

VSG-1200 V2

Vantage Service Gateway

User's Guide

Version 1.00

10/2006

Edition 1

The logo for ZyXEL, featuring the word "ZyXEL" in a bold, blue, sans-serif font. The "Zy" is in a slightly larger font size than "XEL".

Copyright

Copyright © 2006 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

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

ZyNOS (ZyXEL Network Operating System) is a registered trademark of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Certifications

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.

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者
這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Notices

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

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Viewing Certifications

- 1 Go to <http://www.zyxel.com>.

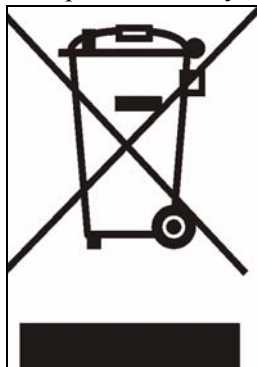
- 2** Select your product from the drop-down list box on the ZyXEL home page to go to that product's page.
- 3** Select the certification you wish to view from this page.

Safety Warnings

For your safety, be sure to read and follow all warning notices and instructions.

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

This product is recyclable. Dispose of it properly.



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 or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact 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.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Customer Support

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	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	
COSTA RICA	soporte@zyxel.co.cr	+506-2017878	www.zyxel.co.cr	ZyXEL Costa Rica Plaza Roble Escazú Etapa El Patio, Tercer Piso San José, Costa Rica
	sales@zyxel.co.cr	+506-2015098	ftp.zyxel.co.cr	
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 Česká 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 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	+33-4-72-52-97-97	www.zyxel.fr	ZyXEL France 1 rue des Vergers Bat. 1 / C 69760 Limonest France
		+33-4-72-52-19-20		
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		
HUNGARY	support@zyxel.hu	+36-1-3361649	www.zyxel.hu	ZyXEL Hungary 48, Zoldomb Str. H-1025, Budapest Hungary
	info@zyxel.hu	+36-1-3259100		
KAZAKHSTAN	http://zyxel.kz/support	+7-3272-590-698	www.zyxel.kz	ZyXEL Kazakhstan 43, Dostyk ave., Office 414 Dostyk Business Centre 050010, Almaty Republic of Kazakhstan
	sales@zyxel.kz	+7-3272-590-689		
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	

LOCATION	METHOD	SUPPORT E-MAIL	TELEPHONE	WEB SITE	REGULAR MAIL
		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		
POLAND		info@pl.zyxel.com	+48 (22) 333 8250	www.pl.zyxel.com	ZyXEL Communications ul. Okrzei 1A 03-715 Warszawa Poland
			+48 (22) 333 8251		
RUSSIA		http://zyxel.ru/support	+7-095-542-89-29	www.zyxel.ru	ZyXEL Russia Ostrovityanova 37a Str. Moscow, 117279 Russia
		sales@zyxel.ru	+7-095-542-89-25		
SPAIN		support@zyxel.es	+34-902-195-420	www.zyxel.es	ZyXEL Communications Arte, 21 5ª planta 28033 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		
UKRAINE		support@ua.zyxel.com	+380-44-247-69-78	www.ua.zyxel.com	ZyXEL Ukraine 13, Pimonenko Str. Kiev, 04050 Ukraine
		sales@ua.zyxel.com	+380-44-494-49-32		
UNITED KINGDOM		support@zyxel.co.uk	+44-1344 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	+44-1344 303034	ftp.zyxel.co.uk	

Table of Contents

Copyright	2
Certifications	3
Safety Warnings	5
ZyXEL Limited Warranty	7
Customer Support.....	8
List of Figures	20
List of Tables	26
Preface	30
Chapter 1	
Getting to Know Your VSG	32
1.1 Introducing the VSG	32
1.2 Features	32
1.3 Applications	35
1.3.1 Internet Access for LAN Networks	35
1.3.2 Internet Access in Public Areas	36
1.3.3 Hotel Application with PMS	36
Chapter 2	
Hardware Installation and Connection	38
2.1 Installation Options	38
2.1.1 Desktop Installation	38
2.1.2 Rack Mount Installation	38
2.2 Hardware Connections	39
2.2.1 Front Panel	39
2.2.1.1 LAN Port	40
2.2.1.2 WAN Port	40
2.2.1.3 Console Port	40
2.2.1.4 PMS Port	40
2.2.1.5 Reset Button	40
2.2.2 Front Panel LEDs	41
2.2.3 Rear Panel	41

2.2.4 Turning on the VSG	41
--------------------------------	----

Chapter 3	
The Web Configurator.....	42

3.1 Introducing the Web Configurator	42
3.2 Accessing the Web Configurator	42
3.3 Navigation Panel	43
3.3.1 The Navigation Panel	44
3.3.2 Screen Specific Links	44
3.4 Screen Overview	44
3.4.1 Saving Configuration Changes	45
3.5 System Login Accounts	45
3.6 Changing System Login Passwords	45
3.7 Resetting the VSG	47
3.8 Restarting the VSG	47
3.9 Logging Out of the Web Configurator	48

Chapter 4	
Initial Setup Example	50

4.1 Overview	50
4.2 Configure the VSG for Internet Access	50
4.3 Create a Billing Profile	51
4.4 Setting User Authentication Method	52
4.5 Creating Customer Accounts	53
4.6 Customer Login Test	53

Chapter 5	
System	56

5.1 General System Setting	56
----------------------------------	----

Chapter 6	
LAN and WAN Setup	60

6.1 Factory Ethernet Defaults	60
6.2 LANs and WANs	60
6.3 IP Address Assignment	60
6.3.1 IP Address and Subnet Mask	60
6.3.2 Private IP Addresses	61
6.3.3 DNS Server Address	61
6.4 LAN Configuration	62
6.5 WAN Configuration	62
6.5.1 WAN MAC Address	62
6.5.2 WAN Port Mode: Dynamic/Fixed IP Address	63
6.5.3 WAN Port Mode: PPPoE	64

6.5.4 WAN Port Mode: PPTP	66
Chapter 7	
Server	70
7.1 DHCP Configuration	70
7.1.1 Public and Private Address Assignment	70
7.1.2 Server Configuration	70
Chapter 8	
NAT Pool	74
8.1 NAT Overview	74
8.1.1 NAT Definitions	74
8.1.2 What NAT Does	75
8.1.3 How NAT Works	75
8.1.4 VPN and NAT	75
8.2 NAT Examples	76
8.2.1 Example 1: One-to-One	76
8.2.2 Example 2: Many-to-One	77
8.2.3 Example 3: One-to-One and Many-to-One	77
8.3 NAT Pool Setup	78
Chapter 9	
Authentication	80
9.1 Authentication Overview	80
9.1.1 User Agreement	80
9.1.2 CAS (Central Authentication Service)	80
9.1.3 Built-in Authentication	81
9.1.4 RADIUS	81
9.1.4.1 RADIUS Accounting	81
9.1.4.2 Vendor Specific Attribute	82
9.2 Authentication Configuration	82
9.2.1 Scenario Options	85
Chapter 10	
Billing	88
10.1 Billing Overview	88
10.1.1 Billing Profile	88
10.1.2 Configuring a Billing Profile	89
10.2 PMS (Property Management System)	91
10.2.1 Port-Location Mapping	91
10.2.2 PMS Configuration	91
10.3 Types of Subscriber Accounts	93

Chapter 11	
Static Subscriber Accounts.....	94
11.1 Static Subscriber Account Overview	94
11.2 Global Static Account Settings	94
11.3 Creating a Static Account	95
11.3.1 Generating Static Accounts Automatically	96
11.3.2 Creating Static Subscriber Accounts Manually	97
11.4 Static Account List Backup and Restore	98
11.4.1 Backing Up a Static Account List	98
11.4.2 Restoring a Static Account List	99
11.5 Editing Subscriber Accounts	100
11.5.1 Static Account Information Print Preview	101
11.6 Viewing the Static Account List	102
 Chapter 12	
Dynamic Subscriber Accounts	104
12.1 Dynamic Subscriber Account Overview	104
12.2 Dynamic Account General Settings	104
12.3 Creating Dynamic Accounts	106
12.3.1 Dynamic Account Generation Using the Web Configurator	106
12.3.2 Dynamic Account Generation Using a Statement Printer	107
12.4 Viewing the Dynamic Account List	108
12.4.1 Backing Up the Dynamic Account List	109
 Chapter 13	
Port-Location Mapping	112
13.1 Port-Location Mapping Overview	112
13.2 Configuring Port-Location Mappings	112
 Chapter 14	
Credit Card.....	116
14.1 Credit Card Overview	116
14.1.1 How Credit Card Billing Works	116
14.1.2 Configuration Steps	116
14.2 Credit Card Billing Service Configuration	117
 Chapter 15	
Customization	120
15.1 Customization Overview	120
15.2 Login Screen	120
15.2.1 Standard Login Screen	121
15.2.2 Redirect Login Screen	122
15.2.3 Advanced Login Screen	123

15.2.4 Framed Login Screen	124
15.2.5 Login Service Selection	125
15.3 Information Window	127
15.4 Account Printout	129
15.5 User Agreement Screen	133
15.6 Credit Card	135
15.6.1 Standard Login Page	135
15.6.2 Service Selection Page	136
15.6.3 Successful Page	139
15.6.4 Fail Page	141
15.7 Bill Output	142
Chapter 16	
Bandwidth Management	144
16.1 Bandwidth Management Overview	144
16.1.1 Bandwidth Allocation	144
16.2 Activating Bandwidth Management	144
16.2.1 Equal Bandwidth Setup	145
16.2.2 Class of Service Bandwidth Setup	146
Chapter 17	
Portal Page, Advertisement Link and Walled Garden	148
17.1 Overview	148
17.2 Portal Page	148
17.3 Advertisement Links	149
17.4 Walled Garden	149
Chapter 18	
Passthrough	152
18.1 Passthrough Overview	152
18.2 Computer IP and MAC Address Passthrough	152
18.2.1 Destination URL and IP Address Passthrough	154
Chapter 19	
Filter	156
19.1 Filter Setup	156
Chapter 20	
Privilege User	158
20.1 Privilege User Setup	158
20.1.1 Accessing Session List As a Privilege User	159

Chapter 21	
LAN Devices	160
21.1 LAN Devices Overview	160
21.1.1 Port Mapping	160
21.2 Configuring LAN Device Port Mapping	160
21.2.1 LAN Device Management Example	162
21.2.2 Specifying an Inside Server Example	163
Chapter 22	
Static Route	164
22.1 Static Route Overview	164
22.2 Static Route Setup	164
Chapter 23	
Private LAN.....	168
23.1 Private LAN Overview	168
23.2 Configuring a Private LAN	168
Chapter 24	
Syslog	170
24.1 Syslog Overview	170
24.1.1 Syslog Server Setup	170
24.1.2 Log Settings	171
Chapter 25	
Session Trace	176
25.1 Session Trace Overview	176
25.1.1 Configuring Session Trace	176
25.1.2 Session Trace Filename Convention	177
Chapter 26	
SNMP	178
26.1 SNMP Overview	178
26.1.1 Network Management System (NMS)	179
26.2 Configuring SNMP	179
Chapter 27	
Miscellanea	182
27.1 Overview	182
27.2 TCP/IP-RS-232 Converter Setup	182

Chapter 28	
System Status.....	184
28.1 System Status Overview	184
28.2 System Information	184
28.3 Current User List	186
28.4 DHCP Client	187
28.5 Session List	188
28.6 NAT Pool Table	189
28.7 LAN Device Status	189
28.7.1 Accessing the LAN Device	190
28.8 Billing Log	191
28.8.1 Billing Logs Backup	192
28.9 PMS Transaction	193
28.10 Static Route Table	193
Chapter 29	
Configuration.....	196
29.1 Configuration Overview	196
29.2 Configuration Backup	196
29.2.1 Configuration Backup Using TFTP	198
29.3 Restore Configuration	199
29.3.1 Restore Configuration Using TFTP	199
29.4 Reset to the Factory Defaults	200
Chapter 30	
Firmware	202
30.1 Firmware Overview	202
30.2 Manual Firmware Upgrade	202
30.2.1 Manual Firmware Upgrade via a TFTP Server	203
30.3 Scheduled Firmware Upgrade	204
Chapter 31	
SSL Certificate.....	206
31.1 SSL Certificate Overview	206
31.1.1 Certificate	206
31.1.2 Certificate Authorities	206
31.2 Downloading SSL Certificate to the VSG	206
31.3 Activating SSL Security	207
31.4 Installing SSL Certificate on a Computer	208
Chapter 32	
Using The SMT	214
32.1 About the SMT	214

32.1.1 Establishing a Console Port Connection	214
32.2 SMT Login Screen	215
32.3 The SMT Main Menu Summary	215
32.4 Navigating the SMT Interface	216
32.4.1 The Navigation Keys	217
32.5 System Configuration	217
32.6 WAN Configuration	218
32.6.1 WAN Type: Static/Dynamic	218
32.6.2 WAN Type: PPPoE	219
32.6.3 WAN Type: PPTP	220
32.7 LAN Configuration	222
32.8 System Status	223
32.9 System Utilities	224
32.9.1 Firmware Upgrade	225
32.9.2 Changing the Administrator Login Password	226
32.10 Restart	227
32.11 SMT Logout	227
32.12 Factory Defaults	227
 Chapter 33	
Troubleshooting	230
33.1 Using the LEDs to Diagnose Problems	230
33.1.1 The Power LED	230
33.1.2 The LAN Port LEDs	230
33.1.3 The WAN Port LEDs	231
33.2 The Console Port	231
33.3 Web Configurator	232
33.4 Internet Access	232
33.5 The Statement Printer	233
 Appendix A	
Product Specifications	234
 Appendix B	
IP Address Assignment Conflicts.....	236
 Appendix C	
Subscriber Login.....	240
 Appendix D	
Vendor Specific Attributes	242
 Appendix E	

Report Printing Using the SP-200.....	246
Appendix F	
Cable Types and Cable Pin Assignments	252
Appendix G	
Setting up Your Computer's IP Address	256
Appendix H	
IP Addresses and Subnetting	268
Index.....	276

List of Figures

Figure 1	Application: Internet Access for LAN Networks	35
Figure 2	Application: Internet Access in Public Areas	36
Figure 3	Application: Hotel	36
Figure 4	Rack Mount: Attaching Brackets	39
Figure 5	Rack Mount: Securing to the Rack	39
Figure 6	Front Panel	40
Figure 7	Rear Panel	41
Figure 8	Entering IP Address in Internet Explorer	42
Figure 9	Web Configurator: Login	43
Figure 10	Web Configurator: Main Menu	43
Figure 11	Web Configurator: Navigation Panel	44
Figure 12	Navigation Panel: Screen specific Links	44
Figure 13	Apply: Success	45
Figure 14	Apply: Restart	45
Figure 15	System Tools: System Account	46
Figure 16	System Tools: Restart	48
Figure 17	System Tools: Logout	48
Figure 18	Initial Setup: Network Example	50
Figure 19	System Setting: System	56
Figure 20	System Settings: WAN/LAN: LAN Configuration	62
Figure 21	System Settings: WAN/LAN: WAN MAC Address	63
Figure 22	System Settings: WAN/LAN: Dynamic/Static WAN IP Address	64
Figure 23	System Settings: WAN/LAN: PPPoE	65
Figure 24	System Settings: WAN/LAN: PPTP	67
Figure 25	System Settings: Server	71
Figure 26	NAT Example: One-to-One	76
Figure 27	NAT Example: Many-to-One	77
Figure 28	NAT Example: One-to-One and Many-to-One	77
Figure 29	System Settings: NAT Pool	78
Figure 30	CAS Example	80
Figure 31	Accounting Usage Time	82
Figure 32	System Settings: Authentication	83
Figure 33	System: Authentication: Scenario Guide	86
Figure 34	Subscriber Login: Scenario A	87
Figure 35	Subscriber Login: Scenario B	87
Figure 36	Subscriber Login: Scenario C	87
Figure 37	System Setting: Billing: Billing Profile	88
Figure 38	System Settings: Billing: Billing Profile Setting	89

Figure 39	System Setting: Billing: PMS Configuration	92
Figure 40	Static Account: Links	94
Figure 41	Static Account Settings: Global Settings	94
Figure 42	System Settings: Create Static Subscriber Account	95
Figure 43	Create Static Subscriber Account: Generate Automatically	96
Figure 44	Create Static Subscriber Account: Manual	97
Figure 45	Static Subscriber Account: Backup and Restore	98
Figure 46	Static Subscriber Account: Backup and Restore: File Download	99
Figure 47	Static Subscriber Account: Backup and Restore: Save As	99
Figure 48	Static Subscriber Account: Backup and Restore	100
Figure 49	Static Account Operator	100
Figure 50	Static Account Information Printout Example	102
Figure 51	Static Account List	102
Figure 52	Dynamic Account: Links	104
Figure 53	Accounting: Dynamic Account Setting	105
Figure 54	SP-200 Button Labels	106
Figure 55	Dynamic Account Operator Panel	107
Figure 56	Dynamic Account Information Printout Example	107
Figure 57	Dynamic Account List	108
Figure 58	Dynamic Account List Backup: File Download	109
Figure 59	Dynamic Account List Backup: Save As	110
Figure 60	System Setting: Port-Location Mapping	113
Figure 61	Advanced Setting: Credit Card	117
Figure 62	Customization: Login	121
Figure 63	Customization: Login: Standard	122
Figure 64	Subscriber Login Screen Example: Standard	122
Figure 65	Customization: Login Screen: Redirect	122
Figure 66	Customization: Login Screen: Advanced	123
Figure 67	Subscriber Login Screen Example: Advanced	124
Figure 68	Customization: Login Screen: Frame	124
Figure 69	Subscriber Login Screen Example: Frame	125
Figure 70	Customization: Service Selection Customization	126
Figure 71	Subscriber Login Screen Example: Service Selection Messages	126
Figure 72	Customization: Information Window	127
Figure 73	Subscriber Pop-up Information Window Example	128
Figure 74	Customization: Account Printout	129
Figure 75	Static Account Printout Example	131
Figure 76	Static Account with PMS Billing Printout Example	131
Figure 77	Static Account Printout: Statement Printer Example	132
Figure 78	Static Account with PMS Billing Printout: Statement Printer Example	132
Figure 79	Dynamic Account Printout Example	133
Figure 80	Dynamic Account Printout: Statement Printer Example	133
Figure 81	Customize: User Agreement	134

Figure 82	Customization: Account Printout: Preview	135
Figure 83	Credit Card Customization: Standard Login Screen Message	135
Figure 84	Credit Card Customization: Standard Login Screen Message: Preview	136
Figure 85	Credit Card Customization: Service Selection Page	137
Figure 86	Credit Card Customization: Service Selection Page: Preview	139
Figure 87	Credit Card Customization: Successful Page	140
Figure 88	Credit Card Customization: Successful Page: Preview	141
Figure 89	Credit Card Customization: Fail Page	141
Figure 90	Credit Card Customization: Fail Page: Preview	142
Figure 91	Customization: Output Bill	142
Figure 92	Customization: Output Bill: Example	143
Figure 93	Bandwidth Management: Activate	145
Figure 94	Bandwidth Management: Equal Share	145
Figure 95	Bandwidth Management: Class of Service	146
Figure 96	Portal Page	148
Figure 97	Advertisement	149
Figure 98	Walled Garden	150
Figure 99	Subscriber Login Screen with Walled Garden Links Example	151
Figure 100	Passthrough: Subscriber IP and MAC Address	153
Figure 101	Passthrough: Destination URL and IP	154
Figure 102	Advanced: Filter	156
Figure 103	Privilege User	158
Figure 104	Privilege User: Access Session List Example	159
Figure 105	LAN Devices	161
Figure 106	LAN Device Remote Management Example 1	162
Figure 107	LAN Devices: Example 1	162
Figure 108	LAN Device Remote Management Example 2	163
Figure 109	LAN Devices: Example 2	163
Figure 110	Sample Static Routing Topology	164
Figure 111	Advanced: Static Route	165
Figure 112	Private LAN Network Example	168
Figure 113	Private LAN	169
Figure 114	Logs: Syslog	170
Figure 115	Logs: Log Settings	172
Figure 116	Advanced: Session Trace	176
Figure 117	Session Trace Information Example	177
Figure 118	SNMP Management Model	178
Figure 119	SNMP	179
Figure 120	Network Example Using TCP/IP-RS232 Convertor	182
Figure 121	Advanced Setup: Miscellanea	183
Figure 122	System Status: System	184
Figure 123	System Status: Current User List	186
Figure 124	System Status: DHCP Clients	188

Figure 125	System Status: Session List	188
Figure 126	System Status: NAT Pool Table	189
Figure 127	System Status: LAN Device Status	190
Figure 128	System Status: Billing Log	191
Figure 129	Billing Log Backup: File Download	192
Figure 130	Billing Log Backup: Save As	192
Figure 131	Billing Log Backup: Example File Content	193
Figure 132	System Status: PMS Transaction Log	193
Figure 133	System Status: Static Route Table	193
Figure 134	Configuration: Backup	197
Figure 135	Configuration Backup: File Download	197
Figure 136	Configuration Backup: Save As	198
Figure 137	Configuration: Backup using TFTP	198
Figure 138	Configuration Backup: TFTP: Successful	199
Figure 139	Configuration: Restore	199
Figure 140	Configuration: Restore: TFTP	200
Figure 141	Configuration: Reset	201
Figure 142	Firmware: Links	202
Figure 143	Firmware: Manual Upgrade	202
Figure 144	Web Configurator: Firmware Upgrade Successful	203
Figure 145	Firmware: Manual Upgrade Using TFTP	203
Figure 146	Scheduled Firmware Upgrade: Synchronization File Example	204
Figure 147	Scheduled Firmware Upgrade Example	204
Figure 148	Firmware: Scheduled Upgrade	204
Figure 149	SSL Certificate	207
Figure 150	System Settings: Server Configuration: Enable SSL Security	207
Figure 151	System Settings: Authentication: Activate SSL Login	208
Figure 152	Installing the SSL Security Certificate: First Security Alert	208
Figure 153	Installing the SSL Security Certificate: Second Security Alert	209
Figure 154	Installing the SSL Security Certificate: View Certificate	209
Figure 155	Installing the SSL Security Certificate: Certificate Import Wizard	210
Figure 156	Certificate Import Wizard: Location	210
Figure 157	Certificate Import Wizard: Finish	211
Figure 158	Root Certificate Store	211
Figure 159	Certificate Import Wizard	211
Figure 160	Certificate: Detailed Information	212
Figure 161	Security Alert: Trusted	212
Figure 162	HyperTerminal Communication Parameter Settings Example	215
Figure 163	SMT: Login Screen	215
Figure 164	SMT: Main Menu	216
Figure 165	SMT: System Configuration	217
Figure 166	SMT: WAN Configuration: Static/Dynamic	218
Figure 167	SMT: WAN Configuration: PPPoE	219

Figure 168 SMT: WAN Configuration: PPTP	221
Figure 169 SMT: LAN Configuration	222
Figure 170 SMT: System Status	223
Figure 171 SMT: Utilities Menu	225
Figure 172 SMT: Firmware Upgrade	225
Figure 173 SMT: Firmware Upgrade Process	226
Figure 174 SMT: Change Administrator Password	226
Figure 175 SMT: Restart	227
Figure 176 SMT: System Logout	227
Figure 177 SMT: Reset to Factory Defaults	228
Figure 178 IP Address Conflicts: Scenario 1	236
Figure 179 IP Address Conflicts: Scenario 2	236
Figure 180 IP Address Conflicts: Scenario 3	237
Figure 181 IP Address Conflicts: Scenario 4	238
Figure 182 Subscriber Login Screen: Framed Example	240
Figure 183 Subscriber Login: Information Window Example	240
Figure 184 SP-200: Daily Account	247
Figure 185 SP-200: Monthly Account	248
Figure 186 SP-200: System Status	249
Figure 187 SP-200: Network Statistics	250
Figure 188 WAN Port Cable Pin Assignments	253
Figure 189 LAN Port Cable Pin Assignments	253
Figure 190 DB25 Male to DB9 Male Connector	254
Figure 191 WIndows 95/98/Me: Network: Configuration	257
Figure 192 Windows 95/98/Me: TCP/IP Properties: IP Address	258
Figure 193 Windows 95/98/Me: TCP/IP Properties: DNS Configuration	259
Figure 194 Windows XP: Start Menu	260
Figure 195 Windows XP: Control Panel	260
Figure 196 Windows XP: Control Panel: Network Connections: Properties	261
Figure 197 Windows XP: Local Area Connection Properties	261
Figure 198 Windows XP: Advanced TCP/IP Settings	262
Figure 199 Windows XP: Internet Protocol (TCP/IP) Properties	263
Figure 200 Macintosh OS 8/9: Apple Menu	264
Figure 201 Macintosh OS 8/9: TCP/IP	264
Figure 202 Macintosh OS X: Apple Menu	265
Figure 203 Macintosh OS X: Network	266

List of Tables

Table 1	Front Panel LEDs	41
Table 2	Web Configurator: Screen Overview	44
Table 3	System Tools: System Account	46
Table 4	System Setting: System	57
Table 5	System Settings: WAN/LAN: LAN Configuration	62
Table 6	System Settings: WAN/LAN: WAN MAC Address	63
Table 7	System Settings: WAN/LAN: WAN IP	64
Table 8	System Settings: WAN/LAN: PPPoE	65
Table 9	System Settings: WAN/LAN: PPTP	67
Table 10	System Settings: Server	71
Table 11	NAT Definitions	74
Table 12	WAN NAT Mapping Types for VPN	76
Table 13	NAT Example: One-to-One	76
Table 14	NAT Example: Many-to-One	77
Table 15	NAT Example: One-to-One and Many-to-One	78
Table 16	System Settings: NAT Pool	78
Table 17	System Settings: Authentication	84
Table 18	System: Authentication: Scenario Guide	87
Table 19	System Setting: Billing: Billing Profile	89
Table 20	System Settings: Billing: Billing Profile Setting	90
Table 21	System Setting: Billing: PMS Configuration	92
Table 22	Static Account Settings: Global Settings	95
Table 23	Create Static Subscriber Account: Generate Automatically	96
Table 24	Create Static Subscriber Account: Manual	97
Table 25	Static Account Operator	100
Table 26	Static Account List	103
Table 27	Accounting: Dynamic Account Setting	105
Table 28	Dynamic Account List	108
Table 29	System Setting: Port-Location Mapping	113
Table 30	Advanced Setting: Credit Card	117
Table 31	Customization: Login: Standard	122
Table 32	Customization: Login Screen: Redirect	123
Table 33	Customization: Login Screen: Advanced	123
Table 34	Customization: Login Screen: Frame	125
Table 35	Customization: Service Selection Customization	126
Table 36	Customization: Information Window	128
Table 37	Customization: Account Printout	129
Table 38	Customization: Account Printout	134

Table 39	Credit Card Customization: Service Selection Page	138
Table 40	Credit Card Customization: Successful Page	140
Table 41	Credit Card Customization: Fail Page	141
Table 42	Customization: Output Bill	143
Table 43	Bandwidth Management: Equal Share	146
Table 44	Portal Page	148
Table 45	Advertisement	149
Table 46	Walled Garden	150
Table 47	Passthrough: Subscriber IP and MAC Address	153
Table 48	Passthrough: Destination URL and IP	154
Table 49	Filter	156
Table 50	Privilege User	158
Table 51	LAN Devices	161
Table 52	Advanced: Static Route	165
Table 53	Advanced: Private LAN	169
Table 54	Logs: Syslog	171
Table 55	Logs: Log Settings	172
Table 56	Logs: Log Format	173
Table 57	Advanced: Session Trace	176
Table 58	Session Trace File Fields	177
Table 59	SNMP	180
Table 60	Miscellanea	183
Table 61	System Status: System	185
Table 62	System Status: Current User List	187
Table 63	System Status: DHCP Clients	188
Table 64	System Status: Session List	188
Table 65	System Status: NAT Tool Table	189
Table 66	System Status: LAN Device Status	190
Table 67	System Status: Billing Log	191
Table 68	System Status: Static Route Table	194
Table 69	Firmware: Scheduled Upgrade	205
Table 70	SSL Certificate	207
Table 71	SMT: Main Menu	216
Table 72	SMT: Control Key Descriptions	217
Table 73	SMT: System Configuration	217
Table 74	SMT: WAN Configuration: Static or Dynamic IP Address	219
Table 75	SMT: WAN Configuration: PPPoE	220
Table 76	SMT: WAN Configuration: PPTP	221
Table 77	SMT: LAN Configuration	222
Table 78	SMT: System Status	223
Table 79	Troubleshooting the Power LED	230
Table 80	Troubleshooting the LAN LED	230
Table 81	Troubleshooting the WAN LED	231

Table 82	Troubleshooting Console Port	231
Table 83	Troubleshooting Web Configurator	232
Table 84	Troubleshooting Internet Browser Display	232
Table 85	Troubleshooting Internet Access	232
Table 86	Troubleshooting the Statement Printer	233
Table 87	Product Specifications: General	234
Table 88	Product Specifications: Performance and Management	235
Table 89	Product Specifications: Physical and Environmental	235
Table 90	VSG-1200 V2 Supported VSAs	243
Table 91	VSA-related Error Messages	244
Table 92	SP-200: Report Printing Key Combination	247
Table 93	SP-200: System Status	249
Table 94	SP-200: Network Statistics	251
Table 95	Network Cable Types	252
Table 96	WAN Port Cable Ping Assignments	252
Table 97	LAN Port Cable Pin Assignments	253
Table 98	Console Port Pin Assignment	254
Table 99	DB25 Male to DB9 Male Connector Ping Assignment	254
Table 100	Classes of IP Addresses	269
Table 101	Allowed IP Address Range By Class	269
Table 102	“Natural” Masks	270
Table 103	Alternative Subnet Mask Notation	270
Table 104	Two Subnets Example	271
Table 105	Subnet 1	271
Table 106	Subnet 2	272
Table 107	Subnet 1	272
Table 108	Subnet 2	273
Table 109	Subnet 3	273
Table 110	Subnet 4	273
Table 111	Eight Subnets	274
Table 112	Class C Subnet Planning	274
Table 113	Class B Subnet Planning	275

Preface

Congratulations on your purchase of the VSG-1200 V2 Vantage Service Gateway.

Note: Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

About This User's Guide

This manual is designed to guide you through the configuration of your VSG-1200 V2 for its various applications. The web configurator parts of this guide contain background information on features configurable by web configurator. The SMT parts of this guide contain background information solely on features not configurable by web configurator.

Note: Use the web configurator or System Management Terminal (SMT) to configure your VSG-1200 V2. Not all features can be configured through all interfaces.

Related Documentation

- Supporting Disk
Refer to the included CD for support documents.
- ZyXEL Glossary and Web Site
Please refer to www.zyxel.com for an online glossary of networking terms and additional support documentation.

User Guide Feedback

Help us help you! E-mail all User 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 Convention

- “Enter” means for you to type one or more characters. “Select” or “Choose” means for you to use one of the predefined choices.
- Command and arrow keys are enclosed in square brackets. [ENTER] means the Enter, or carriage return key; [ESC] means the Escape key and [SPACE BAR] means the Space Bar.
- Mouse action sequences are denoted using a comma. For example, “click the Apple icon, **Control Panels** and then **Modem**” means first click the Apple icon, then point your mouse pointer to **Control Panels** and then click **Modem**.
- For brevity’s sake, we will use “e.g.,” as a shorthand for “for instance”, and “i.e.,” for “that is” or “in other words” throughout this manual.
- The VSG-1200 V2 Vantage Service Gateway may be referred to as “the VSG-1200 V2” or, simply, as “the VSG” in this User’s Guide.

Graphics Icons Key

VSG-1200 V2 	Computer 	Notebook computer 
Server 	Statement Printer 	Access Point 
Switch 	Router 	Internet 

CHAPTER 1

Getting to Know Your VSG

This chapter introduces the features and applications of the VSG.

1.1 Introducing the VSG

The VSG-1200 V2 Vantage Service Gateway is a rack-mountable service gateway that provides multiple subscribers easy Internet connectivity. The VSG is ideal for office, hotspot and hotel network environments.

Hotspots are public areas, such as airports, hotels, coffee shops, where end users (or subscribers) can access the Internet at any time.

1.2 Features

Your VSG provides the following features to accommodate subscribers with a variety of network configurations with little or no technical support.

Property Management System (PMS)

Many hotels use a PMS to perform automatic billing of services the guests use such as room service, mini-bar, pay-per-view TV or telephone calls. The VSG supports PMS from Micros Fidelios.

CAS (Central Authentication Service)

The Hilton Group Corporation developed the High Speed Internet Access (HSIA) service to provide Internet access service across its entire Hilton Group hotels. In order to use the HSIA, hotel guest(s) must be authenticated through the proprietary CAS. The CAS performs both user authentication and accounting.

Credit Card Billing

Your VSG is integrated with various online credit card billing service providers allowing you to use a credit card service to authorize, process, and manage credit card transactions directly through the Internet.

SSL Secure Login

With Secure Socket Layer (SSL) security activated upon login, data exchanged between the VSG and client computers is encrypted and protected.

PPPoE Support (RFC2516)

PPPoE (Point-to-Point Protocol over Ethernet) emulates a dial-up connection. It allows your ISP to use their existing network configuration with newer broadband technologies such as ADSL. The PPPoE driver on the VSG is transparent to the computers on the LAN, which see only Ethernet and are not aware of PPPoE; thus saving you from having to manage PPPoE clients on individual computers.

PPTP Support

Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables secure transfer of data from a remote client to a private server, creating a Virtual Private Network (VPN) using a TCP/IP-based network. PPTP supports on-demand, multi-protocol and virtual private networking over public networks, such as the Internet. Subscribers can use PPTP to connect to a broadband modem to achieve access to high-speed data networks via a familiar "dialup networking" user interface.

Reset Button

Use the reset button to restore the VSG back to its factory defaults.

Plug-and-Play Internet Access

The VSG provides Internet access to attached computer(s) without extra software installation or computer configuration. In addition, with transparent proxy, the VSG resolves any incompatible proxy settings.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network.

DHCP Support

DHCP (Dynamic Host Configuration Protocol) allows the individual computers (DHCP clients) to obtain TCP/IP configuration at start-up from a centralized DHCP server. The VSG has built-in DHCP server capability. It can assign IP addresses, an IP default gateway and DNS servers to DHCP clients. The VSG can also act as a surrogate DHCP server (DHCP Relay) where it relays IP address assignment from the actual real DHCP server to the DHCP clients.

RADIUS (Remote Authentication Dial-In User Service)

The VSG allows you to maintain a central subscriber database on an external RADIUS server. Subscriber accounting and authentication is then done through the external RADIUS server. In addition, the VSG supports Vendor Specific Attributes (VSAs) that allows enforcement of upload/download bandwidth limits or specific advertisement web page per subscriber.

Local Subscriber Database

The VSG allows you to maintain a subscriber database on the VSG without setting up an external RADIUS server. Subscriber accounting and authentication are done using the local subscriber database.

Accounting

Accounting can be done using an external RADIUS server or the built-in accounting feature.

Local Content and Advertising Links

Once connected to the network, the VSG can redirect the subscriber to a specified web site and display advertising links. This can be a source of extra online advertising revenues and increased business exposure.

Access Control (Walled Garden)

With the walled garden feature, subscribers are able to access predetermined web sites without logging in. The VSG blocks full Internet access until the subscribers log in.

E-mail Forwarding

The VSG is able to forward and retrieve e-mail messages when the subscriber's default e-mail server is down or behind a firewall.

DNS Proxy

With DNS proxy, the VSG provides DNS redirection when a subscriber's configured DNS server is behind a firewall or located in a private Intranet.

NAT (Network Address Translation)

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

The VSG automatically performs NAT on the LAN. You can also set the VSG to perform NAT on the WAN for VPN (IPSec and PPTP) connections.

Static Route

Static routes tell the VSG how to forward IP traffic when you configure the TCP/IP parameters manually and disable NAT.

Subscriber Login Page Customization

You can customize the subscriber login page according to your business needs. The advanced settings allow you to include welcome messages, a company logo and basic formatting.

Dual-function Console Port

The VSG provides a console port for local management. You can also set this console port to act as the printer port when connected to an external statement printer.

Web Configurator Management

The VSG comes with an embedded web-based configurator. It offers advanced management features and allows you to manage the VSG remotely using Internet Explorer (version 5.5 or above) or Netscape (version 6.0 or later).

System Maintenance

The firmware of the VSG can be upgraded via the web configurator or the SMT menu. The Embedded FTP server is for firmware upgrades as well as configuration file backups and restoration.

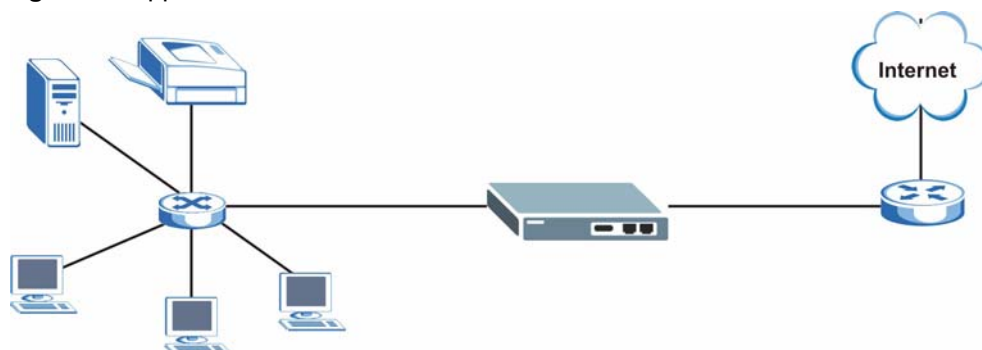
1.3 Applications

The following sections describe network application examples in which the VSG is used.

1.3.1 Internet Access for LAN Networks

With a broadband service account set up, the VSG allows the attached computers to enjoy high speed Internet access.

Figure 1 Application: Internet Access for LAN Networks

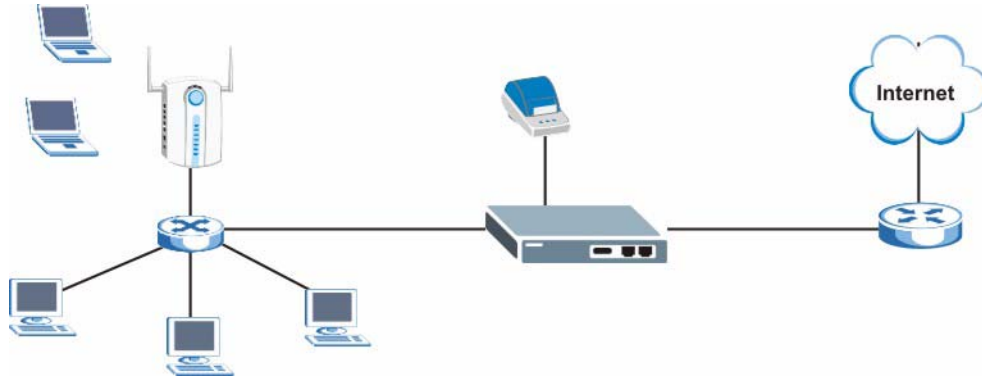


1.3.2 Internet Access in Public Areas

In public areas, such as a hotel, the VSG provides high speed Internet access to subscribers. Account billing and authentication can be done either using an external RADIUS server or the built-in billing function and local subscriber database.

Connect an access point (AP) to bridge the wired and the wireless network allowing wireless stations to access the Internet through the VSG.

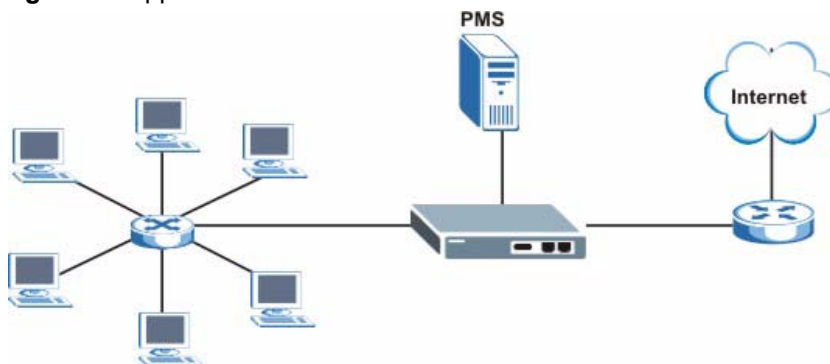
Figure 2 Application: Internet Access in Public Areas



1.3.3 Hotel Application with PMS

The following figure depicts an example where the VSG is used in a hotel to provide Internet service as one of their in-room services. Billing is done through an existing PMS in the hotel.

Figure 3 Application: Hotel



CHAPTER 2

Hardware Installation and Connection

This chapter shows you how to install the VSG and make hardware connections.

2.1 Installation Options

The following sections describe the different installation options.

Note: Do NOT block the ventilation holes and leave adequate space on the rear and sides of the VSG during hardware installation or when stacking.

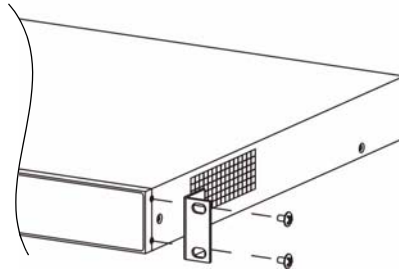
2.1.1 Desktop Installation

- 1 Make sure the VSG is clean and dry. Set the VSG on a smooth space strong enough to support the weight of the VSG and the connected cables. Make sure there is a power outlet nearby.
- 2 Make sure there is enough clearance around the VSG to allow air circulation and the attachment of cables and the power cord.
- 3 Attach the rubber feet to each corner on the bottom of the VSG. These rubber feet help protect the VSG from shock or vibration and ensure space between devices when stacking.

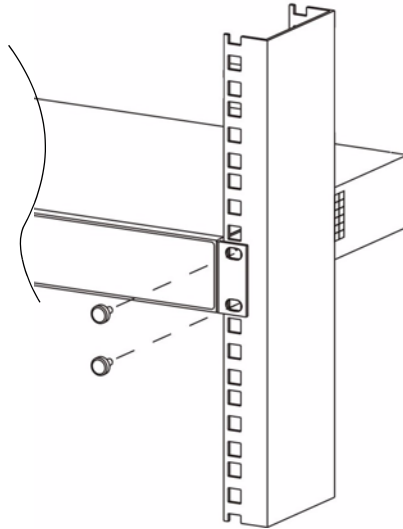
2.1.2 Rack Mount Installation

The VSG can be mounted on an EIA standard size, 19-inch rack or in a wiring closet with other equipment. Follow the steps below to mount your VSG on a standard EIA rack using the included rack-mounting kit.

- 1 Align one bracket with the holes on one side of the VSG and secure it with the bracket screws (smaller than the rack-mounting screws. Similarly, attach the other bracket.

Figure 4 Rack Mount: Attaching Brackets

- 2** After attaching both mounting brackets, position the VSG in the rack by lining up the holes in the brackets with the appropriate holes on the rack. Secure the VSG to the rack with rack-mounting screws.

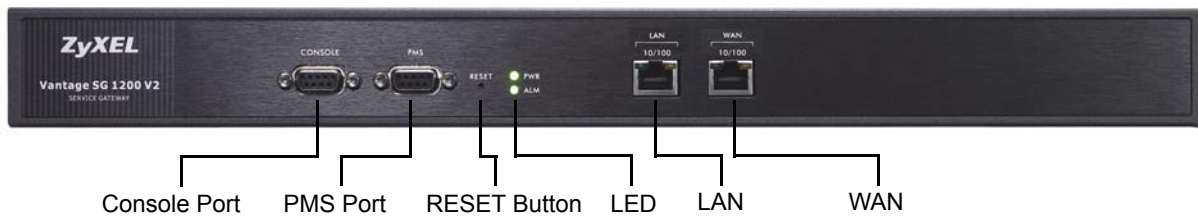
Figure 5 Rack Mount: Securing to the Rack

2.2 Hardware Connections

The following sections describe the hardware connections of the VSG.

2.2.1 Front Panel

The console, LAN and WAN ports, the reset button and the LEDs are located on the front panel.

Figure 6 Front Panel

2.2.1.1 LAN Port

The VSG has one 10/100Mbps Ethernet port. The LAN port is auto-crossover, so you may use a crossover or a straight-through Ethernet cable to connect your VSG to a computer/external switch.

If you want to connect more than one Ethernet devices to your VSG, you must use an external hub/switch. Connect a LAN port on the VSG to a port on the switch using an Ethernet cable.

2.2.1.2 WAN Port

Connect the VSG to a network with broadband Internet service. The WAN port is auto-crossover, so you may use a crossover Ethernet cable or a straight-through Ethernet cable to connect your VSG to a router.

2.2.1.3 Console Port

Local management of the VSG is done through the port labeled **CONSOLE**. It requires a direct connection between the VSG and a computer via a console cable. Refer to chapters on SMT configurations for more information.

You can also connect the **CONSOLE** port to a statement printer (also known as account generator printer, sold separately) with a DB25-male to DB9-male adapter. A statement printer allows you to create and print out subscriber accounts automatically. In addition, you can also print the system status and the account and network reports. Set the function of the console port in the web configurator (see [Section 5.1 on page 56](#)).

2.2.1.4 PMS Port

Use a DB9 console cable to connect the **PMS** port to a PMS system.

2.2.1.5 Reset Button

Use a pointed object to press this button in once to reset the VSG back to the factory defaults.

Note: All your custom configuration including the system usernames and passwords will be erased.

This will NOT delete the subscriber database or the port-location mappings.

2.2.2 Front Panel LEDs

The following table describes the LEDs on the front panel. When turned on, all LEDs are green unless otherwise specified.

Table 1 Front Panel LEDs

LED	STATUS	DESCRIPTION
PWR	On	The VSG is receiving power.
	Off	The VSG is not receiving power.
SYS	On	The system is functioning normally.
	Blinking	The system is not functioning properly.
	Off	The system is not ready or has failed.
LAN or WAN		
10	On	The port is connected at 10 Mbps.
	Blinking	The port is receiving or sending data.
	Off	The port is not connected to an Ethernet device.
100	On	The port is connected at 100 Mbps.
	Blinking	The port is receiving or sending data.
	Off	The port is not connected to an Ethernet device.

2.2.3 Rear Panel

The power socket, the fan and a ventilation hole are located on the rear panel as shown next.

Note: Do NOT block the ventilation hole.

Figure 7 Rear Panel



2.2.4 Turning on the VSG

Connect the female end of the supplied power cord to the power socket on the back of the VSG and the male end to an appropriate power source.

When the power source is turned on, the **PWR** LED on the front panel turns on.

CHAPTER 3

The Web Configurator

This chapter introduces how to access the web configurator and perform general system configuration.

3.1 Introducing the Web Configurator

The web configurator is best viewed with Internet Explorer (version 5.5 or above) or Netscape (version 6. or later).

Note: JavaScript support must be enabled.

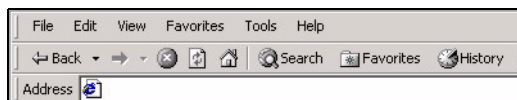
3.2 Accessing the Web Configurator

Follow the steps below to access the web configurator.

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

- 1 Make sure your VSG is properly connected (refer to the instructions in [Chapter 2 on page 38](#)).
- 2 Launch your web browser and type the WAN or LAN IP address of the VSG as the web site address. **192.168.1.1** is the default IP address for the WAN port and **10.59.1.1** is the default IP address for the LAN port.
- 3 If you are using a different port number (between 8000 and 8099) for the web server, you must also append the port number to the WAN IP address separated with a colon “:”, for example, `http://192.168.1.1:8080`.

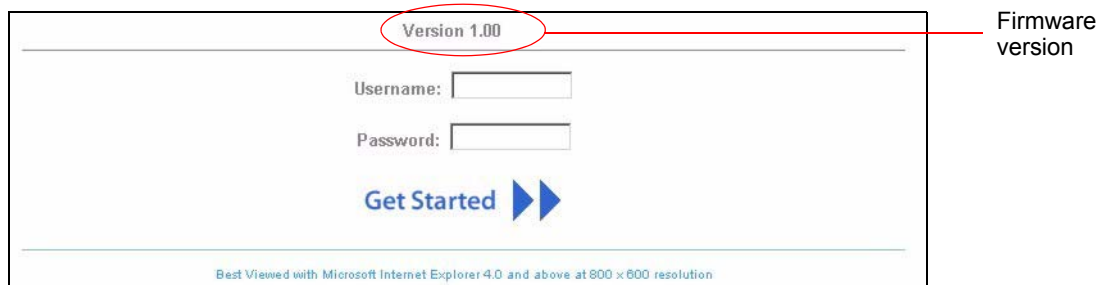
Figure 8 Entering IP Address in Internet Explorer



- 4 A login screen displays. Type “admin” (default) as the administrator user name and “1234” (default) as the password and click **Get Started ...**

Note: The user name and password are case sensitive.

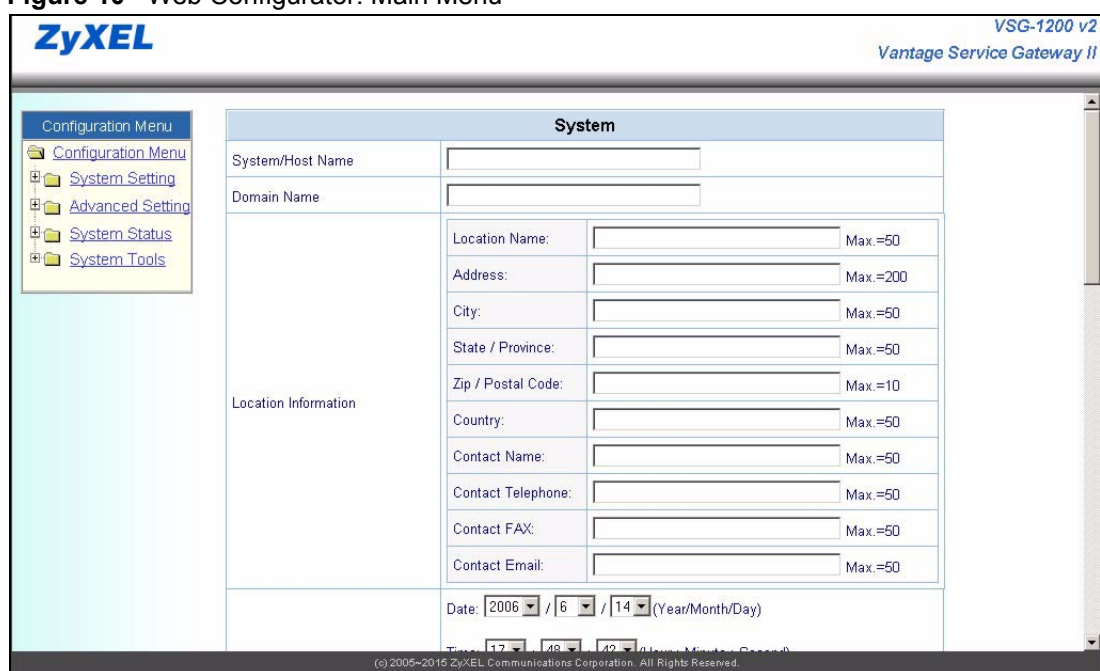
Figure 9 Web Configurator: Login



The login screen displays the text "Version 1.00" at the top center, which is circled in red. Below this, there are two input fields: "Username:" and "Password:". A blue "Get Started" button with a right-pointing arrow is positioned below the password field. At the bottom of the screen, a small note reads "Best Viewed with Microsoft Internet Explorer 4.0 and above at 800 x 600 resolution". A red line points from the text "Firmware version" to the "Version 1.00" text.

5 You should see the main screen as shown.

Figure 10 Web Configurator: Main Menu



The main menu screen features the ZyXEL logo and "VSG-1200 v2 Vantage Service Gateway II" in the top right corner. On the left is a "Configuration Menu" sidebar with links to "Configuration Menu", "System Setting", "Advanced Setting", "System Status", and "System Tools". The main area is titled "System" and contains a form for "Location Information". This form includes fields for "System/Host Name", "Domain Name", "Location Name" (Max.=50), "Address" (Max.=200), "City" (Max.=50), "State / Province" (Max.=50), "Zip / Postal Code" (Max.=10), "Country" (Max.=50), "Contact Name" (Max.=50), "Contact Telephone" (Max.=50), "Contact FAX" (Max.=50), and "Contact Email" (Max.=50). At the bottom, there is a date field set to "2006 / 6 / 14 (Year/Month/Day)". A footer at the very bottom reads "(c) 2005-2015 ZyXEL Communications Corporation. All Rights Reserved."

Note: If there is no activity for longer than five minutes after you log in, the VSG will automatically log you out. If this happens, simply log back in again. You can change the timeout period in the web configurator (refer to [Chapter 7 on page 70](#)).

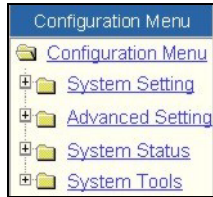
3.3 Navigation Panel

The VSG web configurator provides two levels of navigation: the **Configuration Menu** panel and a screen-specific link panel.

3.3.1 The Navigation Panel

The navigation panel on the left of all web pages provides a consistent way to access the configuration screens. Click each heading to expand the menu.

Figure 11 Web Configurator: Navigation Panel



3.3.2 Screen Specific Links

In some screens, a link panel displays on the top of the screen that allows you to navigate to advanced configuration screens. An example is shown in the figure below.

Figure 12 Navigation Panel: Screen specific Links



3.4 Screen Overview

The following table lists the various web configurator screens.

Table 2 Web Configurator: Screen Overview

SYSTEM SETTINGS	ADVANCED SETTINGS	SYSTEM STATUS	SYSTEM TOOLS

3.4.1 Saving Configuration Changes

In a configuration screen, you must click **Apply** to save the changes. A **Success** screen displays when the configuration settings are saved to the VSG. Click **back** to return to the previous screen.

Figure 13 Apply: Success



For specific settings (such as the device IP address, subscriber authentication method, etc.), you will be prompted to restart the VSG after you click **Apply** in the configuration screen. A **Restart** screen displays. Click **Apply** again to restart the VSG and make the changes take effect.

Figure 14 Apply: Restart



3.5 System Login Accounts

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

- The administrator account allows you full access to all system configurations. The default administrator user name is "admin" and password "1234".
- The account manager account is used for subscriber account management only. No system configuration is allowed. This account is useful for front desk personnel (such as in a hotel) for setting up subscriber accounts without tampering with the system configuration. The default user name and password are "account".
- With the supervisor account, you can only view the system status and change the supervisor account password. The default user name are "supervisor".
- The super subscriber account is used for testing the Internet connection between the VSG and the ISP. There is no time limitation or billing imposed on this account. Thus anyone who logs in with this account is able to gain Internet access for free. The default super subscriber user name and password are "super".

3.6 Changing System Login Passwords

Note: It is recommended that you change the system login passwords.

From the **Main Menu** screen, click **System Tools** and **System Account**. You can enter up to 20 alphanumeric characters for the account user name and password and they are case sensitive.

Figure 15 System Tools: System Account

Administrator Account	
Administrator can fully control this system and modify all settings.	
Username:	admin
Password:	123456
Confirm:	
Accounting Manager	
Accounting Operator allows front desk clerk to operate the web-based accounting system without touching the other system configuration.	
Username:	account
Password:	123456789
Confirm:	
Supervisor Account	
Supervisor can only view system status and change password.	
Username:	supervisor
Password:	1234567890123456
Confirm:	
Super Subscriber Account	
Super subscriber is a built-in subscriber account for system test or premium usage.	
Super Subscriber	Disable
Idle Time Out	5 Min(s) (1~1440)
Username:	super
Password:	123456
Confirm:	
Apply	

The following table describes the labels in this screen.

Table 3 System Tools: System Account

LABEL	DESCRIPTION
Administrator Account	This account permits full access to all system configurations.
Username	Enter the user name for the administrative account. The default is admin .
Password	Enter a new administrative account password. The default is 1234 .
Confirm	Enter the new administrator password again for confirmation.
Account Manager	This account allows you to set up subscriber accounts. No system configuration is allowed.
Username	Enter the user name for the account manager account. The default is account .
Password	Enter a new account manager password. The default is account .

Table 3 System Tools: System Account (continued)

LABEL	DESCRIPTION
Confirm	Enter the new administrator password again for confirmation.
Supervisor Account	This account allows you to view device status only.
Username	Enter the user name for the supervisor account. The default is supervisor
Password	Enter a new supervisor password. The default is supervisor .
Confirm	Enter the new administrator password again for confirmation.
Super Subscriber Account	Once you have configured the Internet connection settings on the VSG, you can use this account to test the Internet connection through the VSG.
Super Subscriber	Select Enable to activate this account. Select Disable to deactivate this account.
Idle Timeout	By default, the VSG automatically logs out a super subscriber after five minutes of inactivity. Enter a number (1 to 1440) to set the VSG to log out the super subscriber after the specified inactivity timeout (in minutes).
Username	Enter the user name for the account manager account. The default is super .
Password	Enter a new account manager password. The default is super .
Confirm	Enter the new administrator password again for confirmation.
Apply	Click Apply to save the changes back to the VSG.

3.7 Resetting the VSG

You can restore the device to the factory defaults in one of the following ways.

- The **RESET** button on the front panel of the VSG (press this button once). Use this method for cases when the username and password of the VSG is not known (refer to [Section 2.2.1.5 on page 40](#)).
- The web configurator (refer to [Section 3.7 on page 47](#)).
- The SMT (refer to [Section 29.4 on page 200](#)).

3.8 Restarting the VSG

Note: You must restart the VSG every time you change the system IP address or upload a firmware or configuration file.

All unsaved changes will be lost once you restart the VSG.

In the **Main Menu** screen, click **System Tools**, **Restart** and click **Apply**.

Figure 16 System Tools: Restart

Restart
To Restart the system, click Apply
Apply

3.9 Logging Out of the Web Configurator

In the **Main Menu** screen, click **System Tools**, **Logout** and click **Apply** to exit from the web configurator.

Figure 17 System Tools: Logout

Logout
To Log out of the web configurator, click Apply
Apply

CHAPTER 4

Initial Setup Example

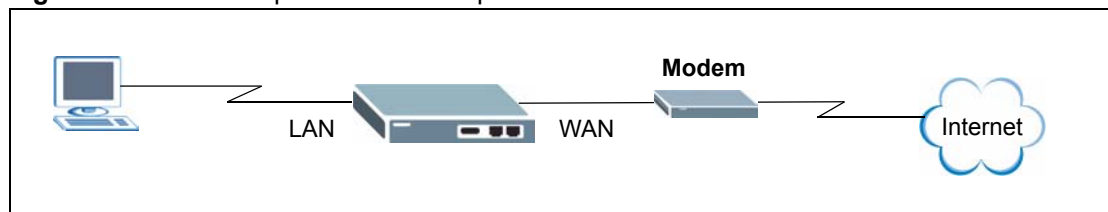
This chapter shows you how to configure the VSG for Internet access and user login.

4.1 Overview

As an Internet cafe owner, you want to set up the VSG in the store and provide Internet service to customers. You have already signed up for Internet access from your local ISP and a DSL modem is installed for Internet connection.

In-store Internet access is provided with a fee. You want to charge \$5 per hour for Internet access and allow customers to purchase up to 15 hours at a time. You create 10 customer accounts and store them on the VSG which checks the account information before Internet access is allowed.

Figure 18 Initial Setup: Network Example



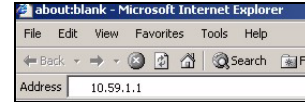
The following outlines the configuration steps.

- 1 You should have already made the hardware connections and turned on the VSG. Refer to [Chapter 2 on page 38](#) for more information.
- 2 Configure the VSG for Internet access using the information provided by your ISP.
- 3 Create a billing profile that charges \$5 per hour of Internet access.
- 4 Set the VSG to prompt for and check customer account information.
- 5 Create customer accounts on the VSG.
- 6 Log in as a customer for connection test.

4.2 Configure the VSG for Internet Access

In this section, you set the VSG to receive a dynamic WAN IP address from the ISP since the ISP does not provide you with a public IP address or Internet access account information.

- 1 Connect your computer to the **LAN** port on the VSG.
Launch your web browser and enter **10.59.1.1** (the default LAN management IP address on the VSG).



- 2 A login screen displays. Type "admin" (default) as the administrator user name and "1234" (default) as the password and click **Get Started ...**

- 3 In the web configurator, click **System Setting > WAN/LAN**.

- 4 Select **Get automatically from a DHCP server** in the **WAN Port Mode** field.
- 5 Click **Apply** to save the changes.
- 6 Click **Apply** again to restart the VSG.
- 7 Log into the web configurator again and check that the VSG has obtained a WAN IP address in the **System Status** screen.

4.3 Create a Billing Profile

Next you create a billing profile that charges \$5 per hour for Internet access and allows customers to purchase up to 15 hours of Internet access time.

- 1 Click **System Setting > Billing** to display the **Billing Profile** screen.
- 2 Change the **Currency** and **Number of decimal places** fields if required.
- 3 To configure a new billing profile, click **Edit** in a new entry.

- 4 The **Billing Profile Setting** screen displays. In the **Name** field, enter “Standard” for identification.
- 5 Enter “\$5/hr” in the **Description** field.
- 6 Select **hour** and enter 5 in the **Charge** field.
- 7 Enter 15 in the **To** field under **Selective Unit**. Leave all other fields to the defaults.
- 8 Click **Apply** and **Close** to save the settings.

Billing Profile Setting

No: 2

Name: Standard

Description: \$5/hr

Price:

Duration	Charge	Check Time	Selective Unit
☐ 1 minute	0	Period Time finish	From: 1 To: 10
☒ 1 hour	5	Period Time finish	From: 1 To: 15
☐ 1 day	10	☐ Period Time finish	From: 1 To: 10
		☐ Expire when 00:00	
☐ 1 week	0	☐ Period Time finish	From: 1 To: 10
		☐ Expire when Sun. 00:00	
☐ 1 month	0	☐ Period Time finish	From: 1 To: 10
		☐ Expire when 01 00:00	
☐ Unlimited	0		

Bandwidth Limit

Note: You must activate the bandwidth management feature and select a class of service

Maximum Upstream Bandwidth: ☐ 64 Kbps ☐ 0 Kbps (64-24576)

Maximum Downstream Bandwidth: ☐ 256 Kbps ☐ 0 Kbps (64-24576)

Service Type

☒ Private Service

☐ Public Service

Reset Apply

- 9 In the **Billing Profile** screen, you should see the name of the profile you have just created. Select **Active** to enable it and click **Apply** to save the settings.

Billing Profile

Currency: \$ (Number of decimals places: 2)

No	Active	Name	Description	Profile Setting
01	☒	Profile 1	1 day \$10.00	Edit
02	☒	Standard	\$5/hr	Edit
03	☐			Edit
04	☐			Edit

4.4 Setting User Authentication Method

You want to configure the VSG to check user account information against the account information stored on its database.

- 1 In the web configurator, click **System Setting > Authentication**.
- 2 Select **Built-in Authentication** and use the default scenario settings.
- 3 Click **Apply** to save the settings.

Authentication Configuration

Authentication Type

☐ No Authentication

☐ User Agreement

☐ Redirect URL Link Code

☐ Standard User Agreement page

☒ Built-in Authentication

Three pre-configured options are provided for easy setup. Select an option that best suits your network needs. You must then proceed to configure the "Billing" and "Accounting" settings to complete your setup.

Current preset option: Scenario C [Select option](#)

☐ RADIUS

- 4 Click **Apply** again to restart the VSG.

4.5 Creating Customer Accounts

For initial setup, you want to configure 10 customer accounts (VIP1, VIP2, VIP3, ..., VIP 10) using the Standard billing profile on the VSG.

- 1 Click **System Setting > Accounting** and click the **Create Static Account**.
- 2 In the **Prefix** field, enter “VIP” which will appear in the account names.
- 3 To create 10 accounts, enter 1 in the **From** field and enter 10 in the **To** field.
- 4 In the **Billing Profile** field, select **Standard** to apply the profile you just created.
- 5 Select **6** in the **Random Password Length** field to have the VSG generate a 6-character password for each account.
- 6 Click **Apply** to generate the accounts. Click **back**.
- 7 To view the list of accounts created, click the **Static Account List** link. You should see the new accounts and the generated passwords.

Create Static Account

Static Accounts can be created and managed by a series of specific number like hotel rooms. Static accounts reside in the flash memory all the time.

Generate a batch of static accounts

This feature can automatically generate a series of specific numbers of accounts like hotel rooms.

Prefix: From: (Maximum 5 numbers)

Postfix: To: (Maximum 5 numbers)

Billing Profile: Random Password Length:

Note: For PMS billing type, use only numbers for subscriber accounts.

Apply

Static Accounts backup and restore

This feature can backup the account information to your computer or restore a previously saved account information file to your system.

Static Account								
refresh		Backup Print List						
No.	Username	Password	Billing Profile	Concurrent Access	First Login	Expiration	Status	Delete
1	VIP1	gw657i64	2 Standard	0			Offline	☐
2	VIP10	djddqz7w	2 Standard	0			Offline	☐
3	VIP2	mmnqv7e	2 Standard	0			Offline	☐
4	VIP3	aebty95v	2 Standard	0			Offline	☐
5	VIP4	nsg7x77j	2 Standard	0			Offline	☐
6	VIP5	ksxmcd7v	2 Standard	0			Offline	☐
7	VIP6	b5tw4277	2 Standard	0			Offline	☐
8	VIP7	9yz6uy7e	2 Standard	0			Offline	☐
9	VIP8	bhgn887b	2 Standard	0			Offline	☐
10	VIP9	qk96xt62	2 Standard	0			Offline	☐
								Delete Delete All
GO 1 Page First Previous Next End								

4.6 Customer Login Test

In this section, you log into the VSG as a customer and test the Internet connection.

- 1 From the **Static Account List** screen, write down a customer account user name and password.
- 2 Log out from the web configurator.
- 3 Make sure your computer is set to use a dynamic IP address and is connected to the **LAN** port on the VSG.
- 4 Open a web browser and enter any web site address (for example, www.zyxel.com).



- 5 A **Welcome** screen displays prompting you to enter the account information.
- 6 Enter the customer account user name and password you wrote down in step 1. Click **Enter**.

A screenshot of a web page titled "Welcome". It features two input fields: "Username:" and "Password:". Below these fields are two buttons: "Enter" and "Cancel".

- 7 An **Information Window** screen displays. This indicates that you have successfully logged into the VSG and Internet access is allowed.



CHAPTER 5

System

This chapter describes the System screen where you can configure general device settings and set up the system time and date.

5.1 General System Setting

The **System** screen displays first when you access the web configurator.

The **Domain Name** entry is what is propagated to the DHCP clients on the LAN. If you leave this blank, the domain name obtained by a DHCP server is used. While you must enter the host name (System Name) on each individual computer, the domain name can be assigned from the VSG via DHCP.

Figure 19 System Setting: System

System							
System/Host Name							
Domain Name							
Location Information	Location Name: Max.=50 Address: Max.=200 City: Max.=50 State / Province: Max.=50 Zip / Postal Code: Max.=10 Country: Max.=50 Contact Name: Max.=50 Contact Telephone: Max.=50 Contact FAX: Max.=50 Contact Email: Max.=50						
	Date: 2006 / 6 / 15 (Year/Month/Day) Time: 09 : 06 : 44 (Hour : Minute : Second) Get from my Computer Get from NTP server ☐ Use NTP (Network Time Protocol) Time Server <table border="1"> <tr> <td>Server IP/Domain Name</td> <td> </td> </tr> <tr> <td>Time Zone</td> <td> GMT-12:00 </td> </tr> <tr> <td>Update Time</td> <td> 0 hours</td> </tr> </table>	Server IP/Domain Name		Time Zone	GMT-12:00	Update Time	0 hours
	Server IP/Domain Name						
	Time Zone	GMT-12:00					
	Update Time	0 hours					
	Date/Time						

	Update Time hours ☐ Daylight Saving Time Start Date: 4 Month / 1 Day End Date: 10 Month / 31 Day
NAT (Network Address Translation)	☒ Enable ☒ IP Plug and Play (iPNP Technology) User Session Limit: ☒ Unlimited ☐ 64 (1~1024) ☐ Disable
Layer 2 Isolation Security	☒ Enable ☐ Disable
Console Type	☒ Console Setting ☐ Statement Printer SP-100
Console Port	Bits per second 9600 Data bits 8 Parity None Stop bits 1
Administrator Authorized Access IP Address	☒ Any ☐ Specify 1 ~ 2 ~ 3 ~ 4 ~ 5 ~
Multicast Passthrough	☐ Enable ☒ Disable
Allow remote user to ping the device	☒ Enable ☐ Disable
SSL Certificate	☒ Default ☐ Custom Certificate
Apply	

The following table describes the labels in this screen.

Table 4 System Setting: System

LABEL	DESCRIPTION
System/ Host Name	Enter a descriptive name (up to 32 characters) for identification purposes.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the VSG may obtain a domain name from a DHCP server. The domain name entered by you is given priority over the DHCP server assigned domain name.
Location Information	Specify where the VSG is located and the person or administrator you can contact in case you have problem using the VSG.
Location Name	Enter a descriptive name of the location for identification purposes.
Address	Enter the street address of the location where the VSG is installed.

Table 4 System Setting: System (continued)

LABEL	DESCRIPTION
City	Enter the name of the city where the VSG is installed.
State/Province	Enter the name of the state or province where the VSG is installed.
Zip/Postal Code	Enter the ZIP or postal code of the location where the VSG is installed.
Country	Enter the name of the country where the VSG is installed.
Contact Name	Enter the name of the person to contact in case there is any problem with the VSG.
Contact Telephone	Enter the telephone number of the person to contact in case there is any problem with the VSG.
Contact Fax	Enter the fax number of the person to contact in case there is any problem with the VSG.
Contact Email	Enter the e-mail address of the person to contact in case there is any problem with the VSG.
Date/Time	To manually set the system date and time, select the appropriate choices from the Date and Time drop-down list boxes. Click Get from my Computer to set the time and date on the VSG to be the same as the computer that you use to configure the VSG. If you select Use NTP (Network Time Protocol) Time Server option and set the necessary fields, you can click Get from NTP Server to update the time and date on the VSG from the NTP time server.
Use NTP (Network Time Protocol) Time Server	Select this option to have the VSG get the date and time information from a time server.
Server IP/ Domain Name	Enter the IP address or the domain name of the time server. Check with your ISP/ network administrator if you are unsure of this information.
Time Zone	Select your time zone from the drop-down list box. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Update Time	Enter the number of hours between updates.
Daylight Savings	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.
Start Date	Specify the month and day that your daylight-savings time starts on if you select Daylight Savings .
End Date	Specify the month and day that your daylight-savings time ends on if you select Daylight Savings .
NAT (Network Address Translation)	NAT (RFC 1631) is the translation of the IP address of a host in a packet, for example, the source address of an outgoing packet, used within one network to a different IP address known within another network. Select Enable to activate Network Address Translation (NAT). Enable this feature to set your VSG to map multiple local IP addresses to one global IP address. This is the default selection. Select Disable to deactivate NAT.
IP Plug and Play (iPnP Technology)	Select this option to allow plug-and-play Internet access which means that subscribers do not have to change their network settings. This feature is activated by default.
DNS Fake IP Reply	Select this option to assign private IP address to a network device (such as the e-mail server). NAT will translate the private IP address to the public IP address on the WAN.

Table 4 System Setting: System (continued)

LABEL	DESCRIPTION
User Session Limit	You can set the VSG to limit the number of sessions each user can use at a time. Select Unlimited to allow each user to use any number of sessions at a time. Select the second option and enter the number of sessions (between 1 and 1024) each user is allowed to use at a time.
Layer 2 Isolation Security	If you activate NAT, select Enable in this field to prevent communication between subscribers. This is the default selection. Select Disable to deactivate layer 2 security and allow communication between subscribers.
Console Type	Use this field to set the function of the console port on the front panel of the VSG. Select Console Setting when you connect the console port directly to a computer for local management. This is the default setting. Select Statement Printer and select the printer model when you connect the console port a statement print.
Console Port	The fields in this section of the screen are applicable when you select Select the fields below to configure the Console port. Note: If you change the console port settings, make sure you also make the same change to the terminal emulator software.
Bits per second	This field only applies when you select Console Setting in the Console Type field. Select a console port speed from the drop-down list box. Choices are 1200, 2400, 4800, 9600 (default), 14400, 19200, 38400, 57600 and 115200 .
Data bits	Select a data bit from the drop-down list box.
Parity	Select the parity from the drop-down list box.
Stop bits	Select the stop bit from the drop-down list box.
Administrator Authorized Access IP Address	Select Any to use any computer to access the web configurator on the VSG. Select Specify and then enter the IP address(es) or a range of IP addresses of the computer(s) that is allowed to log in to configure the VSG.
Multicast Passthrough	Select Enable to allow multicast traffic to pass through the VSG. This may affect your network performance. Select Disable to prevent any multicast traffic from passing through the VSG. This is the default setting.
Allow remote user to ping the device	Select Enable to respond to Ping requests from the LAN or WAN interface. Select Disable to not respond to Ping requests from the LAN or WAN interface.
SSL Certificate	Certificate Secure Socket Layer (SSL) security allows you to create a secure connection between the VSG and the client computer(s). Select Default to use the default system-generated SSL certificate. Select Custom Certificate to use a certificate obtained from a certificate authority. Refer to Chapter 31 on page 206 for more information.
Apply	Click Apply to save the changes.

CHAPTER 6

LAN and WAN Setup

This chapter shows you how to configure the LAN and WAN ports on the VSG.

6.1 Factory Ethernet Defaults

The Ethernet parameters of the VSG are preset to the following values:

- 1** WAN IP address of 192.168.1.1 with subnet mask of 255.255.255.0.
- 2** LAN IP address of 10.59.1.1.
- 3** DHCP server enabled on the LAN with a 252 client IP address pool starting from 10.59.1.2

These parameters should work for the majority of installations. If you wish to change the factory defaults or to learn more about TCP/IP, please read on.

6.2 LANs and WANs

A LAN (Local Area Network) is a computer network limited to the immediate area, usually the same building or floor of a building. A WAN (Wide Area Network), on the other hand, is an outside connection to another network or the Internet.

6.3 IP Address Assignment

A static IP is a fixed IP that you configure on the VSG. A dynamic IP is not fixed; the DHCP server provides an IP address to the VSG each time it connects to the network. When an Ethernet device is configured to obtain a dynamic IP address from a DHCP server, it is known as a DHCP client.

6.3.1 IP Address and Subnet Mask

Like houses on a street that share a common street name, the 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) reserved a block of addresses specifically for private use (refer to [Section 6.3.2 on page 61](#)); please do *not* use any other number unless you are told otherwise. Let's say you select 192.168.1.0 as the network number; which covers 254 individual addresses, from 192.168.1.1 to 192.168.1.254 (zero and 255 are reserved). In other words, the first three numbers specify the network number while the last number identifies an individual computer on that network.

The subnet mask specifies the network number portion of an IP address.

6.3.2 Private IP Addresses

Every machine on the Internet must have a unique address. If your networks are isolated from the Internet, for example, only between your two branch offices, you can assign any IP addresses to the hosts without problems.

However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

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

Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines above.

Note: For more information on address assignment, please refer to RFC 1597, Address Allocation for Private Internets and RFC 1466, Guidelines for Management of IP Address Space.

6.3.3 DNS Server Address

DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa, for example, 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 machine before you can access it. The DNS server addresses that you enter in the DHCP setup are passed to the client machines along with the assigned IP address and subnet mask.

There are two ways that an ISP disseminates the DNS server addresses. The first is for an ISP to tell a customer the DNS server addresses, usually in the form of an information sheet, when s/he signs up. The second is to obtain the DNS server information automatically when a computer is set as a DHCP client.

6.4 LAN Configuration

To configure the LAN settings on the VSG, click **System Settings** and **WAN/LAN** to display the screen as shown.

Figure 20 System Settings: WAN/LAN: LAN Configuration

WAN/LAN	
LAN	The Device IP Address and Subnet mask settings IP Address: 10.59.1.1 Subnet Mask: 255.0.0.0
WAN MAC Address	☒ Default ☐ Change to: 00 : 00 : 00 : 00 : 00 : 00
WAN Port Mode	☒ Get automatically from a DHCP server ☐ Use fixed IP address ☐ PPPoE (Mostly for ADSL modem users) ☐ PPTP (Mostly for Europe ADSL modem users)
Apply	

The following table describes the LAN-related fields in this screen.

Table 5 System Settings: WAN/LAN: LAN Configuration

FIELD	DESCRIPTION
LAN	
IP Address	Enter the LAN IP address of the VSG in dotted decimal notation. The default is 10.59.1.1 .
Subnet Mask	Enter the LAN subnet mask in dotted decimal notation. The default is 255.0.0.0 .

Note: You must restart the VSG if you change the IP address.

If you set the VSG as a DHCP server on the LAN, the VSG will automatically change the LAN DHCP settings based on the new LAN IP address.

6.5 WAN Configuration

To configure the WAN settings on the VSG, click **System Settings** and **WAN/LAN**. The WAN/LAN screen varies depending on the settings in the **WAN Port Mode** field.

6.5.1 WAN MAC Address

Use the **WAN/LAN** screen to configure the MAC address of the WAN port by either setting the VSG to use the factory default or specify the MAC address of a computer on the LAN.

Figure 21 System Settings: WAN/LAN: WAN MAC Address

WAN/LAN	
LAN	The Device IP Address and Subnet mask settings IP Address: 10.59.1.1 Subnet Mask: 255.0.0.0
WAN MAC Address	☒ Default ☐ Change to: 00 : 00 : 00 : 00 : 00 : 00
WAN Port Mode	☒ Get automatically from a DHCP server ☐ Use fixed IP address ☐ PPPoE (Mostly for ADSL modem users) ☐ PPTP (Mostly for Europe ADSL modem users)
Apply	

The following table describes the related field in this screen.

Table 6 System Settings: WAN/LAN: WAN MAC Address

FIELD	DESCRIPTION
WAN MAC Address	Select Default to use the factory assigned MAC address. If your ISP requires MAC address authentication, select Change to and enter the MAC address of a computer on the LAN in the fields provided.

6.5.2 WAN Port Mode: Dynamic/Fixed IP Address

Use the **WAN/LAN** screen to change the WAN IP address settings.

Figure 22 System Settings: WAN/LAN: Dynamic/Static WAN IP Address

WAN/LAN	
LAN	The Device IP Address and Subnet mask settings IP Address: 10.59.1.1 Subnet Mask: 255.0.0.0
WAN MAC Address	☒ Default ☐ Change to: 00 : 00 : 00 : 00 : 00 : 00
WAN Port Mode	☐ Get automatically from a DHCP server ☒ Use fixed IP address You have static IP information from your ISP IP Address: 192.168.1.1 Subnet Mask: 255.255.255.0 Default IP Gateway: 192.168.1.254 Primary DNS Server: 168.95.1.1 Secondary DNS Server:
	☐ PPPoE (Mostly for ADSL modem users) ☐ PPTP (Mostly for Europe ADSL modem users)
Apply	

The following table describes the related labels in this screen.

Table 7 System Settings: WAN/LAN: WAN IP

FIELD	DESCRIPTION
WAN Port Mode	
Get automatically from a DHCP server	Select this option to set the VSG to act as a DHCP client on the WAN. The VSG obtains TCP/IP information (IP address, DNS server information, etc.) from a DHCP server.
Use fixed IP address	Select this option to set the VSG to use a static (or fixed) IP address. This is the default setting.
IP Address	Enter the static IP address in dotted decimal notation. The default WAN IP address is 192.168.1.1 .
Subnet Mask	Enter the subnet mask in dotted decimal notation.
Default IP Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the primary and/or secondary DNS servers.

6.5.3 WAN Port Mode: PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) functions as a dial-up connection. PPPoE is an IETF (Internet Engineering Task Force) draft standard specifying how a host personal computer interacts with a broadband modem (for example DSL, cable, wireless, etc.) to achieve access to high-speed data networks. It preserves the existing Microsoft Dial-Up Networking experience and requires no new learning or procedures.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for instance, RADIUS). For the user, PPPoE provides a login and authentication method that the existing Microsoft Dial-Up Networking software can activate, and therefore requires no new learning or procedures for Windows users.

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

Operationally, PPPoE saves significant effort for both the subscriber and the ISP/carrier, as it requires no specific configuration of the broadband modem at the subscriber's site.

By implementing PPPoE directly on the VSG (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the VSG does that part of the task. Furthermore, with NAT, all of the LAN's computers will have Internet access.

Figure 23 System Settings: WAN/LAN: PPPoE

WAN/LAN															
LAN	The Device IP Address and Subnet mask settings IP Address: 10.59.1.1 Subnet Mask: 255.0.0.0														
WAN MAC Address	☒ Default ☐ Change to: 00 : 00 : 00 : 00 : 00 : 00														
WAN Port Mode	☐ Get automatically from a DHCP server ☐ Use fixed IP address ☒ PPPoE (Mostly for ADSL modem users) Your ISP requires you to input username / password <table border="1"> <tr> <td>Username:</td> <td> </td> </tr> <tr> <td>Password:</td> <td> </td> </tr> <tr> <td>PPP MTU Setting:</td> <td> 1492 (option)</td> </tr> <tr> <td>TCP MSS Setting:</td> <td> 1452 (option)</td> </tr> <tr> <td>Service Name:</td> <td> (option)</td> </tr> <tr> <td>☒ Connect on Demand</td> <td>Max Idle Time: 10 Min.</td> </tr> <tr> <td>☐ Keep alive</td> <td>Redial Period: 30 Sec.</td> </tr> </table> ☐ PPTP (Mostly for Europe ADSL modem users) Apply	Username:		Password:		PPP MTU Setting:	1492 (option)	TCP MSS Setting:	1452 (option)	Service Name:	(option)	☒ Connect on Demand	Max Idle Time: 10 Min.	☐ Keep alive	Redial Period: 30 Sec.
Username:															
Password:															
PPP MTU Setting:	1492 (option)														
TCP MSS Setting:	1452 (option)														
Service Name:	(option)														
☒ Connect on Demand	Max Idle Time: 10 Min.														
☐ Keep alive	Redial Period: 30 Sec.														

The following table describes the related fields in this screen.

Table 8 System Settings: WAN/LAN: PPPoE

FIELD	DESCRIPTION
WAN Port Mode	
PPPoE	Select this option to activate PPPoE support.

Table 8 System Settings: WAN/LAN: PPPoE (continued)

FIELD	DESCRIPTION
Username	Enter the user name exactly as assigned by your ISP. If the name is assigned in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the size of a Maximum Transmission Unit (MTU).
TCP MSS Setting	Enter the size of the Maximum Segment Size (MSS).
Service Name	Enter the name of your PPPoE service.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the Max Idle Time field (maximum 65535 minutes). This is the default setting with an idle timeout of 10 minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the Redial Period field (maximum 65535 seconds). When disconnected, the VSG will attempt to bring up the connection after the redial period.

6.5.4 WAN Port Mode: PPTP

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

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

Figure 24 System Settings: WAN/LAN: PPTP

WAN/LAN																							
LAN	The Device IP Address and Subnet mask settings IP Address: 10.59.1.1 Subnet Mask: 255.0.0.0																						
WAN MAC Address	☒ Default ☐ Change to: 00 : 00 : 00 : 00 : 00 : 00																						
WAN Port Mode	☐ Get automatically from a DHCP server ☐ Use fixed IP address ☐ PPPoE (Mostly for ADSL modem users) ☒ PPTP (Mostly for Europe ADSL modem users) Your ISP requires you to input username / password / PPTP setting <table border="1"> <tr> <td>PPTP Local IP Address:</td> <td> </td> </tr> <tr> <td>PPTP Local Subnet Mask:</td> <td> </td> </tr> <tr> <td>PPTP Local Default Gateway:</td> <td> </td> </tr> <tr> <td>PPTP Server IP Address:</td> <td> </td> </tr> <tr> <td>Username:</td> <td> </td> </tr> <tr> <td>Password:</td> <td> </td> </tr> <tr> <td>PPP MTU Setting:</td> <td> 1460 (option)</td> </tr> <tr> <td>TCP MSS Setting:</td> <td> 1400 (option)</td> </tr> <tr> <td>Connection ID/Name:</td> <td> (option)</td> </tr> <tr> <td>☒ Connect on Demand</td> <td>Max Idle Time: 10 Min.</td> </tr> <tr> <td>☐ Keep alive</td> <td>Redial Period: 30 Sec.</td> </tr> </table>	PPTP Local IP Address:		PPTP Local Subnet Mask:		PPTP Local Default Gateway:		PPTP Server IP Address:		Username:		Password:		PPP MTU Setting:	1460 (option)	TCP MSS Setting:	1400 (option)	Connection ID/Name:	(option)	☒ Connect on Demand	Max Idle Time: 10 Min.	☐ Keep alive	Redial Period: 30 Sec.
PPTP Local IP Address:																							
PPTP Local Subnet Mask:																							
PPTP Local Default Gateway:																							
PPTP Server IP Address:																							
Username:																							
Password:																							
PPP MTU Setting:	1460 (option)																						
TCP MSS Setting:	1400 (option)																						
Connection ID/Name:	(option)																						
☒ Connect on Demand	Max Idle Time: 10 Min.																						
☐ Keep alive	Redial Period: 30 Sec.																						
Apply																							

The following table describes the related fields in this screen.

Table 9 System Settings: WAN/LAN: PPTP

FIELD	DESCRIPTION
WAN Port Mode	
PPTP	Select this option to activate PPTP support. Refer to Section 6.5.4 on page 66 for more information.
PPTP Local IP Address	Enter the IP address assigned to you.
PPTP Local Subnet Mask	Enter the subnet mask assigned to you.
PPTP Local Default Gateway	Enter the IP address of the gateway device.
Username	Enter the user name exactly as your ISP assigned. If assigned a name in the form user@domain where domain identifies a service name, then enter both components exactly as given.
Password	Enter the password associated with the user name above.
PPP MTU Setting	Enter the size of a Maximum Transmission Unit (MTU).

Table 9 System Settings: WAN/LAN: PPTP (continued)

FIELD	DESCRIPTION
TCP MSS Setting	Enter the size of the Maximum Segment Size (MSS).
Connections ID/Name	Enter your identification name of the PPTP server assigned to you by the ISP.
Connect on Demand	Select this option when you don't want the connection up all the time and specify an idle timeout in the Max Idle Time field (maximum 65535 minutes). This is the default setting with an idle timeout of 10 minutes.
Keep Alive	Select this option when you want the Internet connection up all the time and specify a redial period in the Redial Period field (maximum 65535 seconds). When disconnected, the VSG will attempt to bring up the connection after the redial period.

CHAPTER 7

Server

This chapter shows you how to configure the internal web server and set up DHCP settings and email server redirect on the VSG.

7.1 DHCP Configuration

DHCP (Dynamic Host Configuration Protocol) allows the individual clients (Ethernet device) to obtain the TCP/IP configuration from a centralized DHCP server. The VSG has built-in DHCP server capability, which means it can assign IP addresses, an IP default gateway and DNS servers to computer systems that support the DHCP client when this feature is activated. The VSG can also act as a surrogate DHCP server where it relays IP address assignment from the actual DHCP server to the clients.

7.1.1 Public and Private Address Assignment

When you configure the VSG as a DHCP server, you can set the VSG to assign private or public IP addresses to subscriber computer(s) connected to the LAN port.

In most cases, the VSG assigns private IP address to subscriber computer(s) connected on the LAN. When the subscribers access the Internet, NAT is applied. This allows multiple computers to share one Internet connection.

With public IP address assignment through DHCP, the VSG assigns public IP addresses to subscribers connected on the LAN. In this case, the VSG works as a bridge and NAT is NOT applied on the traffic. However, you need to obtain multiple public IP addresses (one for the VSG and one for each computer) from your ISP before you can use this feature.

7.1.2 Server Configuration

Use the **Server Configuration** screen to set the embedded web server, the LAN DHCP server and specify the e-mail server for e-mail redirection on the VSG.

Click **System Settings** and **Server** to display the screen as shown next.

Figure 25 System Settings: Server

Server	
Web Server	Server Port: 80 ☐ SSL Security Administrator Idle-Timeout: 500 Min(s) (1 - 1440)
DHCP Server	☐ Disable ☒ DHCP Relay DHCP Server IP Address
	☒ DHCP Server(Public) IP Pool Starting Address 10.59.1.2
	Pool Size: 253 (Max.=512)
	Lease Time (Private) 1440 (Minutes)
	Lease Time (Temporal) 5 (Minutes)
	Primary DNS Server 168.95.1.1
	Secondary DNS Server
	☐ DHCP Server(Public) If the network ID is different from WAN, this function will be disabled automatically.
	IP Pool Starting Address
	Pool Size: 253 (Max.=512)
Lease Time (Public) 1440 (Minutes)	
Email Server Redirect	IP Address or Domain Name SMTP Port 25 (25, 2500 - 2599)
Apply	

The following table describes the labels in this screen.

Table 10 System Settings: Server

LABEL	DESCRIPTION
Web Server	
Server Port	Specify the port number of the embedded web server on the VSG for accessing the web configurator. The default port number is 80. Enter a number between 8010 and 8060 to access the web configurator behind a NAT-enabled network. If you enter a number between 8010 and 8060, you need to append the port number to the WAN or LAN port IP address to access the web configurator. For example, if you enter "8010" as the web server port number, then you must enter "http://www.192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address.
SSL Security	Security Secure Socket Layer (SSL) security allows you to create a secure connection between the VSG and the client computer(s). Refer to Chapter 31 on page 206 for more information. Select this option to activate SSL security. By default, SSL login security is disabled.

Table 10 System Settings: Server (continued)

LABEL	DESCRIPTION
Administrator Idle-Timeout	Specify how many minutes (between 1 and 1440) the web configuration can be left idle before the session times out. After it times out you have to log in with your username and password again. Very long idle timeouts may have security risks. Note: This does NOT apply to the SMT management session.
DHCP Server	Select the DHCP mode on the LAN.
Disable	Select this option to disable DHCP server on the LAN.
DHCP Relay	Select this option to set the VSG to forward network configuration requests to a DHCP server on the LAN network. Then configure the DHCP Server IP Address field.
DHCP Server IP Address	If you select DHCP Relay , enter the IP address of the real DHCP server.
DHCP Server (Private)	Select this option to set the VSG to assign network information (such as IP address, DNS information etc.) to Ethernet device(s) connected to the LAN port. This is the default setting.
IP Pool Start Address	Enter the first of the continuous addresses in the IP address pool. The default is 10.59.1.2 (based on the default management LAN IP address of 10.59.1.1).
Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 512.
Lease Time (Private)	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
Primary/Secondary DNS IP Address	Enter the IP address of the DNS server(s) in the Primary DNS IP Address and/or Secondary DNS IP Address fields. Note: You must specify a DNS server.
DHCP Server (Public)	Select this option if you want to assign public IP address(es) to the computer(s) connected on the LAN port. The VSG does not apply NAT on traffic using public IP address assigned on the LAN. Note: You must obtain more than one public IP address from your ISP. You need to configure a billing profile with the public service type (see Section 10.1.1 on page 88).
IP Pool Start Address	Enter the first of the continuous addresses in the public client IP address pool. Make sure the IP pool addresses are in the same range as the WAN IP address of the VSG. If they are in different IP ranges, this feature is disabled. If you are given a range of public IP addresses, do not include the VSG's WAN IP address in the address pool.
Pool Size	This field specifies the size or count of the IP address pool. Enter a number not greater than 512.
Lease Time (Public)	Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address.
E-mail Server Redirect	You can set the VSG to redirect and send subscriber's E-mail via a specified e-mail server. This feature allows subscribers to send E-mail via the local E-mail server when their default e-mail server is not working or prevented by relay restrictions.

Table 10 System Settings: Server (continued)

LABEL	DESCRIPTION
IP Address or Domain Name	Specify the IP address or the domain name of the e-mail server to which the VSG forwards e-mail.
SMTP Port	Specify the port number (25 is the default) for SMTP (Simple Mail Transfer Protocol). Enter a number between 2500 and 2599.
Apply	Click Apply to save the settings.

CHAPTER 8

NAT Pool

This chapter shows how to configure Network Address Translation (NAT) on the WAN for VPN packets.

8.1 NAT Overview

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

8.1.1 NAT Definitions

Inside/outside denotes where a host is located relative to the VSG, for example, the computers of your subscribers are the inside hosts, while the web servers on the Internet are the outside hosts.

Global/local denotes the IP address of a host in a packet as the packet traverses a router, for example, the local address refers to the IP address of a host when the packet is in the local network, while the global address refers to the IP address of the host when the same packet is traveling in the WAN side.

Note that inside/outside refers to the location of a host, while global/local refers to the IP address of a host used in a packet. Thus, an inside local address (ILA) is the IP address of an inside host in a packet when the packet is still in the local network, while an inside global address (IGA) is the IP address of the same inside host when the packet is on the WAN side. The following table summarizes this information.

Table 11 NAT Definitions

ITEM	DESCRIPTION
Inside	This refers to the host on the LAN.
Outside	This refers to the host on the WAN.
Local	This refers to the packet address (source or destination) as the packet travels on the LAN.
Global	This refers to the packet address (source or destination) as the packet travels on the WAN.

NAT never changes the IP address (either local or global) of an outside host.

8.1.2 What NAT Does

In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) back to the inside local address before forwarding it to the original inside host. Note that the IP address (either local or global) of an outside host is never changed.

The global IP addresses for the inside hosts can be either static or dynamically assigned by the ISP. In addition, you can designate servers, for example, a web server and a telnet server, on your local network and make them accessible to the outside world. If you do not define any servers, NAT offers the additional benefit of firewall protection. With no servers defined, your VSG filters out all incoming inquiries, thus preventing intruders from probing your network. For more information on IP address translation, refer to RFC 1631, The IP Network Address Translator (NAT).

8.1.3 How NAT Works

Each packet has two addresses – a source address and a destination address. For outgoing packets, the ILA (Inside Local Address) is the source address on the LAN, and the IGA (Inside Global Address) is the source address on the WAN. For incoming packets, the ILA is the destination address on the LAN, and the IGA is the destination address on the WAN. NAT maps private (local) IP addresses to globally unique ones required for communication with hosts on other networks. It replaces the original IP source address in each packet and then forwards it to the Internet. The VSG keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored.

8.1.4 VPN and NAT

A VPN (Virtual Private Network) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing technologies/services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

The VSG allows subscribers to create a VPN tunnel to a remote site.

Note: For IPSec, the VSG does not support AH protocol.

By default, the VSG performs NAT on the LAN; mapping multiple private LAN addresses to a single public address on the WAN. This prevents subscribers from creating multiple VPN connections to a remote VPN device that allows only one VPN connection per source IP address.

In order to allow subscribers to establish multiple VPN connections to a remote VPN device with single-connection-per-source limitation, set the VSG to perform NAT on the WAN. You need to configure NAT address pool for use with VPN connections on the WAN port. The VSG automatically maps one/more private IP addresses to one/more public IP addresses for VPN packets. The following table describes the NAT mapping types on the WAN for VPN packets.

Table 12 WAN NAT Mapping Types for VPN

TYPE	DESCRIPTION
One-to-One	For VPN connections to the same remote VPN device, the VSG maps each private LAN IP address to one public WAN IP address.
One-to-Many	For VPN connections to different remote VPN devices, the VSG maps multiple private LAN IP address to one public WAN IP address.

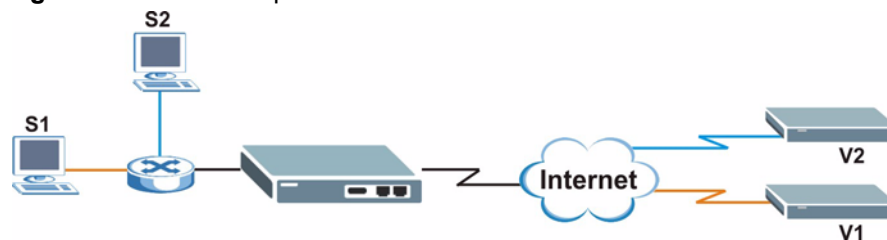
8.2 NAT Examples

The following sections describe some NAT address mapping examples for VPN connections.

8.2.1 Example 1: One-to-One

The figure below shows an example where the two subscribers **S1** and **S2** tries to establish secure VPN connections to the same VPN server **V1** at the same time. For example, the VSG is using a public IP address of 211.21.21.1¹. In this case, the VSG performs One-to-One IP address translation on the WAN.

Figure 26 NAT Example: One-to-One



The following table shows the address mapping.

Table 13 NAT Example: One-to-One

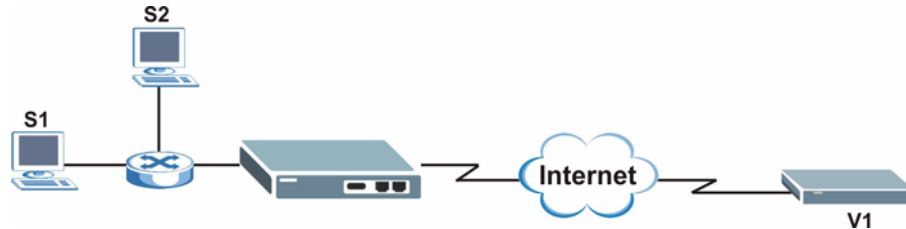
SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	221.21.21.3

1. All public IP address discussed are for examples only.

8.2.2 Example 2: Many-to-One

The figure below shows an example where the two subscribers **S1** and **S2** try to establish a secure VPN connection to VPN servers **V1** and **V2** respectively at the same time. In this case, the VSG performs Many-to-One IP address translation on the WAN since the destination address is different.

Figure 27 NAT Example: Many-to-One



The following table shows the address mapping.

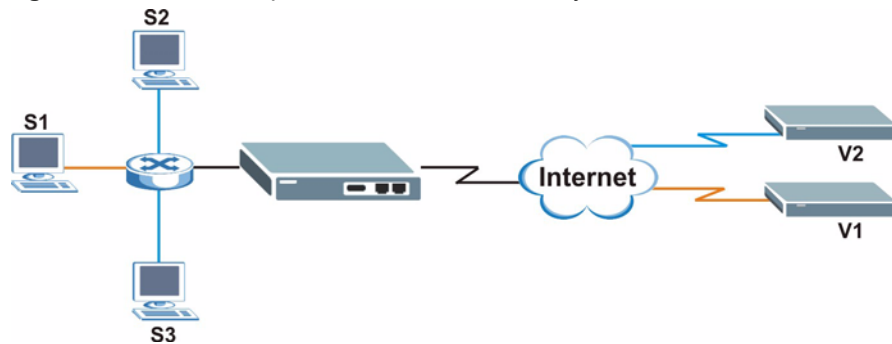
Table 14 NAT Example: Many-to-One

SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	211.21.21.2

8.2.3 Example 3: One-to-One and Many-to-One

The figure below shows an example where subscriber **S1** tries to connect to VPN server **V1** while subscriber **S2** and **S3** try to connect to the same VPN server **V2** at the same time. In this case, subscribers **S1** and **S2** map to the same WAN IP address since the destination is different while subscriber **S3** maps to a different WAN IP address.

Figure 28 NAT Example: One-to-One and Many-to-One



The following table shows the address mapping.

Table 15 NAT Example: One-to-One and Many-to-One

SUBSCRIBER	ORIGINAL SOURCE IP	TRANSLATED SOURCE IP
S1	10.59.1.2	211.21.21.2
S2	10.59.1.3	211.21.21.2
S3	10.59.1.4	211.21.21.3

8.3 NAT Pool Setup

Note: You only need to set the NAT address pool if the remote VPN server(s) allows only one connection per source IP address.

You need to acquire additional public IP address(es) from your ISP to create NAT pool(s).

To set the NAT address pool, click **System Settings** and **NAT Pool** in the navigation panel. A screen displays as shown next.

Figure 29 System Settings: NAT Pool

The following table describes the labels in this screen.

Table 16 System Settings: NAT Pool

LABEL	DESCRIPTION
Disable	Select this option to deactivate this feature. Subscribers are not be able to establish multiple connections simultaneously to the same VPN server (that has the single-connection-per-source limitation).
Enable	Select this option to perform address translation on the WAN to allow subscribers to establish simultaneous connections to the same VPN server (that has the single-connection-per-source limitation). You must then configure the address pool for VPN connections.

Table 16 System Settings: NAT Pool (continued)

LABEL	DESCRIPTION
Start/End IP	Specify the beginning and ending IP addresses of the address pool in the fields provided and click Add to List. The following shows three NAT pool examples if the VSG is using a WAN public IP address of 211.21.21.1: Group 1: 211.21.21.2 ~ 211.21.21.6 (five IP addresses) Group 2: 211.21.21.20 ~ 211.21.21.29 (ten IP addresses) Group 3: 211.21.21.60 ~ 211.21.21.69 (ten IP addresses) Group 4: 211.21.21.75 ~ 211.21.21.76 (two IP addresses) Note: You can configure up to ten address pools (each pool can contain up to 50 addresses) on the VSG.
No.	This read-only field displays the index number.
Address List	This read-only field displays the address pool.
Delete	Click Delete to remove the selected entry(ies).
Apply	Click Apply to save the changes.

CHAPTER 9

Authentication

This chapter shows you how to set up subscriber authentication on the VSG.

9.1 Authentication Overview

You can set the VSG to authenticate subscriber in a number of ways:

- User agreement
- CAS (Central Authentication Service)
- Built-in authentication
- Remote RADIUS server

By default, subscriber authentication is disabled. This allows all subscribers to access the Internet without entering account username and password.

9.1.1 User Agreement

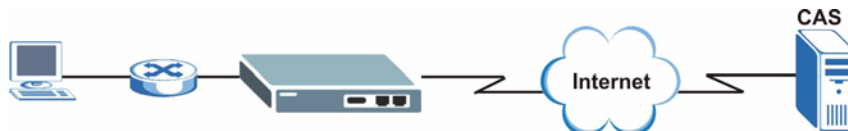
In cases where authentication is not required and anyone can access the Internet through the VSG, you can set the VSG to redirect client users to an Internet service usage agreement page. Users *must* accept the service usage agreement before they can access the Internet.

9.1.2 CAS (Central Authentication Service)

The Hilton Group Corporation developed the High Speed Internet Access (HSIA) service to provide Internet access service across its entire Hilton Group hotels.

In order to use the HSIA, hotel guest(s) must be authenticated through the proprietary CAS (in the local hotel network or the remote network). The CAS performs both user authentication and accounting.

Figure 30 CAS Example



The following summarizes the communication steps before Internet access is allowed.

- 1 A hotel guest launches a web browser.

- 2 The VSG redirects the guest's web browser to a login screen at CAS.
- 3 The guest enters the provided access information.
- 4 Once authentication is successful, CAS informs VSG to allow Internet access to the guest.

9.1.3 Built-in Authentication

The built-in authentication method is useful if you do not have a RADIUS server. You can use the built-in subscriber database to manage the subscribers. With the built-in authentication, the VSG provides three sets of preconfigured scenarios that you can choose for easy and simple setup. For billing, use either a PMS or the built-in billing mechanism to set up accounting information.

9.1.4 RADIUS

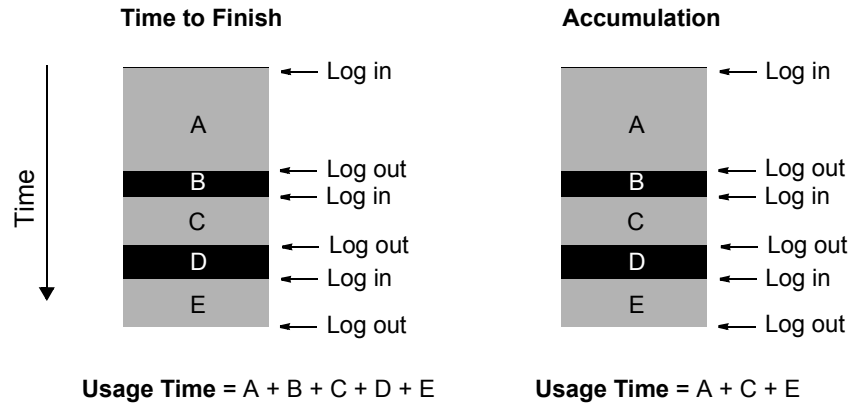
The VSG supports Remote Authentication Dial-In user Service (RADIUS). By integrating RADIUS with the VSG, you can set up the subscriber database on the RADIUS server. In addition to subscriber information, the subscriber database may hold the Internet usage time period each subscriber is allocated. For example, when a subscriber logs in, the RADIUS server will send the time allocation information (such as session time-out) to the VSG, which uses this information to control the subscriber's connection.

9.1.4.1 RADIUS Accounting

The VSG sends "accounting start" and "accounting stop" messages to the RADIUS server, which uses these messages to accurately track subscriber Internet usage.

The VSG provides two accounting methods: **Accumulation** and **Time to Finish**.

- The **Accumulation** accounting method allows multiple re-logins until the allocated time period or until the subscriber account is expired. The VSG accounts for the time the subscriber logs in for Internet access.
- The **Time to Finish** accounting method is good for one-time logins. Once a subscriber logs in, the VSG stores the MAC address of the subscriber's computer for the duration of the time allocated. Thus the subscriber does not have to enter the user name and password again for re-login within the allocated time. Once activated, the subscriber account is valid until the allocated time is reached even if the subscriber disconnects Internet access for a certain period within the allocated time. For example, if Joe purchases a one-hour time-to-finish account. He starts using the Internet for the first 20 minutes and then disconnects Internet access to go to a 15-minute meeting. Then he only has 25 minutes left on his account.

Figure 31 Accounting Usage Time

9.1.4.2 Vendor Specific Attribute

With RADIUS authentication, you can define vendor specific attributes (VSAs) in addition to the set of standard RADIUS attributes defined in RFC 2865 and RFC 2866. A VSA is an attribute-value pair that is sent between a RADIUS server and the VSG. It is necessary you define the VSAs on the RADIUS sever if you want the VSG to perform the following:

- Limit Download bandwidth per subscriber
- Limit Upload bandwidth per subscriber
- Limit Total traffic bandwidth allowed per subscriber
- Specify advertising web site per subscriber
- Enable/disable SMTP redirect

Note: Before you can make use of these functions on the VSG, configure the proprietary VSAs on the RADIUS server. Refer to the documentation that comes with your RADIUS server for more information.

See [Appendix D on page 242](#) for more information on the VSAs.

9.2 Authentication Configuration

To configure the subscriber authentication method, click **System Settings** and **Authentication** to display the screen as shown next.

Figure 32 System Settings: Authentication

Authentication Configuration																																		
Authentication Type	☒ No Authentication ☐ User Agreement ☐ Redirect URL Link Code ☒ Standard User Agreement page ☐ Built-in Authentication Three pre-configured options are provided for easy setup. Select an option that best suits your network needs. You must then proceed to configure the "Billing" and "Accounting" settings to complete your setup. Current preset option: Scenario C Select option ☐ RADIUS ☐ Check Local Account first ☒ Accumulation ☐ Time to Finish (No idle timeout) <table border="1"> <tr> <td rowspan="4">Primary RADIUS Server</td> <td>Server IP address</td> <td> </td> </tr> <tr> <td>Authentication Port</td> <td> 0 </td> </tr> <tr> <td>Accounting Port</td> <td> 0 </td> </tr> <tr> <td>Shared Secret</td> <td> </td> </tr> <tr> <td rowspan="4">Secondary RADIUS Server</td> <td>Server IP address</td> <td> </td> </tr> <tr> <td>Authentication Port</td> <td> 0 </td> </tr> <tr> <td>Accounting Port</td> <td> 0 </td> </tr> <tr> <td>Shared Secret</td> <td> </td> </tr> <tr> <td colspan="2">Retry Attempts when Primary failed</td> <td> 5 </td> </tr> <tr> <td colspan="2">Retry Frequency</td> <td> 3 seconds (3 ~ 75)</td> </tr> <tr> <td>Accounting Service</td> <td colspan="2"> ☒ Disable ☐ Enable Update every: 0 Min(s) </td> </tr> <tr> <td>Authentication Method</td> <td colspan="2"> CHAP </td> </tr> <tr> <td>Vendor Specific Attribute</td> <td colspan="2"> Vendor Code 0 ☐ Send VSA together with Authentication Request </td> </tr> </table>	Primary RADIUS Server	Server IP address		Authentication Port	0	Accounting Port	0	Shared Secret		Secondary RADIUS Server	Server IP address		Authentication Port	0	Accounting Port	0	Shared Secret		Retry Attempts when Primary failed		5	Retry Frequency		3 seconds (3 ~ 75)	Accounting Service	☒ Disable ☐ Enable Update every: 0 Min(s)		Authentication Method	CHAP		Vendor Specific Attribute	Vendor Code 0 ☐ Send VSA together with Authentication Request	
Primary RADIUS Server	Server IP address																																	
	Authentication Port		0																															
	Accounting Port		0																															
	Shared Secret																																	
Secondary RADIUS Server	Server IP address																																	
	Authentication Port	0																																
	Accounting Port	0																																
	Shared Secret																																	
Retry Attempts when Primary failed		5																																
Retry Frequency		3 seconds (3 ~ 75)																																
Accounting Service	☒ Disable ☐ Enable Update every: 0 Min(s)																																	
Authentication Method	CHAP																																	
Vendor Specific Attribute	Vendor Code 0 ☐ Send VSA together with Authentication Request																																	
Idle Time Out	5 Min(s) (1 - 1440)																																	
SSL Login Security	☒ Disable ☐ Enable																																	
Smart Client Support	☐ WISPr Smart Client <table border="1"> <tr> <td rowspan="3">Login Mode</td> <td>☒ Directly Reply</td> </tr> <tr> <td>☐ Proxy Reply with "Redirect Login Page" URL</td> </tr> <tr> <td>☐ Proxy Reply with Specific URL </td> </tr> </table>	Login Mode	☒ Directly Reply	☐ Proxy Reply with "Redirect Login Page" URL	☐ Proxy Reply with Specific URL 																													
Login Mode	☒ Directly Reply																																	
	☐ Proxy Reply with "Redirect Login Page" URL																																	
	☐ Proxy Reply with Specific URL 																																	
Apply																																		

The following table describes the labels in this screen.

Table 17 System Settings: Authentication

LABEL	DESCRIPTION
No Authentication	Select this option to disable subscriber authentication. Subscribers can access the Internet without entering user names and passwords. This is the default setting.
User Agreement	Select User Agreement to direct a subscriber to an Internet service usage agreement page before accessing the Internet.
Redirect Page URL Link	Specify the URL of the user agreement page in the field provided. Click Code to display the HTML source code of a default sample page.
Standard User Agreement Page	Select this option to use the pre-configured user agreement page on the VSG.
Built-in Authentication	Select this option to authenticate the subscribers using the local subscriber database. Then click Select option to choose a per-configured setting in the Current Preset option field. Note: When you select this option, you must also configure the Billing and Accounting screens.
Current preset option	This field is available when you select Built-in Authentication . This field displays the current pre-configured setting for the built-in authentication. To select a predefined option, click Select option to open the Scenario Guide screen (refer to Figure 33 on page 86).
RADIUS	Select this option to authenticate subscribers using a remote RADIUS server. Then configure the following fields.
Check Local Account First	Select this option to have the VSG authenticate a subscriber using the local user database first. If the account information is not found, then the VSG authenticates subscribers using the RADIUS server(s) specified. Clear this check box to have the VSG authenticate subscribers using the RADIUS server(s) only.
Accumulation	Select this option for multiple re-login until the time allocated is used up. If a subscriber logs out and accesses the Internet again within the time period specified in the Idle Timeout field, the subscriber does not have to enter the user name and password again to log in.
Time to Finish	Select this option to allow each subscriber a one-time login. If a subscriber logs out before the allocated time expires, the subscriber does not have to enter the user name and password to access the Internet again.
Primary/Secondary RADIUS Server	Server IP Address Enter the IP address of a RADIUS server in dotted decimal notation.
Authentication Port	Specify the authentication port of the RADIUS server. The common port numbers are 1645 and 1812.
Accounting Port	Specify the accounting port of the RADIUS server. The common port numbers are 1646 and 1813.
Secret Key	Specify a password (up to 31 alphanumeric characters) as the key to be shared between the RADIUS server and the VSG. The key is not sent over the network. Note: This key must be the same on the RADIUS server and the VSG.
Retry Attempts when Primary fail	Specify the number of times (1 to 3) the VSG resends an authentication request to the primary and/or secondary RADIUS servers.

Table 17 System Settings: Authentication (continued)

LABEL	DESCRIPTION
Accounting Service	Select Enable from the drop-down list box to activate the accounting feature and enter the time (in minutes) between updates in the Update every field. Select Disable to de-activate the accounting feature.
Authentication Method	Select either the CHAP or PAP authentication method from the drop-down list box.
Vendor Specific Attribute	In the Vendor Code field, specify a number for the vendor ID. This is an IANA (Internet Assigned Numbers Authority) assigned number that identifies the vendor or enterprise. Enter 890 for ZyXEL devices. Select Send VSA together with Authentication Request to set the VSG to include the VSA information in the authentication requests.
Idle-Timeout	The VSG automatically disconnects a computer from the network after a period of inactivity. The subscriber may need to enter the username and password again before access to the network is allowed. Specify the idle timeout between 1 and 1440 minutes. The default is 5 minutes.
SSL Login Page Security	Select Enable to activate SSL security upon accessing the login screen so that user names and passwords are encrypted before being transmitted to the VSG. Select Disable to de-activate SSL security for the subscriber login screen. Refer to Chapter 31 on page 206 for more information.
Smart Client Support	WISPr (WiFi Internet Service Provider Roaming) allows roaming subscribers to access different service provider networks for seamless network connection.
WISPr Smart Client	Select this option to allow the VSG to accept incoming roaming subscribers. Clear this check box to disable this feature. Your access network is not available for roaming subscribers.
Login Mode	Specify a login method for roaming subscribers. Select Replay Directly to display the VSG's default login screen. Select Proxy Reply with "Redirect Login Page" URL to redirect roaming subscribers to the same login screen as specified in the Login Page screen (see Section 15.2 on page 120 for more information). Select Proxy Reply with "Redirect Login Page" URL and enter the URL of the login page for roaming subscribers only.
Apply	Click Apply to save the changes.

9.2.1 Scenario Options

Note: This feature is for built-in authentication method only.

When you select **Built-in Authentication** in the **Authentication** screen, you must select a pre-configured scenario option by clicking the **Select option** link to display a screen as shown next.

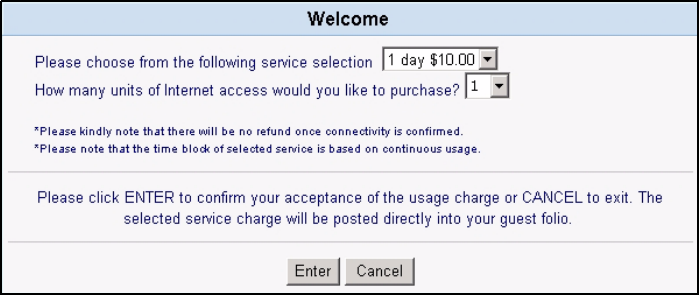
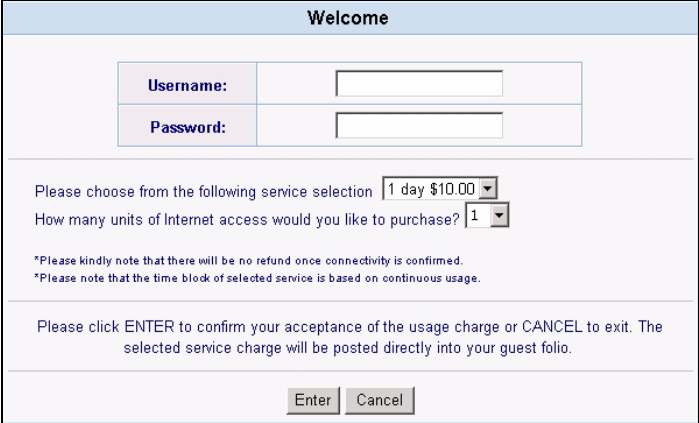
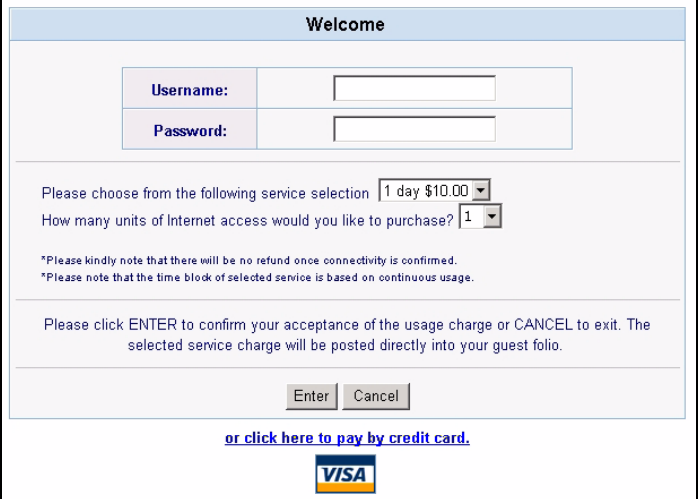
Select a scenario option in the **Items Check** field and click **Apply** to save the settings. Then proceed to configure the billing and accounting settings.

Figure 33 System: Authentication: Scenario Guide

Scenario Guide			
Express way to fit your business model			
Items check	☐ Scenario A	☐ Scenario B	☒ Scenario C
PMS billing system	Yes ☐ Output bill to AG Number of copies 1	Yes	No
Infrastructure	Port-Location Mapping	General	General
Need username/password when guests go to Internet	No	Yes	Yes
Need to create static accounts	Option	Yes	Option
Allow guests to select service when first login	Yes	Yes	No
Billing mode	Time to Finish	Time to Finish	☒ Time to Finish ☐ Accumulation Idle Timeout 5 Min (s).(1 - 1440) Accumulation account will be deleted after logged in 7 days
Billing Charge mode	☒ Based on Room ☐ Based on Subscriber	-	-
Default Billing Profile	Need to continue configuring "Billing" and choose at lease one active billing profile	Need to continue configuring "Billing" and choose at lease one active billing profile	☐ Allow Credit Card Payment
Remarks	Need to continue configuring "Port-Location Mapping Table"		

The following table describes each scenario.

Table 18 System: Authentication: Scenario Guide

OPTION	DESCRIPTION	SAMPLE SUBSCRIBER LOGIN SCREEN
Scenario A	Select this option to use PMS billing with port-location mapping. Once you configure the port-location mappings, subscribers are able to access the Internet without entering usernames and passwords. Subscribers can purchase additional time blocks with different billing plans. You can still create static or dynamic accounts. However, subscribers using the dynamic or static accounts are prompted for usernames and passwords.	Figure 34 Subscriber Login: Scenario A 
Scenario B	Select this option if you want to use PMS billing without port-location mapping. You must then create the subscriber accounts. Subscribers are prompted for their usernames and passwords before Internet access is allowed. Subscribers can purchase additional time blocks with different billing plans.	Figure 35 Subscriber Login: Scenario B 
Scenario C	Select this option to use the VSG's built-in or credit card billing function. No PMS device is needed.	Figure 36 Subscriber Login: Scenario C 

CHAPTER 10

Billing

This chapter shows you how to set up subscriber billing profiles and PMS (Property Management System) configuration.

10.1 Billing Overview

A billing profile contains information such as time unit, unit cost and/or account expiration time. You must associate a subscriber account with a billing profile.

In addition, for PMS billing, subscribers may have a choice of purchasing additional time blocks with different billing profiles you set and activate on the VSG.

10.1.1 Billing Profile

You can create up to ten billing profiles on the VSG. Click **System Setting** , **Billing** and the **Billing Profile** link to display the screen as shown next.

Figure 37 System Setting: Billing: Billing Profile

Billing Profile				
Currency: \$ (Number of decimals places: 2)				
No	Active	Name	Description	Profile Setting
01	☒	Profile 1	1 day \$10.00	Edit
02	☐			Edit
03	☐			Edit
04	☐			Edit
05	☐			Edit
06	☐			Edit
07	☐			Edit
08	☐			Edit
09	☐			Edit
10	☐			Edit
				Apply

The following table describes the labels in this screen.

Table 19 System Setting: Billing: Billing Profile

LABEL	DESCRIPTION
Currency	Specify the type of currency and/or dollar sign for billing.
Number of decimal places	Specify the number of decimal places for the currency. The default is 2 .
No	This field displays the index number of a billing profile.
Active	Select this check box to enable the billing profile.
Name	This field displays the name of a billing profile.
Description	This field displays a description of a billing profile.
Profile Setting	Click Edit to edit the selected billing profile. Refer to Section 10.1.2 on page 89 for more information.
Apply	Click Apply to save the changes.

10.1.2 Configuring a Billing Profile

To edit a billing profile, click the **Edit** button in the **Billing Profile** screen to display the configuration screen for the selected billing profile.

Figure 38 System Settings: Billing: Billing Profile Setting

Billing Profile Setting				
No	1			
Name	Profile 1			
Description	1 day \$10.00			
Price	Duration	Charge	Check Time	Selective Unit
	☐ 1 minute	0	Period Time finish	From: 1 To: 10
	☐ 1 hour	0	Period Time finish	From: 1 To: 10
	☒ 1 day	10.00	☒ Period Time finish	From: 1 To: 10
			☐ Expire when 00:00	
	☐ 1 week	0	☒ Period Time finish	From: 1 To: 10
			☐ Expire when Sun. 00:00	
☐ 1 month	0	☒ Period Time finish	From: 1 To: 10	
		☐ Expire when 01 00:00		
	0			

The screenshot shows a web form for configuring a billing profile. At the top, there are fields for 'Duration' (set to 1 month), 'Period Time Finish' (To: 10), and 'Expire when' (01 00:00). Below these is an 'Unlimited' checkbox and a field for '0'. The 'Bandwidth Limit' section contains a red note: 'Note: You must activate the bandwidth management feature and select a class of service'. It has two rows for 'Maximum Upstream Bandwidth' and 'Maximum Downstream Bandwidth', each with a radio button for a predefined value (64 Kbps and 256 Kbps respectively) and a text input for a custom value (0 Kbps). The 'Service Type' section has radio buttons for 'Private Service' and 'Public Service'. At the bottom are 'Reset' and 'Apply' buttons.

The following table describes the labels in this screen.

Table 20 System Settings: Billing: Billing Profile Setting

LABEL	DESCRIPTION
No	This read-only field displays the index number of the billing profile.
Name	Enter a descriptive name for the billing profile for identification purposes.
Description	Enter a description for this billing profile
Price	
Duration	Select a time period (minute, hour, day, week, month or Unlimited) and enter the time unit in the field provided (not available for Unlimited).
Charge	Specify the unit cost in this field.
Check Time	Select Period Time Finish for time-to-finish billing method. Refer to Section 9.1.4 on page 81 for more information. Select Expired when and specify the time from the drop-down list box(es) for the accumulate billing method. The subscriber accounts will be invalid once the allocated time period is used up. This option is only available when you select the Day, Week or Month option in the Period Time field.
Selective Unit	Specify the range of time units (between 1 and 99) a subscriber is allowed to purchase at any one time. The range is presented as a drop-down list box in the information pop-up window.
Bandwidth Limit	Note: You must activate bandwidth management to use this feature. Refer to Chapter 16 on page 144 . Set the fields below to configure the bandwidth limit for this billing profile.
Uplink Bandwidth Limitation	To use a pre-defined option, select the first option and choose a bandwidth from the drop-down list box. To manually set the bandwidth, select the second option and specify the bandwidth in the field provided.
Downlink Bandwidth Limitation	To use a pre-defined option, select the first option and choose a bandwidth from the drop-down list box. To manually set the bandwidth, select the second option and specify the bandwidth in the field provided.

Table 20 System Settings: Billing: Billing Profile Setting (continued)

LABEL	DESCRIPTION
Service Type	Select Private Service to set the VSG to assign private IP addresses to the subscribers connected on the LAN. Select Public Service to set the VSG to assign public IP addresses to the subscribers connected on the LAN. You must have more than one public IP address from your ISP. Configure private and public DHCP IP address assignment in the Server screen. Refer to Section 7.1.1 on page 70 for more information.
Reset	Click Reset to restart configuring this screen again.
Apply	Click Apply to save the changes.

10.2 PMS (Property Management System)

Many hotels use a PMS device to perform in-room billing for services (such as room services, mini-bar, pay-per-view TV or telephone) that the guests use.

With PMS, the VSG allows subscribers to purchase additional time units online. In addition, subscribers can select from a number of different billing plans.

To use PMS for billing, first connect the VSG to a PMS device using the **PMS** port (refer to [Chapter 2 on page 38](#)), then configure the PMS settings on the VSG.

10.2.1 Port-Location Mapping

When you activate port-location mapping and PMS on the VSG, two charge modes are available: per room and per subscriber.

Select **Based on Room** when location is important. If a subscriber disconnects from one location and reconnects in another location, the VSG prompts for the user name and password again.

Select **Based on Subscriber** to allow a subscriber to freely move between different locations without prompting for user name and password.

10.2.2 PMS Configuration

Click **System Setting**, **Billing** and click the **PMS Configuration** link to display the screen as shown next.

Figure 39 System Setting: Billing: PMS Configuration

PMS Configuration	
Many hotels use PMS as a hotel in-door billing system for their guests including room service, mini-bar, telephone usage; as well as Internet service. By integrating with a hotel's PMS, the system can post charges for Internet access directly to a guest's hotel bill.	
Charge Mode (only for Port-Location Mapping enabled)	☒ Based on Room ☐ Based on Subscriber
Regenerate password of static account with PMS checkout	Enable (only for Scenario B)
PMS Type	☒ Micros Fidelio ☐ Spectrum MK II Revenue Code 1 (1-99) Description Internet ☐ Marriott Revenue Code 1 (1-99) Reference Internet ☐ Proprietary
Speed of PMS interface	Bits per second 9600 Data bits 8 Parity None Stop bits 1
Apply	

The following table describes the labels in this screen.

Table 21 System Setting: Billing: PMS Configuration

LABEL	DESCRIPTION
Charge Mode (only for Port-Location Mapping enabled)	When you set up Port-Location Mapping, your VSG offers two billing modes: Based on Room and Based on Subscriber. Select Based on Room when location is important. If a subscriber disconnects from one location and reconnects in another location, the VSG prompts for the user name and password again. Select Based on Subscriber to allow a subscriber to freely move between different locations without prompting for user name and password. Note: You must activate the port-location mapping feature. Refer to Chapter 13 on page 112.
Regenerate password of static account with PMS checkout.	This feature is applicable when you select Scenario B with Built-in Authentication in the Authentication screen (see Figure 32 on page 83). Select Enable to automatically generate a new password for the static account when a subscriber checks out. Select Disable to keep the password for the static account unchanged after a subscriber checks out.
PMS Type	Select a PMS system and specify the fields below (if available). Currently the VSG supports Micros Fidelio , Spectrum MK II , Marriott and Proprietary .
Micros Fidelio	
Revenue Code	Enter a revenue code (between 01 and 99).
Description	Enter the description for the revenue. Refer to the user's guide that comes with your PMS device.

Table 21 System Setting: Billing: PMS Configuration (continued)

LABEL	DESCRIPTION
Spectrum MK II	
Revenue Code	Enter a revenue code (between 01 and 99).
Description	Enter a description to identify the service. For example, Internet.
Marriott	
Revenue Code	Enter a revenue code (between 01 and 99).
Reference	Enter a description to identify the service. For example, Internet.
Proprietary	Select this option if you are using a proprietary PMS system.
Speed of PMS Interface	Set the fields below to configure the PMS port settings on the VSG. Note: Make sure the port settings are the same on the VSG and the connected PMS device.
Bits per second	Select the speed of the PMS port connection. The default is 9600 .
Data bits	Specify the data bits.
Parity	Specify the parity.
Stop bits	Specify the data stop bits.
Apply	Click Apply to save the changes.

10.3 Types of Subscriber Accounts

After you have set up the subscriber authentication methods and billing profile(s), you need to create subscriber accounts. There are two types of subscriber accounts: static and dynamic.

- For static accounts, refer to [Chapter 11 on page 94](#).
- For dynamic accounts, refer to [Chapter 12 on page 104](#).

CHAPTER 11

Static Subscriber Accounts

This chapter shows you how to set up and manage static subscriber accounts.

11.1 Static Subscriber Account Overview

Static accounts are useful in locations such as hotels where you can match an account user name to a fixed location for easy management. Once a static subscriber account is created, it stays permanently in the VSG unless deleted manually. You can generate static accounts automatically or manually.

The following figure shows the links for accessing the static account configuration screens when you click **System Settings**, **Accounting** and **Static Accounts**.

Figure 40 Static Account: Links

Static Account	Dynamic Account		
Static Account Setting	Create Static Account	Static Account Operator	Static Account List

11.2 Global Static Account Settings

To configure global static account settings, click the **Static Account Setting** link to display the screen as shown.

Figure 41 Static Account Settings: Global Settings

Static Account Setting	
Static Account Setting	
Concurrent Access	☒ Allow concurrent access with one account Max. concurrent access: 2
Customize Printout	Customize printout text
Print to...	☒ Statement Printer  ☐ PC-Connected Printer 
Apply	

The following table describes the labels in this screen.

Table 22 Static Account Settings: Global Settings

LABEL	DESCRIPTION
Concurrent Access	Select Allow concurrent access with one account to allow more than one users to access the Internet using the same account at the same time. Then specify the number of concurrent users from the Max. concurrent access drop-down list box. The default number of concurrent access is 2 users per account.
Customize Printout	Click Customize printout text to set the account printout page. Refer to “Account Printout” on page 129 .
Print To	Select Statement Printer if you want to print the account information using a statement printer connected to the CONSOLE port on the VSG. Select PC-Connected Printer if you want to print the account information using a printer connected to a network computer. Click on the  icon to display a print preview.
Apply	Click Apply to save the settings.

11.3 Creating a Static Account

Click **System Settings, Accounts, Static Accounts** and **Create Static Account** to display the screen as shown next.

Figure 42 System Settings: Create Static Subscriber Account

Create Static Account

Static Accounts can be created and managed by a series of specific number like hotel rooms. Static accounts reside in the flash memory all the time.

Generate a batch of static accounts

This feature can automatically generate a series of specific numbers of accounts like hotel rooms.

Prefix:

Postfix:

From: (Maximum 5 numbers)

To: (Maximum 5 numbers)

Billing Profile: Random Password Length:

Note: For PMS billing type, use only numbers for subscriber accounts.

Apply

Static Accounts backup and restore

This feature can backup the account information to your computer or restore a previously saved account information file to your system.

Backup

Click to save the account information to your computer.

Restore

To restore a previously saved account information file to your system, select this option, locate the account information file and click Apply.

File Path:

Apply

Manually Add Subscriber Account			
No.	Username:	Password:	Billing Profile
1			Profile 1 ▾
2			Profile 1 ▾
3			Profile 1 ▾
4			Profile 1 ▾
5			Profile 1 ▾
6			Profile 1 ▾
7			Profile 1 ▾
8			Profile 1 ▾
9			Profile 1 ▾
10			Profile 1 ▾

There are two ways to create static subscriber accounts as described in the following sections.

11.3.1 Generating Static Accounts Automatically

To generate a list of static subscriber accounts automatically, set the fields in **Generate a batch of static accounts** in the **Create Static Subscriber Account** screen.

Figure 43 Create Static Subscriber Account: Generate Automatically

Generate a batch of static accounts	
This feature can automatically generate a series of specific numbers of accounts like hotel rooms.	
Prefix:	From: (Maximum 5 numbers)
Postfix:	To: (Maximum 5 numbers)
Billing Profile: Profile 1 ▾ Random Password Length: 8 ▾	
Note: For PMS billing type, use only numbers for subscriber accounts.	
Apply	

The following table describes the related labels in this screen.

Table 23 Create Static Subscriber Account: Generate Automatically

LABEL	DESCRIPTION
Generate a batch of static accounts	
Prefix	Specify the starting characters affixed to the beginning of all account user names.
Postfix	Specify the characters to append o the end of all account user names.
From	Enter the first number of the range of static accounts.

Table 23 Create Static Subscriber Account: Generate Automatically (continued)

LABEL	DESCRIPTION
To	Enter the ending number of the range of static accounts.
Billing Profile	Select a predefined billing profile from the drop-down list box. Note: This drop-down list box displays active profiles only. Refer to Section 10.1.1 on page 88 for more information.
Random Password Length	The VSG automatically generates a password for each automatically created static account. Specify the length of the password from the drop-down list box.
Apply	Click Apply to start generating the static accounts based on the above criterion.

After you have generated the list of static accounts in this screen click **Static Account List** to display the list of static accounts. Refer to [Section 11.6 on page 102](#).

11.3.2 Creating Static Subscriber Accounts Manually

To create static accounts manually, display the **Create Static Subscriber Account** screen and scroll down to the **Manually Add Static Subscriber Accounts** section as shown next. You can manually create up to 10 static accounts at a time.

Figure 44 Create Static Subscriber Account: Manual

Manually Add Subscriber Account			
No.	Username:	Password:	Billing Profile
1			Profile 1 ▾
2			Profile 1 ▾
3			Profile 1 ▾
4			Profile 1 ▾
5			Profile 1 ▾
6			Profile 1 ▾
7			Profile 1 ▾
8			Profile 1 ▾
9			Profile 1 ▾
10			Profile 1 ▾
			

The following table describes the related labels in this screen.

Table 24 Create Static Subscriber Account: Manual

LABEL	DESCRIPTION
No	This read-only field displays the index number of an entry.
Username	Enter the user name for a static subscriber account.

Table 24 Create Static Subscriber Account: Manual (continued)

LABEL	DESCRIPTION
Password	Enter the password associated with the user name above. You may also set the VSG to generate a password automatically (refer to Section 11.5 on page 100).
Billing Profile	From the drop-down list box, select a billing profile for the static account. Note: This drop-down list box displays active profiles only. Refer to Section 10.1.1 on page 88 for more information.
Apply	Click Apply to create the static account(s) and save the changes.

11.4 Static Account List Backup and Restore

You can back up and restore static account information in the **Create Static Account** screen.

11.4.1 Backing Up a Static Account List

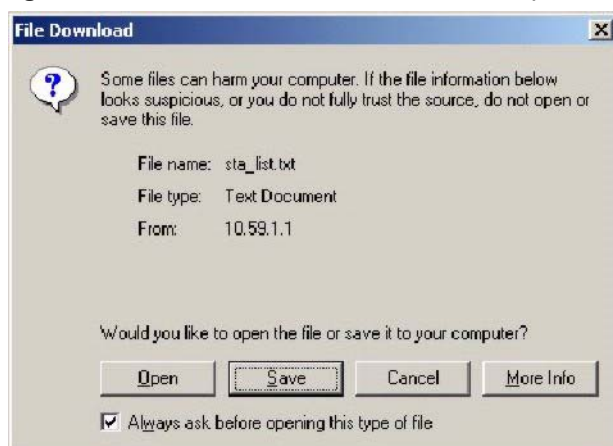
Follow the steps below to back up static subscriber account information to your computer.

- 1 In the **Create Static Subscriber Account** screen and scroll down to the **Static Accounts backup and restore** section.
- 2 Click **Backup**.

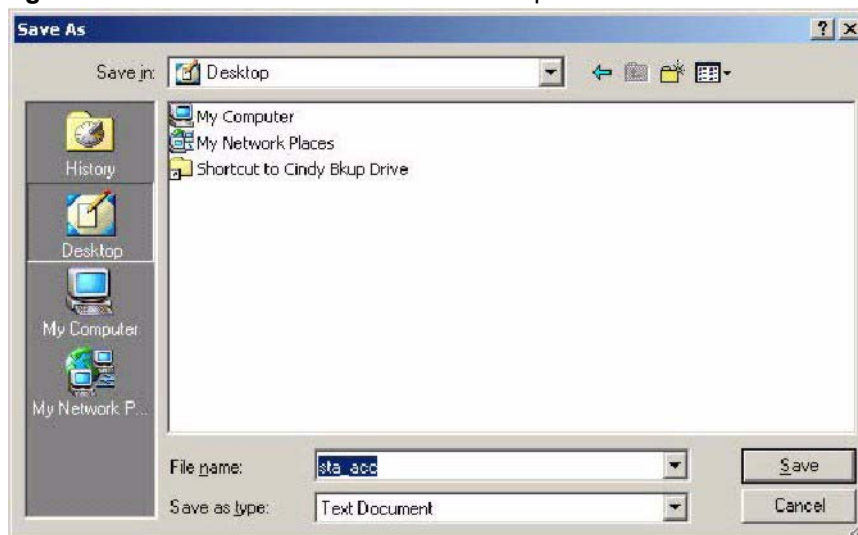
Figure 45 Static Subscriber Account: Backup and Restore

Static Accounts backup and restore	
Backup	Click to save the account information to your computer.
Restore	To restore a previously saved account information file to your system, select this option, locate the account information file and click Apply.
	File Path: Browse...
Apply	

- 3 A **File Download** window displays. Click **Save**.

Figure 46 Static Subscriber Account: Backup and Restore: File Download

- 4 A **Save As** window displays. Specify the filename and/or location and click **Save** to save the backup file.

Figure 47 Static Subscriber Account: Backup and Restore: Save As

You can view the backed up file using any text-editing program.

11.4.2 Restoring a Static Account List

You may restore the static account list if you accidentally reset the VSG back to the factory defaults and erased the subscriber account information.

Follow the steps below to restore a previously backed up subscriber account list.

- 1 In the **Create Static Subscriber Account** screen and scroll down to the **Static Accounts backup and restore** section.

Figure 48 Static Subscriber Account: Backup and Restore

Static Accounts backup and restore	
Backup	Click to save the account information to your computer.
Restore	To restore a previously saved account information file to your system, select this option, locate the account information file and click Apply.
	File Path: Browse...
Apply	

- Specify the location and/or file name of the account information file in the **File Path** field or click **Browse** to locate it.
- Click **Apply** to start the file transfer process. The VSG automatically restarts after the file transfer is complete.

11.5 Editing Subscriber Accounts

To edit a subscriber account, click **System Settings**, **Accounting** and the **Static Account Operator** link to display the screen as shown next.

Figure 49 Static Account Operator

Static Account Operator						
refresh		Print List				
No.	Username	Show Password	Re-Generate Password	ALL	Status	Concurrent Access
1	Admin		Re-Generate Password		Offline	0
2	Cindy		Re-Generate Password		Online	1
GO 1 Page First Previous Next End						

The following table describes the labels in this screen.

Table 25 Static Account Operator

LABEL	DESCRIPTION
Refresh	Click this button to update the screen.
Print List	Click this button to print a list of all subscriber accounts.
No	This read-only field displays the index number of an entry.
Username	This read-only field displays the account user name. Click the heading to sort the entries in ascending or descending order.
Hide Password/ Show Password	Click Hide Password to not display the passwords for the accounts on the screen. Click Show Password to display the passwords for the accounts on the screen.
Re-Generate Password	You may set the VSG to generate a new password for each account. Click All to set the VSG to generate new passwords for all accounts. Click Re-Generate Password to set the VSG to generate a new password for the corresponding account.
Status	This field indicates whether the account is currently in use (Online) or not (Offline).

Table 25 Static Account Operator (continued)

LABEL	DESCRIPTION
Concurrent Access	This field displays how many computers are logged in using this account.
Print	Click the  icon to print the account information of the selected account.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.
Apply	Click Apply to save the changes.

11.5.1 Static Account Information Print Preview

To display a printout preview of static account information, click the **Print** icon to display a printout preview window showing the account information. An example is shown in the following figure.

Refer to [Section 15.4 on page 129](#) to configure the printout page.

Figure 50 Static Account Information Printout Example

Welcome!

This is your account information, please keep this for your Internet Service.

Username: Cindy
 Password: h9fcpc4s
 Usage Time: 1 day
 Billing: Time to Finish
 Profile: 1 day \$10.00
 Purchase Unit: 1
 Total: \$ 10.00

Thank you very much !

-----CUT-----CUT-----CUT-----

Username: Cindy
 Password: h9fcpc4s
 Billing: Time to Finish
 Profile: 1 day \$10.00
 Purchase Unit: 1
 Total: \$ 10.00

Signature:

2006/6/15 17:45:26

Close
Print

11.6 Viewing the Static Account List

To display the static account list, click **Static Account List**.

Figure 51 Static Account List

Static Account								
refresh		Backup Print List						
No.	Username	Password		Billing Profile	Concurrent Access	First Login	Expiration	Status
1	Admin	12345678		None	0			Offline
2	Cindy	12345678	1	Profile 1	1	2006/06/21 09:31:08	2006/06/22 09:31:08	Online
								Delete Delete All
GO 1 Page First Previous Next End								

The following table describes the labels in this screen.

Table 26 Static Account List

LABEL	DESCRIPTION
Refresh	Click Refresh to update this screen.
Backup	Click Backup to backup the account information to a computer.
Print List	Click Print List to print ALL account information on a printer connected to the computer you use to access the web configurator. Note: This does NOT display a print preview window.
No	This field displays the index number.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Password	This field displays the account password.
Billing Profile	This field displays the name of the profile associated to the account.
Concurrent Access	This field displays the number of users are currently using this account for Internet access.
First Login	This field displays the time a subscriber logs in using the account.
Expiration	This field displays the time the account becomes invalid.
Status	This field indicates whether the account is currently is use (Online) or not (Offline).
Delete	Click Delete All to remove all accounts. Click Delete to remove the selected account(s).
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.

CHAPTER 12

Dynamic Subscriber Accounts

This chapter shows you how to set up and manage dynamic subscriber accounts.

12.1 Dynamic Subscriber Account Overview

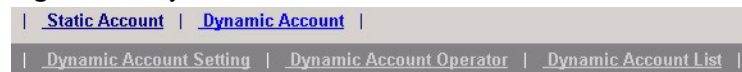
Unlike a static account, a dynamic account is not permanent. Once the time allocated to a dynamic account is used up or a dynamic account remains un-used after the expiration time, the account is deleted from the account list automatically.

Dynamic accounts are automatically generated either by pressing a button on an external statement printer connected to the **CONSOLE** port or using the web configurator (the **Dynamic Account Operator Panel** screen).

Note: You cannot manually add a dynamic account.

The following figure displays the links for accessing the dynamic account configuration screens when you click **System Settings**, **Accounting** and **Dynamic Account**.

Figure 52 Dynamic Account: Links



12.2 Dynamic Account General Settings

There are two ways you can create dynamic accounts on the VSG:

- using a statement printer connected to the VSG.
- using the web configurator.

Before you create dynamic accounts, you must specify the billing profile(s), the number of printout copies and the number of hours before the VSG automatically deletes an inactive account. Refer to the related sections for more information.

For creating dynamic accounts using a statement printer, make sure you connect the statement printer (sold separately) to the **CONSOLE** port on the VSG. Then, in the **Dynamic Account Setting** screen, select the profile setting for each button on the statement printer (refer to the user's guide that comes with the statement printer).

For web-based dynamic account generation, you can specify up to four billing profiles (one for each of the four buttons you click to generate the accounts automatically on the web-based screen).

Click **System Settings, Accounting**, and click the **Dynamic Account Setting** link to display the screen as shown next.

Figure 53 Accounting: Dynamic Account Setting

Dynamic Account Setting			
Dynamic Accounts can be created automatically when you click the button from the Web-based Account Operator or the Statement Printer.			
Web-based Statement Panel Settings			
No.	SP Button	Button name (Max. 12 characters)	Billing Profile
Button 1	SP-100 /200 Button A	Button 1	Profile 1
Button 2	SP-200 Button B	Button 2	Profile 1
Button 3	SP-200 Button C	Button 3	Profile 1
Button 4	-	Button 4	Profile 1
General Settings			
Flexible Digit	8 digits of Dynamic Account Username & Password (4-8)		
General Settings			
Unused Accounts	Automatically delete after 12 hours		
Concurrent Access	☒ Allow concurrent access with one account Max. concurrent access: 2		
Printout copy	Number of copies to print: 1 Customize printout text		
Print to...	☒ Statement Printer ☐ PC-Connected Printer		
Apply			

The following table describes the labels in this screen.

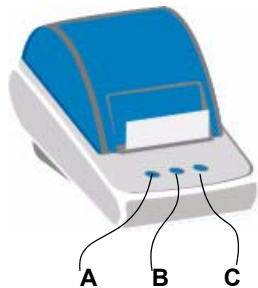
Table 27 Accounting: Dynamic Account Setting

LABEL	DESCRIPTION
Web-based Statement Panel Settings	
No.	This read-only field displays the button index number (Button 1 .. 4). The button numbers correspond to the buttons displayed in the Dynamic Account Operator Panel screen. Refer to Section 12.3.1 on page 106 for more information.
SP Button	This read-only field displays the button label on the statement printer. Refer to Figure 54 on page 106 . Refer to Section 12.3.2 on page 107 for more information on generating dynamic accounts using a statement printer.
Button name	Specify the name of the web-based button (up to 12 characters) in the field provided. The buttons are displayed in the Dynamic Account Operator Panel screen (see Figure 55 on page 107).

Table 27 Accounting: Dynamic Account Setting (continued)

LABEL	DESCRIPTION
Billing Profile	Select a billing profile to associate to the web-based SP buttons from the drop-down list box. Only the activated billing profiles are displayed. Refer to Section 10.1.1 on page 88 for more information on creating billing profiles.
General Settings	
Flexible Digit	Specify how many characters/digits the VSG uses for the generated account username and password.
Unused Accounts	Specify the number of hours to wait before the VSG deletes an inactive dynamic account.
Printout copy	Select the number of copies (1 to 3) to print from the drop-down list box. Click Customize printout text to configure the printout page.
Print to ...	Select Statement Printer if you want to print the account information using a statement printer connected to the CONSOLE port on the VSG. Select PC-Connected Printer if you want to print the account information using a printer connected to a network computer. Click the  icon to display a print preview. Refer to Section 15.4 on page 129 for more information.
Apply	Click Apply to save the changes.

The following figure shows the button labels on the SP-200.

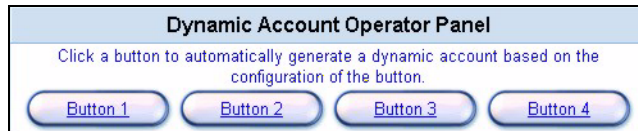
Figure 54 SP-200 Button Labels

12.3 Creating Dynamic Accounts

You can only create dynamic accounts automatically. You can create dynamic accounts using either the web configurator screen or the statement printer.

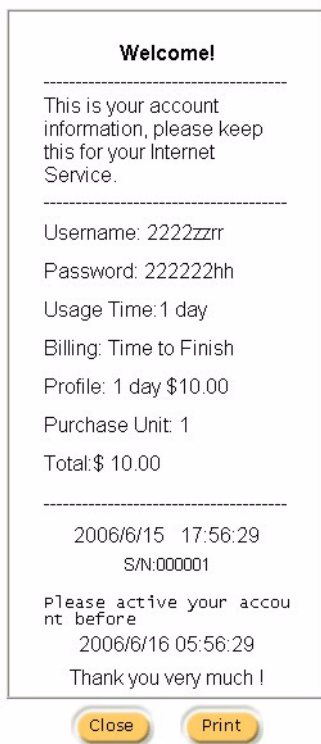
12.3.1 Dynamic Account Generation Using the Web Configurator

Display the **Dynamic Account Operator Panel** screen as shown next.

Figure 55 Dynamic Account Operator Panel

Click a button to generate a dynamic account based on the settings you configure for the button in the **Dynamic Account Setting** screen. A window displays showing a printout preview of the dynamic account generated.

The following figure shows an example. Refer to [Section 15.4 on page 129](#) on account printout to configure the printout page.

Figure 56 Dynamic Account Information Printout Example

12.3.2 Dynamic Account Generation Using a Statement Printer

Follow the steps below to create dynamic accounts and print the account information using a statement printer.

Note: You have to purchase a statement printer separately.

- 1 Connect the statement printer to the port labeled **CONSOLE**. Refer to [Section 2.2 on page 39](#) for more information.
- 2 Configure the **Console Type** field in the **System** screen. Refer to [Section 5.1 on page 56](#).
- 3 Turn on the statement printer and make sure there is printing paper.

- 4 Press the button on the statement printer. A dynamic account is generated and the account information should be printed. Refer to [Figure 79 on page 133](#) for a printout example.

Note: The settings of the buttons on the statement printer correspond to the three SP-200 buttons you set in the **Dynamic Account Operator Panel** screen. Refer to [Section 12.2 on page 104](#).

12.4 Viewing the Dynamic Account List

To display the dynamic account list, click **Dynamic Account List**. Click a heading to sort the entries in ascending or descending order based on the column if applicable.

Figure 57 Dynamic Account List

Dynamic Account List

refresh↺

BackupPrint List

S/N	Username	Password		Billing Profile	Time Created	First Login	Expiration	Status	Delete
2	222222tt	222222tt	1	Profile 1	2006/06/21 09:43:07		2006/06/21 21:43:07	Not In Use	☐
1	2222zzrr	222222hh	1	Profile 1	2006/06/21 09:42:29	2006/06/21 09:44:55	2006/06/22 09:44:55	In Use	☐

DeleteDelete All

GO

1

Page

FirstPreviousNextEnd

The following table describes the labels in this screen.

Table 28 Dynamic Account List

LABEL	DESCRIPTION
Refresh	Click Refresh to update this screen.
Backup	Click Backup to backup the account information to a computer. Refer to Section 12.4.1 on page 109 .
Print List	Click Print List to print all account information to the local printer connected to the computer that you use to configure the VSG. Note: This does NOT display a printout preview window.
S/N	This field displays the serial number (or the Index number) of a dynamic account.
Username	This field displays the account user name. Click the heading to sort the entries in ascending or descending order based on this column.
Password	This field displays the account password.
Billing Profile	This field displays the index number and the name of a billing profile the account is using.
Time Created	This field displays the time the account is created.
First Login	This field displays the time a subscriber logs in using the account.
Expiration	When an account is currently in use, this field displays the time before which a subscriber can still use the account to access the Internet. When an account is never used, this field displays the time the account becomes invalid.

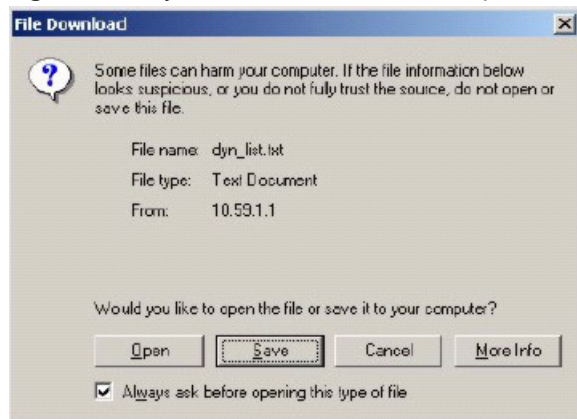
Table 28 Dynamic Account List (continued)

LABEL	DESCRIPTION
Status	This field displays In Use when the account is currently in use. Otherwise it displays Not In Use .
Delete	Click Delete All to remove all accounts. Click Delete to remove the selected account.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.

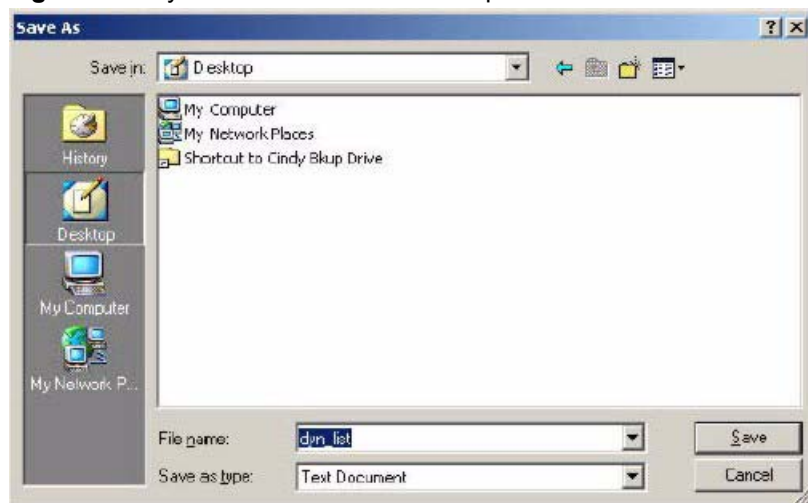
12.4.1 Backing Up the Dynamic Account List

Follow the steps below to backup the dynamic account list to your computer.

- 1 Display the **Dynamic Account Setting** screen (refer to [Figure 53 on page 105](#)).
- 2 Click **Dynamic Account List** (refer to [Figure 57 on page 108](#)).
- 3 Click the **Backup** link.
- 4 A **File Download** window displays. Click **Save**.

Figure 58 Dynamic Account List Backup: File Download

- 5 A **Save As** window displays. Specify the filename and/or location and click **Save**.

Figure 59 Dynamic Account List Backup: Save As

You can view the backed up file using any text-editing program.

CHAPTER 13

Port-Location Mapping

This chapter describes the port-location mapping feature.

13.1 Port-Location Mapping Overview

With port-location mapping, you can map a port on the VSG or a VLAN-enabled switch to a room number in a building (such as a hotel). This is done using IEEE802.1q VLAN tags. The port-location mapping feature is used together with the PMS billing function so charges can be done automatically.

13.2 Configuring Port-Location Mappings

Note: Make sure you select **Built-in Authentication** and **Scenario A** in the **Authentication** screen (see [Figure 32 on page 83](#)) and configure the **PMS Configuration** screen (see [Figure 39 on page 92](#)).

Click **System Settings** in the navigation panel and the **Port-Location Mapping** link to display the screen as shown.

Figure 60 System Setting: Port-Location Mapping

Port-Location Mapping				
Single Create				
Location Identifier (ID)		Port Identifier (ID)		
Description				
Status: ☐ No Charge ☒ Charge for use ☐ Blocked				Add to List
Batch Create				
Location ID From:		Port ID From:		Batch Numbers:
Status: ☐ No Charge ☒ Charge for use ☐ Blocked				Add to List
Note: Use only numbers for the Location Identifier field and Port Identifier field.				
Backup/Restore				
Backup	Backup to Local PC			
	Remote TFTP Server IP Address:		File Name:	Apply
Restore	Local PC File Path		Browse...	Apply
	Remote TFTP Server IP Address:		File Name:	Apply
Port-Location Mapping List				
Location ID	Port ID	Description	Status	Delete
				Delete Delete All
1 Page				

The following table describes the labels in this screen.

Table 29 System Setting: Port-Location Mapping

LABEL	DESCRIPTION
Single Create	Set the related fields to create a port-location mapping one at a time.
Location Identifier (ID)	Enter an identity (up to 20 characters) for a mapping. This field must match the VLAN ID of a port.
Port Identifier (ID)	Enter the an ID number (between 1 and 999999) of a port for this mapping. This is the location ID number you set in the PMS.
Description	Enter a description (up to 32 characters) for this mapping for identification purposes.
Status	Select No Charge if you don't want to bill a subscriber accessing the Internet at this port location. Select Charge for use to bill a subscriber accessing the Internet at this port location. Select Blocked to stop any subscriber from accessing the Internet at this port location.
Add to List	Click Add to List to insert a new mapping rule.

Table 29 System Setting: Port-Location Mapping (continued)

LABEL	DESCRIPTION
Batch Create	Set the related fields to create a specified number of port-location mappings.
Location ID From	Enter an identity (up to 20 characters) of the first location for a mapping. This field must match the VLAN ID of a port.
Port ID From	Enter the an ID number (between 1 and 999999) of the starting port for this mapping. This is the location ID number you set in the PMS.
Batch Numbers	Specify the number of port-location mappings you want to create at a time.
Status	Select No Charge if you don't want to bill a subscriber accessing the Internet at this port location. Select Charge for use to bill a subscriber accessing the Internet at this port location. Select Blocked to stop any subscriber from accessing the Internet at this port location.
Add to List	Click Add to List to insert a new mapping rule.
Backup/ Restore	You can back up or restore the port-location mappings.
Backup	Click Backup to Local PC to save the current port-location mappings to a computer. To back up the current port-location mapping to a TFTP server, specify the IP address of the TFTP server and the file name in the fields provided and click Apply .
Restore	Make sure you have previously backed up the port-location mapping. Note: All current port-location mappings will be lost. To restore from a local computer, specify the name and location of the backup file or click Browse .. to locate it and click Apply . To restore from a TFTP server, specify the IP address of the TFTP server and the file name in the fields provided and click Apply .
Port-Location Mapping List	This table displays a summary of each mapping rule. If applicable, click on a heading to sort the entry.
Location ID	This field displays the ID of a mapping rule.
Port ID	This field displays the port ID.
Description	This field displays a description.
Status	This field displays the status (No Charge , Charge for use or Blocked) of a mapping.
Delete	Click Delete All to remove all accounts. Click Delete to remove the selected account.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.

CHAPTER 14

Credit Card

This chapter shows you how to configure secure online credit card service on the VSG.

14.1 Credit Card Overview

Your VSG is integrated with various online secure credit card billing services that allow you to process credit card transactions via the Internet.

Note: You must register with a credit card billing service provider before you can configure the VSG to handle credit card transactions.

14.1.1 How Credit Card Billing Works

The following summarizes the process of a customer paying for a subscriber account with a credit card.

- 1 A customer accesses the subscriber login screen and selects a credit card payment option.
- 2 The customer selects a service type and enters the contact and billing information.
- 3 Customer billing information is processed real-time via the secure online clearing house.
- 4 After the transaction is successful, the VSG provides the username and password information so the customer can log in for Internet access.

14.1.2 Configuration Steps

Do the following to provide online credit card billing service.

- 1 Obtain a payment account from Authorize.net, iValidate or WorldPay.
- 2 In the **Authentication** screen, select **Built-in Authentication**.
- 3 Click **Select option** to display the **Scenario Guide** screen. Select **Scenario C** and select the **Allow Credit Card Payment** option.
- 4 Enter your payment account information in the **Credit Card** screen.
- 5 Configure the subscriber credit card information screen (see [Section 15.6 on page 135](#) for more information).

14.2 Credit Card Billing Service Configuration

After you have registered a payment account with an online credit card billing service provider, set the payment account information in the **Credit Card** screen. If you are not using one of the credit card billing services supported on the VSG, then you cannot use credit card for billing.

Click **Advanced Setting, Credit Card** to displays the screen as shown below. Enter your payment account in this screen.

Figure 61 Advanced Setting: Credit Card

Credit Card	
☒ Authorize.net	
Version	3.1
Merchant ID	
Merchant Password	☐ Need Password:
Merchant Transaction Key	
Payment Gateway	https://secure.authorize.net/gateway/transact.dll
☐ Email Additional Information	☐ Merchant Name: (max. 40 characters) ☐ Username and Password ☐ Usage Time
☐ i Validate	
Merchant ID	
Terminal ID	
Secure Server Address	https://silverado.trivalley.com/merchant/processcc.asp
☐ World Pay	
Payment Gateway	https://selectworldpay.com/wcc/purchase
Installation ID	
Currency Code	(max. 3 characters)
Description	(max. 100 characters)
☐ Test Mode	Success
Credit Card icons to be displayed on the login page ☒  ☐  ☐  ☐ 	
Apply	

The following table describes the labels in this screen.

Table 30 Advanced Setting: Credit Card

LABEL	DESCRIPTION
Authorize.net	Select this option if you have a payment account from Authorize.net.
Version	This is the (read-only) software version of the Authorize.Net payment gateway.
Merchant ID	Enter the ID number that you received from Authorize.Net.

Table 30 Advanced Setting: Credit Card (continued)

LABEL	DESCRIPTION
Merchant Password	Select Need if a password is required for the Authroize.net account. Then enter the password exactly as you received it from Authorize.Net in the Password field.
Merchant Transaction Key	Then enter the transaction key exactly as you received it from Authorize.Net. The transaction key is similar to a password. The Authorize.Net gateway uses the transaction key to authenticate transactions.
Payment Gateway	Enter the address of the Authorize.Net gateway. The default value is "https://cardpresent.authorize.net/gateway/transact.dll". Note: You don't need to change this address unless instructed by Authorize.net administrator.
Email Additional Information	Select this check box to have the VSG e-mail the subscriber the information that you specify in the following fields.
Merchant Name	Select this check box to have the VSG include the company name in the e-mail that it sends to the subscriber. Enter the company name (up to 40 characters) in the field provided.
Username and Password	Select this check box to have the VSG e-mail the subscriber the subscriber user name and password.
Usage Time	Select this check box to have the VSG e-mail the subscriber the amount of usage time purchased.
i Validate	Select this option if you have a payment account from iValidate.
Merchant ID	Enter the merchant ID number that you received from iValidate.
Terminal ID	Enter the terminal ID number that you received from iValidate.
Secure Server Address	Enter the address of the iValidate gateway. The default value is "https://silverado.trivalley.com/merchant/processcc.asp". Note: You don't need to change this address unless instructed by iValidate administrator.
World Pay	Select this option if you have a payment account from WorldPay.
Payment Gateway	Enter the address of the WorldPay gateway. The default value is "https://select.worldpay.com/wcc/purchase". Note: You don't need to change this address unless instructed by WorldPay administrator.
Installation ID	Enter the payment account ID. Enter the unique reference number assigned by WorldPay. This is the number the VSG send to WorldPay in the payment process. You may get two WorldPay IDs, one for testing and one for payment processing.
Currency Code	Enter the code for the currency charged. For example, "USD".
Description	Enter a descriptive note about the purchase. For example, "Internet Access".
Test Mode	WorldPay provides you with a test account that allows you to test the credit card processing on your site. The test account works the same as the real account except that no funds are actually transferred. For more information, refer to the document on the WorldPay web site. Select Test Mode to use the account for testing purposes. Select Success to always simulate a successful credit card transaction. Select Fail to always simulate a failed credit card transaction.

Table 30 Advanced Setting: Credit Card (continued)

LABEL	DESCRIPTION
Credit card icons to be displayed on the login page	Select the check box(es) of the credit card icon(s) that you want the VSG to display on the subscriber login screen (refer to Figure 36 on page 87 for an example).
Apply	Click Apply to save the changes.

CHAPTER 15

Customization

This chapter shows you how to customize the subscriber login information, user agreement and credit card screens and account or bill printouts.

15.1 Customization Overview

Use the Customization screens to configure the subscriber login screen, the account information screen, credit card option screen, account printouts and bill printouts.

15.2 Login Screen

When subscriber authentication is activated in the **Authentication Configuration** screen, the subscriber login screen is the first screen that all subscribers see when trying to access the Internet. You can configure walled garden web addresses for web sites which all subscribers are allowed to access without logging in (refer to [Section 17.4 on page 149](#)).

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

To customize the subscriber login screen, click **Advanced Settings** and **Customization** to display the screen as shown next.

Figure 62 Customization: Login

Login Page															
☒ Standard	<table border="1"> <tr> <td>Title</td> <td> Welcome (Max. 80 characters)</td> </tr> <tr> <td>☐ Footnote</td> <td> Please contact us if you have any ques (Max. 240 characters)</td> </tr> <tr> <td>☒ Copyright</td> <td> Copyright (c) 2001, 2002 All Rights Res (Max. 80 characters)</td> </tr> <tr> <td>Background Color</td> <td> FFFFFF View Color Grid</td> </tr> </table>  Standard Login Page Preview	Title	Welcome (Max. 80 characters)	☐ Footnote	Please contact us if you have any ques (Max. 240 characters)	☒ Copyright	Copyright (c) 2001, 2002 All Rights Res (Max. 80 characters)	Background Color	FFFFFF View Color Grid						
Title	Welcome (Max. 80 characters)														
☐ Footnote	Please contact us if you have any ques (Max. 240 characters)														
☒ Copyright	Copyright (c) 2001, 2002 All Rights Res (Max. 80 characters)														
Background Color	FFFFFF View Color Grid														
☐ Redirect	Redirect Login Page URL: Code														
☐ Advanced	<table border="1"> <tr> <td>Welcome Slogan</td> <td> Welcome </td> </tr> <tr> <td>Page Background</td> <td> ☒ None ☐ Background Color FFFFFF View Color Grid </td> </tr> <tr> <td>Article</td> <td> </td> </tr> <tr> <td>Article Text Color</td> <td> 000000 View Color Grid</td> </tr> <tr> <td>Article Background Color</td> <td> ☒ None ☐ FFFFFF View Color Grid </td> </tr> <tr> <td>Information</td> <td> </td> </tr> <tr> <td>Comments</td> <td> </td> </tr> </table>	Welcome Slogan	Welcome	Page Background	☒ None ☐ Background Color FFFFFF View Color Grid	Article		Article Text Color	000000 View Color Grid	Article Background Color	☒ None ☐ FFFFFF View Color Grid	Information		Comments	
Welcome Slogan	Welcome														
Page Background	☒ None ☐ Background Color FFFFFF View Color Grid														
Article															
Article Text Color	000000 View Color Grid														
Article Background Color	☒ None ☐ FFFFFF View Color Grid														
Information															
Comments															
☐ Frame	<table border="1"> <tr> <td>Top Frame</td> <td>URL: </td> </tr> <tr> <td>Bottom Frame</td> <td>This frame will show the standard login page</td> </tr> </table>	Top Frame	URL:	Bottom Frame	This frame will show the standard login page										
Top Frame	URL:														
Bottom Frame	This frame will show the standard login page														
Service Selection customization															
Service Selection Message	Please choose from the following service se (Max. 80 characters)														
Purchase Unit Message	How many units of Internet access would you (Max. 80 characters)														
Notification Message 1	*Please kindly note that there will be no refut (Max. 160 characters)														
Notification Message 2	*Please note that the time block of selected (Max. 160 characters)														
Notification Message 3	(Max. 160 characters)														
Additional Remark	Please click ENTER to confirm your accepti (Max. 240 characters)														
Apply															

15.2.1 Standard Login Screen

The standard subscriber login screen is the VSG's pre-configured, default simple login screen. You can modify the screen color and title and add copyright information and a footnote.

In the **Login Screen Configuration** screen, select **Standard**.

Figure 63 Customization: Login: Standard

Standard

Title	Welcome (Max. 80 characters)
☐ Footnote	Please contact us if you have any ques (Max. 240 characters)
☒ Copyright	Copyright (c) 2001, 2002 All Rights Res (Max. 80 characters)
Background Color	FFFFFF View Color Grid

[Standard Login Page Preview](#)

The following table describes the related labels in this screen.

Table 31 Customization: Login: Standard

LABEL	DESCRIPTION
Standard	Select this option to use the standard subscriber login screen.
Title	Enter the login page title (up to 80 characters) in the field provided.
Footnote	Select this check box and enter up to 240 characters in the field provided to add the footnote to the login screen.
Copyright	Select this check box and enter the copyright information (up to 80 characters) in the field provided to add copyright information to the login screen.
Background Color	Specify the color of the registration text. For example, enter '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values. The default is black ("000000").
Standard Login Page Preview	Save the settings and click this link to preview the standard login screen in a new browser window.

The following figure shows an example.

Figure 64 Subscriber Login Screen Example: Standard

Welcome

Username:	
Password:	

Enter Cancel

Note: For credit card settings, refer to [Chapter 14 on page 116](#).

15.2.2 Redirect Login Screen

You can set the VSG to redirect the subscribers a to another login screen.

In the **Login Screen Configuration** screen, select **Redirect**.

Figure 65 Customization: Login Screen: Redirect

☒ **Redirect**

Redirect Login Page URL:	Code
--------------------------	---

The following table describes the related fields.

Table 32 Customization: Login Screen: Redirect

FIELD	DESCRIPTION
Redirect	Select this option to redirect the subscriber to another login screen.
Redirect Login Page URL	Specify the web site address to which the VSG directs the subscribers for logins.
Code	Click Code to display the source code of the web page you specify above.

15.2.3 Advanced Login Screen

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

Figure 66 Customization: Login Screen: Advanced

The following table describes the related fields.

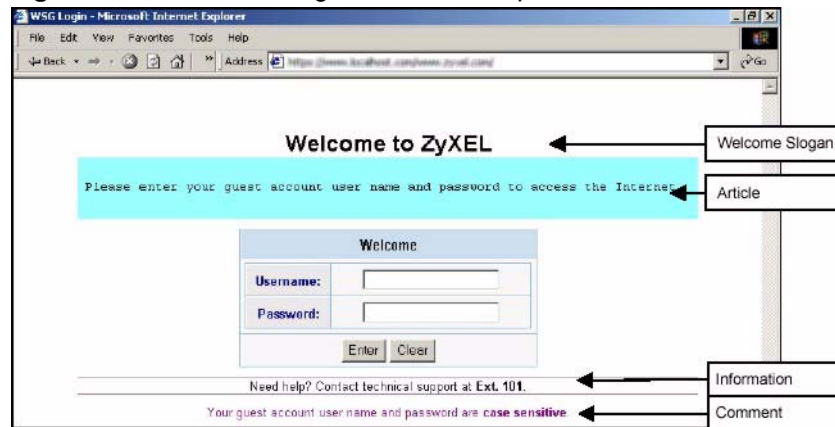
Table 33 Customization: Login Screen: Advanced

LABEL	DESCRIPTION
Advanced	Select this option to set the VSG to display the advanced subscriber login screen.
Welcome Slogan	Enter a welcome message (up to 80 characters long) in the text box provided.
Page Background	Select None to set the background color of the login screen to white ("FFFFFF" the default). Select Background Color to set the color of the login screen background to the color specified, for example, enter '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 1024 characters long) in the text box. This is useful for advertisements or announcements.
Article Text Color	Select None to set the article text color of the login screen to white (the default). Select and set the color of the article text block background to the color specified, for example, enter '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.

Table 33 Customization: Login Screen: Advanced (continued)

LABEL	DESCRIPTION
Article Background Color	Select None to set the background color of the article text block to white ("FFFFFF" the default). Select Background Color to set the background color of the article text block to the color specified, for example, enter '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Information	Enter information such address and telephone or fax numbers in the text box provided. Up to 80 characters allowed.
Comments	Enter any comments (up to 80 characters long) in the text box provided.

The following figure shows an example.

Figure 67 Subscriber Login Screen Example: Advanced

15.2.4 Framed Login Screen

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

Figure 68 Customization: Login Screen: Frame

☐ Frame	Top Frame	URL:
	Bottom Frame	This frame will show the standard login page

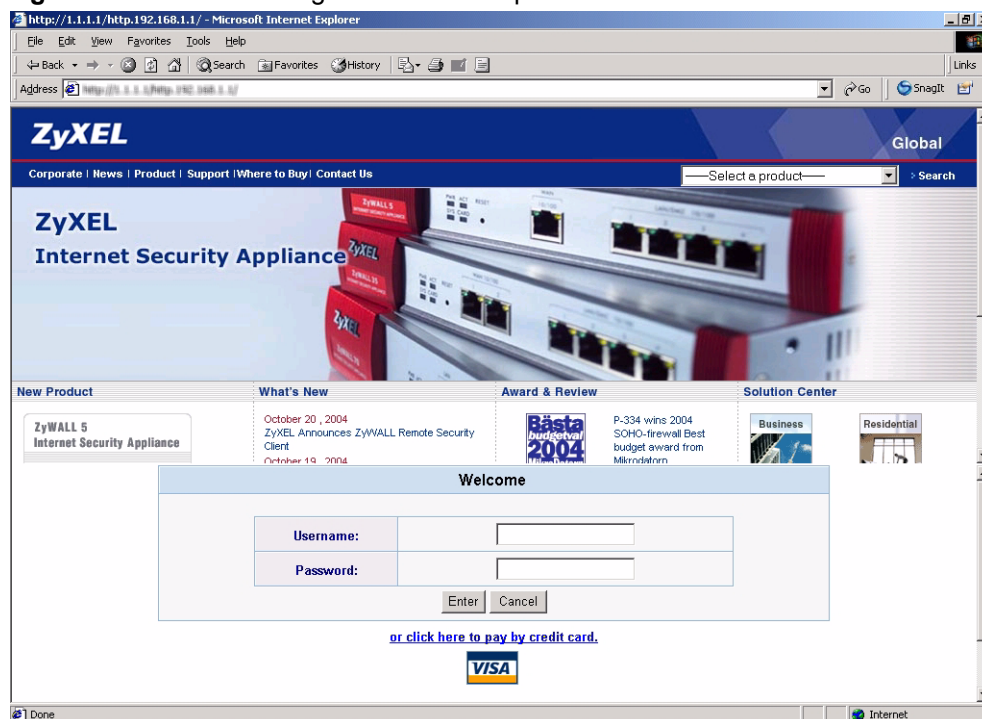
The following table describes the related fields.

Table 34 Customization: Login Screen: Frame

LABEL	DESCRIPTION
Frame	Select this option to configure and set the VSG to display the subscriber login screen in two frames.
Top Frame	Enter a web site address in the URL field, for example, http://www.zyxel.com .
Bottom Frame	The bottom frame of the subscriber login screen displays the default login prompt. You cannot configure this part of the screen.

The following figure shows a framed subscriber login screen example.

Figure 69 Subscriber Login Screen Example: Frame



15.2.5 Login Service Selection

The service selection messages are available in the subscriber login screen *only* when you configure the VSG to use PMS billing.

Figure 70 Customization: Service Selection Customization

Service Selection customization	
Service Selection Message	Please choose from the following service se (Max. 80 characters)
Purchase Unit Message	How many units of Internet access would you (Max. 80 characters)
Notification Message 1	*Please kindly note that there will be no refur (Max. 160 characters)
Notification Message 2	*Please note that the time block of selected (Max. 160 characters)
Notification Message 3	(Max. 160 characters)
Additional Remark	Please click ENTER to confirm your accepti (Max. 240 characters)

The following table describes the related labels.

Table 35 Customization: Service Selection Customization

LABEL	DESCRIPTION
Service Selection Customization	
Service Selection Messages	Enter a message to instruct the subscribers to select a billing profile.
Purchase Unit Message	Enter a message to instruct the subscribers to select the number of time units to purchase.
Notification Message 1 .. 3	Enter additional message(s) regarding the replenish feature. For example, you may enter a refund policy.
Additional Remark	Enter any additional information. For example, enter contact information for help.

The following figure shows an example of a standard subscriber login screen with the service selection messages.

Figure 71 Subscriber Login Screen Example: Service Selection Messages

Welcome

Username:	
Password:	

Please choose from the following service selection 1 day \$10.00

How many units of Internet access would you like to purchase? 1

*Please kindly note that there will be no refund once connectivity is confirmed.

*Please note that the time block of selected service is based on continuous usage.

Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.

15.3 Information Window

You can set the VSG to display an information window after a subscriber has successfully logged in. This information window shows the amount of time a subscriber has used or the time the subscriber still has to access the Internet. The subscriber information window varies depending on the billing and accounting configuration you set on the VSG.

The information window displays the amount of time used for Internet access when you select **Built-in Authentication** in the **Authentication Configuration** screen or when you select **RADIUS Server** and the RADIUS server is configured not to send session timeout messages.

The information window displays the amount of time a subscriber still has to use for Internet access when you select **RADIUS Server** in the **Authentication Configuration** screen and the RADIUS server is configured to send session timeout messages.

Click **Advanced Settings, Customization** and click the **Information Window** link to display a screen as shown next.

Figure 72 Customization: Information Window

Information Window	
Information window is a pop-up window that is presented to subscribers with their browser once after subscriber login successfully. The subscriber can type http://1.1.1.1/info to open this window again.	
☒ Display Information Window once after a subscriber logs in successfully	
☐ Redirect	
☒ Pop Up ☐ Allow to close the pop up window	
Information Window Content	
Window Name	Information Window (Max. 30 character)
Main message	You can use Internet now! (Max. 30 character)
Message Description	This is an information window to sl (Max. 150 character)
Usage count label	Standard usage count time/traffic label or RADIUS with session timeout Remaining Usage (Max. 30 character) without session timeout Connecting Usage (Max. 30 character)
☐ Warning/Alarm message	If you don't want to continue using (Max. 150 character)
☐ Notice Message	Notice Text 1 Notice! (Max. 150 character) Notice Text 2 If you are going to use VPN, pleas (Max. 150 character) Notice Text 3 (Max. 150 character)
 Preview	
 Apply	

The following table describes the labels in this screen that you set to customize the information window.

Table 36 Customization: Information Window

LABEL	DESCRIPTION
Window Name	Enter a descriptive name (up to 30 characters) as the title of the window.
Display Information Window once after a subscriber logs in successfully	Select this option to display the information window on the subscriber's computer after a successful login. Clear this check box to disable this feature.
Redirect	Select Redirect to display the information in the same web browser screen.
Pop Up	Select Pop Up to display the information in a separate pop-up web browser screen. Select Allow to close the pop up window if you want to allow subscribers to close the information pop-up screen. Clear this check box to display the information pop-up screen all the time.
Information Window Content	
Window Name	Enter a descriptive name for the window title.
Main message	Enter a short message (up to 30 characters).
Message Description	Enter a short description about the information window.
Usage count label	Enter the label for the field displaying the remaining time in the first text box provided. This field displays when the VSG is set to use proprietary or RADIUS server (without session timeout messages) authentication. Enter the label for the field displaying the amount of time used in the second text box provided. This field displays when the VSG is set to use RADIUS (without session timeout messages) authentication.
Warning/Alarm Messages	Select this check box to display the warning message that you enter in the text box provided.
Notice Message	Select this check box to display any additional message(s) that you enter in the test box(es) provided. You can specify up to three additional messages (such as discount information) in the information window.
Preview	Click to display a preview of the information window.
Apply	Click Apply to save the changes.

The following figure shows an information window example.

Figure 73 Subscriber Pop-up Information Window Example

15.4 Account Printout

After you have created the subscriber accounts, you can print out the account information. The printout page is different for static and dynamic subscriber accounts.

To customize the account printout, click **Advanced Settings, Customization** and click the **Account Printout** link to display the screen as shown.

Figure 74 Customization: Account Printout

Account Printout Customization	
Title:	Welcome! (Max.=23)
Subtitle:	This is your account information, please keep this for y (Max.=80)
Username:	Username:
Password:	Password:
Usage Time:	Usage Time:
Billing Method:	Billing:
Billing Profile Description:	Profile:
Purchase Unit:	Purchase Unit
☐ Additional Label 1:	ESSID: Value: (Max.=23)
☐ Additional Label 2:	WEP: Value: (Max.=23)
☒ Price:	Total:
☒ Account Create Time:	yyyy/mm/dd HH:mm:ss (HH:24h hh:12h tt:AM/PM)
Expire	Please active your account before Description: (Max.=72) Date/Time: yyyy/mm/dd HH:mm:ss (HH:24h hh:12h tt:AM/PM) Accumulation: After your first logged-in, please finish your usage time within (Max.=96)
☒ Ending:	Thank you very much! (Max.=23)
☒ Serial Number	
Preview of PC-connected printer for static account printout Preview of account generator printer with static account printout Preview of PC-connected printer for dynamic account printout Preview of account generator printer with dynamic account printout	
Apply	

The following table describes the labels in this screen.

Table 37 Customization: Account Printout

LABEL	DESCRIPTION
Title	Enter a title (up to 24 characters) for the printout.
Subtitle	Enter a subtitle (up to 80 characters) for the printout.
Username	Enter the label name for the field displaying the account username.

Table 37 Customization: Account Printout (continued)

LABEL	DESCRIPTION
Password	Enter the label name for the field displaying the account password.
Usage Time	Enter the label name for the field displaying the amount of time an account is allowed for Internet access.
Billing Method	Enter the label name for the field displaying the method for billing.
Billing Profile Description	Enter the label name for the field displaying the name for the billing profile used.
Purchase Unit	Enter the label name for the field displaying the number of time units purchased.
Additional Label 1.. 2	Select this check box to display the specified label name(s) for the field(s) displaying any additional information. For example, you can specify additional information such as ESS ID and/or WEB key for wireless stations when you connect an access point to the VSG.
Price	Select this check box to display the specified label name for the field displaying the total price.
Account Create Time	Select this check box to display the time an account is created. Select a time format from the drop-down list boxes.
Expire	
Description	Enter a short description that tells the subscribers when they should activate their accounts before the displayed time.
Date/Time	Select a date and time format for the expiry date.
Accumulation	Enter a short description that tells the subscribers when they should use their purchased Internet access service before the displayed time.
Ending	Select this check box to display a message to display at the end of the printout. Enter the message in the text box provided.
Serial Number	Select this check box to display a serial number on the printout.
Preview of PC-Connected printer for Static Account printout.	Click this link to display a preview of a static account printout as it would print on a printer connected to a computer.
Preview of account generator printer with Static Account printout.	Click this link to display a preview of a static account printout as it would print on a statement printer.
Preview of PC-Connected printer for Dynamic Account printout.	Click this link to display a preview of a dynamic account printout as it would print on a printer connected to a computer.
Preview of account generator printer with Dynamic Account printout.	Click this link to display a preview of a dynamic account printout as it would print on a statement printer).
Apply	Click Apply to save the changes.

Note: The account information printout for a static account varies depending on whether PMS billing is used or not.

The following figures show the account printout examples.

Figure 75 Static Account Printout Example

Welcome!	
This is your account information, please keep this for your Internet Service.	
Username:	x0000000x
Password:	x0000000x
Billing:	Time to Finish
Profile:	1 day \$10.00
Purchase Unit:	1
Total:	\$ 10.00
Thank you very much !	
----- cut ----- cut ----- cut -----	
Username:	x0000000x
Billing:	Time to Finish
Profile:	1 day \$10.00
Purchase Unit:	1
Total:	\$ 10.00
Signature:	

2006/6/16 14:45:06

Figure 76 Static Account with PMS Billing Printout Example

Welcome!	
This is your account information, please keep this for your Internet Service.	
Username:	x0000000x
Password:	x0000000x
Thank you very much !	

Figure 77 Static Account Printout: Statement Printer Example

Welcome!

This is your account information, please keep
this for your Internet Service.

Username:xxxxxxxx

Password:xxxxxxxx

Usage Time:

Billing: Time to Finish

Profile: 1 day \$10.00

Purchase Unit: 1

Total: \$ 10.00

Thank you very much !

-----CUT-----CUT-----CUT-----

Username:xxxxxxxx

Password:xxxxxxxx

Billing: Time to Finish

Profile: 1 day \$10.00

Purchase Unit: 1

Total: \$ 10.00

Signature:

2006/6/16 14:48:23

[Close](#) [Print](#)

Figure 78 Static Account with PMS Billing Printout: Statement Printer Example

Welcome!

This is your account information, please keep
this for your Internet Service.

Username:xxxxxxxx

Password:xxxxxxxx

Thank you very much !

Figure 79 Dynamic Account Printout Example

Welcome!	
This is your account information, please keep this for your Internet Service.	
Username:	xxxxxxxx
Password:	xxxxxxxx
Billing:	Time to Finish
Profile:	1 day \$10.00
Purchase Unit:	1
Total:	\$ 10.00
S/N:000001 2006/6/16 14:50:56	
Please active your account before 2006/6/17 02:50:56	
Thank you very much !	
Close Print	

Figure 80 Dynamic Account Printout: Statement Printer Example

Welcome! ----- This is your account information, please keep this for your Internet Service. ----- Username:xxxxxxxx Password:xxxxxxxx Usage Time: Billing: Time to Finish Profile: 1 day \$10.00 Purchase Unit: 1 Total: \$ 10.00 ----- 2006/6/16 14:51:56 S/N:000001 Please active your account before 2006/6/17 02:51:56 Thank you very much !
Close Print

15.5 User Agreement Screen

In cases where authentication is not required and anyone can access the Internet through the VSG, you can set the VSG to require users to accept a service usage agreement before they can access the Internet. The VSG has a built-in user agreement page that you can customize.

To customize the user agreement page, click **Advanced Setting**, **Customization** and click the **User Agreement Page** link to display the screen as shown.

Figure 81 Customize: User Agreement

User Agreement Page	
Title	User Agreement Page (Max. 100 characters)
Title Text Color	000000 View Color Grid
Article	(Max. 5000 characters)
Article Text Color	000000 View Color Grid
Article Background Color	FFFFFF View Color Grid
Page Background Color	FFFFFF View Color Grid
Agree Button	Agree (Max. 50 characters)
Disagree Button	Do not agree (Max. 50 characters)
Standard User Agreement Page Preview	
Apply	

The following table describes the labels in this screen.

Table 38 Customization: Account Printout

LABEL	DESCRIPTION
Title	Enter a title (up to 100 characters) for the user agreement page.
Title Text Color	Set the color of the title text. For example, use '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Article	Enter a block of text (up to 12000 characters long) in the text box. This is the restrictions or conditions that you want the user to agree to before allowing Internet access.
Article Text Color	Set the color of the article text. For example, use '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Article Background Color	Specify the background color of the article text color. For example, enter '000000' for black. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Page Background Color	Set the background color for the article. For example, use 'FFFFFF' for white. Click View Color Grid to display a list of web-friendly colors and corresponding hexadecimal values.
Agree Button	Enter the label name for the button the subscribers click to accept the service usage agreement before they can access the Internet.
Disagree Button	Enter the label name for the button the subscribers click to decline the service usage agreement. They will not be able to access the Internet.

Table 38 Customization: Account Printout (continued)

LABEL	DESCRIPTION
Standard User Agreement Preview	Click this link to preview the standard user agreement screen in a new browser window.
Apply	Click Apply to save the changes.

The following figure shows a user agreement page example.

Figure 82 Customization: Account Printout: PreviewA screenshot of a web form titled "User Agreement Page". It contains a text area labeled "Article text". Below the text area are two radio buttons: "Regular User" (selected) and "VPN User". At the bottom are two buttons: "Agree" and "Do not agree".

15.6 Credit Card

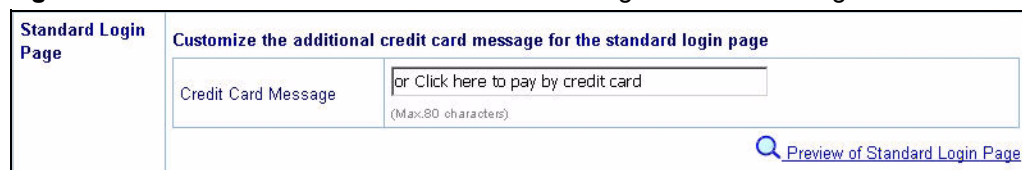
After you have entered your Authorize.net account information in the **Credit Card** screen, you may customize the credit card information screen the subscribers use.

Click **Advanced**, **Customization** and click the **Credit Card** link to display the **Credit Card Customization** screen. Configure the fields in this screen and click **Apply** to save the changes.

15.6.1 Standard Login Page

If you use the standard subscriber login screen, you can specify a message to re-direct credit-card-paying subscribers to the credit card information screen.

In the **Credit Card Customization** screen, enter the message in the **Credit Card Message** field and click **Apply** to save the changes.

Figure 83 Credit Card Customization: Standard Login Screen MessageA screenshot of the "Standard Login Page" customization screen. The title is "Customize the additional credit card message for the standard login page". It features a text input field labeled "Credit Card Message" with the placeholder text "or Click here to pay by credit card" and a note "(Max:80 characters)". At the bottom right is a link with a magnifying glass icon labeled "Preview of Standard Login Page".

Click **Preview of Standard Login Page** to display a preview screen.

Figure 84 Credit Card Customization: Standard Login Screen Message: Preview

The image shows a web form titled "Welcome" in a light blue header. Below the header is a login section with two fields: "Username:" and "Password:", each followed by a text input box. Below the login section is a service selection area. It contains the text "Please choose from the following service selection" followed by a dropdown menu showing "1 day \$10.00". Below this is the text "How many units of Internet access would you like to purchase?" followed by a dropdown menu showing "1". Below these are two lines of small text: "*Please kindly note that there will be no refund once connectivity is confirmed." and "*Please note that the time block of selected service is based on continuous usage." Below this is a paragraph: "Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio." Below this paragraph are two buttons: "Enter" and "Cancel". Below the buttons is a link: "or click here to pay by credit card." and below the link is a VISA logo.

Welcome	
Username:	
Password:	
Please choose from the following service selection 1 day \$10.00	
How many units of Internet access would you like to purchase? 1	
*Please kindly note that there will be no refund once connectivity is confirmed.	
*Please note that the time block of selected service is based on continuous usage.	
Please click ENTER to confirm your acceptance of the usage charge or CANCEL to exit. The selected service charge will be posted directly into your guest folio.	
Enter	Cancel
or click here to pay by credit card.	
	

15.6.2 Service Selection Page

Specify the service selection and credit card messages to display on the subscriber login screen in the **Credit Card Customization** screen.

Figure 85 Credit Card Customization: Service Selection Page

Service Selection Page	Customize the message for the service selection page	
Service Selection Message	Please choose from the following service selection (Max. 80 characters)	
Purchase Unit Message	How many units of Internet access would you like to (Max. 80 characters)	
Notification Message 1	*Please kindly note that there will be no refund on (Max. 160 characters)	
Notification Message 2	*Please note that the time block of selected service (Max. 160 characters)	
Notification Message 3		
Enter Payment Information	Enter Payment Information (all info is required) (Max. 160 characters)	
Enter Credit Card Number	Credit card number: (Max. 80 characters)	
Enter Credit Card expiration date	Credit card expiration date: (Max. 80 characters)	
Enter Email Address	Enter Email Address (Max. 80 characters)	
Submit Button	Submit Transaction and Login (Max. 40 characters)	
Additional Customer Data Merchants may provide additional customer information with a transaction, based on their respective requirements.		
☐ Customer ID	Customer ID: (Max. 40 characters)	
☒ First/Last Name	First Name: (Max. 20 characters)	Last Name: (Max. 20 characters)
☐ Company	Company: (Max. 40 characters)	
☒ Address	Address: (Max. 40 characters)	
☒ City	City: (Max. 40 characters)	
☒ State/Province	State/Province: (Max. 40 characters)	
☒ ZIP/Postal Code	ZIP/Postal Code: (Max. 40 characters)	
☒ Country	Country: (Max. 40 characters)	
☒ Phone	Phone: (Max. 40 characters)	
☐ Fax	Fax: (Max. 40 characters)	
 Preview of Service Selection Page		

The following table describes the labels in this screen.

Table 39 Credit Card Customization: Service Selection Page

LABEL	DESCRIPTION
Service Selection Page	
Customize the message for the service selection page.	Specify the service selection messages in the fields provided.
Service Selection Messages	Enter a message to instruct the subscribers to select a billing profile.
Purchase Unit Message	Enter a message to instruct the subscribers to select the number of time units to purchase.
Notification Message 1 .. 3	Enter additional message(s) regarding the replenish feature. For example, you may enter a refund policy.
Enter Payment Information	Enter the heading label name to prompt for the payment information.
Enter Credit Card Number	Enter the label name of a field in which subscribers enter the credit card number.
Enter Credit Card expiration date	Enter the label name of a field in which subscribers enter the expiration date of the credit card.
Enter Email Address	Enter the field label for the subscriber's e-mail address. The VSG sends the subscriber account information to this e-mail address if you enable the feature in the Credit Card screen (refer to Section 14.2 on page 117 for more information).
Submit Button	Enter the label of the button on which subscribers clicks to send the information in the screen.
Additional Customer Data	If you want to obtain more information from the subscribers, select the checkbox(es) and specify the corresponding field label(s).
Customer ID	Select this checkbox to display this field and enter the field label for customer ID information.
First/Last Name	Select this checkbox to display these two fields and specify the field labels for the subscriber to enter the first and last names.
Company	Select this checkbox to display this field and specify the label name of a field in which subscribers enter a company name.
Address	Select this checkbox to display this field and specify the label name of a field in which subscribers enter their addresses.
City	Select this checkbox to display this field and specify the label name of a the field in which subscribers enter the city.
State/Province	Select this checkbox to display this field and specify the label name of the field in which subscribers enter the state or province name.
Zip/Postal Code	Select this checkbox to display this field and specify the label name of the field in which subscribers enter the ZIP or postal code.
Country	Select this checkbox to display this field and specify the label name of the field in which subscribers enter the country.
Phone	Select this checkbox to display this field and specify the label name of a field in which subscribers enter the phone numbers.

Table 39 Credit Card Customization: Service Selection Page (continued)

LABEL	DESCRIPTION
Fax	Select this checkbox to display this field and specify the label name of the field in which subscribers enter the fax numbers.
Preview of the Service Selection Page	Click Preview of the Service Selection Page for a preview screen (see Figure 86 on page 139 for an example).

The following figure shows an example of the subscriber credit card information screen. Field labels display in red are the required fields.

Figure 86 Credit Card Customization: Service Selection Page: Preview

Welcome

Please choose from the following service selection 1 day \$10.00

How many units of Internet access would you like to purchase? 1

*Please kindly note that there will be no refund once connectivity is confirmed.
*Please note that the time block of selected service is based on continuous usage.

Enter Payment Information (all info is required)

Credit card number:	
Credit card expiration date:	(MMYY)
Enter Email Address	
First Name:	
Last Name:	
Address:	
City:	
State/Province:	
ZIP/Postal Code:	
Country:	
Phone:	

Submit Transaction and Login

15.6.3 Successful Page

You can customize the notification screen to display on the subscriber's computer when the credit card is validated and the transaction is successful.

Scroll down the **Credit Card Customization** screen and configure the **Successful Page** fields and click **Apply** to save the changes.

Figure 87 Credit Card Customization: Successful Page

Successful Page	
Customize the message for the successful page	
Successful Message	You may now use the Internet ! (Max: 80 characters)
Notification Message 1	IMPORTANT! Make a note of your username and p. (Max: 160 characters)
Notification Message 2	 (Max: 160 characters)
Account Information	This is your account information, please keep this f (Max: 160 characters)
Username	Your username is (Max: 80 characters)
Password	Your password is (Max: 80 characters)
Usage Time	Your usage time is (Max: 80 characters)
Expiration Time	Please activate your account before (Max: 80 characters) Format: yyyy/mm/dd HH:mm:ss (HH:24h hh:12h tt:AM/PM)
Email Button	Email this webpage to myself (Max: 40 characters)
Submit Button	Use this account to LOGIN now (Max: 40 characters)

 [Preview of Successful Page](#)

The following table describes the labels in this screen.

Table 40 Credit Card Customization: Successful Page

LABEL	DESCRIPTION
Successful Message	Enter a message to notify the subscribers that the credit card validation is successful.
Notification Message 1 .. 2	Enter additional message(s). For example, you may enter a refund policy.
Account Information	Enter the caption for the account information.
Username	Enter the label name for the username field.
Password	Enter the label name for the password field.
Usage Time	Enter the label name for the usage time field.
Expiration Date	Enter the label name for the expiration date field.
Email Button	Enter the label name for the e-mail button the subscribers click to have the VSG e-mail this information in this screen to the subscribers.
Submit Button	Enter the label name for the button the subscribers click to confirm and log in for I
Preview of Successful Page	Click Preview of Successful Page for a preview screen (see Figure 88 on page 141 for an example).

The following figure shows an example.

Figure 88 Credit Card Customization: Successful Page: Preview

15.6.4 Fail Page

You can customize the notification screen to display on the subscriber's computer when the credit card is not validated or the transaction is not successful.

Scroll down the **Credit Card Customization** screen and configure the **Fail Page** fields and click **Apply** to save the changes.

Figure 89 Credit Card Customization: Fail Page

The following table describes the labels in this screen.

Table 41 Credit Card Customization: Fail Page

LABEL	DESCRIPTION
Notification Message 1 .. 3	Enter additional message(s). For example, why the transaction failed. .
Try Again Button	Enter the label name for the button subscribers click to display the screen in which the subscribers can enter the credit card information again.

Table 41 Credit Card Customization: Fail Page (continued)

LABEL	DESCRIPTION
Close Button	Enter the label name for the button subscribers click to close this screen.
Preview of Fail Page	Click Preview of Fail Page for a preview screen (see Figure 90 on page 142 for an example).

The following figure shows an example.

Figure 90 Credit Card Customization: Fail Page: Preview

15.7 Bill Output

In a hotel, you have the option of printing a separate bill for Internet access service in a hotel room. You can customize how the bill will printout in the **Output Bill Customization** screen.

Click **Advanced Setting, Customization** and the **Output Bill** link to display the screen as shown.

Figure 91 Customization: Output Bill

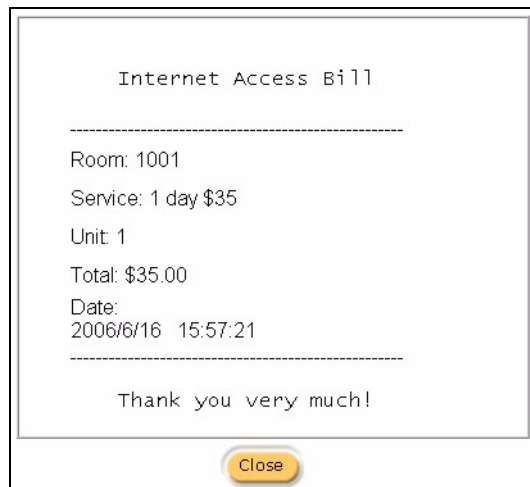
The following table describes the labels in this screen.

Table 42 Customization: Output Bill

LABEL	DESCRIPTION
Title	Select this checkbox to display this field and enter the field label for the screen title.
Room No.	Specify the field label name to display the hotel room number.
Service	Specify the field label name to display the service type. For example, "Internet Access".
Unit	Specify the field label name to display the number of time units purchased.
Price	Specify the field label name to display the total price.
Purchase Time	Select this checkbox to display this field and select the time and date format to display the purchase time.
Ending	Select this checkbox to display this field and specify a closing sentence for the bill printout.
Preview	Click this link to preview a bill printout in a new browser window.
Apply	Click Apply to save the changes.

The following figure shows a bill printout example.

Figure 92 Customization: Output Bill: Example



CHAPTER 16

Bandwidth Management

This chapter describes the bandwidth feature and shows you how to configure bandwidth control.

16.1 Bandwidth Management Overview

Bandwidth management allows you to control the amount of outbound and inbound traffic on the LAN. This helps reduce delays and dropped packets due to busy network traffic. On the VSG, outbound traffic refers to network traffic coming from a LAN port to the WAN port whereas inbound traffic refers to network traffic coming from the WAN port to a LAN port.

16.1.1 Bandwidth Allocation

The VSG provides two types of bandwidth control based on a subscriber's computer MAC address: equal share or class-based.

With equal share bandwidth allocation, the VSG allocates an equal amount of outgoing and incoming bandwidth for each subscriber on the LAN.

With class-based bandwidth allocation, you can set up bandwidth classes in the billing profiles on the VSG or on a RADIUS server.

16.2 Activating Bandwidth Management

To activate bandwidth management, click **Advanced Setting** , **Bandwidth** and select the **Bandwidth Management** check box.

Figure 93 Bandwidth Management: Activate

Bandwidth Management

☒ **Bandwidth Management**

☒ **Equal bandwidth for all subscribers**

The function enables administrator to limit bandwidth usage on a per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.

Maximum Upstream Bandwidth	☒ 256Kbps ☐ 0 Kbps (64-24576)
Maximum Downstream Bandwidth	☒ 256Kbps ☐ 0 Kbps (64-24576)

☐ **Class of service based on RADIUS or billing profile settings**

The function enables administrator to limit bandwidth usage according to the RADIUS vendor-specific attribute (RADIUS authentication) or billing profile setting (Built-in authentication). This allows every user to have a different service quality for Internet bandwidth.

Apply

16.2.1 Equal Bandwidth Setup

To configure the VSG to impose the same bandwidth limits on all subscribers, select **Equal bandwidth for all subscribers** in the **Bandwidth Management** screen and set the related fields.

Figure 94 Bandwidth Management: Equal Share

Bandwidth Management

☒ **Bandwidth Management**

☒ **Equal bandwidth for all subscribers**

The function enables administrator to limit bandwidth usage on a per user basis (MAC address). That prevents users from consuming a disproportionately large amount of bandwidth so every user gets a fair share of the available bandwidth.

Maximum Upstream Bandwidth	☒ 256Kbps ☐ 0 Kbps (64-24576)
Maximum Downstream Bandwidth	☒ 256Kbps ☐ 0 Kbps (64-24576)

☐ **Class of service based on RADIUS or billing profile settings**

The function enables administrator to limit bandwidth usage according to the RADIUS vendor-specific attribute (RADIUS authentication) or billing profile setting (Built-in authentication). This allows every user to have a different service quality for Internet bandwidth.

Apply

The following table describes the related labels in this screen.

Table 43 Bandwidth Management: Equal Share

LABEL	DESCRIPTION
Maximum Upstream Bandwidth	To use a pre-defined option, select the first option and choose a bandwidth from the drop-down list box. To manually set the bandwidth, select the second option and specify the bandwidth in the field provided.
Maximum Downstream Bandwidth	To use a pre-defined option, select the first option and choose a bandwidth from the drop-down list box. To manually set the bandwidth, select the second option and specify the bandwidth in the field provided.

16.2.2 Class of Service Bandwidth Setup

To set the VSG to impose different bandwidth limits based on the configurations in a RADIUS server or a billing profile, select **Class of service based on RADIUS or Billing profile settings** in the **Bandwidth Management** screen.

You must then set the bandwidth management on a RADIUS server or in a billing profile. Refer to [Chapter 10 on page 88](#) to set the bandwidth limits in a billing profile.

Figure 95 Bandwidth Management: Class of Service

The screenshot shows the 'Bandwidth Management' configuration window. At the top, there is a header 'Bandwidth Management'. Below it, a checkbox labeled 'Bandwidth Management' is checked. Underneath, there are two radio button options. The first option, 'Equal bandwidth for all subscribers', is currently selected. The second option, 'Class of service based on RADIUS or billing profile settings', is highlighted with a red rectangle. Below the first option, there are two rows of configuration fields: 'Maximum Upstream Bandwidth' and 'Maximum Downstream Bandwidth'. Each row has a radio button for a predefined value (256Kbps) and a radio button for a manual input (0 Kbps). The 'Class of service based on RADIUS or billing profile settings' option is described as: 'The function enables administrator to limit bandwidth usage according to the RADIUS vendor-specific attribute (RADIUS authentication) or billing profile setting (Built-in authentication). This allows every user to have a different service quality for Internet bandwidth.' An 'Apply' button is located at the bottom right of the window.

CHAPTER 17

Portal Page, Advertisement Link and Walled Garden

This chapter shows you how to set a portal web site, advertisement links and create walled garden web sites.

17.1 Overview

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

17.2 Portal Page

A portal page is the first web site to which a subscriber is redirected after logging in successfully. If you do not specify a portal web site, the subscriber will be directed to the intended web site specified.

Click **Advanced** and **Portal Page** to display the screen as shown next.

Figure 96 Portal Page

Portal Page	
This feature allows to redirect subscriber's browser to a specified portal page after successful login.	
URL Link	
Apply	

The following table describes the labels in this screen.

Table 44 Portal Page

LABEL	DESCRIPTION
URL Link	Enter the web site address of a portal page.
Apply	Click Apply to save the settings.

17.3 Advertisement Links

You can set the VSG to display an advertisement web page first on the subscriber's computer once connected to the Internet. Click **Advanced** and **Advertisement** to display the screen as shown next.

Figure 97 Advertisement

Advertisement	
Frequency	☒ One Time Only ☐ Every 0 Min(s)
Sequence	☒ Randomly ☐ Orderly (From 1 to 10)
Link 1	
Link 2	
Link 3	
Link 4	
Link 5	
Link 6	
Link 7	
Link 8	
Link 9	
Link 10	
Apply	

The following table describes the labels in this screen.

Table 45 Advertisement

LABEL	DESCRIPTION
Frequency	Select One Time Only to display an advertisement web site in a pop-up browser window once after a subscriber logs in successfully. Select Every ... Min(s) to display an advertisement web site in a pop-up browser window once every time period specified (between 1 and 60 minutes) after a subscriber logs in successfully.
Sequence	Select Randomly to display the advertisement web pages in random order. Select In Order to display the advertisement web pages in the order as configured.
Link 1 .. 10	Enter the web site addresses in the fields provided.
Apply	Click Apply to save the changes.

17.4 Walled Garden

A subscriber must log in before the VSG allows the subscriber access to the Internet. However, with walled garden, you can define the web site address(es) which all users can access without logging in.

Note: A walled garden web site may not display properly or even be accessible if the domain name contains multiple IP addresses.

Click **Advanced** and then **Walled Garden** to display the screen as shown.

Figure 98 Walled Garden

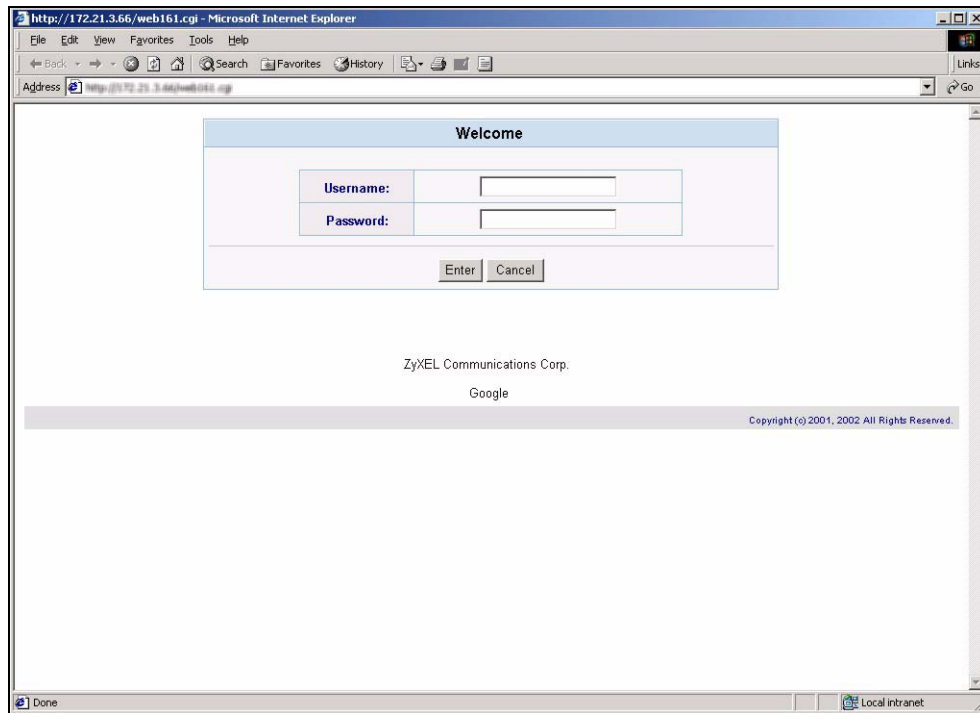
Walled Garden	
Link 1	Name: URL:
Link 2	Name: URL:
Link 3	Name: URL:
Link 4	Name: URL:
Link 5	Name: URL:
Link 6	Name: URL:
Link 7	Name: URL:
Link 8	Name: URL:
Link 9	Name: URL:
Link 10	Name: URL:
Apply	

The following table describes the labels to configure the walled garden feature.

Table 46 Walled Garden

LABEL	DESCRIPTION
Link 1 ... 10	In the Name field, enter a descriptive name (up to 80 characters) for the walled garden link to be displayed in the web browser. In the URL field, enter the web site address (up to 200 characters) of the web site.
Apply	Click Apply to save the changes.

The following figure shows a subscriber login screen example with walled garden links.

Figure 99 Subscriber Login Screen with Walled Garden Links Example

CHAPTER 18

Passthrough

This chapter shows you how to set up computer and web site passthrough.

18.1 Passthrough Overview

There are two types of pass through you can set up on the VSG: by device or by web site address. You can set the VSG to allow specific computers (based on the IP or MAC address) to access the Internet without prompting for a user name and password.

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

To configure passthrough on the VSG, click **Advanced** and then **Passthrough**.

18.2 Computer IP and MAC Address Passthrough

You can specify the IP or MAC address(es) of a computer that can access the Internet without entering a user name and password. This feature is useful, for example, if you want to set up computers to provide free Internet access in the VIP room or for sponsors in events.

Figure 100 Passthrough: Subscriber IP and MAC Address

Subscriber IP & MAC Address Passthrough					
No.	IP Address	No.	IP Address	No.	IP Address
1		13		25	
2		14		26	
3		15		27	
4		16		28	
5		17		29	
6		18		30	
7		19		31	
8		20		32	
9		21		33	
10		22		34	
11		23		35	
12		24		36	
No.	MAC Address	No.	MAC Address	No.	MAC Address
1		11		21	
2		12		22	
3		13		23	
4		14		24	
5		15		25	
6		16		26	
7		17		27	
8		18		28	
9		19		29	
10		20		30	

The following table describes the fields in this screen.

Table 47 Passthrough: Subscriber IP and MAC Address

FIELD	DESCRIPTION
Subscriber IP & MAC Address Passthrough	
No.	This read-only field displays the index number of an entry.
IP Address	Enter the IP address of a computer (in dotted decimal notation) whose packets are allowed to pass through the VSG. For example, 10.59.1.10.
MAC Address	Enter the MAC address of a computer (in 6 hexadecimal pairs separated by a hyphen "-", for example, 00-50-BA-8D-22-96) whose packets are allowed to pass through the VSG.

18.2.1 Destination URL and IP Address Passthrough

You can specify the IP address or the URL of the web site(s) that any user can access without entering a user name or password.

Figure 101 Passthrough: Destination URL and IP

Destination IP Address Passthrough					
No.	IP Address	No.	IP Address	No.	IP Address
1		13		25	
2		14		26	
3		15		27	
4		16		28	
5		17		29	
6		18		30	
7		19		31	
8		20		32	
9		21		33	
10		22		34	
11		23		35	
12		24		36	

Destination URL Passthrough	
No.	URL Link Page
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

The following table describes the fields in this screen.

Table 48 Passthrough: Destination URL and IP

FIELD	DESCRIPTION
Destination IP Address Passthrough	
No.	This read-only field displays the index number of an entry.
IP Address	Enter the IP address of a web site in dotted decimal notation, for example, 192.168.1.10
Pass Through Destination URL	

Table 48 Passthrough: Destination URL and IP (continued)

FIELD	DESCRIPTION
No.	This read-only field displays the index number of an entry.
URL Link Page	Enter the web site address, for example, http://www.zyxel.com .

CHAPTER 19

Filter

This chapter shows you how to configure filters to restrict access to the specified IP addresses through the VSG.

19.1 Filter Setup

You can set the VSG to restrict access to specified IP address(es) via the VSG. You can prevent subscribers from accessing certain web sites (for example, playboy) based on the IP address.

To configure a filter, click **Advanced** and **Filtering** in the navigation panel.

Figure 102 Advanced: Filter

FILTER			
☐ ENABLE FILTER			
Filtering allows the system administrator to have a list of restricted destinations.			
Single IP Address			
NO.	IP ADDRESS	NO.	IP ADDRESS
1		4	
2		5	
3		6	
IP Address Range			
NO.	IP ADDRESS		
1		~	
2		~	
3		~	
4		~	
5		~	
Apply			

The following table describes the fields in this screen.

Table 49 Filter

FIELD	DESCRIPTION
ENABLE FILTER	Select this option to activate this feature.
Single IP Address	

Table 49 Filter (continued)

FIELD	DESCRIPTION
No.	This read-only field displays the index number of an entry.
IP Address	Specify the IP address of a network device you want to block Internet access through the VSG. Enter the IP address in dotted decimal notation. For example, 10.59.1.10.
IP Address Range	
No.	This read-only field displays the index number of an entry.
IP Address	Specify a range of IP addressed for the network devices you want to block Internet access through the VSG. Enter the beginning and ending IP addresses in dotted decimal notation. For example, 10.59.1.10 to 10.59.1.20.
Apply	Click Apply to save the changes.

CHAPTER 20

Privilege User

This chapter shows how to set the VSG to allow computers with the specified IP addresses to access the **Session List** screen.

20.1 Privilege User Setup

The VSG allows specified computer(s) to access the **Session List** screen without having to log in first. This allows administrators, network operators or supervisors to view the current connection information on the VSG instantly without having to enter the user name and password and navigating to the screen.

Click **Advanced Settings** and **Privilege User** to display the configuration screen.

Figure 103 Privilege User

Privilege User for Session List

☐ Disable
☒ Enable

Start IP: End IP: (Max. 10 IPs)

No.	Address List	Delete
1	172.23.37.102	☐

The following table describes the fields in this screen.

Table 50 Privilege User

FIELD	DESCRIPTION
Disable	Select Disable to deactivate this feature. You need to log into the web configurator first to view the Session List screen.
Enable	Select Enable to allow the computer(s) with the specified IP address(es) to access the Session List screen without logging in. Set the IP address(es) in the fields below.
Start IP	Enter the IP address in dotted decimal notation. For example, 10.59.1.10.
End IP	If you want to specify one IP address, enter the same IP address as in the Start IP field. If you want to specify a range of IP addresses, enter the last IP address in the range.
Add to List	Click Add to List to save the settings to the table below.
No.	This read-only field displays the index number of an entry.

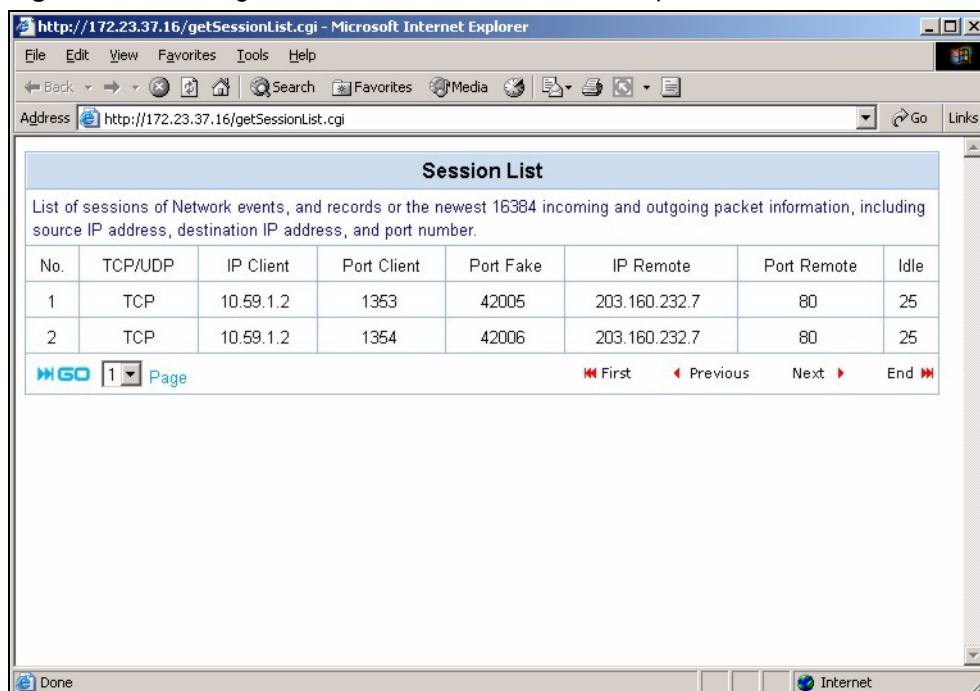
Table 50 Privilege User

FIELD	DESCRIPTION
Address List	This field displays one or a range of privilege IP address(es).
Delete	Click Delete to remove the selected IP address(es).
Apply	Click Apply to save the changes.

20.1.1 Accessing Session List As a Privilege User

On the computer whose IP address is included in the **Privilege User** screen, enter `http://VSG-IP/getSessionList.cgi` (where VSG-IP is the WAN or LAN IP address of the VSG) in the web browser. The **Session List** screen displays. Refer to [Section 28.5 on page 188](#) for the field descriptions.

The following figure shows an example where the WAN IP address of the VSG is 172.23.37.16.

Figure 104 Privilege User: Access Session List Example

CHAPTER 21

LAN Devices

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

21.1 LAN Devices Overview

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

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

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

21.1.1 Port Mapping

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

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

21.2 Configuring LAN Device Port Mapping

Click **Advanced** and **LAN Devices** to display the **LAN Device Management** screen as shown.

Note: You can configure port mapping for up to 300 LAN devices on the VSG.

Figure 105 LAN Devices

The following table describes the labels in this screen.

Table 51 LAN Devices

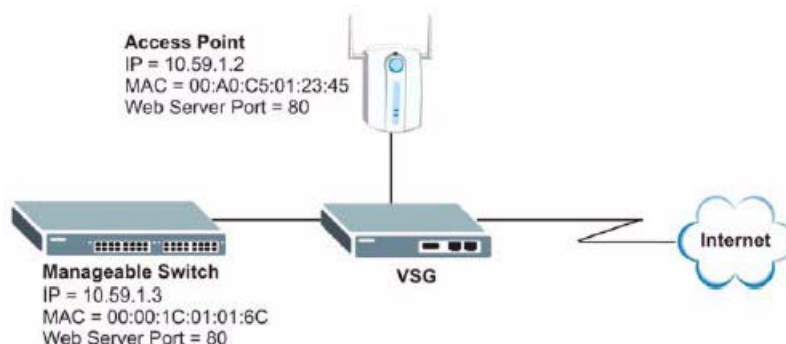
LABEL	DESCRIPTION
Polling Interval	Specify the time interval (in minutes) between the VSG's probes for device availability.
No.	This read-only field displays the index number of an entry.
Device Name	Enter the name of the LAN device for identification purposes.
Virtual Port	Enter a unique port number between 60001 and 60300 to map to the port number in the Server Port field.
Device IP Address	Enter the IP address of a LAN device in dotted decimal notation. For example, 10.59.1.111.
Device Server Port	Enter the port number of a management service (for example, 80 for HTTP) on the LAN device.
MAC Address	Enter the MAC address of the LAN device in hexadecimal notation in 6 hexadecimal pairs, for example, 0050BA8D2296. Note: Make sure you enter the correct MAC address.
Application	Select an application type from the drop-down list box. Choose from TCP or UDP . Only requests for the selected application type are forwarded to the specified server port on the LAN device.
Delete	Click Delete All to remove all accounts. Click Delete to remove the selected account.

Table 51 LAN Devices (continued)

LABEL	DESCRIPTION
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.
Apply	Click Apply to save the changes.

21.2.1 LAN Device Management Example

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

Figure 106 LAN Device Remote Management Example 1

You map virtual port 60001 on the VSG to the web server port on the access point and 60002 to the web server port on the manageable switch.

Figure 107 LAN Devices: Example 1

LAN Devices						
Accommodate up to 300 entries				Polling Interval: 1 Min(s)		
No.	Device Name	Virtual Port (60001~60300)	Device IP Address	Device Server Port	Device MAC Address	Application
1	AP	60001	10.59.1.2	80	00A0C5012345	TCP
2	ES Switch	60002	10.59.1.3	80	0001C001016C	TCP
3		0		0		TCP

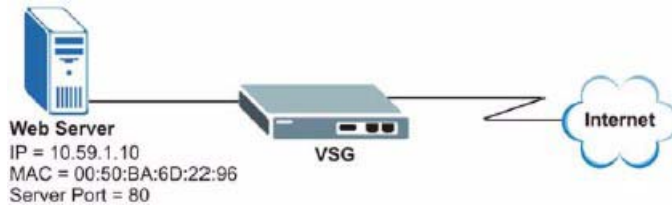
To access the web-based management interface, enter the WAN IP address of your VSG and the virtual port number of the LAN device separated by a colon. In this example, to access the access point (AP), enter “http:// 192.168.1.1:60001” where 192.168.1.1 is the WAN IP address of the VSG. The login screen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

You can also access the LAN devices through the VSG web configurator, refer to [Section 28.7.1 on page 190](#) for more information.

21.2.2 Specifying an Inside Server Example

Let's say you have a web server behind the VSG as shown in the next figure.

Figure 108 LAN Device Remote Management Example 2



In the **LAN Device Management** screen, you map virtual port 60001 to the server port (80) on the web server.

Figure 109 LAN Devices: Example 2

LAN Devices						
Accommodate up to 300 entries				Polling Interval: 1 Min(s)		
No.	Device Name	Virtual Port (60001~60300)	Device IP Address	Device Server Port	Device MAC Address	Application
1	web server	6010	10.59.1.10	80	0050BA6D2296	TCP
2		0		0		TCP

To access an inside server on the LAN, enter the WAN IP address of your VSG and the virtual port number of the inside server separated by a colon. In this example, to access the web server, enter “http:// 192.168.1.1:9602” where 192.168.1.1 is the WAN IP address of the VSG.

You can also access the server by entering the domain name provided that you specified a DNS server on the VSG. Enter the domain name and the virtual port number separated by a colon, for example, http://www.domainName:60001.

You can also access the LAN devices through the VSG web configurator, refer to [Section 28.7.1 on page 190](#) for more information.

CHAPTER 22

Static Route

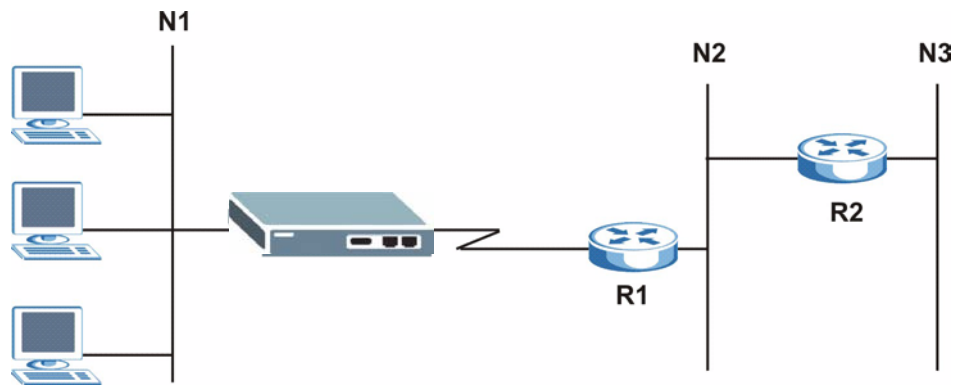
This chapter shows you how to configure static routes to specified destinations.

22.1 Static Route Overview

Static routes tell the VSG routing information that it cannot learn automatically through other means. This can arise in cases where RIP is disabled on the LAN or a remote network is beyond the one that is directly connected to a remote node.

Each remote node specifies only the network to which the gateway is directly connected and the VSG has no knowledge of the networks beyond. For instance, the VSG knows about network N2 in the following figure through remote node Router 1. However, the VSG is unable to route a packet to network N3 because it does not know that there is a route through remote node Router 1 (via Router 2). The static routes allow you to tell the VSG about the networks beyond the remote nodes.

Figure 110 Sample Static Routing Topology



22.2 Static Route Setup

Configure and view static route settings in the **Static Route** screen.

Click **Advanced** and **Static Route** to display the configuration screen.

Figure 111 Advanced: Static Route

Static Route					
No.	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Hop Count	Interface
1				1 ▾	LAN ▾
2				1 ▾	LAN ▾
3				1 ▾	LAN ▾
18				1 ▾	LAN ▾
19				1 ▾	LAN ▾
20				1 ▾	LAN ▾

Static Route Table						
No.	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Hop Count	Interface	Delete

The following table describes the labels in this screen.

Table 52 Advanced: Static Route

LABEL	DESCRIPTION
Static Route	Set the fields below to configure static route settings. You can configure up to 20 static routes at a time.
No.	This is the index number of the static route that you chose in menu 12.1.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Destination Subnet Mask	Type the subnet mask for this destination.
Gateway IP Address	Type the IP address of the gateway. The gateway is a router or switch on the same network segment as the device's LAN or WAN port. The gateway helps forward packets to their destinations.
Hop Count	Hop count represents the cost of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Select a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Interface	Specify whether the static route setting applies to the LAN or the WAN interface.
Apply	Click Apply to save the changes. New static route entries display in the table below.
Static Route Table	This table displays the static routes configured.
No.	This field displays the index number.
Destination IP Address	This field displays the IP address of the final destination.
Destination Subnet Mask	This field displays the subnet mask of the final destination.

Table 52 Advanced: Static Route (continued)

LABEL	DESCRIPTION
Gateway IP Address	This field displays the IP address of the gateway device.
Hop Count	This field displays the “cost” of this static route.
Interface	This field displays whether the static routing setting is applied on the LAN or WAN interface.
Delete	Select this option and click Delete to remove the selected static route(s).

CHAPTER 23

Private LAN

This chapter shows you how to set up a private LAN that allows specified devices to communicate with each other.

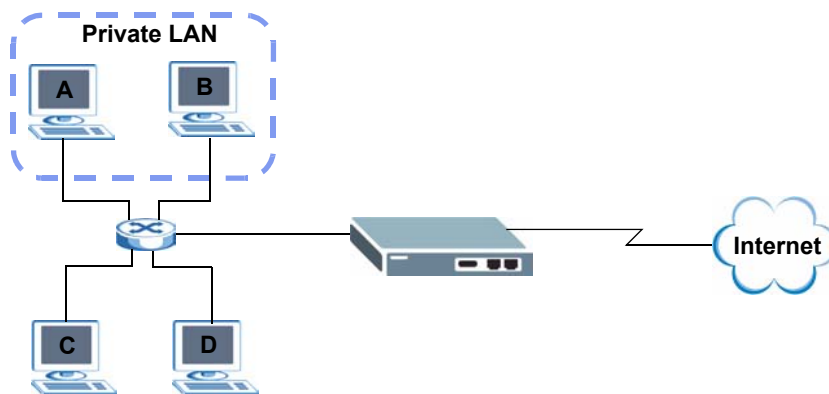
23.1 Private LAN Overview

By default the IP Plug and Play (iPnP) and layer-2 isolation features (see [Section 5.1 on page 56](#)) are enabled to prevent devices on the LAN from communicating with each other. These features provide additional security protection.

However, you can configure a private LAN to allow communication between devices with the specified IP addresses in the **Private LAN** screen. The VSG does not apply iPnP or layer-2 isolation on the devices in a private LAN.

The following figure shows a network example where computers **A** and **B** can communicate with each other in the private LAN. Since computers **C** and **D** are not in the private LAN, the VSG disallows communication between the two.

Figure 112 Private LAN Network Example



23.2 Configuring a Private LAN

To specify the IP address(es) to belong to the private LAN, click **Advanced** and **Private LAN** in the navigation panel.

Figure 113 Private LAN

Private LAN

Private LAN: Disable

This feature allows to have a Private LAN under Plug and Play mode and Layer 2 Isolation enable.

Please enter new Private LAN device (up to 50 entries)

☒ Start / End IP Address: ~

☐ IP Address:

Add to List

Private LAN device List

No.	Active	Private LAN Device IP Address List	Delete
001	☐	10.59.1.2	☐
002	☐	10.59.1.10 ~ 10.59.1.20	☐

Delete All

Apply

The following table describes the labels in this screen.

Table 53 Advanced: Private LAN

LABEL	DESCRIPTION
Private LAN	Select Enable to activate the private LAN settings. This allows Select Disable to deactivate this feature.
Start/End IP Address	Select this option to specify a range of IP addresses to belong to the private LAN. Enter the beginning and the ending IP addresses in the fields provided.
IP Address	Select this option to specify one IP address to belong to the private LAN. Enter the IP address in field provided.
Add to List	Click Add to List to insert the new setting in the table below.
Private LAN device List	This table displays the IP addresses or ranges of IP addresses in the private LAN.
No.	This field displays the index number.
Active	Select this option to set the selected entry to participate in the private LAN.
Private LAN Device IP Address List	This field displays one or a range of device IP addresses to belong in the private LAN.
Delete	Click Delete All to remove all accounts. Click Delete to remove the selected account.
Apply	Click Apply to save the changes.

CHAPTER 24

Syslog

This chapter shows you how to configure syslog logging.

24.1 Syslog Overview

Syslog logging allows the VSG to send logs to an external syslog server that is used to store and analyze logs.

24.1.1 Syslog Server Setup

Use the **Syslog** screen to configure to where the VSG is to send logs. To configure the syslog settings, click **Advanced**, **Logs** to display the screen as shown next.

Figure 114 Logs: Syslog

Syslog		
Syslog Server	☒ Disable ☐ Enable	
	☐ Syslog on LAN: Server IP Address: Server MAC Address:	
	☐ Syslog on WAN: Server 1 IP Address: Server 2 IP Address:	
	☒ Disable ☐ Enable	
Send to Email	IP Address or Domain Name: SMTP Port: 25	
	☐ E-mail (SMTP) server needs to check my account Username: Password:	
	Name: Email From: Address:	
	Email To: Email Address 1: Email Address 2:	
	Apply	

The following table describes the labels in this screen.

Table 54 Logs: Syslog

LABEL	DESCRIPTION
Syslog Server	Select Enable to activate the syslog function. Select Disable to de-activate the syslog function.
Syslog on LAN	Select this check box to specify a syslog server on the LAN.
Server IP Address	Enter the IP address (in dotted decimal notation) of the syslog server on the LAN.
Server MAC Address	Enter the MAC address of the syslog server on the LAN.
Syslog on WAN	Select this check box to specify a syslog server on the WAN.
Server 1 IP Address	Enter the IP address of the first syslog server on the WAN in dotted decimal notation.
Server 2 IP Address	Enter the IP address of the second syslog server on the WAN in dotted decimal notation.
Send to Email	Select Enable to have the VSG send logs to the specified email address. Select Disable to deactivate this feature. In this case, you can only view the log information on the VSG or the syslog server(s).
Email Server	
IP Address or Domain Name	Enter the IP address or domain name of the mail server.
SMTP Port	Enter the port number for SMTP email service on the mail server.
E-mail (SMTP) server needs to check my account	Select this option if you need to enter a user name and password to log into the mail server.
Username	Enter the username for your email account.
Password	Enter the password associated with the username above.
Email from	Specify the information of the email sender.
Name	Enter a descriptive name (up to 20 printable characters) of the sender. This is for identification purposes.
Email Address	Enter the email address of the sender. For example, vsg-1200@change.com
Email To	
Email Address 1..2	Enter the email addresses to which the VSG sends the logs.
Apply	Click Apply to save the settings.

24.1.2 Log Settings

To specify which logs the VSG is to send and the schedule for when the VSG is to send the logs, click **Advanced**, **Logs** and click the **Log Settings** link.

Figure 115 Logs: Log Settings

Log Settings					
The Syslog supports 4 types of syslog level. (161 Alert / 164 Warning / 165 Notice / 166 Inform)					
System					
Syslog	Email	Syslog Name	Description	Interval Time	Type
☐	☐	System Information	A log including the system information will be sent according to specified interval time	60 minutes	166
☐	☐	System Boot Notice	Once system reboots, the log will be sent	When system reboot	165
☐	☐	System Account Activity Information	A log would be sent if system account (Administrator, Supervisor or Account Operator) login to or logout from the device	When system account login or logout.	166
Accounting					
Syslog	Email	Syslog Name	Description	Interval Time	Type
☐	☐	Account Created	A log will be sent once after an account is created	When an account is created	166
☐	☐	Subscriber Trace	A log including subscribers login/logout time will be sent once after subscriber logout	When subscriber logout	165
☐	☐	Logged-in Users	A login users information will be sent according to specified interval time	60 minutes	166
☐	☐	User Agreement	A log would be sent when "user agreement" enabled	When subscriber login	166
Billing					
Syslog	Email	Syslog Name	Description	Interval Time	Type
☐	☐	Billing Log	A log would be sent according to specified interval time	When log created	166
LAN Devices Management					
Syslog	Email	Syslog Name	Description	Interval Time	Type
☐	☐	LAN Devices Information	A log including current LAN Devices Status will be sent according to specified interval time	60 minutes	166 164
☐	☐	LAN Devices Alarm	A log will be sent if one of the LAN Devices detected result is "Fail"	When device fail	161
Alert					
Syslog	Email	Syslog Name	Description	Interval Time	Type
☐	☐	Administration access Fail	A log would be sent when someone failed to access the administration web server	When someone failed to access the system web server	161
☐	☐	NAT Pool exhausted (IP / Port)	A log would be sent when IP or Port mapping exhausted	When NAT Pool exhausted	161
					Apply

The following table describes the labels in this screen.

Table 55 Logs: Log Settings

LABEL	DESCRIPTION
Syslog	Select this option to record and send this type of logs to the syslog server(s). Configure syslog server settings in the Syslog screen.
Email	Selec this option to send this type of logs to the specified email address(es). Configure email address settings in the Syslog screen.
Syslog Name	This field displays the name (or type) of the log. Select the check box(es) to send the syslog.

Table 55 Logs: Log Settings (continued)

LABEL	DESCRIPTION
Description	This field displays a short description about the syslog.
Interval Time	This field displays how often the VSG sends the logs. If available, enter the number of minutes the VSG waits between sending the syslog.
Type	This field displays the type number of a log. This number is read-only.
Apply	Click Apply to save the settings.

The following table describes the log formats.

Table 56 Logs: Log Format

SYSLOG NAME	FORMAT	CREATED
System Information	Id <MAC Address> System Uptime <0 days 00h:04m:00s> WAN <FrameTxOK FrameRxOK FrameTxError FrameRxError> LAN <FrameTxOK FrameRxOK FrameTxError FrameRxError>	Each time interval specified (between 1 and 10080 minutes).
System Boot Notice	Id <MAC Address> System Up	Each time when the device reboots.
System Account Activity Information	Id <MAC Address> System Account Activity Information <Username, User IP, Status> Where: Username = Administrator Supervisor Accounting Operator User IP = IP Address Status = Login Logout Idle Time Out	Each time when the system account logs in or logs out.
Account Created	Id <Mac Address> Account Create <username, Account usage time, Billing profile information> Where: Username = Single account <username> or Batch account <prefix, from, to, postfix> Billing profile information = index, name	When an account is created.
Subscriber Trace	Id <MAC Address> Subscriber Trace <username, user IP, user MAC, interface, login time, logout time, RxData count, TxData count>	When a subscriber logs out.
Logged-in Users	Id <MAC Address> Logged-in Users <Number of Logged-in users, Start Number, End Number> (Username, user IP, user MAC, interface, login time, RxData count, TxData count) [additional information]	Each time interval specified.
User Agreement		
Billing Log	Id <Mac Address> Billing Log <Username, Billing profile information, Log time, Usage time, Bill, Charge From> Where: Charge From = PMS Dynamic Billing profile name = Name Log time = MM/DD/YYYY HH:MM:SS Usage time = "x minutes" "Expire when 00:00" Billing profile information = index, name	When a log is created

Table 56 Logs: Log Format (continued)

SYSLOG NAME	FORMAT	CREATED
LAN Devices Information	Id <MAC Address> LAN Devices Information <Number of devices, Start Number, End number> Device name <status> [additional information]	Each time interval specified (between 1 and 10080 minutes).
LAN Devices Alarm	Id <MAC Address> LAN Device Alarm <Device name, FAIL>	When the VSG cannot connect to an attached LAN device.
Administrator access Fail	Id <MAC Address> Administration Access Fail <Fail message, User IP, Username> Where: Fail message = Bad Username/Password Unauthorized IP Exceeded Maximum Login Note: If Fail message = Unauthorized IP and no user name can be obtained, then Username = None . If Fail message = Exceeded Maximum Login , then Username = Administrator Supervisor Accounting Operator	Each time a system login attempt fails.
NAT Pool Exhausted (IP/Port)	Id <MAC Address>) NAT Pool Exhausted <Type> where: Type = NAT pool IP address NAT Port number	When no IP address or port is available for additional NAT mapping.

CHAPTER 25

Session Trace

This chapter shows you how to view subscriber session information on the VSG.

25.1 Session Trace Overview

You can set the VSG to send session information of subscribers accessing the Internet. The VSG records the session information and stores it temporary. Once the session trace information reaches a maximum of 50 records or the specified time period is reached, the VSG sends the session information to the specified TFTP server.

25.1.1 Configuring Session Trace

To configure the VSG to send subscriber session information, click **Advanced**, **Session Trace** to display the screen as shown.

Figure 116 Advanced: Session Trace

Session Trace	
Session Trace	☐ Enable ☒ Disable
TFTP Server IP Address	Primary TFTP Server IP Address Secondary TFTP Server IP Address
	Send Session Trace log file every 10 minutes. (5 ~ 1440) (Note: Session Trace log file will be sent also when collected 50 logs)
Apply	

The following table describes the labels in this screen.

Table 57 Advanced: Session Trace

LABEL	DESCRIPTION
Session Trace	Select Enable to set the VSG to record and send subscriber session information. Select Disable to de-activate this feature.

Table 57 Advanced: Session Trace (continued)

LABEL	DESCRIPTION
TFTP Server IP Address	Specify the primary and/or secondary TFTP IP address in the Primary TFTP Server IP Address and/or Secondary TFTP IP Address fields. Enter the IP address(es) in dotted decimal notation. For example, 192.168.1.10. Enter the time interval (in minutes between 5 and 1440) the VSG waits before sending the session information to the TFTP server(s). Note: If there are 50 session trace records, the VSG sends the session information to the TFTP server even if the time interval is not up.
Apply	Click Apply to save the settings.

25.1.2 Session Trace Filename Convention

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

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

Figure 117 Session Trace Information Example

Host Name	User Name	Date	VLANId	SourceIP	SourceMac	SourcePort	DestIP	DestPort
MIS	Cindy	22Oct04130403		192.168.1.10	0085A0010104	3974	192.168.1.1	80
MIS	Cindy	22Oct04130404		192.168.1.10	0085A0010104	3977	172.20.0.63	53
MIS	Cindy	22Oct04130440		192.168.1.10	0085A0010104	3991	172.20.0.27	80

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

Table 58 Session Trace File Fields

FIELD	DESCRIPTION
Host Name	This is the host (or system) name of the VSG.
User Name	This is the subscriber account username. This field is empty if you disable authentication in the Authentication screen (see Chapter 9 on page 80 for more information).
Date	This is the date and time the VSG creates a session trace record.
VLANId	This is the VID of the VLAN to which a subscriber belongs. This field is empty if no VLAN tag is present (see Chapter 13 on page 112 for more information).
SourceIP	This is the IP address of the subscriber.
SourceMac	This is the MAC address of the subscriber's computer.
SourcePort	This is the source port number of the subscriber.
DestIP	This is the destination IP address the subscriber accesses.
DestPort	This is the destination port number for this session.

CHAPTER 26

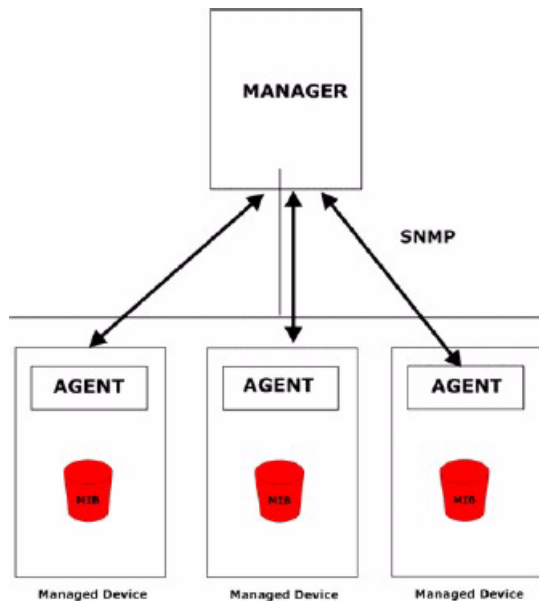
SNMP

This chapter shows you how to set up SNMP on the VSG in order to use a third-party management software to remotely manage the VSG.

26.1 SNMP Overview

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 VSG supports SNMP version one and version 2. The next figure illustrates an SNMP management operation.

Figure 118 SNMP Management Model



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

An agent is a management software module that resides in a managed device. 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.

26.1.1 Network Management System (NMS)

An NMS (Network Management System) is a management station that receives traps (the system alerts generated).

If no NMS is defined, then no traps are generated.

26.2 Configuring SNMP

Click **Advanced Settings** and **SNMP** to display the screen as shown next.

Figure 119 SNMP

SNMP					
SNMP	☐ Enable ☒ Disable				
Port	SNMP Port: 161 (161 or 16100 ~ 16199) Trap Port: 162 (162 or 16200 ~ 16299)				
Configuration	No	Community Name	NMS Address	Privileges	Status
	1	public	ANY	Read	Valid
	2	private	ANY	Write	Valid
	3		ANY	Read	Invalid
	4		ANY	Read	Invalid
	5		ANY	Read	Invalid
Apply					

The following table describes the labels in this screen.

Table 59 SNMP

LABEL	DESCRIPTION
SNMP	Select Enable to activate SNMP support. Select Disable to de-activate the SNMP support.
Port	
SNMP Port	Enter a port number on the VSG for SNMP management. The default is 161 . Otherwise enter a port number between 16100 and 16199.
Trap Port	Enter a port number on the VSG for sending SNMP traps. The default is 162 . Otherwise enter a port number between 16200 and 16299.
Configuration	
No	This read-only field displays the index number of the entry.
Community Name	Enter the community string (or the password) of the management station.
NMS Address	Enter the IP address of the management station.
Privileges	Select a privilege level from the drop-down list box. Options are Read , Write , Trap Recipient and All .
Status	Select Valid to activate the selected SNMP configuration entry. Select Invalid to disable the selected SNMP configuration entry.
Apply	Click Apply to save the changes.

CHAPTER 27

Miscellanea

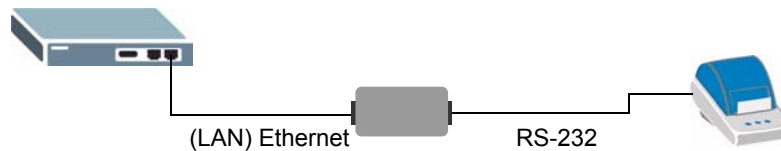
This chapter shows you how to configure TCP/IP-to-RS-232 convertor settings on the VSG to extend the connection to the account statement printer.

27.1 Overview

In cases where you need to install the VSG and the statement print in different locations and the RS-232 console cable is not long enough for the connection, you can use a TCP/IP-RS-232 convertor to make an extension. The TCP/IP-RS-232 convertor is a hardware device installed between the VSG and the statement printer on the LAN.

The following figure shows a network example where the VSG connects to the statement printer via the TCP/IP-RS-232 convertor.

Figure 120 Network Example Using TCP/IP-RS232 Convertor



27.2 TCP/IP-RS-232 Converter Setup

Configure the TCP/IP-RS-232 converter settings in the **Miscellanea** screen. Click **Advanced Setup** and **Miscellanea** to display the screen as shown.

Figure 121 Advanced Setup: Miscellanea

Miscellanea	
TCP/IP-RS-232 Converter: Disable ▾	
This function enables administrator to extend the distance between SP and Device with a TCP/IP-RS-232 Converter.	
Socket Port :	1001 (1001~1005)
Statement Printer Device	SP-200 ▾
Converter IP Address:	1.
	2.
	3.
	4.
	5.
	6.
	7.
	8.
	9.
	10.
Apply	

The following table describes the labels in this screen.

Table 60 Miscellanea

LABEL	DESCRIPTION
TCP/IP-RS-232 Converter	Select Enable to activate this feature. Select Disable to deactivate this feature.
Socket Port	Enter the number of the service port for the IP-serial conversion service.
Statement Printer Device	Select the model name of your statement printer.
Converter IP Address	Specify the IP address of the converter. Enter the IP address in dotted decimal notation. For example, 10.59.1.100.
Apply	Click Apply to save the changes.

CHAPTER 28

System Status

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

28.1 System Status Overview

Use the **System Status** screen to view current device status such as the WAN/LAN settings, current online user list, session lists, etc.

28.2 System Information

Click **System Status** and **System** to display the screen as shown next. The **System** screen automatically updates every 5 seconds.

Figure 122 System Status: System

System		
		refresh↻
System Status	Host Name:	
	Domain Name:	
	Bootrom Version:	1.00
	Firmware Version:	1.00.02
	Concurrent Users Limitation:	1024
	WAN MAC Address:	00:13:49:7D:39:A1
	LAN MAC Address:	00:13:49:7D:39:A0
WAN IP Settings	WAN Port Mode:	Get automatically from a DHCP server
	IP Address:	172.23.37.16
	Subnet Mask:	255.255.255.0
	Default IP Gateway:	172.23.37.254
DNS	Primary DNS Server:	172.23.5.2
	Secondary DNS Server:	172.23.5.1
DHCP	DHCP Status	Server
	Start IP Address (Private):	10.59.1.2
	End IP Address (Private):	10.59.1.254
	Lease Time (Private):	1440
E-Mail	Server IP Address:	
	Country	00
	State	Local State
	Local City	Local City

SSL Certificate	State	Local State
	Local City	Local City
	Organization	Local Group
	Organization Unit	Local Host
	Common Name	1.1.1.1
	Email Address	mail@1.1.1.1

The following table describes the fields in this screen.

Table 61 System Status: System

FIELD	DESCRIPTION
System Status	
Host Name	This field displays the description name of the VSG for identification purposes.
Domain Name	This field displays the domain name of the VSG.
Bootrom Version	This field displays the version of the bootrom.
Firmware Version	This field displays the version of the firmware on the VSG.
Concurrent User Limitation	This field displays the maximum number of users that can log in simultaneously for Internet access.
WAN MAC Address	This field displays the MAC address of the VSG on the WAN.
LAN MAC Address	This field displays the MAC address of the VSG on the LAN.
WAN IP Settings	
WAN Port Mode	This field displays the DHCP mode of the WAN port.
IP Address	This field displays the IP address of the WAN port on the VSG.
Subnet Mask	This field displays the subnet mask of the WAN port on the VSG.
Default IP Gateway	This field displays the IP address of the default gateway of the WAN port on the VSG.
DNS	
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
DHCP	
DHCP Status	This field displays the DHCP mode (Server , Relay or Disable) on the LAN.
Server IP Address	This field is visible when the DHCP Status is Server or Relay . This field displays the IP address of the DHCP server on the network.
Start IP Address (Private)	This field is visible when the DHCP Status is Server or Relay . This field displays the first of the continuous addresses in the IP address pool.

Table 61 System Status: System (continued)

FIELD	DESCRIPTION
End IP Address (Private)	This field is visible when the DHCP Status is Server . This field displays the end of the continuous addresses in the IP address pool.
Lease Time (Private)	This field is visible when the DHCP Status is Server . This field displays the time (in minutes) a DHCP client is allowed to use an assigned IP address.
E-mail	
Server IP Address	The field displays the IP address or the domain name of the e-mail server.
SSL Certificate	
Country	This field displays the two-letter abbreviation of your country.
State	This field displays the name of the state or province where your organization is located.
Local City	This field displays the name of the city your organization is located.
Organization	This field displays the name of your organization.
Origination Unit	This field displays additional information about your organization.
Common Name	This field displays the fully qualified domain name of your web server.
Email Address	This field displays your e-mail address.

28.3 Current User List

The **Current User List** screen displays a list of subscribers currently logged on to the VSG for Internet access.

Click **System Status** and **Current User List** to display the screen as shown. Click a column heading to sort the entries if applicable.

Note: The fields displayed in the **Current User List** screen vary depending on the subscriber account type or authentication method.

Figure 123 System Status: Current User List

Current User List									
refresh 									Print List
No.	Type	Username	Billing Profile	Login Time	Expiration	IP Address	MAC Address	Disconnect	
1	Static	Cindy	1	Profile 1	2006/06/21 09:31:08	2006/06/22 09:31:08	10.59.1.2	00:0F:FE:32:B4:12	☐
									Disconnect Disconnect All
 1 Page  First  Previous Next  End									

The following table describes the labels in this screen.

Table 62 System Status: Current User List

LABEL	DESCRIPTION
Refresh	Click Refresh to update this screen.
Print List	Click Print List to print the current user list to a printer. No preview option is available.
No	This field displays the index number.
Type	This field displays the type of subscriber accounts. This field displays Static for a static subscriber account. This field displays Dynamic for a dynamic subscriber account. This field displays Location for a subscriber accessing using port-location mapping. This field displays Agreement for a subscriber accessing through the agreement screen. This field displays Non_Auth for a subscriber accessing without authentication.
Username	This field displays the username of a subscriber account.
Billing Profile	This field displays the number of concurrent access allowed and the name of the billing profile that the subscriber uses.
Login Time	This field displays the time the subscriber logs in.
Expiration	This field displays the time this account expires. This field displays N/A when total bandwidth limitation is enforced on this account. Refer to Section 9.1.4.2 on page 82 and Appendix D on page 242 for more information.
IP Address	This field displays the IP address of the subscriber's computer.
MAC Address	This field displays the MAC address of the computer that is logged in using this account.
Disconnect	Select this check box and click Disconnect to log out the selected subscriber. Click Disconnect All to log out all subscribers.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.

28.4 DHCP Client

The DHCP client table shows current DHCP client information of all network clients using the DHCP server on the VSG.

Click **System Status** and **DHCP** to display the screen as shown. The **DHCP Clients** screen automatically updates every 5 seconds.

Figure 124 System Status: DHCP Clients

DHCP Clients (Private IP)		
No.	MAC Address	IP Address
1	00:0F:FE:32:B4:12	10.59.1.2

The following table describes the labels in this screen.

Table 63 System Status: DHCP Clients

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

28.5 Session List

To display a list session information, click **System Status** and **Session List**. The **Session List** screen displays up to 2048 entries. When all rows are used, the entries wrap around and the old entries are erased. This screen automatically updates every 5 seconds.

Figure 125 System Status: Session List

Session List							
List of sessions of Network events, and records or the newest 16384 incoming and outgoing packet information, including source IP address, destination IP address, and port number.							
No.	TCP/UDP	IP Client	Port Client	Port Fake	IP Remote	Port Remote	Idle
1	TCP	10.59.1.2	1353	42005	203.160.232.7	80	25
2	TCP	10.59.1.2	1354	42006	203.160.232.7	80	25


 Page
 




The following table describes the labels in this screen.

Table 64 System Status: Session List

LABEL	DESCRIPTION
No	This field displays the index number of an entry.
TCP/UDP	This field displays the type of traffic (TCP or UDP).
IP Client	This field displays the IP address of the client computer.
Port Client	This field displays the port number through which the client computer transmits the traffic.
Port Fake	This field displays the virtual port number for a session.
Port Remote	This field displays the port number of a remote device the client computer accesses.

Table 64 System Status: Session List (continued)

LABEL	DESCRIPTION
Idle	This field displays the number of seconds of inactivity for a session.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.
Next	Click Next to go to the next page.
End	Click End to go to the last page.

28.6 NAT Pool Table

The VSG provides a NAT address pool feature for use with VPN. It allows subscribers to connect to remote VPN servers that allow only one connection per source IP address.

Click **System Status** and **NAT Pool Table** to open the screen shown next. This screen displays the LAN and WAN IP addresses that are currently being used as well the VPN types.

Figure 126 System Status: NAT Pool Table

NAT Pool Table				
NAT Pool information. Source IP address, Source MAC address and Translated IP address				
No.	Source IP Address	Source MAC Address	Translated IP Address	VPN Type
1	192.168.100.1	0E-90-80-90-EE-12	211.21.185.240	PPTP
2	192.168.100.2	0E-90-80-90-EE-13	211.21.185.241	PPTP
3	192.168.100.3	0E-90-80-90-EE-14	211.21.185.242	PPTP

The following table describes the labels in this screen.

Table 65 System Status: NAT Tool Table

LABEL	DESCRIPTION
No	This field displays the index number of an entry.
Source IP Address	This field displays the IP address of the subscriber device on the LAN that is using the VPN.
Source MAC Address	This field displays the MAC address of the subscriber device on the LAN that is using the VPN.
Translated IP Address	This field displays the WAN IP address of the VSG to which the LAN IP address of the subscriber using the VPN was translated.
VPN Type	This field displays the type of VPN connection that is being used (IPSec or PPTP).

28.7 LAN Device Status

The **LAN Devices Status** screen displays the status of LAN devices configured in the **LAN Devices** screen (refer to [Chapter 21 on page 160](#)).

Click **System Status** and **LAN Devices Status** to display the screen as shown next. This screen automatically updates every minute.

Figure 127 System Status: LAN Device Status

LAN Devices Status							
We detect below listed devices to check if alive every 1 min . You can manage below listed devices by clicking device name to access its Web-based UI.							
No.	Device Name	Status	Virtual Port (60001~60300)	Device IP Address	Device Server Port	Device MAC Address	Application
1	B-3000	OK	60001	10.59.1.30	80	00:A0:C5:00:00:05	TCP
2	P662HW	OK	60002	10.59.1.62	80	00:A0:C5:01:23:45	TCP

The following table describes the labels in this screen.

Table 66 System Status: LAN Device Status

LABEL	DESCRIPTION
No	This field displays the index number.
Device Name	This field displays the name of the LAN device. Click the device name to access web-based management interface of the LAN device if the Status field is OK . For more information on accessing a LAN device, refer to Section 28.7.1 on page 190 .
Status	This field displays the current status of the LAN device. It displays OK when the LAN device is turned on and working properly. Otherwise it displays Fail .
Virtual Port	This field displays the virtual port number.
Device IP Address	This field displays the IP address of the LAN device.
Device Server Port	This field displays the server port number of the LAN device.
Device MAC Address	This field displays the MAC address of the LAN device.
Application	This field displays the type of application packet that is forwarded to the LAN device.

28.7.1 Accessing the LAN Device

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

- The LAN device has a web-based management interface and it is enabled.
- You have set up the virtual port mapping to the LAN device server port in the **LAN Device Management** screen.
- The LAN device status is **OK** in the **LAN Device Status** screen.

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

- To access the LAN device through the web configurator, open the **LAN Device Status** screen and click the device name. A new Internet browser should display showing the login screen of the LAN device management interface.

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

28.8 Billing Log

Click **System Status** and **Billing Log** in the navigation panel to display the screen as shown. Refer to [Section 28.8.1 on page 192](#) for information on backing up the billing logs to a computer.

Figure 128 System Status: Billing Log

Billing Log								
Refresh		Export to Txt File Clear Log						
No.	Username/Location	Billing Profile	Log Time	Usage Time	Bill	Service Type	Charge from	Status
1	2222zzrr	Profile 1	2006/06/15 17:56:29	1 day(s)	10.00	Private	Dynamic	In-Use
2	222222tt	Profile 1	2006/06/21 09:43:07	1 day(s)	10.00	Private	Dynamic	Expired
3	2222zzrr	Profile 1	2006/06/21 09:42:29	1 day(s)	10.00	Private	Dynamic	Finished
4	Cindy	Profile 1	2006/06/21 09:31:08	1 day(s)	10.00	Private	Static	Finished
1 Page First Previous Next End 								

The following table describes the labels in this screen.

Table 67 System Status: Billing Log

LABEL	DESCRIPTION
Refresh	Click Refresh to update the screen.
Export to Txt File	Click Export to File to back the billing logs. Refer to Section 28.8.1 on page 192 for instructions.
Clear Log	Click Clear Log to clear all log entries.
No	This field displays the index number of the entry.
Username/Location	This field displays the user name or the room number (for Dynamic , PMS or Static accounts only).
Billing Profile	This field displays the name of the billing profile an account is using.
Log Time	This field displays the time the subscriber logged in using the account.
Usage Time	This field displays the time period allocated for an account.
Bill	This field displays the amount of money charged for the time unit(s) purchased.
Charge from	This field displays the type of the account billing (Dynamic , PMS or Static).
Status	This field displays the billing status or account status.
Go .. page	Select a page number from the drop-down list box to display the selected page.
First	Click First to go to the first page.
Previous	Click Previous to return to the previous page.

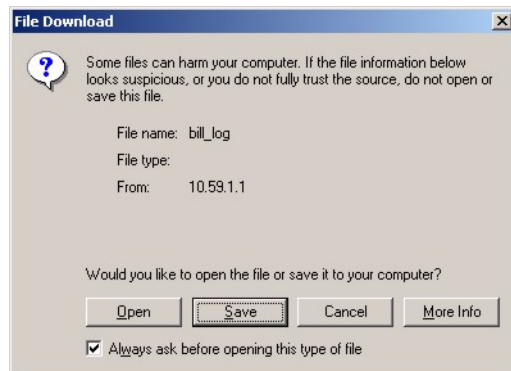
Table 67 System Status: Billing Log (continued)

LABEL	DESCRIPTION
Next	Click Next to go to the next page.
End	Click End to go to the last page.

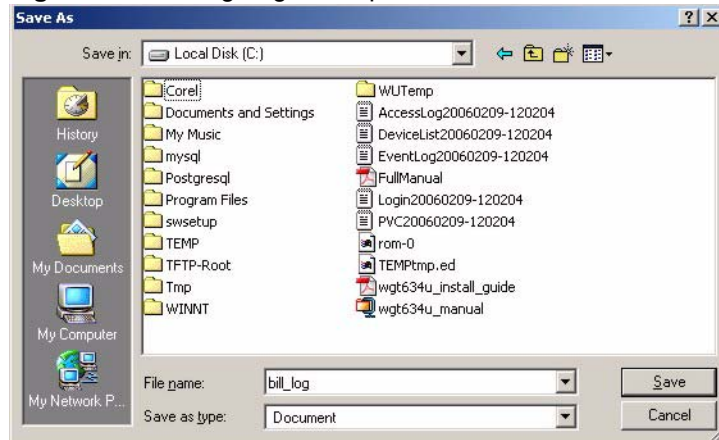
28.8.1 Billing Logs Backup

Follow the steps below to back up billing logs to a computer.

- 1 In the **Billing Log** screen, click the **Export to Txt File** link. A **File Download** screen displays.

Figure 129 Billing Log Backup: File Download

- 2 Select **Save this file to disk** and click **OK**. A **Save As** window displays.

Figure 130 Billing Log Backup: Save As

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

To view the billing logs, open the log file using any text editor. The following figure shows an example.

Figure 131 Billing Log Backup: Example File Content

[Billing Log Profile]							
NO.	Username/Location	BillingProfile	Log Time	Usage Time	Bill	Charge from	Status
1	222222tt	Profile 1	2006/06/21 09:43:07	1 day(s)	10.00	Dynamic	Un-used
2	2222zzrr	Profile 1	2006/06/21 09:42:29	1 day(s)	10.00	Dynamic	Un-used
3	2222zzrr	Profile 1	2006/06/15 17:56:29	1 day(s)	10.00	Dynamic	In-Use
4	Cindy	Profile 1	2006/06/21 09:31:08	1 day(s)	10.00	Static	In-Use

28.9 PMS Transaction

This screen is applicable when account billing is done using a PMS.

To display transaction messages between the VSG and PMS, click **System Status** and **PMS Transaction**.

Figure 132 System Status: PMS Transaction Log

PMS Transaction Log	
	Clear log
(HST<-MDS) LS DA040726 T1151913	

28.10 Static Route Table

You can view the list of static routes configured in the **Static Route Table** screen.

Click **System Status** and **Static Route Table** to display the screen.

Figure 133 System Status: Static Route Table

Static Route Table					
No.	Destination IP Address	Destination Subnet Mask	Gateway IP Address	Hop Count	Interface
1	192.168.2.1	255.255.255.0	192.168.1.254	1	WAN

The following table describes the labels in this screen.

Table 68 System Status: Static Route Table

LABEL	DESCRIPTION
Static Route Table	This table displays the static routes configured.
No.	This field displays the index number.
Destination IP Address	This field displays the IP address of the final destination.
Destination Subnet Mask	This field displays the subnet mask of the final destination.
Gateway IP Address	This field displays the IP address of the gateway device.
Hop Count	This field displays the “cost” of this static route.
Interface	This field displays the name of the interface this static route is applied.

CHAPTER 29

Configuration

This chapter shows you how to back up, restore or reset the configuration on the VSG.

29.1 Configuration Overview

The configuration file contains the factory default settings in the menus such as password, DHCP Setup, TCP/IP Setup, etc. Once you have customized the settings of the VSG, they can be saved back to your computer under a filename of your choosing.

There is not a specific file extension or filename conventions that you need to follow. Therefore, you can specify any name or file extension the configuration files. It is recommended that you to use the “.rom” file extension for the configuration file for management purposes.

You can use the **Configuration** screen in the web configurator to back up and restore configuration or reset the device to the factory defaults.

You can back up and restore the configuration file either through the web configurator or using an external TFTP server.

Note: Do NOT interrupt the file transfer process as this may permanently damage your device.

29.2 Configuration Backup

Backup is highly recommended once your VSG is functioning properly.

- 1 Click **System Tools** and **Configuration**. A screen displays as shown next.

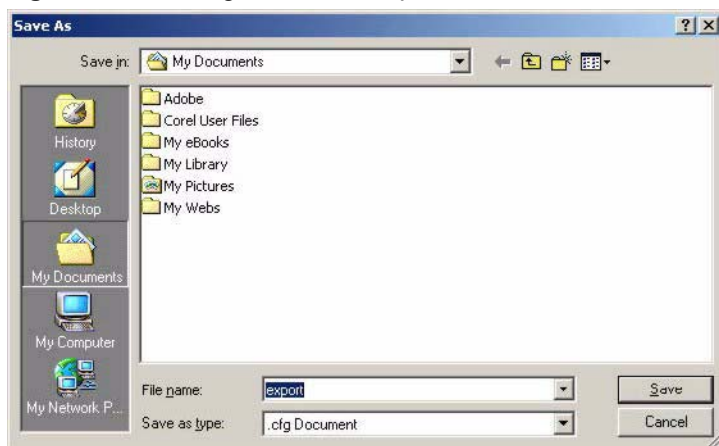
Figure 134 Configuration: Backup

Configuration	
This feature can import your saved settings to this device or export the stored settings from this device to your PC.	
Backup	
Click Backup to save current system configuration from this device to your computer or to the remote TFTP server.	
TFTP Server IP Address:	Text File Name: Apply
Restore	
To restore your stored system configuration to this device	
File Path:	Browse... Apply
TFTP Server IP Address:	Text File Name: Apply
Reset the system back to factory defaults	
☐ Keep subscriber profile	
☐ Keep port-location mapping profile Apply	

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

Figure 135 Configuration Backup: File Download

3 Select **Save this file to disk** and click **OK**. A **Save As** window displays.

Figure 136 Configuration Backup: Save As

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

29.2.1 Configuration Backup Using TFTP

- 1 Click **System Tools** and **Configuration**. A screen displays as shown next.
- 2 In the **Backup** section, enter the IP address of the TFTP server in dotted decimal notation in the **TFTP Server IP Address** field.
- 3 Specify a file name for the configuration backup in the **Text File Name** field.

Figure 137 Configuration: Backup using TFTP

Configuration	
This feature can import your saved settings to this device or export the stored settings from this device to your PC.	
Backup	
Click Backup to save current system configuration from this device to your computer or to the remote TFTP server.	
TFTP Server IP Address:	Text File Name:
Apply	
Restore	
To restore your stored system configuration to this device	
File Path:	Browse...
Apply	
TFTP Server IP Address:	Text File Name:
Apply	
Reset the system back to factory defaults	
☐ Keep subscriber profile	
☐ Keep port-location mapping profile	
Apply	

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

Figure 138 Configuration Backup: TFTP: Successful

29.3 Restore Configuration

This section shows you how to restore a previously saved configuration.

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

- 1 Click **System Tools** and **Configuration**. A screen displays as shown next.

Figure 139 Configuration: RestoreA screenshot of the "Configuration" screen. The screen has a blue header with the word "Configuration". Below the header, there is a section titled "Backup" with a description: "This feature can import your saved settings to this device or export the stored settings from this device to your PC." Below this is a section titled "Restore" with a description: "Click Backup to save current system configuration from this device to your computer or to the remote TFTP server." Below this is a section titled "Reset the system back to factory defaults" with two checkboxes: "Keep subscriber profile" and "Keep port-location mapping profile". The "File Path" field in the "Restore" section is highlighted with a red rectangle. The "File Path" field is a text input field with a "Browse..." button next to it. There are "Apply" buttons for the "Backup", "Restore", and "Reset" sections. The "File Path" field is a text input field with a "Browse..." button next to it.

- 2 In the **Restore** section, specify the location and filename of a configuration file in the **File Path** field or click **Browse**.
- 3 Click **Apply** to start the configuration restore process. The VSG automatically restarts after the restoration process is complete.

29.3.1 Restore Configuration Using TFTP

This section shows you how to restore a previously saved configuration.

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

- 1 Click **System Tools and Configuration**. A screen displays as shown next.

Figure 140 Configuration: Restore: TFTP

Configuration	
This feature can import your saved settings to this device or export the stored settings from this device to your PC.	
Backup	
Click Backup to save current system configuration from this device to your computer or to the remote TFTP server.	
TFTP Server IP Address:	Text File Name:
Apply	
Restore	
To restore your stored system configuration to this device	
File Path:	Browse...
	Apply
TFTP Server IP Address:	Text File Name:
Apply	
Reset the system back to factory defaults	
☐ Keep subscriber profile	
☐ Keep port-location mapping profile	
Apply	

- 2 In the **Restore** section, Enter the IP address of the TFTP server in dotted decimal notation in the **TFTP Server IP Address** field.
- 3 Specify a file name for the configuration backup in the **Text File Name** field.
- 4 Click **Apply** to start the configuration restore process. The VSG automatically restarts after the restoration process is complete.

29.4 Reset to the Factory Defaults

This section shows you how to reset the device configuration back to the factory defaults. If you have forgotten the administrator login password or username, you need to use the **RESET** button.

Note: All your custom configuration will be erased once you reset the VSG. You may choose to keep the subscriber account information and the port-location mapping settings.

Follow the steps below to reset the VSG back to the factory default settings.

- 1 Click **System Tools, Configuration** to display the screen as shown next.

Figure 141 Configuration: Reset

Configuration	
This feature can import your saved settings to this device or export the stored settings from this device to your PC.	
Backup	
Click Backup to save current system configuration from this device to your computer or to the remote TFTP server.	
TFTP Server IP Address:	Text File Name: Apply
Restore	
To restore your stored system configuration to this device	
File Path:	Browse... Apply
TFTP Server IP Address:	Text File Name: Apply
Reset the system back to factory defaults	
☐ Keep subscriber profile	
☐ Keep port-location mapping profile Apply	

- 2 Scroll down to the **Reset the system back to factory defaults** section at the bottom of the screen.
- 3 If you want to keep all subscriber account information, select **Keep subscriber profile** and/or **Keep port-location mapping profile**.
- 4 Click **Apply**.
- 5 Wait for the VSG to finish restarting before accessing the VSG again.

CHAPTER 30

Firmware

This chapter shows you how to upgrade firmware on the VSG using the web configurator.

Note: o NOT interrupt the file upload process as this may PERMANENTLY damage the device.

30.1 Firmware Overview

In the web configurator you can manually upgrade the firmware on the VSG or have it done automatically by setting up a schedule.

To manually upgrade the firmware, you have to down the latest firmware from www.zyxel.com. With scheduled firmware upgrade, the VSG automatically checks for, downloads and upgrades the latest firmware every time interval specified.

The following figure shows the links in the **Firmware** screen.

Figure 142 Firmware: Links

[Manual Firmware Upgrade](#) | [Scheduled Firmware Upgrade](#)

30.2 Manual Firmware Upgrade

Follow the steps below to upgrade the firmware manually.

- 1 Download the latest firmware from www.zyxel.com to your computer. Unzip the file if it is zipped.
- 2 Access the web configurator. Refer to the section on accessing the web configurator for instructions.
- 3 Click **System Tools**, **Firmware** and the **Manual Firmware Upgrade** link to display the screen as shown.

Figure 143 Firmware: Manual Upgrade

Manual Firmware Upgrade

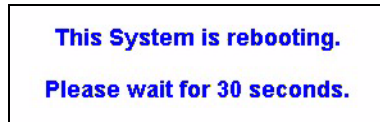
To upgrade the firmware, click **Browse** to locate the firmware file and click **Apply**, or use remote TFTP server.

Local PC File Path

TFTP Server IP Address: Binary File Name:

- 4 Specify the firmware file name in the **Local PC File Path** field (or click **Browse** to locate it).
- 5 Click **Apply** to start the file transfer process.
- 6 When the file transfer is completed successfully, the following message displays and the VSG automatically restarts to complete the firmware upgrade process.

Figure 144 Web Configurator: Firmware Upgrade Successful



- 7 After the VSG finishes restarting, access the web configurator again. Check the firmware version number in the **System Status** screen.

30.2.1 Manual Firmware Upgrade via a TFTP Server

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

- 1 Download the latest firmware from www.zyxel.com and store it in a TFTP server. Unzip the file if it is zipped.
- 2 Run a TFTP server program and specify the location of the firmware file and the communication mode. Refer to the documentation that comes with your TFTP server program for instructions.
- 3 Access the web configurator. Refer to the section on accessing the web configurator for instructions.
- 4 Click **System Tools**, **Firmware** and the **Manual Firmware Upgrade** link to display the screen as shown.

Figure 145 Firmware: Manual Upgrade Using TFTP

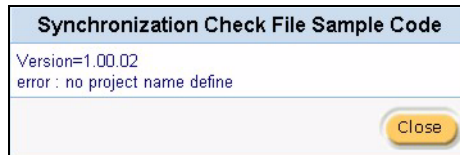
Manual Firmware Upgrade	
To upgrade the firmware, click Browse to locate the firmware file and click Apply . or use remote TFTP server.	
Local PC File Path	Browse... Apply
TFTP Server IP Address:	Apply
Binary File Name:	Apply

- 5 Specify the IP address of the TFTP server in the **TFTP Server IP Address** field.
- 6 Specify the name of the firmware file in the **Binary File Name** field.
- 7 Click **Apply** to start the file transfer process.
- 8 When the file transfer is completed successfully, the following message displays and the VSG automatically restarts to complete the firmware upgrade process.
- 9 After the VSG finishes restarting, access the web configurator again. Check the firmware version number in the **System Status** screen.

30.3 Scheduled Firmware Upgrade

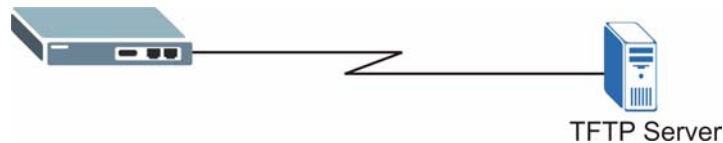
You can set the VSG to automatically check and download a new firmware from a TFTP server. This allows you to automate the firmware upgrade process if you have more than one VSG on your network. A synchronization file contains information on firmware version and filename. A sample synchronization file is shown next.

Figure 146 Scheduled Firmware Upgrade: Synchronization File Example



You have to manually download the latest firmware from www.zyxel.com to the TFTP server and update the synchronization file.

Figure 147 Scheduled Firmware Upgrade Example



The following describes the automatic firmware upgrade process.

- 1 The VSG checks the synchronization file on the TFTP server for the firmware version number.
- 2 If the synchronization file has the latest firmware version number, VSG retrieves the latest firmware file as specified in the synchronization file.
- 3 VSG upgrades the firmware and restarts.

Note: During the firmware upgrade process, the VSG disconnects all subscriber Internet access. Subscribers need to log in again.

Click **System Tools**, **Firmware** and click the **Scheduled Firmware Upgrade** link to display the screen as shown next.

Figure 148 Firmware: Scheduled Upgrade

The following table describes the labels in this screen.

Table 69 Firmware: Scheduled Upgrade

LABEL	DESCRIPTION
Disable	Select Disable to de-activate scheduled firmware upgrade.
Enable	Select Enable to activate scheduled firmware upgrade. Then set the following fields.
TFTP Server IP	Enter the IP address of the TFTP server where the firmware resides.
Synchronization Check File	A Synchronization Check file is a file containing the latest firmware filename and version number on the TFTP server. Click View Sample File to display an example. Enter the name of the check file.
Frequency	Set how often (Weekly, Daily or Hourly) you want to have the VSG check for new firmware and upgrade to new firmware if available (default Weekly). Then select the day (applies only when you select Weekly), the hour (applies when you select Daily or Hourly) and the minute that you want the VSG to do the check and upload.
Apply	Click Apply to save the changes.

CHAPTER 31

SSL Certificate

This chapter shows you how to set up Secure Socket Layer (SSL) certificates on the VSG.

31.1 SSL Certificate Overview

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

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

31.1.1 Certificate

A digital certificate (also referred to as a certificate) contains the key owner's name and public key, the name of the issuing certification authority, the certification authority's digital signature and a certificate validity time limit and other optional information fields.

31.1.2 Certificate Authorities

A Certification Authority (CA) issues digital certificates and guarantees the identity of the certificate owner. When someone requests a certificate from a CA, the CA requires proof of identity. There are both commercial certificate authorities like CyberTrust and VeriSign, as well as government certificate authorities.

31.2 Downloading SSL Certificate to the VSG

After you apply for and receive a certificate from a certificate authority, import the certificate and the private key to the VSG.

Click **System Tools** and **SSL Certificate** in the navigation panel to display the screen as shown next.

Figure 149 SSL Certificate

The following table describes the labels in this screen.

Table 70 SSL Certificate

LABEL	DESCRIPTION
Password	Enter the secret password you used when applying for the certificate. Note: This password must be the same as the one you entered at the CA's site when creating a certificate.
Certificate File	Specify the certificate sent to you by a CA.
Private Key File	Specify the file that holds the private key.
Apply	Click Apply to start the file transfer process.

31.3 Activating SSL Security

Follow the steps below to activate the SSL security in the VSG.

- 1 Click **System Settings, Servers** in the navigation panel and select the **SSL Security** check box in the **Web Server** field.

Figure 150 System Settings: Server Configuration: Enable SSL Security

- 2 Click **Apply** to save the changes and restart the VSG when prompted.
- 3 Enable SSL security in the **Authentication** screen. Click **System Setting** and **Authentication** in the navigation panel
- 4 A screen displays as shown. Select **Enable** in the **SSL Login Security** field

Figure 151 System Settings: Authentication: Activate SSL Login

	Vendor Specific Attribute	Vendor Code 0 ☐ Send VSA together with Authentication Request
Idle Time Out	5	Min(s) (1 - 1440)
SSL Login Security	☒ Disable ☐ Enable	
Smart Client Support	☐ WISPr Smart Client Login Mode ☒ Directly Reply ☐ Proxy Reply with "Redirect Login Page" URL ☐ Proxy Reply with Specific URL 	
Apply		

5 Click **Apply** to save the changes and restart the VSG when prompted.

31.4 Installing SSL Certificate on a Computer

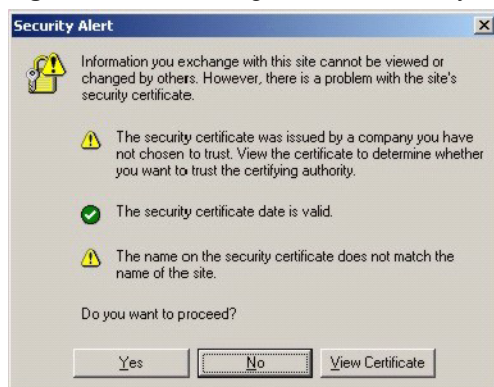
After you enable and activate the SSL login security on the VSG, you can access the VSG through a secure connection.

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

- 1 Access the VSG. A **Security Alert** window displays. Click **OK** to continue and close the window.

Figure 152 Installing the SSL Security Certificate: First Security Alert

- 2 A second **Security Alert** window displays.

Figure 153 Installing the SSL Security Certificate: Second Security Alert

- 3** Click **View Certificate** to display the **Certificate** window as shown. Notice the warning about the untrusted certificate.

Figure 154 Installing the SSL Security Certificate: View Certificate

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

Figure 155 Installing the SSL Security Certificate: Certificate Import Wizard

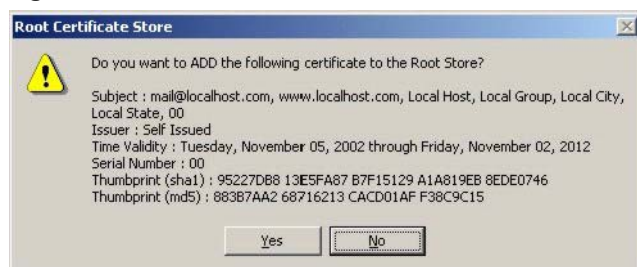
5 Accept the default or specify the location to store the certificate. Click **Next**.

Figure 156 Certificate Import Wizard: Location

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

Figure 157 Certificate Import Wizard: Finish

7 A **Root Certificate Store** window displays as shown. Click **Yes** to store the certificate to the computer.

Figure 158 Root Certificate Store

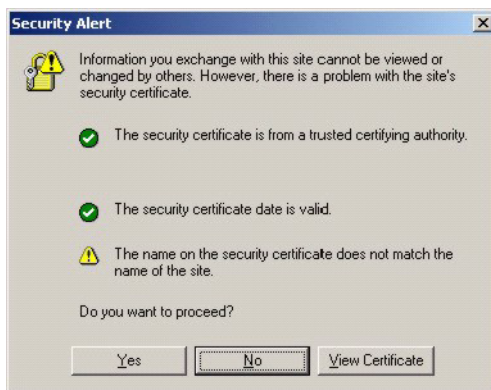
8 When the certificate is saved successfully, a **Certificate Import Wizard** window displays. Click **OK**.

Figure 159 Certificate Import Wizard

9 A **Certificate** window displays the detailed information. Notice that the certificate is now trusted.

Figure 160 Certificate: Detailed Information

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

Figure 161 Security Alert: Trusted

Note: Once you are logged in with SSL security, the URL starts with “https://” instead of “http://”.

CHAPTER 32

Using The SMT

This chapter introduces the SMT (System Management Terminal) and shows you how to use the SMT to configure the VSG.

32.1 About the SMT

The System Management Terminal (SMT) is a menu – driven interface that you use to configure the VSG. Access the SMT using the console port.

Note: You can connect the CONSOLE port on the VSG directly to a computer serial port or to a statement printer (also known as an account generator printer).

Make sure the CONSOLE port is set to the correct mode. Refer to [Chapter 3 on page 42](#) on system settings using the web configurator.

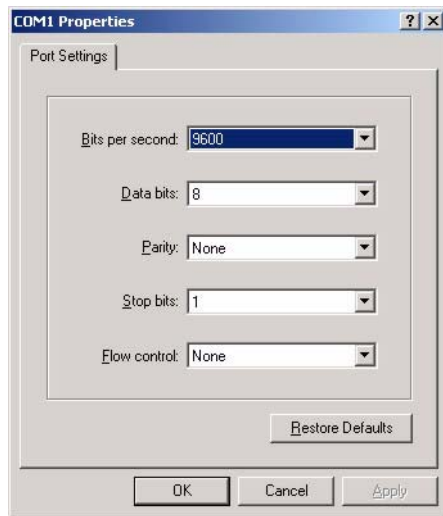
Use the SMT to set general system settings, configure the LAN and WAN settings, change the administrator login password, upgrade firmware or reset the device to the factory defaults.

For advanced configuration, use the web configurator. Refer to the corresponding web configurator chapters for background information.

32.1.1 Establishing a Console Port Connection

After the VSG is directly connected to a computer using the console port, turn on the computer and run a terminal emulation program (for example, Hyper Terminal in Windows) and configure its communication parameters as follows:

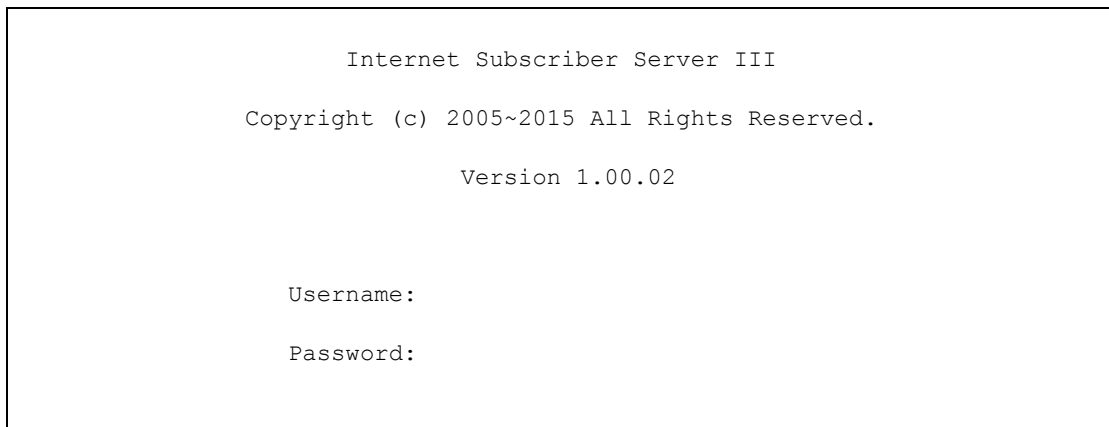
- 9600 bits per second.
- Parity none
- 8 data bits
- 1 stop bit
- Flow-control none.

Figure 162 HyperTerminal Communication Parameter Settings Example

32.2 SMT Login Screen

Press [ENTER] to display the login screen. For your first login, enter the default administrator user name “admin” and default password “1234” and then press [ENTER].

Note: The user name and password are case sensitive.

Figure 163 SMT: Login Screen

Note: The VSG automatically logs you out after five minutes of inactivity. Simply log back into the VSG if this happens.

32.3 The SMT Main Menu Summary

The SMT main menu is shown next.

Figure 164 SMT: Main Menu

```

Main Menu

1)System Configuration
2)Wan Configuration
3)Lan Configuration
4)System Status
5)Utilities
6)Restart
7)Logout
8)Factory Defaults

Enter selection:

Enter a numeric between 1 and 8.

```

The following table describes the menu choices in this screen.

Table 71 SMT: Main Menu

NUMBER	MENU TITLE	FUNCTION
1	System Configuration	Use this menu to set up general system setup.
2	WAN Configuration	Use this menu to configure the WAN port.
3	LAN Configuration	Use this menu to configure the LAN port.
4	System Status	Use this menu to view the current configuration of the VSG.
5	Utilities	Use this menu to perform firmware upgrades and change the login password.
6	Restart	Use this menu to restart your VSG.
7	Logout	Use this menu to log out of the SMT.
8	Factory Defaults	Use this menu to reset the VSG back to the factory default settings.

32.4 Navigating the SMT Interface

Familiarize yourself with the SMT operations before you attempt to modify the configuration.

32.4.1 The Navigation Keys

The following table describes the keystrokes that you use in the SMT screens.

Table 72 SMT: Control Key Descriptions

KEY	DESCRIPTION
[ENTER]	To go to the selected menu.
[ESC]	In any SMT screen. press [ESC] and enter Y (yes) to discard any changes and return to the main screen.
[TAB]	To move to the next configuration field.
[SPACE]	To toggle between field choices.

32.5 System Configuration

Use the **System Configuration** menu to set general system settings such as the system name, the domain name or change the console port speed.

From the **Main Menu** screen, type 1 and press [ENTER] to display the menu as shown.

Figure 165 SMT: System Configuration

	System Configuration
System Name	:
Domain Name	:
Console Port Speed	:9600
Web Server Port	:80
E-Mail Server Redirect	:

The following table describes the fields in this menu.

Table 73 SMT: System Configuration

FIELD	DESCRIPTION
System Name	Enter a descriptive name (up to 32 characters) for identification purposes.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the VSG may obtain a domain name from a DHCP server. The domain name you entered is given priority over the DHCP server assigned domain name.
Console Port Speed	Enter 1200, 2400, 4800, 9600, 14400, 19200, 38400, 57600, or 115200 to set the console port speed. The default setting is 9600. Note: If you change the console port speed, make sure you also make the same change to the terminal emulator software.

Table 73 SMT: System Configuration (continued)

FIELD	DESCRIPTION
Web Server Port	Specify the port number of the embedded web server on the VSG to access the web configurator. The default port number is 80. Enter a number between 8010 and 8060 to access the web configurator behind a NAT-enabled network. If you enter a number between 8010 and 8060, you need to append the port number to the WAN or LAN port IP address to access the web configurator. For example, if you enter "8010" as the web server port number, then you must enter "http://www.192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address.
E-mail Server Redirect	Enter the IP address or domain name of the e-mail server to which the VSG forwards e-mail. This field should be configured if the e-mail server is behind a firewall or on a NAT-enabled network.
At the "(S)ave and return R)eturn without saving M)odify:" prompt, type S and press [ENTER] to save the changes and return to the previous screen, type R and press [ENTER] to discard all changes and return to the previous screen or type M and press [ENTER] to continue configuring the fields. Restart the device when prompted. Press [ESC] and enter Y to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

32.6 WAN Configuration

From the main menu, type **1** and press [ENTER] to display the **System Configuration** menu. The **WAN Configuration** menu varies depending on the selection in the **WAN Type** field.

Refer to [Chapter 6 on page 60](#) for background information.

32.6.1 WAN Type: Static/Dynamic

You can set the VSG to use a static (fixed) or dynamic IP address.

Figure 166 SMT: WAN Configuration: Static/Dynamic

WAN Configuration	
WAN Type? (D/S/P/T)	:S
IP Address	:192.168.1.1
Subnet Mask	:255.255.255.0
Gateway	:192.168.1.254
Primary DNS Server	:168.95.1.1
Secondary DNS Server	:

The follow table describes the fields in this menu.

Table 74 SMT: WAN Configuration: Static or Dynamic IP Address

FIELD	DESCRIPTION
WAN Type? (D/S/P/T)	Enter D (Dynamic) to set the VSG to dynamically obtain an IP address and other network information (IP address, DNS information etc.) from a DHCP server on the WAN network. This is the default setting. Enter S (Static) to set the VSG to use a static (or fixed) IP address. Then set the following fields.
IP Address	This field is available when you select S in the WAN Mode field. Enter the static IP address assigned to you by your ISP or network administrator.
Subnet Mask	This field is available when you select D in the WAN Mode field. Enter the subnet mask depending on your network needs. The default is 255.255.255.0 . Refer to Appendix H on page 268 if you are implementing subnetting.
Default Gateway	Enter the IP address of the default gateway.
Primary/Secondary DNS IP Address	Enter the IP address of the DNS server(s) in the Primary DNS IP Address and/or Secondary DNS IP Address fields. The default primary DNS server IP address is 168.95.1.1 . You <i>must</i> specify a DNS server if you set the VSG to use a static WAN IP address.
At the "(S)ave and return R)eturn without saving M)odify:" prompt, type S and press [ENTER] to save the changes and return to the previous screen, type R and press [ENTER] to discard all changes and return to the previous screen or type M and press [ENTER] to continue configuring the fields. Restart the device when prompted Press [ESC] and enter Y to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

32.6.2 WAN Type: PPPoE

To activate PPPoE support on the VSG, enter **P** in the **WAN Type** field to display the **WAN Configuration** screen as shown next. Refer to the related web configurator section for background information.

Figure 167 SMT: WAN Configuration: PPPoE

WAN Configuration	
WAN Type? (D/S/P/T)	:P
Username	:
Password	:
Connect Setting? (C/K)	:C
Max idle Time(Min)	:10
Optional Setting	
Service name	:
PPP MTU Setting	:1492
TCP MSS setting	:1452

The following table describes the PPPoE related fields in this menu.

Table 75 SMT: WAN Configuration: PPPoE

FIELD	DESCRIPTION
WAN Type? (D/S/P/T)	Enter P to enable PPPoE support.
Username	Enter the login user name assigned to you by your ISP.
Password	Enter the password associated with the user name above.
Connect Setting? (C/K)	Enter C (Connect on demand) when you don't want the connection up all the time and specify an idle time-out in the Max. Idle Timeout Setting field. This is the default selection. Enter K (Keep alive) when you want your connection up all the time and specify the redial time in the Redial Period field to set how long the VSG waits before trying to bring up the connection automatically if it is disconnected.
Redial Period (Sec)	The field is only visible when you select K in the Connect Setting field. Type the time in seconds that elapses before the VSG automatically attempts to reconnect to the PPPoE server. The default is 30 seconds.
Max Idle Time (Min)	This field is only visible when you select C in the Connect Setting field. Type the time in minutes that elapses before the VSG automatically disconnects from the PPPoE server. The default is 10 minutes.
Optional Setting	
Service Name	Enter the name of your Internet service provider.
PPP MTU Setting	Enter the size of a Maximum Transmission Unit (MTU).
TCP MSS Setting	Enter the size of the Maximum Segment Size (MSS).
At the "(S)ave and return R)eturn without saving M)odify:" prompt, type S and press [ENTER] to save the changes and return to the previous screen, type R and press [ENTER] to discard all changes and return to the previous screen or type M and press [ENTER] to continue configuring the fields. Restart the device when prompted. Press [ESC] and enter Y to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

32.6.3 WAN Type: PPTP

To activate PPTP support on the VSG, enter **T** in the **WAN Type** field to display the **WAN Configuration** screen as shown next. Refer to the related web configurator section for background information.

Figure 168 SMT: WAN Configuration: PPTP

WAN Configuration	
WAN Type? (D/S/P/T)	:T
Local IP Address	:
Local Subnet Mask	:
Gateway IP Address	:
Server IP Address	:
Username	:
Password	:
Connect Setting? (C/K)	:C
Max idle Time (Min)	:10
Optional Setting	
Connection ID/Name	:
PPP MTU Setting	:1460
TCP MSS setting	:1400

The following table describes the PPTP-related fields in this menu.

Table 76 SMT: WAN Configuration: PPTP

FIELD	DESCRIPTION
WAN Type? (D/S/P/T)	Enter T to enable PPTP support.
Local IP Address	Enter the (static) IP address assigned to you by your ISP for the WAN interface.
Local Subnet Mask	Enter the subnet mask assigned to you by your ISP (if given) for the WAN interface.
Gateway IP Address	Type the IP address of the gateway device (if given).
Server IP Address	Enter the IP address of the PPTP server.
Username	Enter the login user name assigned to you by your ISP.
Password	Enter the password associated with the user name above.
Connect Setting? (C/K)	Enter C (Connect on demand) when you don't want the connection up all the time and specify an idle time-out in the Max. Idle Timeout Setting field. This is the default selection. Enter K (Keep alive) when you want your connection up all the time and specify the redial time in the Redial Period field to set how long the VSG waits before trying to bring up the connection automatically if it is disconnected.
Redial Period (Sec)	The field is only visible when you select K in the Connect Setting field. Type the time in seconds that elapses before the VSG automatically attempts to reconnect to the PPTP server. The default is 30 seconds.
Max Idle Time Setting	This field is only visible when you select C in the Connect Setting field. Type the time in minutes that elapses before the VSG automatically disconnects from the PPTP server. The default is 10 minutes.
Optional Setting	
Connection ID/ Name	If your ISP has provided a connection ID name, enter it in this field exactly as provided.
PPP MTU Setting	Enter the size of a Maximum Transmission Unit (MTU).

Table 76 SMT: WAN Configuration: PPTP (continued)

FIELD	DESCRIPTION
TCP MSS Setting	Enter the size of the Maximum Segment Size (MSS).
At the "(S)ave and return R)eturn without saving M)odify:" prompt, type S and press [ENTER] to save the changes and return to the previous screen, type R and press [ENTER] to discard all changes and return to the previous screen or type M and press [ENTER] to continue configuring the fields. Restart the device when prompted Press [ESC] and enter Y to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

32.7 LAN Configuration

From the **Main Menu** screen, enter 3 to display the **LAN Configuration** menu as shown next. Refer to [Chapter 6 on page 60](#) for background information.

Figure 169 SMT: LAN Configuration

LAN Configuration	
DHCP Configuration	
DHCP Service? (D/R/S)	:S
Start IP Address (Private)	:10.59.1.2
DHCP Pool Size (Private)	:20
Lease Time (Private)	:1440
Primary DNS IP Address	:168.95.1.1
Secondary DNS IP Address	:

The following table describes the fields in this menu.

Table 77 SMT: LAN Configuration

FIELD	DESCRIPTION
DHCP Service? (D/R/S)	Enter D (Disable) to deactivate DHCP services on the LAN. Ethernet devices connected to the LAN interface <i>must</i> use static IP addresses. Enter R (Relay) to set the VSG to forward network configuration requests to a DHCP server on the LAN network. Then configure the Server IP Address and Agent IP Address fields. Enter S (Server) to set the VSG to assign network information (IP address, DNS information etc.) to Ethernet device(s) connected to the LAN port. This is the default setting.
Start IP Address	This field is visible when you enter S in the DHCP Service field. Enter the first of the continuous addresses in the IP address pool. The default is 10.59.1.2.
DHCP Pool Size	This field is visible when you enter S in the DHCP Service field. This field specifies the size or count of the IP address pool. Enter a number not greater than 1024. The default is 253.
Lease Time	This field is visible when you enter S in the DHCP Service field. Specify the time (in minutes between 1 and 71582788) a DHCP client is allowed to use an assigned IP address. When the lease time expires, the DHCP client is given a new, unused IP address. The default is 1440 minutes.

Table 77 SMT: LAN Configuration (continued)

FIELD	DESCRIPTION
Relay Server IP Address	This field is only visible when you enter R in the DHCP Service field. If the VSG is set to function as a DHCP relay, enter the IP address of the DHCP server.
Primary/Secondary DNS IP Address	These fields are visible when you enter S in the DHCP Service field. Enter the IP address of the DNS server(s) in the Primary DNS IP Address and/or Secondary DNS IP Address fields. You <i>must</i> specify a DNS server.
At the "(S)ave and return R)eturn without saving M)odify:" prompt, type S and press [ENTER] to save the changes and return to the previous screen, type R and press [ENTER] to discard all changes and return to the previous screen or type M and press [ENTER] to continue configuring the fields. Restart the device when prompted Press [ESC] and enter Y to stop any actions in the current screen and return to the previous screen. All changes will be discarded.	

32.8 System Status

From the main menu, enter 4 and press [ENTER] to display the **System Status** menu as shown next.

Figure 170 SMT: System Status

System Status	
System Name	:
Doamin Name	:
Console Port Speed	:9600
Web Server Port	:80
E-Mail Server Redirect	:
WAN Configuration	
WAN Type? (D/S/P/T)	:DHCP Client
IP Address	:172.21.3.66
Subnet Mask	:255.255.0.0
Gateway	:172.21.0.254
Primary DNS Server	:172.20.0.63
Secondary DNS Server	:172.20.0.27
DHCP Configuration	
DHCP Service? (D/R/S)	:Disable
Press any key to return.	

The following table describes the fields in this screen.

Table 78 SMT: System Status

FIELD	DESCRIPTION
System Name	This field displays the name of the VSG for identification purposes.
Domain Name	This field displays the domain name.

Table 78 SMT: System Status (continued)

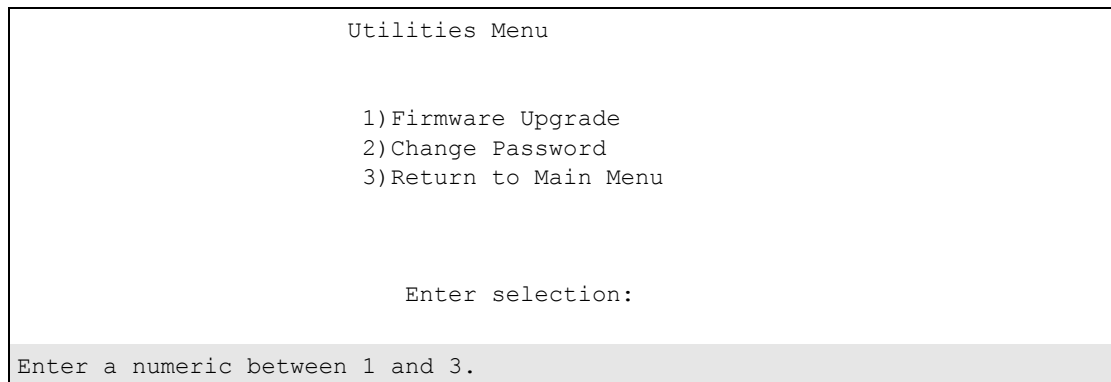
FIELD	DESCRIPTION
Console Port Speed	This field displays the console port speed.
Web Server Port	This field displays the port number for the embedded web server. If the port number is not 80 , then you need to append the port number to the WAN port IP address to access the VSG web configurator. For example, if 8010 is the web server port number, then you must enter "http://www.192.168.1.1:8010" in the address bar on the web browser where 192.168.1.1 is the WAN or LAN port IP address.
E-mail Server IP Address	This field displays the IP address of the e-mail server to which the VSG forwards the e-mail when the subscriber's e-mail server(s) is behind a NAT-enabled network or firewall.
WAN Configuration	
WAN Type? (D/S/P/T)	This field displays the WAN IP address assignment method (Static IP Setting or DHCP Client).
IP Address	This field displays the WAN IP address of the VSG.
Subnet Mask	This field displays the subnet mask on the WAN port.
Gateway	This field displays the IP address of the default gateway.
Primary DNS Server	This field displays the IP address of the primary DNS server.
Secondary DNS Server	This field displays the IP address of the secondary DNS server.
DHCP Configuration	
DHCP Service? (D/R/S)	This field displays the DHCP mode (Server , Relay or Disable) on the LAN port.
Start IP Address	This field is visible when the DHCP Service field is Server . This field displays the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This field is visible when the DHCP Service field is Server . This field displays the size of the DHCP client pool.
Lease Time	This field is visible when the DHCP Service field is Server . This field displays for how many minutes a DHCP client is allowed to use an assigned IP address.
Agent Server IP Address	This field is visible when the DHCP Service field displays Relay . This field displays the IP address of the DHCP relay agent.
Primary/Secondary DNS IP Address	These fields are visible when the DHCP Service field is Server . These two fields display the IP address(es) of the DNS server(s).
Press any key at the "Press any to return" prompt to go back to the previous screen.	

32.9 System Utilities

Use the **System Utilities** menus to upgrade firmware on the VSG or change the administrator login password.

In the SMT main menu, type 5 and press [ENTER] to display the **Utilities Menu** screen. To return to the **Main Menu** screen, press 3.

Figure 171 SMT: Utilities Menu



```
Utilities Menu

1)Firmware Upgrade
2)Change Password
3)Return to Main Menu

Enter selection:

Enter a numeric between 1 and 3.
```

32.9.1 Firmware Upgrade

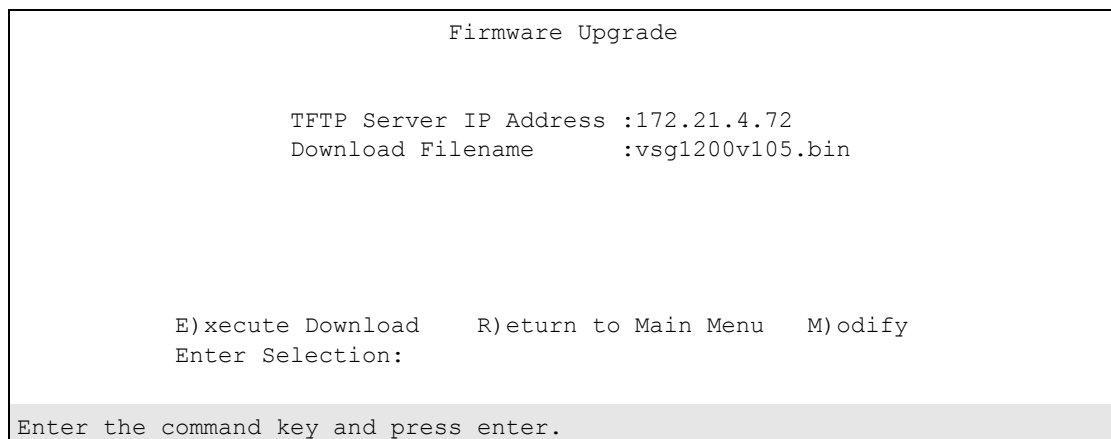
Note: You **MUST** run a TFTP server on a computer where a firmware file is stored to upgrade the firmware on the VSG.

You **MUST** have a WAN/LAN connection between the VSG and the TFTP server computer at the same time.

Follow the steps below to configure the TFTP settings in the SMT.

- 1** Connect the computer directly to the VSG through the console port. Refer to the section on establishing a console port connection for more information.
- 2** In the SMT main menu, type 5 and press [ENTER] to display the **Utilities Menu** screen.
- 3** Type 1 and press [ENTER] to display the Firmware Upgrade screen.
- 4** Enter the IP address of the computer running the TFTP server in the TFTP Server IP Address field.
- 5** Specify the name of the firmware file in the Download Filename field.

Figure 172 SMT: Firmware Upgrade



```
Firmware Upgrade

TFTP Server IP Address :172.21.4.72
Download Filename      :vsg1200v105.bin

E)ecute Download      R)eturn to Main Menu  M)odify
Enter Selection:

Enter the command key and press enter.
```

- 6 Type **E** at the “Enter Selection:” prompt to get the firmware file from the TFTP server.

Figure 173 SMT: Firmware Upgrade Process

```

Firmware Upgrade

TFTP Server IP Address :172.21.4.72
Download Filename      :vsg1200v105.bin

|-----+-----+-----+-----+-----|
*****

```

- 7 When the file transfer is complete, the VSG automatically reboots. Wait until the VSG finishes rebooting before accessing the VSG again.

32.9.2 Changing the Administrator Login Password

Note: It is recommended you change the default administrator login password.

To change other system login passwords, use the web configurator.

Follow the steps below to change the administrator login password.

- 1 In the main menu, type 5 and press [ENTER] to display the **Utilities** menu.
- 2 In the **Utilities** menu, type 2 and press [ENTER]. The **Change Administrator Password** menu displays.

Figure 174 SMT: Change Administrator Password

```

Change Administrator Password

Enter the old password :

Enter the new password :

Confirm the new password:

```

- 3 Type your current system password in the **Enter the old password** field, and press [ENTER].
- 4 Type your new system password in the **Enter the new password** field, and press [ENTER].
- 5 Re-type your new system password in the **Confirm the new password** field for confirmation and press [ENTER].
- 6 Save the settings.

Note: Note that as you type a password, the screen displays an asterisk “*” for each character you type.

32.10 Restart

Follow the steps below to restart the VSG.

- 1 In the main menu, type 6 and press [ENTER]. A screen displays prompting you to confirm.

Figure 175 SMT: Restart

Restart System (Y/N)?

- 2 Type **Y** and press [ENTER] to restart the VSG. Otherwise, type **N** and press [ENTER] to cancel the action and return to the main menu.

32.11 SMT Logout

To log out of the SMT, enter 7 in the main menu screen. A “Logout System (Y/N)?” prompt displays. Enter **Y** to log out.

Figure 176 SMT: System Logout

Logout System (Y/N)?

32.12 Factory Defaults

If you forgot your administrator login user name and password, you have to use the **RESET** button to reset the VSG back to the factory defaults. Refer to [Chapter 2 on page 38](#).

Resetting the VSG restores all system configuration back to the factory defaults. However, you may retain the subscriber account information.

Note: All system settings will be lost once you reset to the default settings.

Press [ESC] to return to the Main Menu screen.

Follow the steps below to reset the VSG back to the factory defaults.

- 1 In the main menu, type 8 and press [ENTER]. A screen displays prompting you to confirm.
- 2 Type **Y** and press [ENTER] to reset the VSG.

- 3** Type **Y** and press [ENTER] to retain the subscriber account information in the local subscriber database. Type **N** and press [ENTER] to delete all subscriber account information.
- 4** Press [ENTER] to reset the VSG. The VSG automatically restarts.

Figure 177 SMT: Reset to Factory Defaults

Change to factory defaults and the system will be restarted!
Are you sure (Y/N)?

CHAPTER 33

Troubleshooting

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

33.1 Using the LEDs to Diagnose Problems

The LEDs are useful aides for finding possible problem causes.

33.1.1 The Power LED

The LED on the front panel does not light up.

Table 79 Troubleshooting the Power LED

STEPS	CORRECTIVE ACTION
1	Check the connections from the VSG to the power source. Make sure you are using the supplied power cord and proper power supply. Refer to the appendix on product specifications.
2	Make sure the power source is turned on and that the VSG is receiving sufficient power.
3	If these steps fail to correct the problem, contact your local distributor for assistance.

33.1.2 The LAN Port LEDs

None of the LEDs for the LAN port(s) light up when connected to an Ethernet device.

Table 80 Troubleshooting the LAN LED

STEPS	CORRECTIVE ACTION
1	Make sure you are using the correct Ethernet cable. Connect the LAN port to a hub/switch using a crossover Ethernet cable or directly to a computer using a straight-through Ethernet cable.
2	Verify that the attached device(s) is turned on and properly connected to the VSG.
3	Verify that Ethernet cable length does not exceed 100 meters.
4	Make sure the network adapters are working on the attached devices.

33.1.3 The WAN Port LEDs

None of the LEDs for the WAN port light up when connected to an Ethernet device.

Table 81 Troubleshooting the WAN LED

STEP	CORRECTIVE ACTION
1	Verify that the attached device(s) is turned on and properly connected to the VSG.
2	Verify that Ethernet cable length does not exceed 100 meters.
3	Make sure the network adapters are working on the attached devices.

33.2 The Console Port

I cannot access the VSG through the console port.

Table 82 Troubleshooting Console Port

STEP	CORRECTIVE ACTION
1	Check to see if the VSG is connected to your computer using a console cable.
2	Check to see if the communications program is configured correctly. Set the communication parameters as stated here. • Emulation: auto detect • Baud Rate: 9600 bps • No Parity, 8 data bits, 1 stop bit • Flow Control: None
3	Make sure you entered the correct username and password. The default administrator username is "admin" and the default password is "1234". The username and password are case sensitive. If you have forgotten the administrator user name and/or password, you must reset the VSG back to the factory defaults using the reset button. Use a pointed object to press the reset button on the front panel to reset the VSG. All your custom configuration will be lost.

33.3 Web Configurator

I cannot access the web configurator.

Table 83 Troubleshooting Web Configurator

STEP	CORRECTIVE ACTION
1	Make sure you are using the correct WAN or LAN IP address.
2	Make sure you entered the correct username and password. The default administrator username is "admin" and the default password is "1234". The username and password are case-sensitive. If you change the server port number, you need to append the port number to the WAN or LAN port IP address to access the web configurator. For example, if you enter "8010" as the web server port number, then you must enter "http://www.192.168.1.1:8010" where 192.168.1.1 is the WAN or LAN port IP address. If you have forgotten the administrator user name and/or password, you must reset the VSG back to the factory defaults using the reset button. Use a pointed object to press the reset button on the front panel to reset the VSG. All your custom configuration will be lost.
3	Ping the VSG from your computer on the WAN or LAN.

The web configurator does not display properly.

Table 84 Troubleshooting Internet Browser Display

STEP	CORRECTIVE ACTION
1	Make sure you are using Internet Explorer (version 4.0 and later) or Netscape (version 6.0 or later) with JavaScript support enabled.
2	Delete the temporary web files and log in again. In Internet Explorer, click Tools, Internet Options and then click the Delete Files ... button. When a Delete Files window displays, select Delete all offline content and click OK. (Steps may vary depending on the version of your Internet browser.)

33.4 Internet Access

A subscriber cannot connect to the Internet through the VSG.

Table 85 Troubleshooting Internet Access

STEPS	CORRECTIVE ACTION
1	Check your Internet settings on your modem and/or router.
2	Make sure the subscriber enters the correct user name and password to log in to the VSG. The user name and password are case sensitive.
3	Make sure the account is still valid.
4	Make sure there is no conflict in IP address assignment. Refer to the appendix.

33.5 The Statement Printer

This section is applicable when you purchase an external statement printer, also known as an account generator printer.

I cannot print account information using a statement printer.

Table 86 Troubleshooting the Statement Printer

STEP	CORRECTIVE ACTION
1	Make sure the statement printer is connected to a power source and is turned on.
2	Check that the statement printer is connected to the port labeled Console .
3	Make sure there is enough printing paper in the statement printer.
4	Check that you select Statement Printer Device in the Console Type field in the System screen.
5	4 Make sure you configure and associate a billing profile for the first button in the Dynamic Account Operator Panel screen. The first button corresponds to the button on the statement printer.

Appendix A

Product Specifications

Table 87 Product Specifications: General

Standard	IEEE 802.3 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet
Interface	One 10/100 Ethernet WAN port One 10/100 Ethernet LAN port One RS232 serial port for console setting or an external statement printer One PMS RS232 serial port One reset button
Networking	Plug-and-play subscriber Internet access Supports 250 simultaneous users NAT (RFC1631) LAN DHCP server (with client pool size of 512) and DHCP relay HTTP proxy SMTP/DNS redirection WAN connection (static IP/DHCP client /PPPoE/PPTP) NAT for VPN (IPSec/PPTP)
AAA	Web-based authentication RADIUS AAA Secondary RADIUS server Proprietary CAS (Central Authentication Service) Global roaming support Built-in Authentication and accounting Vendor Specific Attributes Static/Dynamic Accounting
Security	Port-based VLAN Layer 2 isolation VPN pass through (PPTP/ L2TP) SSL secure user login process SSL secure web-based administration Authorized remote management MAC address filter Session limit
Billing	Flexible, time-based billing Port-Location Mapping Credit cards (via Authorize.net, iValidate and WorldPay)

Table 87 Product Specifications: General (continued)

PMS Billing	Supports Micros Fidelio, Spectrum MK II, Marriott and Proprietary. PMS transaction logs Supports IEEE802.1q tag-based VLAN infrastructure
Local Services	Walled garden Advertisement URL link Login page re-direction Customizable subscriber login page and login messages MAC/IP/URL passthrough

Table 88 Product Specifications: Performance and Management

Maximum Throughput	72 Mbps
Concurrent Users	1,024
Management	Web-based management TFTP/HTTP firmware upgrade Schedules firmware upgrade Backup/Restore configuration Real-time status list Remote authorized management Configuration file import/export LAN device management Syslog Session trace SNMP v1/v2 (MIB II with traps)

Table 89 Product Specifications: Physical and Environmental

LED	Power SYS WAN/LAN: 10, 100
Dimension	440(W) x 116(L) x 44(H) mm
Temperature	0°C to 50°C
Humidity	10% to 95% (non-condensing)
Power	Internal universal switching power supply 100-220 V AC, 50/60 Hz Maximum power consumption: 10W
Certifications	FCC part 15 Class A CE CSA RoHS VCCI WEEE

Appendix B

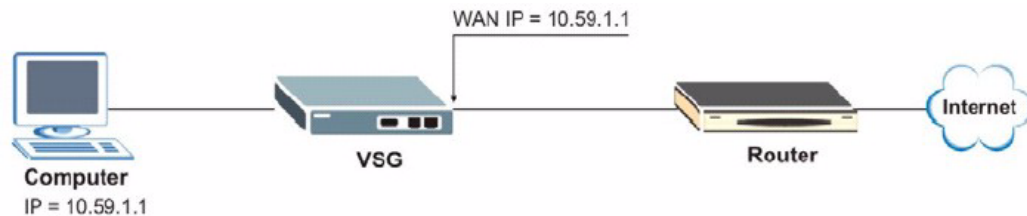
IP Address Assignment Conflicts

This appendix describes situations where IP address conflicts may occur. Subscribers with duplicate IP addresses will not be able to access the Internet.

Scenario 1: The VSG is using the same LAN and WAN IP addresses

The following figure shows an example where the VSG is using a WAN IP address that is the same as the IP address of a computer on the LAN.

Figure 178 IP Address Conflicts: Scenario 1



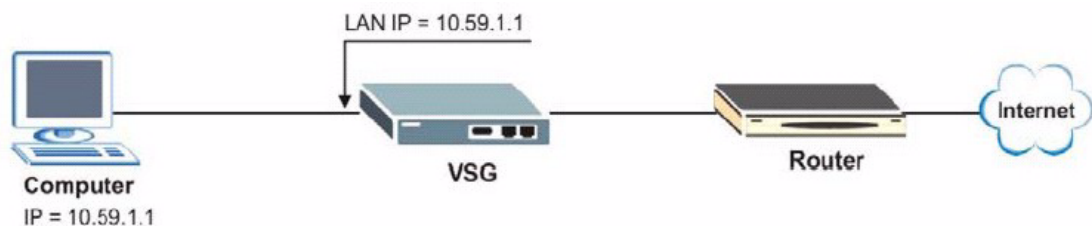
You must set the VSG to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the VSG. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1.

Otherwise, It is recommended the VSG use a public WAN IP address.

Scenario 2: The VSG LAN IP address conflicts with the DHCP client IP address

In the following figure, the VSG is acting as a DHCP server. The VSG assigns an IP address, which is the same as its LAN port IP address, to a DHCP client attached to the LAN.

Figure 179 IP Address Conflicts: Scenario 2

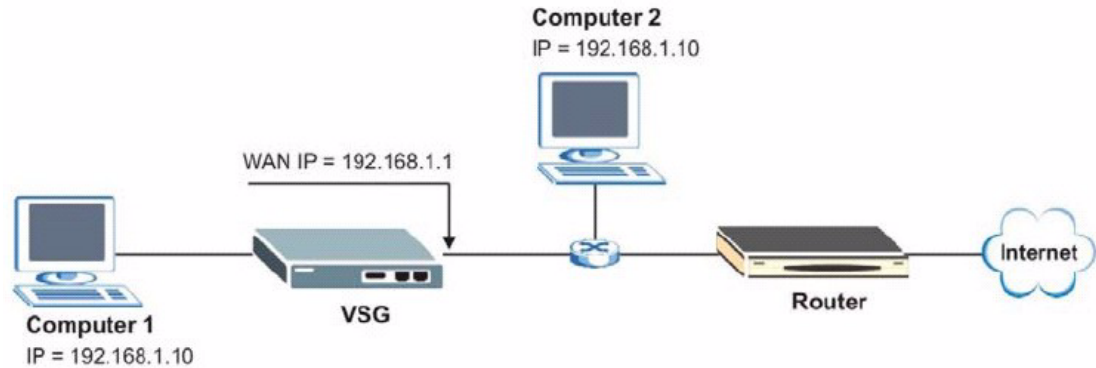


To solve this problem, make sure the VSG LAN IP address is not in the DHCP IP address pool.

Scenario 3: The Subscriber IP address is the same as the IP address of a network device

The following figure depicts an example where the subscriber IP address is the same as the IP address of a network device not attached to the VSG.

Figure 180 IP Address Conflicts: Scenario 3



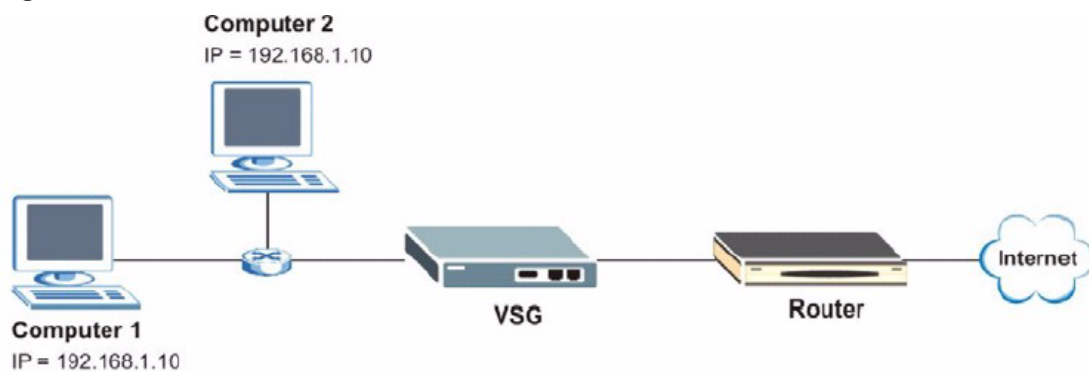
You must set the VSG to use different LAN and WAN IP addresses on different subnets if you enable DHCP server on the VSG. For example, you set the WAN IP address to 192.59.1.1 and the LAN IP address to 10.59.1.1.

Otherwise, It is recommended the VSG use a public WAN IP address.

Scenario 4: Two or more subscribers have the same IP address.

By converting all private IP addresses to the WAN IP address, the VSG allows subscribers with different network configurations to access the Internet. However, there are situations where two or more subscribers are using the same private IP address. This may happen when a subscriber is configured to use a static (or fixed) IP address that is the same as the IP address the VSG DHCP server assigns to another subscriber acting as a DHCP client.

In this case, the subscribers are not able to access the Internet.

Figure 181 IP Address Conflicts: Scenario 4

This problem can be solved by adding a VLAN-enabled switch or setting the computers to obtain IP addresses dynamically.

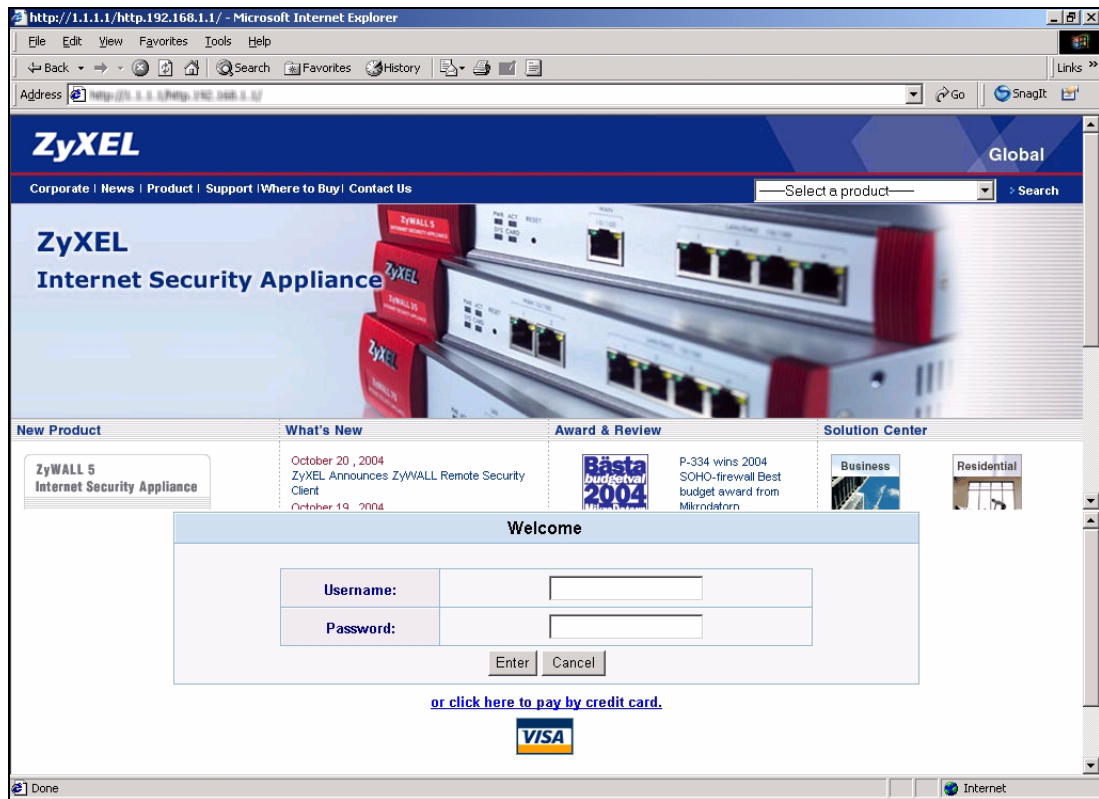
Appendix C

Subscriber Login

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

Depending on the settings, a subscriber login screen displays prompting for a user name and password.

Figure 182 Subscriber Login Screen: Framed Example



Enter a user name and password and click **Enter**. Depending on the settings in the VSG, either the specified web page or an advertisement web page displays. After a successful login, an information window may display.

Figure 183 Subscriber Login: Information Window Example

Information Window	
You can use Internet now!	
This is an information window to show the usage and notice. You can type http://1.1.1.1/info to open this window again without VPN connection.	
Remaining Usage	hh:mm:ss

Appendix D

Vendor Specific Attributes

This appendix describes the format of the vendor specific attributes supported.

Overview

With RADIUS server authentication, you can define vendor specific attributes (VSAs) in addition to the set of standard RADIUS attributes defined in RFC 2865 and RFC 2866. A VSA is an attribute-value pair that is sent between a RADIUS server and the VSG. It is necessary you define the VSAs on the RADIUS sever if you want the VSG to perform any of the additional functions listed below:

- Limit Download bandwidth per subscriber
- Limit Upload bandwidth per subscriber
- Limit Total traffic bandwidth allowed per subscriber
- Specify advertising web site per subscriber
- Enable/disable SMTP redirect

Note: Before you can make use of these functions, configure the proprietary VSAs on the RADIUS server. Refer to the documentation that comes with your RADIUS server for more information.

VSG-1200 V2 Supported VSAs

The following table describes the VSGs specific to the VSG-1200 V2.

Table 90 VSG-1200 V2 Supported VSAs

NO.	NAME	DESCRIPTION	TYPE	VALUE
1	Traffic-Limit	This attribute defines total bandwidth (in Mbytes) allowed for a subscriber. Internet access is based on the total upload/download bandwidth regardless of the account expiration time. This attribute is supported when you set the VSG to use an external RADIUS server for user authentication in accumulation mode.	Integer	maximum 4095
2	SMTP Redirect	This attribute indicates whether the VSG is to re-direct E-mails. Values: 0 = do not redirect e-mails. 1 = allow e-mail redirection. Note: To allow e-mail redirection, you <i>must</i> configure the SMTP settings on the VSG. Refer to Section "Server" on page 70 for more information.	Integer	0, 1
3	BW-Up	This attribute defines the upload bandwidth allowed for a subscriber. Internet access is based on the upload bandwidth regardless of the account expiration time. This means that a subscriber is allowed to access the Internet until the total upload bandwidth allocated is reached. This attribute is supported when you enable bandwidth management on the VSG with the class of service based on the RADIUS settings. Refer to Chapter 16, "Bandwidth Management," on page 144 for more information. Note: You <i>must</i> also specify the BW-Down attribute.	Integer	64 -24567
4	BW-Down	This attribute defines the download bandwidth allowed for a subscriber. Internet access is based on the download bandwidth regardless of the account expiration time. This means that a subscriber is allowed to access the Internet until the total download bandwidth allocated is reached. This attribute is supported when you enable bandwidth management on the VSG with the class of service based on the RADIUS settings. Refer to Chapter 16, "Bandwidth Management," on page 144 for more information. Note: You <i>must</i> also specify the BW-Up attribute.	Integer	64 - 24567
5	Portable Page URL	This attribute allows you to specify a different advertising web site for each subscriber after a successful login.	String	maximum 200

Error Messages

The following table describes the VSA-related error messages.

Table 91 VSA-related Error Messages

ERROR MESSAGE	DESCRIPTION
VSA Error!-Traffic limit-Time to finish is selected	The VSG is set to use the "Time to Finish" mode while the VSA response from the external RADIUS server include the Traffic-limit attribute.
VSA Error!-Traffic limit-Over value	The value for Traffic-limit attribute is more than the maximum allowed (4095).
VSA Error!-SMTP Redirect-no SMTP server setup	No e-mail server configuration is set on the VSG while the VSA response from the external RADIUS server indicates SMTP redirection is activated (with an attribute value of 1).
VSA Error!-BW-up/down-Bandwidth Management =disable	Bandwidth management is not activated on the VSG while the VSA response from the external RADIUS server contains upload and download bandwidth limits.
VSA Error!-BW-up/down-Equal bandwidth for all subscriber selected	Bandwidth management is activated on the VSG with equal bandwidth applied to all subscribers.
VSA Error!-BW-up/down-Class of service is selected but no BW-up/down	Bandwidth management is activated on the VSG with class of service selected while no upload/download bandwidth information is obtained from the external RADIUS server.
VSA Error!-BW-up/down-No BW-down	The external RADIUS server does not send the BW-down attribute value to the VSG.
VSA Error!-BW-up/down-No BW-up	The external RADIUS server does not send the BW-up attribute value to the VSG.
VSA Error!-BW-up/down-BW-up out of range	The value for BW-up attribute is invalid.
VSA Error!-BW-up/down-BW-down out of range	The value for BW-down attribute is invalid.

Appendix E

Report Printing Using the SP-200

This appendix shows you how to print reports using the SP-200.

Overview

The SP-200 allows you to print status reports about the subscriber accounts and general VSG system information . Simply press a key combination on the SP-200 to print a report instantly without accessing the web configurator.

The following lists the reports that you can print using the SP-200.

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

Initial Setup

Do the following before you start report printing using an SP-200.

- 1** Purchase an SP-200 from your local dealer if you don't have one.
- 2** Set the function of the console port on the VSG for statement printer connection (see [Section 5.1 “General System Setting” on page 56](#)).
- 3** Connect the SP-200 to the **CONSOLE** port on the VSG (see [Section 2.2 “Hardware Connections” on page 39](#)).
- 4** Turn on the power to the SP-200.

Refer to the user's guide that comes with your SP-200 for more information.

Key Combination

The following table lists the key combination to print each report. Refer to [Figure 54 on page 106](#) for button labels on the SP-200.

Note: You must press the key combination on the SP-200 within five seconds to print.

Table 92 SP-200: Report Printing Key Combination

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

The following sections describe each report printout in detail.

Daily Account Summary

This report shows the username and price for the subscriber account(s) that is created for the current day.

Key combination: A B C A A

The following figure shows an example.

Figure 184 SP-200: Daily Account

Daily Account	

2004/10/28	

Username	Price
9v269m55	10.00
bwh2y943	20.00

TOTAL ACCOUTNS: 2	
TOTAL PRICE: \$ 30.00	

2004/10/28 14:12:11	
---End---	

Monthly Account Summary

This report shows the username and price for the subscriber account(s) that is created for the current month.

Key combination: A B C B B

The following figure shows an example.

Figure 185 SP-200: Monthly Account

Monthly Account	

2004/10	

Username	Price
bwh2y936	10.00
Cindy	10.00
9v269m55	10.00
bwh2y943	20.00

TOTAL ACCOUTNS: 4	
TOTAL PRICE: \$ 50.00	

2004/10/28 14:11:26	
---End---	

System Status

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

Key combination: A B C C C

The following figure shows an example.

Figure 186 SP-200: System Status

```

      System Status
-----
ITEM DESCRIPTION
-----
WAST ESTABLISHED
SYST 02D:02H:42M:46S
-----

HOST VSG-1200
FRMW 1.05
BTRM 1.01
LOCA
WAMA 00-90-0E-00-4A-29
LAMA 00-90-0E-00-4A-28
WATP DHCP
WAIP 172.21.2.67
WASM 255.255.0.0
WAGW 172.21.0.254
PDNS 172.20.0.63
SDNS 172.20.0.27
DHCP DHCP SERVER
DHSP 10.59.1.2
DHEP 10.59.1.254
DHLT 1440
EMAIL /PORT25
-----

      2004/10/28 11:24:42

      ---End---

```

The following table describes the labels in this report.

Table 93 SP-200: System Status

LABEL	DESCRIPTION
WAST	This field displays the WAN connection status.
SYST	This field displays the time since the system was last restarted.
HOST	This field displays the description name of the VSG for identification purposes.
FRMW	This field displays the version of the firmware on the VSG.
BTRM	This field displays the version of the bootrom.
WAMA	This field displays the MAC address of the VSG on the WAN.
LAMA	This field displays the MAC address of the VSG on the LAN.
WATP	This field displays the mode of the WAN port.
WAIP	This field displays the IP address of the WAN port on the VSG.
WASM	This field displays the subnet mask of the WAN port on the VSG.
WAGW	This field displays the IP address of the default gateway of the WAN port on the VSG.
PDNS	This field displays the IP address of the primary DNS server.
SDNS	This field displays the IP address of the secondary DNS server.

Table 93 SP-200: System Status (continued)

LABEL	DESCRIPTION
DHCP	This field displays the DHCP mode (DHCP Server , Relay or DHCP Disable) on the LAN.
DHSP	If the DHCP field is DHCP Server , this field displays the first of the continuous addresses in the IP address pool. If the DHCP field is DHCP Relay , this field displays the DHCP server IP address.
DHEP	This field is visible when the DHCP is DHCP Server . This field displays the end of the continuous addresses in the IP address pool.
DHLT	This field is visible when the DHCP is DHCP Server . This field displays the time (in minutes) a DHCP client is allowed to use an assigned IP address.
EMAIL	The field displays e-mail server port number.

Network Statistics

This report shows the network statistics on the VSG.

Key combination: A B C A B

The following figure shows an example.

Figure 187 SP-200: Network Statistics

Network	
ITEM	DESCRIPTION
WAST	ESTABLISHED
SYST	02D:02H:42M:46S
WATD	37
WARD	4816
WATE	0
WARE	0
LATD	1768
LARD	4616
LATE	0
LARE	0
2004/10/28 15:24:42	
---End---	

The following table describes the labels in this report.

Table 94 SP-200: Network Statistics

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

Appendix F

Cable Types and Cable Pin Assignments

RJ-45 Ethernet Port

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

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

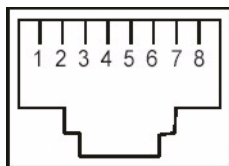
Table 95 Network Cable Types

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

The WAN Port

The following table describes the Ethernet cable pin assignments for the WAN port.

Table 96 WAN Port Cable Ping Assignments



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

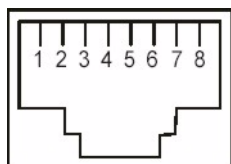
Make sure that the Ethernet cable connection between the VSG and the hub or router conforms to the pin assignments as shown in the following diagram.

Figure 188 WAN Port Cable Pin Assignments

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

The LAN Port

The following table describes the Ethernet cable pin assignments for the LAN port.

Table 97 LAN Port Cable Pin Assignments

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

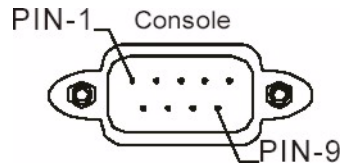
Make sure that the Ethernet cable connection between the VSG and a computer or switch uplink port conforms to the pin assignments as shown in the figure.

Figure 189 LAN Port Cable Pin Assignments

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

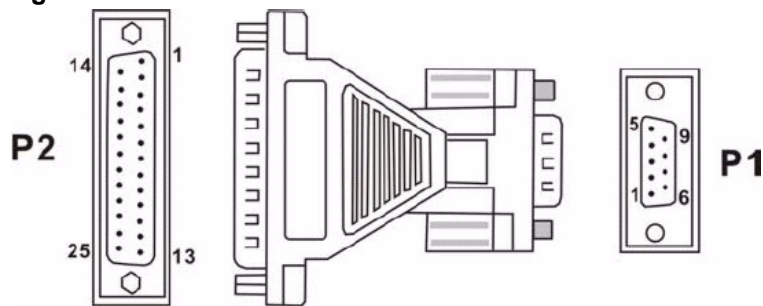
Serial Console Port

The following table describes the console cable pin assignments for the serial console port.

Table 98 Console Port Pin Assignment

PIN NO	MNEMONIC	FUNCTION
1	DCD	Received Line Signal Detector to the VSG.
2	TXT	Transmitted Data from the VSG.
3	RXT	Received Data to the VSG.
4	DTR	Data Terminal Ready from the VSG.
5	GND	Signal Ground (Common)
6	DSR	Data Set Ready to the VSG.
7	RTS	Request to Send from the VSG.
8	CTS	Clear to Send to the VSG.
9	RI	Ring Indicator to the VSG.

DB25 Male to DB9 Male Connector

Figure 190 DB25 Male to DB9 Male Connector**Table 99** DB25 Male to DB9 Male Connector Ping Assignment

P1	P2
1	8
2	2
3	3
4	20
5	7
6	6
7	4
8	5
9	22

Appendix G

Setting up Your Computer's 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.

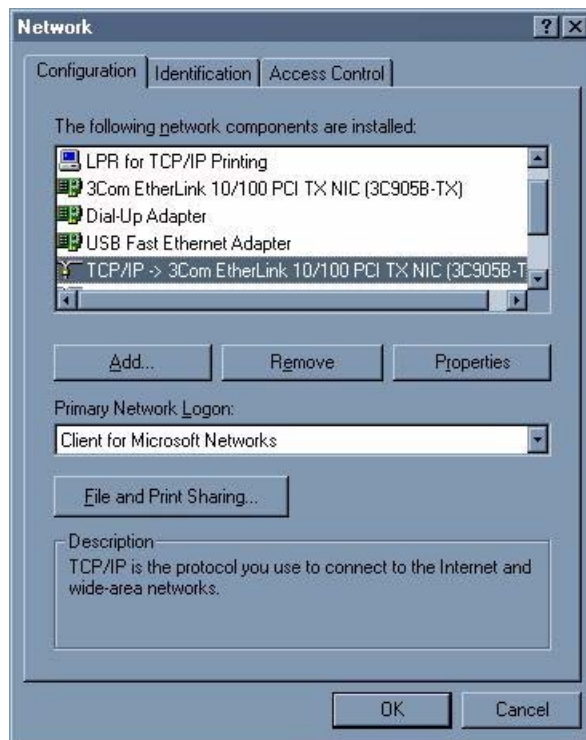
TCP/IP should already be installed on computers using Windows NT/2000/XP, Macintosh OS 7 and later operating systems.

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 the VSG-1200 V2's LAN port.

Windows 95/98/Me

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

Figure 191 Windows 95/98/Me: Network: Configuration

Installing Components

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:

- 1 In the **Network** window, click **Add**.
- 2 Select **Adapter** and then click **Add**.
- 3 Select the manufacturer and model of your network adapter and then click **OK**.

If you need TCP/IP:

- 1 In the **Network** window, click **Add**.
- 2 Select **Protocol** and then click **Add**.
- 3 Select **Microsoft** from the list of **manufacturers**.
- 4 Select **TCP/IP** from the list of network protocols and then click **OK**.

If you need Client for Microsoft Networks:

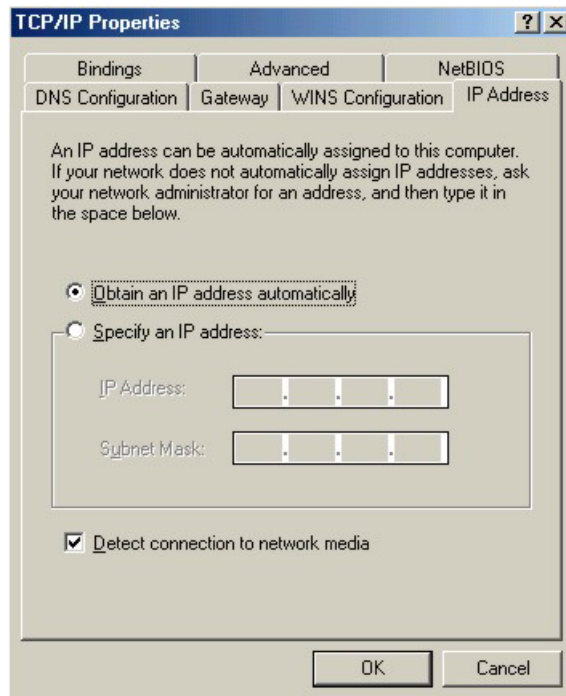
- 1 Click **Add**.
- 2 Select **Client** and then click **Add**.

- 3 Select **Microsoft** from the list of manufacturers.
- 4 Select **Client for Microsoft Networks** from the list of network clients and then click **OK**.
- 5 Restart your computer so the changes you made take effect.

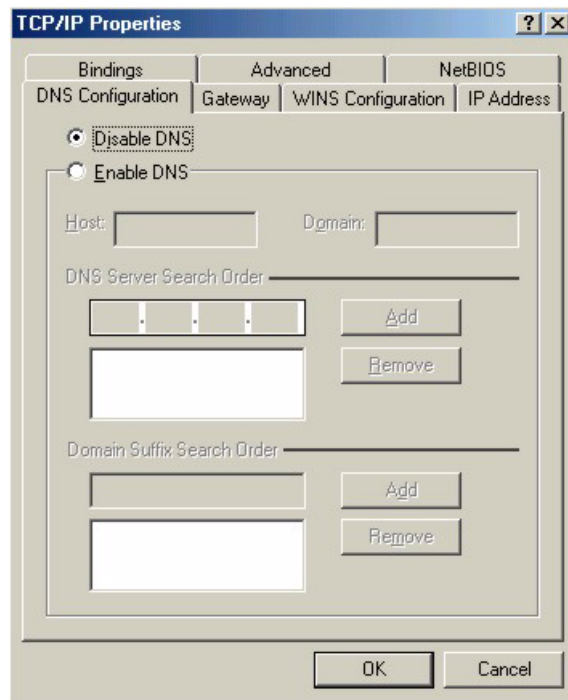
Configuring

- 1 In the **Network** window **Configuration** tab, select your network adapter's TCP/IP entry and click **Properties**
- 2 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.

Figure 192 Windows 95/98/Me: TCP/IP Properties: IP Address



- 3 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).

Figure 193 Windows 95/98/Me: TCP/IP Properties: DNS Configuration

4 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**.

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

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

7 Turn on your VSG-1200 V2 and restart your computer when prompted.

Verifying Settings

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

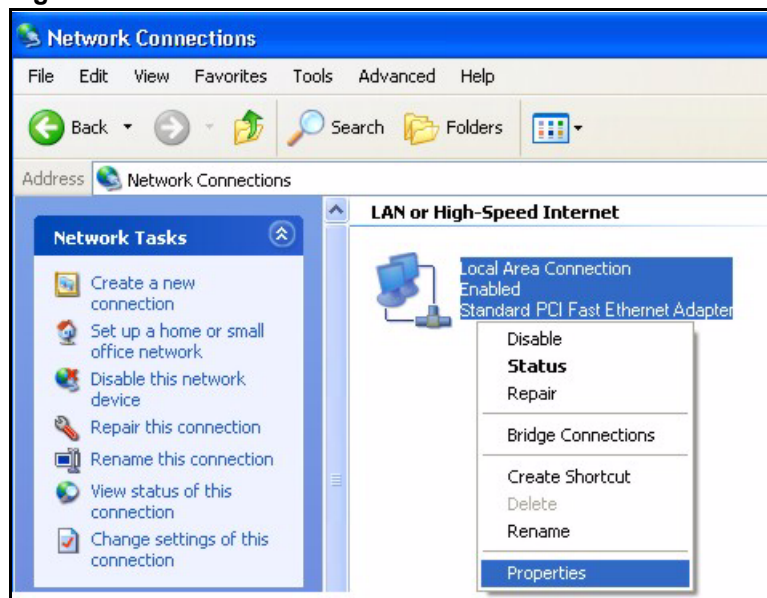
1 For Windows XP, click **start**, **Control Panel**. In Windows 2000/NT, click **Start**, **Settings**, **Control Panel**.

Figure 194 Windows XP: Start Menu

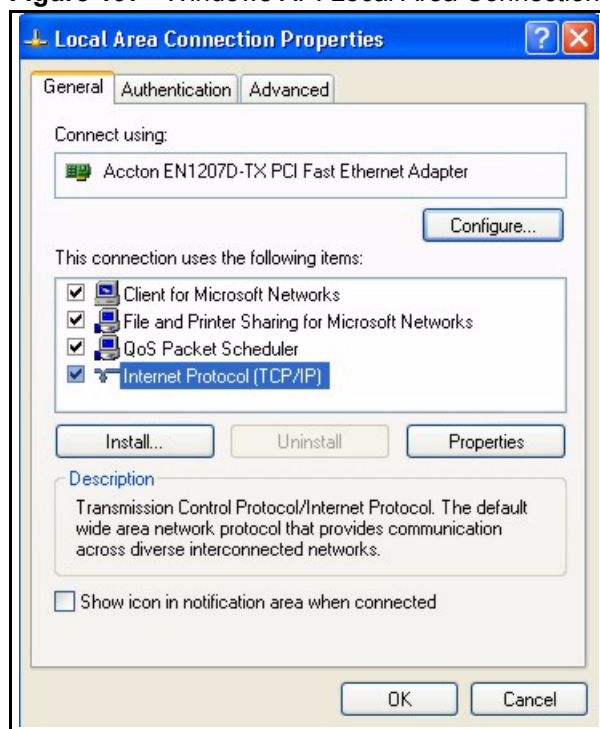
2 For Windows XP, click **Network Connections**. For Windows 2000/NT, click **Network and Dial-up Connections**.

Figure 195 Windows XP: Control Panel

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

Figure 196 Windows XP: Control Panel: Network Connections: Properties

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

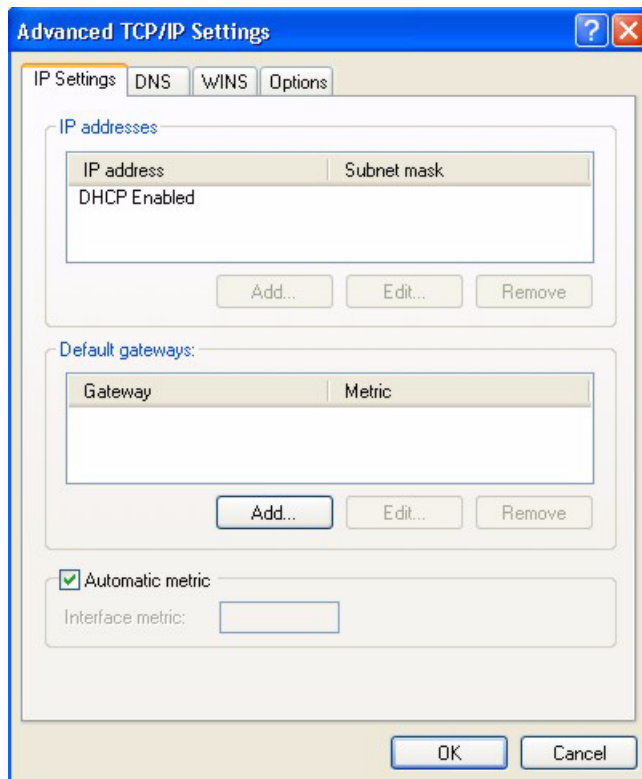
Figure 197 Windows XP: Local Area Connection Properties

- 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**.

Figure 198 Windows XP: Advanced TCP/IP Settings



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

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

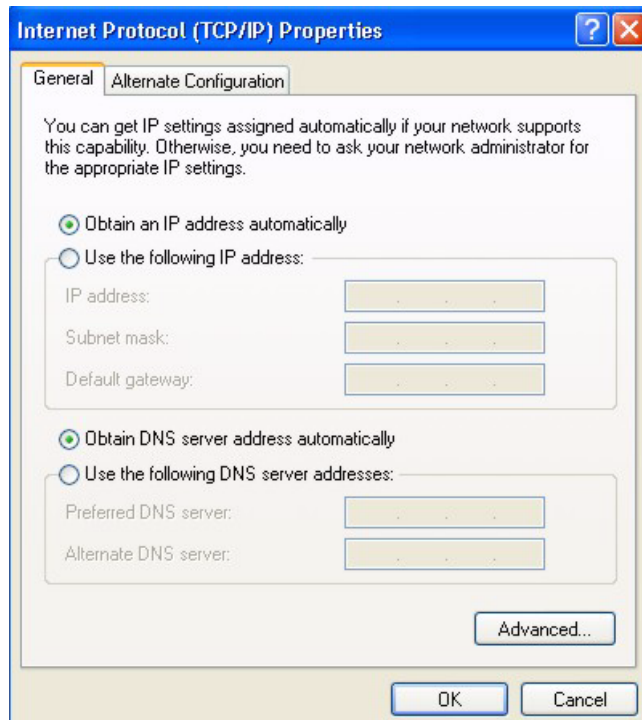
- In the **IP Settings** tab, in IP addresses, click **Add**.
- In **TCP/IP Address**, type an IP address in **IP address** and a subnet mask in **Subnet mask**, and then click **Add**.
- Repeat the above two steps for each IP address you want to add.
- Configure additional default gateways in the **IP 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.

- 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.

Figure 199 Windows XP: Internet Protocol (TCP/IP) Properties



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

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

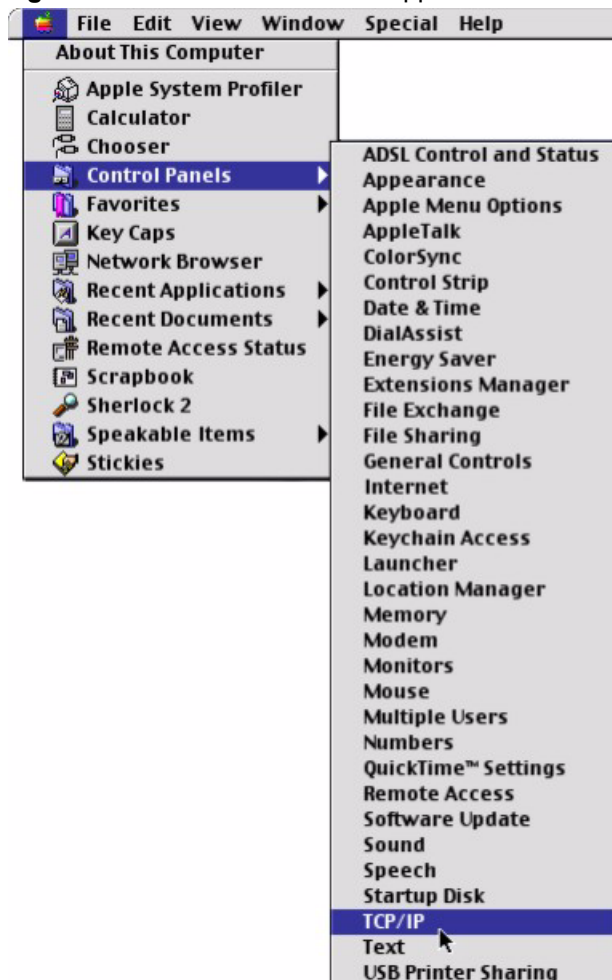
10 Turn on your VSG-1200 V2 and restart your computer (if prompted).

Verifying Settings

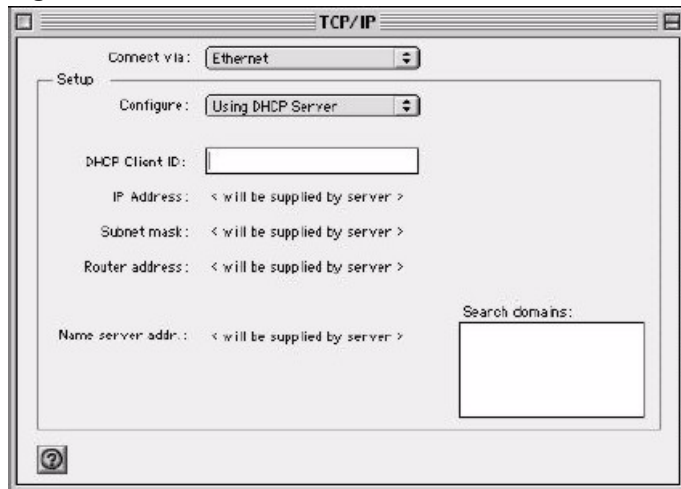
- 1** Click **Start**, **All Programs**, **Accessories** and then **Command Prompt**.
- 2** In the **Command Prompt** window, type "ipconfig" and then press [ENTER]. You can also open **Network Connections**, right-click a network connection, click **Status** and then click the **Support** tab.

Macintosh OS 8/9

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

Figure 200 Macintosh OS 8/9: Apple Menu

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

Figure 201 Macintosh OS 8/9: TCP/IP

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 VSG-1200 V2 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 VSG-1200 V2 and restart your computer (if prompted).

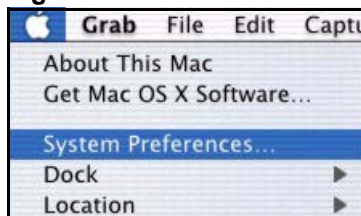
Verifying Settings

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

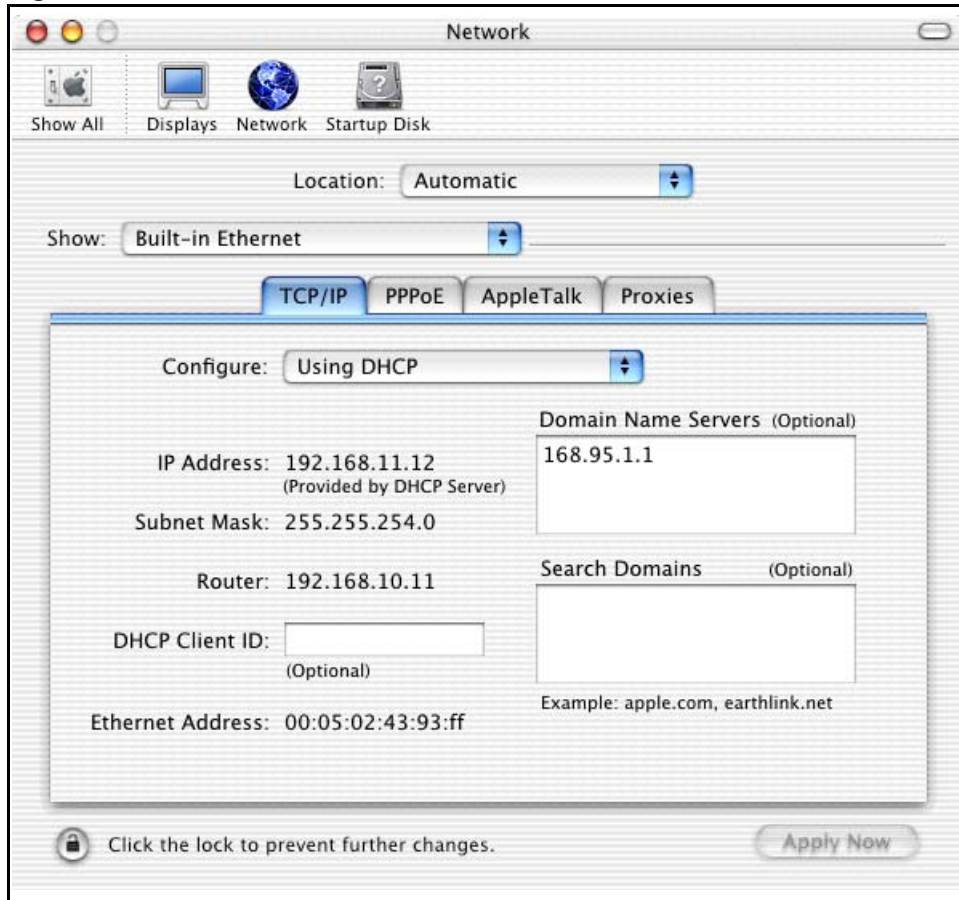
Macintosh OS X

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

Figure 202 Macintosh OS X: Apple Menu



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

Figure 203 Macintosh OS X: Network

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 VSG-1200 V2 in the **Router address** box.

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

6 Turn on your VSG-1200 V2 and restart your computer (if prompted).

Verifying Settings

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

APPENDIX H

IP Addresses and Subnetting

This appendix introduces IP addresses, IP address classes and subnet masks. You use subnet masks to subdivide a network into smaller logical networks.

Introduction to IP Addresses

An IP address has two parts: the network number and the host ID. Routers use the network number to send packets to the correct network, while the host ID identifies a single device on the network.

An IP address is made up of four octets, written in dotted decimal notation, for example, 192.168.1.1. (An octet is an 8-digit binary number. Therefore, each octet has a possible range of 00000000 to 11111111 in binary, or 0 to 255 in decimal.)

There are several classes of IP addresses. The first network number (192 in the above example) defines the class of IP address. These are defined as follows:

- Class A: 0 to 127
- Class B: 128 to 191
- Class C: 192 to 223
- Class D: 224 to 239
- Class E: 240 to 255

IP Address Classes and Hosts

The class of an IP address determines the number of hosts you can have on your network.

- In a class A address the first octet is the network number, and the remaining three octets are the host ID.
- In a class B address the first two octets make up the network number, and the two remaining octets make up the host ID.
- In a class C address the first three octets make up the network number, and the last octet is the host ID.

The following table shows the network number and host ID arrangement for classes A, B and C.

Table 100 Classes of IP Addresses

IP ADDRESS	OCTET 1	OCTET 2	OCTET 3	OCTET 4
Class A	Network number	Host ID	Host ID	Host ID
Class B	Network number	Network number	Host ID	Host ID
Class C	Network number	Network number	Network number	Host ID

An IP address with host IDs of all zeros is the IP address of the network (192.168.1.0 for example). An IP address with host IDs of all ones is the broadcast address for that network (192.168.1.255 for example). Therefore, to determine the total number of hosts allowed in a network, deduct two as shown next:

- A class C address (1 host octet: 8 host bits) can have $2^8 - 2$, or 254 hosts.
- A class B address (2 host octets: 16 host bits) can have $2^{16} - 2$, or 65534 hosts.

A class A address (3 host octets: 24 host bits) can have $2^{24} - 2$ hosts, or approximately 16 million hosts.

IP Address Classes and Network ID

The value of the first octet of an IP address determines the class of an address.

- Class A addresses have a **0** in the leftmost bit.
- Class B addresses have a **1** in the leftmost bit and a **0** in the next leftmost bit.
- Class C addresses start with **1 1 0** in the first three leftmost bits.
- Class D addresses begin with **1 1 1 0**. Class D addresses are used for multicasting, which is used to send information to groups of computers.
- There is also a class E. It is reserved for future use.

The following table shows the allowed ranges for the first octet of each class. This range determines the number of subnets you can have in a network.

Table 101 Allowed IP Address Range By Class

CLASS	ALLOWED RANGE OF FIRST OCTET (BINARY)	ALLOWED RANGE OF FIRST OCTET (DECIMAL)
Class A	00000000 to 01111111	0 to 127
Class B	10000000 to 10111111	128 to 191
Class C	11000000 to 11011111	192 to 223
Class D	11100000 to 11101111	224 to 239
Class E (reserved)	11110000 to 11111111	240 to 255

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. 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 like IP addresses. The “natural” masks for class A, B and C IP addresses are as follows.

Table 102 “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 leftmost 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.

Table 103 Alternative Subnet Mask Notation

SUBNET MASK	SUBNET MASK “1” BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.0	/24	0000 0000	0
255.255.255.128	/25	1000 0000	128
255.255.255.192	/26	1100 0000	192
255.255.255.224	/27	1110 0000	224

Table 103 Alternative Subnet Mask Notation (continued)

SUBNET MASK	SUBNET MASK "1" BITS	LAST OCTET BIT VALUE	DECIMAL
255.255.255.240	/28	1111 0000	240
255.255.255.248	/29	1111 1000	248
255.255.255.252	/30	1111 1100	252

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.

Table 104 Two Subnets Example

IP/SUBNET MASK	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").

To make two 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.

Note: In the following charts, shaded/bolded last octet bit values indicate host ID bits "borrowed" to make 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.

Table 105 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000

Table 105 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
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	

Table 106 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask	255.255.255.	128
Subnet Mask (Binary)	11111111.11111111.11111111.	10000000
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	

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 (00, 01, 10 and 11). The subnet mask is 26 bits (11111111.11111111.11111111.11000000) or 255.255.255.192. Each subnet contains 6 host ID bits, giving $2^6 - 2$ or 62 hosts for each subnet (all zeroes is the subnet itself, all ones is the broadcast address on the subnet).

Table 107 Subnet 1

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	0
IP Address (Binary)	11000000.10101000.00000001.	00000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000

Table 107 Subnet 1 (continued)

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
Subnet Address: 192.168.1.0	Lowest Host ID: 192.168.1.1	
Broadcast Address: 192.168.1.63	Highest Host ID: 192.168.1.62	

Table 108 Subnet 2

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	64
IP Address (Binary)	11000000.10101000.00000001.	01000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.64	Lowest Host ID: 192.168.1.65	
Broadcast Address: 192.168.1.127	Highest Host ID: 192.168.1.126	

Table 109 Subnet 3

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	128
IP Address (Binary)	11000000.10101000.00000001.	10000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.128	Lowest Host ID: 192.168.1.129	
Broadcast Address: 192.168.1.191	Highest Host ID: 192.168.1.190	

Table 110 Subnet 4

IP/SUBNET MASK	NETWORK NUMBER	LAST OCTET BIT VALUE
IP Address	192.168.1.	192
IP Address (Binary)	11000000.10101000.00000001.	11000000
Subnet Mask (Binary)	11111111.11111111.11111111.	11000000
Subnet Address: 192.168.1.192	Lowest Host ID: 192.168.1.193	
Broadcast Address: 192.168.1.255	Highest Host ID: 192.168.1.254	

Example Eight Subnets

Similarly use a 27-bit mask to create eight subnets (000, 001, 010, 011, 100, 101, 110 and 111).

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

Table 111 Eight Subnets

SUBNET	SUBNET ADDRESS	FIRST ADDRESS	LAST ADDRESS	BROADCAST ADDRESS
1	0	1	30	31
2	32	33	62	63
3	64	65	94	95
4	96	97	126	127
5	128	129	158	159
6	160	161	190	191
7	192	193	222	223
8	224	225	254	255

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

Table 112 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
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 [Table 100 on page 269](#)) available for subnetting.

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

Table 113 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

Index

A

AAA [234](#)
 access control [34](#)
 access point (AP) [36](#)
 accessing a LAN device [190](#)
 methods [190](#)
 requirements [190](#)
 account billing
 account expiration [103](#)
 account printout [95](#), [129](#)
 customize [129](#)
 examples [130](#)
 preview [130](#)
 account printout preview [101](#)
 accounting [34](#)
 Accumulation [81](#)
 Time to Finish [81](#)
 accounting port [84](#)
 Accumulation [81](#), [84](#)
 advanced subscriber login screen [123](#)
 advertisement link [149](#), [243](#)
 frequency [149](#)
 sequence [149](#)
 alternative subnet mask notation [270](#)
 assign IP address to a computer [256](#)
 authentication [34](#), [80](#)
 Built-in Authentication [81](#)
 CAS [80](#)
 RADIUS [81](#)
 types [80](#)
 User Agreement [80](#)
 authentication port [84](#)
 authentication setup [82](#)
 automate firmware upgrade [204](#)
 automatic firmware upgrade
 process [204](#)

B

backing up billing logs [192](#)
 bandwidth control [144](#)
 bandwidth limit
 downlink [90](#)
 uplink [90](#)

Bandwidth Management [90](#), [144](#)
 activate [144](#)
 class-based [144](#)
 equal share [144](#)
 RADIUS [146](#)
 types [144](#)
 bandwidth management [243](#)
 billing [88](#), [234](#)
 account
 credit card [32](#)
 billing logs [191](#)
 backup [192](#)
 charge type [191](#)
 delete all [191](#)
 export [191](#)
 opening [192](#)
 sample [193](#)
 billing profile [88](#)
 bandwidth limit [90](#)
 create [88](#)
 currency [89](#)
 duration [90](#)
 edit [89](#)
 setting [89](#)
 built-in authentication [34](#), [84](#)
 information window [127](#)
 scenario options [85](#)

C

CA [206](#)
 CAS [80](#)
 Central Authentication Service
 See CAS
 certificate [206](#)
 private key [207](#)
 secret password [207](#)
 Certification Authority (CA) [206](#)
 certifications [3](#)
 notices [3](#)
 viewing [3](#)
 class-based bandwidth allocation [144](#)
 activate [146](#)
 community [180](#)
 Concurrent Access [95](#)
 concurrent access [103](#)
 concurrent user [95](#), [235](#)

- allowable [185](#)
- set [95](#)
- configuration file
 - backup [196](#)
 - backup via TFTP [198](#)
 - restore [199](#)
 - restore via TFTP [199](#)
- configuration file management [35](#)
- console port [35](#), [40](#), [214](#), [253](#)
 - cable pin assignments [253](#)
 - change function [59](#)
 - communication parameters [214](#)
 - DB25 male connector [254](#)
 - DB9 male connector [254](#)
 - establish a connection [214](#)
 - SMT interface [214](#)
 - speed [217](#), [224](#)
 - statement printer [59](#)
- Copyright [2](#)
- Cost Of Transmission [165](#)
- create billing profiles [88](#)
- create dynamic subscriber account [106](#)
- create port-location mapping [112](#)
- create static subscriber account [95](#)
- create static subscriber accounts manually [97](#)
- credit card billing [32](#), [116](#)
 - authentication scenario option [87](#)
 - configuration steps [116](#)
 - credit card icons [119](#)
 - how it works [116](#)
 - service selection message [136](#)
 - setup [117](#)
 - subscriber login message [135](#)
 - successful notification [139](#)
 - transaction failed message [141](#)
- current user list [186](#)
- Customer Support [8](#)
- customize subscriber login screen [120](#)

D

- daily account summary [247](#)
- desktop installation [38](#)
- device reset [33](#), [40](#), [47](#)
- DHCP [33](#)
 - lease time [222](#)
 - mode
- DHCP client [56](#)
 - pool size [234](#)
- DHCP client table [187](#)
 - update interval [187](#)
- DHCP pool size [222](#)

- DHCP relay [223](#)
- DHCP server [56](#), [222](#), [236](#)
- DHCP services [222](#)
- digital certificate [206](#)
- digital signature [206](#)
- dimension [235](#)
- disclaimer [2](#)
- display subscriber account [102](#)
- DNS [258](#)
- DNS proxy [34](#)
- DNS server [219](#), [223](#)
- document feedback [30](#)
- domain name [56](#), [217](#), [223](#)
- Dynamic Host Configuration Protocol
 - See DHCP
- dynamic IP address [219](#)
- dynamic subscriber account [104](#)
 - backup [109](#)
 - configuration [105](#)
 - create using statement printer [107](#)
 - create using web configurator [106](#)
 - display [108](#)
 - general settings [104](#)
 - method to create [104](#)
 - print [108](#)

E

- edit a subscriber account [100](#)
- edit billing profiles [89](#)
- EIA standard size rack [38](#)
- e-mail forwarding [34](#)
- e-mail server
 - redirect [218](#)
- equal-share bandwidth allocation [144](#)
 - configure [145](#)
- error messages [244](#)
- Ethernet cable [230](#)
 - length specifications [252](#)
 - types [252](#)
- Ethernet port [252](#)
 - speed [252](#)
- export billing logs [191](#)

F

- FCC interference statement [3](#)
- feature [32](#)

feedback [30](#)
 firmware
 download to TFTP server [204](#)
 firmware download [202](#)
 firmware upgrade [35](#)
 about subscriber connection [204](#)
 automatic [204](#)
 from a TFTP Server [203](#)
 from computer [202](#)
 from TFTP server [225](#)
 important note on SMT [225](#)
 manual [202](#)
 schedule frequency [205](#)
 scheduled [204](#)
 firmware version [185](#), [249](#)
 forward e-mails [34](#)

G

Gateway [165](#)
 general setup [56](#)
 generate static subscriber accounts automatically [96](#)
 glossary [30](#)

H

hardware installation [38](#)
 desktop [38](#)
 rack mounting [38](#)
 hardwired address [188](#)
 High Speed Internet Access
 See HSIA
 Hilton Group Corporation
 Hop Count [165](#)
 host name [56](#)
 hotspot [32](#)
 HSIA [80](#)

I

IANA (Internet Assigned Numbers Authority) [85](#)
 idle timeout [43](#)
 IEEE802.1q VLAN [112](#)
 information window [127](#)
 example [128](#)
 session timeout messages [127](#)
 setup [128](#)

in-room billing [91](#)
 install SSL certificate [208](#)
 installation option [38](#)
 interface [234](#)
 IP Address [165](#)
 IP address [236](#)
 setup [256](#)
 IP address assignment [224](#), [236](#)
 important note [256](#)
 IP address conflicts [236](#)
 scenario 1 [236](#)
 scenario 2 [236](#)
 scenario 3 [237](#)
 scenario 4 [237](#)
 IP address setup [256](#)
 DNS information [258](#), [263](#)
 install components [257](#)
 Macintosh OS 8/9 [263](#)
 Macintosh OS X [265](#)
 verify settings [259](#), [263](#), [266](#)
 Windows 2000/NT/XP [259](#)
 Windows 95/98/Me [256](#)
 IP Static Route [164](#)
 ipconfig [263](#)

L

LAN bandwidth management [144](#)
 LAN device
 accessing via the VSG [190](#)
 management example [162](#)
 port mapping [160](#)
 remote management [160](#), [190](#)
 status [189](#)
 LAN device management [160](#)
 LAN devices [160](#)
 LAN port [40](#)
 cable pin assignment [253](#)
 LAN port, the [253](#)
 local management [40](#)
 Location Identifier [113](#)
 log schedule [171](#)
 login
 subscriber [35](#)
 logs [170](#), [171](#)
 formats [173](#)
 name [172](#)
 time interval [173](#)

M

MAC (Media Access Control) [188](#)
maintenance [35](#)
Management Information Base (MIB) [179](#)
management interface [30, 35](#)
manual firmware upgrade [202](#)
mapping profiles to buttons on the statement printer [104](#)
Maximum Segment Size (MSS) [222](#)
Maximum Transmission Unit (MTU) [221](#)
merchant password [118](#)
MIB [179](#)
monthly account summary [247](#)

N

NAT [34, 74, 160](#)
 Definitions [74](#)
 How it works [75](#)
 on LAN [160](#)
 What it does [75](#)
 What NAT does [75](#)
NAT address pool [78](#)
NAT examples [76](#)
NAT Mapping Types [76](#)
NAT Pool [78](#)
NAT-enabled device [160](#)
navigation panel [43](#)
Network Address Translation
 See NAT
network application [35](#)
 hotel with PMS [36](#)
 Internet access [35](#)
network cable [252](#)
Network Management System (NMS) [179](#)
network statistics [250](#)
NMS [179, 180](#)

O

online glossary [30](#)

P

passthrough [152](#)

 destination URL or IP [154](#)
 subscriber computer IP or MAC [152](#)
 types [152](#)
pin assignment [252](#)
pin assignments [252](#)
PMS [40, 88, 91](#)
 Based on Room [91](#)
 Based on Subscriber [91](#)
 charge modes [91](#)
 connection speed [93](#)
 port-location mapping [91](#)
 type of [92](#)
PMS billing [88](#)
 service selection messages [125](#)
PMS port connector [40](#)
PMS port settings [93](#)
PMS setup [92](#)
PMS transaction [193](#)
PMS transaction messages [193](#)
Point-to-Point Protocol over Ethernet
 See PPPoE
Point-to-Point Tunneling Protocol
 See PPTP
Port Identifier [113](#)
port mapping [161](#)
 application type [161](#)
 port number [161](#)
portal page [148](#)
portal web site [148](#)
Port-Location Mapping [92, 112](#)
 backup [114](#)
 configuring [112](#)
 create mapping [113, 114](#)
 restore [114](#)
power connection [41](#)
power specification [235](#)
PPPoE [33, 219](#)
 connect on demand [220](#)
 idle timeout [220](#)
 keep alive [220](#)
 Redial Period [220](#)
PPTP [33, 220](#)
 connect on demand [221](#)
 connection ID [221](#)
 idle timeout [221](#)
 keep alive [221](#)
 Redial Period [221](#)
print dynamic subscriber account [108](#)
print reports [246](#)
printout preview [106](#)
problems [230](#)
product certifications [235](#)
product registration [7](#)
product specifications [234](#)

- environmental [235](#)
- general [234](#)
- management [235](#)
- performance [235](#)
- physical [235](#)
- Property Management System
 - See PMS

R

- rack mounting installation [38](#)
- rack mounting kit [38](#)
- RADIUS [84](#)
 - accounting methods [81](#)
 - secret key [84](#)
- RADIUS authentication
 - information window [127](#)
- RADIUS server [242](#)
- rear panel [41](#)
- redirect subscriber login screen [122](#)
- registration
 - product [7](#)
- related document [30](#)
- Remote Authentication Dial-In User Service
 - See RADIUS
- report printing on SP-200 [246](#)
 - daily account summary [247](#)
 - initial setup [246](#)
 - key combination [246](#)
 - monthly account summary [247](#)
 - network statistics [250](#)
 - system status [248](#)
- reset [227](#), [231](#)
- reset button [33](#), [40](#)
- reset to the factory defaults [40](#), [47](#)
- restart the VSG [227](#)
- restore configuration file [199](#)
- RFC 1631 [34](#), [74](#)
- RFC2516 [33](#)
- RJ-45 [252](#)

S

- safety warnings [5](#)
- scenario option [85](#)
- scheduled firmware upgrade [204](#)
- Secure Socket Layer [206](#)
 - See SSL
- security [234](#)

- serial console port [253](#)
- server port [160](#)
- server port number [232](#)
- service selection messages [125](#)
- session information [188](#)
 - client computer [188](#)
 - total entries [188](#)
 - update interval [188](#)
- session timeout messages [127](#)
- session trace [176](#)
 - example [177](#)
 - filename convention [177](#)
 - number of records [176](#)
 - setup [176](#)
 - TFTP server [177](#)
- Setting up your computer's IP address [256](#)
- Simple Network Management Protocol (SNMP) [178](#)
- SMT [30](#), [214](#)
 - accessing [214](#)
 - basic configuration [214](#)
 - idle timeout period [215](#)
 - LAN setup [222](#)
 - login [215](#)
 - main menu [216](#)
 - menu overview [215](#)
 - navigating [216](#)
 - navigation keystrokes [217](#)
 - system status [223](#)
 - WAN setup [218](#)
- SNMP [178](#)
 - community [180](#)
 - components [178](#)
 - Get [179](#)
 - GetNext [179](#)
 - management model [178](#)
 - object variables [179](#)
 - overview [178](#)
 - privilege [180](#)
 - protocol operations [179](#)
 - Set [179](#)
 - setup [179](#)
 - Trap [179](#)
 - versions supported [178](#)
- SNMP agent [178](#)
- SNMP manager [178](#)
- SNMP port [180](#)
- SP-200 [246](#)
 - button labels [106](#)
 - creating dynamic accounts [107](#)
 - mapping profiles to buttons [104](#)
 - report printing [246](#)
- specifications [234](#)
- SSL [85](#), [206](#)
 - activate [207](#)
 - certificate [206](#)
 - download certificate to VSG [206](#)

- install certificate [208](#)
- requirement [206](#)
- SSL certificate information [186](#)
- standard subscriber login screen [121](#)
- statement printer [40, 95, 104, 106, 246](#)
- statement printer port [35, 40](#)
- static IP address [219](#)
- static route [34](#)
- Static Routing Topology [164](#)
- static subscriber account [94](#)
 - auto create [96](#)
 - backup [98](#)
 - create [95](#)
 - display [102](#)
 - edit [100](#)
 - global settings [94](#)
 - manual create [97](#)
 - printout preview [101](#)
 - restore [99](#)
- status [184](#)
- subnet [268](#)
- subnet mask [270](#)
- subnetting [270](#)
- subscriber
 - idle-timeout [85](#)
- subscriber account [93](#)
 - backup [98, 109](#)
 - dynamic [93, 104](#)
 - expiration [108](#)
 - printout [129](#)
 - restore [98](#)
 - static [93, 94](#)
 - types [93](#)
- subscriber account first login [103](#)
- subscriber authentication [120](#)
- subscriber database [34](#)
- subscriber login [240](#)
 - information window [240](#)
- subscriber login page [35](#)
- subscriber login screen
 - credit card billing [135](#)
 - customize [120](#)
 - standard [121](#)
- synchronization check file [205](#)
- synchronization file [204, 205](#)
 - example [204](#)
- syntax convention [30](#)
- syslog [170](#)
 - on the LAN [171](#)
 - on the WAN [171](#)
- syslog server [171](#)
- syslog settings [170](#)
- system information [184](#)
- System Management Terminal

- See SMT
- System Management Terminal (SMT) [214](#)
- system name [56](#)
- system reset [33, 40, 47](#)
- system setup [56](#)
- system status [184, 248](#)

T

- TCP/IP components [256](#)
- TCP/IP protocol [257](#)
- TCP/IP settings [256](#)
- TFTP server [205](#)
- throughput [235](#)
- Time to Finish [81, 84](#)
- trademarks [2](#)
- transaction key [118](#)
- trap port [180](#)
- traps [179](#)
- troubleshooting [230](#)
 - console port [231](#)
 - Internet access [232](#)
 - LAN port LEDs [230](#)
 - Power LED [230](#)
 - statement printer [233](#)
 - WAN port LEDs [231](#)
 - Web Configurator [232](#)
 - Web Configurator display [232](#)

U

- uplink port [253](#)
- User Agreement [84](#)

V

- Vendor Specific Attribute [242](#)
 - See VSA
- vendor specific attributes (VSAs) [82](#)
- ventilation [38](#)
- ventilation hole [41](#)
- virtual port [160, 161, 190](#)
- Virtual Private Network [75](#)
- Virtual Private Network (VPN) [33](#)
- VLAN [177](#)
- VLAN-enabled switch [112](#)

VPN

- connection type [34](#)
- single-connection-per-source limitation [76, 78](#)

VSA [82, 85, 242](#)

- format [243](#)
- related error messages [244](#)
- vendor ID [85](#)

VSG

- reset to factory defaults [227](#)

W

walled garden [34, 149](#)

- example [150](#)
- important note [150](#)

WAN port [40](#)

- cable pin assignment [252](#)

WAN port, the [252](#)**warranty**

- note [7](#)

web configurator [35, 42](#)

- configuration menu [44](#)
- idle timeout [43](#)
- menu summary [44](#)
- navigation panel [43](#)
- supported browser [35](#)

web redirect [34](#)**web server port [218](#)****winipcfg [259](#)**