields provided.

Figure 168 openSUSE 10.3: Network Settings



9 Click **Finish** to save your settings and close the window.

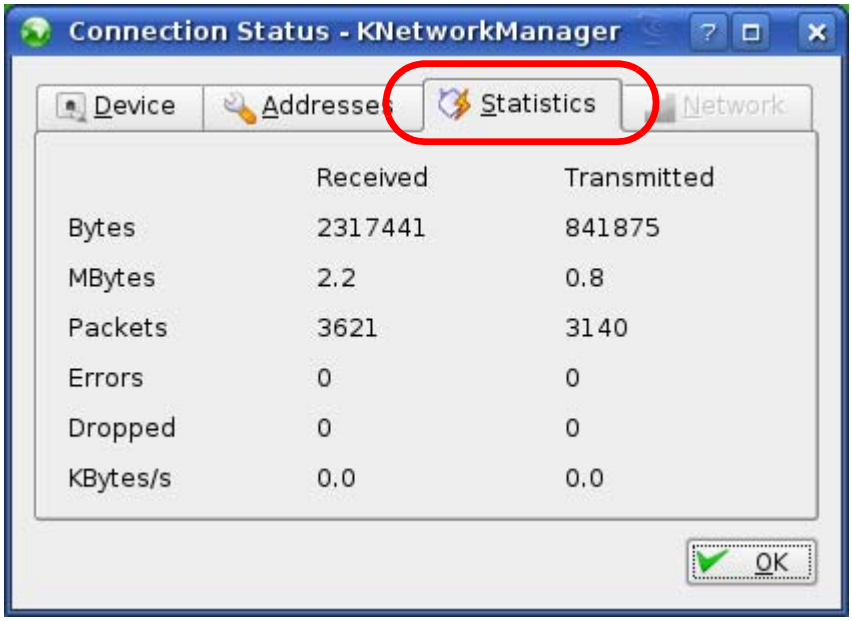
Verifying Settings

Click the **KNetwork Manager** icon on the **Task bar** to check your TCP/IP properties. From the **Options** sub-menu, select **Show Connection Information**.

Figure 169 openSUSE 10.3: KNetwork Manager

When the **Connection Status - KNetwork Manager** window opens, click the **Statistics tab** to see if your connection is working properly.

Figure 170 openSUSE: Connection Status - KNetwork Manager



B

Pop-up Windows, JavaScripts and Java Permissions

In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions may vary.

Internet Explorer Pop-up Blockers

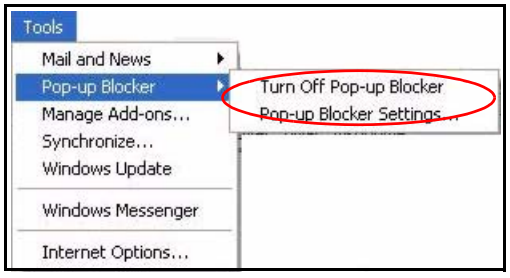
You may have to disable pop-up blocking to log into your device.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or allow pop-up blocking and create an exception for your device's IP address.

Disable Pop-up Blockers

1 In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 171 Pop-up Blocker



You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

1 In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen. This disables any web pop-up blockers you may have enabled.

Figure 172 Internet Options: Privacy

3 Click **Apply** to save this setting.

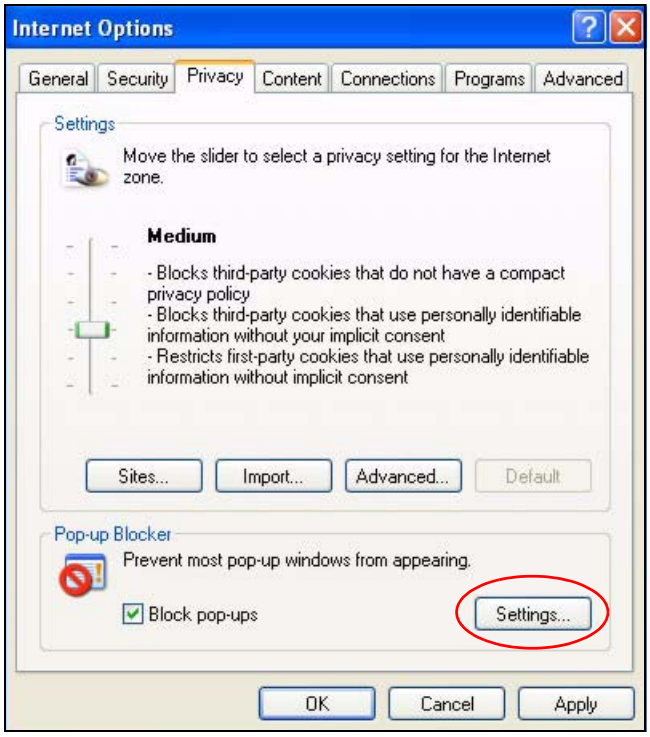
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

1 In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

2 Select **Settings...**to open the **Pop-up Blocker Settings** screen.

Figure 173 Internet Options: Privacy



3 Type the IP address of your device (the web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.167.1.

4 Click **Add** to move the IP address to the list of **Allowed sites**.

Figure 174 Pop-up Blocker Settings

5 Click **Close** to return to the **Privacy** screen.

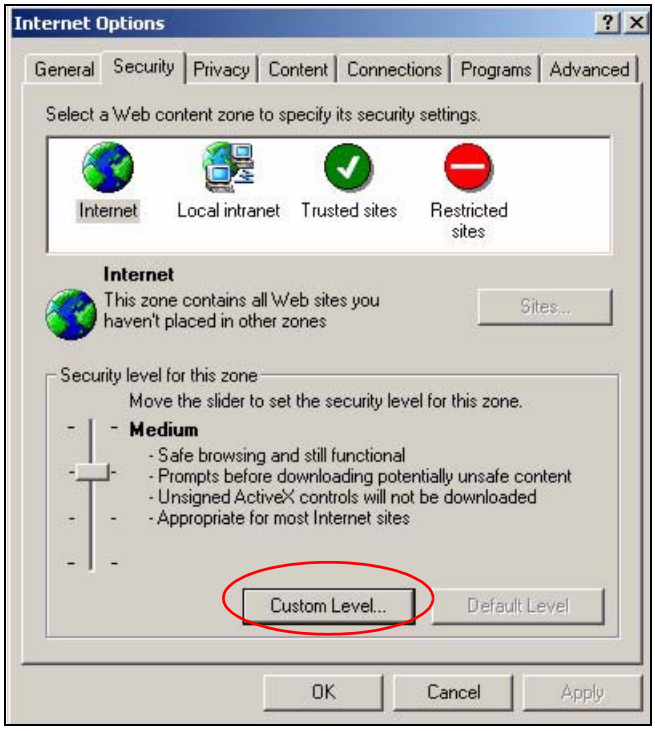
6 Click **Apply** to save this setting.

JavaScripts

If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

1 In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Figure 175 Internet Options: Security



2 Click the **Custom Level...** button.

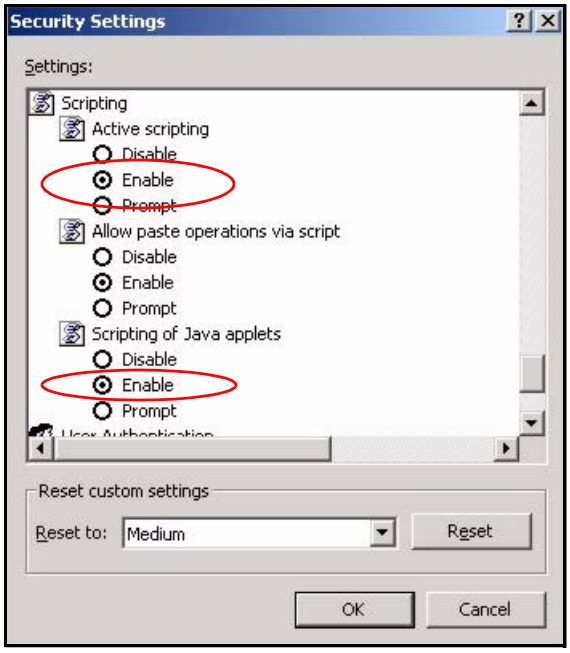
3 Scroll down to **Scripting**.

4 Under **Active scripting** make sure that **Enable** is selected (the default).

5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

6 Click **OK** to close the window.

Figure 176 Security Settings - Java Scripting



Java Permissions

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

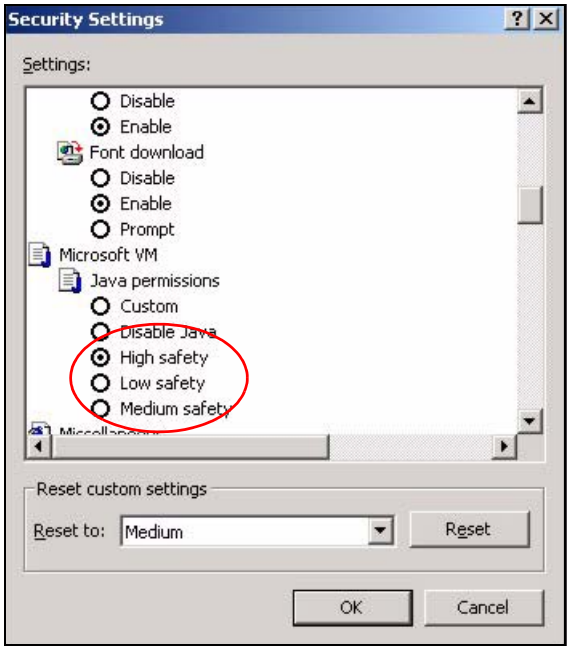
2 Click the **Custom Level...** button.

3 Scroll down to **Microsoft VM**.

4 Under **Java permissions** make sure that a safety level is selected.

5 Click **OK** to close the window.

Figure 177 Security Settings - Java



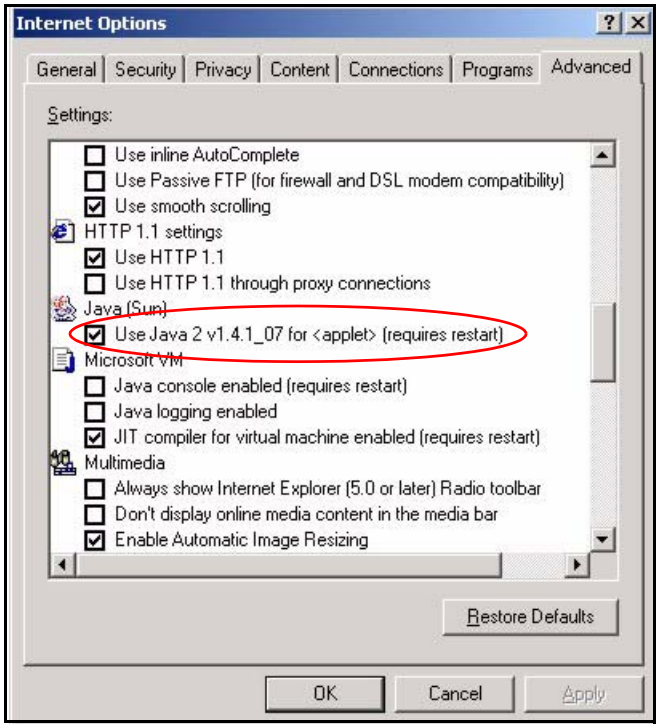
JAVA (Sun)

1 From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

3 Click **OK** to close the window.

Figure 178 Java (Sun)

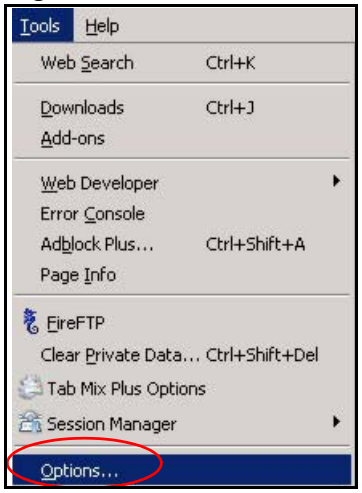


Mozilla Firefox

Mozilla Firefox 2.0 screens are used here. Screens for other versions may vary.

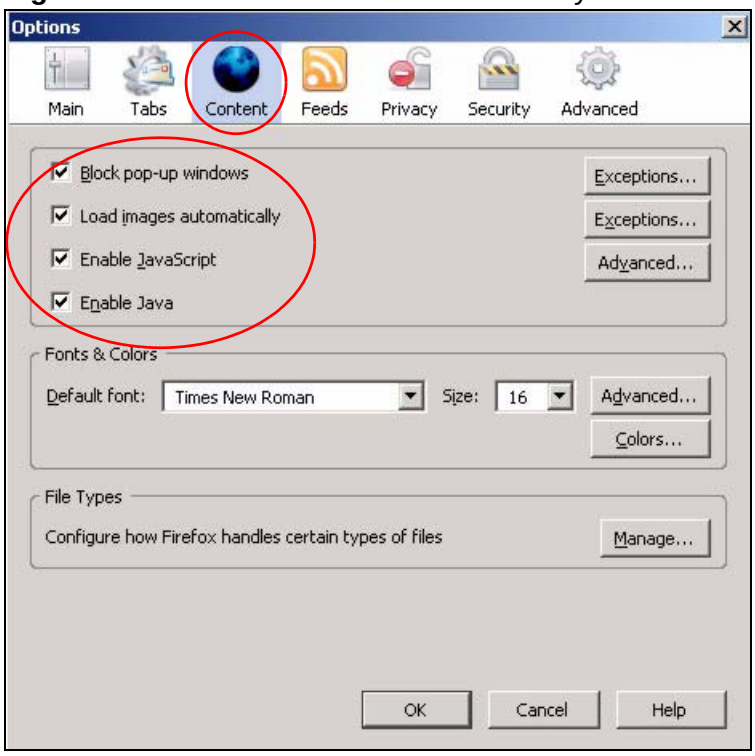
You can enable Java, Javascripts and pop-ups in one screen. Click **Tools,** then click **Options** in the screen that appears.

Figure 179 Mozilla Firefox: Tools > Options



Click **Content**.to show the screen below. Select the check boxes as shown in the following screen.

Figure 180 Mozilla Firefox Content Security



C

IP Addresses and Subnetting

This appendix introduces IP addresses and subnet masks.

IP addresses identify individual devices on a network. Every networking device (including computers, servers, routers, printers, etc.) needs an IP address to communicate across the network. These networking devices are also known as hosts.

Subnet masks determine the maximum number of possible hosts on a network. You can also use subnet masks to divide one network into multiple sub-networks.

Introduction to IP Addresses

One part of the IP address is the network number, and the other part is the host ID. In the same way that houses on a street share a common street name, the hosts on a network share a common network number. Similarly, as each house has its own house number, each host on the network has its own unique identifying number - the host ID. Routers use the network number to send packets to the correct network, while the host ID determines to which host on the network the packets are delivered.

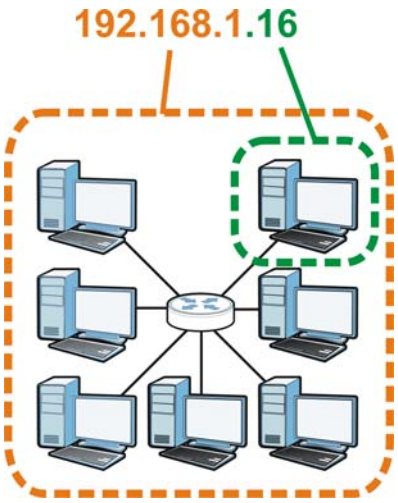
Structure

An IP address is made up of four parts, written in dotted decimal notation (for example, 192.168.1.1). Each of these four parts is known as an octet. An octet is an eight-digit binary number (for example 11000000, which is 192 in decimal notation).

Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.

The following figure shows an example IP address in which the first three octets (192.168.1) are the network number, and the fourth octet (16) is the host ID.

Figure 181 Network Number and Host ID



How much of the IP address is the network number and how much is the host ID varies according to the subnet mask.

Subnet Masks

A subnet mask is used to determine which bits are part of the network number, and which bits are part of the host ID (using a logical AND operation). The term “subnet” is short for “sub-network”.

A subnet mask has 32 bits. If a bit in the subnet mask is a “1” then the corresponding bit in the IP address is part of the network number. If a bit in the subnet mask is “0” then the corresponding bit in the IP address is part of the host ID.

The following example shows a subnet mask identifying the network number (in bold text) and host ID of an IP address (192.168.1.2 in decimal).

Table 75 IP Address Network Number and Host ID Example

	1ST OCTET: (192)	2ND OCTET: (168)	3RD OCTET: (1)	4TH OCTET (2)
IP Address (Binary)	11000000	10101000	00000001	00000010
Subnet Mask (Binary)	**11111111**	**11111111**	**11111111**	00000000
Network Number	**11000000**	**10101000**	**00000001**	
Host ID				00000010

By convention, subnet masks always consist of a continuous sequence of ones beginning from the leftmost bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

Subnet masks can be referred to by the size of the network number part (the bits with a “1” value). For example, an “8-bit mask” means that the first 8 bits of the mask are ones and the remaining 24 bits are zeroes.

Subnet masks are expressed in dotted decimal notation just like IP addresses. The following examples show the binary and decimal notation for 8-bit, 16-bit, 24-bit and 29-bit subnet masks.

Table 76 Subnet Masks

	BINARY				DECIMAL
	1ST OCTET	2ND OCTET	3RD OCTET	4TH OCTET	
8-bit mask	11111111	00000000	00000000	00000000	255.0.0.0
16-bit mask	11111111	11111111	00000000	00000000	255.255.0.0
24-bit mask	11111111	11111111	11111111	00000000	255.255.255.0
29-bit mask	11111111	11111111	11111111	11111000	255.255.255.248

Network Size

The size of the network number determines the maximum number of possible hosts you can have on your network. The larger the number of network number bits, the smaller the number of remaining host ID bits.

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 with a 24-bit subnet mask, for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 with a 24-bit subnet mask, for example).

As these two IP addresses cannot be used for individual hosts, calculate the maximum number of possible hosts in a network as follows:

Table 77 Maximum Host Numbers

SUBNET MASK		HOST ID SIZE		MAXIMUM NUMBER OF HOSTS
8 bits	255.0.0.0	24 bits	$2^{24} – 2$	16777214
16 bits	255.255.0.0	16 bits	$2^{16} – 2$	65534
24 bits	255.255.255.0	8 bits	$2^{8} – 2$	254
29 bits	255.255.255.248	3 bits	$2^{3} – 2$	6

Notation

Since the mask is always a continuous number of ones beginning from the left, followed by a continuous number of zeros for the remainder of the 32 bit mask, you can simply specify the number of ones instead of writing the value of each octet. This is usually specified by writing a "/" followed by the number of bits in the mask after the address.

For example, 192.1.1.0 /25 is equivalent to saying 192.1.1.0 with subnet mask 255.255.255.128.

The following table shows some possible subnet masks using both notations.

Table 78 Alternative Subnet Mask Notation

SUBNET MASK	ALTERNATIVE NOTATION	LAST OCTET (BINARY)	LAST OCTET (DECIMAL)
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

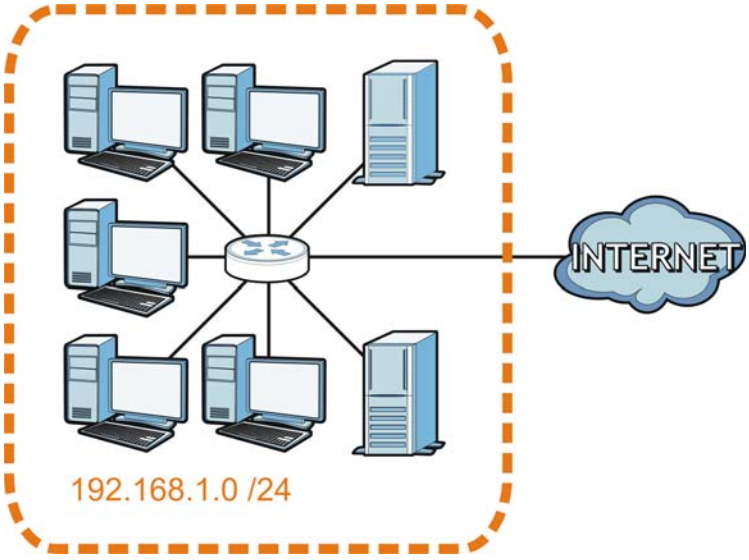
Subnetting

You can use subnetting to divide one network into multiple sub-networks. In the following example a network administrator creates two sub-networks to isolate a group of servers from the rest of the company network for security reasons.

In this example, the company network address is 192.168.1.0. The first three octets of the address (192.168.1) are the network number, and the remaining octet is the host ID, allowing a maximum of 2^8 – 2 or 254 possible hosts.

The following figure shows the company network before subnetting.

Figure 182 Subnetting Example: Before Subnetting

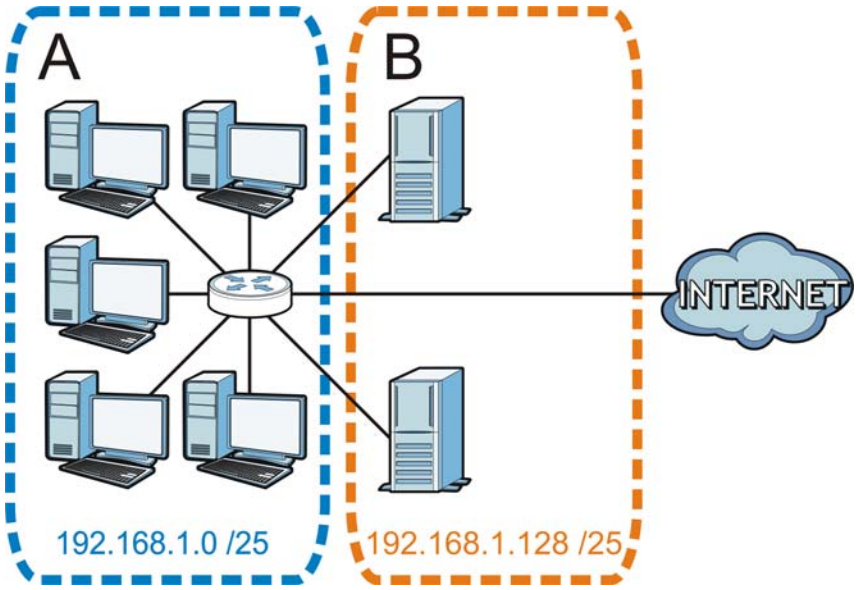


You can “borrow” one of the host ID bits to divide the network 192.168.1.0 into two separate sub-networks. The subnet mask is now 25 bits (255.255.255.128 or /25).

The “borrowed” host ID bit can have a value of either 0 or 1, allowing two subnets; 192.168.1.0 /25 and 192.168.1.128 /25.

The following figure shows the company network after subnetting. There are now two sub-networks, **A** and **B**.

Figure 183 Subnetting Example: After Subnetting



In a 25-bit subnet the host ID has 7 bits, so each sub-network has a maximum of $2^7 - 2$ or 126 possible hosts (a host ID of all zeroes is the subnet's address itself, all ones is the subnet's broadcast address).

192.168.1.0 with mask 255.255.255.128 is subnet **A** itself, and 192.168.1.127 with mask 255.255.255.128 is its broadcast address. Therefore, the lowest IP address that can be assigned to an actual host for subnet **A** is 192.168.1.1 and the highest is 192.168.1.126.

Similarly, the host ID range for subnet **B** is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The previous example illustrated using a 25-bit subnet mask to divide a 24-bit address into two subnets. Similarly, to divide a 24-bit address into four subnets, you need to "borrow" two host ID bits to give four possible combinations (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.**11**000000) or 255.255.255.192.

Each subnet contains 6 host ID bits, giving 2^6 - 2 or 62 hosts for each subnet (a host ID of all zeroes is the subnet itself, all ones is the subnet's broadcast address).

Table 79 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address (Decimal)	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**00**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 80 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	**01**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 81 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**10**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 82 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	**11**000000
Subnet Mask (Binary)	11111111.11111111.11111111.	**11**000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example: Eight Subnets

Similarly, use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

The following table shows IP address last octet values for each subnet.

Table 83 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

Subnet Planning

The following table is a summary for subnet planning on a network with a 24-bit network number.

Table 84 24-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.255.128 (/25)	2	126
2	255.255.255.192 (/26)	4	62
3	255.255.255.224 (/27)	8	30
4	255.255.255.240 (/28)	16	14
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

The following table is a summary for subnet planning on a network with a 16-bit network number.

Table 85 16-bit Network Number Subnet Planning

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
1	255.255.128.0 (/17)	2	32766
2	255.255.192.0 (/18)	4	16382
3	255.255.224.0 (/19)	8	8190
4	255.255.240.0 (/20)	16	4094
5	255.255.248.0 (/21)	32	2046
6	255.255.252.0 (/22)	64	1022
7	255.255.254.0 (/23)	128	510
8	255.255.255.0 (/24)	256	254
9	255.255.255.128 (/25)	512	126
10	255.255.255.192 (/26)	1024	62
11	255.255.255.224 (/27)	2048	30
12	255.255.255.240 (/28)	4096	14
13	255.255.255.248 (/29)	8192	6
14	255.255.255.252 (/30)	16384	2
15	255.255.255.254 (/31)	32768	1

Configuring IP Addresses

Where you obtain your network number depends on your particular situation. If the ISP or your network administrator assigns you a block of registered IP

addresses, follow their instructions in selecting the IP addresses and the subnet mask.

If the ISP did not explicitly give you an IP network number, then most likely you have a single user account and the ISP will assign you a dynamic IP address when the connection is established. If this is the case, it is recommended that you select a network number from 192.168.0.0 to 192.168.255.0. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; please do not use any other number unless you are told otherwise. You must also enable Network Address Translation (NAT) on the N4100.

Once you have decided on the network number, pick an IP address for your N4100 that is easy to remember (for instance, 192.168.1.1) but make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your N4100 will compute the subnet mask automatically based on the IP address that you entered. You don't need to change the subnet mask computed by the N4100 unless you are instructed to do otherwise.

Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet (running only between two branch offices, for example) you can assign any IP addresses to the hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

You can obtain your IP address from the IANA, from an ISP, or it can be assigned from a private network. If you belong to a small organization and your Internet access is through an ISP, the ISP can provide you with the Internet addresses for your local networks. On the other hand, if you are part of a much larger organization, you should consult your network administrator for the appropriate IP addresses.

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above. For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

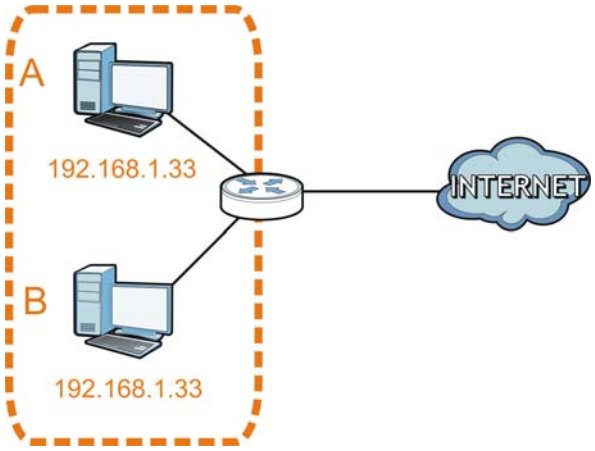
IP Address Conflicts

Each device on a network must have a unique IP address. Devices with duplicate IP addresses on the same network will not be able to access the Internet or other resources. The devices may also be unreachable through the network.

Conflicting Computer IP Addresses Example

More than one device can not use the same IP address. In the following example computer **A** has a static (or fixed) IP address that is the same as the IP address that a DHCP server assigns to computer **B** which is a DHCP client. Neither can access the Internet. This problem can be solved by assigning a different static IP address to computer **A** or setting computer **A** to obtain an IP address automatically.

Figure 184 Conflicting Computer IP Addresses Example

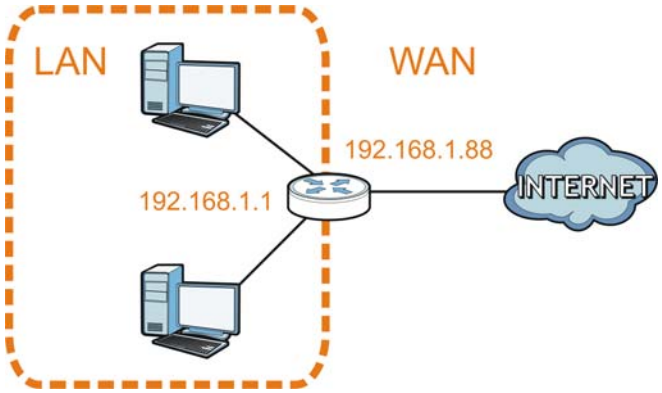


Conflicting Router IP Addresses Example

Since a router connects different networks, it must have interfaces using different network numbers. For example, if a router is set between a LAN and the Internet (WAN), the router's LAN and WAN addresses must be on different subnets. In the

following example, the LAN and WAN are on the same subnet. The LAN computers cannot access the Internet because the router cannot route between networks.

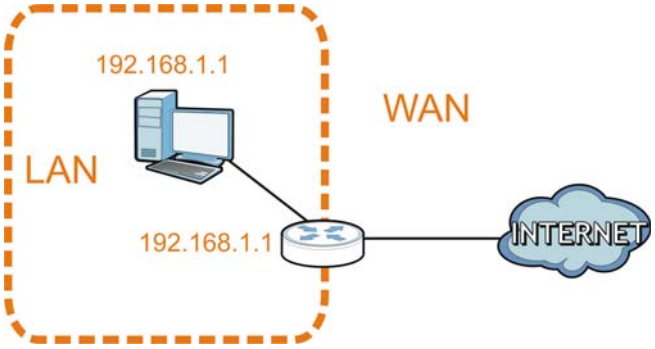
Figure 185 Conflicting Router IP Addresses Example



Conflicting Computer and Router IP Addresses Example

More than one device can not use the same IP address. In the following example, the computer and the router's LAN port both use 192.168.1.1 as the IP address. The computer cannot access the Internet. This problem can be solved by assigning a different IP address to the computer or the router's LAN port.

Figure 186 Conflicting Computer and Router IP Addresses Example



D

Wireless LANs

Note: Your specific N4100 may not support all of the wireless security types described in this appendix. See the product specifications for more information about which wireless security types are supported.

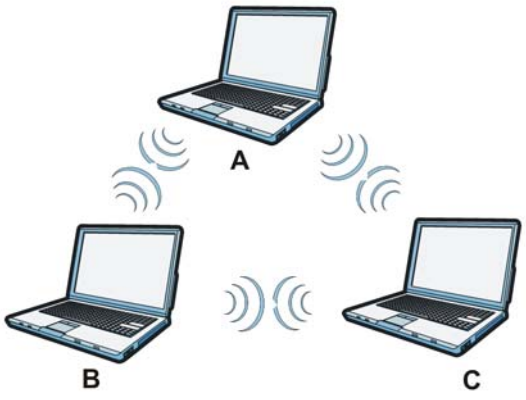
Wireless LAN Topologies

This section discusses ad-hoc and infrastructure wireless LAN topologies.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless adapters (A, B, C). Any time two or more wireless adapters are within range of each other, they can set up an independent network, which is commonly referred to as an ad-hoc network or Independent Basic Service Set (IBSS). The following diagram shows an example of notebook computers using wireless adapters to form an ad-hoc wireless LAN.

Figure 187 Peer-to-Peer Communication in an Ad-hoc Network

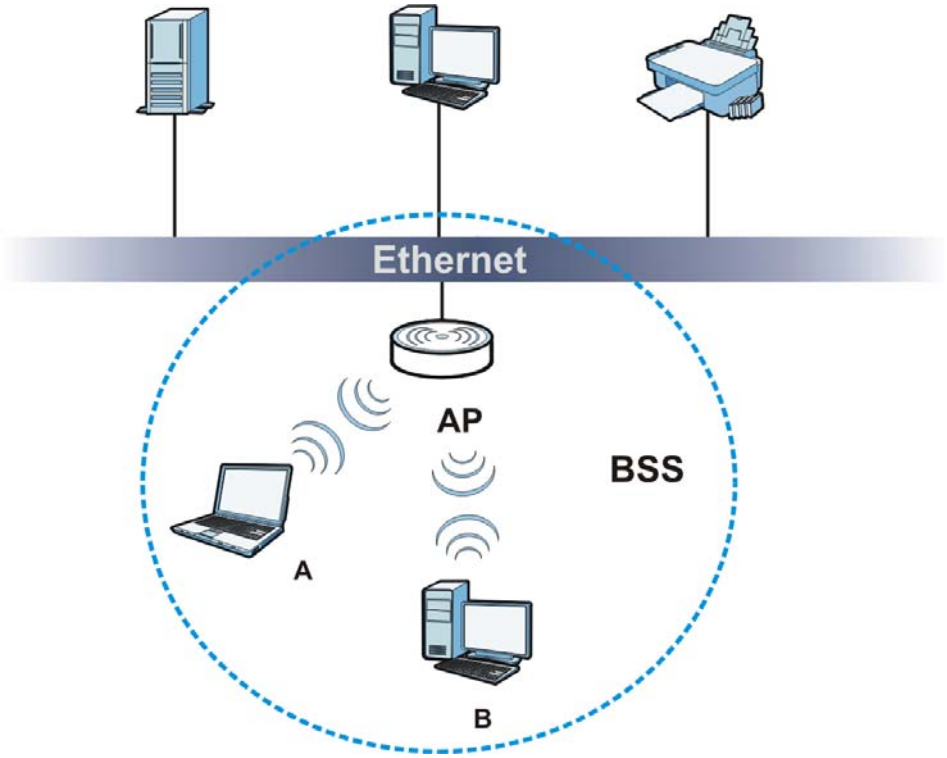


BSS

A Basic Service Set (BSS) exists when all communications between wireless clients or between a wireless client and a wired network client go through one access point (AP).

Intra-BSS traffic is traffic between wireless clients in the BSS. When Intra-BSS is enabled, wireless client **A** and **B** can access the wired network and communicate with each other. When Intra-BSS is disabled, wireless client **A** and **B** can still access the wired network but cannot communicate with each other.

Figure 188 Basic Service Set



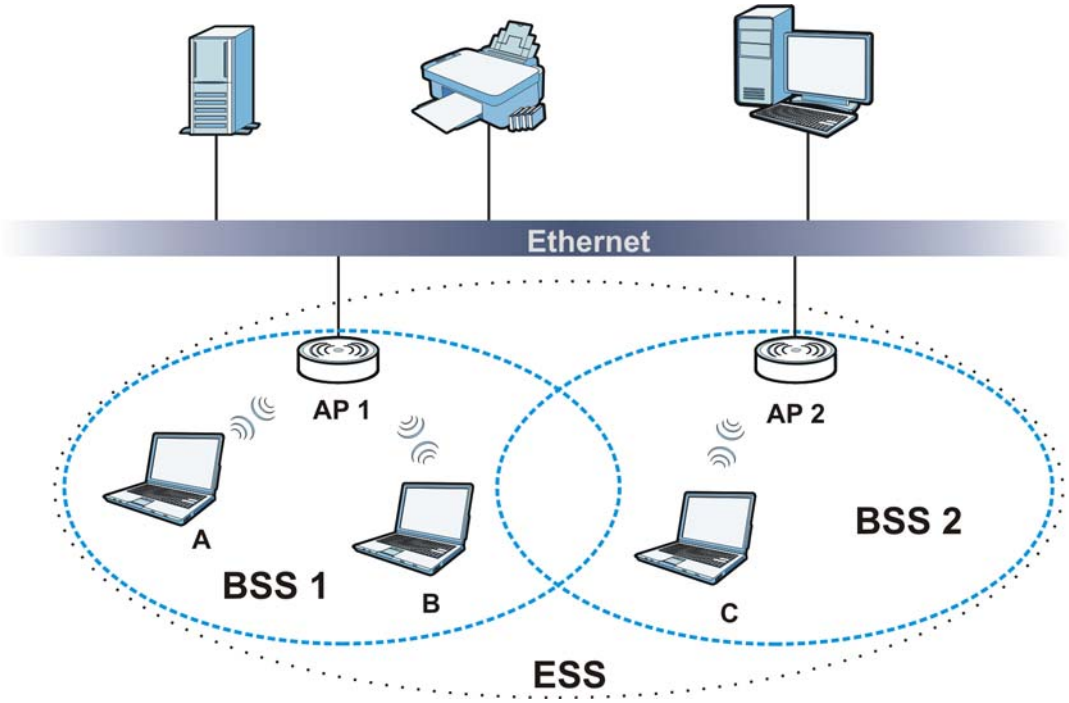
ESS

An Extended Service Set (ESS) consists of a series of overlapping BSSs, each containing an access point, with each access point connected together by a wired network. This wired connection between APs is called a Distribution System (DS).

This type of wireless LAN topology is called an Infrastructure WLAN. The Access Points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood.

An ESSID (ESS IDentification) uniquely identifies each ESS. All access points and their associated wireless clients within the same ESS must have the same ESSID in order to communicate.

Figure 189 Infrastructure WLAN



Channel

A channel is the radio frequency(ies) used by wireless devices to transmit and receive data. Channels available depend on your geographical area. You may have a choice of channels (for your region) so you should use a channel different from an adjacent AP (access point) to reduce interference. Interference occurs when radio signals from different access points overlap causing interference and degrading performance.

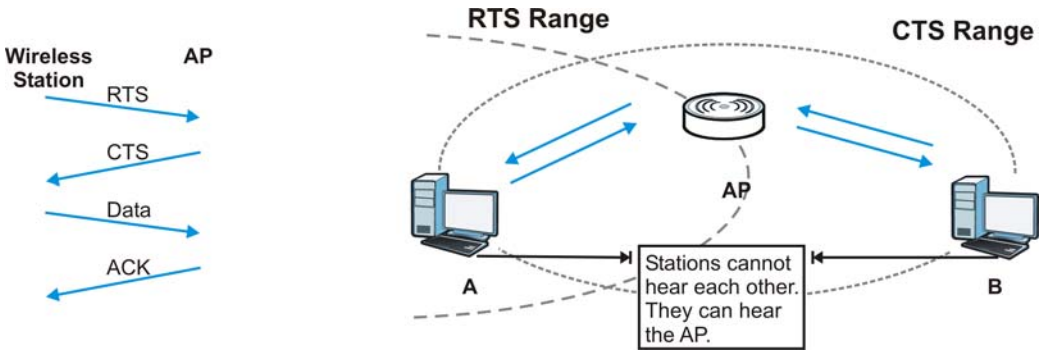
Adjacent channels partially overlap however. To avoid interference due to overlap, your AP should be on a channel at least five channels away from a channel that an adjacent AP is using. For example, if your region has 11 channels and an adjacent AP is using channel 1, then you need to select a channel between 6 or 11.

RTS/CTS

A hidden node occurs when two stations are within range of the same access point, but are not within range of each other. The following figure illustrates a

hidden node. Both stations (STA) are within range of the access point (AP) or wireless gateway, but out-of-range of each other, so they cannot "hear" each other, that is they do not know if the channel is currently being used. Therefore, they are considered hidden from each other.

Figure 190 RTS/CTS



When station **A** sends data to the AP, it might not know that the station **B** is already using the channel. If these two stations send data at the same time, collisions may occur when both sets of data arrive at the AP at the same time, resulting in a loss of messages for both stations.

RTS/CTS is designed to prevent collisions due to hidden nodes. An **RTS/CTS** defines the biggest size data frame you can send before an RTS (Request To Send)/CTS (Clear to Send) handshake is invoked.

When a data frame exceeds the **RTS/CTS** value you set (between 0 to 2432 bytes), the station that wants to transmit this frame must first send an RTS (Request To Send) message to the AP for permission to send it. The AP then responds with a CTS (Clear to Send) message to all other stations within its range to notify them to defer their transmission. It also reserves and confirms with the requesting station the time frame for the requested transmission.

Stations can send frames smaller than the specified **RTS/CTS** directly to the AP without the RTS (Request To Send)/CTS (Clear to Send) handshake.

You should only configure **RTS/CTS** if the possibility of hidden nodes exists on your network and the "cost" of resending large frames is more than the extra network overhead involved in the RTS (Request To Send)/CTS (Clear to Send) handshake.

If the **RTS/CTS** value is greater than the **Fragmentation Threshold** value (see next), then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Note: Enabling the RTS Threshold causes redundant network overhead that could negatively affect the throughput performance instead of providing a remedy.

Fragmentation Threshold

A **Fragmentation Threshold** is the maximum data fragment size (between 256 and 2432 bytes) that can be sent in the wireless network before the AP will fragment the packet into smaller data frames.

A large **Fragmentation Threshold** is recommended for networks not prone to interference while you should set a smaller threshold for busy networks or networks that are prone to interference.

If the **Fragmentation Threshold** value is smaller than the **RTS/CTS** value (see previously) you set then the RTS (Request To Send)/CTS (Clear to Send) handshake will never occur as data frames will be fragmented before they reach **RTS/CTS** size.

Preamble Type

Preamble is used to signal that data is coming to the receiver. Short and long refer to the length of the synchronization field in a packet.

Short preamble increases performance as less time sending preamble means more time for sending data. All IEEE 802.11 compliant wireless adapters support long preamble, but not all support short preamble.

Use long preamble if you are unsure what preamble mode other wireless devices on the network support, and to provide more reliable communications in busy wireless networks.

Use short preamble if you are sure all wireless devices on the network support it, and to provide more efficient communications.

Use the dynamic setting to automatically use short preamble when all wireless devices on the network support it, otherwise the N4100 uses long preamble.

Note: The wireless devices MUST use the same preamble mode in order to communicate.

IEEE 802.11g Wireless LAN

IEEE 802.11g is fully compatible with the IEEE 802.11b standard. This means an IEEE 802.11b adapter can interface directly with an IEEE 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. IEEE 802.11g has

several intermediate rate steps between the maximum and minimum data rates. The IEEE 802.11g data rate and modulation are as follows:

Table 86 IEEE 802.11g

DATA RATE (MBPS)	MODULATION
1	DBPSK (Differential Binary Phase Shift Keyed)
2	DQPSK (Differential Quadrature Phase Shift Keying)
5.5 / 11	CCK (Complementary Code Keying)
6/9/12/18/24/36/ 48/54	OFDM (Orthogonal Frequency Division Multiplexing)

Wireless Security Overview

Wireless security is vital to your network to protect wireless communication between wireless clients, access points and the wired network.

Wireless security methods available on the N4100 are data encryption, wireless client authentication, restricting access by device MAC address and hiding the N4100 identity.

The following figure shows the relative effectiveness of these wireless security methods available on your N4100.

Table 87 Wireless Security Levels

SECURITY LEVEL	SECURITY TYPE
Least Secure	Unique SSID (Default)
	Unique SSID with Hide SSID Enabled
	MAC Address Filtering
	WEP Encryption
	IEEE802.1x EAP with RADIUS Server Authentication
	Wi-Fi Protected Access (WPA)
Most Secure	WPA2

Note: You must enable the same wireless security settings on the N4100 and on all wireless clients that you want to associate with it.

IEEE 802.1x

In June 2001, the IEEE 802.1x standard was designed to extend the features of IEEE 802.11 to support extended authentication as well as providing additional

accounting and control features. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification that allows for roaming.
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the access point or the wireless clients.

RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks:

- Authentication

  Determines the identity of the users.
- Authorization

  Determines the network services available to authenticated users once they are connected to the network.
- Accounting

  Keeps track of the client's network activity.

RADIUS is a simple package exchange in which your AP acts as a message relay between the wireless client and the network RADIUS server.

Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user authentication:

- Access-Request

  Sent by an access point requesting authentication.
- Access-Reject

  Sent by a RADIUS server rejecting access.
- Access-Accept

  Sent by a RADIUS server allowing access.
- Access-Challenge

  Sent by a RADIUS server requesting more information in order to allow access. The access point sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the access point and the RADIUS server for user accounting:

- Accounting-Request

  Sent by the access point requesting accounting.
- Accounting-Response

  Sent by the RADIUS server to indicate that it has started or stopped accounting.

In order to ensure network security, the access point and the RADIUS server use a shared secret key, which is a password, they both know. The key is not sent over the network. In addition to the shared key, password information exchanged is also encrypted to protect the network from unauthorized access.

Types of EAP Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wireless LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, an access point helps a wireless station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary AP(s) that supports IEEE 802.1x. .

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificate(s) from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless client. The wireless client ‘proves’ that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plaintext passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5

authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wireless clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement EAP-TLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending username and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple username and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

Dynamic WEP Key Exchange

The AP maps a unique key that is generated with the RADIUS server. This key expires when the wireless connection times out, disconnects or reauthentication times out. A new WEP key is generated each time reauthentication is performed.

If this feature is enabled, it is not necessary to configure a default encryption key in the wireless security configuration screen. You may still configure and store keys, but they will not be used while dynamic WEP is enabled.

Note: EAP-MD5 cannot be used with Dynamic WEP Key Exchange

For added security, certificate-based authentications (EAP-TLS, EAP-TTLS and PEAP) use dynamic keys for data encryption. They are often deployed in corporate environments, but for public deployment, a simple user name and password pair is more practical. The following table is a comparison of the features of authentication types.

Table 88 Comparison of EAP Authentication Types

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP	LEAP
Mutual Authentication	No	Yes	Yes	Yes	Yes
Certificate – Client	No	Yes	Optional	Optional	No
Certificate – Server	No	Yes	Yes	Yes	No
Dynamic Key Exchange	No	Yes	Yes	Yes	Yes
Credential Integrity	None	Strong	Strong	Strong	Moderate
Deployment Difficulty	Easy	Hard	Moderate	Moderate	Moderate
Client Identity Protection	No	No	Yes	Yes	No

WPA and WPA2

Wi-Fi Protected Access (WPA) is a subset of the IEEE 802.11i standard. WPA2 (IEEE 802.11i) is a wireless security standard that defines stronger encryption, authentication and key management than WPA.

Key differences between WPA or WPA2 and WEP are improved data encryption and user authentication.

If both an AP and the wireless clients support WPA2 and you have an external RADIUS server, use WPA2 for stronger data encryption. If you don't have an external RADIUS server, you should use WPA2-PSK (WPA2-Pre-Shared Key) that only requires a single (identical) password entered into each access point, wireless gateway and wireless client. As long as the passwords match, a wireless client will be granted access to a WLAN.

If the AP or the wireless clients do not support WPA2, just use WPA or WPA-PSK depending on whether you have an external RADIUS server or not.

Select WEP only when the AP and/or wireless clients do not support WPA or WPA2. WEP is less secure than WPA or WPA2.

Encryption

WPA improves data encryption by using Temporal Key Integrity Protocol (TKIP), Message Integrity Check (MIC) and IEEE 802.1x. WPA2 also uses TKIP when

required for compatibility reasons, but offers stronger encryption than TKIP with Advanced Encryption Standard (AES) in the Counter mode with Cipher block chaining Message authentication code Protocol (CCMP).

TKIP uses 128-bit keys that are dynamically generated and distributed by the authentication server. AES (Advanced Encryption Standard) is a block cipher that uses a 256-bit mathematical algorithm called Rijndael. They both include a per-packet key mixing function, a Message Integrity Check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA and WPA2 regularly change and rotate the encryption keys so that the same encryption key is never used twice.

The RADIUS server distributes a Pairwise Master Key (PMK) key to the AP that then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients. This all happens in the background automatically.

The Message Integrity Check (MIC) is designed to prevent an attacker from capturing data packets, altering them and resending them. The MIC provides a strong mathematical function in which the receiver and the transmitter each compute and then compare the MIC. If they do not match, it is assumed that the data has been tampered with and the packet is dropped.

By generating unique data encryption keys for every data packet and by creating an integrity checking mechanism (MIC), with TKIP and AES it is more difficult to decrypt data on a Wi-Fi network than WEP and difficult for an intruder to break into the network.

The encryption mechanisms used for WPA(2) and WPA(2)-PSK are the same. The only difference between the two is that WPA(2)-PSK uses a simple common password, instead of user-specific credentials. The common-password approach makes WPA(2)-PSK susceptible to brute-force password-guessing attacks but it's still an improvement over WEP as it employs a consistent, single, alphanumeric password to derive a PMK which is used to generate unique temporal encryption keys. This prevent all wireless devices sharing the same encryption keys. (a weakness of WEP)

User Authentication

WPA and WPA2 apply IEEE 802.1x and Extensible Authentication Protocol (EAP) to authenticate wireless clients using an external RADIUS database. WPA2 reduces the number of key exchange messages from six to four (CCMP 4-way handshake) and shortens the time required to connect to a network. Other WPA2 authentication features that are different from WPA include key caching and pre-

authentication. These two features are optional and may not be supported in all wireless devices.

Key caching allows a wireless client to store the PMK it derived through a successful authentication with an AP. The wireless client uses the PMK when it tries to connect to the same AP and does not need to go with the authentication process again.

Pre-authentication enables fast roaming by allowing the wireless client (already connecting to an AP) to perform IEEE 802.1x authentication with another AP before connecting to it.

Wireless Client WPA Supplicants

A wireless client supplicant is the software that runs on an operating system instructing the wireless client how to use WPA. At the time of writing, the most widely available supplicant is the WPA patch for Windows XP, Funk Software's Odyssey client.

The Windows XP patch is a free download that adds WPA capability to Windows XP's built-in "Zero Configuration" wireless client. However, you must run Windows XP to use it.

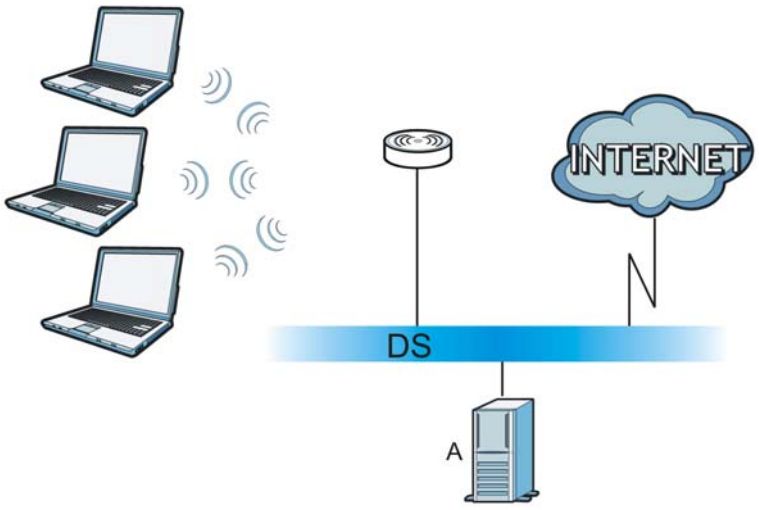
WPA(2) with RADIUS Application Example

To set up WPA(2), you need the IP address of the RADIUS server, its port number (default is 1812), and the RADIUS shared secret. A WPA(2) application example with an external RADIUS server looks as follows. "A" is the RADIUS server. "DS" is the distribution system.

1. The AP passes the wireless client's authentication request to the RADIUS server.
2. The RADIUS server then checks the user's identification against its database and grants or denies network access accordingly.
3. A 256-bit Pairwise Master Key (PMK) is derived from the authentication process by the RADIUS server and the client.

4 The RADIUS server distributes the PMK to the AP. The AP then sets up a key hierarchy and management system, using the PMK to dynamically generate unique data encryption keys. The keys are used to encrypt every data packet that is wirelessly communicated between the AP and the wireless clients.

Figure 191 WPA(2) with RADIUS Application Example



WPA(2)-PSK Application Example

A WPA(2)-PSK application looks as follows.

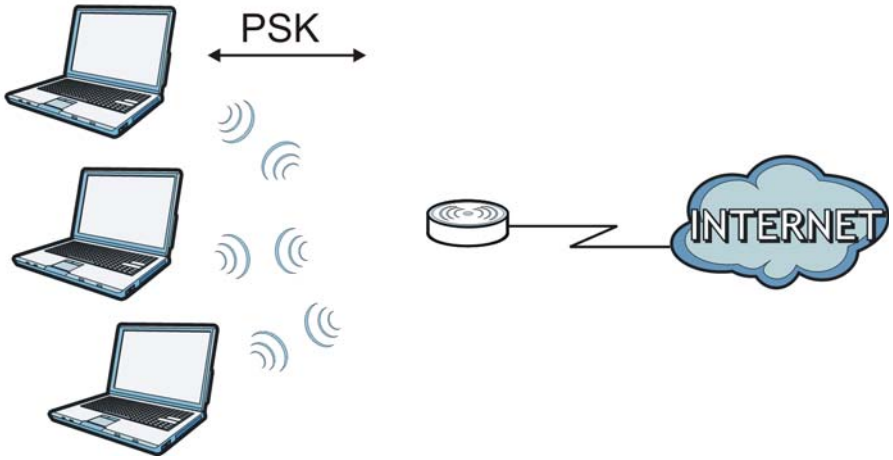
1 First enter identical passwords into the AP and all wireless clients. The Pre-Shared Key (PSK) must consist of between 8 and 63 ASCII characters or 64 hexadecimal characters (including spaces and symbols).

2 The AP checks each wireless client's password and allows it to join the network only if the password matches.

3 The AP and wireless clients generate a common PMK (Pairwise Master Key). The key itself is not sent over the network, but is derived from the PSK and the SSID.

4 The AP and wireless clients use the TKIP or AES encryption process, the PMK and information exchanged in a handshake to create temporal encryption keys. They use these keys to encrypt data exchanged between them.

Figure 192 WPA(2)-PSK Authentication



Security Parameters Summary

Refer to this table to see what other security parameters you should configure for each authentication method or key management protocol type. MAC address filters are not dependent on how you configure these security features.

Table 89 Wireless Security Relational Matrix

AUTHENTICATION METHOD/ KEY MANAGEMENT PROTOCOL	ENCRYPTION METHOD	ENTER MANUAL KEY	IEEE 802.1X
Open	None	No	Disable
			Enable without Dynamic WEP Key
Open	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
Shared	WEP	No	Enable with Dynamic WEP Key
		Yes	Enable without Dynamic WEP Key
		Yes	Disable
WPA	TKIP/AES	No	Enable
WPA-PSK	TKIP/AES	Yes	Disable
WPA2	TKIP/AES	No	Enable
WPA2-PSK	TKIP/AES	Yes	Disable

Antenna Overview

An antenna couples RF signals onto air. A transmitter within a wireless device sends an RF signal to the antenna, which propagates the signal through the air. The antenna also operates in reverse by capturing RF signals from the air.

Positioning the antennas properly increases the range and coverage area of a wireless LAN.

Antenna Characteristics

Frequency

An antenna in the frequency of 2.4GHz (IEEE 802.11b and IEEE 802.11g) or 5GHz (IEEE 802.11a) is needed to communicate efficiently in a wireless LAN

Radiation Pattern

A radiation pattern is a diagram that allows you to visualize the shape of the antenna's coverage area.

Antenna Gain

Antenna gain, measured in dB (decibel), is the increase in coverage within the RF beam width. Higher antenna gain improves the range of the signal for better communications.

For an indoor site, each 1 dB increase in antenna gain results in a range increase of approximately 2.5%. For an unobstructed outdoor site, each 1dB increase in gain results in a range increase of approximately 5%. Actual results may vary depending on the network environment.

Antenna gain is sometimes specified in dBi, which is how much the antenna increases the signal power compared to using an isotropic antenna. An isotropic antenna is a theoretical perfect antenna that sends out radio signals equally well in all directions. dBi represents the true gain that the antenna provides.

Types of Antennas for WLAN

There are two types of antennas used for wireless LAN applications.

- Omni-directional antennas send the RF signal out in all directions on a horizontal plane. The coverage area is torus-shaped (like a donut) which makes these antennas ideal for a room environment. With a wide coverage area, it is possible to make circular overlapping coverage areas with multiple access points.
- Directional antennas concentrate the RF signal in a beam, like a flashlight does with the light from its bulb. The angle of the beam determines the width of the coverage pattern. Angles typically range from 20 degrees (very directional) to 120 degrees (less directional). Directional antennas are ideal for hallways and outdoor point-to-point applications.

Positioning Antennas

In general, antennas should be mounted as high as practically possible and free of obstructions. In point-to–point application, position both antennas at the same height and in a direct line of sight to each other to attain the best performance.

For omni-directional antennas mounted on a table, desk, and so on, point the antenna up. For omni-directional antennas mounted on a wall or ceiling, point the antenna down. For a single AP application, place omni-directional antennas as close to the center of the coverage area as possible.

For directional antennas, point the antenna in the direction of the desired coverage area.

E

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name**: This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol**: This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **USER-DEFINED**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s)**: This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
  - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
  - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description**: This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 90 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.

Table 90 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Management Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).

Table 90 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.

Table 90 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

F

Open Software Announcements

End-User License Agreement for "N4100"

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE COMPLETING THE INSTALLATION PROCESS AS INSTALLING THE SOFTWARE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN ZyXEL, IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE UNINSTALLED SOFTWARE AND PACKAGING TO THE PLACE FROM WHICH IT WAS ACQUIRED OR ZyXEL, AND YOUR MONEY WILL BE REFUNDED.

1 Grant of License for Personal Use

ZyXEL Communications Corp. ("ZyXEL") grants you a non-exclusive, non-sublicense, non-transferable license to use the program with which this license is distributed (the "Software"), including any documentation files accompanying the Software ("Documentation"), for internal business use only, for up to the number of users specified in sales order and invoice. You have the right to make one backup copy of the Software and Documentation solely for archival, back-up or disaster recovery purposes. You shall not exceed the scope of the license granted hereunder. Any rights not expressly granted by ZyXEL to you are reserved by ZyXEL, and all implied licenses are disclaimed.

2 Ownership

You have no ownership rights in the Software. Rather, you have a license to use the Software as long as this License Agreement remains in full force and effect. Ownership of the Software, Documentation and all intellectual property rights therein shall remain at all times with ZyXEL. Any other use of the Software by any other entity is strictly forbidden and is a violation of this License Agreement.

3 Copyright

The Software and Documentation contain material that is protected by International Copyright Law and trade secret law, and by international treaty provisions. All rights not granted to you herein are expressly reserved by ZyXEL. You may not remove any proprietary notice of ZyXEL or any of its licensors from any copy of the Software or Documentation.

4 Restrictions

You may not publish, display, disclose, sell, rent, lease, modify, store, loan, distribute, or create derivative works of the Software, or any part thereof. You may not assign, sublicense, convey or otherwise transfer, pledge as security or otherwise encumber the rights and licenses granted hereunder with respect to the Software. Certain components of the Software, and third party open source programs included with the Software, have been or may be made available by ZyXEL listed in the below Table (collectively the "Open-Sourced Components") You may modify or replace only these Open-Sourced Components; provided that you comply with the terms of this License and any applicable licensing terms governing use of the Open-Sourced Components, which have been provided on the online electronic documents for the Software (ftp://opensource.zyxel.com). ZyXEL is not obligated to provide any maintenance, technical or other support for the resultant modified Software. You may not copy, reverse engineer, decompile, reverse compile, translate, adapt, or disassemble the Software, or any part thereof, nor shall you attempt to create the source code from the object code for the Software. Except as and only to the extent expressly permitted in this License, by applicable licensing terms governing use of the Open-Sourced Components, or by applicable law, you may not market, co-brand, private label or otherwise permit third parties to link to the Software, or any part thereof. You may not use the Software, or any part thereof, in the operation of a service bureau or for the benefit of any other person or entity. You may not cause, assist or permit any third party to do any of the foregoing. Portions of the Software utilize or include third party software and other copyright material. Acknowledgements, licensing terms and disclaimers for such material are contained in the online electronic documentation for the Software (ftp://opensource.zyxel.com), and your use of such material is governed by their respective terms. ZyXEL has provided, as part of the Software package, access to certain third party software as a convenience. To the extent that the Software contains third party software, ZyXEL has no express or implied obligation to provide any technical or other support for such software. Please contact the appropriate software vendor or manufacturer directly for technical support and customer service related to its software and products.

5 Confidentiality

You acknowledge that the Software contains proprietary trade secrets of ZyXEL and you hereby agree to maintain the confidentiality of the Software using at least as great a degree of care as you use to maintain the confidentiality of your own most confidential information. You agree to reasonably communicate the terms and conditions of this License Agreement to those persons employed by you who

come into contact with the Software, and to use reasonable best efforts to ensure their compliance with such terms and conditions, including, without limitation, not knowingly permitting such persons to use any portion of the Software for the purpose of deriving the source code of the Software.

6 No Warranty

THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, ZyXEL DISCLAIMS ALL WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. ZyXEL DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET ANY REQUIREMENTS OR NEEDS YOU MAY HAVE, OR THAT THE SOFTWARE WILL OPERATE ERROR FREE, OR IN AN UNINTERUPTED FASHION, OR THAT ANY DEFECTS OR ERRORS IN THE SOFTWARE WILL BE CORRECTED, OR THAT THE SOFTWARE IS COMPATIBLE WITH ANY PARTICULAR PLATFORM. SOME JURISDICTIONS DO NOT ALLOW THE WAIVER OR EXCLUSION OF IMPLIED WARRANTIES SO THEY MAY NOT APPLY TO YOU. IF THIS EXCLUSION IS HELD TO BE UNENFORCEABLE BY A COURT OF COMPETENT JURISDICTION, THEN ALL EXPRESS AND IMPLIED WARRANTIES SHALL BE LIMITED IN DURATION TO A PERIOD OF THIRTY (30) DAYS FROM THE DATE OF PURCHASE OF THE SOFTWARE, AND NO WARRANTIES SHALL APPLY AFTER THAT PERIOD.

7 Limitation of Liability

IN NO EVENT WILL ZyXEL BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, INDIRECT, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES FOR LOSS OF BUSINESS, LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE PROGRAM, OR FOR ANY CLAIM BY ANY OTHER PARTY, EVEN IF ZyXEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ZyXEL's AGGREGATE LIABILITY WITH RESPECT TO ITS OBLIGATIONS UNDER THIS AGREEMENT OR OTHERWISE WITH RESPECT TO THE SOFTWARE AND DOCUMENTATION OR OTHERWISE SHALL BE EQUAL TO THE PURCHASE PRICE, BUT SHALL IN NO EVENT EXCEED THE PRODUCT'S PRICE. BECAUSE SOME STATES/COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

8 Export Restrictions

THIS LICENSE AGREEMENT IS EXPRESSLY MADE SUBJECT TO ANY APPLICABLE LAWS, REGULATIONS, ORDERS, OR OTHER RESTRICTIONS ON THE EXPORT OF THE SOFTWARE OR INFORMATION ABOUT SUCH SOFTWARE WHICH MAY BE IMPOSED FROM TIME TO TIME. YOU SHALL NOT EXPORT THE SOFTWARE, DOCUMENTATION OR INFORMATION ABOUT THE SOFTWARE AND DOCUMENTATION WITHOUT COMPLYING WITH SUCH LAWS, REGULATIONS,

ORDERS, OR OTHER RESTRICTIONS. YOU AGREE TO INDEMNIFY ZyXEL AGAINST ALL CLAIMS, LOSSES, DAMAGES, LIABILITIES, COSTS AND EXPENSES, INCLUDING REASONABLE ATTORNEYS' FEES, TO THE EXTENT SUCH CLAIMS ARISE OUT OF ANY BREACH OF THIS SECTION 8.

9 Audit Rights

ZyXEL SHALL HAVE THE RIGHT, AT ITS OWN EXPENSE, UPON REASONABLE PRIOR NOTICE, TO PERIODICALLY INSPECT AND AUDIT YOUR RECORDS TO ENSURE YOUR COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT.

10 Termination

This License Agreement is effective until it is terminated. You may terminate this License Agreement at any time by destroying or returning to ZyXEL all copies of the Software and Documentation in your possession or under your control. ZyXEL may terminate this License Agreement for any reason, including, but not limited to, if ZyXEL finds that you have violated any of the terms of this License Agreement. Upon notification of termination, you agree to destroy or return to ZyXEL all copies of the Software and Documentation and to certify in writing that all known copies, including backup copies, have been destroyed. All provisions relating to confidentiality, proprietary rights, and non-disclosure shall survive the termination of this Software License Agreement.

11 General

This License Agreement shall be construed, interpreted and governed by the laws of Republic of China without regard to conflicts of laws provisions thereof. The exclusive forum for any disputes arising out of or relating to this License Agreement shall be an appropriate court or Commercial Arbitration Association sitting in ROC, Taiwan. This License Agreement shall constitute the entire Agreement between the parties hereto. This License Agreement, the rights granted hereunder, the Software and Documentation shall not be assigned by you without the prior written consent of ZyXEL. Any waiver or modification of this License Agreement shall only be effective if it is in writing and signed by both parties hereto. If any part of this License Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this License Agreement shall be interpreted so as to reasonably effect the intention of the parties.

Note: Some components of this product incorporate source code covered under the open source code licenses. To obtain the source code covered under those Licenses, please check ZyXEL Technical Support (support@zyxel.com.tw) to get it.

Open-Source Packages for "N4100"

3RD PARTY SOFTWARE	VERSION	WEB ADDRESS OF THE SOFTWARE / LICENSE TERM
Boa	0.94.14	http://www.boa.org
Bridge-Utils	1.2	http://www.linuxfoundation.org/collaborate/workgroups/networking/bridge
Busybox	1.4.2	http://www.busybox.net/
Cgic	2.05	http://www.boutell.com/cgic/
Curl	7.16.2	http://curl.haxx.se/
Dnrd	2.20.3	http://dnrd.sourceforge.net/
Dropbear	0.49	http://matt.ucc.asn.au/dropbear/dropbear.html
Ebtables	2.0.8.2	http://ebtables.sourceforge.net/
ez-ipupdate	3.0.11b7	http://www.gusnet.cx/proj/ez-ipupdate
Iproute2	2.6.20	http://www.linuxfoundation.org/collaborate/workgroups/networking/iproute2
Iptables	1.3.7	http://www.netfilter.org/
ixp400_xscale_sw	3.01	http://www.intel.com/design/network/products/npfamily/download_ixp400.htm
Libnl	1.0-pre6	http://www.mail-archive.com/pld-cvs-commit@lists.pld-linux.org/msg78936.html
Lighttpd	1.4.13	http://www.lighttpd.net/
Pimd	2.1.0-alpha29.17	http://packages.debian.org/changelogs/pool/main/p/pimd/pimd_2.1.0-alpha29.17-9/pimd.copyright
Msmtp	1.4.14	http://msmtp.sourceforge.net/
Ntpclient	2000_339	http://doolittle.icarus.com/ntpclient/
Openssl	0.9.8g	http://www.openssl.org/
Ppp	2.4.4	http://gentoo-portage.com/net-dialup/ppp
Rp-pppoe	3.8	http://www.roaringpenguin.com/products/pppoe
Freeradius	1.1.7	http://www.freeradius.org
Net-snmp	5.5	http://www.net-snmp.org/
Squid	2.5.stable14	http://www.squid-cache.org/
Udev	103	http://www.kernel.org/pub/linux/utils/kernel/hotplug/udev.html
Zlib	1.2.3	http://www.zlib.net/

G

Legal Information

Copyright

Disclaimers

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Your use of the N4100 is subject to the terms and conditions of any related service providers.

Certifications

Federal Communications Commission (FCC) Interference Statement

The device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operations.

This device has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to

provide reasonable protection against harmful interference in a residential installation. This device generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this device does cause harmful interference to radio/television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and the receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.
- To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons.

Industry Canada Statement

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

1) this device may not cause interference and

2) this device must accept any interference, including interference that may cause undesired operation of the device

This device has been designed to operate with an antenna having a maximum gain of 2dBi.

Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the EIRP is not more than required for successful communication.

IC Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance.

注意 !

依據　低功率電波輻射性電機管理辦法

第十二條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。
前項合法通信，指依電信規定作業之無線電信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

本機限在不干擾合法電臺與不受被干擾保障條件下於室內使用。
減少電磁波影響，請妥適使用。

Notices

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device has been designed for the WLAN 2.4 GHz network throughout the EC region and Switzerland, with restrictions in France.

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Viewing Certifications

1. Go to http://www.zyxel.com.
2. Select your product on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W