Vantage RADIUS 50

User's Guide

Version 1.0

8/2005

ZyXEL

Copyright

Copyright © 2005 by ZyXEL Communications Corporation.

Disclaimer

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.

Trademarks

Trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Federal Communications Commission (FCC) Interference Statement

This 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 equipment has been tested and found to comply with the limits for a CLASS B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This equipment 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.

If this equipment does cause harmful interference to radio/television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and the receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Notice 1

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Certifications

1. Go to www.zyxel.com
2. Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
3. Select the certification you wish to view from this page

FC Tested To Comply
With FCC Standards
FOR HOME OR OFFICE USE

Information for Canadian Users

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Industry Canada does not guarantee that the equipment will operate to a user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly. The customer should be aware that the compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

For their own protection, users should ensure that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.

Note

This digital apparatus does not exceed the class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of Industry Canada.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to two years from the date of purchase. 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 value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product is 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 of character to the purchaser.

To obtain the services of this warranty, contact ZyXEL's Service Center for your Return Material Authorization number (RMA). Products must be returned Postage Prepaid. It is recommended that the unit be insured when shipped. Any returned products without proof of purchase or those with an out-dated warranty will be repaired or replaced (at the discretion of ZyXEL) and the customer will be billed for parts and labor. All repaired or replaced products will be shipped by ZyXEL to the corresponding return address, Postage Paid. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

Online Registration

Register online registration at www.zyxel.com for free future product updates and information.

Customer Support

When you contact your customer support representative please have the following information ready: Please have the following information ready when you contact customer support.

- 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.

METHOD	SUPPORT E-MAIL	TELEPHONE [1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
CORPORATE HEADQUARTERS (WORLDWIDE)	support@zyxel.com.tw	+886-3-578-3942	www.zyxel.com www.europe.zyxel.com	ZyXEL Communications Corp. 6 Innovation Road II Science Park Hsinchu 300 Taiwan
	sales@zyxel.com.tw	+886-3-578-2439	ftp.zyxel.com ftp.europe.zyxel.com	
CZECH REPUBLIC	info@cz.zyxel.com	+420 241 091 350	www.zyxel.cz	ZyXEL Communications Czech s.r.o. Modranská 621 143 01 Praha 4 – Modrany Ceská Republika
	info@cz.zyxel.com	+420 241 091 359		
DENMARK	support@zyxel.dk	+45 39 55 07 00	www.zyxel.dk	ZyXEL Communications A/S Columbusvej 5 2860 Soeborg Denmark
	sales@zyxel.dk	+45 39 55 07 07		
FINLAND	support@zyxel.fi	+358-9-4780-8411	www.zyxel.fi	ZyXEL Communications Oy Malminkaari 10 00700 Helsinki Finland
	sales@zyxel.fi	+358-9-4780 8448		
FRANCE	info@zyxel.fr	+33 (0)4 72 52 97 97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33 (0)4 72 52 19 20		
GERMANY	support@zyxel.de	+49-2405-6909-0	www.zyxel.de	ZyXEL Deutschland GmbH. Adenauerstr. 20/A2 D-52146 Wuerselen Germany
	sales@zyxel.de	+49-2405-6909-99		
NORTH AMERICA	support@zyxel.com	+1-800-255-4101 +1-714-632-0882	www.us.zyxel.com	ZyXEL Communications Inc. 1130 N. Miller St. Anaheim CA 92806-2001 U.S.A.
	sales@zyxel.com	+1-714-632-0858	ftp.us.zyxel.com	

[1] "+" is the (prefix) number you enter to make an international telephone call.

METHOD	SUPPORT E-MAIL	TELEPHONE [1]	WEB SITE	REGULAR MAIL
LOCATION	SALES E-MAIL	FAX	FTP SITE	
NORWAY	support@zyxel.no	+47 22 80 61 80	www.zyxel.no	ZyXEL Communications A/S Nils Hansens vei 13 0667 Oslo Norway
	sales@zyxel.no	+47 22 80 61 81		
SPAIN	support@zyxel.es	+34 902 195 420	www.zyxel.es	ZyXEL Communications Alejandro Villegas 33 1º, 28043 Madrid Spain
	sales@zyxel.es	+34 913 005 345		
SWEDEN	support@zyxel.se	+46 31 744 7700	www.zyxel.se	ZyXEL Communications A/S Sjöporten 4, 41764 Göteborg Sweden
	sales@zyxel.se	+46 31 744 7701		
UNITED KINGDOM	support@zyxel.co.uk	+44 (0) 1344 303044 08707 555779 (UK only)	www.zyxel.co.uk	ZyXEL Communications UK Ltd., 11, The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom (UK)
	sales@zyxel.co.uk	+44 (0) 1344 303034	ftp.zyxel.co.uk	

Table of Contents

List of Figures

List of Tables

List of Charts

Preface

About This User's Manual

Congratulations on your purchase of Vantage RADIUS 50. This manual is designed to guide you through the configuration of your Vantage RADIUS for its various applications.

Use the web configurator, or command interpreter interface to configure your Vantage RADIUS Server. Not all features can be configured through all interfaces.

This manual may refer to Vantage RADIUS 50 as Vantage RADIUS.

Related Documentation

- Support Disk
  Refer to the included CD for support documents.
- Quick Start Guide
  The Quick Start Guide is designed to help you get up and running right away. It contains a detailed easy-to-follow connection diagram, default settings, handy checklists and information on setting up your network and configuring for Internet access.
- Web Configurator Online Help
  Embedded web help for descriptions of individual screens and supplementary information.
- Packing List Card
  The Packing List Card lists all items that should have come in the package.
- Certifications
  Refer to the product page at www.zyxel.com for information on product certifications.
- ZyXEL Glossary and Web Site
  Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User’s Guide Feedback

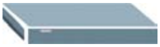
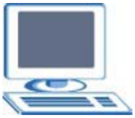
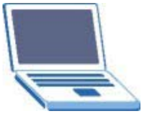
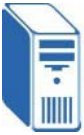
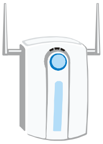
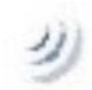
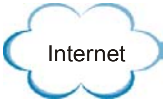
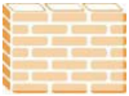
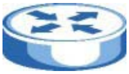
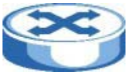
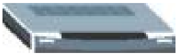
Help us help you. E-mail all User’s Guide-related comments, questions or suggestions for improvement to techwriters@zyxel.com.tw or send regular mail to The Technical Writing Team, ZyXEL Communications Corp., 6 Innovation Road II, Science-Based Industrial Park, Hsinchu, 300, Taiwan. Thank you.

Syntax Conventions

- The version number on the title page is the latest firmware version that is documented in this User’s Guide. Earlier versions may also be included.
- “Enter” means for you to type one or more characters and press the carriage return. “Select” or “Choose” means for you to use one of the predefined choices.

- Mouse action sequences are denoted using a comma. For example, “In Windows, click **Start**, **Settings** and then **Control Panel**” means first click the **Start** button, then point your mouse pointer to **Settings** and then click **Control Panel**.
- “e.g.” is a shorthand for “for instance”, and “i.e,” means “that is” or “in other words”.

Graphics Icons Key

 Vantage RADIUS	 Computer	 Notebook Computer
 Server	 Wireless Access Point	 Wireless Signal
 Internet	 Firewall	 Router
 Switch	 Modem	

Part I:

Getting Started

This part helps you get to know your Vantage RADIUS, introduces the web configurator and how to configure for first use.

Chapter 1
Getting to Know Your Vantage RADIUS

This chapter introduces the main features and applications of Vantage RADIUS.

1.1 Introducing Vantage RADIUS

Vantage RADIUS (Remote Authentication Dial-In User Service) 50 (referred to in this guide as Vantage RADIUS) is a standalone RADIUS server. Vantage RADIUS maintains a list of accounts that are allowed to access a wireless network that supports IEEE 802.1x authentication.

It provides a single point of authentication that is particularly useful when applied to wireless networks where a mobile device could potentially access many servers.

Vantage RADIUS can be set up as a local or remote server. Multiple Vantage RADIUS devices can be set up as remote servers with different user accounts for decentralization and network flexibility.

The device's web configurator allows easy management and configuration.

1.2 Features

1.2.1 Physical

Auto-negotiating 10/100 Mbps Ethernet LAN

The LAN port automatically detects if there is a 10 or 100 Mbps Ethernet connection.

Auto-sensing 10/100 Mbps Ethernet LAN

The LAN port automatically adjusts to either a crossover or straight-through Ethernet cable.

Time and Date

Vantage RADIUS allows you to get the current time and date from an external server when switched on. You can also set the time manually.

Reset Button

The reset button is built into the front panel. Use this button to restore Vantage RADIUS to factory defaults.

1.2.2 Firmware

All-in-one Box

Vantage RADIUS consists of a private certificate authority, Remote Authentication Dial-In User Service Server, user account database and user's connection records. It provides a secure WLAN with one "BOX" and Access Point.

User Authentication and Accounting

Vantage RADIUS supports triple-A (Authentication, Authorization, Accounting) network management.

- Authentication

Clients that require access to the wireless network must first be authenticated before they can be authorized. Vantage RADIUS identifies valid clients using certificates and shared keys.

Each new connection is monitored and information is sent to the wireless client, such as what IP address to use, session time-limit information, or which type of tunnel to set up

- Authorization

Validate any WLAN client's username and password to ensure that only individuals with valid accounts will be granted network access.

- Accounting

Vantage RADIUS logs all authentication transactions, so you can to view the entire history of authentication requests and responses. If the wireless networked device supports RADIUS accounting, you can also track connection time and even which user is connected.

Accounting data can easily be exported to spreadsheets, databases, and specialized billing software.

Dynamic DNS Support

With Dynamic DNS (Domain Name System) support, you can have a static hostname alias for a dynamic IP address, allowing the host to be more easily accessible from various locations on the Internet. You must register for this service with a Dynamic DNS service provider.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) allows the individual client computers to obtain the TCP/IP configuration at start-up from a centralized DHCP server. Vantage RADIUS has built-in DHCP server capability (disabled by default) which means it can assign IP addresses, an IP default gateway and DNS servers to all systems that support the DHCP client.

Security

Secure WLAN connections against wireless eavesdropping and other attacks with the supported IEEE 802.1x security standard, including the WLAN security protocols EAP-MD5 and PEAP

SNMP Support

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Vantage RADIUS supports SNMP agent functionality, which allows a remote station to maintain and monitor Vantage RADIUS over the network.

Certificates

Vantage RADIUS provides a private Certificate Authority (CA), which can be used to create a server certificate (also called digital IDs). Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication. The certificates are self-signed so there is no need to purchase them from commercial certificate providers.

Remote Access

The administrator can access Vantage RADIUS by using web browsers such as Netscape Navigator or Microsoft Internet Explorer. This system allows a remote user to view or modify system configuration via Internet.

SSH

Vantage RADIUS uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure web configurator access to Vantage RADIUS.

Wireless Accounts

Manage up to 50 connections at the same time from a possible 200 accounts.

User Trace Record

Trace client records such as login time, logout time and access point information. Export the records via a syslog or e-mail server.

System and RADIUS Logs

Vantage RADIUS provides real-time system logs and RADIUS logs to perform real time transactions of the RADIUS server such as administrator login, the RADIUS server authenticate request, the RADIUS accounting request, authenticate reply and accounting reply. The last seven days log files are kept in Vantage RADIUS, export them with TFTP or e-mail servers. Refer to *section 4.1* for details about file-size restrictions.

1.3 Application

Below are examples of what you can do with your Vantage RADIUS.

1.3.1 Wireless Network Authentication

Wireless clients connect to the WLAN in the same way you would access an authenticated wireless Access Point (AP). The wireless AP provides authentication for user accounts via Vantage RADIUS, which is invisible to the individual clients.

Client usernames and passwords are forwarded from a wireless network to Vantage RADIUS, which then validates them against its own list. This ensures that only individuals with valid accounts will be granted network access.

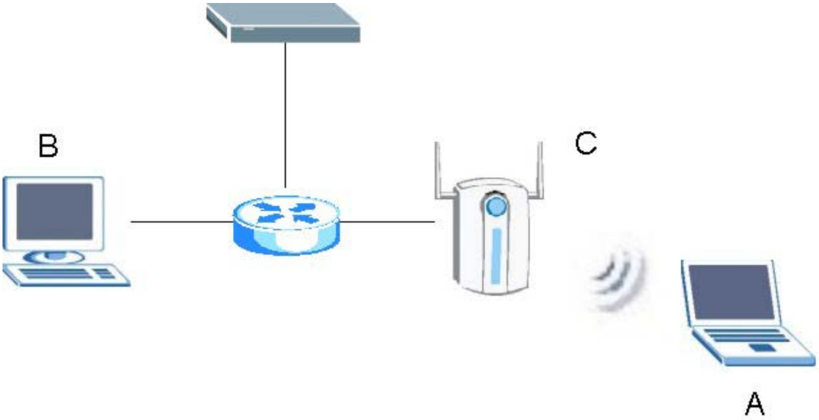


Figure 1-1 Secure Wireless Connection

The following gives an overview of Vantage RADIUS' role in a network.

- Wireless station **A** attempts to communicate with **B** over the wireless network via **C**.
- **C** sends a "request identity" message to **A** for authentication.
- **A** replies with identity information, including username and password.
- **C** communicates with Vantage RADIUS, which checks the user information against its list of valid accounts and determines whether or not to authenticate **A**.
- **A** is authenticated and can communicate with **B** over the wireless network.

1.3.2 Remote RADIUS Authentication

Vantage RADIUS can forward authentication for user accounts to other remote or proxy RADIUS servers behind the local Vantage RADIUS. With remote RADIUS servers, wireless client authentication can be easily managed and more wireless clients can be authenticated. These remote RADIUS servers can be other Vantage RADIUS' or a RADIUS server computer (for example, Windows 2003 IAS).

Client usernames and passwords are forwarded from a wireless network to either the local or remote RADIUS server, which then validates them against its own list. This ensures that only individuals with valid accounts will be granted network access.

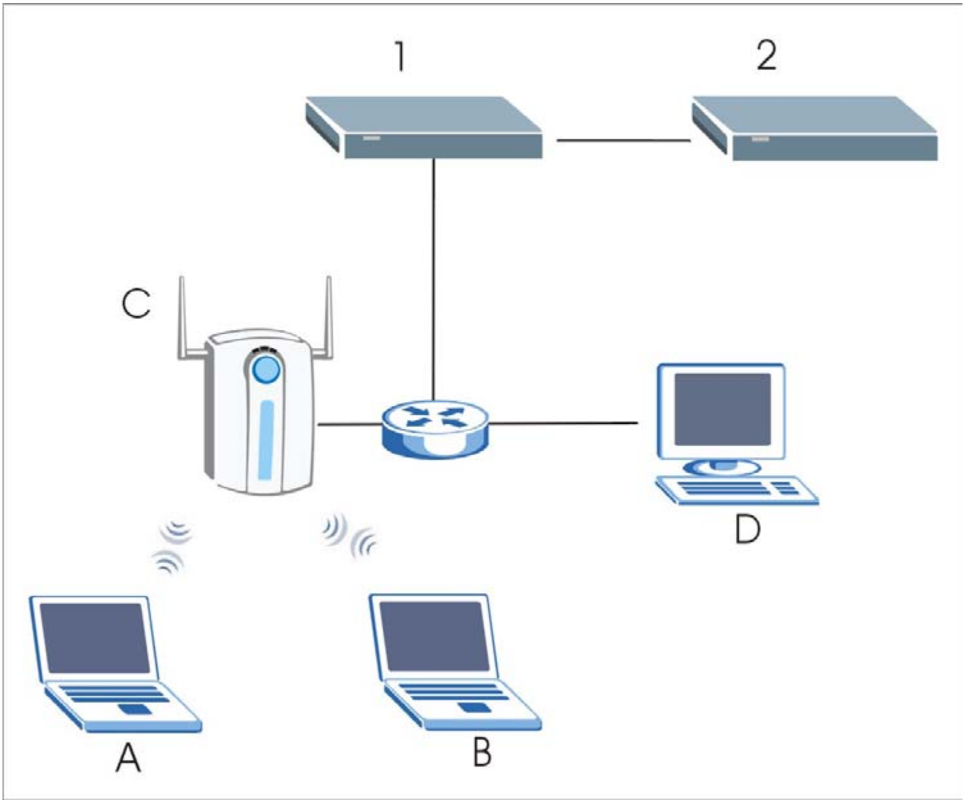


Figure 1-2 Remote RADIUS Authentication

The following gives an overview of how remote RADIUS authentication operates in a network.

- Wireless station **A** attempts to communicate with **D** over the wireless network via **C**.
- **C** sends a "request identity" message to **A** for authentication.
- **A** replies with identity information, including username and password.
- **C** communicates with Vantage RADIUS (local RADIUS server **1**), which checks if the realm of **A** belongs to a local user account or a remote user account. If **A** has a local user account then

Vantage RADIUS checks the password and username against its list of valid accounts and determines whether or not to authenticate **A**. If **A** has a remote user account, Vantage RADIUS forwards the authentication to a remote RADIUS server **2**.The remote RADIUS server checks the password and username against its list of valid accounts and determines whether or not to authenticate **A**.

- **A** is authenticated and can communicate with **D** over the wireless network.
- Wireless client **B** is authenticated by either the local or remote RADIUS server depending on whether **B** has a user account on the local RADIUS or remote RADIUS.

Chapter 2
Introducing the Web Configurator

This chapter describes how to access the web configurator, reset your Vantage RADIUS and navigate the menu system.

2.1 Web Configurator Overview

The web configurator is an HTML-based management interface that allows easy Vantage RADIUS setup and management via Internet browser. Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

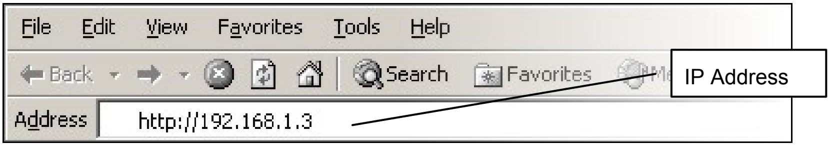
In order to use the web configurator you need to allow:

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

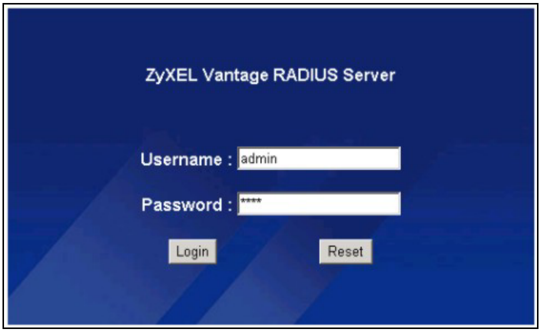
See the *Troubleshooting* appendix if you want to make sure these functions are allowed in Internet Explorer or Netscape Navigator.

The following steps describe how to perform initial configuration.

Step 1. Launch your web browser. Enter the device's management IP address (default 192.168.1.3).



Step 2. Type the default **Username** (admin) and **Password** (1234) and click **Login**.



ZyXEL Vantage RADIUS Server

Username : admin

Password : ****

Figure 2-1 Admin Account

Step 3. You should now see the web configurator **MAIN MENU** screen.

- Click the **HELP** icon (located in the top right corner of most screens) to view online help.
- Click a link under **ADVANCED** to configure device features.
- Click a link under **RADIUS** to enter user accounts for authentication and configure for use with your wireless access point.
- Click a link under **MAINTENANCE** to see system status, user information, upload firmware and back up, or restore or upload a configuration file.
- Click a link under **MANAGEMENT** to set up your Vantage RADIUS for remote access and monitoring connections.
- Click **LOGOUT** in the navigation panel when you have finished managing your device. The device automatically logs you out if it is left idle for five minutes. If this occurs, refresh your browser to display the **Login** screen again and then log back in.

Follow the instructions you see in the MAIN MENU screen or click the HELP ⓘ icon (located in the top right corner of most screens) to view online help.

2.2 Resetting Vantage RADIUS

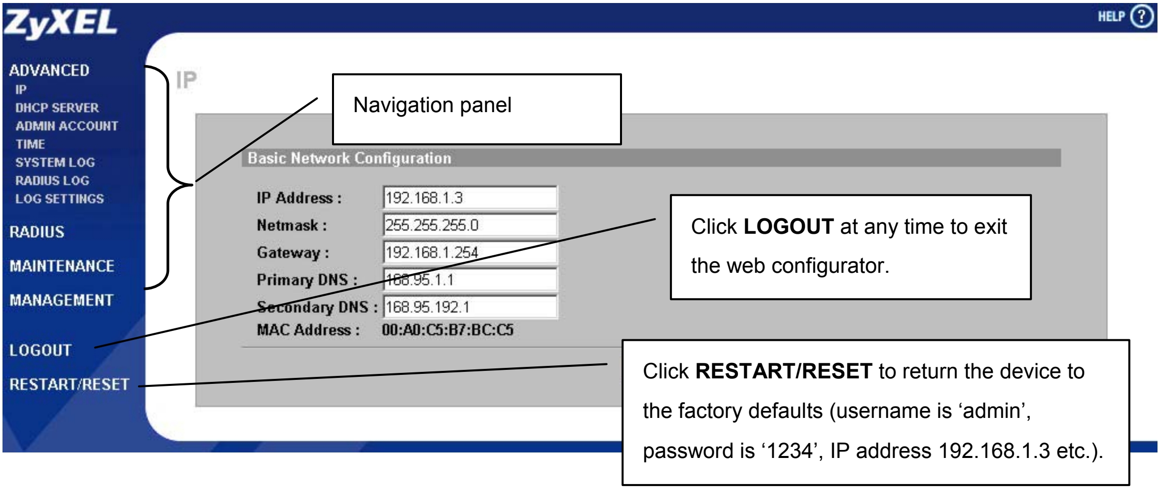
If you forget your password or cannot access the web configurator, you will need to use the **RESET** button on the front panel of Vantage RADIUS to reload the factory-default configuration file. This means that you will lose all configurations that you had previously and the password will be reset to "1234".

2.2.1 Using the Reset Button

Make sure the **PWR** LED is on (not blinking) before you begin. Press the **RESET** button for five seconds or until the **SYS** LED begins to blink and then release it. When the **SYS** LED begins to blink, the defaults have been restored and Vantage RADIUS restarts.

2.3 Navigating the Web Configurator

The following summarizes how to navigate the web configurator from the **MAIN MENU** screen.



Basic Network Configuration

IP Address : 192.168.1.3
Netmask : 255.255.255.0
Gateway : 192.168.1.254
Primary DNS : 168.95.1.1
Secondary DNS : 168.95.192.1
MAC Address : 00:A0:C5:B7:BC:C5

Navigation panel

Click **LOGOUT** at any time to exit the web configurator.

Click **RESTART/RESET** to return the device to the factory defaults (username is 'admin', password is '1234', IP address 192.168.1.3 etc.).

Figure 2-2 Admin Account MAIN MENU Screen of the Web Configurator

2.3.1 Navigation Panel

After you enter the password, use the sub-menus on the navigation panel to configure Vantage RADIUS features.

The following table describes the sub-menus.

Table 2-1 Web Configurator Screens Summary

LINK	TAB	FUNCTION
ADVANCED	IP	Use this screen to configure basic network configuration on Vantage RADIUS.
	DHCP SERVER	Use this screen to configure the DHCP Server.. Select the **DHCP Client List** tab to display a list of all network clients using the DHCP server
	ADMIN ACCOUNT	Use this screen to change your system password and username.
	TIME	Use this screen to change the time and date of your Vantage RADIUS.
	SYSTEM LOG	Use these screens to monitor system-related events and download log files.
	RADIUS LOG	Use these screens to monitor RADIUS-related events and download log files
	LOG SETTINGS	Use this screen to configure the syslog, TFTP and Mail servers to specify when and where log files are generated and sent.
RADIUS	ROOT CA	Use this screen to configure and download a certificate used to authenticate wireless clients.
	SERVER CERTIFICATE	Use this screen to configure the server certificate used with the TLS security protocol.
	RADIUS SERVER	Use this screen to configure Vantage RADIUS Active Directory, Remote RADIUS servers or authentication and accounting server ports and the IP addresses or networks that can use them.
	USER ACCOUNT	Use this screen to configure accounts for wireless clients requiring authorization.
MAINTENANCE	SYSTEM STATUS	This screen contains administrative and system-related information.
	F/W UPLOAD	Use this screen to upload firmware to your Vantage RADIUS.

Table 2-1 Web Configurator Screens Summary

LINK	TAB	FUNCTION
	CONFIGURATION	Use this screen to backup and restore the configuration or reset the factory defaults to your Vantage RADIUS.
MANAGEMENT	REMOTE ACCESS	Use this screen to configure which IP address(es) can access Vantage RADIUS.
	SNMP AGENT	Use this screen to configure which IP address(es) can access Vantage RADIUS using SNMP and the access level.
	USER TRACE	Use these screens to monitor client access and generate log files.
LOGOUT		Click this label to exit the web configurator.
RESTART/RESET		You only need to use this button if you’ve forgotten the device’s password. It returns the device to the factory defaults (username is ‘admin’, password is ‘1234’, IP address 192.168.1.3 etc.).

Chapter 3 Advanced Settings

This chapter provides information on the advanced settings screens.

3.1 Advanced Settings Overview

The advanced settings screens allow you to configure your Vantage RADIUS for first use, including setting up Internet access for your wireless network, DHCP server settings, managing web configurator access, time server settings and configuring the types of log services available.

3.2 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.

The Internet Assigned Number Authority (IANA) reserves blocks of addresses specifically for private use; please do not use any other numbers unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 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, 192.168.1.3, for your Vantage RADIUS, 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. This field must be configured manually; the default setting is 255.255.255.0. Unless you are implementing sub-netting, there is no need to change this field.

3.3 DNS Server Address Assignment

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for instance, the IP address of www.zyxel.com is 204.217.0.2. The DNS server is extremely important because without it, you must know the IP address of a computer before you can access it.

Your ISP should have given you the DNS server addresses, usually in the form of an information sheet, when you sign up.

If you are using a ZyXEL gateway/router, you can use it’s DNS proxy feature by entering the LAN IP address of the gateway/router in the DNS field.

3.4 MAC Address

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.

Table 3-1 Example of Network Properties for LAN Servers with Fixed IP Addresses

Choose an IP address	192.168.1.2-192.168.1.32; 192.168.1.65-192.168.1.254.
Subnet mask	255.255.255.0
Gateway (or default route)	192.168.1.1

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

3.6 IP Pool Setup

The IP pool specifies the number of consecutive IP addresses to reserve for computers on your network, starting from a specified IP address. Vantage RADIUS supports a pool size of up to 253 IP addresses.

It is recommended that you assign IP addresses starting from the higher end of your subnet address. For example, 192.168.1.33 with a pool size of 32 reserves 192.168.33 to 192.168.1.64. This leaves 31 IP addresses (excluding Vantage RADIUS) in the lower range for other server computers, for instance, servers for mail, FTP, TFTP, web, etc., that you may have.

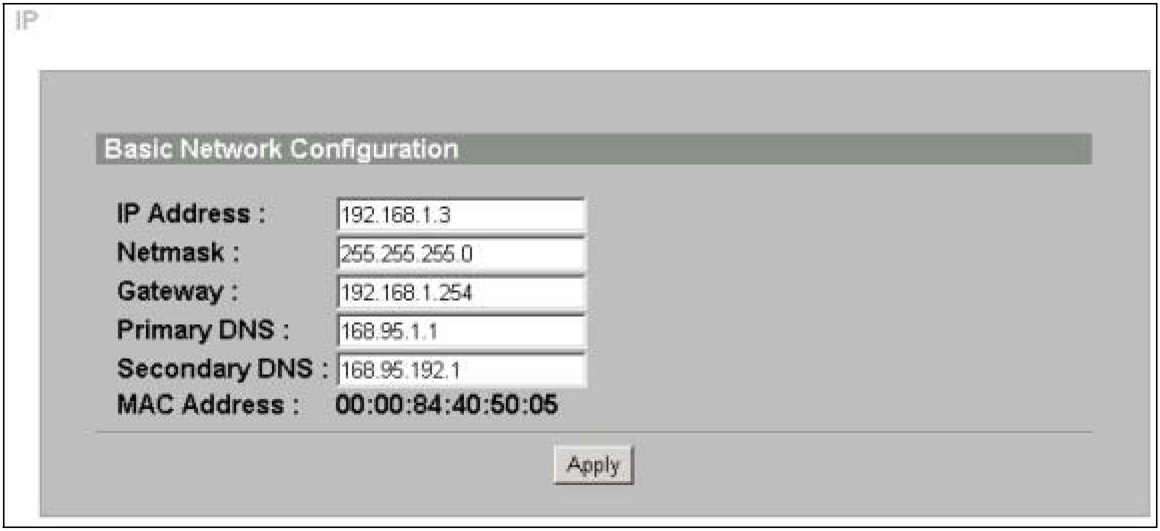
3.7 Domain Name

The **Domain Name** entry is what is propagated to the DHCP clients on the wireless network. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from Vantage RADIUS via DHCP. This domain name is for administrators to identify which DHCP server assigned your IP address.

3.8 Basic Network Configuration

Wireless clients need to be in the same subnet as Vantage RADIUS. Clients access the network through Vantage RADIUS. Now configure your Vantage RADIUS to access the gateway or router that provides access to your network. See the *Required Information* section in your *Quick Start Guide* for this information from your ISP or network administrator.

Click **ADVANCED** and then **IP** in the main menu. The following screen displays.



IP

Basic Network Configuration

IP Address : 192.168.1.3

Netmask : 255.255.255.0

Gateway : 192.168.1.254

Primary DNS : 168.95.1.1

Secondary DNS : 168.95.192.1

MAC Address : 00:00:84:40:50:05

Figure 3-1 IP Configuration

The following table describes the labels in this screen.

Table 3-2 IP Configuration

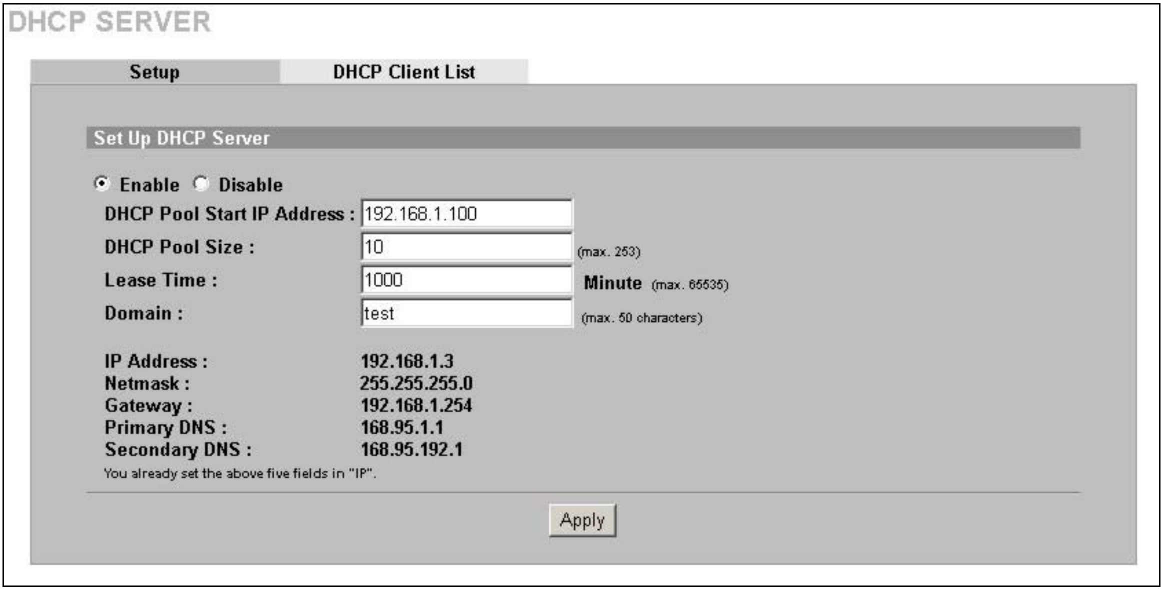
LABEL	DESCRIPTION
Basic Network Configuration	
IP Address	Type an IP address in dotted decimal notation.
Netmask	Type the IP subnet mask of the RADIUS server (if your ISP gave you one) in this field.
Gateway	Type the IP address of the gateway device used to connect your RADIUS to the Internet.
Primary DNS	DNS (Domain Name System) is for mapping 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 machine before you can access it. The RADIUS uses a system DNS server (in the order you specify here) to resolve domain names. Type an IP address in dotted decimal notation if given to you by your ISP.
Secondary DNS	Type a backup DNS Server IP address in dotted decimal notation if given to you by your ISP.

Table 3-2 IP Configuration

LABEL	DESCRIPTION
MAC Address	This field displays the physical address of your RADIUS server on the network.
Apply	Click **Apply** to save your changes back to the RADIUS.

3.9 DHCP Server Setup

Vantage RADIUS dynamically assigns IP addresses to clients. Click **ADVANCED** and then **DHCP SERVER** in the main menu to configure your Vantage RADIUS as a DHCP server.



DHCP SERVER

Set Up DHCP Server

● Enable ○ Disable

DHCP Pool Start IP Address : 192.168.1.100

DHCP Pool Size : 10 (max. 253)

Lease Time : 1000 Minute (max. 65535)

Domain : test (max. 50 characters)

IP Address : 192.168.1.3

Netmask : 255.255.255.0

Gateway : 192.168.1.254

Primary DNS : 168.95.1.1

Secondary DNS : 168.95.192.1

You already set the above five fields in "IP".

Figure 3-2 DHCP Server: Setup

The following table describes the labels in this screen.

Table 3-3 DHCP Server: Setup

LABEL	DESCRIPTION
Set Up DHCP Server	
Enable/Disable	DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) allows individual clients (workstations) to obtain TCP/IP configuration at startup from a server. Disable this field to stop the RADIUS acting as a DHCP server. When configured as a server, the RADIUS provides TCP/IP configuration for the clients. If not, DHCP service is disabled and you must have another DHCP server on your LAN, or else the client computer must be manually configured. When set as a server, fill in the following four fields.
DHCP Pool Start IP Address	This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.100.
DHCP Pool Size	This field specifies the size, or count, of the IP address pool. The default is 10.
Lease Time	Type a time between 1 and 65535 minutes.
Domain	This field identifies your Vantage RADIUS DHCP server on the network and informs administrators which DHCP server you are using.
The following fields are taken from the IP screen and are not configurable. See *Figure 3-1* for details on how to configure these fields.	
Network Address	This field displays the **IP Address** field of the **IP** screen (see *Figure 3-1*)
Netmask	The subnet mask specifies the network number portion of an IP address. Unless you are implementing subnetting, use the default subnet mask 255.255.255.0.
Gateway	This field displays the IP address of the gateway used to connect your RADIUS to the Internet.
Primary DNS	This displays the IP Address of the DNS Server used for resolving host names.
Secondary DNS	This is the backup DNS Server.
Apply	Click **Apply** to save your changes back to the RADIUS.

3.10 DHCP Client List

Click **ADVANCED** in the main menu and then **DHCP SERVER**. Now click the **DHCP Client List** tab. The read-only information here relates to your DHCP status. The **DHCP Client List** shows current DHCP client information (including **IP Address** and **MAC Address**) of all network clients using the DHCP server.

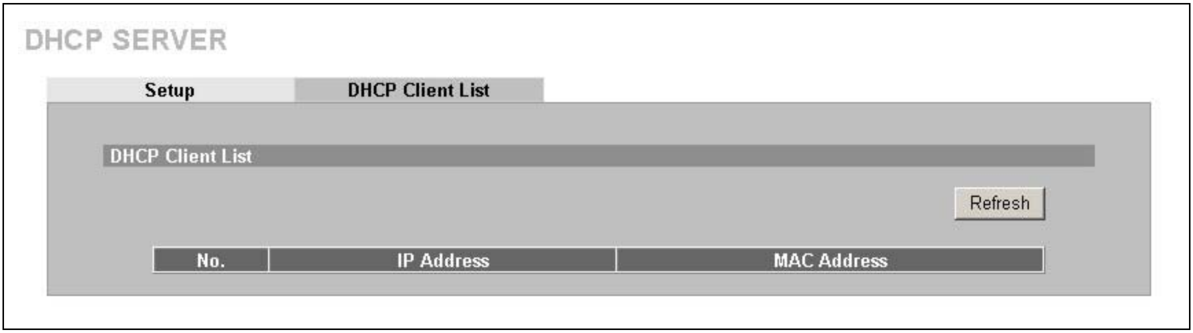


Figure 3-3 DHCP Server: Client List

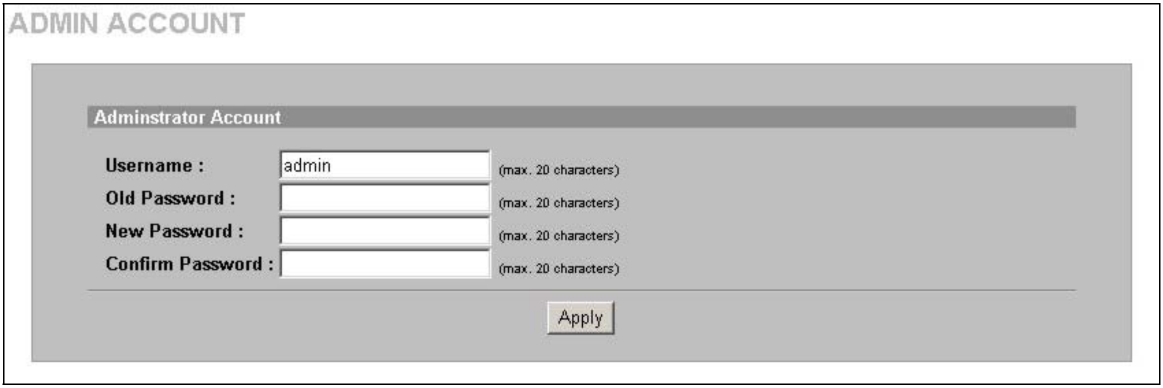
The following table describes the labels in this screen.

Table 3-4 DHCP Server: Client List

LABEL	DESCRIPTION
DHCP Client List	
Refresh	Click this button to update the **DHCP Client List**.
No.	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the **No** field listed above.
MAC Address	This field shows the MAC address of the computer with the IP address in the **IP Address** field. 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.

3.11 Administrator's Account

To change your RADIUS system password (recommended) click **ADVANCED** and then **ADMIN ACCOUNT** from the main menu. This screen allows you to change the administrator account name and password.


ADMIN ACCOUNT

Adminstrator Account

Username :	admin	(max. 20 characters)
Old Password :		(max. 20 characters)
New Password :		(max. 20 characters)
Confirm Password :		(max. 20 characters)

Figure 3-4 Administrator Account

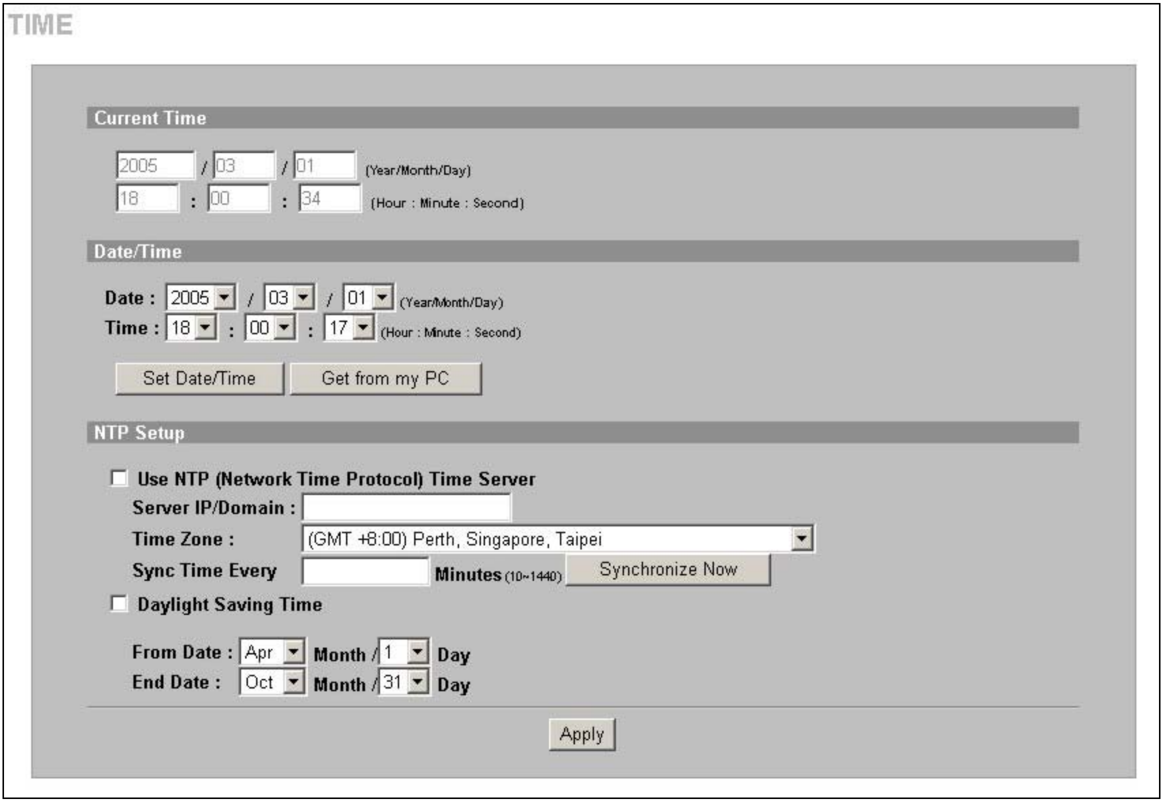
The following table describes the labels in this screen.

Table 3-5 Administrator Account

LABEL	DESCRIPTION
Administrator Account	
Username	Type up to 20 alphanumeric characters to associate a name with administrator access to the RADIUS.
Password	Type the default password or the existing password you use to access the system in this field.
New Password	Type the new password in this field.
Confirm Password	Type the new password again in this field.
Apply	Click **Apply** to save your changes back to the RADIUS.

3.12 Time Settings

Vantage RADIUS uses a system clock to synchronize time across the network and generates accurate log files. Time can be obtained from the connecting computer, or an NTP (Network Time Protocol) Server. To change your time settings, click **ADVANCED** in the main menu, and then click **TIME**.



TIME

Current Time

2005 / 03 / 01 (Year/Month/Day)
18 : 00 : 34 (Hour : Minute : Second)

Date/Time

Date : 2005 / 03 / 01 (Year/Month/Day)
Time : 18 : 00 : 17 (Hour : Minute : Second)

NTP Setup

□ Use NTP (Network Time Protocol) Time Server
Server IP/Domain :
Time Zone : (GMT +8:00) Perth, Singapore, Taipei
Sync Time Every Minutes (10~1440)

□ Daylight Saving Time
From Date : Apr Month / 1 Day
End Date : Oct Month / 31 Day

Figure 3-5 Time Settings

The following table describes the labels in this screen.

Table 3-6 Time Settings

LABEL	DESCRIPTION
Current Time	
Year/Month/Day	This field displays the date of your RADIUS. Each time you reload this page, the RADIUS synchronizes the time with the time server.
Hour: Minute: Second	This field displays the time of your RADIUS. Each time you reload this page, the RADIUS synchronizes the time with the time server.
Date/Time	
Date	This field displays the last updated date from the time server if you have one configured; otherwise use the drop down list boxes to manually set a date here.
Time	This field displays the last updated time from the time server if you have one configured; otherwise use the drop down list boxes to manually set a time here.
Set Date/Time	Click this button to apply the manual date and time configured to the RADIUS device.
Get from my PC	Click this button to have the RADIUS obtain the current time and date from your computer.
NTP Setup	
Use NTP (Network Time Protocol) Time Server	Enable the network time server to have the RADIUS automatically synchronize the current rime and date with a time server.
Server IP/Domain Name	Type the address of your time server. Check with your ISP/network administrator if you are unsure of this information.
Time Zone	Choose the time setting of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Sync Time Every	Type the time in minutes from 10 to 1440 to have the RADIUS synchronize the time with the time server.
Synchronize Now	Click this button to get the time and date from the time server you specified above. If there is no response from the time server, Vantage RADIUS attempts three times to connect. If there is no response within approximately ten seconds, check your time server settings and try again, or click **Get from my PC** to obtain the current time from your computer without the time server.

Table 3-6 Time Settings

LABEL	DESCRIPTION
Daylight Saving Time	Select this option if you use daylight savings time. Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening.
From Date	Enter the month and day that your daylight-savings time starts on if you selected **Daylight Saving Time**.
End Date	Enter the month and day that your daylight-savings time ends on if you selected **Daylight Saving Time**.
Apply	Click **Apply** to save your changes back to the RADIUS.

Chapter 4
System Logs

This chapter details the various logs generated by Vantage RADIUS and their role in your network.

4.1 Logs Overview

Vantage RADIUS generates log files that can be sent via e-mail or to a syslog server (see *section 4.3*) for troubleshooting, maintenance, monitoring clients’ activities, statistics and collecting information about internal events and network traffic that are otherwise hidden from view.

Vantage RADIUS generates three different types of logs:

- System Logs record internal events (see *Section 4.4*)
- RADIUS Logs records communication between the wireless AP and Vantage RADIUS (see *section 4.5*). Refer to your wireless AP *User’s Guide* for details of log messages.
- User Trace records client interaction with Vantage RADIUS (*see section 4.6*).

The table below describes the maximum file size for each log before a new file is created. It also shows the maximum number of files allowed before the first file generated is overwritten.

Table 4-1 Logs Table

LOG NAME	MAX FILE SIZE	MAX NUMBER. OF FILES	MAX NUMBER OF ENTRIES PER FILE
RADIUS	200K	8	30
System	30K	8	30
User Trace	30K	8	30

4.2 TFTP Server

Trivial File Transfer Protocol (TFTP) is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol). UDP is faster than TCP and more portable. The advantage is very fast transfer times that allows a server to perform real-time logging.

4.3 Syslog server

Syslog servers listen for incoming syslog messages and decodes them for logging purposes. All log files are sent to a syslog server specified in the **Send Every Real-Time Event to Syslog Server** fields in the **Log Settings** screen, see *section 4.13*.

Vantage RADIUS allows you to choose seven different locations to save your log files on the syslog server. This is useful if there is more than one Vantage RADIUS on your network. For more details please refer to your syslog program documentation.

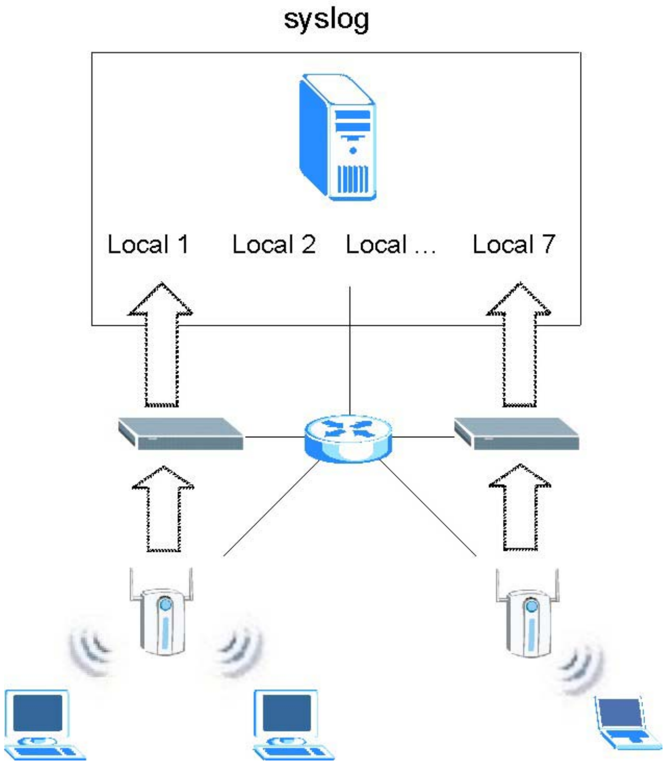


Figure 4-1 Syslog Application

To avoid confusion about which log came from which Vantage RADIUS, you should configure each Vantage RADIUS on the network to send its log files to different log stores inside the syslog server.

4.4 System Log Messages

There are nine cases when a system log message is generated. The table below outlines the messages logged by Vantage RADIUS and the meaning of the log.

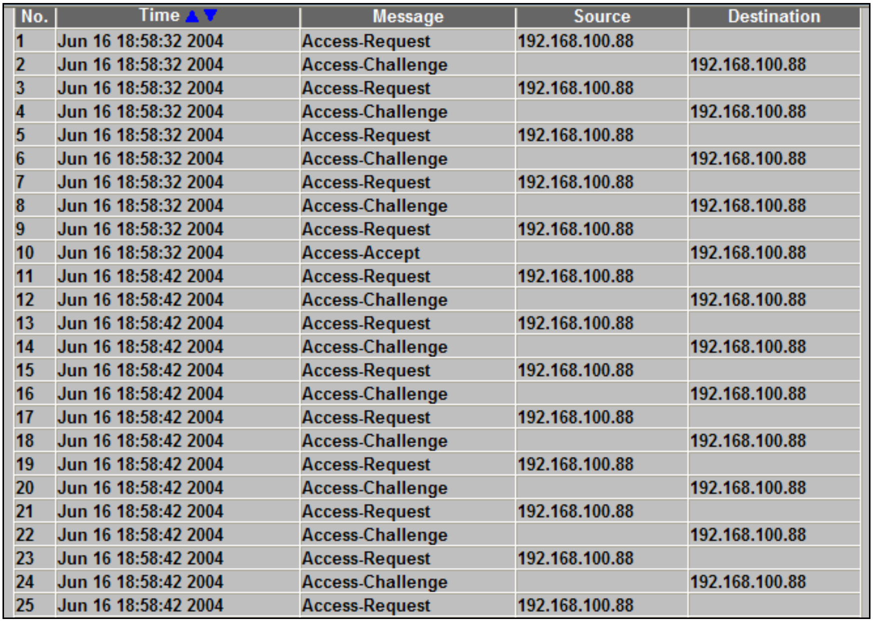
Table 4-2 System Logs

MESSAGE	MEANING
Admin login Http OK/Fail : user = admin source IP	Someone has logged in to the web configurator using the administrator account via an HTTP connection.
Admin login https OK/Fail : user = admin source IP	Someone has logged in to the web configurator using the administrator account via a telnet connection over a secured (HTTPS) connection.
Admin login Telnet OK/Fail : user = admin source IP	Someone has logged in the command interface using the administrator account via a telnet connection.
Admin login SSH OK/Fail : user = admin source IP	Someone has logged in the command interface using the administrator account via a secured shell connection.
Admin login Serial OK/Fail : user = admin source =console	Someone has logged to the command interface using the administrator account via the console.
NTP Time synchronize destination IP	An NTP server address was entered into the NTP **Server IP/Domain** field on the **TIME** settings screen, see *section 3.12*.
NTP Time synchronize OK/Fail destination IP	Vantage RADIUS has synchronized its time settings with the NTP server.
TFTP System/Radius/User Trace log destination IP	This message is generated every time a log file is sent to the TFTP server.
Mail System/Radius/User Trace log destination IP	This message is generated every time a log file is sent via e-mail.

4.5 RADIUS Log Messages

Packets sent to Vantage RADIUS from a wireless AP generate RADIUS log messages. For details of specific log messages sent by your wireless AP, please refer to your wireless AP’s *user’s guide*.

Typical log messages sent between Vantage RADIUS and a wireless AP are shown below.



No.	Time ▲▼	Message	Source	Destination
1	Jun 16 18:58:32 2004	Access-Request	192.168.100.88	
2	Jun 16 18:58:32 2004	Access-Challenge		192.168.100.88
3	Jun 16 18:58:32 2004	Access-Request	192.168.100.88	
4	Jun 16 18:58:32 2004	Access-Challenge		192.168.100.88
5	Jun 16 18:58:32 2004	Access-Request	192.168.100.88	
6	Jun 16 18:58:32 2004	Access-Challenge		192.168.100.88
7	Jun 16 18:58:32 2004	Access-Request	192.168.100.88	
8	Jun 16 18:58:32 2004	Access-Challenge		192.168.100.88
9	Jun 16 18:58:32 2004	Access-Request	192.168.100.88	
10	Jun 16 18:58:32 2004	Access-Accept		192.168.100.88
11	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
12	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
13	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
14	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
15	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
16	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
17	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
18	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
19	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
20	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
21	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
22	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
23	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	
24	Jun 16 18:58:42 2004	Access-Challenge		192.168.100.88
25	Jun 16 18:58:42 2004	Access-Request	192.168.100.88	

Figure 4-2 Example Of RADIUS Log Messages

4.5.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the access point and Vantage RADIUS for user authentication:

- **Access-Request**

  Sent by an access point, requesting authentication.

- **Access-Reject**

  Sent by Vantage RADIUS rejecting access.

- **Access-Accept**

  Sent by Vantage RADIUS allowing access.

- **Access-Challenge**

  Sent by Vantage RADIUS 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 Vantage RADIUS for user accounting:

- **Accounting-Request**

  Sent by the access point requesting accounting.

- **Accounting-Response**

  Sent by Vantage RADIUS to indicate that it has started or stopped accounting.

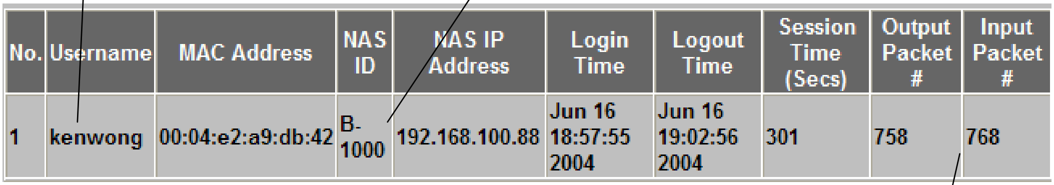
4.6 User Trace Records

Every time a wireless client is authenticated, the details of the connection are recorded in the **User Trace Records** table. Vantage RADIUS tracks recent event logs, including username, MAC address, client IP address, access point IP address, login time, logout time and other information.

The following figure shows an example of a typical user trace record.

This field displays the account name of the wireless client connected to the network.

This field displays the name of the wireless AP used by the wireless client to connect to the network.



No.	Username	MAC Address	NAS ID	NAS IP Address	Login Time	Logout Time	Session Time (Secs)	Output Packet #	Input Packet #
1	kenwong	00:04:e2:a9:db:42	B-1000	192.168.100.88	Jun 16 18:57:55 2004	Jun 16 19:02:56 2004	301	758	768

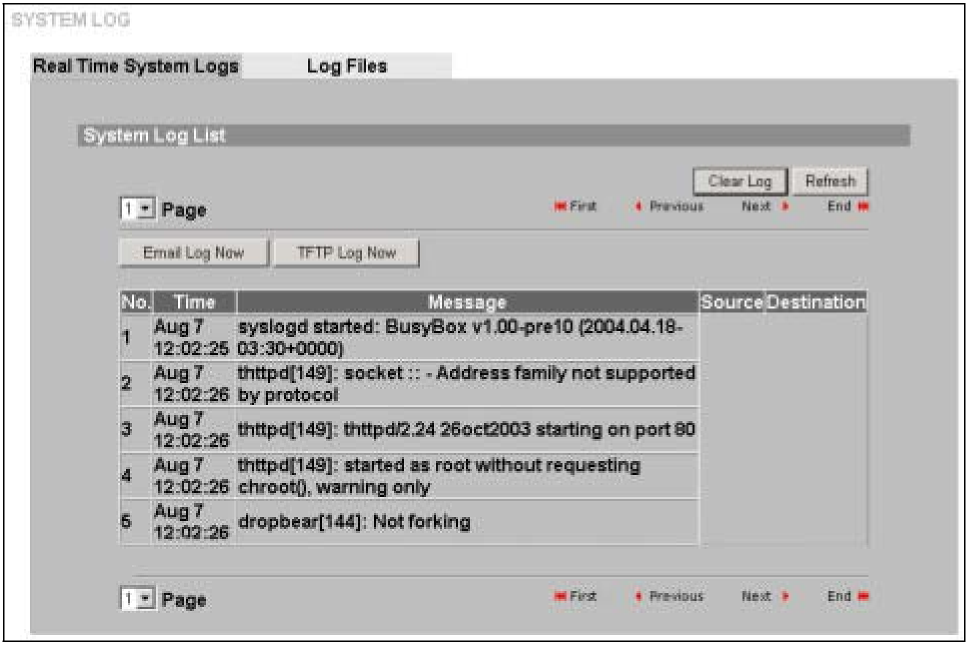
These fields refer to the total number of packets transmitted (**Output Packet**) and received (**Input Packet**) by the wireless client. This number is based on the accounting request sent by AP. See your wireless AP’s *User’s Guide* for how to set up accounting.

Figure 4-3 Example of User Trace Records

For a full description of the fields in the above example, see *section 4.11*.

4.7 Real Time System Logs

System Logs record real-time event messages inside your Vantage RADIUS. The following screens allow you to send the events to an e-mail address or TFTP server for monitoring and troubleshooting (see *section 4.4* for details of system log messages). To view logs of system events, click **ADVANCED** in the main menu, then click **SYSTEM LOG**.



No.	Time	Message	Source	Destination
1	Aug 7 12:02:25	syslogd started: BusyBox v1.00-pre10 (2004.04.18-03:30+0000)		
2	Aug 7 12:02:26	thttpd[149]: socket :: - Address family not supported by protocol		
3	Aug 7 12:02:26	thttpd[149]: thttpd/2.24 26oct2003 starting on port 80		
4	Aug 7 12:02:26	thttpd[149]: started as root without requesting chroot(), warning only		
5	Aug 7 12:02:26	dropbear[144]: Not forking		

Figure 4-4 SYSTEM LOG: Real Time System Logs

The following table describes the labels in this screen.

Table 4-3 SYSTEM LOG: Real Time System Logs

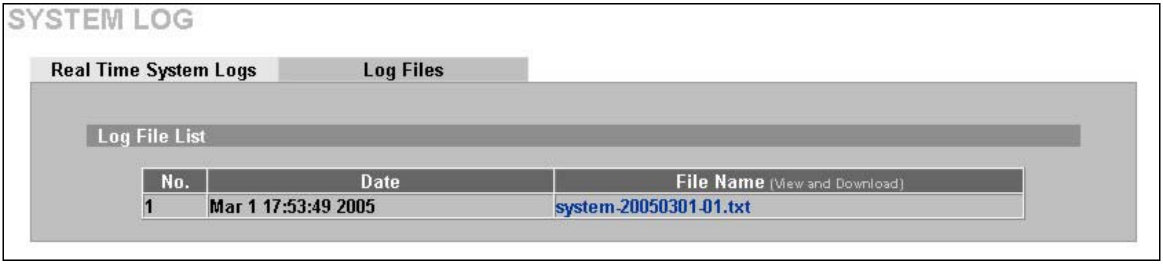
LABEL	DESCRIPTION
System Log List	
Clear Log	Click this button to remove all log entries from the **System Log List**.
Refresh	Click this button to update the **System Log List** with the most recent recordable events.
Email Log Now	Click **Email Log Now** to send logs to the e-mail address specified in the **Log Settings** screen. Make sure that you have first filled in the **Send log file to mail server** fields in **Log Settings** screen, see *section 4.13*.

Table 4-3 SYSTEM LOG: Real Time System Logs

LABEL	DESCRIPTION
TFTP Log Now	Click this button to send the current log to the TFTP server specified in the **Log Settings** screen. Make sure that you have first filled in the **Send Every Real Time Event to Syslog server** fields in the **Log Settings** screen, see *section 4.13*.
No.	This field displays the message index in the order of arrival.
Time	This field displays the time and date the packet was logged.
Message	This field displays the logged packets details, see *section* 4.4 for details of system log messages.
Source	This field displays the IP address where the packet originated.
Destination	This field displays the destination IP address for the incoming packet.

4.8 System Log Files

Recorded system events (see *section 4.4*) are sent to the syslog server (see *section 4.3*) and are available for download on the **Log Files** screen shown below. Click **ADVANCED** in the main menu, then click **SYSTEM LOG**. Now click the **Log Files** tab to display a history of log files generated by system events.



No.	Date	File Name (View and Download)
1	Mar 1 17:53:49 2005	system-20050301-01.txt

Figure 4-5 SYSTEM LOG: Log Files

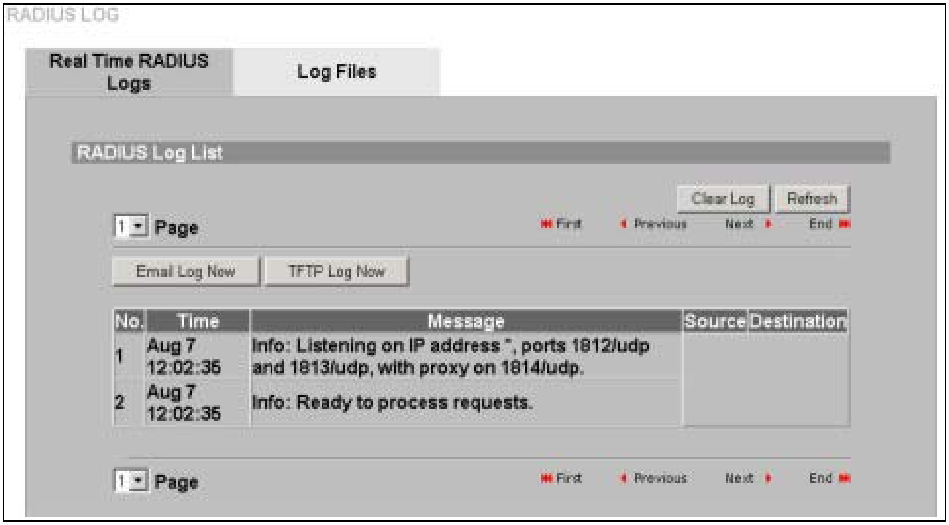
The following table describes the labels in this screen.

Table 4-4 SYSTEM LOG: Log Files

LABEL	DESCRIPTION
Log File List	
No.	This field displays the index of the log file.
Date	This field displays the date and time the last log file was added.
File Name (View and Download)	Click this link to download the .txt log file from the TFTP server. The file is in ASCII format and can be read by any text editor.

4.9 Real Time RADIUS Logs

Click **ADVANCED** in the main menu and then **RADIUS LOG** to view messages passed between your wireless AP and Vantage RADIUS. For details of log messages, please refer to your wireless AP's user-guide.



No.	Time	Message	Source	Destination
1	Aug 7 12:02:36	Info: Listening on IP address *, ports 1812/udp and 1813/udp, with proxy on 1814/udp.		
2	Aug 7 12:02:36	Info: Ready to process requests.		

Figure 4-6 RADIUS LOG: Real Time RADIUS Logs

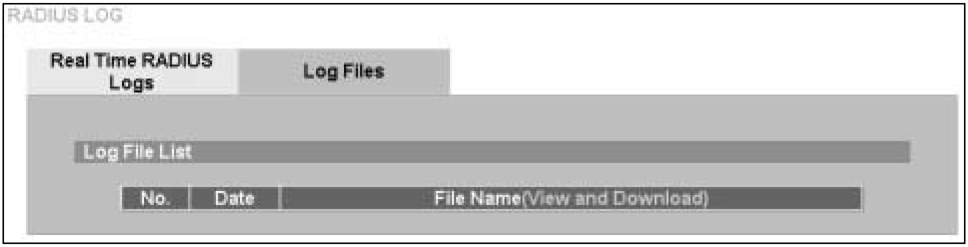
The following table describes the labels in this screen.

Table 4-5 RADIUS LOG: Real Time RADIUS Logs

LABEL	DESCRIPTION
RADIUS Log List	
Clear Log	Click this button to remove all entries
Refresh	Click this button to update the log entries
Email Log Now	Click **Email Log Now** to send logs to the e-mail address specified in the **Log Settings** screen. Make sure that you have first filled in the **Send log file to mail server** fields in **Log Settings** screen, see *section 4.13*.
TFTP Log Now	Click this button to send current logs to the TFTP server specified in the **Log Settings** screen. Make sure that you have first filled in the **Send log file to TFTP server** fields in the **Log Settings** screen, see *section 4.13.*
No.	This field displays the index number in the order of arrival.
Time	This field displays the time and date the log was created.
Message	This field displays the log entry details, see *section* 4.4 for details of system log messages.
Source	This field displays the IP address where the packet originated.
Destination	This field displays the destination IP address for the incoming packet.

4.10 RADIUS Log Files

Click **ADVANCED** in the main menu and then **RADIUS LOG**. Now click **Log Files** to view files containing previous log entries or download in standard ASCII format.



No.	Date	File Name(View and Download)

Figure 4-7 RADIUS LOG: Log Files

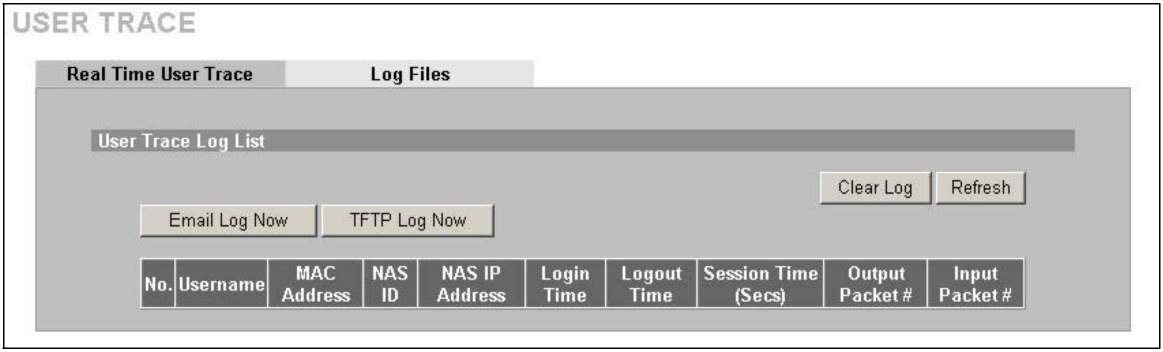
The following table describes the labels in this screen.

Table 4-6 RADIUS LOG: Log Files

LABEL	DESCRIPTION
Log File List	
No.	This field displays the index of the log file.
Date	This field displays the date and time the last log file was added.
File Name (View and Download)	Click this link to download the .txt log file from the TFTP server. The file is in ASCII format and can be read by any text editor.

4.11 User Trace

Vantage RADIUS monitors and records network sessions initiated by wireless clients. These screens display events triggered by a wireless client, so you can see details about the network session including the time of connection and from which AP the connection came from. For a detailed description of user trace records, please refer to *section 4.6.* Click **MANAGEMENT** in the web configurator main menu, and then click **USER TRACE**.



No.	Username	MAC Address	NAS ID	NAS IP Address	Login Time	Logout Time	Session Time (Secs)	Output Packet #	Input Packet #

Figure 4-8 USER TRACE: Real Time User Trace

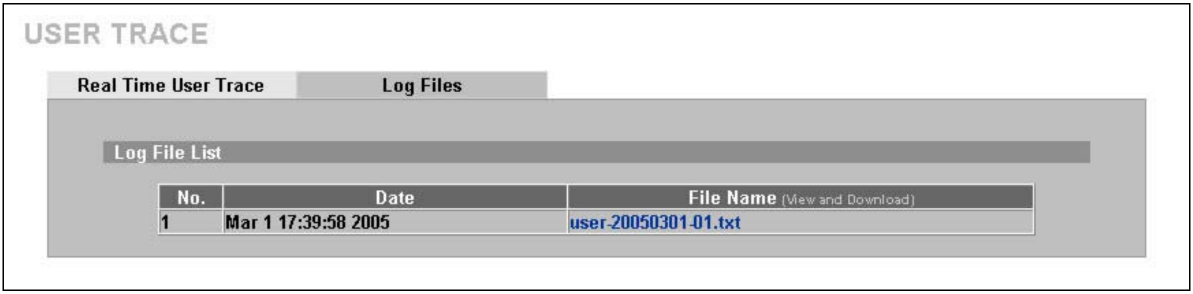
The following table describes the labels in this screen.

Table 4-7 USER TRACE: Real Time User Trace

LABEL	DESCRIPTION
System Log List	
Clear Log	Click this button to remove all entries
Refresh	Click this button to update the log entries
Email Log Now	Click **Email Log Now** to send the logs to the e-mail address specified in the **Log Settings** screen. Make sure that you have first filled in the **Send log file to mail server** fields in **Log Settings** screen, see *section 4.13*.
TFTP Log Now	Click this button to send the current logs to the TFTP server specified in the **Log Settings** screen. Make sure that you have first filled in the **Send log file to TFTP server** fields in the **Log Settings** screen, see *section 4.13*.
No.	This field displays the message index in the order of arrival.
Username	This field displays the name of the account authenticated by Vantage RADIUS.
MAC Address	This is the MAC address of the wireless AP used by the wireless client to connect to the network.
NAS ID	Network Access Server (NAS) ID displays the ID of the wireless AP that the wireless client uses to access the network.
NAS IP Address	This field displays the IP address of the wireless AP that the wireless client is uses to access the network.
Login Time	This field displays the time accessed by a wireless client.
Logout Time	This field displays the time the wireless client disconnected.
Session Time (Secs)	This field displays the length of time the client is/was connected.
Output Packet	This field displays the total number of packets sent during a session.
Input Packet	This field displays the total number of packets received during a session.

4.12 User Trace Log Files

Click **MANAGEMENT** in the main menu and then **USER TRACE**. Now click **Log Files** to view files containing previous log entrees or download in standard ASCII format.



No.	Date	File Name (View and Download)
1	Mar 1 17:39:58 2005	user-20050301-01.txt

Figure 4-9 User Trace: Log Files

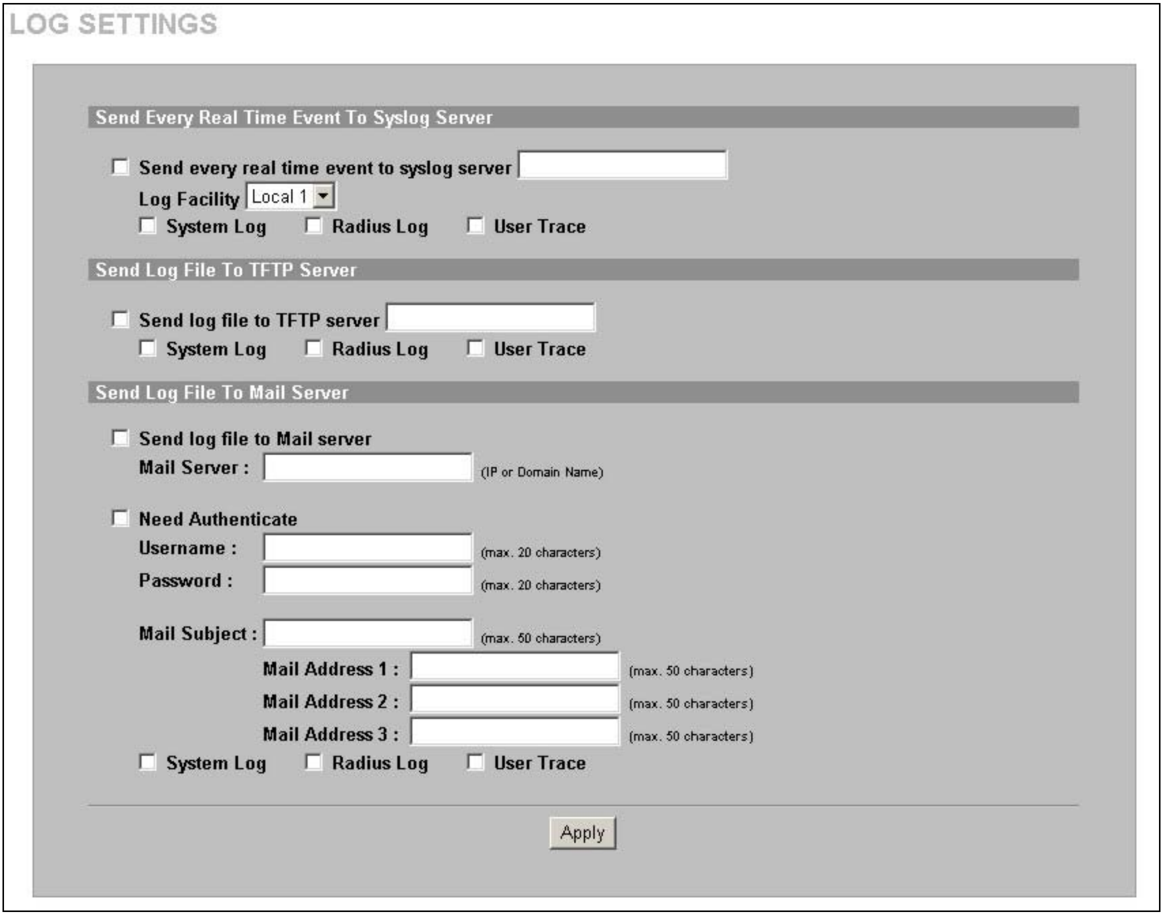
The following table describes the labels in this screen.

Table 4-8 RADIUS Logs: Log Files

LABEL	DESCRIPTION
Log File List	
No.	This field displays the index of the log file.
Date	This field displays the date and time the log file was created. Note that there can only be one log file per day. If a new log file is generated, it appends the old one and changes the time to reflect the time updated.
File Name (View and Download)	Click this link to download the .txt log file from the TFTP server. The file is in ASCII format and can be read by any text editor.

4.13 Log Settings Screen

This screen allows you to specify where you want your log files sent (see *section 4.1*), what types of logs are sent and what time to send them. Click **ADVANCED** in the main menu and then **LOG SETTINGS** to begin configuring your log file settings.



LOG SETTINGS

Send Every Real Time Event To Syslog Server

□ Send every real time event to syslog server

Log Facility Local 1

□ System Log □ Radius Log □ User Trace

Send Log File To TFTP Server

□ Send log file to TFTP server

□ System Log □ Radius Log □ User Trace

Send Log File To Mail Server

□ Send log file to Mail server

Mail Server : (IP or Domain Name)

□ Need Authenticate

Username : (max. 20 characters)

Password : (max. 20 characters)

Mail Subject : (max. 50 characters)

Mail Address 1 : (max. 50 characters)

Mail Address 2 : (max. 50 characters)

Mail Address 3 : (max. 50 characters)

□ System Log □ Radius Log □ User Trace

Figure 4-10 RADIUS Logs: Log Files

The following table describes the labels in this screen.

Table 4-9 RADIUS Logs: Log Files

LABEL	DESCRIPTION
Send every real time event to syslog server	

Table 4-9 RADIUS Logs: Log Files

LABEL	DESCRIPTION
Send every real time event to syslog server	Enable this field to have Vantage RADIUS log every system, RADIUS and user events to a syslog server. Type the syslog server IP address or domain name.
Log facility	The log facility allows you to log the messages to different files in the syslog server see *section 4.3*.
System Log	Enable this field to record system events for logging to the syslog server, see *section 4.4*.
Radius Log	Enable this field to record messages passed between your Vantage RADIUS and the wireless AP's accessing it to the syslog server, see *section 4.5*.
User Trace	Enable this field to record wireless clients' activities on the network to the syslog server, see *section 4.6*.
Send log file to TFTP server	
Send log file to TFTP Server	Enable this field to have Vantage RADIUS transmit log files location to the specified TFTP server. Type the TFTP server IP address.
System Log	Enable this field to record system events for logging to the TFTP server, see *section 4.4*.
Radius Log	Enable this field to record messages passed between your Vantage RADIUS and the wireless AP's accessing it to the TFTP server, see *section 4.5*.
User Trace	Enable this field to record wireless clients' activities on the network to the TFTP server, see *section 4.6*.
Send log file to mail server	
Send log file to mail server everyday	Enable this field to have Vantage RADIUS e-mail log files to the specified e-mail addresses.
Mail Server	Type the IP address or domain name of your e-mail server.
Need Authenticate	Enable this field if your e-mail server requires authentication.
Username	Type a username of a valid account that can send e-mails using the **Mail Server** entered above.
Password	Type a password required to validate the **Username** entered above.

Table 4-9 RADIUS Logs: Log Files

LABEL	DESCRIPTION
Mail Subject	Type a name to identify your log e-mails from other messages sent to the same address. If there are other devices generating logs (for example, another Vantage RADIUS) on the same network, make sure you can identify the log origin.
Mail Address1	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs are not sent via e-mail.
Mail Address2	Type a second e-mail address if you want your log files to be sent to a second destination.
Mail Address3	Type a third e-mail address if you want your log files to be sent to a third destination.
System Log	Enable this field to record system events for logging to the above e-mail addresses, see *section 4.4*.
Radius Log	Enable this field to record messages passed between your Vantage RADIUS and the wireless AP's accessing it to the above e-mail addresses, see *section 4.5*.
User Trace	Enable this field to record wireless clients' activities on the network to the above e-mail addresses, see *section 4.6*.
Apply	Click **Apply** to save your changes back to the RADIUS.

Part II:

RADIUS Server

This part introduces the RADIUS Server screens.

Chapter 5 RADIUS Configuration

5.1 802.1x Overview

The IEEE 802.1x standard outlines enhanced security methods for both the authentication of wireless stations and encryption key management. Vantage RADIUS provides authentication for clients of wireless access points.

5.2 Introduction to RADIUS

RADIUS is based on a client-sever model that supports authentication and accounting, where access point is the client and the server is the RADIUS server. The RADIUS server handles the following tasks among others:

- **Authentication**

  Determines the identity of the users.

- **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 station and the network RADIUS server.

For information about message exchanges between Vantage RADIUS and wireless APs refer to the *System Logs* chapter.

5.3 Secure Connections

Vantage RADIUS authenticates wireless clients using secure connections. The access point and Vantage RADIUS use a shared secret key, which is a password that must be configured on both. The key is not sent over the network. In addition to the shared key, password information exchanged over the wired network is also encrypted to protect it from unauthorized access.

5.3.1 EAP Authentication Overview

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, the access point helps a wireless station and the RADIUS server perform authentication.

Vantage RADIUS supports PEAP and EAP-MD5 (Message-Digest Algorithm 5). Refer to the *Types of EAP Authentication* appendix for descriptions on common types.

The following figure shows an overview of authentication when you specify a RADIUS server on your access point.

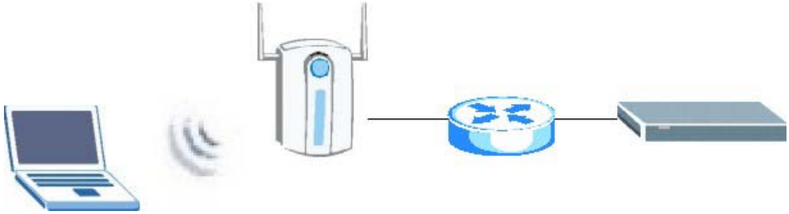


Figure 5-1 EAP Authentication

The details below provide a general description of how IEEE 802.1x EAP authentication works.

- The wireless station sends a "start" message to the access point.
- The access point sends a "request identity" message to the wireless station for identity information.
- The wireless station replies with identity information, including username and password.
- The access point sends this information to the RADIUS server.

- The RADIUS server checks the user information against its user profile database and determines whether or not to authenticate the wireless station.

MD5 authentication does not use certificates for authentication. If your wireless clients are not going to use other protocols for authentication, you do not need to configure any certificates.

The Vantage RADIUS can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities.

In public-key encryption and decryption, each host has two keys. One key is public and can be made openly available; the other key is private and must be kept secure. Public-key encryption in general works as follows.

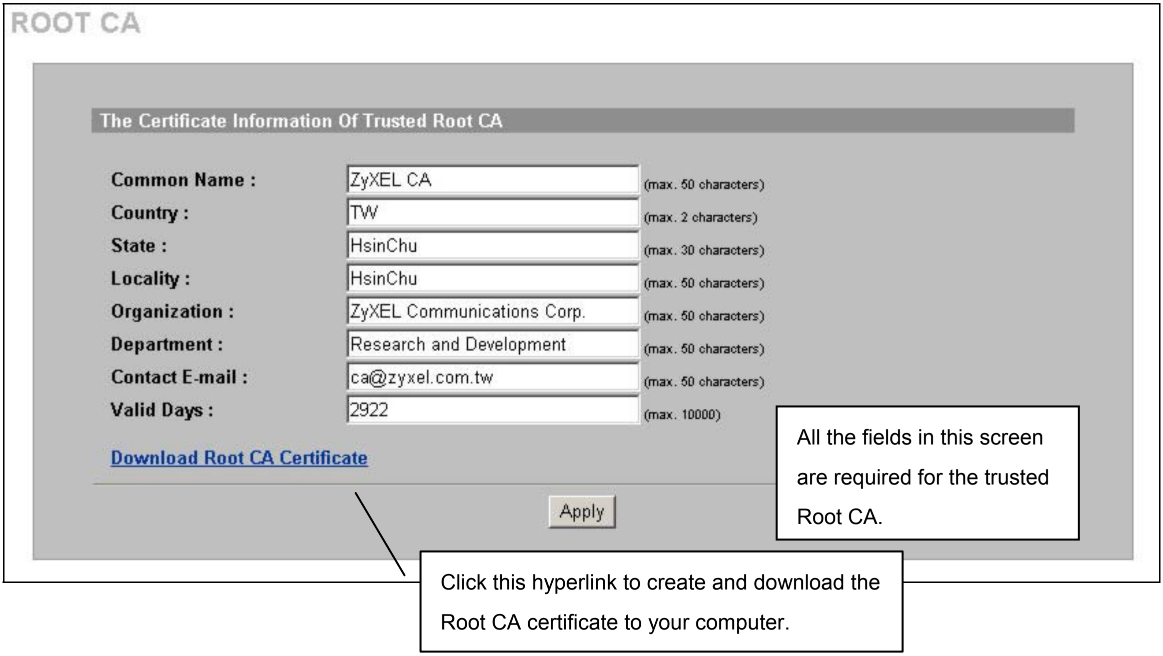
1. Tim wants to send a private message to Jenny. Tim generates a public key pair. What is encrypted with one key can only be decrypted using the other.
2. Tim keeps the private key and makes the public key openly available.
3. Tim uses his private key to encrypt the message and sends it to Jenny.
4. Jenny receives the message and uses Tim's public key to decrypt it.
5. Additionally, Jenny uses her own private key to encrypt a message and Tim uses Jenny's public key to decrypt the message.

You can set your Vantage RADIUS to generate a trusted Root CA (self-signed certificates), which is a special kind of certificate that does not require a CA to guarantee identification. The trust part is based on knowledge of the certificates origin. For example, you trust a certificate is from a valid source because you know the issuer or you trust the service that you are subscribing to.

This certificate is directly downloaded to a computer via an Ethernet connection during a management session. Clients cannot download the certificate themselves. Therefore the certificate must be transferred manually to each client wanting to use the network.

5.4 Trusted Root CA

If your wireless clients use MD5 authentication protocol, you do not need to configure any certificates. Otherwise click **RADIUS** in the main menu and then click **ROOT CA** to set up a certificate for use with PEAP authentication.



ROOT CA

The Certificate Information Of Trusted Root CA

Common Name :	ZyXEL CA	(max. 50 characters)
Country :	TW	(max. 2 characters)
State :	HsinChu	(max. 30 characters)
Locality :	HsinChu	(max. 50 characters)
Organization :	ZyXEL Communications Corp.	(max. 50 characters)
Department :	Research and Development	(max. 50 characters)
Contact E-mail :	ca@zyxel.com.tw	(max. 50 characters)
Valid Days :	2922	(max. 10000)

All the fields in this screen are required for the trusted Root CA.

Click this hyperlink to create and download the Root CA certificate to your computer.

Figure 5-2 Trusted Root Certificate

Each time you change this screen, a new certificate is required for successful wireless client authentication.

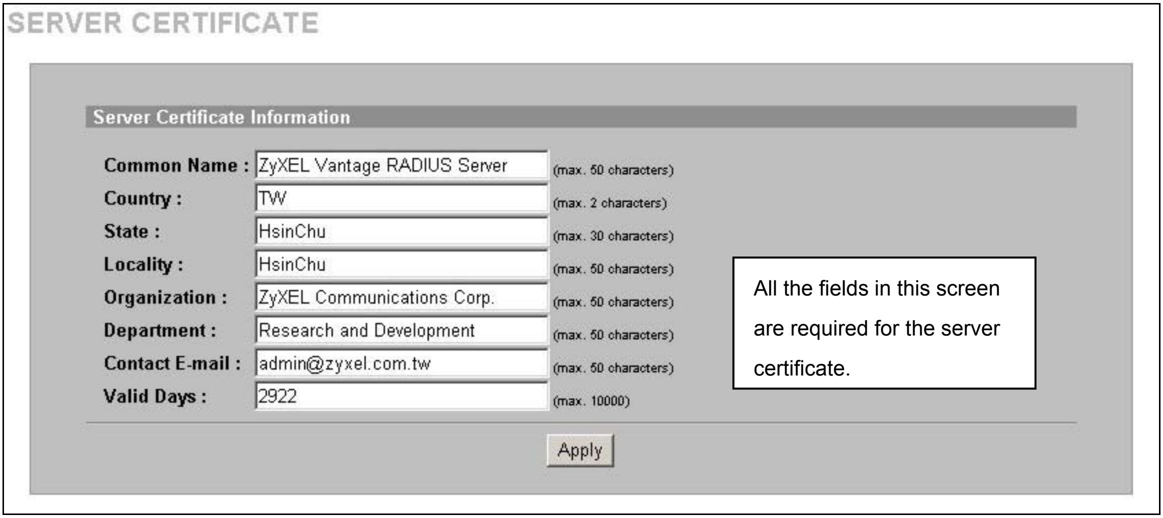
The following table describes the labels in this screen.

Table 5-1 Trusted Root Certificate

LABEL	DESCRIPTION
Common Name	Type up to 50 ASCII characters (not including spaces) to identify this certificate.
Country	Type two characters to identify the nation where the certificate owner is located.
State	Type up to 30 ASCII characters to identify your state, district or region.
Locality	Type up to 50 ASCII characters to identify the city or town where your organization's office is located.
Organization	Type up to 50 ASCII characters to identify your organizations name.
Department	Type up to 50 ASCII characters to detail the department that is issuing the certificate.
Contact E-mail	Type a valid e-mail to contact your Certificate Authority.
Valid Days	Type a period in days that the certificate is valid for.
Download Root CA Certificate	Click this hyperlink to create and download the Root CA certificate to your computer. cert.cer
Apply	Click this button to save the changes back to Vantage RADIUS.

5.5 Server Certificate

If your wireless clients use MD5 authentication protocol, you do not need to configure any certificates and can leave the defaults as they are. Click **RADIUS** in the main menu and then click **SERVER CERTIFICATE** to set up a certificate that identifies Vantage RADIUS to clients.



SERVER CERTIFICATE

Server Certificate Information

Common Name : ZyXEL Vantage RADIUS Server (max. 50 characters)

Country : TW (max. 2 characters)

State : HsinChu (max. 30 characters)

Locality : HsinChu (max. 50 characters)

Organization : ZyXEL Communications Corp. (max. 50 characters)

Department : Research and Development (max. 50 characters)

Contact E-mail : admin@zyxel.com.tw (max. 50 characters)

Valid Days : 2922 (max. 10000)

All the fields in this screen are required for the server certificate.

Figure 5-3 Server Certificate

The following table describes the labels in this screen.

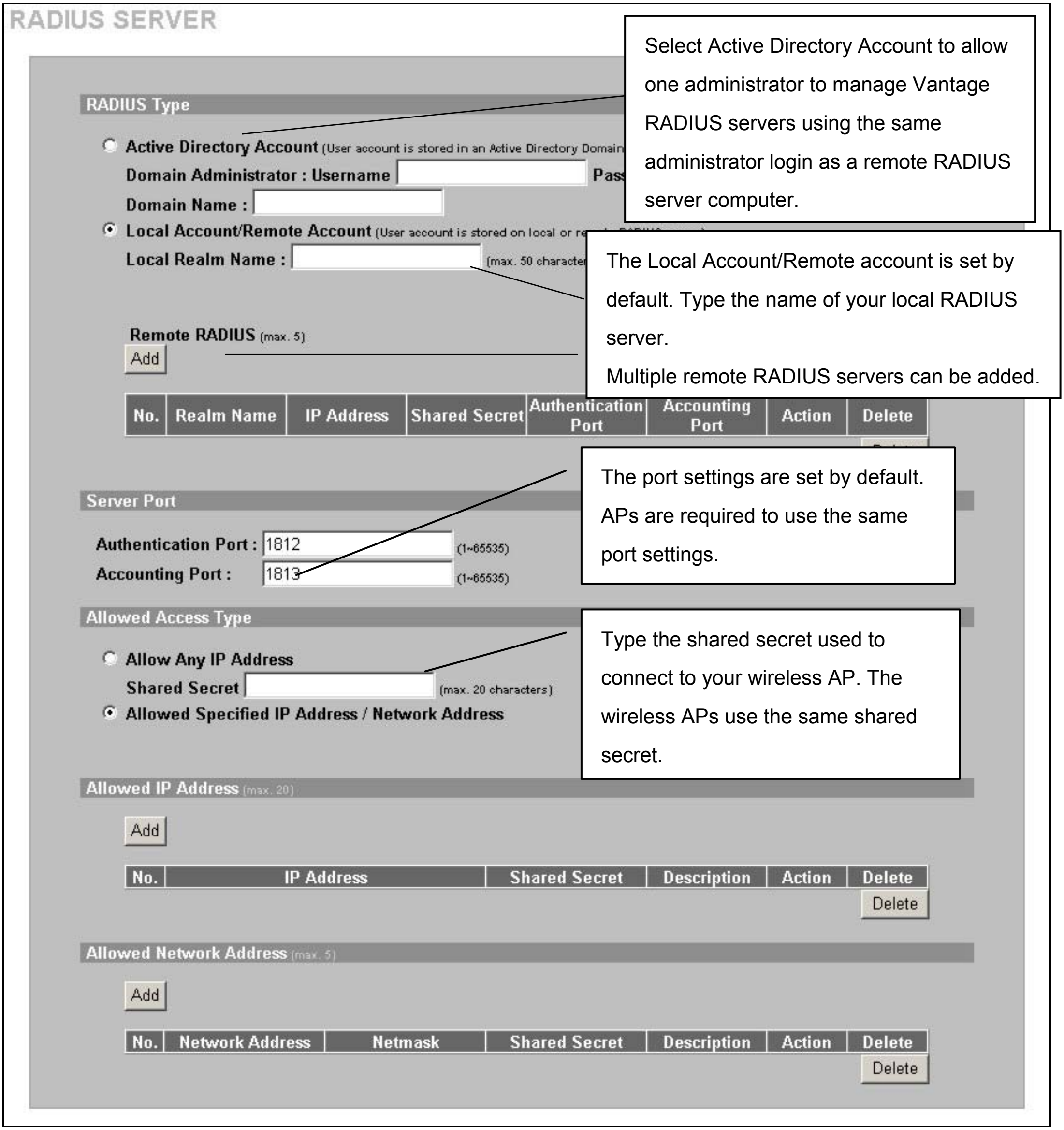
Table 5-2 Server Certificate

LABEL	DESCRIPTION
Common Name	Type up to 50 ASCII characters (not including spaces) to identify this certificate.
Country	Type two characters to identify the nation where the certificate owner is located.
State	Type up to 30 ASCII characters to identify your state, district or region.
Locality	Type up to 50 ASCII characters to identify the city or town where your organization’s office is located.
Organization	Type up to 50 ASCII characters to identify your organizations name.
Department	Type up to 50 ASCII characters to detail the department that is issuing the certificate.
Contact E-mail	Type a valid e-mail to contact your Certificate Authority.
Valid Days	Type a period in days that the certificate is valid for.
Apply	Click this button to save the changes back to Vantage RADIUS.

5.6 RADIUS Server

An access point can manage authentication of wireless clients via a RADIUS server. Multiple RADIUS servers can be used by forwarding authentication requests from wireless clients. Forwarding authentication to different RADIUS servers allows wireless clients to be authenticated by a user account specific to each RADIUS server.

Click **RADIUS** and then **RADIUS SERVER** in the main menu to set up your Vantage RADIUS to manage connections with wireless APs.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain

Domain Administrator : Username Pass

Domain Name :

● Local Account/Remote Account (User account is stored on local or re

Local Realm Name : (max. 50 character

Remote RADIUS (max. 5)

Add

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete

Server Port

Authentication Port : 1812 (1~65535)

Accounting Port : 1813 (1~65535)

Allowed Access Type

○ Allow Any IP Address

Shared Secret (max. 20 characters)

● Allowed Specified IP Address / Network Address

Allowed IP Address (max. 20)

Add

No.	IP Address	Shared Secret	Description	Action	Delete

Delete

Allowed Network Address (max. 5)

Add

No.	Network Address	Netmask	Shared Secret	Description	Action	Delete

Delete

Select Active Directory Account to allow one administrator to manage Vantage RADIUS servers using the same administrator login as a remote RADIUS server computer.

The Local Account/Remote account is set by default. Type the name of your local RADIUS server.
Multiple remote RADIUS servers can be added.

The port settings are set by default. APs are required to use the same port settings.

Type the shared secret used to connect to your wireless AP. The wireless APs use the same shared secret.

Figure 5-4 RADIUS Server Settings

Table 5-3 RADIUS Server Settings

LABEL	DESCRIPTION
RADIUS Type	
Active Directory Account	Select this radio button to allow an administrator to manage a local Vantage RADIUS server using the same administrator login and domain name as a remote RADIUS server computer. The remote server computer must exist behind a local Vantage RADIUS server. 1. Authentication requests are sent to a local Vantage RADIUS server. 2. The Vantage RADIUS server searches for a server computer with the same **Domain Administrator Username**, **Domain Administrator Password** and computer **Domain Name**, see below. 3. If the administrator username, password and domain name of a computer server is found matching the same fields in the Vantage RADIUS, the wireless client is authenticated by the AP.
Domain Administrator	Type the server computer administrator **Username** and **Password**.
Domain Name	Type the **Domain Name** of a server computer.
Local Account/ Remote Account	Select the **Local Account/Remote Account** radio button to have the local RADIUS server or remote RADIUS server authenticate wireless clients via the AP(s).
Local Realm Name	Type a **Local Realm Name** to identify the local RADIUS server name.
Apply	Click this button to save the changes back to Vantage RADIUS.
Remote RADIUS	Click the **Add** button to create a remote RADIUS server account.
No.	This displays the index number of the remote RADIUS server.
Realm Name	This displays the name of a remote RADIUS server.
IP Address	This displays the IP address of a remote RADIUS server. The remote RADIUS server does not have to be in the same subnet as the local RADIUS server.
Shared Secret	This field displays the key used by the remote RADIUS server to connect to your wireless AP.
Authentication Port	This displays the port number of the remote RADIUS authentication server. The default port number is **1812**. Make sure your wireless AP uses the same port number.
Accounting Port	This displays the port number of the remote RADIUS accounting server. The default port number is **1813**. Make sure your wireless AP uses the same port number.

Table 5-3 RADIUS Server Settings

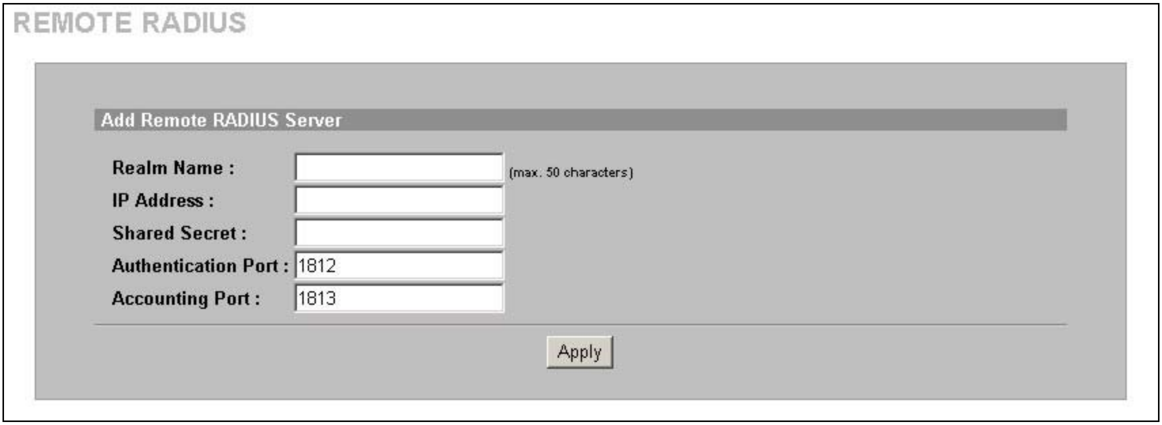
LABEL	DESCRIPTION
Action	Click the **Modify** button in this field to edit information about a remote RADIUS server.
Delete	Select the check box next to the remote RADIUS server description in this list that you want to delete, then click **Delete** to remove this entry.
Server Port	
Authentication Port	Enter the port number of the authentication server. The default port number is **1812**. Make sure your AP uses the same port number.
Accounting Port	Enter the port number of the accounting server. The default port number is **1813**. Make sure your AP uses the same port number.
Allowed Access Type	
Allow Any IP Address	Enable this field to have Vantage RADIUS accept connections from all incoming IP addresses using the shared secret below.
Shared Secret	Type a password as the key to be shared. The key must be the same on Vantage RADIUS and your AP. The key is not sent over the network.
Allowed Specified IP Address/Network Address	Enable this field to allow specified IP addresses of AP's or network addresses in this list to access Vantage RADIUS.
Apply	Click this button to save your configurations back to Vantage RADIUS.
Allowed IP Address (max 20)	
Add	Click this button to add an IP address of an AP to the **Allowed IP Address** list.
No.	This field displays the index number of allowed IP address entries in the list.
IP Address	This field displays the IP address of an AP allowed to access Vantage RADIUS.
Shared Secret	This field displays the key used to connect to your wireless AP.
Description	This field displays the description entered in the **Allowed IP Address** screen to identify your wireless AP.
Action	Click the **Modify** button in this field to edit the information required to access your AP.
Delete	Select the check box next to the AP(s) description in this list that you want to delete, then click **Delete** to remove this entry.

Table 5-3 RADIUS Server Settings

LABEL	DESCRIPTION
Allowed Network Address (max 5)	
Add	Click this button to add a range of IP addresses to the **Allowed IP Address** list.
No.	This field displays an index number of allowed IP address entries in the list.
Network Address	This field displays the IP address of an accepted source to access Vantage RADIUS.
Netmask	This field displays subnet mask used to specify the network range limits for accepted IP addresses.
Shared Secret	Click this button to add an IP address of a wireless AP to the **Allowed IP Address** list.
Description	This field displays the description entered in the **Allowed IP Address** screen to identify your AP.
Action	Click the button in this field to edit the information required to access your wireless AP.
Delete	Select the check box next to the AP(s) description in this list that you want to delete, then click **Delete** to remove this entry.

5.6.1 Add Remote RADIUS Server

Click the **Add** button to create a remote RADIUS server account. This screen allows you to add a remote RADIUS server to a list of remote RADIUS servers that are allowed to communicate with Vantage RADIUS. You need to make sure that you use the same shared secret as your wireless AP. Up to a maximum of five accounts can be created.



REMOTE RADIUS

Add Remote RADIUS Server

Realm Name : (max. 50 characters)

IP Address :

Shared Secret :

Authentication Port : 1812

Accounting Port : 1813

Figure 5-5 RADIUS Server: Add Remote RADIUS Server

Table 5-4 RADIUS Server: Add Remote RADIUS Server

LABEL	DESCRIPTION
Add Remote RADIUS Server	
Realm Name	Type up to 50 ASCII characters the name of a remote RADIUS server.
IP Address	Type the IP address of a remote RADIUS server.
Shared Secret	Type a key used by the remote RADIUS server to connect to your AP.
Authenticating Port	Type the port number of a remote RADIUS authentication server. The default port number is **1812**. Make sure your AP uses the same port number.
Accounting Port	Type the port number of a remote RADIUS accounting server. The default port number is **1813**. Make sure your AP uses the same port number.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **RADIUS SERVER** screen.

5.6.2 Insert/Modify Allowed IP Addresses

This screen allows you to specify which APs are allowed to communicate with Vantage RADIUS. You need to make sure you are using the same shared secret used with your APs to configure this screen.

If you enabled **Allow Any IP Address** in the preceding **RADIUS SERVER** screen, you do not need to configure allowed IP addresses.

Click **RADIUS** and then **RADIUS SERVER** in the main menu. Now click the **Add** button in the **Allowed IP Address** section or click **Modify** next to an entry you want to change. The following screen displays.

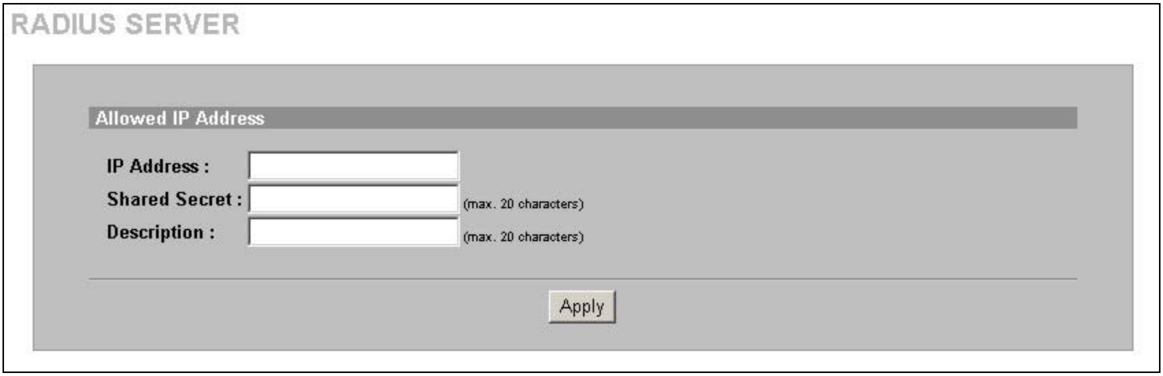


Figure 5-6 RADIUS Server: Add Allowed IP Address

Table 5-5 RADIUS Server: Add Allowed IP Address

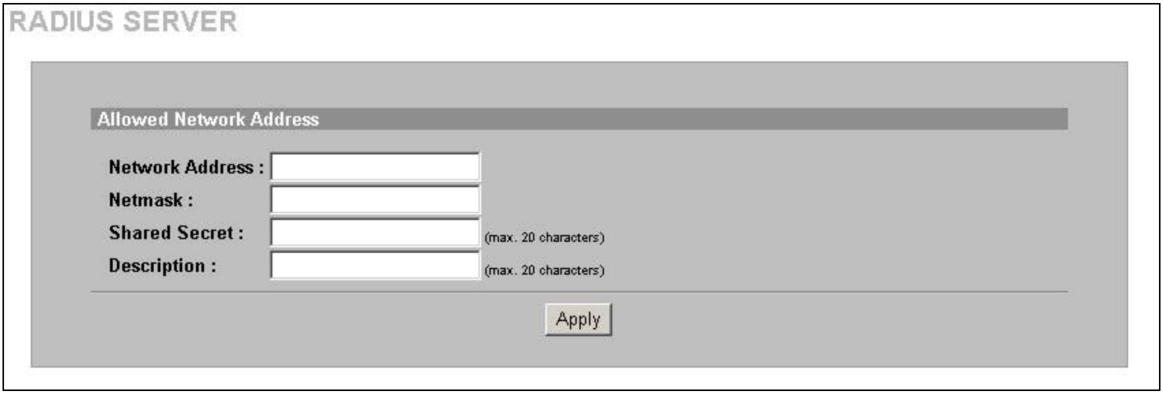
LABEL	DESCRIPTION
Allowed IP Address	
IP Address	Type the IP address in dotted decimal notation of an AP.
Shared Secret	Type a password as the key to be used. The shared secret is the WEP Key used to access an AP on the network. The key must be the same on Vantage RADIUS and your AP. The key is not sent over the network.
Description	Type a description for identification purposes of your AP in the **Allowed IP Address** list.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **RADIUS SERVER** screen.

5.6.3 Insert/Modify Allowed Network Range

This screen allows you to specify a network range in which an AP is allowed to communicate with Vantage RADIUS. You need to know the WEP key or shared secret used with your wireless APs in the network range to configure this screen.

If you enabled **Allow Any IP Address** in the preceding **RADIUS SERVER** screen, you do not need to configure allowed IP addresses.

Click **RADIUS** and then **RADIUS SERVER** in the main menu. Now click the **Add** button in the **Allowed Network IP Address** section or click **Modify** next to an entry you want to change. The following screen displays.



RADIUS SERVER

Allowed Network Address

Network Address :

Netmask :

Shared Secret : (max. 20 characters)

Description : (max. 20 characters)

Figure 5-7 RADIUS Server: Add Allowed Network Address

Table 5-6 RADIUS Server: Add Allowed Network Address

LABEL	DESCRIPTION
Allowed Network Address	
Network Address	Type the first address in your network. This is the start address from which Vantage RADIUS uses the **Netmask** to allow access from many APs.
Netmask	This field displays subnet mask used to specify the network range limits for accepted IP addresses.

Table 5-6 RADIUS Server: Add Allowed Network Address

LABEL	DESCRIPTION
Shared Secret	Type a password as the key to be used. The key must be the same on Vantage RADIUS as the APs on your network. The key is not sent over the network.
Description	Type a name to identify your wireless AP network in the **Allowed Network Address** list.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **RADIUS SERVER** screen.

5.7 RADIUS Server Examples

The following examples show you how to configure different scenarios for your Vantage RADIUS.

See Section 5.8 for information on wireless client computer account user names. Unless otherwise specified, a wireless client computer will be referred to as 'computer' in these examples. The RADIUS server domain name will be referred to as 'realm' name.

5.7.1 Example 1: Vantage RADIUS Local and Remote Server Setup

In the following example A, B and C request access to E. The wireless clients are authenticated by D using local RADIUS server 1 and remote RADIUS servers 2 and 3. Forwarding authentication requests to different servers allows wireless clients to be authenticated by a user account specific to each RADIUS server. The following table displays an example list of user accounts; see the *User Account* section for information on how to configure these.

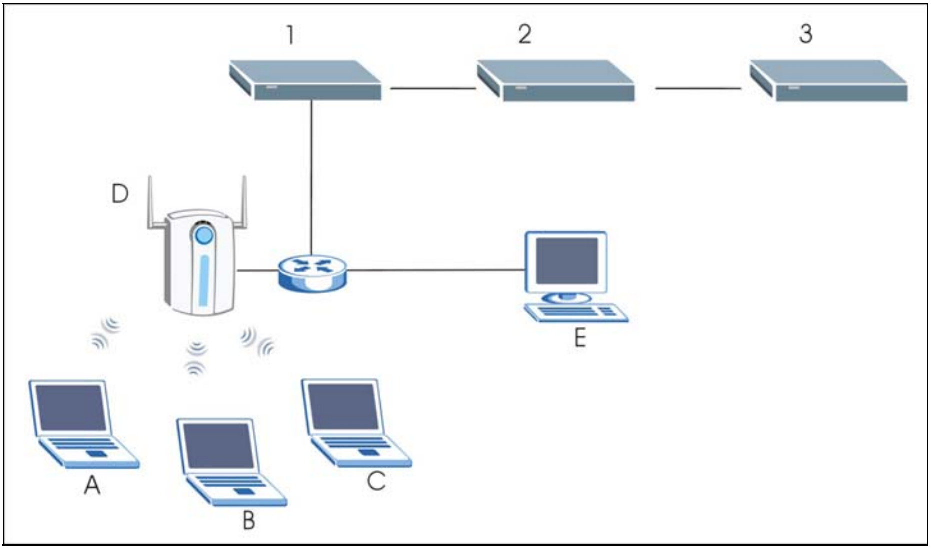


Figure 5-8 Example 1: Vantage RADIUS Local and Remote Server Setup

Table 5-7 Example 1: RADIUS Server User Accounts

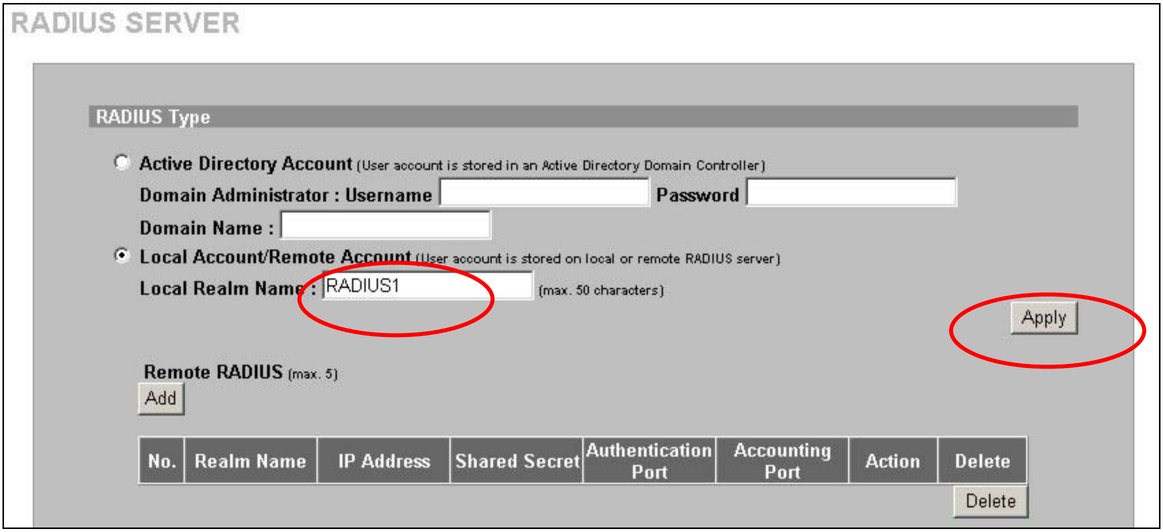
RADIUS1	RADIUS2	RADIUS3
ComputerA	ComputerB	ComputerC

RADIUS1 and Computer A Configuration

1. In the **RADIUS SERVER** screen type the name of your local RADIUS server in the **Local Realm Name** field.

2. Click the **Apply** button.

The local RADIUS server is connected to the AP. If you have any Remote RADIUS servers, they exist behind the local RADIUS server.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username ______ Password ______

Domain Name : ______

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete

Figure 5-9 Example 1: Vantage RADIUS Local Server Setup

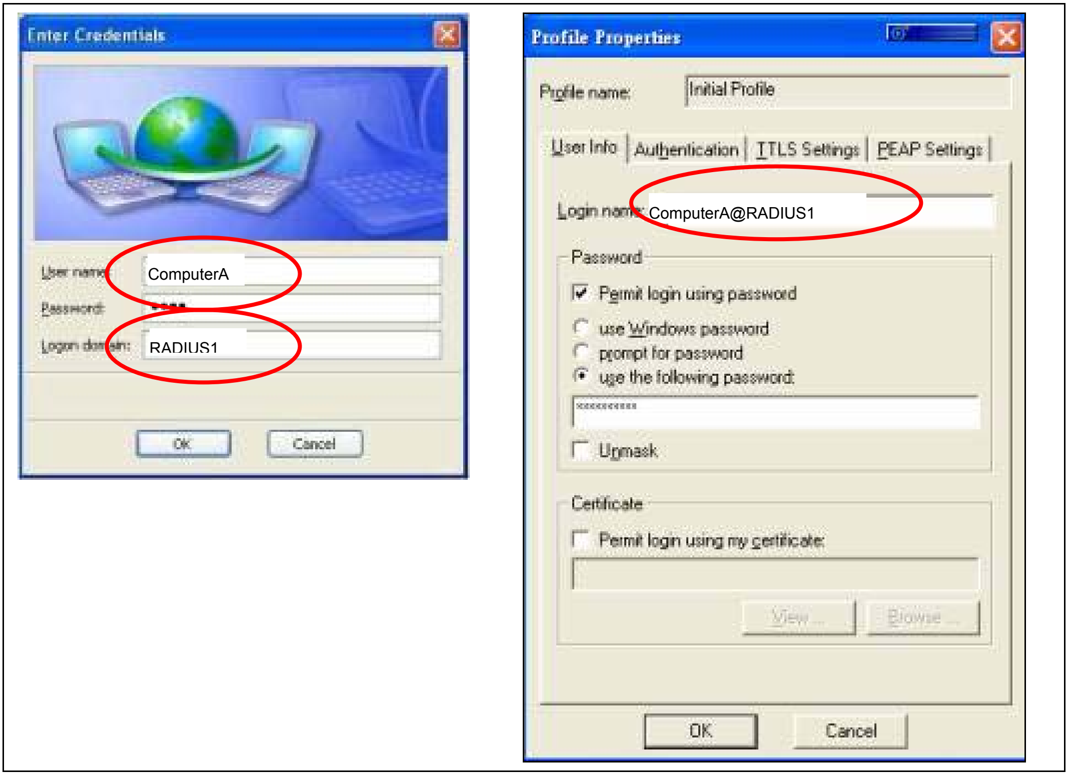
Follow the steps to set up computer A.

- If computer A uses Wireless Zero Configuration utility, then type the **User name** ("ComputerA" in this example) and the user account **Password**. See the section on User Account for more information. Type "RADIUS1" in the **Logon domain** field.

You can leave the Logon domain **field blank if you do not know the realm of your local RADIUS server. You must enter this field for remote RADIUS servers.**

- If computer A uses Odyssey Client utility, then type the **Login name** in computer@realm format.

You can type the Login name **as a user account name only, without the @realm domain. This applies to local RADIUS servers only.**



User name: ComputerA

Password: ****

Logon domain: RADIUS1

Profile name: Initial Profile

Login name: ComputerA@RADIUS1

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password:

****

□ Unmask

Certificate

□ Permit login using my certificate:

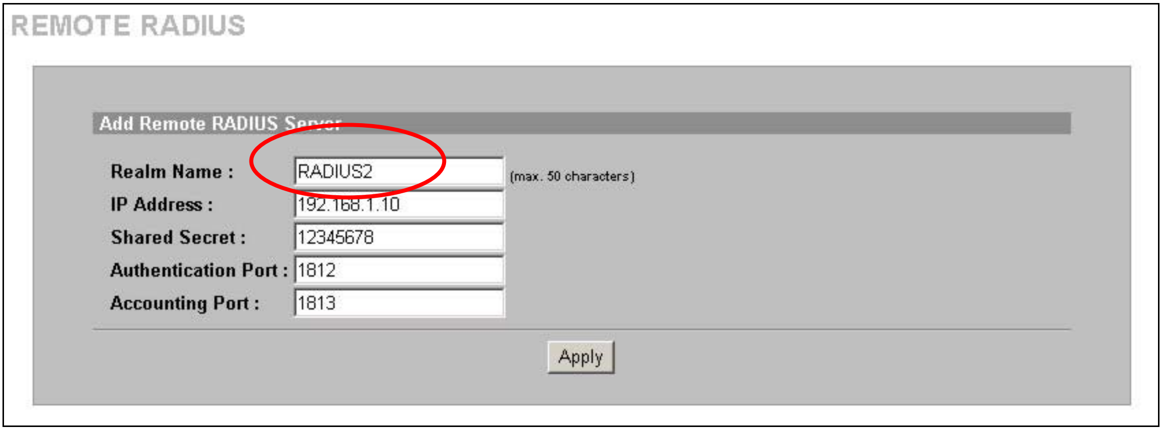
Figure 5-10 Example 1: Using WZC or Odyssey Client: Computer A

3. If successfully authenticated, computer A can communicate with E.

RADIUS2 and Computer B Configuration

1. In the **RADIUS SERVER** screen click the **Add** button under **Remote RADIUS**.
2. The **Add Remote RADIUS Server** screen displays.
3. Type the name of a remote RADIUS server in the **Realm Name** field.
4. Type the **IP Address** of the remote RADIUS server.
5. Type a **Shared Secret** that matches the shared secret in D.
6. The **Authentication Port** and **Accounting Port** must match those in D.

7. Click **Apply** to save the settings and return to the **RADIUS SERVER** screen.



REMOTE RADIUS

Add Remote RADIUS Server

Realm Name : RADIUS2 (max. 50 characters)

IP Address : 192.168.1.10

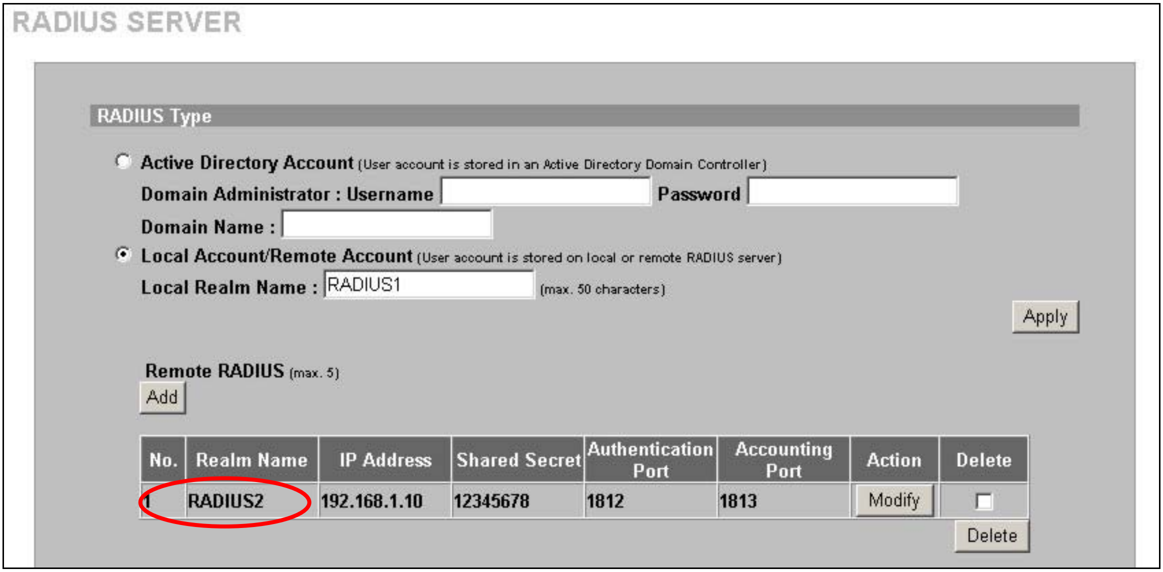
Shared Secret : 12345678

Authentication Port : 1812

Accounting Port : 1813

Figure 5-11 Example 1: Add Remote RADIUS Server

The Vantage RADIUS now has a remote RADIUS server named "RADIUS2".



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username Password

Domain Name :

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

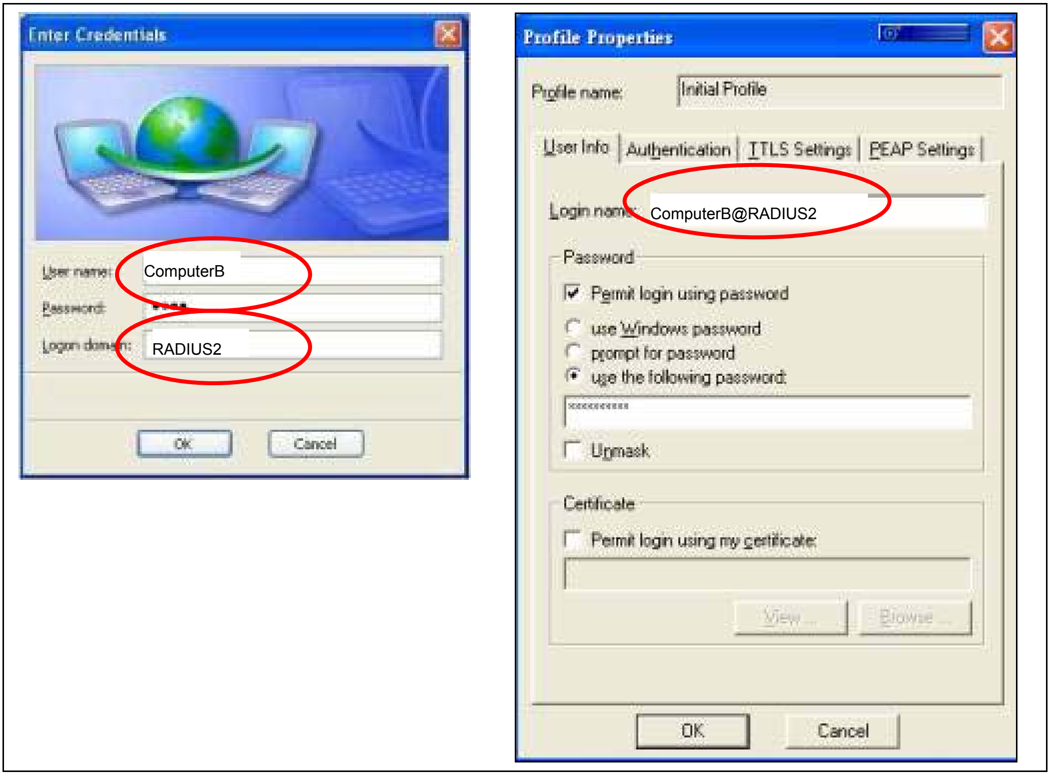
No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete
1	RADIUS2	192.168.1.10	12345678	1812	1813	Modify	□

Figure 5-12 Example 1: Vantage RADIUS Remote Server Setup

Follow the steps to set up computer B.

- If computer B uses Wireless Zero Configuration utility, then type the **User name** "ComputerB" and the user account **Password**. See the section on User Account for more information. Type "RADIUS2" in the **Login domain** field.
- If computer B uses Odyssey Client utility, then type the **Login name** in computer@realm format.

If the remote server is a computer with Windows 2003 IAS, the Odyssey Client Login name **must by typed in realm\computer format, for example** RADIUS2\ComputerB.



User name: ComputerB
Password: ••••
Logon domain: RADIUS2

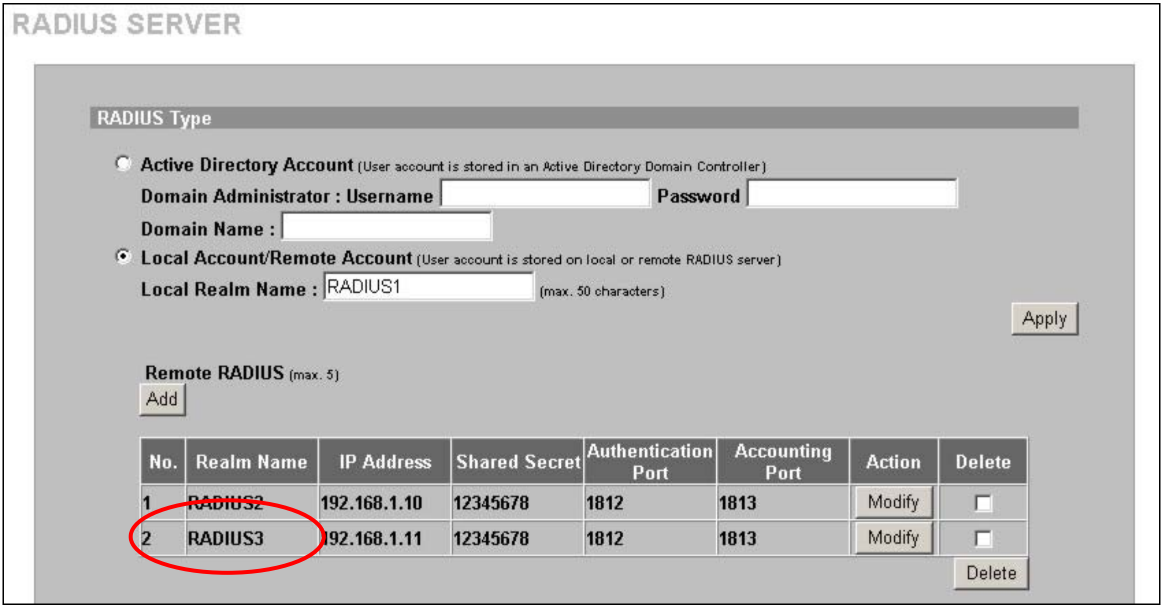
Profile name: Initial Profile
Login name: ComputerB@RADIUS2
Password
☑ Permit login using password
○ use Windows password
○ prompt for password
● use the following password:
xxxxxxxxxx
□ Unmask
Certificate
□ Permit login using my certificate:

Figure 5-13 Example 1: Using WZC or Odyssey Client: Computer B

The AP forwards an authentication request to the local RADIUS server. Computer B has a realm RADIUS2. The authentication request is then forwarded to the remote RADIUS server, named RADIUS2. Computer B is listed as a user account. If successfully authenticated, B can communicate with E.

RADIUS3 and Computer C Configuration

1. In the **RADIUS SERVER** screen click the **Add** button and create a remote RADIUS server named "RADIUS3" in the same manner that you configured RADIUS2.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username
Password

Domain Name :

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

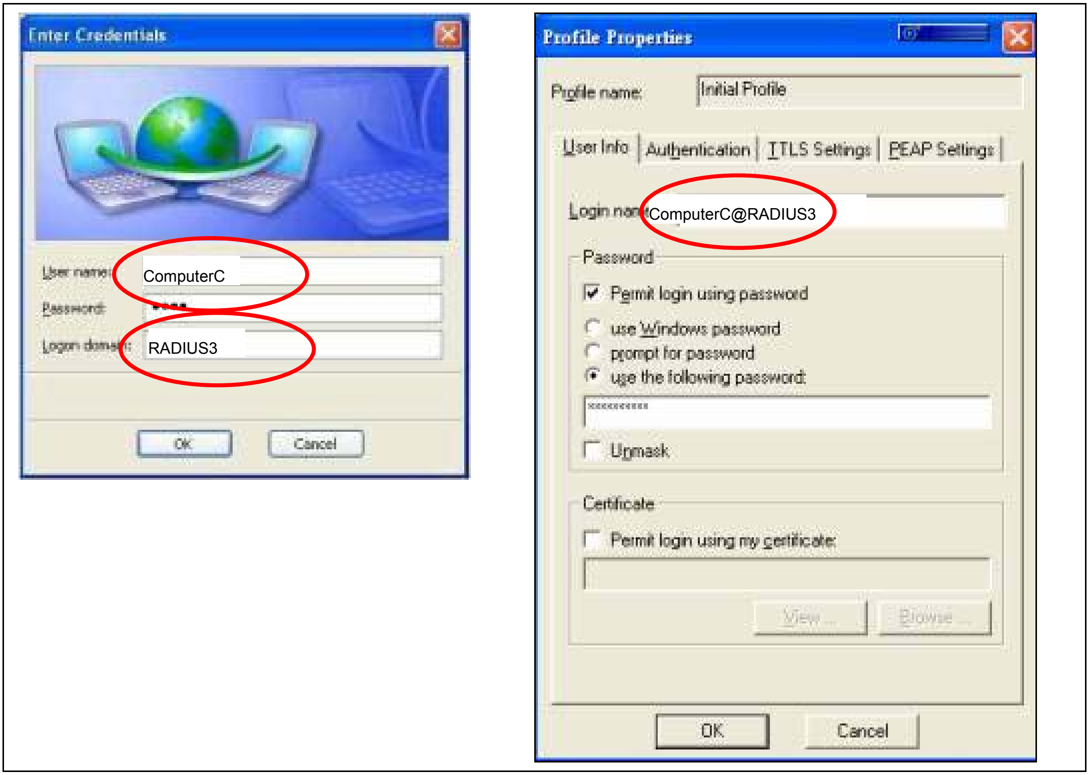
Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete
1	RADIUS2	192.168.1.10	12345678	1812	1813	Modify	□
2	RADIUS3	192.168.1.11	12345678	1812	1813	Modify	□

Figure 5-14 Example 1: Vantage RADIUS Remote Servers

Set up the wireless client computer as displayed in the following screen.



Enter Credentials

User name: ComputerC

Password: ****

Logon domain: RADIUS3

Profile Properties

Profile name: Initial Profile

Login name: ComputerC@RADIUS3

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password:

****

□ Unmask

Certificate

□ Permit login using my certificate:

Figure 5-15 Example 1: Using WZC or Odyssey Client: Computer C

The AP forwards an authentication request to the local RADIUS server. Computer C has a realm RADIUS3. The authentication request is then forwarded to the remote RADIUS server, named RADIUS3. Computer C is listed as a user account. If successfully authenticated, C can communicate with E.

5.7.2 Example 2: Vantage RADIUS Local and Remote Server Setup

In the following example computers A and B request access to E. Computer A is authenticated by C using RADIUS server 1. Computer B is authenticated by D using RADIUS server 1. The following table displays an example list of user accounts; see the User Account section for information on how to configure these.

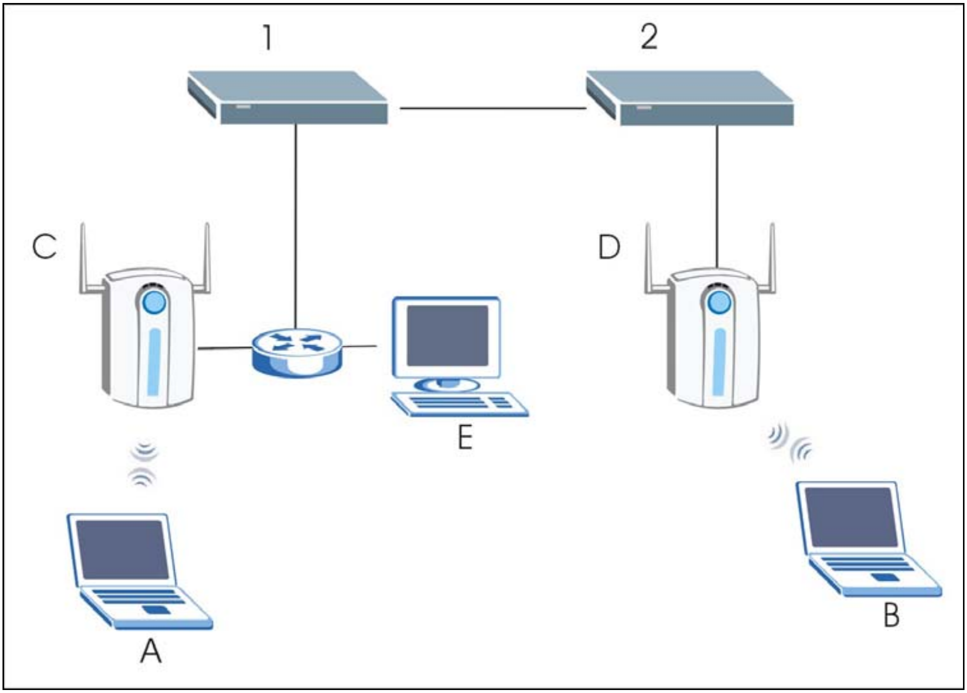


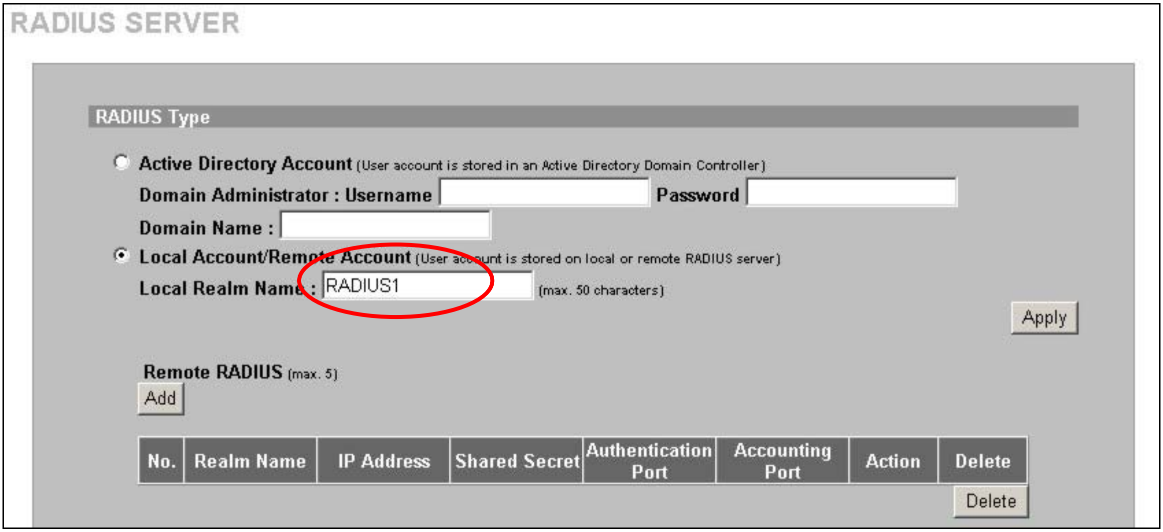
Figure 5-16 Example 2: Vantage RADIUS Local and Remote Server Setup

Table 5-8 Example 2: RADIUS Server User Accounts

RADIUS1
ComputerA
ComputerB

RADIUS1 and Computer A Configuration

In the **RADIUS SERVER** screen type the name of your local RADIUS server in the **Local Realm Name** field.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username [ ] Password [ ]

Domain Name : [ ]

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

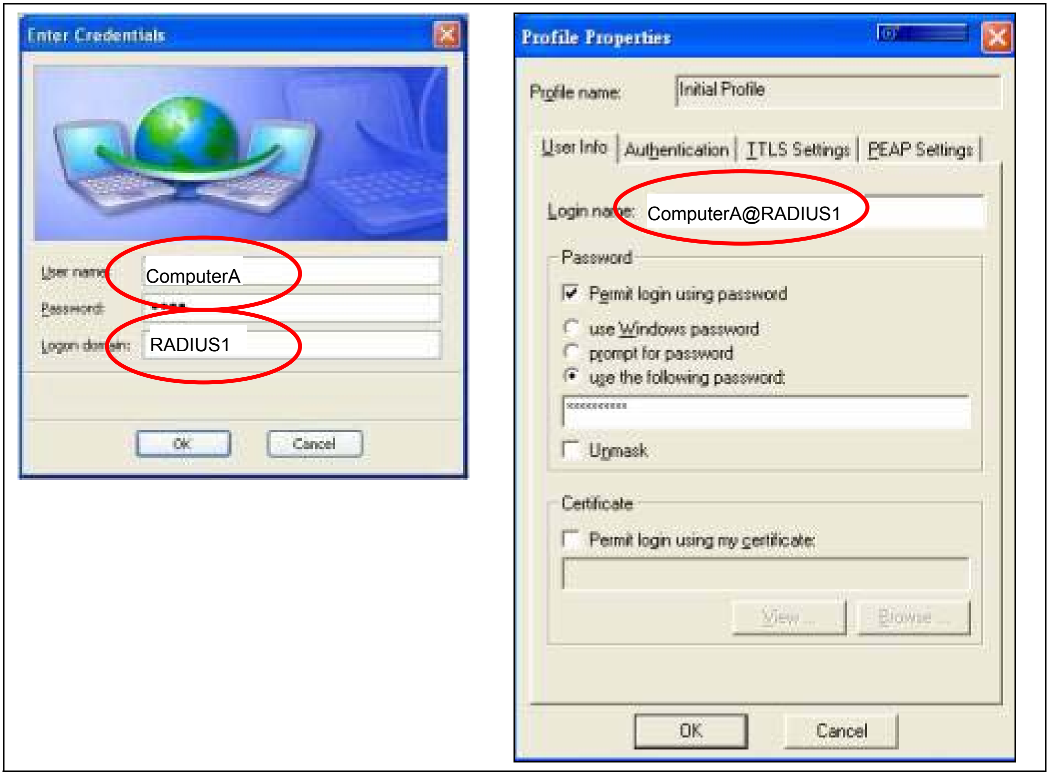
No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete

Figure 5-17 Example 2: Vantage RADIUS Local Server 1 Setup

Follow the steps to set up computer A.

- If computer A uses Wireless Zero Configuration utility, then type the **User name** "ComputerA" and the user account **Password**. See the section on User Account for more information. Type "RADIUS1" in the **Login domain** field.
- If computer A uses Odyssey Client utility, then type the **Login name** in computer@realm format.

Set up the wireless client computer as displayed in the following screen.



User name: ComputerA
Password: ****
Logon domain: RADIUS1

Profile name: Initial Profile

Login name: ComputerA@RADIUS1

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password

****

□ Unmask

Certificate

□ Permit login using my certificate:

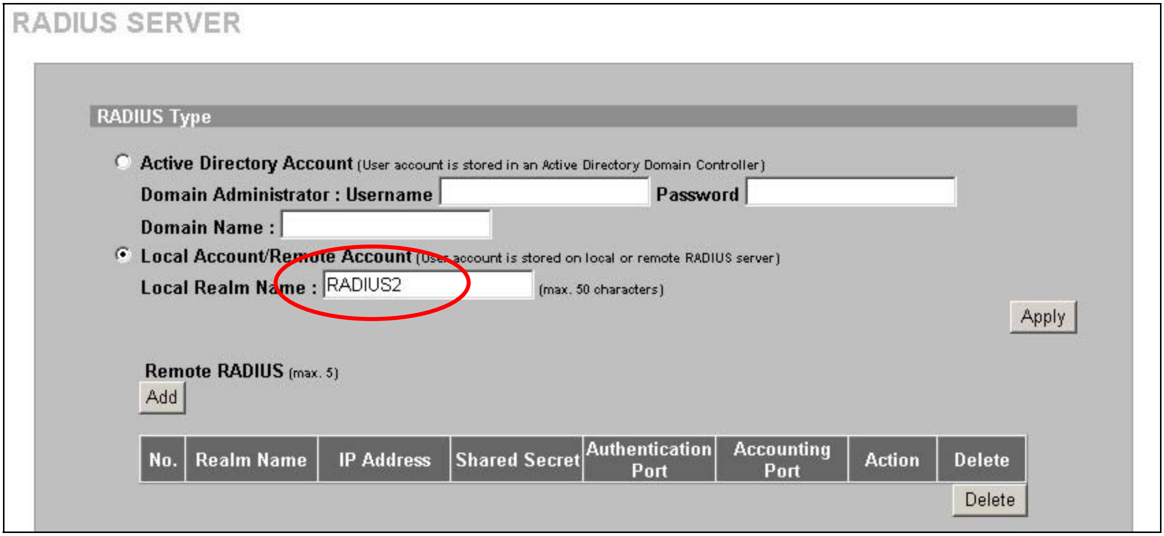
Figure 5-18 Example 2: Using WZC or Odyssey Client: Computer A

If successfully authenticated, A can communicate with E.

RADIUS2 and Computer B Configuration

The local RADIUS server is in the same subnet as B. The RADIUS server 2 must be set as the local RADIUS server and the RADIUS server 1 must be set as a remote RADIUS server.

1. In the web configurator of Vantage RADIUS 2, go to the **RADIUS SERVER** screen and type the name of your local RADIUS server in the **Local Realm Name** field.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username Password

Domain Name :

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS2 (max. 50 characters)

Remote RADIUS (max. 5)

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete

Figure 5-19 Example 2: Vantage RADIUS Local Server 2 Setup

2. In the **RADIUS SERVER** screen click the **Add** button under **Remote RADIUS**.

3. The **Add Remote RADIUS Server** screen displays.

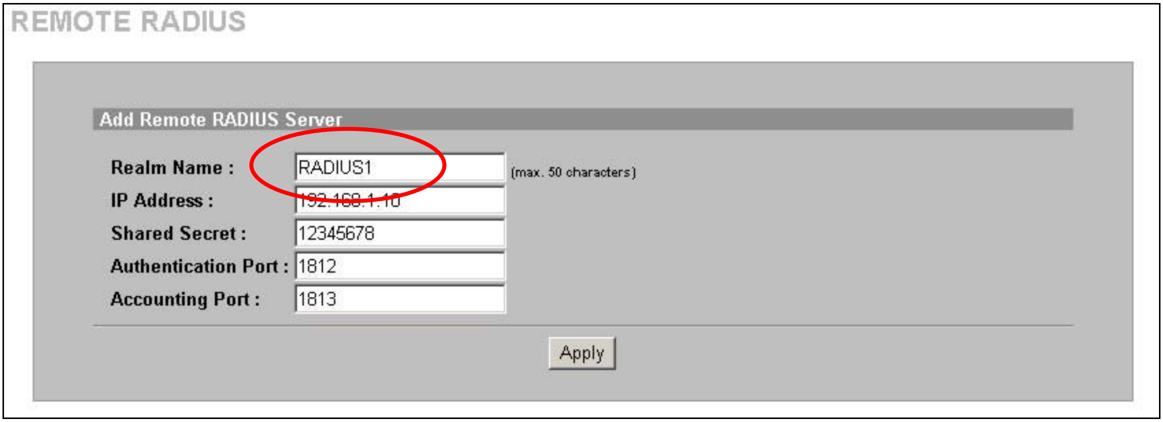
4. Type the name of the remote RADIUS server in the **Realm Name** field.

5. Type the **IP Address** of the remote RADIUS server.

6. Type a **Shared Secret** that matches the shared secret in C.

7. The **Authentication Port** and **Accounting Port** must match those in C.

8. Click **Apply** to save the settings and return to the **RADIUS SERVER** screen.



REMOTE RADIUS

Add Remote RADIUS Server

Realm Name : RADIUS1 (max. 50 characters)

IP Address : 192.168.1.10

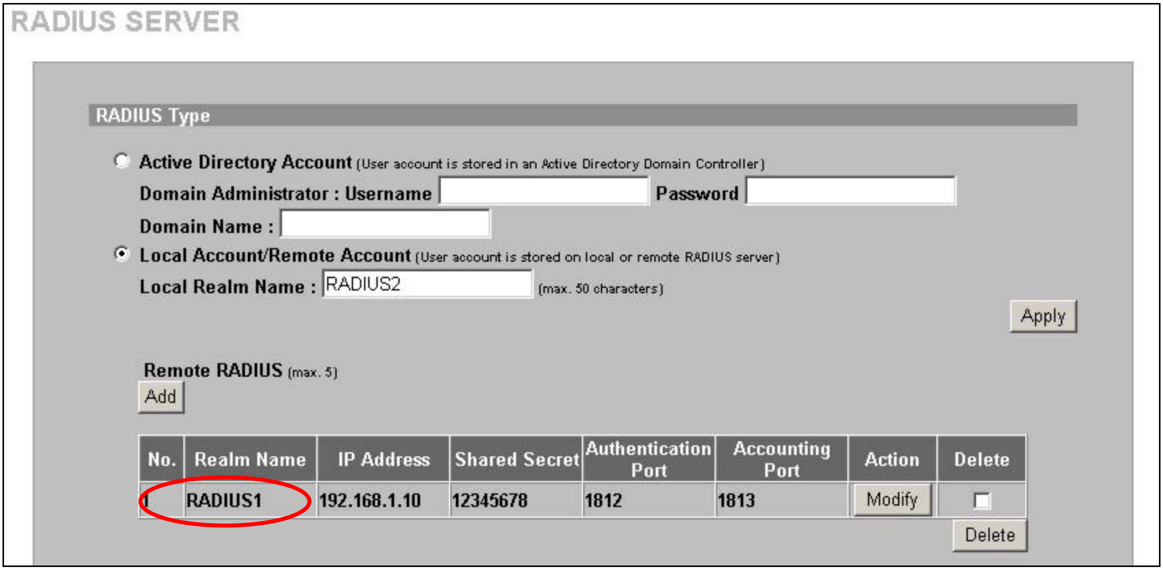
Shared Secret : 12345678

Authentication Port : 1812

Accounting Port : 1813

Figure 5-20 Example 2: Add Remote RADIUS Server

RADIUS server 2 now has a remote RADIUS server named "RADIUS1".



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username   Password

Domain Name :

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS2 (max. 50 characters)

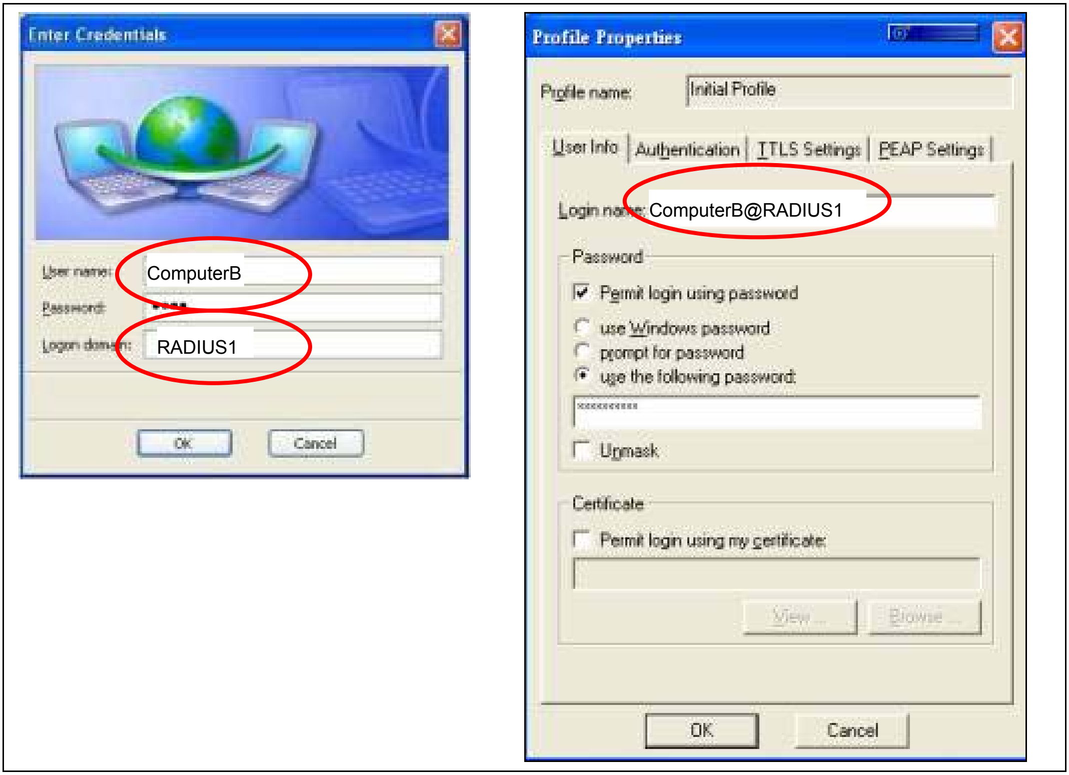
Remote RADIUS (max. 5)

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete
1	RADIUS1	192.168.1.10	12345678	1812	1813	Modify	□

Figure 5-21 Example 2: Vantage RADIUS Remote Server 2 Setup

Follow the steps to set up computer B.

- If computer B uses Wireless Zero Configuration utility, then type the **User name** ComputerB and the user account **Password**. See the section on User Account for more information. Type RADIUS1 in the **Login domain** field.
- If your wireless client computer B uses Odyssey Client utility, then type the **Login name** in computer@realm format.



User name: ComputerB

Password: ****

Logon domain: RADIUS1

Profile name: Initial Profile

Login name: ComputerB@RADIUS1

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password

****

□ Unmask

Certificate

□ Permit login using my certificate

Figure 5-22 Example 2: Using WZC or Odyssey Client: Computer B

AP D forwards an authentication request to Vantage RADIUS server 2. Computer B has a realm RADIUS1. The authentication request is then forwarded to the remote RADIUS server, named RADIUS1. Computer B is listed as a user account. If successfully authenticated, B can communicate with E.

5.7.3 Example 3: Vantage RADIUS and Remote Computer Server Setup

In the following example the computer A requests access to B. Computer A is authenticated by C via a remote RADIUS server computer 2.

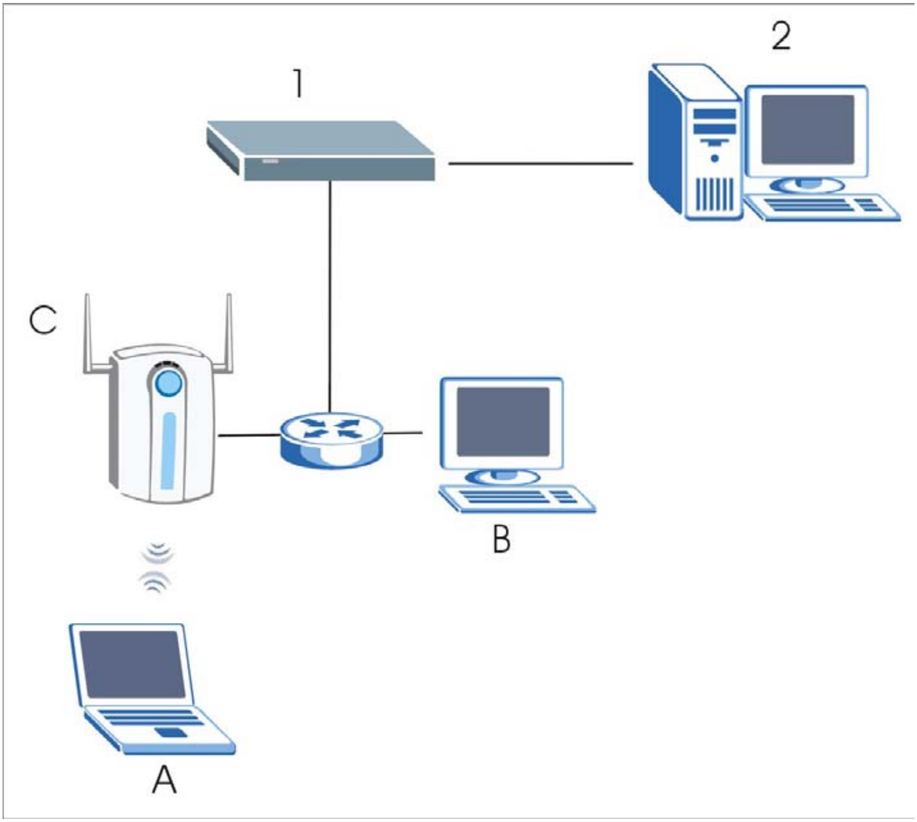


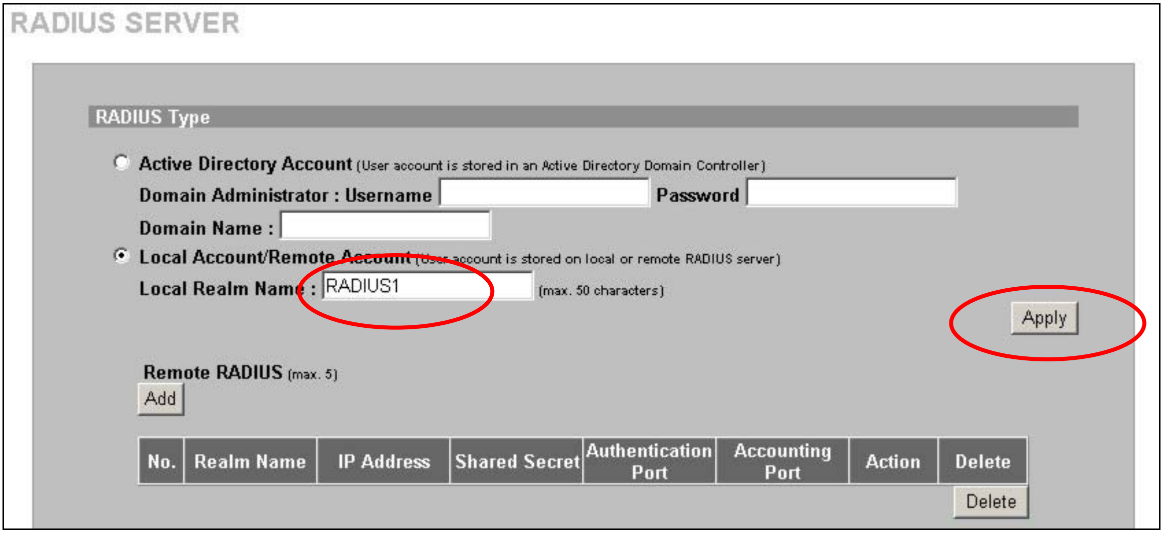
Figure 5-23 Example 3: Vantage RADIUS and Remote Computer Server

Table 5-9 Example 3: RADIUS Server User Accounts

COMSERVER2
ComputerA

Computer A and Remote RADIUS Server Computer Configuration

In the **RADIUS SERVER** screen type the name of your local RADIUS server in the **Local Realm Name** field. Click the **Apply** button.



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username

Password

Domain Name :

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

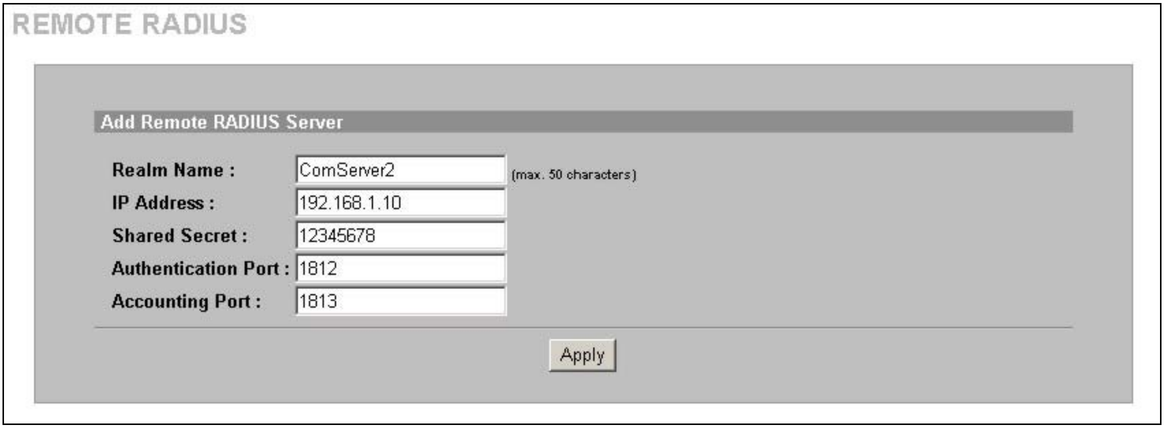
Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete

Figure 5-24 Example 3: Vantage RADIUS Local Server Setup

1. In the **RADIUS SERVER** screen click the **Add** button and create a remote RADIUS server.
2. The **Add Remote RADIUS Server** screen displays.
3. Type the name of the remote RADIUS server in the **Realm Name** field.
4. Type the **IP Address** of the remote RADIUS server.
5. Type a **Shared Secret** that matches the shared secret in C.
6. The **Authentication Port** and **Accounting Port** must match those in C.
7. Click **Apply** to save the settings and return to the **RADIUS SERVER** screen.

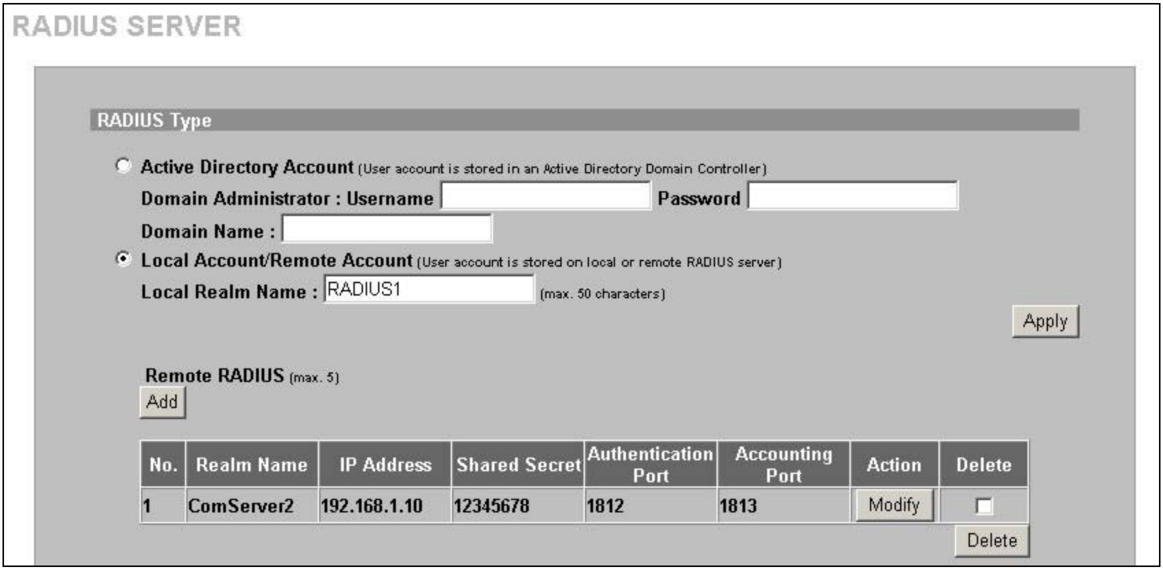


REMOTE RADIUS

Add Remote RADIUS Server

Realm Name :	ComServer2 (max. 50 characters)
IP Address :	192.168.1.10
Shared Secret :	12345678
Authentication Port :	1812
Accounting Port :	1813

Figure 5-25 Example 3: Add Remote RADIUS Server



RADIUS SERVER

RADIUS Type

○ Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username ______ Password ______

Domain Name : ______

● Local Account/Remote Account (User account is stored on local or remote RADIUS server)

Local Realm Name : RADIUS1 (max. 50 characters)

Remote RADIUS (max. 5)

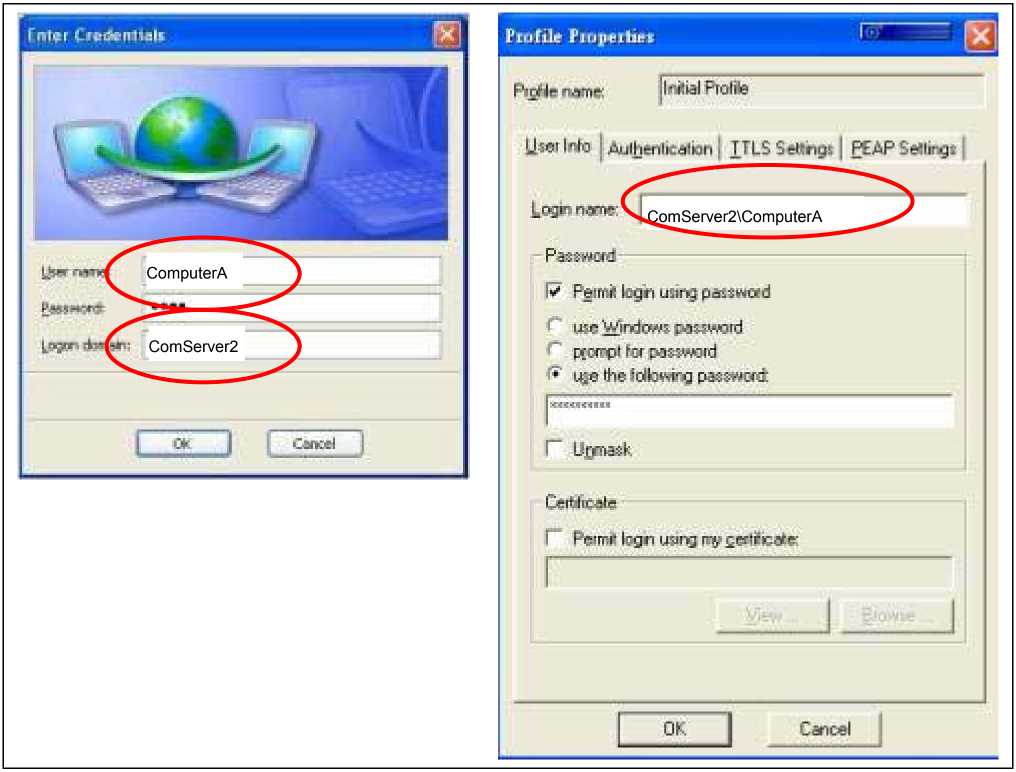
No.	Realm Name	IP Address	Shared Secret	Authentication Port	Accounting Port	Action	Delete
1	ComServer2	192.168.1.10	12345678	1812	1813	Modify	□

Figure 5-26 Example 3: Vantage RADIUS Remote Server Setup

Follow the steps to set up computer A.

- If computer A uses Wireless Zero Configuration utility, then type the **User name** “ComServer2” and the user account **Password**. See the section on User Account for more information. Type ComServer2 in the **Logon domain** field.
- If computer A uses Odyssey Client utility, then type the **Login name** in computer@realm format.

If the remote server is a computer with Windows 2003 IAS, the Odyssey Client Login name **must by typed in realm\computer format, for example** ComServer2\ComputerA.



Enter Credentials

User name: ComputerA

Password: ****

Logon domain: ComServer2

Profile Properties

Profile name: Initial Profile

Login name: ComServer2\ComputerA

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password:

****

□ Unmask

Certificate

□ Permit login using my certificate:

Figure 5-27 Example 3: Using WZC or Odyssey Client: Computer A

1. In the remote RADIUS server computer, open the **Internet Authentication Service** screen.

2. A new server group must be created so that the RADIUS server computer can receive authentication requests from a local RADIUS server, such as a Vantage RADIUS device.

3. To create a new server group:

4. Right-click the **Remote RADIUS Server Group** and create a **New Remote RADIUS Server Group**.

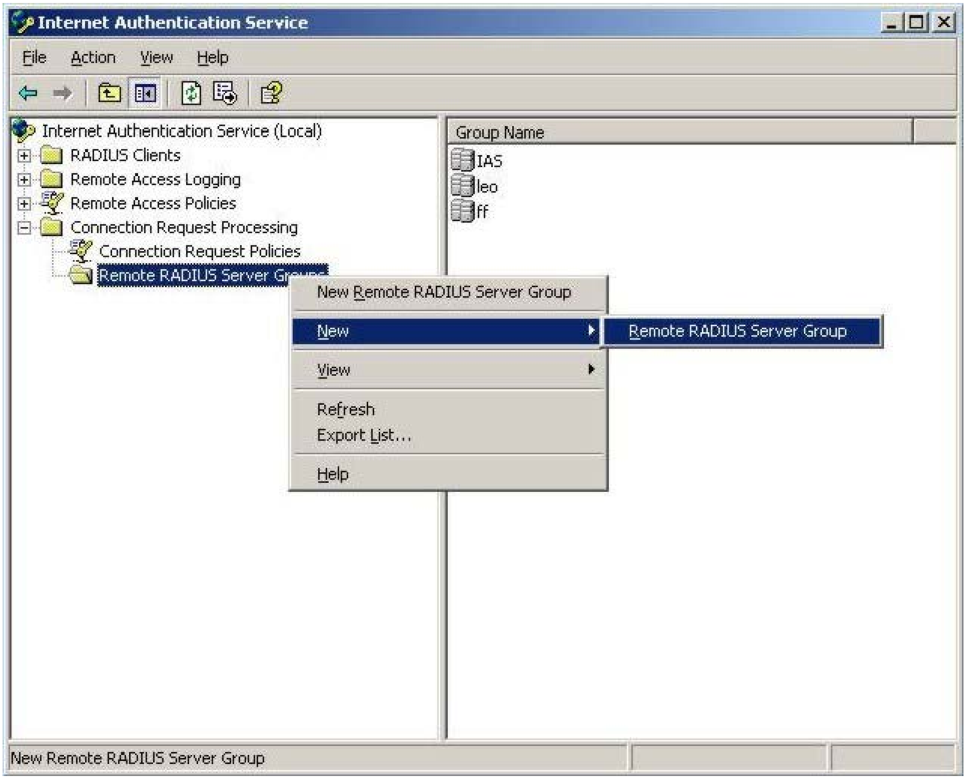
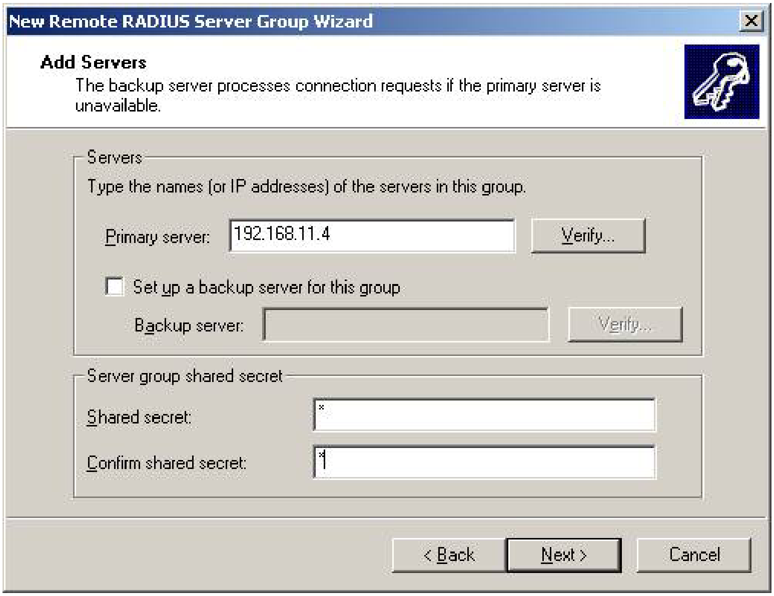

Internet Authentication Service
File
Action
View
Help
Internet Authentication Service (Local)
RADIUS Clients
Remote Access Logging
Remote Access Policies
Connection Request Processing
Connection Request Policies
Remote RADIUS Server Groups
Group Name
IAS
leo
ff
New Remote RADIUS Server Group
New
Remote RADIUS Server Group
View
Refresh
Export List...
Help
New Remote RADIUS Server Group

Figure 5-28 New Remote RADIUS Server Group

5. The **New Remote RADIUS Server Group Wizard** opens. Type the IP address of the Vantage RADIUS server in the **Primary server** field.

6. Type the **Shared secret** in the **Server group shared secret** section. This should match the shared secret in the AP that you want to use to authenticate a wireless client.

7. Click **Next** to continue.



New Remote RADIUS Server Group Wizard

Add Servers

The backup server processes connection requests if the primary server is unavailable.

Servers

Type the names (or IP addresses) of the servers in this group.

Primary server: 192.168.11.4

☐ Set up a backup server for this group

Backup server:

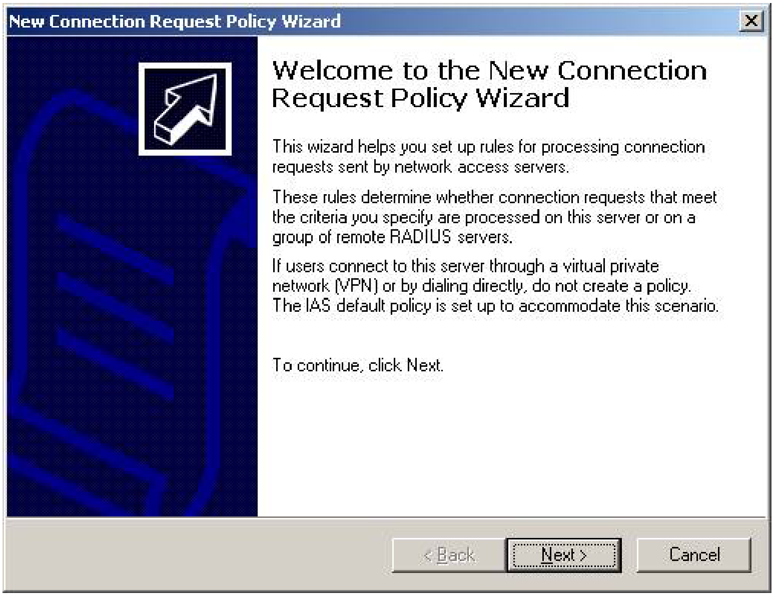
Server group shared secret

Shared secret: *

Confirm shared secret: *

Figure 5-29 New Remote RADIUS Server Group Wizard

8. The **New Connection Request Policy Wizard** opens. Click **Next** to continue.



New Connection Request Policy Wizard

Welcome to the New Connection Request Policy Wizard

This wizard helps you set up rules for processing connection requests sent by network access servers.

These rules determine whether connection requests that meet the criteria you specify are processed on this server or on a group of remote RADIUS servers.

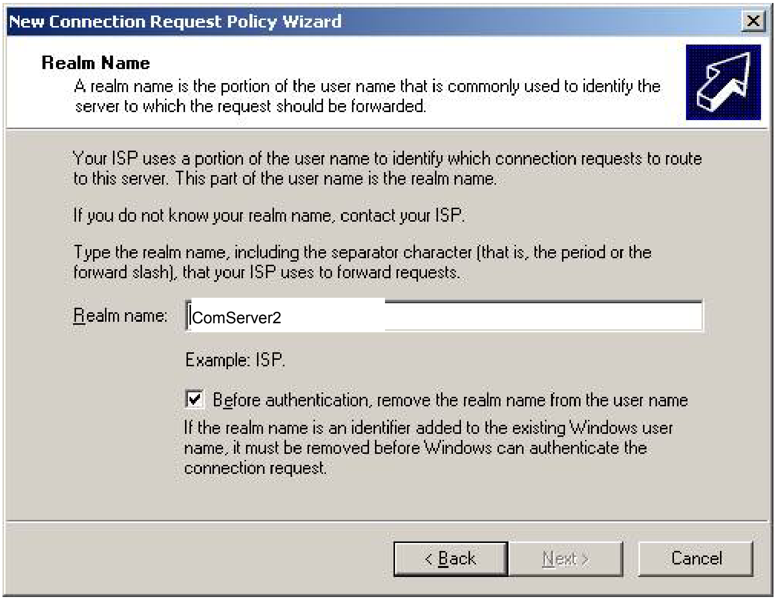
If users connect to this server through a virtual private network (VPN) or by dialing directly, do not create a policy. The IAS default policy is set up to accommodate this scenario.

To continue, click Next.

Figure 5-30 New Connection Request Policy Wizard

9. Enter the name of the Windows 2003 IAS computer RADIUS server in the **Realm name** field.

10. Click **Next** to complete the wizard setup.



Realm Name

A realm name is the portion of the user name that is commonly used to identify the server to which the request should be forwarded.

Your ISP uses a portion of the user name to identify which connection requests to route to this server. This part of the user name is the realm name.

If you do not know your realm name, contact your ISP.

Type the realm name, including the separator character (that is, the period or the forward slash), that your ISP uses to forward requests.

Realm name: ComServer2

Example: ISP.

☑ Before authentication, remove the realm name from the user name

If the realm name is an identifier added to the existing Windows user name, it must be removed before Windows can authenticate the connection request.

Figure 5-31 Realm Name

5.7.4 Example 4: Vantage RADIUS and Windows Active Directory[1]

In the following example the computer A requests access to B. Computer A is authenticated by C via a local Vantage RADIUS server using an active directory.

You can manage the Vantage RADIUS server using the same administrator login and domain name as a remote RADIUS server computer. The remote server computer must exist behind a local Vantage RADIUS server.

- Authentication requests are sent to a local Vantage RADIUS server.
- The Vantage RADIUS server searches for a server computer with the same **Domain Administrator Username**, **Domain Administrator Password** and computer **Domain Name**.

[1] At the time of writing, the Windows active directory version compatible with Vantage RADIUS is Windows 2003 IAS.

- If the administrator username, password and domain name of a computer server is found matching the same fields in the Vantage RADIUS, the wireless client is authenticated by the AP.

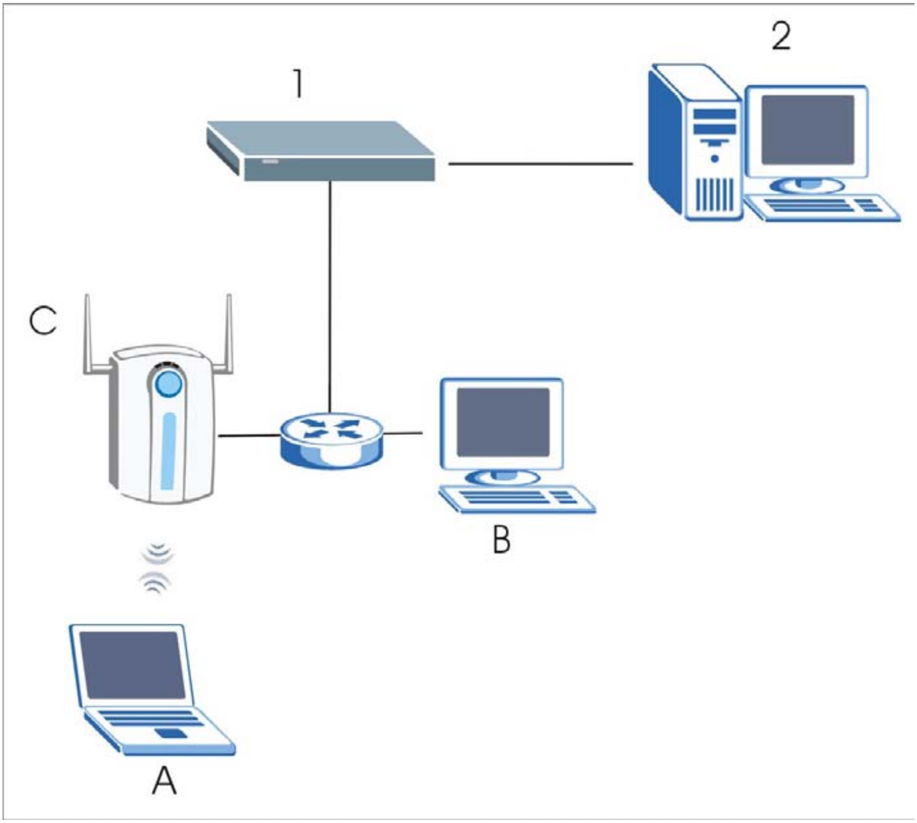


Figure 5-32 Example 4: Vantage RADIUS and Windows Active Directory

Table 5-10 Example 4: RADIUS Server User Accounts

RADIUS1
ComputerA

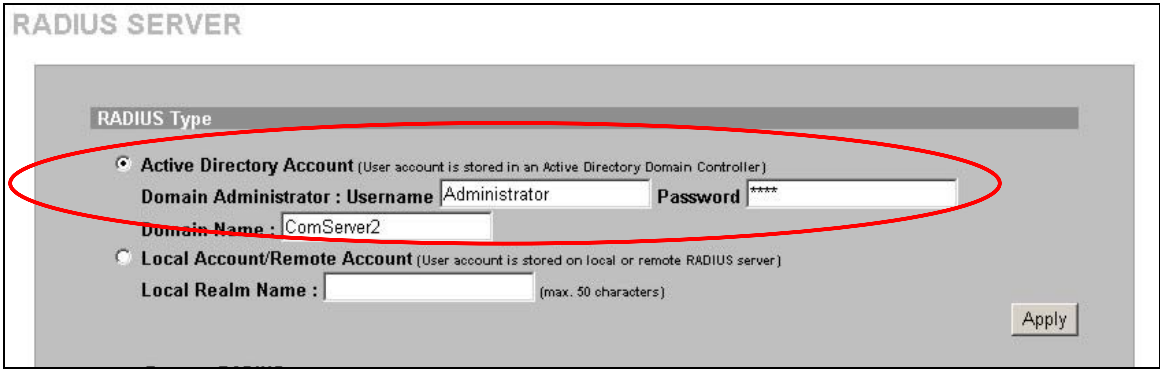
1. In the **RADIUS SERVER** screen select the **Active Directory Account** radio button.

2. In the **Domain Administrator : Username** field type the administrator login name of the Windows server computer, for example "Administrator".

3. In the **Domain Administrator : Password** field type the administrator login name of the Windows server computer, for example "5678".

4. Type the **Domain Name** of the Windows server computer. This is usually displayed in the NetBIOS setup of the Windows server computer, for example "ComServer2".

5. Click the **Apply** button.



RADIUS SERVER

RADIUS Type

● Active Directory Account (User account is stored in an Active Directory Domain Controller)

Domain Administrator : Username Administrator Password ****

Domain Name : ComServer2

○ Local Account/Remote Account (User account is stored on local or remote RADIUS server)

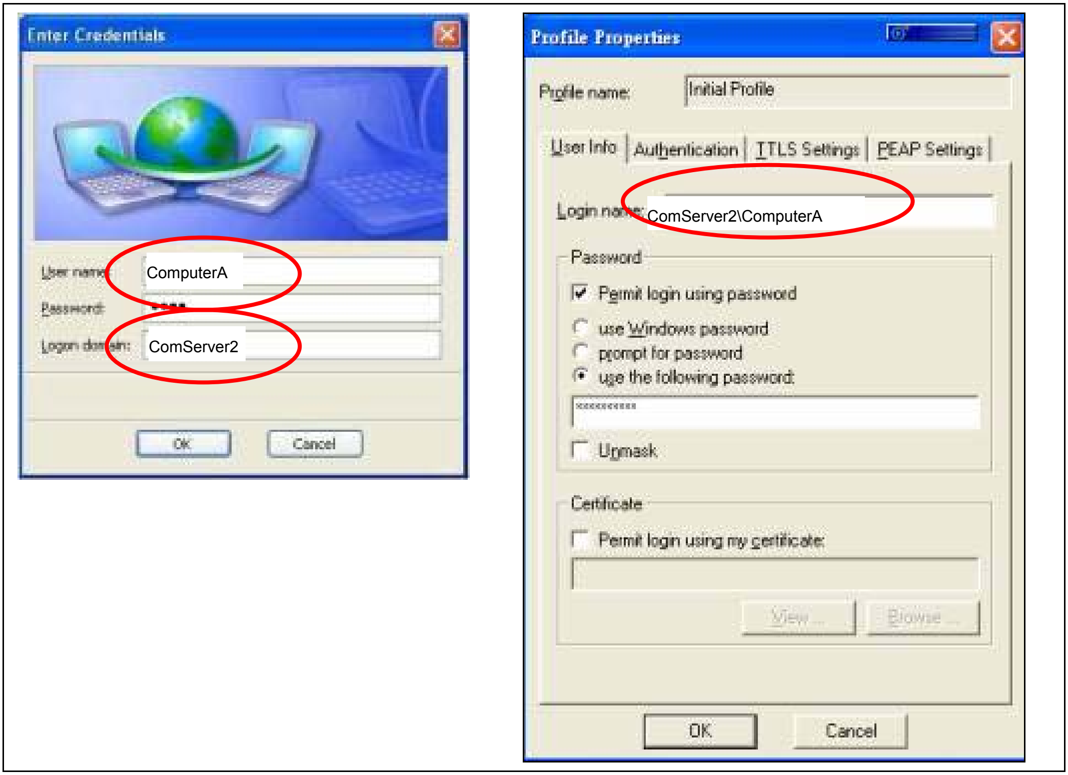
Local Realm Name : (max. 50 characters)

Figure 5-33 Example 4: Vantage RADIUS Active Directory Account Setup

Follow the steps to set up computer A.

- If computer A uses Wireless Zero Configuration utility, then type the **User name** "ComputerA" and the user account **Password**. See the section on User Account for more information. Type ComServer2 in the **Logon domain** field.

- If computer A uses Odyssey Client utility, then type the **Login name** in domain\computer format.



Enter Credentials

User name: ComputerA

Password: ****

Logon domain: ComServer2

Profile Properties

Profile name: Initial Profile

Login name: ComServer2\ComputerA

Password

☑ Permit login using password

○ use Windows password

○ prompt for password

● use the following password:

****

☐ Unmask

Certificate

☐ Permit login using my certificate:

Figure 5-34 Example 4: Using WZC or Odyssey Client: Computer A

6. If a RADIUS server computer is found with an administrator username, password and domain name that match the active directory fields configured in Vantage RADIUS

   and

   Computer A is listed as a user account with Vantage RADIUS, then computer A is authenticated by C and can successfully communicate with B.

5.8 User Account

Click **RADIUS** and then **USER ACCOUNT** to begin adding user accounts to your RADIUS server. Each client requiring access to the wireless network needs a username and password.

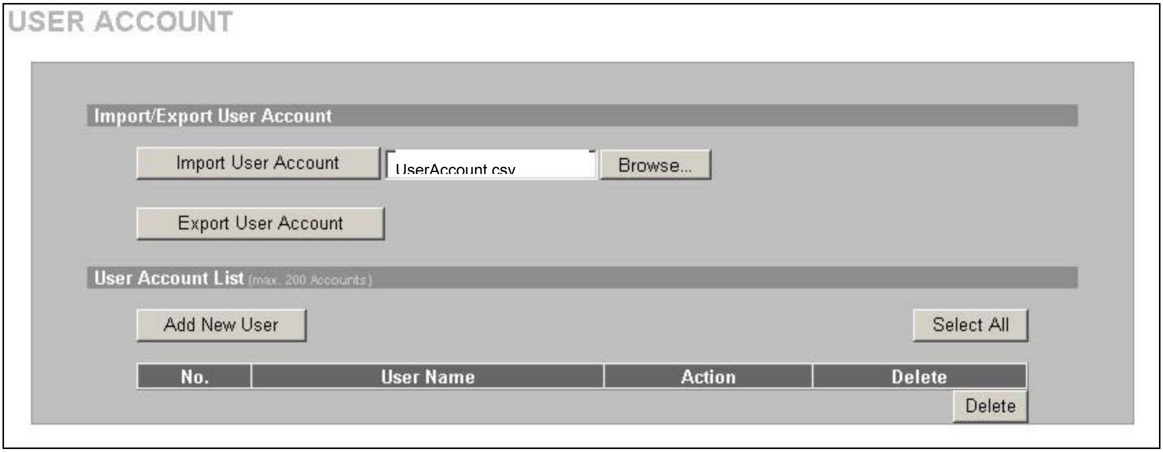


Figure 5-35 User Account

The following table describes the labels in this screen.

Table 5-11 User Account

LABEL	DESCRIPTION
Import/Export User Account	
Import User Account	You can import user names and passwords of up to 200 user accounts. Type the name of a CSV file or click the browse button to search for a CSV file on your computer. Click **Import User Account** to import the CSV file.
Export User Account	You can save a list of user names and passwords to your computer in CSV file format. When typing the name of the CSV file, the characters in the square brackets [' / " \ ] and spaces are not allowed. Click the **Export User Account** to search for a location to save the file.

Table 5-11 User Account

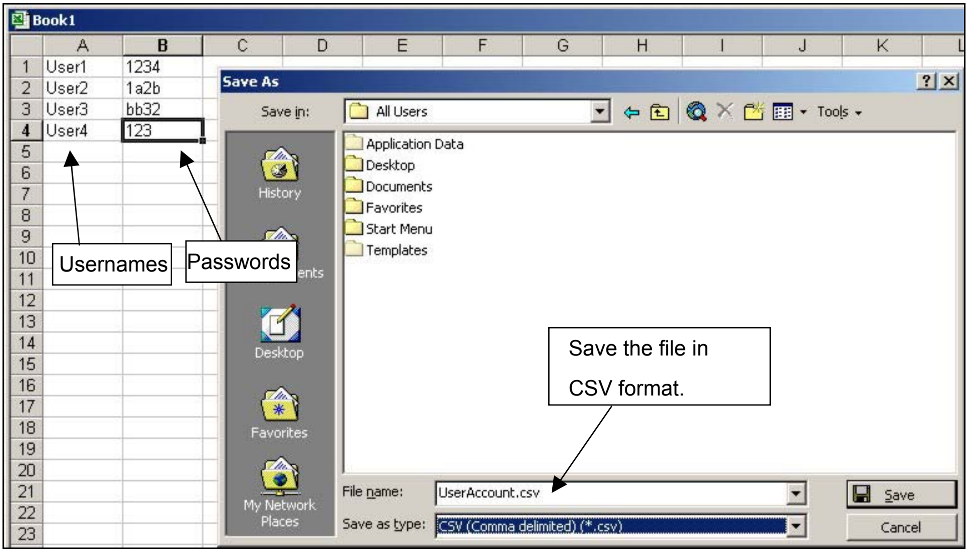
LABEL	DESCRIPTION
User Account List The maximum number of configurable accounts is 200. Vantage RADIUS allows up to 50 connections at the same time. Duplicate usernames and passwords are not allowed.	
Add New User	Click this button to add a new user account.
No.	This is the index number of a user account.
User Name	The field displays the account user name.
Action Change Password	 Click this button to modify user's password.
Select All	Click this button to select all user accounts.
Delete	Select a check box next to the user(s) you want to remove and click **Delete**.

5.8.1 CSV File

The CSV ("Comma Separated Value") file format is often used to exchange data between disparate applications. Microsoft Excel is an application that produces and uses CSV.

Microsoft Excel will *always* remove leading zeros from fields before displaying them. It will also *always* remove leading spaces.

The following screen displays an example CSV file using Microsoft Excel.



	A	B
1	User1	1234
2	User2	1a2b
3	User3	bb32
4	User4	123

Usernames

Passwords

Save the file in CSV format.

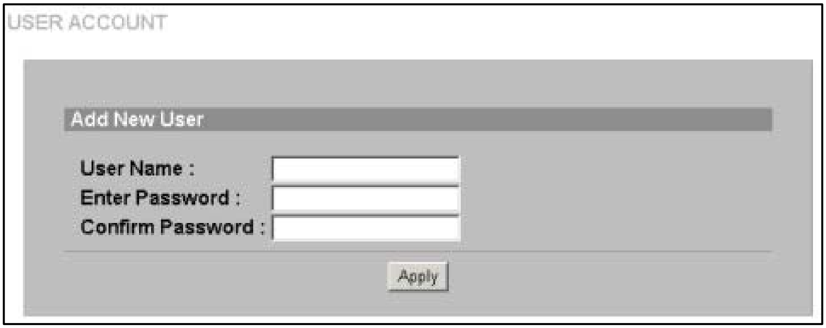
File name: UserAccount.csv

Save as type: CSV (Comma delimited) (*.csv)

Figure 5-36 CSV File Example

5.8.2 Adding a New Client

Click **Add New User** in the **USER ACCOUNT** screen to add a new client account to your Vantage RADIUS.



USER ACCOUNT

Add New User

User Name :

Enter Password :

Confirm Password :

Figure 5-37 User Account: Add New User

The following table describes the labels in this screen.

Table 5-12 User Account: Add New User

LABEL	DESCRIPTION
User Name	Type the wireless client's username. The username can consist of up to 80 alphanumeric characters and is case sensitive.
Enter Password	Type the password corresponding to the name above. The password can consist of up to 80 alphanumeric characters and is case sensitive.
Confirm Password	Type the password again for confirmation.
Apply	Click this button to save your change back to Vantage RADIUS and return to the **USER ACCOUNT** screen.

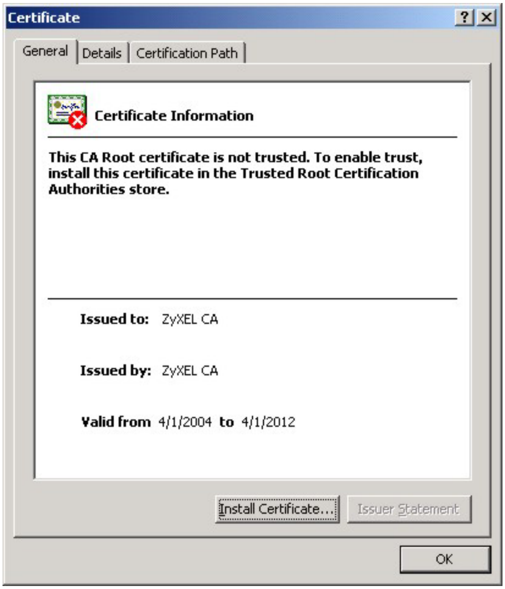
In order to authenticate your wireless client a username and password for your RADIUS account is required. If your AP uses PEAP authentication you are required to have a CA Root Certificate as well (see the *Trusted Root CA* section).

5.9 Importing A Certificate

If you download a certificate from the **ROOT CA** screen (see *section 5.4*), you need to import the certificate into every client that requires access to Vantage RADIUS.

Step 1. Double click the certificate's icon, the **Certificate Information** window displays.

Step 2. Click **Install Certificate** to open the **Certificate Import Wizard** as shown below. Then click **Next**.



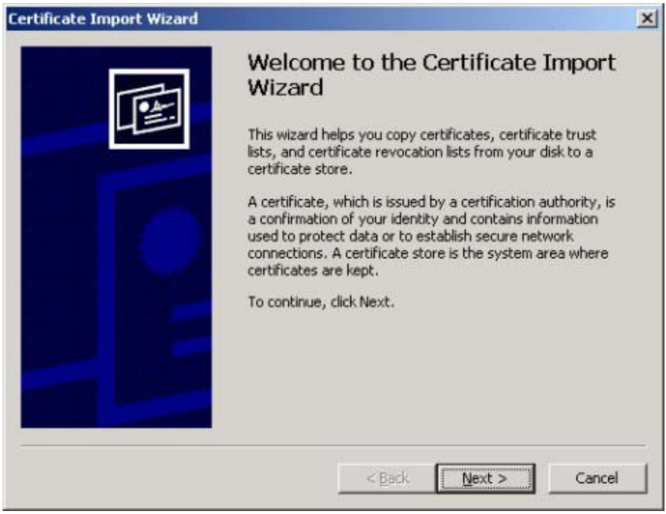
Certificate Information

This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: ZyXEL CA

Issued by: ZyXEL CA

Valid from 4/1/2004 to 4/1/2012



Welcome to the Certificate Import Wizard

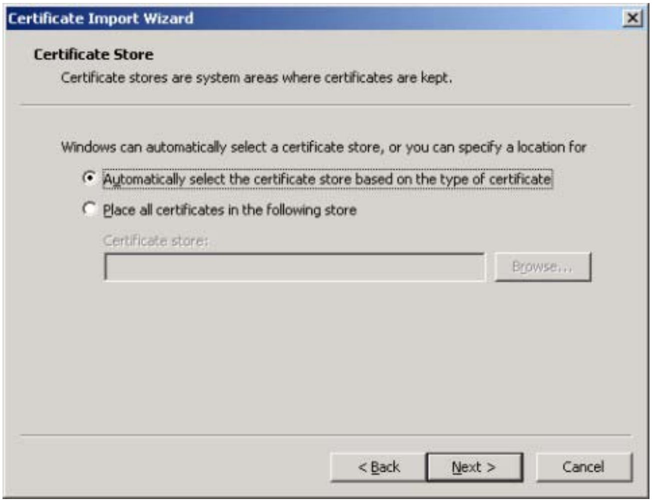
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

.

Step 3. Click **Automatically select the certificate store based on the type of certificate**, or if you prefer, specify the location for the certificate to be stored, then click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

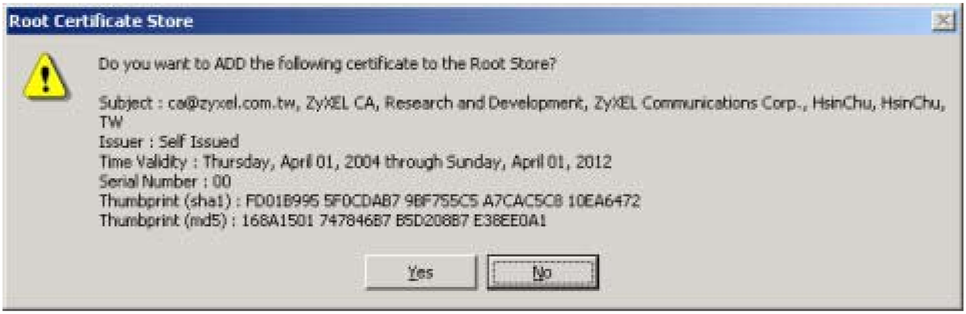
Windows can automatically select a certificate store, or you can specify a location for

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Step 4. Click **Yes** to add this certificate to your computer.

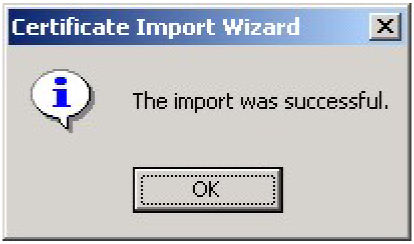


Root Certificate Store

Do you want to ADD the following certificate to the Root Store?

Subject : ca@zyxel.com.tw, ZyXEL CA, Research and Development, ZyXEL Communications Corp., HsinChu, HsinChu, TW
Issuer : Self Issued
Time Validity : Thursday, April 01, 2004 through Sunday, April 01, 2012
Serial Number : 00
Thumbprint (sha1) : FD01B995 5F0CDAB7 9BF755C5 A7CAC5C8 10EA6472
Thumbprint (md5) : 168A1501 747846B7 B5D208B7 E38EE0A1

The **Certificate Import Wizard** dialog box appears as below.



Certificate Import Wizard

The import was successful.

Step 5. Click **OK** to complete the installation.

5.10 Setting Up Your Access Point (AP)

This section assumes knowledge of how to configure a management session on your AP. The following examples use screenshots from ZyXEL's ZyAIR G-3000. Actual screens and products differ from the ones displayed. Please consult your AP's *User's Guide* before making the changes below.

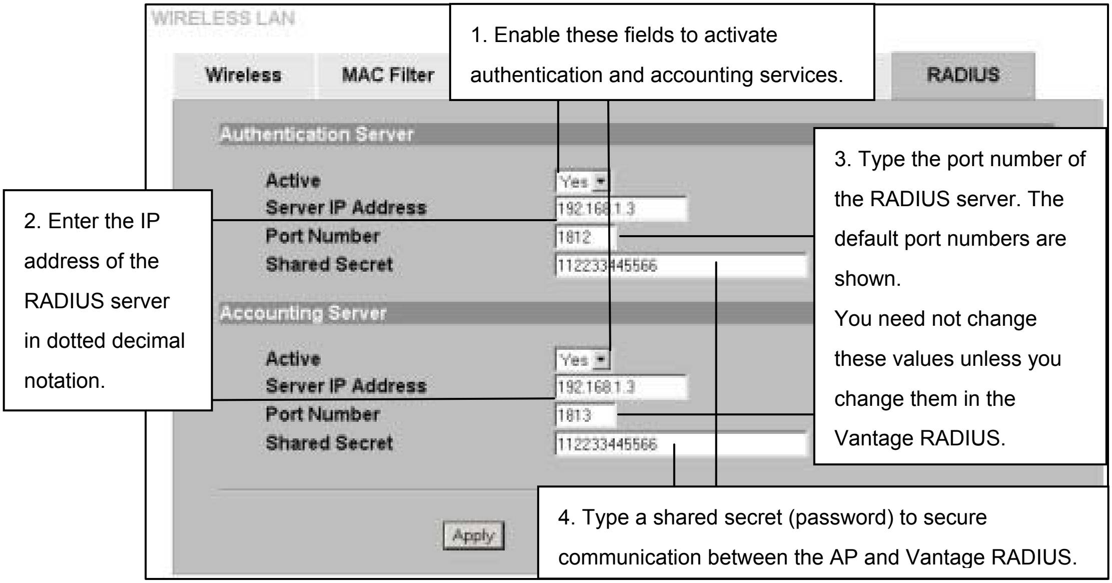
To avoid errors, make sure you first configure your access point before configuring authentication settings and wireless clients.

5.10.1 ZyAIR G-3000 RADIUS Setup Example

The following example describes how to configure your AP's RADIUS server settings for use with Vantage RADIUS.

To set up your ZyAIR's RADIUS server settings, click the **WIRELESS** link under **ADVANCED** and then the **RADIUS** tab. The screen appears as shown.

1. Make sure your RADIUS servers are activated.
2. Type the IP address of your Vantage RADIUS in the **Server IP Address** field.
3. Type the port numbers of the external authentication and accounting servers. The default port numbers are **1812** and **1813** respectively. Make sure ZyAIR and Vantage RADIUS use the same port numbers.
4. Type a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the wireless AP. The key must be the same on the external authentication server and your wireless AP. The key is not sent over the network.



Authentication Server

Active: Yes

Server IP Address: 192.168.1.3

Port Number: 1812

Shared Secret: 112233445566

Accounting Server

Active: Yes

Server IP Address: 192.168.1.3

Port Number: 1813

Shared Secret: 112233445566

1. Enable these fields to activate authentication and accounting services.

2. Enter the IP address of the RADIUS server in dotted decimal notation.

3. Type the port number of the RADIUS server. The default port numbers are shown.
You need not change these values unless you change them in the Vantage RADIUS.

4. Type a shared secret (password) to secure communication between the AP and Vantage RADIUS.

Figure 5-38 ZyAIR RADIUS Settings Example

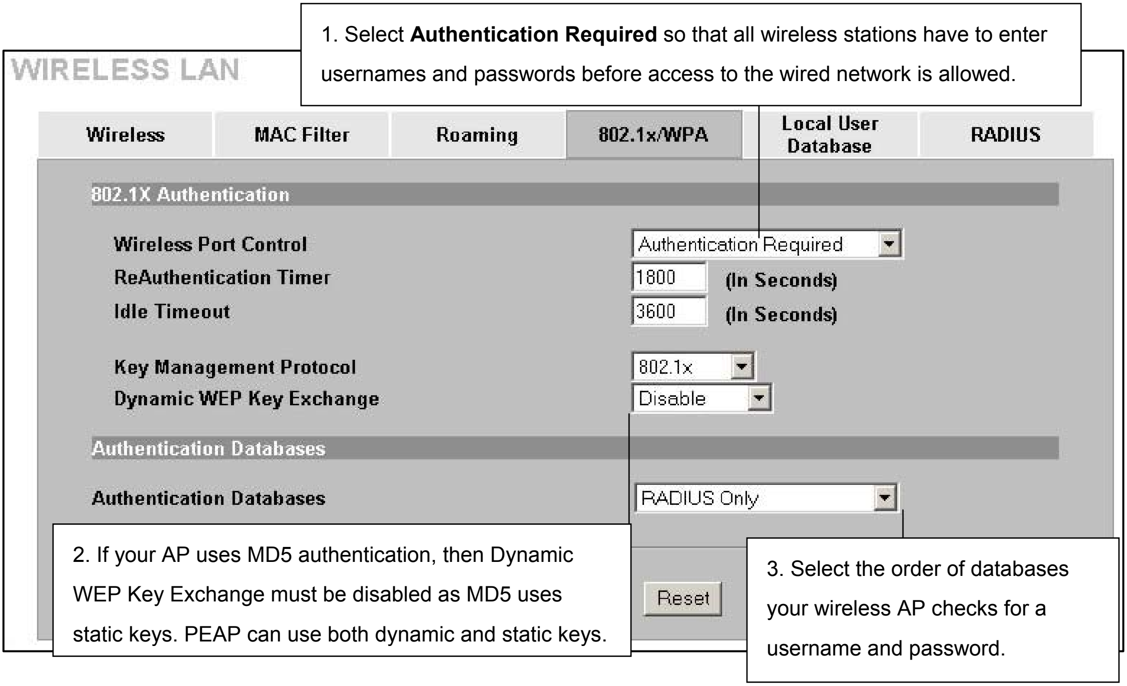
5.10.2 ZyAIR G-3000 Wireless Authentication Setup Example

The following example describes how to configure a wireless AP for use with Vantage RADIUS.

To change your ZyAIR’s authentication settings, click the **WIRELESS** link under **ADVANCED** and then the **802.1x/WPA** tab. Configure your wireless AP to enable authentication through an external authentication server (Vantage RADIUS).

If your wireless client uses MD5 authentication, either choose static key exchange, or disable dynamic key exchange.

The authentication database contains wireless station login information. Vantage RADIUS is an external authentication server. Use this drop-down list box to select the order the wireless AP checks the databases to authenticate a wireless station.



802.1X Authentication

Wireless Port Control: Authentication Required

ReAuthentication Timer: 1800 (In Seconds)

Idle Timeout: 3600 (In Seconds)

Key Management Protocol: 802.1x

Dynamic WEP Key Exchange: Disable

Authentication Databases

Authentication Databases: RADIUS Only

1. Select **Authentication Required** so that all wireless stations have to enter usernames and passwords before access to the wired network is allowed.

2. If your AP uses MD5 authentication, then Dynamic WEP Key Exchange must be disabled as MD5 uses static keys. PEAP can use both dynamic and static keys.

3. Select the order of databases your wireless AP checks for a username and password.

Figure 5-39 ZyAIR Wireless Settings Example

Part III:

Maintenance and Management

This part explains how to maintain and manage your Vantage RADIUS.

Chapter 6
Maintenance

This chapter covers system maintenance screens

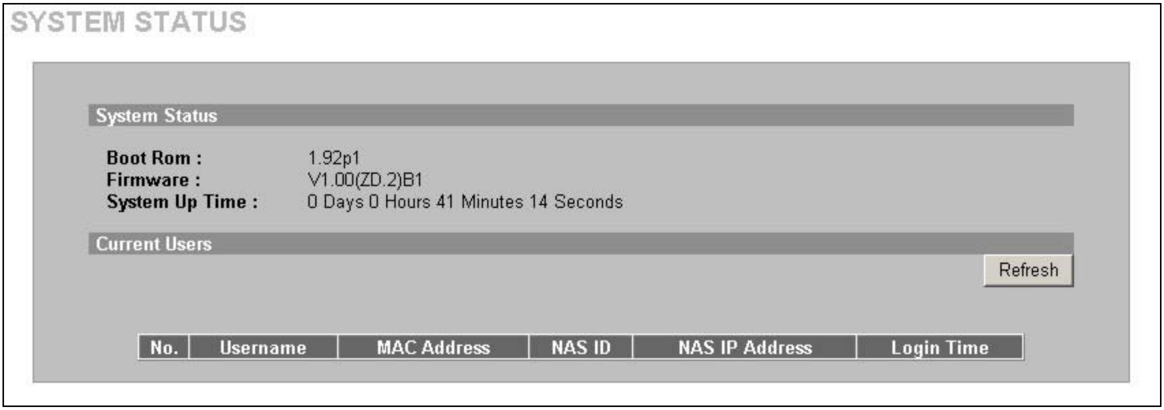
6.1 Overview

The maintenance screens can help you view system information, upload new firmware and manage your configuration.

6.2 System Status

This screen displays details about the Vantage RADIUS firmware, time running since last startup, and a list of wireless clients authenticated and currently connected to the network.

Click **MAINTENANCE** in the main menu of the web configurator, and then click **SYSTEM STATUS** to display the following screen. Note that these fields are READ-ONLY and only used for diagnostic purposes.



SYSTEM STATUS

System Status

Boot Rom : 1.92p1
Firmware : V1.00(ZD.2)B1
System Up Time : 0 Days 0 Hours 41 Minutes 14 Seconds

Current Users

No.	Username	MAC Address	NAS ID	NAS IP Address	Login Time

Figure 6-1 System Status

The following table describes the labels in this screen.

Table 6-1 System Status

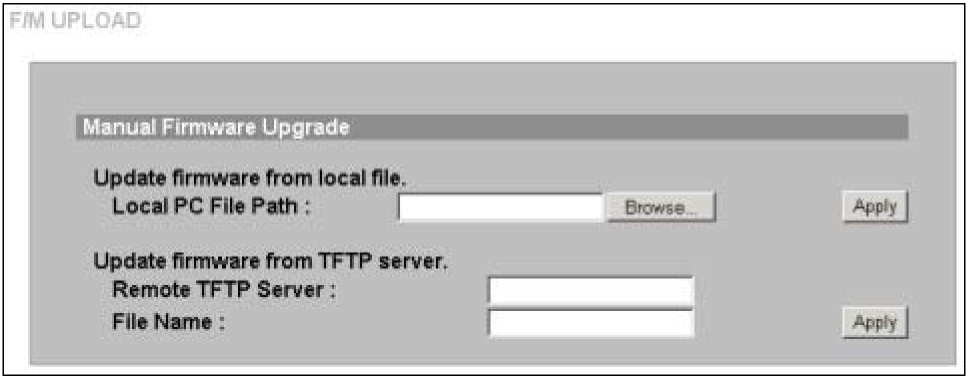
LABEL	DESCRIPTION
System Status	
Boot Rom	This field displays the Boot Rom's version number.
Firmware	This field displays the firmware version number.
System Up Time	This field displays the length of time since Vantage RADIUS server was last started.
Current Users This table lists the wireless clients currently using the network.	
Refresh	Click this button to update the **Current Users** list.
No.	This field displays the index number of an entry.
Username	This field displays the wireless client's username.
MAC Address	This field displays the MAC address.
NAS ID	This field displays the wireless client's IP address.
NAS IP Address	This field displays the IP address of the wireless AP that the wireless client uses to access the network.
Login Time	This field displays the length of time the wireless client is connected for.

6.3 Firmware Upload

Find the latest firmware at www.ZyXEL.com in a file that uses the system model name with a "*.bin" extension, e.g., "Vantage.bin". The upload process may take up to two minutes. After a successful upload, the system will reboot.

Only use firmware for your Vantage RADIUS specific model. Refer to the label on the bottom of your Vantage RADIUS.

Click **MAINTENANCE**, and then **F/W UPLOAD** from the main menu. Follow the instructions in this screen to upload firmware to your Vantage RADIUS.



F/M UPLOAD

Manual Firmware Upgrade

Update firmware from local file.

Local PC File Path :

Update firmware from TFTP server.

Remote TFTP Server :

File Name :

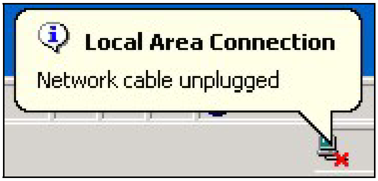
Figure 6-2 F/W Upload

The following table describes the fields in this screen.

Figure 6-3 F/W Upload

LABEL	DESCRIPTION
Update firmware from local file.	
Local PC File Path	Type in the location of the file you want to upload in this field or click **Browse** to find it.
Browse...	Click this button to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Apply	Click this button to begin the upload process. This process may take up to two minutes.
Update firmware from TFTP server. Use this feature to have Vantage RADIUS automatically update the firmware.	
Remote TFTP Server	Type the IP address of your TFTP server.
File Name	Type the filename of the firmware to upload.
Apply	Click this button to start the upload process.

Do not turn off Vantage RADIUS while firmware upload is in progress!

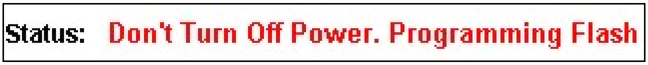


Local Area Connection

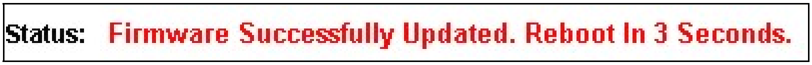
Network cable unplugged

Figure 6-4 Network Temporarily Disconnected

The following messages display at the bottom of the screen.



Status: Don't Turn Off Power. Programming Flash

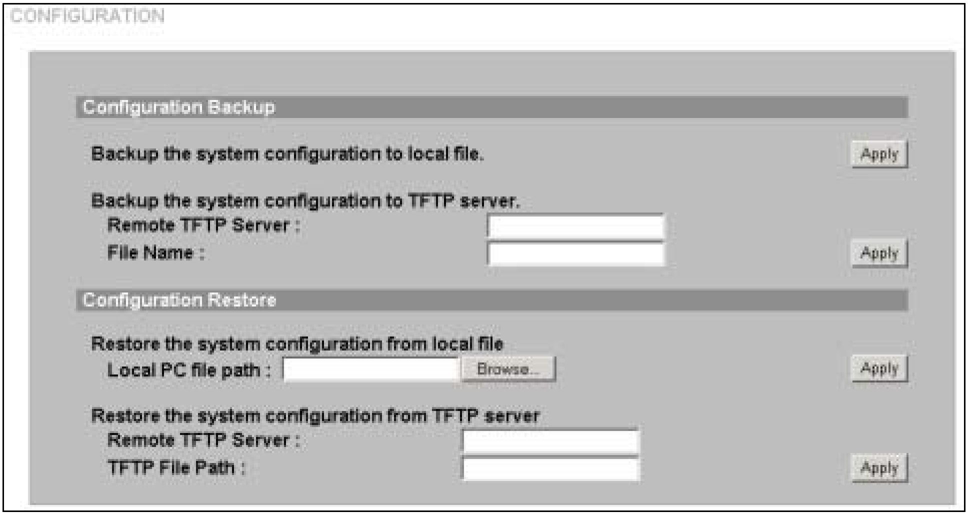


Status: Firmware Successfully Updated. Reboot In 3 Seconds.

Wait for about two minutes, log in again and check your new firmware version in the **SYSTEM STATUS** screen.

6.4 Configuration

Click **MAINTENANCE**, and then the **Configuration** tab. Use this screen to backup or restore Vantage RADIUS configuration.



CONFIGURATION

Configuration Backup

Backup the system configuration to local file.

Backup the system configuration to TFTP server.

Remote TFTP Server :

File Name :

Configuration Restore

Restore the system configuration from local file

Local PC file path :

Restore the system configuration from TFTP server

Remote TFTP Server :

TFTP File Path :

Figure 6-5 Configuration Backup

6.4.1 Configuration Backup

Configuration Backup allows you to backup (save) the current system (Vantage RADIUS) configuration to your computer or a TFTP server. Backup is highly recommended once your Vantage RADIUS is functioning properly.

Table 6-2 Configuration Backup

LABEL	DESCRIPTION
Configuration Backup	
Backup the system configuration to a local file.	
Apply	Click this button to begin the backup process to your computer.
Backup the system configuration to TFTP server.	
Remote TFTP Server	Type the IP address of the TFTP server.
File Name	Type the filename of the file to backup.
Apply	Click this button to begin the backup process.

6.4.2 Configuration Restore

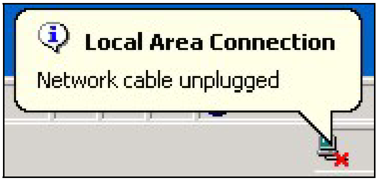
Restore Configuration allows you to restore a previously saved configuration file from your computer to your Vantage RADIUS.

Table 6-3 Configuration Restore

LABEL	DESCRIPTION
Restore the system configuration from local file	
Local PC File Path	Type in the location of the file you want to restore in this field or click **Browse** to find it.
Browse	Click **Browse** to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Apply	Click this button to begin the upload process.
Restore the system configuration from TFTP server.	
Remote TFTP Server	Type the IP address of the TFTP server.
TFTP File Path	Type the path and filename of the file to restore.
Apply	Click this button to begin the restore process.

Do not turn off the device while configuration file upload is in progress.

After you see a "configuration upload successful" screen, you must then wait for about one minute before logging into the device again.



Local Area Connection

Network cable unplugged

Figure 6-6 Network Temporarily Disconnected

If you uploaded the default configuration file you may need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.3). See your *Quick Start Guide* or the *Appendices* for details on how to set up your computer's IP address.

Chapter 7
Management

This chapter details how to configure your Vantage RADIUS for remote access

7.1 Remote Management Overview

Remote management allows you to determine which services/protocols can access which Vantage RADIUS interface (if any) from which computers.

To disable remote management of a service, select **Disable** in the corresponding field.

You may only have one remote management session running at a time. Vantage RADIUS automatically disconnects a remote management session of lower priority when another remote management session of higher priority starts. The priorities for the different types of remote management sessions are as follows.

1. Console port
2. SSH
3. Telnet
4. HTTPS and HTTP

7.1.1 Remote Management Limitations

Remote management will not work when:

1. You have disabled that service in the remote management screen.
2. The client IP address does not correspond to an **Allowed IP Address** or an **Allowed Network Address**. If it does not match, Vantage RADIUS will disconnect the session immediately.
3. There is already another remote management session with an equal or higher priority running. You may only have one remote management session running at one time.

7.1.2 System Timeout

There is a system timeout of five minutes (three hundred seconds) for either the console port or telnet/web/FTP connections. Your Vantage RADIUS automatically logs you out if you do nothing in this timeout period. See the **REMOTE ACCESS** screen to change the timeout period in the **Idle Time Out** field.

7.2 Introduction to 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).

HTTPS on Vantage RADIUS is used so that you may securely access Vantage RADIUS using the web configurator.

Please refer to the following figure.

1. HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on Vantage RADIUS's WS (web server).
2. HTTP connection requests from a web browser go to port 80 (by default) on Vantage RADIUS's WS (web server).

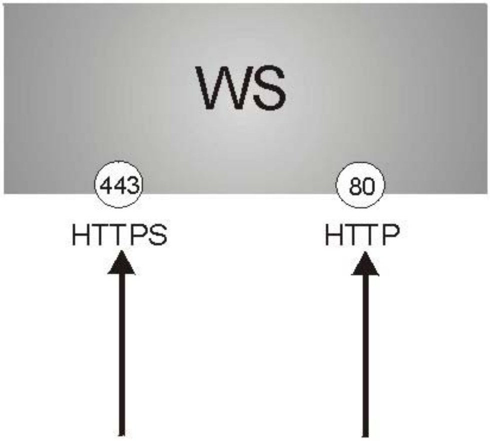


Figure 7-1 HTTPS Implementation

If you disable HTTP (Disable**) in the** REMOTE ACCESS **screen, then Vantage RADIUS blocks all HTTP connection attempts.**

7.3 SSH

Unlike Telnet, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

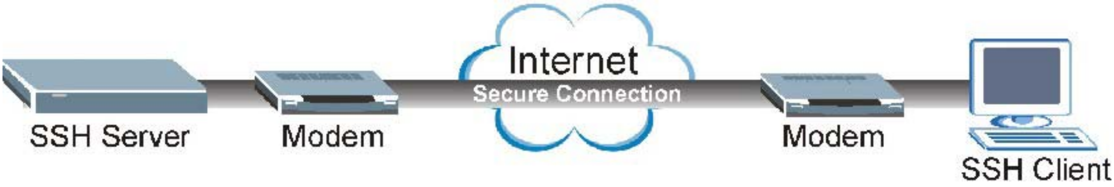


Figure 7-2 SSH Communication Example

7.3.1 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

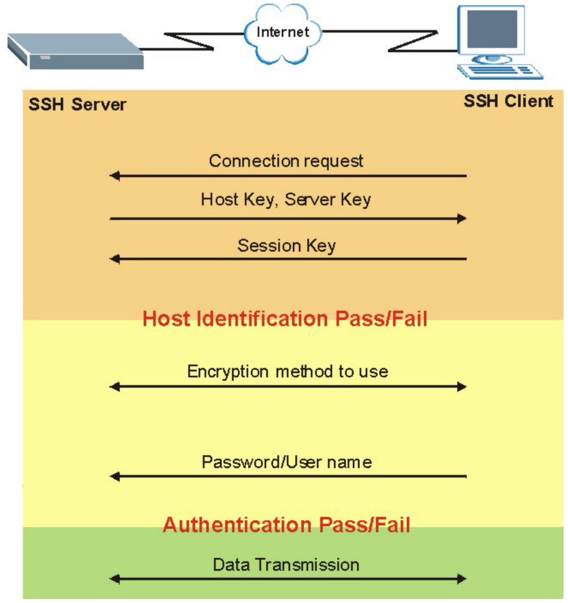
<table>
<tr><td rowspan="3">

Figure 7-3 How SSH Works</td>
<td><b>1. Host Identification</b>
The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.
The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.</td></tr>
<tr><td><b>2. Encryption Method</b>
Once the identification is verified, both the client and server must agree on the type of encryption method to use.</td></tr>
<tr><td><b>3. Authentication and Data Transmission</b>
After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.</td></tr>
</table>

7.3.2 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to Vantage RADIUS over SSH.

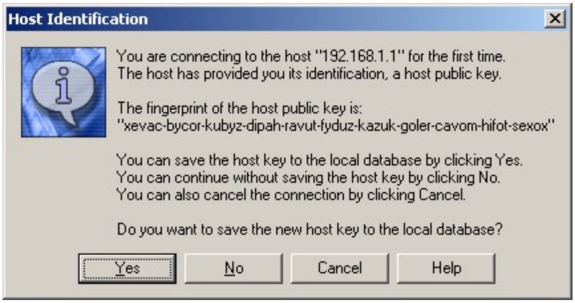
7.4 Secure Telnet Using SSH Examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access Vantage RADIUS. The configuration and connection steps are similar for most SSH client programs. Refer to your SSH client program user’s guide.

7.4.1 Example 1: Microsoft Windows

This section describes how to access Vantage RADIUS using the Secure Shell Client program.

1. Launch the SSH client and specify the connection information (IP address, port number or device name) for Vantage RADIUS.
2. Configure the SSH client to accept connection using SSH version 1.
3. A window displays prompting you to store the host key in you computer. Click **Yes** to continue.



Host Identification

You are connecting to the host "192.168.1.1" for the first time.
The host has provided you its identification, a host public key.

The fingerprint of the host public key is:
"xevac-bycor-kubyz-dipah-ravut-fyduz-kazuk-goler-cavom-hifot-sexox"

You can save the host key to the local database by clicking Yes.
You can continue without saving the host key by clicking No.
You can also cancel the connection by clicking Cancel.

Do you want to save the new host key to the local database?

Figure 7-4 SSH Example 1: Store Host Key

4. Enter the password to log in to Vantage RADIUS. The command prompt **Vantage>** displays next.

7.4.2 Example 2: Linux

This section describes how to access Vantage RADIUS using the OpenSSH client program that comes with most Linux distributions.

1. Test whether the SSH service is available on Vantage RADIUS.
2. Enter "`telnet 192.168.1.1 22`" at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on Vantage RADIUS (using the default IP address of 192.168.1.3).

   A message displays indicating the SSH protocol version supported by Vantage RADIUS.

```
$ telnet 192.168.1.1 22
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
SSH-1.5-1.0.0
```

Figure 7-5 SSH Example 2: Test

3. Enter "`ssh –2 192.168.1.3`". This command forces your computer to connect to Vantage RADIUS using SSH version 1. If this is the first time you are connecting to Vantage RADIUS using SSH, a message displays prompting you to save the host information of Vantage RADIUS. Type "`yes`" and press [ENTER].
4. Now enter the password to log in to Vantage RADIUS.

```
$ ssh -1 192.168.1.3
The authenticity of host '192.168.1.3 (192.168.1.3)' can't be established.
RSA1 key fingerprint is 21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.3' (RSA1) to the list of known hosts.
Administrator@192.168.1.3's password:
```

Figure 7-6 SSH Example 2: Log in

7.5 Telnet

You can configure your Vantage RADIUS for remote Telnet access as shown next.

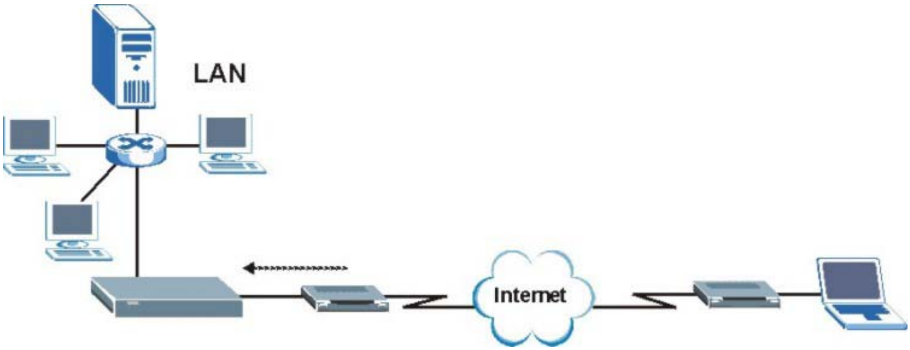
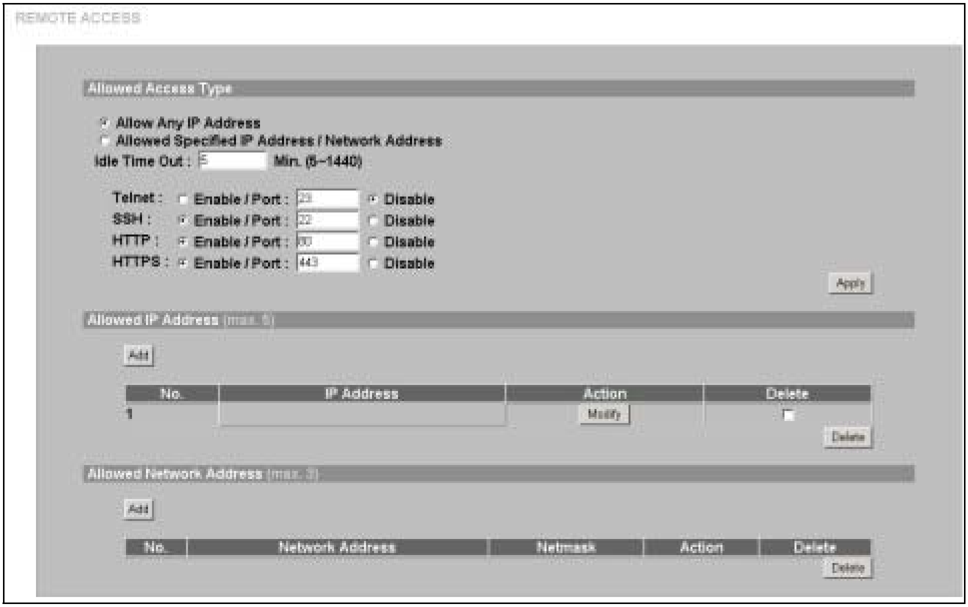


Figure 7-7 Telnet Configuration on a TCP/IP Network

7.6 Remote Access

To configure your Vantage RADIUS for remote access, click **MANAGEMENT** in the main menu, and then click **REMOTE ACCESS**.



REMOTE ACCESS

Allowed Access Type

● Allow Any IP Address
○ Allowed Specified IP Address / Network Address

Idle Time Out : 5 Min. (5~1440)

Telnet :	☐ Enable / Port :	23	● Disable
SSH :	● Enable / Port :	22	○ Disable
HTTP :	● Enable / Port :	80	○ Disable
HTTPS :	● Enable / Port :	443	○ Disable

Allowed IP Address (max. 5)

No.	IP Address	Action	Delete
1		Modify	☐

Allowed Network Address (max. 3)

No.	Network Address	Netmask	Action	Delete

Figure 7-8 Remote Access

Table 7-1 Remote Access

LABEL	DESCRIPTION
Allowed Access Type	
Allow Any IP Address	Enable this field to have Vantage RADIUS accept connections from all incoming IP addresses.
Allow Specified IP Address / Network Address	Enable this field to have Vantage RADIUS restricts access to the list of network addresses and IP addresses in the **Allow IP Address** and **Allowed Network Address** lists.
Idle Time Out	The default timeout is five minutes for either the console port or telnet/web/FTP connections. Type the length of time a connection can idle before Vantage RADIUS disconnects.
Telnet	**Enable** this field to allow telnet access to the Vantage RADIUS. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.

Table 7-1 Remote Access

LABEL	DESCRIPTION
SSH	SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network. **Enable** this field to allow SSH access to the Vantage RADIUS. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management
HTTP	**Enable** this field to allow Internet (Web Configurator) access to the Vantage RADIUS. You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
HTTPS	**Enable** this field to allow secure Internet (Web Configurator) access to the Vantage RADIUS. The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number, for example **8443**, then you must notify people who need to access the web configurator to use “https://Vantage RADIUS IP Address:**8443**” as the URL.
Allowed IP Address This list displays IP addresses of clients that are allowed to use the enabled (see above) remote services to access Vantage RADIUS.	
Add	Click this button to insert a new entry into the **Allowed IP Address** list.
No.	This field displays the index number.
IP Address	This field displays the IP address of a client that is allowed to use the remote access services to manage Vantage RADIUS.
Action	Click the **Modify** button in this field to edit the IP address for this entry.
Delete	Select the check box(es) next to the IP address(es) you want removed and then click **Delete**.
Delete	Click this button to delete the IP address(es) you selected in the **Allowed IP Address** list.
Allowed Network IP Address	
Add	Click this button to insert a new entry into the **Allowed IP Address** list.

Table 7-1 Remote Access

LABEL	DESCRIPTION
No.	This field displays the index number.
Network IP Address	This field displays the network address in which a client is allowed to use the services to manage Vantage RADIUS.
Netmask	This field displays the subnet mask used to specify the network range limits for accepted IP addresses.
Action	Click the **Modify** button in this field to edit the IP address for this entry.
Delete	Select the check box(es) next to the IP address(es) you want removed and then click **Delete**.
Delete	Click this button to delete the IP address(es) you selected in the **Allowed IP Address** list.

7.6.1 Insert/Modify Allowed IP Address

In the **REMOTE ACCESS** screen, click **Add** to insert a new entry in the **Allowed IP Address** list. To edit an existing entry, click the **Modify** button next to a Network IP address you want to change.

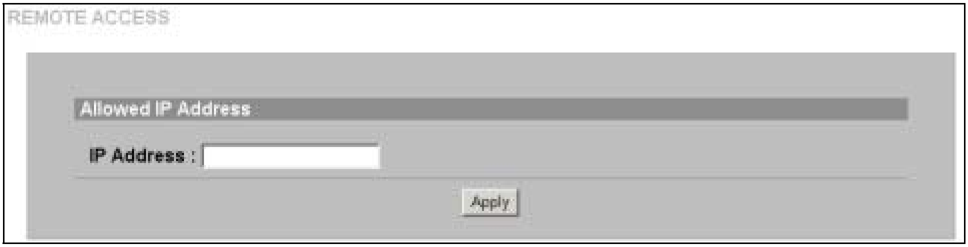


Figure 7-9 Remote Access: Add/Modify IP Address

The following table describes the fields in this screen.

Table 7-2 Remote Access: Add/Modify IP Address

LABEL	DESCRIPTION
Allowed IP Address	
IP Address	Type the IP address in dotted decimal notation of an acceptable computer.

Table 7-2 Remote Access: Add/Modify IP Address

LABEL	DESCRIPTION
Apply	Click this button to save changes back to Vantage RADIUS and return to the **REMOTE ACCESS** screen.

7.6.2 Insert/Modify Allowed Network IP Address

In the **REMOTE ACCESS** screen, click **Add** to insert a new entry in the **Allowed Network IP Address** list,. To edit an existing entry, click the **Modify** button next to a Network IP address you want to change.

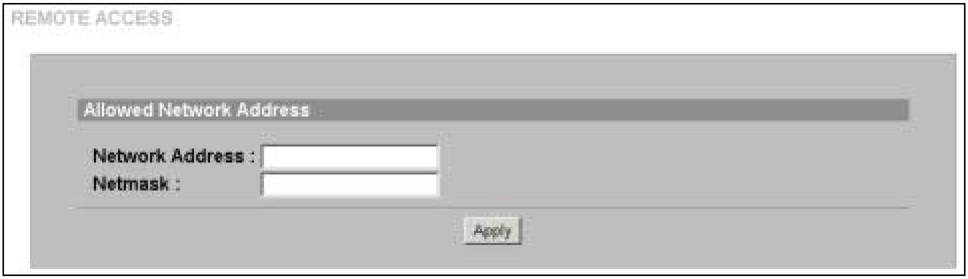


Figure 7-10 Remote Access: Add/Modify Network IP Address

The following table describes the fields in this screen.

Table 7-3 Remote Access: Add/Modify Network IP Address

LABEL	DESCRIPTION
Allowed Network Address	
Network Address	Type the first address in your network. This is the start address from which Vantage RADIUS uses the **Netmask** to allow access from many IP addresses.
Netmask	Type the subnet mask used to specify the network range limits for accepted IP addresses.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **REMOTE ACCESS** screen.

7.7 SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your Vantage RADIUS supports SNMP agent functionality, which allows a manager station to manage and monitor Vantage RADIUS through the network. Vantage RADIUS supports SNMP version one (SNMPv1). The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

SNMP is only available if TCP/IP is configured.

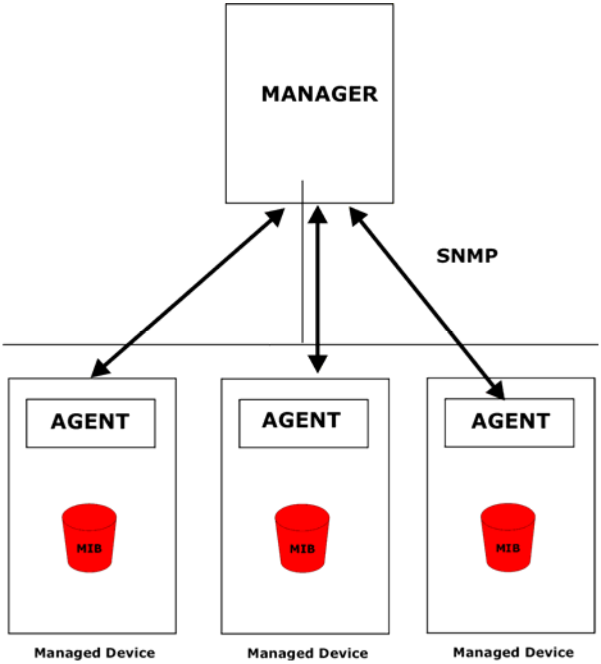


Figure 7-11 SNMP Management Model

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

An agent is a management software module that resides in a managed device (Vantage RADIUS). An agent translates the local management information from the managed device 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 device. Examples of variables include such as number of packets received, node port status etc. 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:

- 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.

7.7.1 Supported MIBs

Vantage RADIUS supports MIB II that is defined in RFC-1213 and RFC-1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

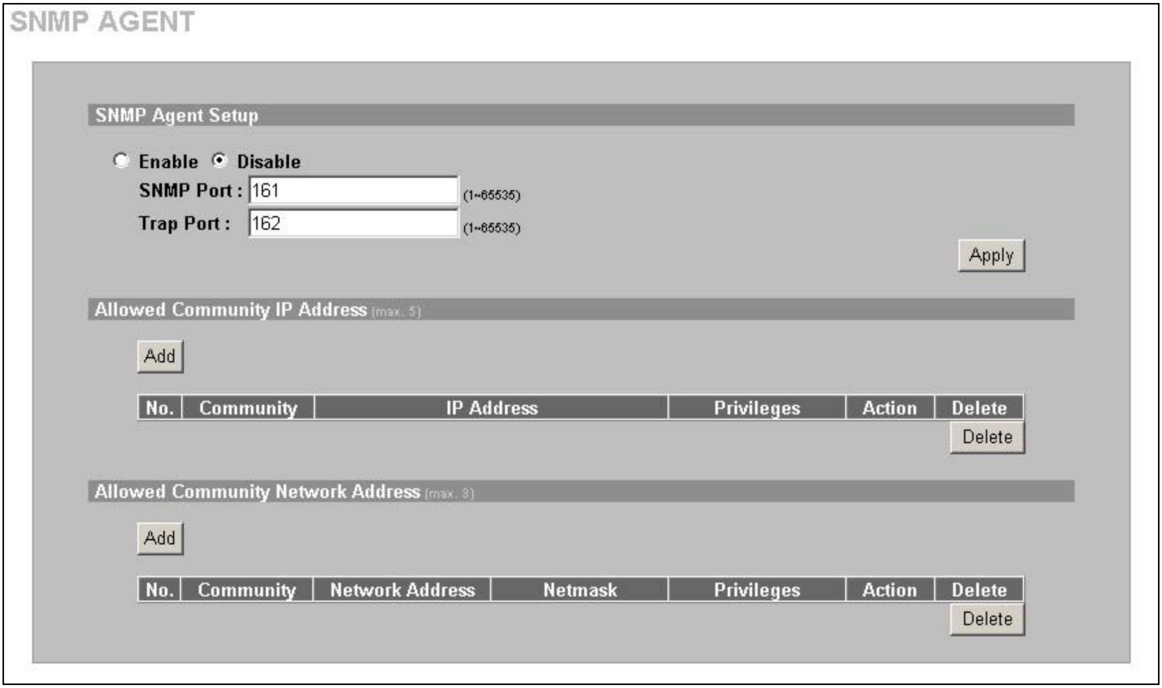
7.7.2 SNMP Traps

Vantage RADIUS sends traps to the SNMP manager when the following event occurs: Currently a single trap is available.

- ➢ warmStart (defined in *RFC-1215*). A trap is sent after booting (software reboot).

7.8 Configuring SNMP[1]

To configure your SNMP settings, click **MAINTENANCE** in the main menu, and then click **SNMP AGENT**.



SNMP AGENT

SNMP Agent Setup

○ Enable ● Disable

SNMP Port : 161 (1~65535)

Trap Port : 162 (1~65535)

Allowed Community IP Address (max. 5)

No.	Community	IP Address	Privileges	Action	Delete

Allowed Community Network Address (max. 3)

No.	Community	Network Address	Netmask	Privileges	Action	Delete

Figure 7-12 SNMP Agent

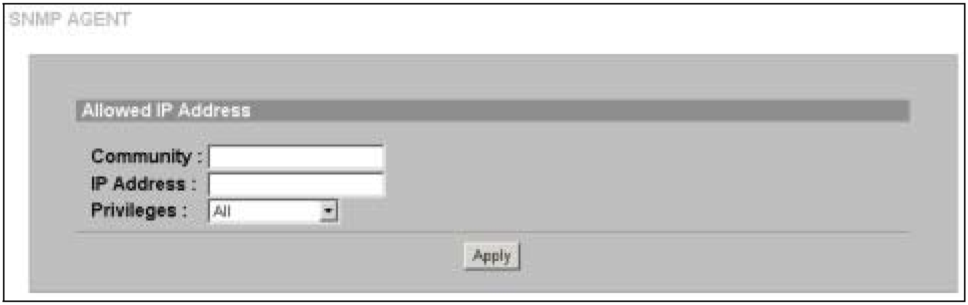
[1] At the time of writing, SNMP only has write access to the **IP** screen in the **ADVANCED** menu.

Table 7-4 SNMP Agent

LABEL	DESCRIPTION
SNMP Agent Setup	
Enable	Click this radio button to allow SNMP access to Vantage RADIUS.
Disable	Click this radio button to have Vantage RADIUS ignore SNMP requests.
SNMP Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Trap Port	You may change the server port number for a service if needed, however you must use the same port number in order to use that service for remote management.
Allowed Community IP Address	
Add	Click this button to insert a new trusted IP address to this list.
No.	This field displays a running count of entries in this list.
Community	This field displays the community, which is the password sent with each request to the SNMP manager. The default is public and allows all requests.
IP Address	Vantage RADIUS only responds to SNMP messages from the address displayed in this field.
Privileges	This field displays whether or not this entry has read or write SNMP access.
Action	Click the **Modify** button next to an entry in this list to edit that entry.
Delete	Click this button to remove a trusted network IP address from the list.
Allowed Community Network IP Address	
Add	Click this button to insert a new trusted network to this list.
No.	This field displays a running count of entries in this list.
Community	This field displays the community, which is the password sent with each request to the SNMP manager. The default is public and allows all requests.
Network IP Address	Vantage RADIUS only responds to SNMP messages from addresses inside the network displayed in this field.
Netmask	This field displays the subnet mask used to specify the network range limits for accepted IP addresses.
Privileges	This field displays whether or not this entry has read or write SNMP access.
Action	Click the **Modify** button next to an entry in this list to edit that entry.
Delete	Click this button to remove a trusted network IP address from the list.

7.8.1 Insert/Modify Allowed IP Address

In the **SNMP AGENT** screen, click **Add** to insert a new entry in the **Allowed IP Address** list. To edit an existing entry, click the **Modify** button next to an IP address you want to change.



SNMP AGENT

Allowed IP Address

Community :

IP Address :

Privileges : All

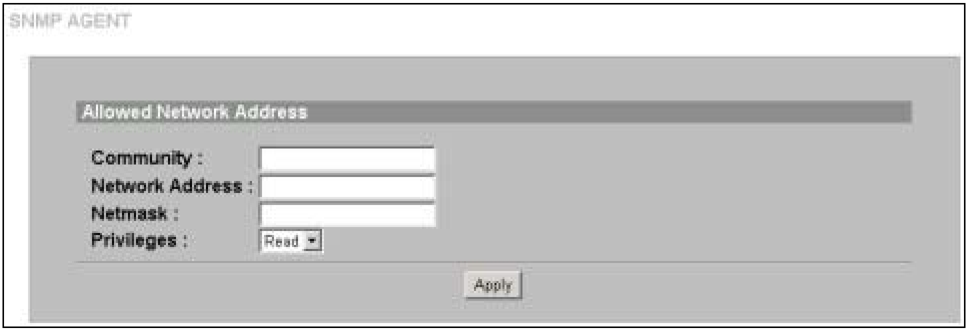
Figure 7-13 SNMP: Allowed IP Address

Table 7-5 SNMP: Allowed IP Address

LABEL	DESCRIPTION
Allowed Network Address	
Community	Type the community, which is the password sent with each request to the SNMP manager. The default is public and allows all requests.
IP Address	Type the IP address in dotted decimal notation of an allowed computer
Privileges	Select **Write**, **Read, Trap Recipients** or **All** from the drop-down list box to allow reading and writing via SNMP.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **SNMP AGENT** screen.

7.8.2 Insert/Modify Allowed Network IP Address

In the **SNMP AGENT** screen, to insert a new entry in the **Allowed Network IP Address** list, click **Add** in that section. To edit an existing entry, click the **Modify** button next to an IP address you want to change.


SNMP AGENT

Allowed Network Address

Community :

Network Address :

Netmask :

Privileges : Read

Figure 7-14 SNMP: Allowed Network Address

Table 7-6 SNMP: Allowed Network Address

LABEL	DESCRIPTION
Allowed Network Address	
Community	Type the community, which is the password sent with each request to the SNMP manager. The default is public and allows all requests.
Network Address	Type the first address in your network. This is the start address from which Vantage RADIUS uses the **Netmask** to allow access to many clients.
Netmask	Type the subnet mask used to specify the network range limits for accepted IP addresses.
Privileges	Select **Write**, or **Read** from the drop-down list box to allow reading and writing via SNMP.
Apply	Click this button to save changes back to Vantage RADIUS and return to the **SNMP AGENT** screen.

7.9 User Trace Records

See the chapter on *System Logs* for the screen detailing how to monitor wireless clients.

Chapter 8
RESET and RESTART Vantage RADIUS

This chapter details how to reset and restart your Vantage RADIUS

8.1 Resetting Vantage RADIUS

If you forget your password or cannot access the web configurator, you will need to reload the factory-default configuration file or use the RESET button on the side panel of the ZyAIR. Uploading this configuration file replaces the current configuration file with the factory-default configuration file. This means that you will lose all configurations that you had previously. The username will be reset to ADMIN and the password will be reset to 1234.

8.2 Procedure To Use The Reset Button

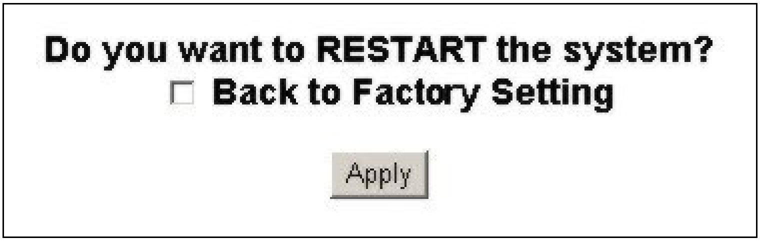
Make sure the SYS LED is on (not blinking) before you begin this procedure.

1. Press the RESET button for ten seconds or until the SYS LED and PWR LED turns red, and then release it. If the SYS LED begins to blink, the defaults have been restored and the Vantage RADIUS restarts. Otherwise, go to step 2.
2. Turn the Vantage RADIUS off (disconnect the device from the power source).
3. While pressing the RESET button, turn the Vantage RADIUS on (connect the device to the power source).
4. Continue to hold the RESET button. The SYS LED will begin to blink and flicker very quickly after about 20 seconds. This indicates that the defaults have been restored and Vantage RADIUS is now restarting.
5. Release the RESET button and wait for the Vantage RADIUS to finish restarting.

8.3 Back to Factory Defaults

The following screen allows you to reset Vantage RADIUS back to the default configuration file without turning the power off or using the RESET button.

1. Click **RESTART/RESET** in the main menu.
2. Select the check box and then click **Apply**.



Do you want to RESTART the system?

□ Back to Factory Setting

Figure 8-1 RESTART/RESET

Part IV:

APPENDICES

This part provides troubleshooting and background information about setting up your computer's IP address, wireless LAN, 802.1x and IP subnetting. It also provides information on the command interpreter interface.

Appendix A Troubleshooting

This appendix covers potential problems and possible remedies. After each problem description, some instructions are provided to help you to diagnose and to solve the problem.

Problems Starting Up Vantage RADIUS

Chart A-1 Troubleshooting the Start-Up of Your Vantage RADIUS

PROBLEM	CORRECTIVE ACTION
None of the LEDs turn on when I plug in the power adaptor.	Make sure you are using the supplied power adaptor and that it is plugged in to an appropriate power source. Check that the power source is turned on. If the problem persists, you may have a hardware problem. In this case, you should contact your local vendor.
Vantage RADIUS reboots automatically sometimes.	The supplied power to Vantage RADIUS is too low. Check that Vantage RADIUS is receiving enough power. Make sure the power source is working properly.

Problems with the Ethernet Interface

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
Cannot access Vantage RADIUS from the LAN.	If the **ETHERNET** LED on the front panel is off, check the Ethernet cable connection between your Vantage RADIUS and the Ethernet device connected to the **ETHERNET** port. Check for faulty Ethernet cables. Make sure your computer's Ethernet adapter is installed and working properly. Check the IP address of the Ethernet device. Verify that the IP address and the subnet mask of Vantage RADIUS, the Ethernet device and your computer are on the same subnet.

Chart A-2 Troubleshooting the Ethernet Interface

PROBLEM	CORRECTIVE ACTION
I cannot ping any computer on the LAN.	If the **ETHERNET** LED on the front panel is off, check the Ethernet cable connections between your Vantage RADIUS and the Ethernet device. Check the Ethernet cable connections between the Ethernet device and the LAN computers. Check for faulty Ethernet cables. Make sure the LAN computer’s Ethernet adapter is installed and working properly. Verify that the IP address and the subnet mask of Vantage RADIUS, the Ethernet device and the LAN computers are on the same subnet.
I cannot access the web configurator.	Your computer’s and the Vantage RADIUS’s IP addresses must be on the same subnet for LAN access. If you changed the Vantage RADIUS’s IP address, then enter the new one as the URL. See the following section to check that pop-up windows, JavaScripts and Java permissions are allowed. You may also need to clear your Internet browser’s cache. In Internet Explorer, click **Tools** and then **Internet Options** to open the **Internet Options** screen. In the **General** tab, click **Delete Files**. In the pop-up window, select the **Delete all offline content** check box and click **OK**. Click **OK** in the **Internet Options** screen to close it. If you disconnect your computer from one device and connect it to another device that has the same IP address, your computer’s ARP (Address Resolution Protocol) table may contain an entry that maps the management IP address to the previous device’s MAC address). In Windows, use **arp -d** at the command prompt to delete all entries in your computer’s ARP table.

Problems with the Password

Chart A-3 Troubleshooting the Password

PROBLEM	CORRECTIVE ACTION
I cannot access Vantage RADIUS.	The **Password** and **Username** fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing. Use the **RESET** button on the front panel of Vantage RADIUS to restore the factory default configuration file (hold this button in for about 5 seconds or until the **SYS** LED starts to blink). This will restore all of the factory defaults including the password. Check that the access method is not disabled in the **REMOTE MANAGEMENT** screen. Check that the computer IP address is allowed to access Vantage RADIUS. For HTTPS, check the port number has not changed in the **REMOTE MANAGEMENT** screen.

Problems with Telnet

Chart A-4 Troubleshooting Telnet

PROBLEM	CORRECTIVE ACTION
I cannot access Vantage RADIUS through Telnet.	Refer to the *Problems with the Ethernet Interface* section for instructions on checking your Ethernet connection. Check that telnet is enabled in the **REMOTE MANAGEMENT** screen.

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).

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

Step 1. In Internet Explorer, select **Tools**, **Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

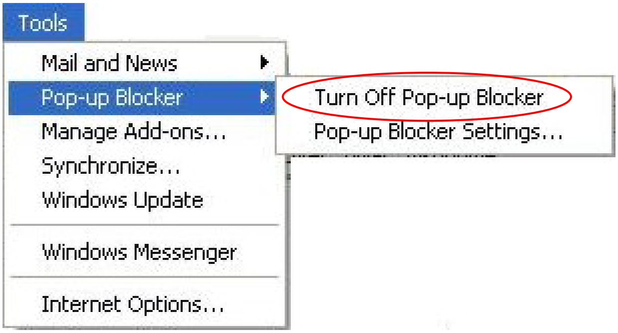
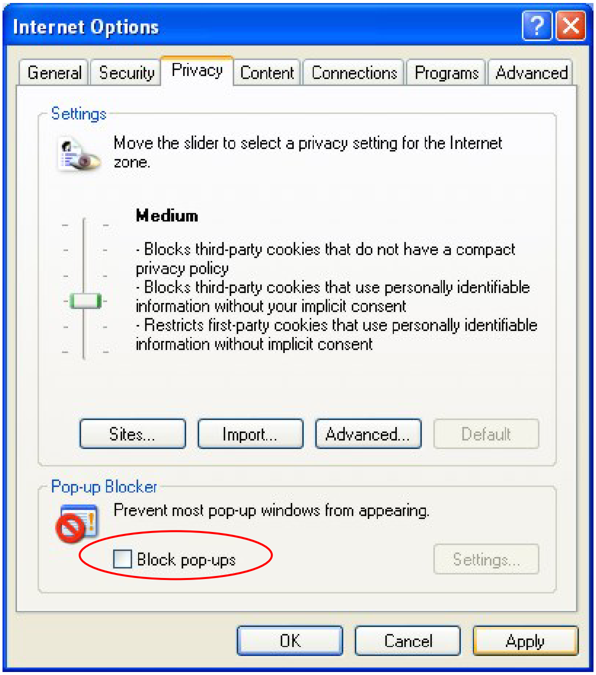


Figure A-1 Pop-up Blocker

You can also check if pop-up blocking is disabled in the **Pop-up Blocker** section in the **Privacy** tab.

Step 1. In Internet Explorer, select **Tools**, **Internet Options**, **Privacy**.

Step 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.



Settings

Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Pop-up Blocker

Prevent most pop-up windows from appearing.

□ Block pop-ups

Figure A-2 Internet Options: Privacy

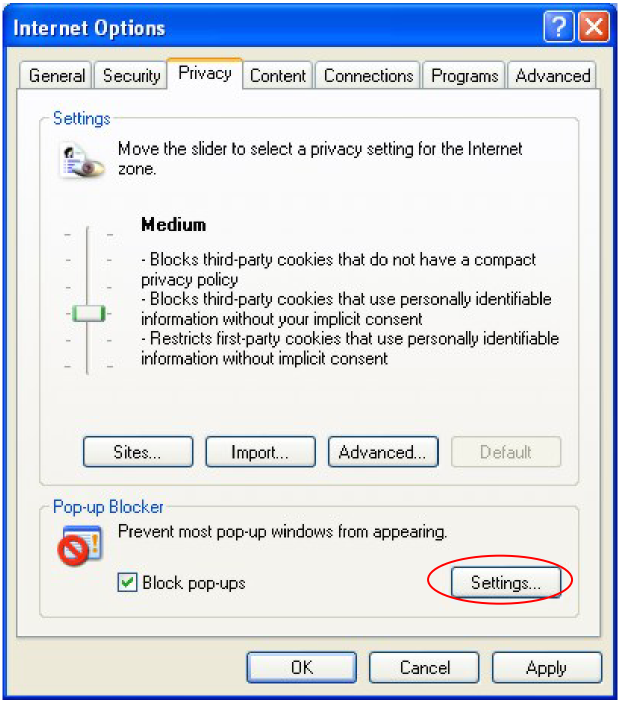
Step 3. Click **Apply** to save this setting.

Enable pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, see the following steps.

Step 1. In Internet Explorer, select **Tools**, **Internet Options** and then the **Privacy** tab.

Step 2. Select **Settings…** to open the **Pop-up Blocker Settings** screen.



Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

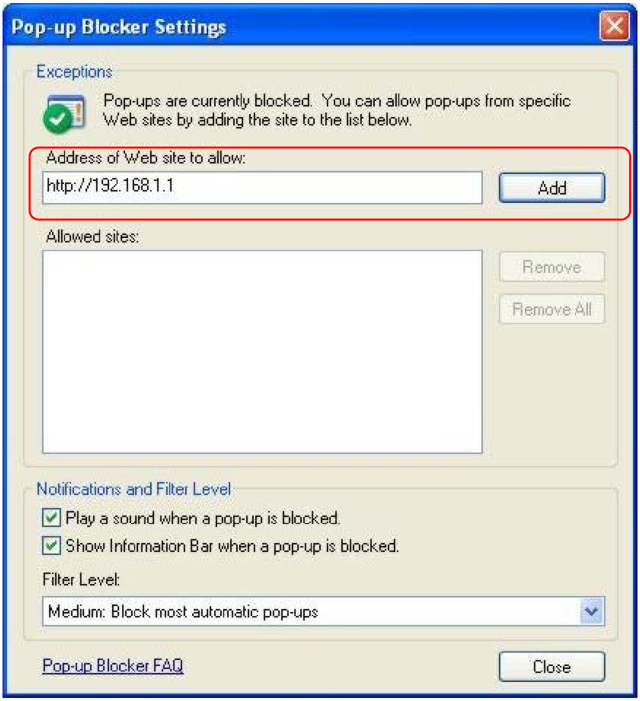
Prevent most pop-up windows from appearing.

☑ Block pop-ups

Figure A-3 Internet Options: Privacy

Step 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://192.168.1.1.

Step 4. Click **Add** to move the IP address to the list of **Allowed sites**.



Pop-up Blocker Settings

Exceptions

Pop-ups are currently blocked. You can allow pop-ups from specific Web sites by adding the site to the list below.

Address of Web site to allow: http://192.168.1.1

Allowed sites:

Notifications and Filter Level

☑ Play a sound when a pop-up is blocked.

☑ Show Information Bar when a pop-up is blocked.

Filter Level: Medium: Block most automatic pop-ups

Figure A-4 Pop-up Blocker Settings

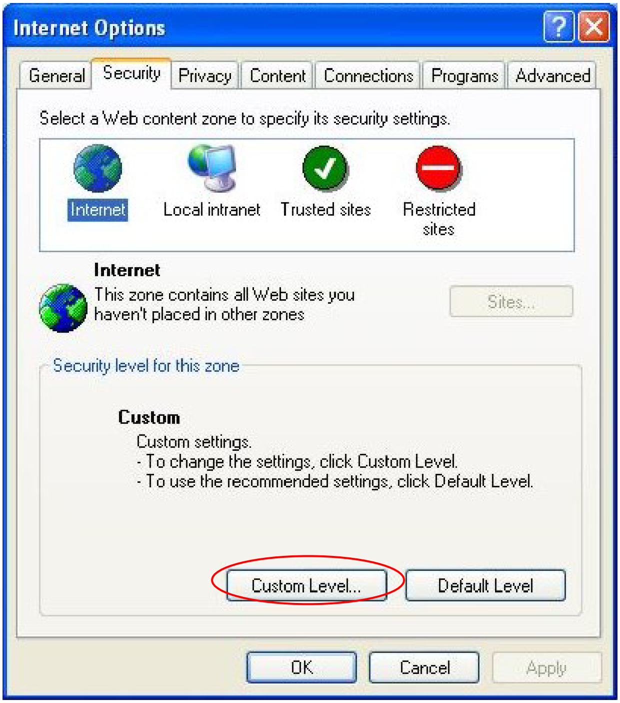
Step 5. Click **Close** to return to the **Privacy** screen.

Step 6. Click **Apply** to save this setting.

JavaScripts

Step 1. If pages of the web configurator do not display properly in Internet Explorer, check that JavaScripts are allowed.

Step 2. In Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.



Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

Security level for this zone

Custom

Custom settings.

- To change the settings, click Custom Level.
- To use the recommended settings, click Default Level.

Figure A-5 Internet Options: Security

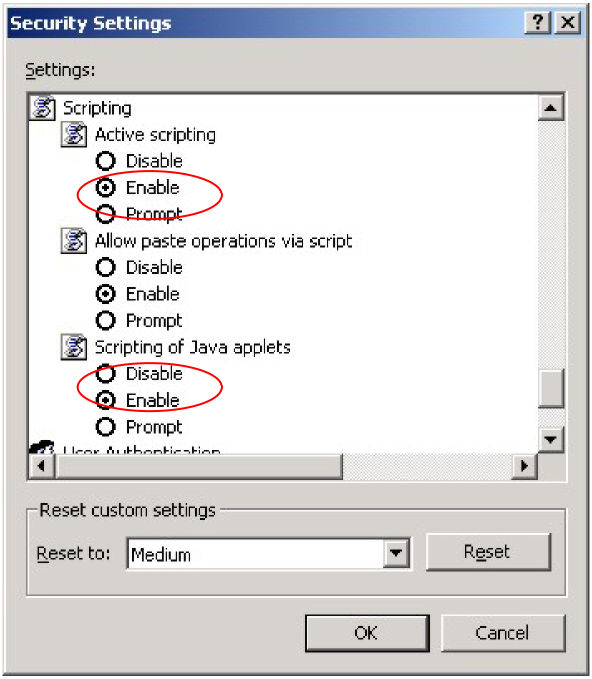
Step 3. Click the **Custom Level...** button.

Step 4. Scroll down to **Scripting**.

Step 5. Under **Active scripting** make sure that **Enable** is selected (the default).

Step 6. Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

Step 7. Click **OK** to close the window.



Security Settings

Settings:

Scripting

Active scripting
○ Disable
● Enable
○ Prompt

Allow paste operations via script
○ Disable
● Enable
○ Prompt

Scripting of Java applets
○ Disable
● Enable
○ Prompt

User Authentication

Reset custom settings

Reset to: Medium

Figure A-6 Security Settings - Java Scripting

Java Permissions

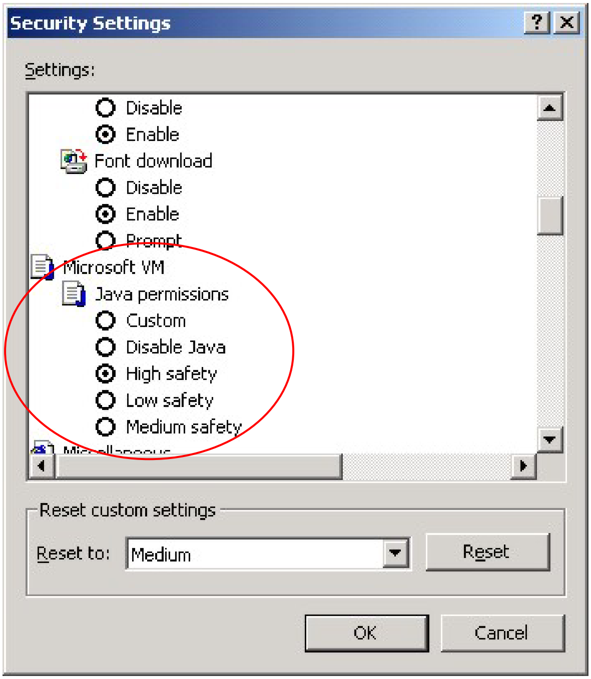
Step 1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Security** tab.

Step 2. Click the **Custom Level...** button.

Step 3. Scroll down to **Microsoft VM**.

Step 4. Under Java permissions make sure that a safety level is selected.

Step 5. Click **OK** to close the window.



Settings:

- ○ Disable
- ● Enable
- Font download
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Microsoft VM
  - Java permissions
    - ○ Custom
    - ○ Disable Java
    - ● High safety
    - ○ Low safety
    - ○ Medium safety
- Miscellaneous

Reset custom settings

Reset to: Medium

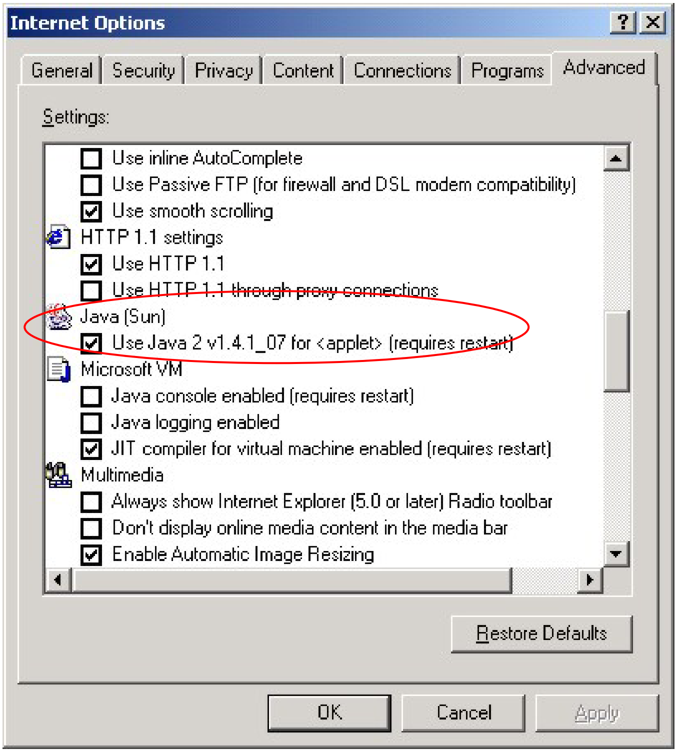
Figure A-7 Security Settings - Java

JAVA (Sun)

Step 1. From Internet Explorer, click **Tools**, **Internet Options** and then the **Advanced** tab.

Step 2. Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.

Step 3. Click **OK** to close the window.



□ Use inline AutoComplete
□ Use Passive FTP (for firewall and DSL modem compatibility)
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
□ Use HTTP 1.1 through proxy connections
Java (Sun)
☑ Use Java 2 v1.4.1_07 for <applet> (requires restart)
Microsoft VM
□ Java console enabled (requires restart)
□ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
□ Always show Internet Explorer (5.0 or later) Radio toolbar
□ Don't display online media content in the media bar
☑ Enable Automatic Image Resizing

Figure A-8 Java (Sun)

Appendix B Specifications

Hardware

Chart B-1 HARDWARE SPECIFICATIONS

Power Specification	DC 5V 3Amp Max.
Operation Temperature	0º C ~ 50º C
Storage Temperature	-10º C ~ 60º C
Operation Humidity	10% to 90% (Non-condensing)
Storage Humidity	5% to 95% (Non-condensing)

Firmware

CHART B-2 FIRMWARE SPECIFICATIONS	
Standards	IEEE802.3u 100BASE-TX. IEEE 802.3 and 802.3u 10Base-T and 100Base-TX. IEEE 802.1x security standard. IEEE 802.3af draft.
Spanning Tree Protocol	IEEE 802.1d
Security	IEEE 802.1x security; MD5, and PEAP included. WPA support. Dynamic WEP key exchange. Built-in RADIUS server, MD5 security and 200-entry local user database.

CHART B-2 FIRMWARE SPECIFICATIONS	
Diagnostics Capabilities	The access point can perform self-diagnostic tests. These tests check the integrity of the following circuits: ➢ FLASH memory. ➢ DRAM. ➢ Dual Ethernet port. ➢ Syslog. ➢ RADIUS log ➢ User Trace log.
Management	Embedded Web Configurator management. Command-line interface. Telnet support; Password-protected telnet access to internal configuration manager. TFTP/Web for firmware downloading, configuration backup and restoration. Telnet remote access support. Built-in Diagnostic Tool. SNMP Management. RADIUS client. Secure connections using SSH and HTTPS

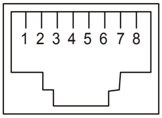
Appendix C
Power over Ethernet Specifications

You can use a power over Ethernet injector to power this device. The injector must comply to IEEE 802.3af.

Chart C-1 Power over Ethernet Injector Specifications

Power Output	15.4 Watts maximum
Power Current	400 mA maximum

Chart C-2 Power over Ethernet Injector RJ-45 Port Pin Assignments

	PIN NO	RJ-45 SIGNAL ASSIGNMENT
	1	Output Transmit Data +
	2	Output Transmit Data -
	3	Receive Data +
	4	Power +
	5	Power +
	6	Receive Data -
	7	Power -
	8	Power -

Appendix D
Setting up Your Computer's IP Address

This appendix is a general guide on how to set an IP address on your computer or have it receive an IP address automatically if the device you are connecting it to can assign it an IP address.

All computers must have a 10M or 100M Ethernet adapter card and TCP/IP installed.

Windows 95/98/Me/NT/2000/XP, Macintosh OS 7 and later operating systems and all versions of UNIX/LINUX include the software components you need to install and use TCP/IP on your computer. Windows 3.1 requires the purchase of a third-party TCP/IP application package.

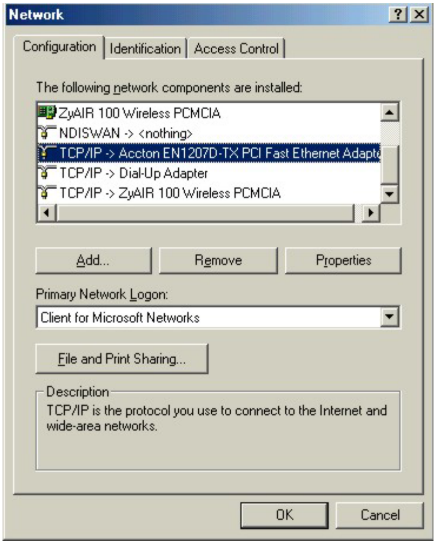
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

After the appropriate TCP/IP components are installed, configure the TCP/IP settings in order to "communicate" with your network.

If you manually assign IP information instead of using dynamic assignment, make sure that your computers have IP addresses that place them in the same subnet as Vantage RADIUS' LAN port.

Windows 95/98/Me

Click **Start**, **Settings**, **Control Panel** and double-click the **Network** icon to open the **Network** window.



The following network components are installed:

- ZyAIR 100 Wireless PCMCIA
- NDISWAN -> <nothing>
- TCP/IP -> Accton EN1207D-TX PCI Fast Ethernet Adapte
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> ZyAIR 100 Wireless PCMCIA

Primary Network Logon: Client for Microsoft Networks

Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

The **Network** window **Configuration** tab displays a list of installed components. You need a network adapter, the TCP/IP protocol and Client for Microsoft Networks.

If you need the adapter:

a. In the **Network** window, click **Add**.

b. Select **Adapter** and then click **Add**.

c. Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

a. In the **Network** window, click **Add**.

b. Select **Protocol** and then click **Add**.

c. Select **Microsoft** from the list of **manufacturers**.

d. Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

a. Click **Add**.

b. Select **Client** and then click **Add**.

c. Select **Microsoft** from the list of manufacturers.

d. Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.

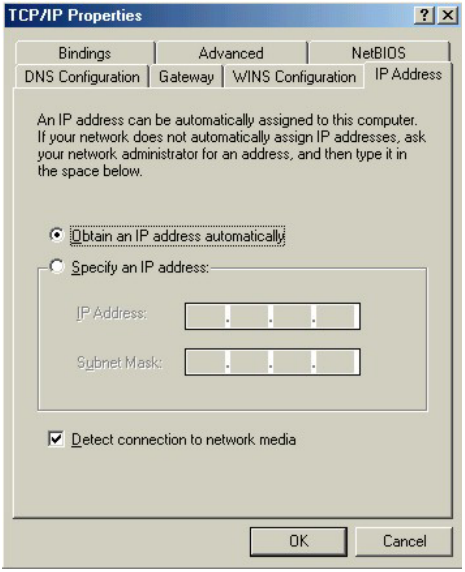
e. Restart your computer so the changes you made take effect.

In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**.

1. Click the **IP Address** tab.

   -If your IP address is dynamic, select **Obtain an IP address automatically**.

   -If you have a static IP address, select **Specify an IP address** and type your information into the **IP Address** and **Subnet Mask** fields.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

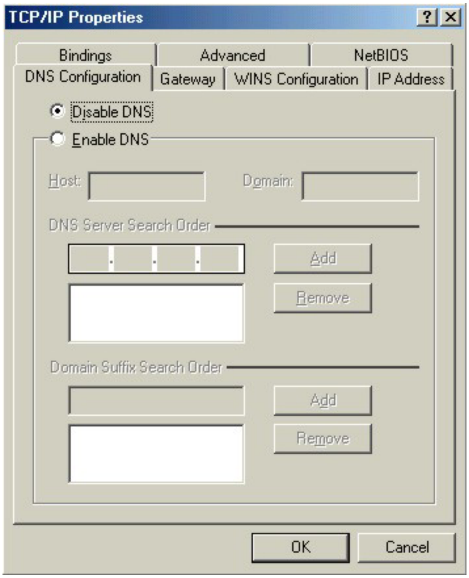
○ Specify an IP address:

☑ Detect connection to network media

2. Click the **DNS** Configuration tab.

   -If you do not know your DNS information, select **Disable DNS**.

   -If you know your DNS information, select **Enable DNS** and type the information in the fields below (you may not need to fill them all in).



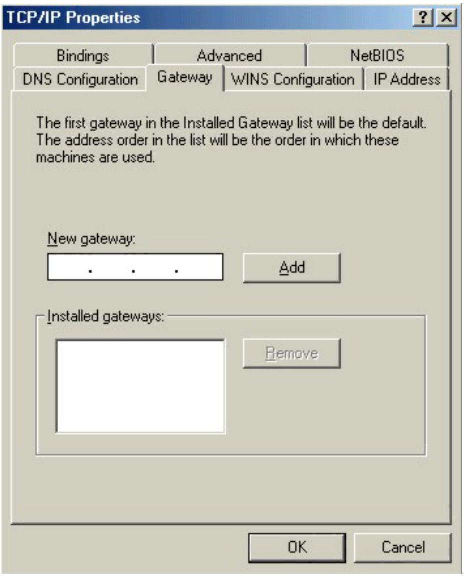
● Disable DNS

○ Enable DNS

3. Click the **Gateway** tab.

   -If you do not know your gateway's IP address, remove previously installed gateways.

   -If you have a gateway IP address, type it in the **New gateway field** and click **Add**.



The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

4. Click **OK** to save and close the **TCP/IP Properties** window.

5. Click **OK** to close the **Network** window. Insert the Windows CD if prompted.

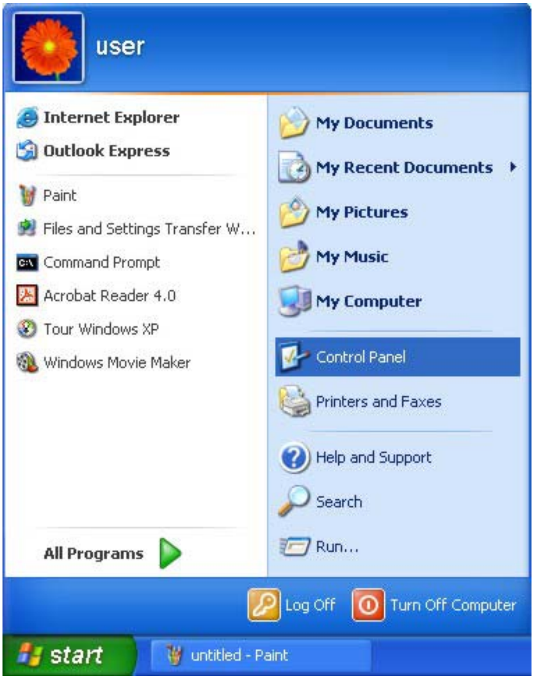
6. Turn on your Vantage RADIUS and restart your computer when prompted.

Verifying Your Computer's IP Address

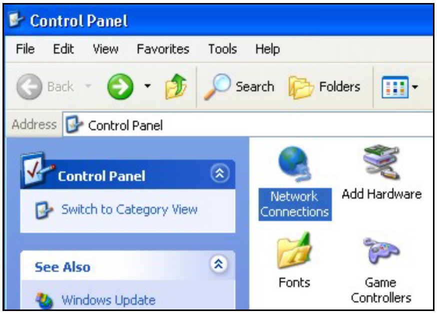
1. Click **Start** and then **Run**.
2. In the **Run** window, type "winipcfg" and then click **OK** to open the **IP Configuration** window.
3. Select your network adapter. You should see your computer's IP address, subnet mask and default gateway.

Windows 2000/NT/XP

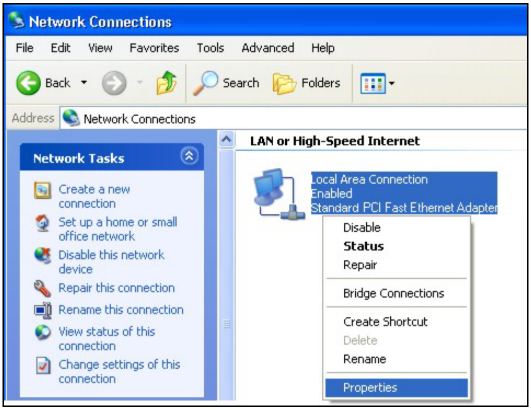
1. For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.



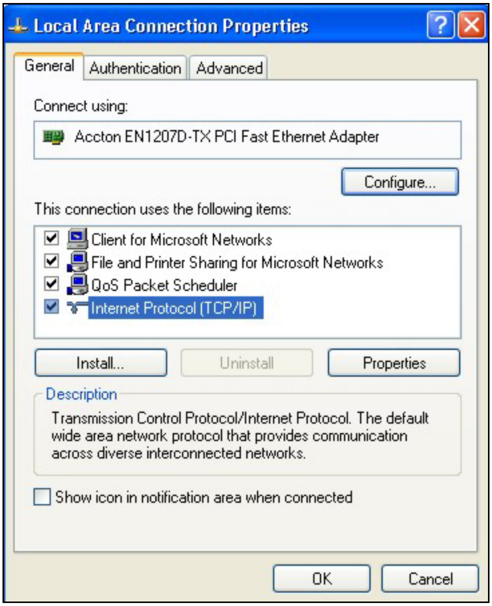
2. For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.



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


Network Connections
File Edit View Favorites Tools Advanced Help
Back
Search
Folders
Address Network Connections
Network Tasks
Create a new connection
Set up a home or small office network
Disable this network device
Repair this connection
Rename this connection
View status of this connection
Change settings of this connection
LAN or High-Speed Internet
Local Area Connection
Enabled
Standard PCI Fast Ethernet Adapter
Disable
Status
Repair
Bridge Connections
Create Shortcut
Delete
Rename
Properties

4. Select **Internet Protocol (TCP/IP)** (under the **General** tab in Win XP) and click **Properties**.


Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Accton EN1207D-TX PCI Fast Ethernet Adapter

Configure...

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Install... | Uninstall | Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

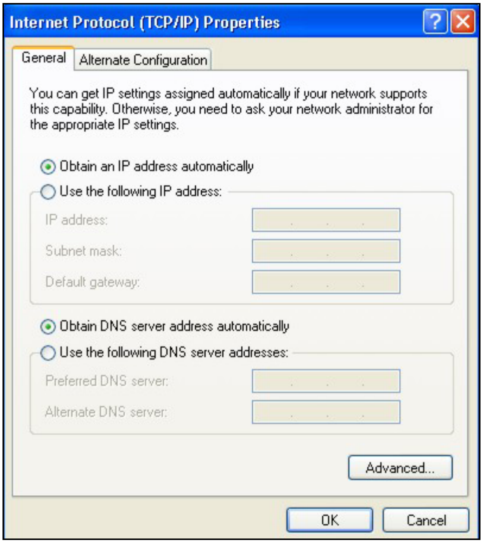
OK | Cancel

5. The **Internet Protocol TCP/IP Properties** window opens (the **General tab** in Windows XP).

-If you have a dynamic IP address click **Obtain an IP address automatically**.

-If you have a static IP address click **Use the following IP Address** and fill in the **IP address**, **Subnet mask**, and **Default gateway** fields.

Click **Advanced**.


Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

IP address: . . .
Subnet mask: . . .
Default gateway: . . .

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

Advanced...

OK | Cancel

6. -If you do not know your gateway's IP address, remove any previously installed gateways in the **IP Settin**gs tab and click **OK**.

   Do one or more of the following if you want to configure additional IP addresses:

   -In the **IP Settings** tab, in IP addresses, click **Add**.

   -In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.

   -Repeat the above two steps for each IP address you want to add.

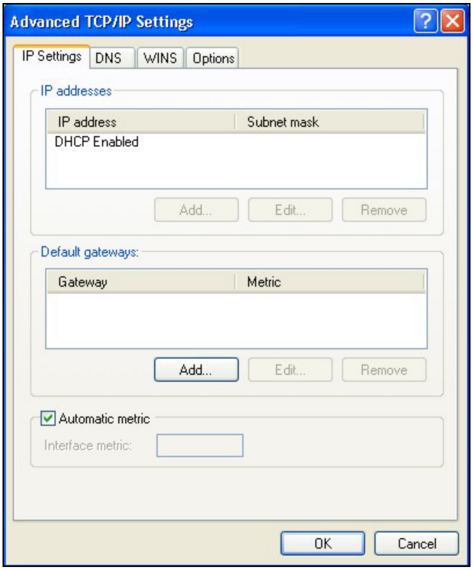
   -Configure additional default gateways in the **IP Settings** tab by clicking **Add** in **Default gateways**.

   -In **TCP/IP Gateway Address**, type the IP address of the default gateway in **Gateway**. To manually configure a default metric (the number of transmission hops), clear the **Automatic metric** check box and type a metric in **Metric**.

   -Click **Add**.

   -Repeat the previous three steps for each default gateway you want to add.

   -Click **OK** when finished.



Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

IP addresses

IP address	Subnet mask
DHCP Enabled	

Default gateways:

Gateway	Metric

☑ Automatic metric

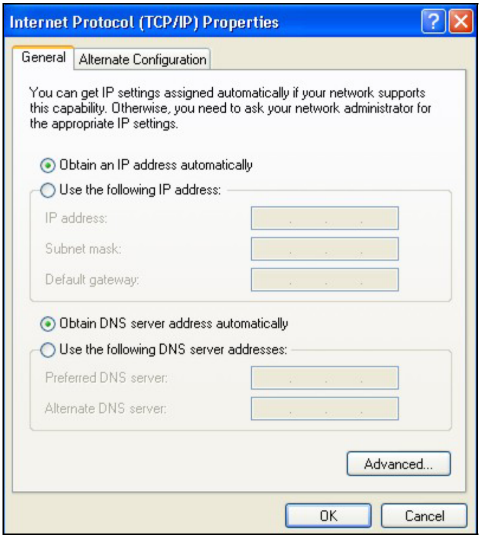
Interface metric:

7. In the **Internet Protocol TCP/IP Properties** window (the **General tab** in Windows XP):

   -Click **Obtain DNS server address automatically** if you do not know your DNS server IP address(es).

   -If you know your DNS server IP address(es), click **Use the following DNS server addresses**, and type them in the **Preferred DNS server** and **Alternate DNS server** fields.

   If you have previously configured DNS servers, click **Advanced** and then the **DNS** tab to order them.



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

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

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

10. Turn on your Vantage RADIUS and restart your computer (if prompted).

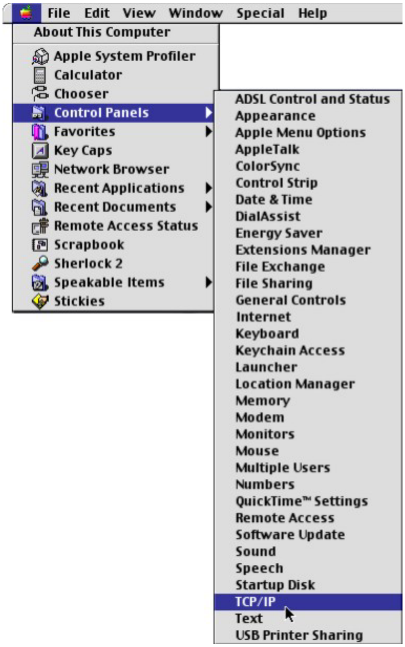
Verifying Your Computer's IP Address

1. Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.

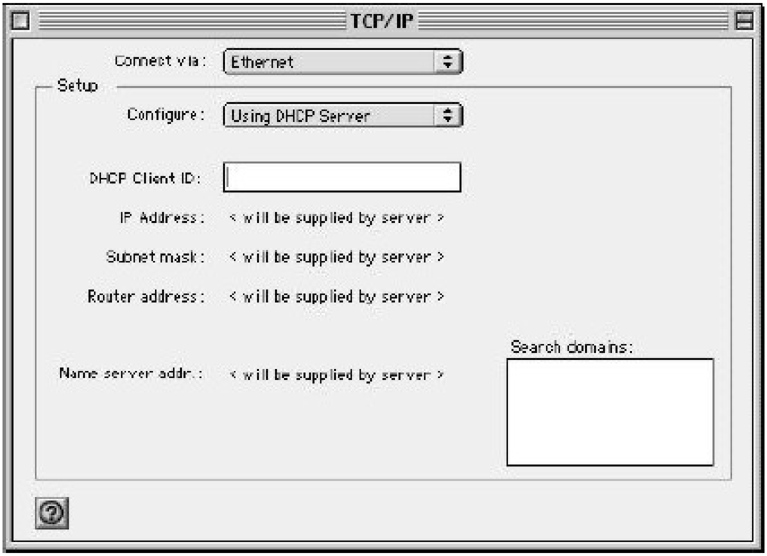
2. In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

1. Click the **Apple** menu, **Control Panel** and double-click **TCP/IP** to open the **TCP/IP Control Panel**.



2. Select **Ethernet built-in** from the **Connect via** list.



TCP/IP

Connect via: Ethernet

Setup

Configure: Using DHCP Server

DHCP Client ID:

IP Address: < will be supplied by server >

Subnet mask: < will be supplied by server >

Router address: < will be supplied by server >

Name server addr.: < will be supplied by server >

Search domains:

3. For dynamically assigned settings, select **Using DHCP Server** from the **Configure:** list.
4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

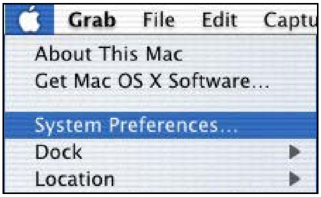
   -Type the IP address of your Vantage RADIUS in the **Router address** box.
5. Close the **TCP/IP Control Panel**.
6. Click **Save** if prompted, to save changes to your configuration.
7. Turn on your Vantage RADIUS and restart your computer (if prompted).

Verifying Your Computer's IP Address

Check your TCP/IP properties in the **TCP/IP Control Panel** window.

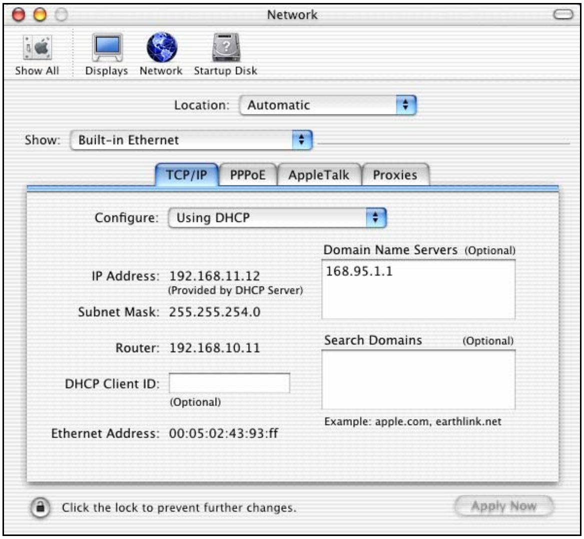
Macintosh OS X

1. Click the **Apple** menu, and click **System Preferences** to open the **System Preferences** window.



2. Click **Network** in the icon bar.

   - Select **Automatic** from the **Location** list.
   - Select **Built-in Ethernet** from the **Show** list.
   - Click the **TCP/IP** tab.



Location: Automatic

Show: Built-in Ethernet

Configure: Using DHCP

IP Address: 192.168.11.12 (Provided by DHCP Server)

Subnet Mask: 255.255.254.0

Router: 192.168.10.11

DHCP Client ID: (Optional)

Ethernet Address: 00:05:02:43:93:ff

Domain Name Servers (Optional): 168.95.1.1

Search Domains (Optional)

Example: apple.com, earthlink.net

Click the lock to prevent further changes.

3. For dynamically assigned settings, select **Using DHCP** from the **Configure** list.

4. For statically assigned settings, do the following:

   -From the **Configure** box, select **Manually**.

   -Type your IP address in the **IP Address** box.

   -Type your subnet mask in the **Subnet mask** box.

   -Type the IP address of your Vantage RADIUS in the **Router address** box.

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

6. Turn on your Vantage RADIUS and restart your computer (if prompted).

Verifying Your Computer's IP Address

Check your TCP/IP properties in the **Network** window.

Appendix E
Wireless LAN and IEEE 802.11

A wireless LAN (WLAN) provides a flexible data communications system that you can use to access various services (navigating the Internet, email, printer services, etc.) without the use of a cabled connection. In effect a wireless LAN environment provides you the freedom to stay connected to the network while roaming around in the coverage area. WLAN is not available on all models.

Benefits of a Wireless LAN

Wireless LAN offers the following benefits:

1. It provides you with access to network services in areas otherwise hard or expensive to wire, such as historical buildings, buildings with asbestos materials and classrooms.
2. It provides healthcare workers like doctors and nurses access to a complete patient's profile on a handheld or notebook computer upon entering a patient's room.
3. It allows flexible workgroups a lower total cost of ownership for workspaces that are frequently reconfigured.
4. It allows conference room users access to the network as they move from meeting to meeting, getting up-to-date access to information and the ability to communicate decisions while "on the go".
5. It provides campus-wide networking mobility, allowing enterprises the roaming capability to set up easy-to-use wireless networks that cover the entire campus transparently.

IEEE 802.11

The 1997 completion of the IEEE 802.11 standard for wireless LANs (WLANs) was a first important step in the evolutionary development of wireless networking technologies. The standard was developed to maximize interoperability between differing brands of wireless LANs as well as to introduce a variety of performance improvements and benefits.

The IEEE 802.11 specifies three different transmission methods for the PHY, the layer responsible for transferring data between nodes. Two of the methods use spread spectrum RF signals, Direct Sequence Spread Spectrum (DSSS) and Frequency-Hopping Spread Spectrum (FHSS), in the 2.4 to 2.4825 GHz unlicensed ISM (Industrial, Scientific and Medical) band. The third method is infrared technology, using very high frequencies, just below visible light in the electromagnetic spectrum to carry data.

Ad-hoc Wireless LAN Configuration

The simplest WLAN configuration is an independent (Ad-hoc) WLAN that connects a set of computers with wireless nodes or stations (STA), which is called a Basic Service Set (BSS). In the most basic form, a wireless LAN connects a set of computers with wireless adapters. 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). See the following diagram of an example of an Ad-hoc wireless LAN.

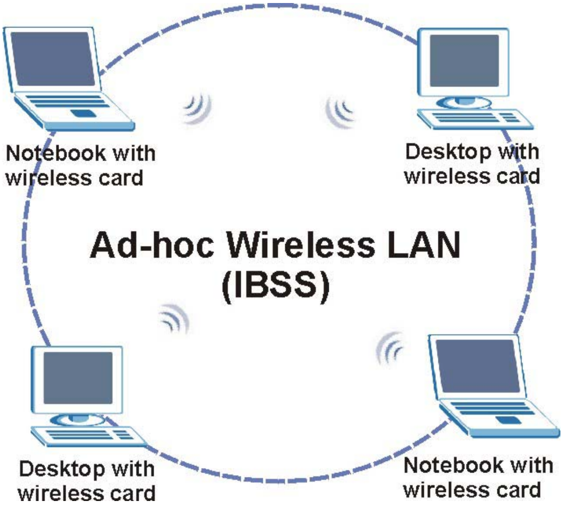

Notebook with wireless card
Desktop with wireless card
Ad-hoc Wireless LAN (IBSS)
Desktop with wireless card
Notebook with wireless card

Diagram E-1 Peer-to-Peer Communication in an Ad-hoc Network

Infrastructure Wireless LAN Configuration

For infrastructure WLANs, multiple access points (APs) link the WLAN to the wired network and allow users to efficiently share network resources. The access points not only provide communication with the wired network but also mediate wireless network traffic in the immediate neighborhood. Multiple access points can provide wireless coverage for an entire building or campus. All communications between stations or between a station and a wired network client go through the access point.

The Extended Service Set (ESS) shown in the next figure consists of a series of overlapping BSSs (each containing an Access Point) connected together by means of a Distribution System (DS). Although the DS could be any type of network, it is almost invariably an Ethernet LAN. Mobile nodes can roam between access points and seamless campus-wide coverage is possible.

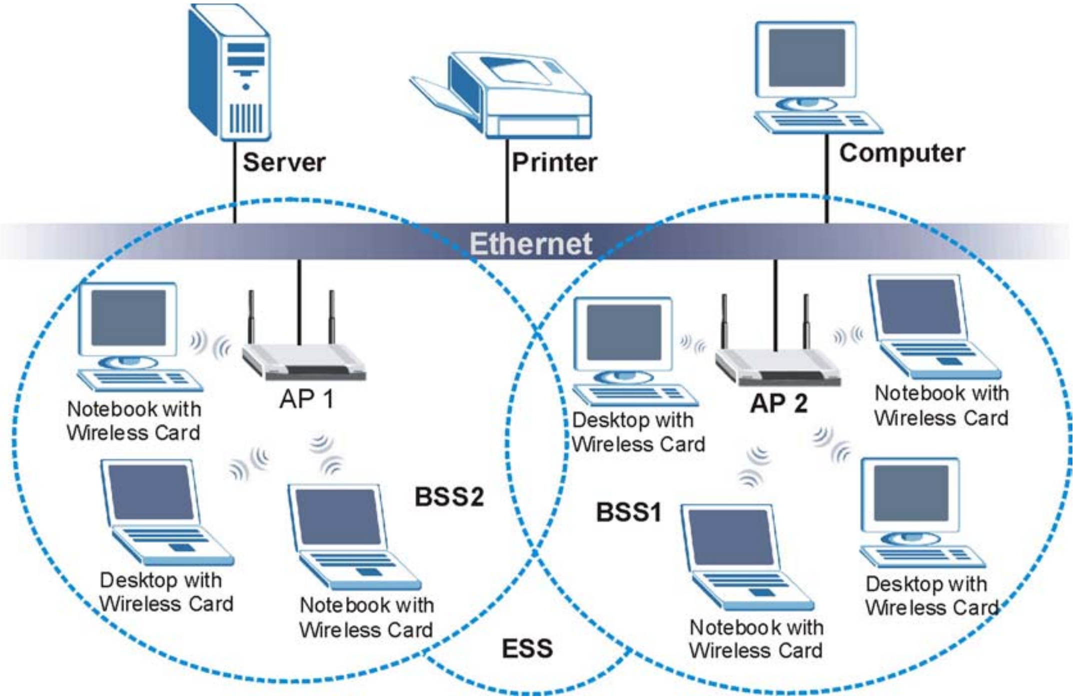

Server
Printer
Computer
Ethernet
Notebook with Wireless Card
AP 1
Desktop with Wireless Card
AP 2
Notebook with Wireless Card
Desktop with Wireless Card
Notebook with Wireless Card
BSS2
BSS1
Notebook with Wireless Card
Desktop with Wireless Card
ESS

Diagram E-2 ESS Provides Campus-Wide Coverage

Appendix F
Wireless LAN With IEEE 802.1x

As wireless networks become popular for both portable computing and corporate networks, security is now a priority.

Security Flaws with IEEE 802.11

Wireless networks based on the original IEEE 802.11 have a poor reputation for safety. The IEEE 802.11b wireless access standard, first published in 1999, was based on the MAC address. As the MAC address is sent across the wireless link in clear text, it is easy to spoof and fake. Even the WEP (Wire Equivalent Privacy) data encryption is unreliable as it can be easily decrypted with current computer speed

Deployment Issues with IEEE 802.11

User account management has become a network administrator's nightmare in a corporate environment, as the IEEE 802.11b standard does not provide any central user account management. User access control is done through manual modification of the MAC address table on the access point. Although WEP data encryption offers a form of data security, you have to reset the WEP key on the clients each time you change your WEP key on the access point.

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.

Advantages of the IEEE 802.1x

- 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 stations.

RADIUS Server Authentication Sequence

The following figure depicts a typical wireless network with a remote RADIUS server for user authentication using EAPOL (EAP Over LAN).

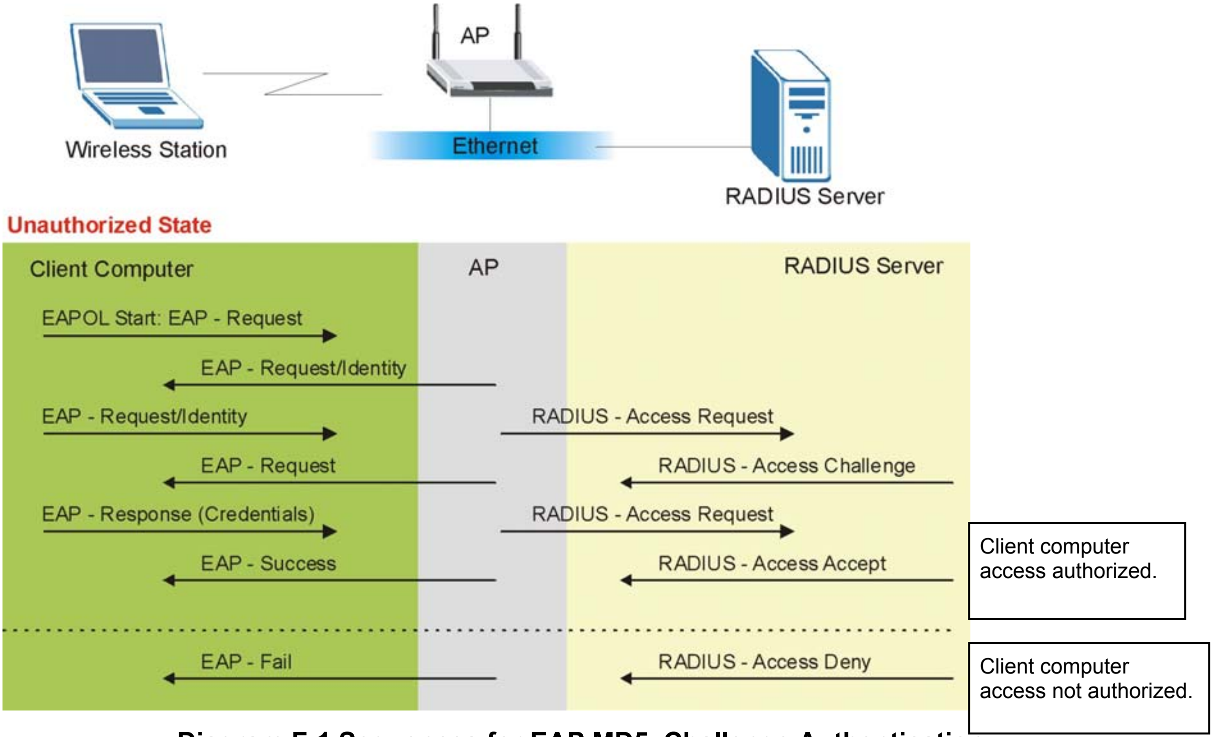


Diagram F-1 Sequences for EAP MD5–Challenge Authentication

Appendix G Types of EAP Authentication

This appendix discusses the five popular EAP authentication types: **EAP-MD5**, **EAP-TLS**, **EAP-TTLS**, **PEAP** and **LEAP**. The type of authentication you use depends on the RADIUS server. Consult your network administrator for more information.

EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wireless station. The wireless station ‘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 stations 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 (Light Extensible Authentication Protocol) is a Cisco implementation of IEEE802.1x.

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.

Appendix H
IP Subnetting

IP Addressing

Routers "route" based on the network number. The router that delivers the data packet to the correct destination host uses the host ID.

IP Classes

An IP address is made up of four octets (eight bits), written in dotted decimal notation, for example, 192.168.1.1. IP addresses are categorized into different classes. The class of an address depends on the value of its first octet.

- Class "A" addresses have a 0 in the left most bit. In a class "A" address the first octet is the network number and the remaining three octets make up the host ID.
- Class "B" addresses have a 1 in the left most bit and a 0 in the next left most bit. In a class "B" address the first two octets make up the network number and the two remaining octets make up the host ID.
- Class "C" addresses begin (starting from the left) with 1 1 0. In a class "C" address the first three octets make up the network number and the last octet is the host ID.
- Class "D" addresses begin with 1 1 1 0. Class "D" addresses are used for multicasting. (There is also a class "E" address. It is reserved for future use.)

Chart H-1 Classes of IP Addresses

IP ADDRESS:		OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	0	Network number	Host ID	Host ID	Host ID
Class B	10	Network number	Network number	Host ID	Host ID
Class C	110	Network number	Network number	Network number	Host ID

Host IDs of all zeros or all ones are not allowed.

Therefore:

- A class "C" network (8 host bits) can have 2^{8} –2 or 254 hosts.
- A class "B" address (16 host bits) can have 2^{16} –2 or 65534 hosts.

A class "A" address (24 host bits) can have 2^{24} –2 hosts (approximately 16 million hosts).

Since the first octet of a class "A" IP address must contain a "0", the first octet of a class "A" address can have a value of 0 to 127.

Similarly the first octet of a class "B" must begin with "10", therefore the first octet of a class "B" address has a valid range of 128 to 191. The first octet of a class "C" address begins with "110", and therefore has a range of 192 to 223.

Chart H-2 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	**0**0000000 to **0**1111111	0 to 127
Class B	**10**000000 to **10**111111	128 to 191
Class C	**110**00000 to **110**11111	192 to 223
Class D	**1110**0000 to **1110**1111	224 to 239

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). A subnet mask has 32 bits; each bit of the mask corresponds to a bit of the IP address. 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.

Subnet masks are expressed in dotted decimal notation just as IP addresses are. The "natural" masks for class A, B and C IP addresses are as follows.

Chart H-3 "Natural" Masks

CLASS	NATURAL MASK
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Subnetting

With subnetting, the class arrangement of an IP address is ignored. For example, a class C address no longer has to have 24 bits of network number and 8 bits of host ID. With subnetting, some of the host ID bits are converted into network number bits. By convention, subnet masks always consist of a continuous sequence of ones beginning from the left most bit of the mask, followed by a continuous sequence of zeros, for a total number of 32 bits.

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 mask 255.255.255.128.

The following table shows all possible subnet masks for a class "C" address using both notations.

Chart H-4 Alternative Subnet Mask Notation

SUBNET MASK IP ADDRESS	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE
255.255.255.0	/24	0000 0000
255.255.255.128	/25	1000 0000
255.255.255.192	/26	1100 0000
255.255.255.224	/27	1110 0000
255.255.255.240	/28	1111 0000
255.255.255.248	/29	1111 1000
255.255.255.252	/30	1111 1100

The first mask shown is the class "C" natural mask. Normally if no mask is specified it is understood that the natural mask is being used.

Example: Two Subnets

As an example, you have a class "C" address 192.168.1.0 with subnet mask of 255.255.255.0.

	NETWORK NUMBER	HOST ID
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	0
Subnet Mask (Binary)	11111111.11111111.11111111.	00000000

The first three octets of the address make up the network number (class "C"). You want to have two separate networks.

Divide the network 192.168.1.0 into two separate subnets by converting one of the host ID bits of the IP address to a network number bit. The "borrowed" host ID bit can be either "0" or "1" thus giving two subnets; 192.168.1.0 with mask 255.255.255.128 and 192.168.1.128 with mask 255.255.255.128.

☞ **In the following charts, shaded/bolded last octet bit values indicate host ID bits “borrowed” to form network ID bits. The number of “borrowed” host ID bits determines the number of subnets you can have. The remaining number of host ID bits (after “borrowing”) determines the number of hosts you can have on each subnet.**

Chart H-5 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	**0**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.0		Lowest Host ID: 192.168.1.1
Broadcast Address: 192.168.1.127		Highest Host ID: 192.168.1.126

Chart H-6 Subnet 2

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	**1**0000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	**1**0000000
Subnet Address: 192.168.1.128		Lowest Host ID: 192.168.1.129
Broadcast Address: 192.168.1.255		Highest Host ID: 192.168.1.254

The remaining 7 bits determine the number of hosts each subnet can have. Host IDs of all zeros represent the subnet itself and host IDs of all ones are the broadcast address for that subnet, so the actual number of hosts available on each subnet in the example above is $2^7 – 2$ or 126 hosts for each subnet.

192.168.1.0 with mask 255.255.255.128 is the subnet itself, and 192.168.1.127 with mask 255.255.255.128 is the directed broadcast address for the first subnet. Therefore, the lowest IP address that can be assigned to an actual host for the first subnet is 192.168.1.1 and the highest is 192.168.1.126. Similarly the host ID range for the second subnet is 192.168.1.129 to 192.168.1.254.

Example: Four Subnets

The above example illustrated using a 25-bit subnet mask to divide a class "C" address space into two subnets. Similarly to divide a class "C" address into four subnets, you need to "borrow" two host ID bits to give four possible combinations of 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 (all 0's is the subnet itself, all 1's is the broadcast address on the subnet).

Chart H-7 Subnet 1

	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	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	

Chart H-8 Subnet 2

	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	

Chart H-9 Subnet 3

	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	

Chart H-10 Subnet 4

	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 8 subnets (001, 010, 011, 100, 101, 110).

The following table shows class C IP address last octet values for each subnet.

Chart H-11 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	223	254	255

The following table is a summary for class “C” subnet planning.

Chart H-12 Class C 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

NO. "BORROWED" HOST BITS	SUBNET MASK	NO. SUBNETS	NO. HOSTS PER SUBNET
5	255.255.255.248 (/29)	32	6
6	255.255.255.252 (/30)	64	2
7	255.255.255.254 (/31)	128	1

Subnetting With Class A and Class B Networks.

For class "A" and class "B" addresses the subnet mask also determines which bits are part of the network number and which are part of the host ID.

A class "B" address has two host ID octets available for subnetting and a class "A" address has three host ID octets (see *Chart J-1*) available for subnetting.

The following table is a summary for class "B" subnet planning.

Chart H-13 Class B 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

Appendix I
Command Interpreter

The following describes how to use the command interpreter.

Use of undocumented commands or misconfiguration can damage the unit and possibly render it unusable.

Command Syntax

- The interface outputs are in `courier new` font.
- Command keywords are **emboldened** and you should enter them exactly as shown, do not abbreviate.
- The required fields in a command are enclosed in angle brackets <>.
- The optional fields in a command are enclosed in square brackets `[]`.
- The `|`symbol means "or".
- For example,

  `netconf <type> <on|off>`

  means that you must specify the type of netbios filter and whether to turn it on or off.

Command Usage

A list of valid commands can be found by typing `help` or `?` at the command prompt. Always type the full command. Type exit to close the session when you are finished.

Command List

The following lists all the available commands on your Vantage RADIUS.

h or help

Type **h** or **help** to display the following list of available commands.

```
help [netconf|exit]
help [http/https]
```

Type **h** or **help** before a command to see its usage.

```
Vantage> help netconf
netconf
netconf ip [IP address] netmask [netmask] gateway
[gateway IP address]
netconf dns1 [dns1 IP address] dns2 [dns2 IP address]
Vantage> help exit
exit
Vantage> help http
http
http [enable/disable]
Vantage> help https
https
https [enable/disable]
```

For example, **help https** shows that you can type **https** or **https enable** or **https disable**.

netconf

Type **netconf** display the IP, netmask, gateway, primary DNS, secondary DNS and MAC address of your Vantage RADIUS.

```
IP Address    : 192.168.1.3
Netmask       : 255.255.255.0
Gateway       : 192.168.1.254
Primary DNS   : 168.95.1.1
Secondary DNS : 168.95.192.1
MAC           : 00:00:84:40:50:05
```

For example, if you wanted to change the IP address on your Vantage RADIUS from 192.168.1.3 to 192.168.1.40 because another device has the same IP address and also the gateway address has changed to 192.168.1.154, type the following:

```
netconf IP 192.168.1.40 gateway 192.168.1.154
```

```
IP Address    : 192.168.1.40
Netmask       : 255.255.255.0
Gateway       : 192.168.1.154
Primary DNS   : 168.95.1.1
Secondary DNS : 168.95.192.1
MAC           : 00:00:84:40:50:05
```

The changes are reflected in the above example

exit

Type this command to logout from the console and return to the login prompt.

```
Vantage> exit

Vantage login:
```

http

Type **http**, to show the current status of your HTTP settings.

```
Vantage> http
REMOTE ACCESS
HTTP : yes
Port : 80
```

Type **http enable** to allow remote HTTP access to Vantage RADIUS.

Type **http disable** to have Vantage RADIUS block remote http access.

https

Type **https**, to show the current status of your HTTPS settings.

```
Vantage> http
REMOTE ACCESS
HTTP : yes
Port : 80
```

Type **https enable** to allow remote HTTPS access to Vantage RADIUS.

Type **https disable** to have Vantage RADIUS block remote HTTPS access.

Appendix J
Power Adaptor Specifications

NORTH AMERICAN PLUG STANDARDS	
AC Power Adaptor Model	HPW-1005U
Input Power	AC120V/60HZ
Output Power	DC 5V
Power Consumption	2.2W
Safety Standards	UL/C-UL
EUROPEAN PLUG STANDARDS	
AC Power Adaptor Model	HPW-1005U
Input Power	AC220V/50HZ
Output Power	DC 5V
Power Consumption	5.8W
Safety Standards	CB, TUV
UNITED KINGDOM PLUG STANDARDS	
AC Power Adaptor Model	HPW-1005U
Input Power	AC240V/50HZ
Output Power	DC 5V
Power Consumption	6.5W
Safety Standards	CB, TUV

JAPAN PLUG STANDARDS	
AC Power Adaptor Model	HPW-1005U
Input Power	AC100V/50HZ
Output Power	DC 5V
Power Consumption	1.8 W
Safety Standards	PSE

AUSTRALIA AND NEW ZEALAND PLUG STANDARDS	
AC Power Adaptor Model	HPW-1005U
Input Power	AC240V/50HZ
Output Power	DC 5V
Power Consumption	6.5W
Safety Standards	DFT

Appendix K
Open Software Announcements

Notice

Information herein is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, except the express written permission of ZyXEL Communications Corporation.

This Product includes Zlib under Zlib License

Zlib License

ZLIB is third party library and has its own license

files under src/acdk/vfile/zlib are published under following Copyright and license:

Jean-loup Gailly	Mark Adler
jloup@gzip.org	madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files ftp://ds.internic.net/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

This Product includes OpenSSL under OpenSSL License

OpenSSL

Overview

The licence agreement for the usage of the OpenSSL command line utility shipped with Orbix2000 SSL/TLS is as follows:

LICENSE ISSUES

==============

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

========

==================

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"
   The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:
   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes NTP under NTP License

NTP License

This product includes netkit-telnet under BSD License

BSD

This products includes Dropbear under Dropbear License

Dropbear License

The majority of code is written by Matt Johnston, under the following license:

=====

LibTomCrypt and LibTomMath are (c) Tom St Denis, under TDCAL (Tom Doesn't Care About Licenses) some files are from public domain sources, see libtomcrypt/legal.txt

=====

sshpty.c is taken from OpenSSH 3.5p1,

"As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible

with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".
"

=====

loginrec.c

loginrec.h

atomicio.h

atomicio.c

and strlcat() (included in util.c) are from OpenSSH 3.6.1p2, and are licensed

under the 2 point BSD license.

loginrec is written primarily by Andre Lucas, atomicio.c by Theo de Raadt.

strlcat() is (c) Todd C. Miller

=====

Import code in keyimport.c is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham.

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

This product include glibc, busybox, hwclock, mtd-snapshot, libtool, tinylogin, iptable, dhcpcd, dnrd, freeradius, nbsmtp, Samba, and Redboot under GPL License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any

derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the

scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or

unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES

ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS. All other trademarks or trade names mentioned herein, if any, are the property of their respective owners.

NOTE: Some components of the “Vantage RADIUS 50 ”software incorporate source code covered under the Zlib License, OpenSSL License, BSD License, NTP License, Dropbear License and GPL License. To obtain the source code covered under those Licenses, please contact ZyXEL Communications Corporation at: support@zyxel.com.tw

End-User License Agreement for “Vantage RADIUS 50”

WARNING: ZyXEL Communications Corp. IS WILLING TO LICENSE THE ENCLOSED 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, INC. 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, 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 United States 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. 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. 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.

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 $1,000. 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.

12. 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.

Appendix L
Index