



BCM50a Integrated Router Configuration — Basics

BCM50a
BCM50a Integrated Router

Document Number: **N0115790**

Document Version: **1.0**

Date: **September 2006**

Copyright © Nortel 2005–2006

All rights reserved.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel.

Trademarks

Nortel, Nortel (Logo), the Globemark, and This is the way, This is Nortel (Design mark) are trademarks of Nortel.

Microsoft, MS, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Contents

Preface	27
Before you begin	27
Text conventions	27
Related publications	28
Hard copy technical manuals	28
How to get Help	28
Getting Help from the Nortel Web site	29
Getting Help over the phone from a Nortel Solutions Center	29
Getting Help from a specialist by using an Express Routing Code	29
Getting Help through a Nortel distributor or reseller	30
Chapter 1	
Getting to know your BCM50a Integrated Router	31
Introducing the BCM50a Integrated Router	31
Features	31
Physical features	32
High-speed Internet access	32
ADSL standards	32
Networking compatibility	33
Multiplexing	33
Encapsulation	33
Four-Port switch	33
Autonegotiating 10/100 Mb/s Ethernet LAN	34
Autosensing 10/100 Mb/s Ethernet LAN	34
Time and date	34
Reset button	34
Nonphysical features	34
IPSec VPN capability	34

Nortel Contivity Client Termination	34
Certificates	35
SSH	35
HTTPS	35
Firewall	35
Brute force password guessing protection	35
Content filtering	36
Packet filtering	36
Universal Plug and Play (UPnP)	36
Call scheduling	36
PPPoE	36
Dynamic DNS support	36
IP Multicast	37
IP Alias	37
Central Network Management	37
SNMP	37
Network Address Translation (NAT)	37
Traffic Redirect	38
Port Forwarding	38
DHCP (Dynamic Host Configuration Protocol)	38
Full network management	38
Logging and tracing	38
Upgrade BCM50a Integrated Router Firmware	39
Embedded FTP and TFTP Servers	39
Applications for the BCM50a Integrated Router	39
Secure broadband internet access and VPN	39
Chapter 2	
Introducing the WebGUI	41
WebGUI overview	41
Accessing the BCM50a Integrated Router WebGUI	41
Restoring the factory-default configuration settings	44
Navigating the BCM50a Integrated Router WebGUI	44

Chapter 3	
Wizard setup	47
Wizard overview	47
Encapsulation	47
ENET ENCAP	47
PPP over Ethernet	48
PPPoA	48
RFC 1483	48
Multiplexing	48
VC-based multiplexing	49
LLC-based multiplexing	49
VPI and VCI	49
Wizard setup configuration: first screen	49
IP address and subnet mask	51
IP address assignment	51
IP assignment with PPPoA or PPPoE encapsulation	52
IP assignment with RFC 1483 encapsulation	52
IP assignment with ENET ENCAP encapsulation	52
Private IP addresses	52
Nailed-up connection (only with PPP)	53
NAT	53
Wizard setup configuration: second screen	53
DHCP setup	59
IP pool setup	59
Wizard setup configuration: third screen	59
Wizard setup configuration: connection tests	63
Test your Internet connection	63
Chapter 4	
User Notes	65
General Notes	65
General	65
Firewall	66
NAT	66
VPN Client Termination	66

Security	68
Routing	68
Advanced Router Configuration	68
Setting up the router when the system has a server	69
Connecting two sites to establish a virtual private network	69
Adding IP telephony to a multi-site network	70
Configuring the router to act as a Nortel VPN Server (Client Termination) . . .	71
Configuring the router to connect to a Nortel VPN Server (Client Emulation) .	71
Configuring the router to allow remote management of a LAN-connected BCM50	
71	
Setting up the router for guest access	72
Preventing heavy data traffic from impacting telephone calls	72

Chapter 5

System screens 75

System overview	75
DNS overview	75
Private DNS server	75
Configuring General Setup	76
Dynamic DNS	79
DYNDNS wildcard	79
Configuring Dynamic DNS	79
Configuring Password	81
Predefined NTP time server list	83
Configuring Time and Date	84
ALG	88
Configuring ALG	88

Chapter 6

LAN screens 89

LAN overview	89
DHCP setup	89
IP pool setup	89
DNS servers	90
LAN TCP/IP	90

Factory LAN defaults	90
RIP setup	90
Multicast	91
Configuring IP	92
Configuring Static DHCP	95
Configuring IP Alias	97
Chapter 7	
WAN screens	99
WAN overview	99
TCP/IP Priority (metric)	99
Configuring General	100
PPPoE encapsulation	102
Configuring WAN ISP	103
Configuring WAN IP	105
Traffic redirect	109
Configuring Traffic Redirect	111
Configuring Dial Backup	112
Advanced Modem Setup	117
AT Command Strings	117
DTR Signal	117
Response Strings	117
Configuring Advanced Modem Setup	118
Chapter 8	
Network Address Translation (NAT) Screens	121
NAT overview	121
NAT definitions	121
What NAT does	122
How NAT works	123
Port restricted cone NAT	123
NAT application	124
NAT mapping types	125
Using NAT	126
SUA (Single User Account) versus NAT	126

SUA Server	127
Default server IP address	127
Port forwarding: Services and Port Numbers	128
Configuring servers behind SUA (example)	128
Configuring SUA Server	129
Configuring Address Mapping	131
Trigger Port Forwarding	135
Trigger Port Forwarding example	135
Two points to remember about Trigger Ports	136
Configuring Trigger Port Forwarding	137
Chapter 9	
Static Route screens	139
Static Route overview	139
Configuring IP Static Route	140
Configuring Route entry	142
Chapter 10	
Firewalls	145
Firewall overview	145
Types of firewalls	145
Packet filtering firewalls	146
Application level firewalls	146
Stateful Inspection firewalls	146
Introduction to the BCM50a Integrated Router firewall	147
Denial of Service	148
Basics	148
Types of DoS attacks	149
Stateful inspection	153
Stateful inspection process	154
Stateful inspection and the BCM50a Integrated Router	155
TCP security	156
UDP/ICMP security	157
Upper layer protocols	157
Guidelines for enhancing security with your firewall	158

Packet filtering vs. firewall	158
Packet filtering:	159
When to use filtering	159
Firewall	159
When to use the firewall	160
Chapter 11	
Firewall screens	161
Access methods	161
Firewall policies overview	161
Rule logic overview	163
Rule checklist	163
Security ramifications	163
Key fields for configuring rules	164
Action	164
Service	164
Source address	164
Destination address	164
Connection direction examples	164
LAN to WAN rules	165
WAN to LAN rules	166
Configuring firewall	166
Configuring firewall rules	170
Configuring source and destination addresses	173
Configuring custom ports	174
Example firewall rule	175
Predefined services	178
Alerts	181
Configuring attack alert	182
Threshold values	182
Half-open sessions	182
TCP maximum incomplete and blocking period	183

Chapter 12	
Content filtering	187
Introduction to content filtering	187
Restrict web features	187
Days and Times	187
Configure Content Filtering	188
Chapter 13	
VPN	191
VPN	191
IPSec	191
BCM50a Integrated Router VPN functions	191
VPN screens overview	192
Other terminology	193
Encryption	193
Data confidentiality	193
Data integrity	193
Data origin authentication	193
VPN applications	193
IPSec architecture	194
IPSec algorithms	195
AH (Authentication Header) protocol	196
ESP (Encapsulating Security Payload) protocol	196
Key management	197
Encapsulation	198
Transport mode	198
Tunnel mode	199
IPSec and NAT	199
Secure Gateway Address	200
Dynamic Secure Gateway Address	201
Summary screen	201
Keep Alive	204
Nailed up	204
NAT Traversal	205
NAT Traversal configuration	206

Preshared key	206
Configuring Contivity Client VPN Rule Setup	206
Configuring Advanced Setup	208
ID Type and content	210
ID type and content examples	211
My IP Address	212
Configuring Branch Office VPN Rule Setup	213
Configuring an IP Policy	222
Port forwarding server	228
Configuring a port forwarding server	228
IKE phases	230
Negotiation Mode	232
Preshared key	232
Diffie-Hellman (DH) Key Groups	233
Perfect Forward Secrecy (PFS)	233
Configuring advanced Branch office setup	233
SA Monitor	237
Global settings	239
VPN Client Termination	240
VPN Client Termination IP pool summary	244
VPN Client Termination IP pool edit	246
VPN Client Termination advanced	247
Chapter 14	
Certificates	253
Certificates overview	253
Advantages of certificates	254
Self-signed certificates	254
Configuration summary	255
My Certificates	255
Certificate file formats	258
Importing a certificate	259
Creating a certificate	261
My Certificate details	265
Trusted CAs	269

Importing a Trusted CA certificate	272
Trusted CA Certificate details	273
Trusted remote hosts	277
Verifying a certificate of a trusted remote host	279
Trusted remote host certificate fingerprints	279
Importing a certificate of a trusted remote host	281
Trusted remote host certificate details	282
Directory servers	286
Add or edit a directory server	287

Chapter 15

Bandwidth management 291

Bandwidth management overview	291
Bandwidth classes and filters	292
Proportional bandwidth allocation	292
Application based bandwidth management	292
Subnet based bandwidth management	292
Application and subnet based bandwidth management	293
Reserving bandwidth for nonbandwidth class traffic	293
Configuring summary	294
Configuring class setup	295
Bandwidth Manager Class Configuration	297
Bandwidth management statistics	300
Monitor	302

Chapter 16

Authentication server 303

Introduction to Local User database	303
Local User database	303
Edit Local User Database	305
Current split networks	308
Current split networks edit	309
Configuring RADIUS	311

Chapter 17	
Remote management screens	315
Remote management overview	315
Remote management limitations	315
Remote management and NAT	316
System timeout	316
Introduction to HTTPS	317
Configuring WWW	318
HTTPS example	320
Internet Explorer warning messages	321
Netscape Navigator warning messages	321
Avoiding the browser warning messages	323
Logon screen	324
SSH overview	329
How SSH works	330
SSH implementation on the BCM50a Integrated Router	331
Requirements for using SSH	331
Configuring SSH	331
Secure Telnet using SSH examples	333
Example 1: Microsoft Windows	333
Example 2: Linux	334
Secure FTP using SSH example	335
Telnet	336
Configuring TELNET	337
Configuring FTP	338
Configuring SNMP	339
Supported MIBs	341
SNMP Traps	341
REMOTE MANAGEMENT: SNMP	342
Configuring DNS	343
Configuring Security	344
Chapter 18	
UPnP	347
Universal Plug and Play overview	347

How do I know if I am using UPnP?	347
NAT Traversal	347
Cautions with UPnP	348
UPnP implementation	348
Configuring UPnP	348
Displaying UPnP port mapping	350
Installing UPnP in Windows example	351
Installing UPnP in Windows Me	352
Installing UPnP in Windows XP	353
Using UPnP in Windows XP example	354
Autodiscover Your UPnP-enabled Network Device	355
WebGUI easy access	357
Chapter 19	
Logs Screens	359
Configuring View Log	359
Configuring Log settings	361
Configuring Reports	364
Viewing Web site hits	367
Viewing Protocol/Port	369
Viewing LAN IP address	370
Reports specifications	372
Chapter 20	
Call scheduling screens	373
Call scheduling introduction	373
Call schedule summary	373
Call scheduling edit	375
Applying Schedule Sets to a remote node	377
Chapter 21	
Maintenance	379
Maintenance overview	379
Status screen	379
System statistics	381

DHCP Table screen	383
Diagnostic Screen	384
F/W Upload screen	386
Configuration screen	389
Back to Factory Defaults	389
Backup configuration	390
Restore configuration	390
Restart screen	392
Appendix A	
Troubleshooting	393
Problems Starting Up the BCM50a Integrated Router	393
Problems with the LAN LED	394
Problems with the LAN interface	394
Problems with the WAN interface	395
Problems with Internet access	395
Problems accessing an Internet Web site	396
Problems with the password	396
Problems with the WebGUI	396
Problems with Remote Management	396
Allowing Pop-up Windows, JavaScript and Java Permissions	397
Internet Explorer Pop-up Blockers	397
Allowing Pop-ups	397
Enabling Pop-up Blockers with Exceptions	399
Internet Explorer JavaScript	401
Internet Explorer Java Permissions	403
JAVA (Sun)	404
Netscape Pop-up Blockers	405
Allowing Pop-ups	406
Enable Pop-up Blockers with Exceptions	407
Netscape Java Permissions and JavaScript	409
Appendix B	
Log Descriptions	413
VPN/IPSec Logs	422

VPN Responder IPSec Log	423
Log Commands	431
Configuring what you want the BCM50a Integrated Router to log	431
Displaying Logs	432
Log Command Example	433
Index	435

Figures

Figure 1	Secure Internet Access and VPN Application	40
Figure 2	Login screen	42
Figure 3	Change password screen	43
Figure 4	Replace certificate screen	43
Figure 5	MAIN MENU Screen	45
Figure 6	Contact Support	46
Figure 7	Wizard Screen 1	50
Figure 8	Internet connection with PPPoA	54
Figure 9	Internet connection with RFC 1483	55
Figure 10	Internet connection with ENET ENCAP	56
Figure 11	Internet connection with PPPoE	57
Figure 12	Wizard Screen 3	60
Figure 13	Wizard: LAN configuration	61
Figure 14	Wizard Screen 4	63
Figure 15	Private DNS server example	76
Figure 16	System general setup	77
Figure 17	DDNS	80
Figure 18	Password	82
Figure 19	Time and Date	85
Figure 20	ALG	88
Figure 21	LAN IP	92
Figure 22	Static DHCP	96
Figure 23	IP Alias	97
Figure 24	WAN: General	100
Figure 25	WAN: WAN ISP	103
Figure 26	WAN: IP	106
Figure 27	Traffic Redirect WAN Setup	110
Figure 28	Traffic Redirect LAN Setup	110
Figure 29	Traffic Redirect	111

Figure 30	Dial Backup Setup	113
Figure 31	Advanced Setup	118
Figure 32	How NAT works	123
Figure 33	Port Restricted Cone NAT	124
Figure 34	NAT application with IP Alias	125
Figure 35	Multiple servers behind NAT example	129
Figure 36	SUA/NAT setup	130
Figure 37	Address Mapping	132
Figure 38	Address Mapping edit	134
Figure 39	Trigger Port Forwarding process: example	136
Figure 40	Trigger Port	137
Figure 41	Example of Static Routing topology	140
Figure 42	Static Route screen	141
Figure 43	Edit IP Static Route	142
Figure 44	BCM50a Integrated Router firewall application	148
Figure 45	Three-way handshake	150
Figure 46	SYN flood	151
Figure 47	Smurf attack	152
Figure 48	Stateful inspection	154
Figure 49	LAN to WAN traffic	166
Figure 50	WAN to LAN traffic	166
Figure 51	Enabling the firewall	168
Figure 52	Creating and editing a firewall rule	171
Figure 53	Adding or editing source and destination addresses	173
Figure 54	Creating or editing a custom port	174
Figure 55	Firewall edit rule screen example	175
Figure 56	Firewall rule edit IP example	176
Figure 57	Edit custom port example	176
Figure 58	MyService rule configuration example	177
Figure 59	My Service example rule summary	178
Figure 60	Attack alert	184
Figure 61	Content filter	188
Figure 62	Encryption and decryption	193
Figure 63	IPSec architecture	195
Figure 64	Transport and Tunnel mode IPSec encapsulation	198

Figure 65	IPSec summary fields	201
Figure 66	Summary	202
Figure 67	NAT router between IPSec routers	205
Figure 68	VPN Contivity Client rule setup	207
Figure 69	VPN Contivity Client advanced rule setup	209
Figure 70	VPN Branch Office rule setup	214
Figure 71	VPN Branch Office — IP Policy	223
Figure 72	VPN Branch Office — IP Policy - Port Forwarding Server	229
Figure 73	Two phases to set up the IPSec SA	231
Figure 74	VPN Branch Office advanced rule setup	234
Figure 75	VPN SA Monitor	238
Figure 76	VPN Global Setting	239
Figure 77	VPN Client Termination	241
Figure 78	VPN Client Termination IP pool summary	245
Figure 79	VPN Client Termination IP pool edit	246
Figure 80	VPN Client Termination advanced	248
Figure 81	Certificate configuration overview	255
Figure 82	My Certificates	256
Figure 83	My Certificate Import	260
Figure 84	My Certificate create	262
Figure 85	My Certificate details	266
Figure 86	Trusted CAs	270
Figure 87	Trusted CA import	272
Figure 88	Trusted CA details	274
Figure 89	Trusted remote hosts	278
Figure 90	Remote host certificates	280
Figure 91	Certificate details	280
Figure 92	Trusted remote host import	281
Figure 93	Trusted remote host details	283
Figure 94	Directory servers	286
Figure 95	Directory server add	288
Figure 96	Subnet based bandwidth management example	293
Figure 97	Bandwidth Manager: Summary	294
Figure 98	Bandwidth Manager: Class setup	296
Figure 99	Bandwidth Manager: Edit class	298

Figure 100	Bandwidth management statistics	301
Figure 101	Bandwidth manager monitor	302
Figure 102	Local User database	304
Figure 103	Local User database edit	306
Figure 104	Current split networks	308
Figure 105	Current split networks edit	310
Figure 106	RADIUS	312
Figure 107	HTTPS implementation	318
Figure 108	WWW	319
Figure 109	Security Alert dialog box (Internet Explorer)	321
Figure 110	Figure 18-4 Security Certificate 1 (Netscape)	322
Figure 111	Security Certificate 2 (Netscape)	323
Figure 112	Logon screen (Internet Explorer)	325
Figure 113	Login screen (Netscape)	326
Figure 114	Replace certificate	327
Figure 115	Device-specific certificate	328
Figure 116	Common BCM50a Integrated Router certificate	329
Figure 117	SSH Communication Example	330
Figure 118	How SSH Works	330
Figure 119	SSH	332
Figure 120	SSH Example 1: Store Host Key	333
Figure 121	SSH Example 2: Test	334
Figure 122	SSH Example 2: Log on	335
Figure 123	Secure FTP: Firmware Upload Example	336
Figure 124	Telnet configuration on a TCP/IP network	336
Figure 125	Telnet	337
Figure 126	FTP	338
Figure 127	SNMP Management Model	340
Figure 128	SNMP	342
Figure 129	DNS	344
Figure 130	Security	345
Figure 131	Configuring UPnP	349
Figure 132	UPnP Ports	350
Figure 133	Add/Remove programs: Windows setup	352
Figure 134	Communications	353

Figure 135	Network connections	353
Figure 136	Windows optional networking components wizard	354
Figure 137	Windows XP networking services	354
Figure 138	Internet gateway icon	355
Figure 139	Internet connection properties	355
Figure 140	Internet connection properties advanced setup	356
Figure 141	Service settings	356
Figure 142	Internet connection icon	357
Figure 143	Internet connection status	357
Figure 144	Network connections	358
Figure 145	My Network Places: Local network	358
Figure 146	View Log	360
Figure 147	Log settings	362
Figure 148	Reports	366
Figure 149	Web site hits report example	368
Figure 150	Protocol/Port report example	369
Figure 151	LAN IP address report example	371
Figure 152	Call schedule summary	374
Figure 153	Call schedule edit	375
Figure 154	System Status	380
Figure 155	System Status: Show statistics	382
Figure 156	DHCP Table	384
Figure 157	Diagnostic	385
Figure 158	Firmware upload	387
Figure 159	Firmware Upload In Process	388
Figure 160	Network Temporarily Disconnected	388
Figure 161	Firmware upload error	388
Figure 162	Configuration	389
Figure 163	Reset warning message	390
Figure 164	Configuration Upload Successful	391
Figure 165	Network Temporarily Disconnected	391
Figure 166	Restart screen	392
Figure 167	Pop-up Blocker	398
Figure 168	Internet Options	399
Figure 169	Internet options	400

Figure 170	Pop-up Blocker settings	401
Figure 171	Internet options	402
Figure 172	Security Settings - Java Scripting	403
Figure 173	Security Settings - Java	404
Figure 174	Java (Sun)	405
Figure 175	Allow Popups from this site	406
Figure 176	Netscape Search Toolbar	406
Figure 177	Popup Windows	407
Figure 178	Popup Windows	408
Figure 179	Allowed Sites	409
Figure 180	Advanced	410
Figure 181	Scripts & Plug-ins	411
Figure 182	Example VPN Initiator IPSec Log	423
Figure 183	Example VPN Responder IPSec Log	424

Tables

Table 1	Feature specifications	31
Table 2	Wizard Screen 1	50
Table 3	Internet connection with PPPoA	54
Table 4	Internet connection with RFC 1483	55
Table 5	Internet connection with ENET ENCAP	56
Table 6	Internet connection with PPPoE	58
Table 7	Wizard: LAN configuration	61
Table 8	System general setup	77
Table 9	DDNS	80
Table 10	Password	82
Table 11	Default Time Servers	84
Table 12	Time and Date	86
Table 13	ALG	88
Table 14	LAN IP	93
Table 15	Static DHCP	96
Table 16	IP Alias	98
Table 17	WAN: General	101
Table 18	WAN: WAN ISP	104
Table 19	WAN: IP	107
Table 20	Traffic Redirect	111
Table 21	Dial Backup Setup	114
Table 22	Advanced Setup	119
Table 23	NAT definitions	122
Table 24	NAT mapping type	126
Table 25	Services and port numbers	128
Table 26	SUA/NAT setup	130
Table 27	Address Mapping	132
Table 28	Address Mapping edit	134
Table 29	Trigger Port	138

Table 30	IP Static Route summary	141
Table 31	Edit IP Static Route	142
Table 32	Common IP ports	149
Table 33	ICMP commands that trigger alerts	152
Table 34	Legal NetBIOS commands	152
Table 35	Legal SMTP commands	153
Table 36	Firewall rules summary: First screen	168
Table 37	Creating and editing a firewall rule	171
Table 38	Adding or editing source and destination addresses	173
Table 39	Creating/Editing A Custom Port	174
Table 40	Predefined services	179
Table 41	Attack alert	184
Table 42	Content filter	189
Table 43	VPN Screens Overview	192
Table 44	AH and ESP	197
Table 45	VPN and NAT	200
Table 46	Summary	203
Table 47	VPN Contivity Client rule setup	207
Table 48	VPN Contivity Client advanced rule setup	209
Table 49	Local ID type and content fields	211
Table 50	Peer ID type and content fields	211
Table 51	Matching ID type and content configuration example	212
Table 52	Mismatching ID Type and Content Configuration Example	212
Table 53	VPN Branch Office rule setup	215
Table 54	VPN Branch Office — IP Policy	224
Table 55	VPN Branch Office — IP Policy - Port Forwarding Server	229
Table 56	VPN Branch Office Advanced Rule Setup	234
Table 57	VPN SA Monitor	238
Table 58	VPN Global Setting	239
Table 59	VPN Client Termination	242
Table 60	VPN Client Termination IP pool summary	245
Table 61	VPN Client Termination IP pool edit	246
Table 62	VPN Client Termination advanced	249
Table 63	My Certificates	257
Table 64	My Certificate Import	260

Table 65	My Certificate create	263
Table 66	My Certificate details	267
Table 67	Trusted CAs	270
Table 68	Trusted CA import	272
Table 69	Trusted CA details	275
Table 70	Trusted Remote Hosts	278
Table 71	Trusted remote host import	282
Table 72	Trusted remote host details	284
Table 73	Directory Servers	287
Table 74	Directory server add	288
Table 75	Application and Subnet based Bandwidth Management Example	293
Table 76	Bandwidth Manager: Summary	294
Table 77	Bandwidth Manager: Class Setup	296
Table 78	Bandwidth Manager: Edit class	298
Table 79	Services and port numbers	300
Table 80	Bandwidth management statistics	301
Table 81	Bandwidth manager monitor	302
Table 82	Local User database	304
Table 83	Local User database edit	307
Table 84	Current split networks	309
Table 85	Current split networks edit	310
Table 86	RADIUS	312
Table 87	WWW	319
Table 88	SSH	332
Table 89	Telnet	337
Table 90	FTP	338
Table 91	SNMP traps	341
Table 92	SNMP	342
Table 93	DNS	344
Table 94	Security	345
Table 95	Configuring UPnP	349
Table 96	UPnP Ports	350
Table 97	View Log	360
Table 98	Log settings	363
Table 99	Reports	366

Table 100	Web site hits report	368
Table 101	Protocol/ Port Report	370
Table 102	LAN IP Address Report	371
Table 103	Report Specifications	372
Table 104	Call Schedule Summary	374
Table 105	Call schedule edit	376
Table 106	System Status	380
Table 107	System Status: Show Statistics	382
Table 108	DHCP Table	384
Table 109	Diagnostic	385
Table 110	Firmware Upload	387
Table 111	Restore configuration	390
Table 112	Troubleshooting the Start-Up of your BCM50a Integrated Router	393
Table 113	Troubleshooting the LAN LED	394
Table 114	Troubleshooting the LAN interface	394
Table 115	Troubleshooting the WAN Interface	395
Table 116	Troubleshooting Internet access	395
Table 117	Troubleshooting Web Site Internet Access	396
Table 118	Troubleshooting the password	396
Table 119	Troubleshooting Remote Management	396
Table 120	System Error Logs	413
Table 121	System Maintenance Logs	413
Table 122	UPnP Logs	414
Table 123	Content Filtering Logs	414
Table 124	Attack Logs	414
Table 125	Access Logs	416
Table 126	ACL Setting Notes	421
Table 127	ICMP Notes	421
Table 128	Sys log	422
Table 129	Sample IKE Key Exchange Logs	425
Table 130	Sample IPSec Logs During Packet Transmission	427
Table 131	RFC 2408 ISAKMP Payload Types	428
Table 132	PKI Logs	428
Table 133	Certificate Path Verification Failure Reason Codes	430
Table 134	Log categories and available settings	431

Preface

Before you begin

This guide assists you through the basic configuration of your BCM50a Integrated Router for its various applications.



Note: This guide explains how to use the WebGUI to configure your BCM50a Integrated Router. See for how to use the System Management Terminal (SMT) or the command interpreter interface to configure your BCM50a Integrated Router. Not all features can be configured through all interfaces.

The WebGUI parts of this guide contain background information on features configurable by the WebGUI and the SMT. For features not configurable by the WebGUI, only background information is provided.

Text conventions

This guide uses the following text conventions:

Enter means type one or more characters and press the enter key. Select or Choose means use one of the predefined choices.

The SMT menu titles and labels are written in **Bold Times New Roman** font.

The choices of a menu choices are written in **Bold Arial** font.

A single keystroke is written in Arial font and enclosed in square brackets. For instance, [ENTER] means the Enter key; [ESC] means the escape key and [SPACE BAR] means the space bar. [UP] and [DOWN] are the up and down arrow keys.

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**.

Related publications

- For more information about using the BCM50a Integrated Router, refer to the following publications: *BCM50a Integrated Router Configuration — Advanced* (N0115789)

This guide covers how to use the SMT menu to configure your BCM50a Integrated Router.

- *WebGUI Online Help*

Embedded WebGUI help is available to provide descriptions of individual screens and supplementary information.

Hard copy technical manuals

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/documentation. Find the product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of Adobe Reader.

How to get Help

This section explains how to get help for Nortel products and services.

Getting Help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. More specifically, the site enables you to:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting Help over the phone from a Nortel Solutions Center

If you don't find the information you require on the Nortel Technical Support Web site, and have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following Web site to obtain the phone number for your region:

www.nortel.com/callus

Getting Help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting Help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

Chapter 1

Getting to know your BCM50a Integrated Router

This chapter introduces the main features and applications of the BCM50a Integrated Router.

Introducing the BCM50a Integrated Router

The BCM50a Integrated Router is an ideal secure gateway for all data passing between the Internet and the Local Area Network (LAN).

Your BCM50a Integrated Router integrates high-speed 10/100 Megabits per second (Mb/s) autonegotiating LAN interfaces and a high-speed Asymmetrical Digital Subscriber Line Plus (ADSL2+) port into a single package. The BCM50a Integrated Router is ideal for high-speed Internet browsing and making LAN-to-LAN connections to remote networks. By integrating Digital Subscriber Line (DSL) and Network Address Translation (NAT), the BCM50a Integrated Router provides easy installation and Internet access. By integrating firewall and Virtual Private Network (VPN) capabilities, the BCM50a Integrated Router is a complete security solution that protects your Intranet and efficiently manages data traffic on your network.

Features

This section lists the key features of the BCM50a Integrated Router.

Table 1 Feature specifications

Feature	Specification
Number of static routes	12
Number of NAT sessions	4096

Table 1 Feature specifications

Feature	Specification
Number of SUA (Single User Account) servers	12
Number of address mapping rules	10
Number of configurable VPN rules (gateway policies)	10
Number of configurable IPsec VPN IP policies (network policies)	60
Number of concurrent IKE (Internet Key Exchange) Phase 1 Security Associations: These correspond to the gateway policies.	10
Number of concurrent IPsec VPN tunnels (Phase 2 Security Associations): These correspond to the network policies and are also monitorable and manageable. For example, 5 IKE gateway policies could each use 12 IPsec tunnels for a total of 60 phase 2 IPsec VPN tunnels. This total includes both branch office tunnels and VPN client-termination tunnels.	60
Number of IP pools that can be used to assign IP addresses to remote users for VPN client termination	3
Number of configurable split networks for VPN client termination	16
Number of configurable inverse split networks for VPN client termination	16
Number of configurable subnets per split network for VPN client termination	64

Physical features

High-speed Internet access

Your BCM50a Integrated Router supports ADSL2+ (Asymmetrical Digital Subscriber Line) for high transmission speeds and long connection distances.

ADSL standards

- Multimode standard (ANSI (American National Standards Institute) T1.413, Issue 2; G.dmt (G.992.1 Discrete Multitone Modulation)
- EOC (Embedded Operations Channel) specified in ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union) G.992.1
- ADSL2 G.dmt.bis (G.992.3)
- ADSL2+ (G.992.5)

- Extended-reach ADSL (ER ADSL)
- SRA (Seamless Rate Adaptation)
- Autonegotiating rate adaptation
- ADSL physical connection ATM (Asynchronous Transfer Mode) AAL5 (Adaptation Layer type 5)
- Multiprotocol over AAL5 (Request For Comments (RFC) 2684/1483)
- Support Point-to-Point-Protocol over ATM AAL5 (PPPoA) (RFC 2364)
- PPP over Ethernet support for DSL (Digital Subscriber Line) connection (RFC 2516)
- Support Virtual Circuit (VC) based and LLC (Logical Link Control) based multiplexing
- Support OAM (Operational, Administration and Maintenance) VC Hunt
- I.610 F4/F5 OAM

Networking compatibility

Your BCM50a Integrated Router is compatible with the major ADSL Digital Subscriber Line Access Multiplexer (DSLAM) providers, making configuration as simple as possible.

Multiplexing

The BCM50a Integrated Router supports VC-based and LLC-based multiplexing.

Encapsulation

The BCM50a Integrated Router supports PPPoA (RFC 2364 - PPP over ATM Adaptation Layer 5), RFC 1483 encapsulation over ATM, MAC (Media Access Control) encapsulated routing (ENET encapsulation) as well as PPP over Ethernet (RFC 2516).

Four-Port switch

A combination of switch and router makes your BCM50a Integrated Router a cost-effective and viable network solution. You can connect up to four computers or phones to the BCM50a Integrated Router without the cost of a switch. Use a switch to add more than four computers or phones to your LAN.

Autonegotiating 10/100 Mb/s Ethernet LAN

The LAN interfaces automatically detect if they are on a 10 or a 100 Mb/s Ethernet.

Autosensing 10/100 Mb/s Ethernet LAN

The LAN interfaces automatically adjust to either a crossover or straight through Ethernet cable.

Time and date

Using the BCM50a Integrated Router, you can get the current time and date from an external server when you turn on your BCM50a Integrated Router. You can also set the time manually.

Reset button

There is a 'Cold Reset Router' button that is accessible from the Element Manager Administration/Utilities/Reset page. Use this button to restore the factory default password to setup and the IP address to 192.168.1.1, subnet mask 255.255.255.0, and DHCP server enabled with a pool of 126 IP addresses starting at 192.168.1.2.

Nonphysical features

IPSec VPN capability

Establish Virtual Private Network (VPN) tunnels to connect home or office computers to your company network using data encryption and the Internet; thus providing secure communications without the expense of leased site-to-site lines. VPN is based on the IPSec standard and is fully interoperable with other IPSec-based VPN products.

Nortel Contivity Client Termination

The BCM50a Integrated Router supports VPN connections from computers using Nortel Contivity VPN Client 3.0, 5.01, 5.11, 6.01, 6.02, or 7.01 software.

Certificates

The BCM50a Integrated Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. Certificates provide a way to exchange public keys for use in authentication.

SSH

The BCM50a Integrated Router uses the SSH (Secure Shell) secure communication protocol to provide secure encrypted communication between two hosts over an unsecured network.

HTTPS

HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL is a web protocol that encrypts and decrypts web sessions. Use HTTPS for secure WebGUI access to the BCM50a Integrated Router.

Firewall

The BCM50a Integrated Router has a stateful inspection firewall with DoS (Denial of Service) protection. By default, when the firewall is activated, all incoming traffic from the WAN (Wide Area Network) to the LAN is blocked unless it is initiated from the LAN. The BCM50a Integrated Router firewall supports TCP/UDP inspection, DoS detection and protection, real time alerts, reports and logs.

Brute force password guessing protection

The BCM50a Integrated Router has a special protection mechanism to discourage brute force password guessing attacks on the BCM50a Integrated Router management interfaces. You can specify a wait time that must expire before you can enter a fourth password after entering three incorrect passwords.

Content filtering

The BCM50a Integrated Router can block web features such as ActiveX controls, Java applets, and cookies, as well as disable web proxies. The BCM50a Integrated Router can block specific URLs by using the keyword feature. The administrator can also define time periods and days during which content filtering is enabled.

Packet filtering

The packet filtering mechanism blocks unwanted traffic from entering or leaving your network.

Universal Plug and Play (UPnP)

Using the standard TCP/IP protocol, the BCM50a Integrated Router and other UPnP-enabled devices can dynamically join a network, obtain an IP address, and convey its capabilities to other devices on the network.

Call scheduling

Configure call time periods to restrict and allow access for users on remote nodes.

PPPoE

PPPoE facilitates the interaction of a host with an Internet modem to achieve access to high-speed data networks through a familiar dial-up networking user interface.

Dynamic DNS support

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

IP Multicast

The BCM50a Integrated Router can use IP multicast to deliver IP packets to a specific group of hosts. IGMP (Internet Group Management Protocol) is the protocol used to support multicast groups. The BCM50a Integrated Router supports versions 1 and 2.

IP Alias

Using IP Alias, you can partition a physical network into logical networks over the same Ethernet interface. The BCM50a Integrated Router supports three logical LAN interfaces through its single physical Ethernet LAN interface with the BCM50a Integrated Router itself as the gateway for each LAN network.

Central Network Management

With Central Network Management (CNM), an enterprise or service provider network administrator can manage your BCM50a Integrated Router. The enterprise or service provider network administrator can configure your BCM50a Integrated Router, perform firmware upgrades, and do troubleshooting for you.

SNMP

SNMP (Simple Network Management Protocol) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your BCM50a Integrated Router supports SNMP agent functionality, which means that a manager station can manage and monitor the BCM50a Integrated Router through the network. The BCM50a Integrated Router supports SNMP versions 1 and 2 (SNMPv1 and SNMPv2).

Network Address Translation (NAT)

NAT (Network Address Translation — NAT, RFC 1631) translate multiple IP addresses used within one network to different IP addresses known within another network.

Traffic Redirect

Traffic Redirect forwards WAN traffic to a backup gateway when the BCM50a Integrated Router cannot connect to the Internet, thus acting as an auxiliary backup when your regular WAN connection fails.

Port Forwarding

Use this feature to forward incoming service requests to a server on your local network. You can enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server.

DHCP (Dynamic Host Configuration Protocol)

With DHCP (Dynamic Host Configuration Protocol), individual client computers can obtain the TCP/IP configuration at start-up from a centralized DHCP server. The BCM50a Integrated Router has built in DHCP server capability, enabled by default, which means it can assign IP addresses, an IP default gateway, and DNS servers to all systems that support the DHCP client. The BCM50a Integrated Router can also act as a surrogate DHCP server, where it relays IP address assignment from another DHCP server to the clients.

Full network management

The embedded web configurator is an all platform, web based utility that you can use to easily manage and configure the BCM50a Integrated Router. Most functions of the BCM50a Integrated Router are also software configurable through the SMT (System Management Terminal) interface. The SMT is a menu driven interface that you can access over a Telnet connection.

Logging and tracing

The BCM50a Integrated Router supports the following logging and tracing functions to help with management:

- Built in message logging and packet tracing
- Unix syslog facility support

Upgrade BCM50a Integrated Router Firmware

The firmware of the BCM50a Integrated Router can be upgraded manually through the WebGUI.

Embedded FTP and TFTP Servers

The embedded FTP and TFTP servers enable fast firmware upgrades, as well as configuration file backups and restoration.

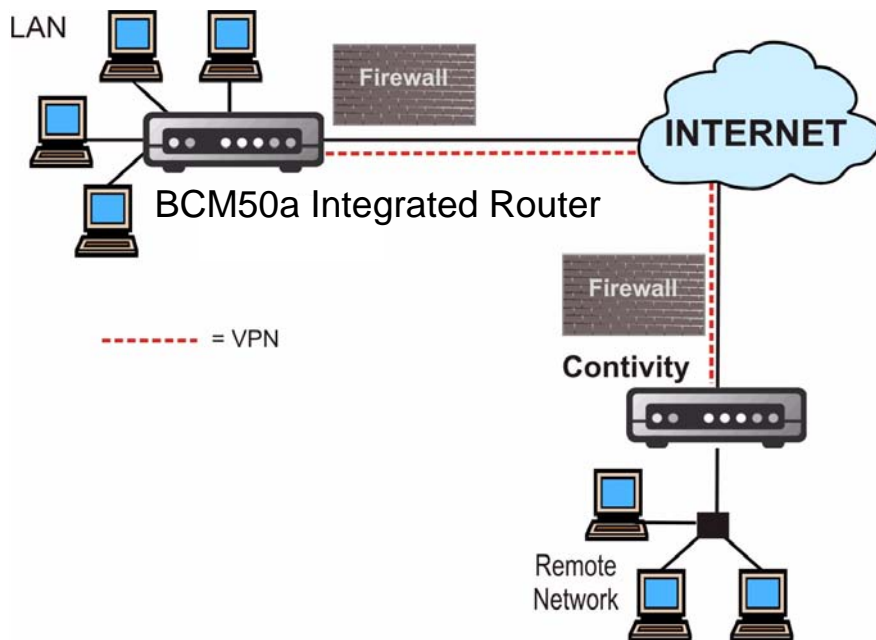
Applications for the BCM50a Integrated Router

Secure broadband internet access and VPN

The BCM50a Integrated Router provides broadband Internet access through ADSL. The BCM50a Integrated Router also provides IP address sharing and a firewall protected local network with traffic management.

The BCM50a Integrated Router VPN is an ideal, cost effective way to connect branch offices and business partners over the Internet without the need (and expense) of leased lines between sites. The LAN computers can share the VPN tunnels for secure connections to remote computers.

Figure 1 Secure Internet Access and VPN Application



Caution: Electro-static Discharge can disrupt the router. Use appropriate handling precautions to avoid ESD. Avoid touching the connectors on the router, particularly when it is in use.

Chapter 2

Introducing the WebGUI

This chapter describes how to access the BCM50a Integrated Router WebGUI and provides an overview of its screens.

WebGUI overview

There are two methods to access the WebGUI for the BCM50a Integrated Router. It can be launched from Element Manager or can be launched from a web browser on the same subnet as the router.

Use Internet Explorer 6.0 and later or Netscape Navigator 7.0 and later versions. The recommended screen resolution is 1 024 by 768 pixels.

In order to use the WebGUI you need to allow:

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

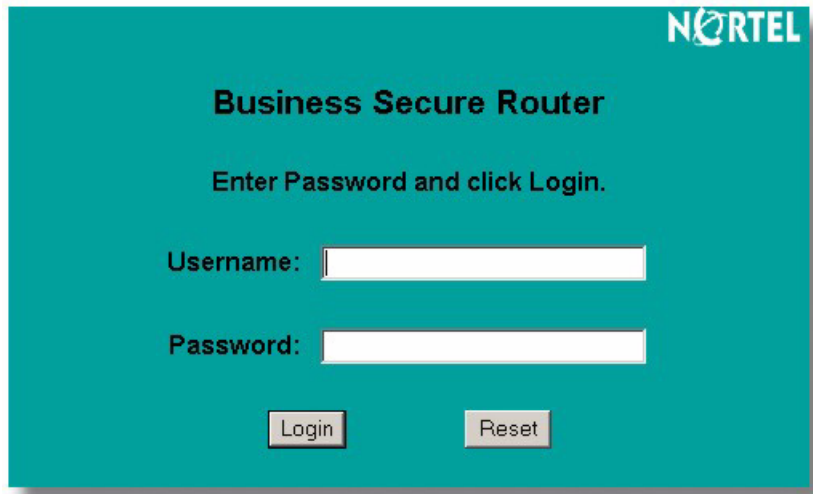
See [“Allowing Pop-up Windows, JavaScript and Java Permissions”](#) on page 397 if you want to make sure these functions are allowed in Internet Explorer.

Accessing the BCM50a Integrated Router WebGUI

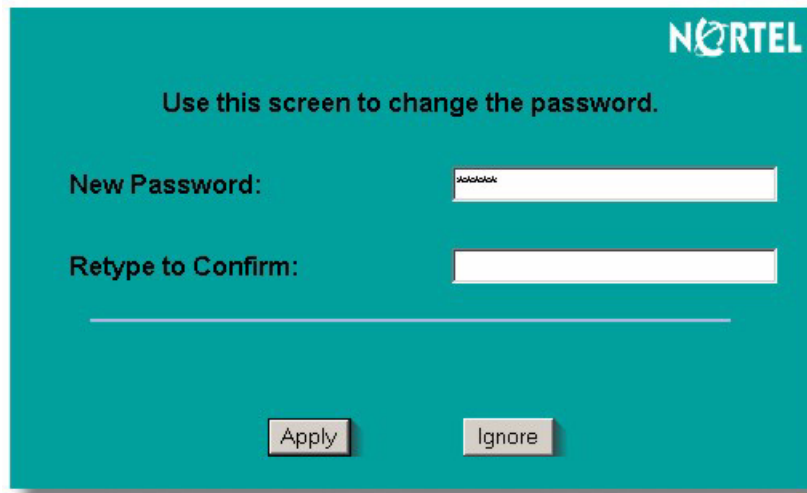
Make sure your BCM50a Integrated Router hardware is properly connected and prepare your computer and computer network to connect to the BCM50a Integrated Router

- 1 Launch your web browser.
- 2 Type 192.168.1.1 as the URL.
- 3 Type the username (“nnadmin” is the default) and the password (“PlsChgMe!” is the default) and click **Login**. Click **Reset** to clear any information you have entered in the **Username** and **Password** fields.

Figure 2 Login screen



- 4 A screen asking you to change your password (highly recommended) appears and is shown in [Figure 3](#). Type a new password (and retype it to confirm) and click **Apply** or click **Ignore**.

Figure 3 Change password screen

Use this screen to change the password.

New Password:

Retype to Confirm:

Apply Ignore

- 5 Click **Apply** in the **Replace Certificate** screen to create a certificate using your BCM50a Integrated Router MAC address that is specific to this device.

Figure 4 Replace certificate screen

Replace Factory Default Certificate

The factory default certificate is common to Business Secure Router series models. Click Apply to create a certificate using your Business Secure Router 's MAC address that will be specific to this device.

Apply Ignore

The **MAIN MENU** screen appears.



Note: The management session automatically times out when the time period set in the Administrator Inactivity Timer field expires (default five minutes). Simply log back on to the BCM50a Integrated Router if this happens to you.

Restoring the factory-default configuration settings

If you forget your password or cannot access the SMT menu, you will need to restore the factor-default configuration. This means that you will lose all configurations that you had previously. The password will be reset to “PlsChgMe!”.

Use one of the following ways to perform a reset on the BCM50a Integrated Router:

- 1 Router WebGUI LineFeed LAN access is required. Navigate to the Maintenance screen and select the Reset button.
- 2 Element Manager LineFeed. Navigate to the Administration screen, Utilities, Reset select the Router Cold Reset.

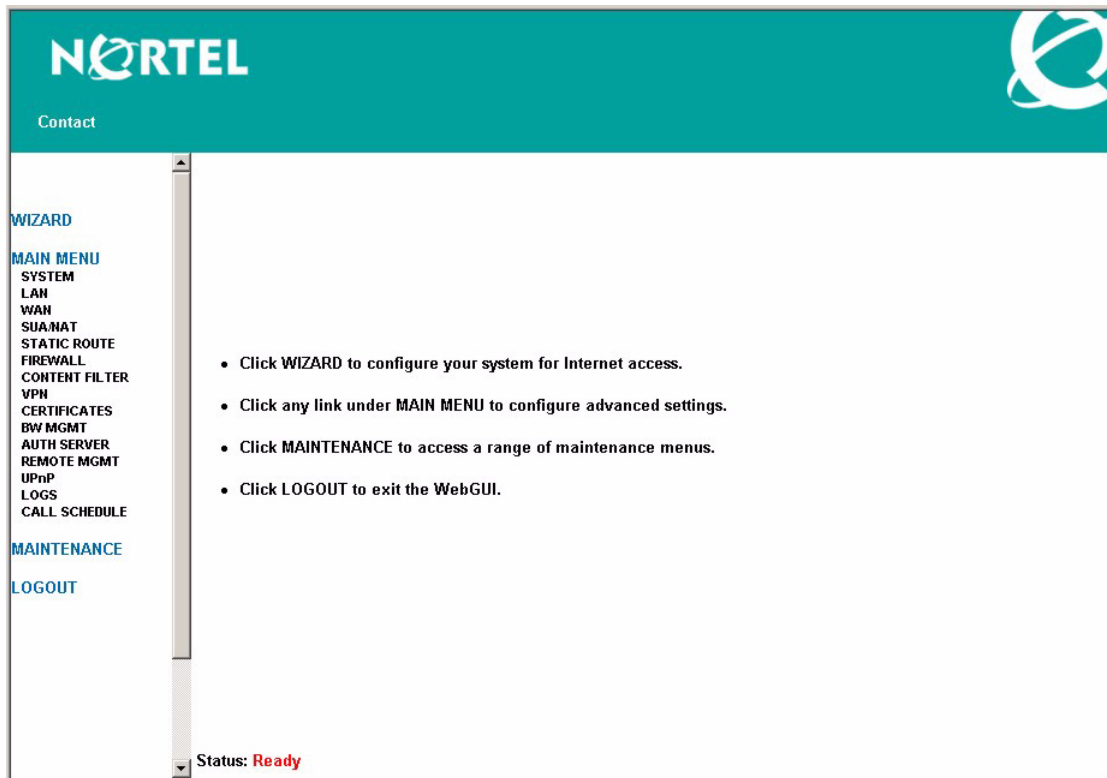
Navigating the BCM50a Integrated Router WebGUI

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



Note: The help icon does not appear in the MAIN MENU screen.

Figure 5 MAIN MENU Screen



Click the **Contact** link to display the customer support contact information. Figure 7 is a sample of what displays.

Figure 6 Contact Support

Contact
NORTEL NETWORKS

Technical Support Contact Numbers:

USA and Canada

Authorized Distributors - Nortel Networks Global Networks Technical Support (NNTS)
 Telephone: 1-800-4NORTEL (1-800-466-7833)
 If you already have a FDI Code, you can enter Express Routing Code (ERC) 196W.
 If you do not yet have a FDI Code, or for general questions and first line support, you can enter ERC 330W

Pre-sales Support (CSA7)
 Telephone: 1-800-4NORTEL (1-800-466-7833)
 Use Express Routing Code (ERC) 1063W

EMEA (Europe, Middle East, Africa)

Country/Call Center	Phone Number
European Freephone	00000.0000.9009
European Alternative	+44 (0)870.907.9009
Africa	+27.11.300.4000
Israel	800.945.9779
United Kingdom	+44 (0)870.907.9009

*Note: Calls are not free from all countries in Europe, Middle East and Africa

CALA (Caribbean & Latin America)

Country/Call Center	Phone Number
Anguilla	1-919-903-4211
Antigua	1-8003270797
Argentina	1-919-903-4211
Aruba	1-919-903-4211
Bahamas	1-866-291-1737
Barbados	1-800-5342119
Belize	1-919-903-4211
Bermuda	1-866-291-1737
Bolivia	1-919-903-4211
Bonaire	1-919-903-4211
Brazil	00014.550.4189
BVI	1-919-903-4211
Cayman Islands	1-866-291-1737
Chile	1230-020-3016
Colombia	01800.915.5093
Costa Rica	0-800-012-1039
Cuba	1-919-903-4211
Dominica	1-919-903-4211
Dominican Republic	1-888-136-1837
Ecuador	1-919-903-4211
El Salvador	1-919-903-4211
Guatemala	1-919-903-4211
Guatemala	1-919-903-4211
Honduras	1-866-291-1737
Haiti	1-919-903-4211
Honduras	1-919-903-4211
Mexico	001-866-291-1737
Montserrat	1-919-903-4211
Nicaragua	001-800-220-1152
Panama	001-800-507-1567
Paraguay	1-919-903-4211
Peru	0000.50755
Puerto Rico	1-800-484rtx*(1-800-466-7833)
St. Kitts & Nevis	1-866-291-1737
St. Lucia	1-866-291-1737
St. Maarten	1-919-903-4211
St. Thomas	1-800-484rtx*(1-800-466-7833)
St. Vincent	1-866-291-1737
Surinam	1-919-903-4211
Tinidad & Tobago	1-8003270797
Turks & Caicos Islands	1-866-291-1737
Uruguay	000-413-595-2271
US Virgin Islands	1-800-484rtx*(1-800-466-7833)
Venezuela	0000-1-00-2721

APAC (Asia Pacific)

Country/Call Center	Phone Number
Australia	1-800-Nortel (1-800-667833)
China	800 810 3000 or 86-10-6510 7770
Hong Kong	800 96 4199
India	491.11.51.34.2210
Indonesia	0018 036 1004
Japan	0120-332-533
South Korea	0079 8611 2001
Malaysia	1 800 805 300
New Zealand	0 800 449 716
Philippines	+63-2-385-3561
Singapore	800 616 2004
Taiwan	0800 810 300
Thailand	001 800 611 3007
All Other Countries	+61 2 8870 8800

Chapter 3

Wizard setup

This chapter provides information on the Wizard screens in the WebGUI.

Wizard overview

The setup wizard in the WebGUI helps you configure your device to access the Internet. The second screen has three variations, depending on which encapsulation type you use. Refer to your ISP checklist in the *Nortel BCM50a Integrated Router 252 — Fundamentals* (NN47923-301) to know what to enter in each field. Leave a field blank if you do not have the required information.

Encapsulation

Be sure to use the encapsulation method required by your ISP. The BCM50a Integrated Router supports the following methods.

ENET ENCAP

The MAC Encapsulated Routing Link Protocol (ENET ENCAP) is only implemented with the IP network protocol. IP packets are routed between the Ethernet interface and the WAN interface and then formatted so that they can be understood in a bridged environment. For instance, the BCM50a Integrated Router encapsulates routed Ethernet frames into bridged ATM cells. ENET ENCAP requires that you specify a gateway IP address in the **ENET ENCAP Gateway** field in the second wizard screen. You can get this information from your ISP.

PPP over Ethernet

PPP over Ethernet (PPPoE) provides access control and billing functionality in a manner similar to dial-up services using PPP. The BCM50a Integrated Router bridges a PPP session over Ethernet (PPP over Ethernet, RFC 2516) from your computer to an ATM (Asynchronous Transfer Mode) PVC (Permanent Virtual Circuit), which connects to an ADSL Access Concentrator where the PPP session terminates. One PVC can support any number of PPP sessions from your LAN. For more information about PPPoE, see the PPPoE appendix in the *BCM50a Integrated Router Configuration — Advanced* guide.

PPPoA

A Point to Point Protocol over ATM Adaptation Layer 5 (PPPoA) connection functions like a dial-up Internet connection. The BCM50a Integrated Router encapsulates the PPP session based on RFC 1483 and sends it through an ATM PVC (Permanent Virtual Circuit) to the Internet Service Provider (ISP) DSLAM (Digital Subscriber Line Access Multiplexer). For more information about PPPoA, refer to RFC 2364. For more information about PPP, refer to RFC 1661.

RFC 1483

RFC 1483 describes two methods for Multiprotocol Encapsulation over ATM Adaptation Layer 5 (AAL5). Using the first method, you can multiplex multiple protocols over a single ATM virtual circuit (LLC-based multiplexing). The second method assumes that each protocol is carried over a separate ATM virtual circuit (VC-based multiplexing). For more detailed information, see RFC 1483.

Multiplexing

There are two conventions to identify which protocols the virtual circuit (VC) carries. Be sure to use the multiplexing method required by your ISP.

VC-based multiplexing

In this case, by prior mutual agreement, each protocol is assigned to a specific virtual circuit; for example, VC1 carries IP. VC-based multiplexing can be dominant in environments where dynamic creation of large numbers of ATM VCs is fast and economical.

LLC-based multiplexing

In this case, one VC carries multiple protocols with protocol-identifying information being contained in each packet header. Despite the extra bandwidth and processing overhead, this method can be advantageous if it is not practical to have a separate VC for each carried protocol, for example, if charging heavily depends on the number of simultaneous VCs.

VPI and VCI

Be sure to use the correct Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) numbers assigned to you. The valid range for the VPI is 0 to 255 and 32 to 65535 for the VCI (0 to 31 is reserved for local management of ATM traffic).

Wizard setup configuration: first screen

In the **Site Map** screen, click **Wizard Setup** to display the first wizard screen.

Figure 7 Wizard Screen 1

Wizard Setup - ISP Parameters for Internet Access

Mode Routing ▾

Encapsulation ENET ENCAP ▾

Multiplex LLC ▾

Virtual Circuit ID

VPI 0

VCI 33

Table 2 describes the fields in Figure 7.

Table 2 Wizard Screen 1

Label	Description
Mode	From the Mode drop-down list box, select Routing (default) if your ISP allows multiple computers to share an Internet account. Otherwise, select Bridge .
Encapsulation	Select the encapsulation type your ISP uses from the Encapsulation drop-down list box. Choices vary depending on what you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP , or PPPoE .
Multiplex	Select the multiplexing method used by your ISP from the Multiplex drop-down list box, either VC-based or LLC-based.
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
VPI	Enter the VPI assigned to you. This field can already be configured.
VCI	Enter the VCI assigned to you. This field can already be configured.
Next	Click this button to go to the next wizard screen. The next wizard screen you see depends on which encapsulation you chose above.

IP address and subnet mask

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

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

If the ISP did not explicitly give you an IP network number, you most likely have a single user account and the ISP assigns you a dynamic IP address when the connection is established. The Internet Assigned Number Authority (IANA) reserved this block of addresses specifically for private use; do not use any other number unless you are told otherwise. For example, 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 (0 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.

After you select the network number, pick an IP address that is easy to remember, for instance, 192.168.1.1, for your BCM50a Integrated Router. Make sure that no other device on your network is using that IP address.

The subnet mask specifies the network number portion of an IP address. Your BCM50a Integrated Router computes the subnet mask automatically based on the IP address that you entered. You do not need to change the subnet mask computed by the BCM50a Integrated Router unless you are instructed to do so.

IP address assignment

A static IP is a fixed IP that your ISP gives you. A dynamic IP is not fixed; the ISP assigns you a different one each time. The Single User Account feature can be enabled or disabled if you have either a dynamic or static IP. However, the encapsulation method assigned influences your choices for IP address and ENET ENCAP gateway.

IP assignment with PPPoA or PPPoE encapsulation

If you have a dynamic IP, the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A). If you have a static IP, then you only need to fill in the **IP Address** field and not the **ENET ENCAP Gateway** field.

IP assignment with RFC 1483 encapsulation

In this case, the IP address assignment *must* be static with the same requirements for the **IP Address** and **ENET ENCAP Gateway** fields as stated above.

IP assignment with ENET ENCAP encapsulation

In this case, you can have either a static or dynamic IP. For a static IP, you must fill in all the **IP Address** and **ENET ENCAP Gateway** fields as supplied by your ISP. However, for a dynamic IP, the BCM50a Integrated Router acts as a DHCP client on the WAN and so the **IP Address** and **ENET ENCAP Gateway** fields are not applicable (N/A) as the DHCP server assigns them to the BCM50a Integrated Router.

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, consult your network administrator for the appropriate IP addresses.



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

Nailed-up connection (only with PPP)

A nailed-up connection is a dial-up line where the connection is always up regardless of traffic demand. The BCM50a Integrated Router does two things when you specify a nailed-up connection. First, idle timeout is disabled. Second, the BCM50a Integrated Router tries to bring up the connection when turned on and whenever the connection is down. A nailed-up connection can be expensive if you are billed by your Internet connection usage time.

Do not specify a nailed-up connection unless your telephone company offers flat-rate service or you need a constant connection and the cost is of no concern

NAT

Network Address Translation (NAT) 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.

Wizard setup configuration: second screen

The second wizard screen varies depending on which mode and encapsulation type you use. All screens shown use the routing mode. Configure the fields and click **Next** to continue.

Figure 8 Internet connection with PPPoA

Wizard Setup - ISP Parameters for Internet Access

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

[Table 3](#) describes the fields in [Figure 8](#).

Table 3 Internet connection with PPPoA

Label	Description
User Name	Enter the logon name your ISP gave you.
Password	Enter the password associated with the username above.
IP Address	<p>This option is available if you select Routing in the Mode field.</p> <p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Click Obtain an IP Address Automatically if you have a dynamic IP address; otherwise click Static IP Address and type your ISP-assigned IP address in the IP Address text box below.</p>

Table 3 Internet connection with PPPoA (continued)

Label	Description
Connection	Select Connect on Demand if you do not want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session does not timeout. Select Nailed-Up Connection if you want your connection up all the time. The BCM50a Integrated Router tries to bring up the connection automatically if it is disconnected. The schedule rules in SMT menu 26 has priority over your Connection settings.
Network Address Translation	This option is available if you select Routing in the Mode field. Select None , SUA Only , or Full Feature from the drop-down list box. For more details, see Chapter 8, "Network Address Translation (NAT) Screens," on page 121.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 9 Internet connection with RFC 1483

The screenshot shows a configuration window titled "Wizard Setup - ISP Parameters for Internet Access". It contains two main fields: "IP Address" with a text input field containing "0.0.0.0", and "Network Address Translation" with a dropdown menu currently set to "SUA Only". At the bottom right of the window, there are two buttons labeled "Back" and "Next".

[Table 4](#) describes the fields in [Figure 9](#).

Table 4 Internet connection with RFC 1483

Label;	Description
IP Address	This field is available if you select Routing in the Mode field. Type your ISP-assigned IP address in this field.

Table 4 Internet connection with RFC 1483 (continued)

Network Address Translation	Select None , SUA Only , or Full Feature from the drop-down list box. For more details, see Chapter 8, “Network Address Translation (NAT) Screens,” on page 121.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 10 Internet connection with ENET ENCAP

Wizard Setup - ISP Parameters for Internet Access

IP Address

Obtain an IP Address Automatically

Static IP Address

IP Address

Subnet Mask

ENET ENCAP Gateway

Network Address Translation

[Table 5](#) describes the fields in [Figure 10](#).

Table 5 Internet connection with ENET ENCAP

Label	Description
IP Address	A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address. Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP-assigned IP address in the IP Address text box below.
Subnet Mask	Enter a subnet mask in dotted decimal notation. If you are implementing subnetting, see the IP subnetting appendix in the <i>BCM50a Integrated Router Configuration — Advanced</i> guide.

Table 5 Internet connection with ENET ENCAP (continued)

Label	Description
ENET ENCAP Gateway	You must specify a gateway IP address (supplied by your ISP) when you use ENET ENCAP in the Encapsulation field in the previous screen.
Network Address Translation	Select None , SUA Only , or Full Feature from the drop-down list box. For more details, see Chapter 8, "Network Address Translation (NAT) Screens," on page 121.
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

Figure 11 Internet connection with PPPoE

Wizard Setup - ISP Parameters for Internet Access

Service Name

User Name

Password

IP Address

Obtain an IP Address Automatically

Static IP Address

Connection

Connect on Demand: Max Idle Timeout sec

Nailed-Up Connection

Network Address Translation

Table 6 describes the fields in Figure 11.

Table 6 Internet connection with PPPoE

Label	Description
Service Name	Type the name of your PPPoE service here.
User Name	Enter the username 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 username above.
IP Address	<p>A static IP address is a fixed IP that your ISP gives you. A dynamic IP address is not fixed; the ISP assigns you a different one each time you connect to the Internet. The Single User Account feature can be used with either a dynamic or static IP address.</p> <p>Select Obtain an IP Address Automatically if you have a dynamic IP address; otherwise select Static IP Address and type your ISP-assigned IP address in the IP Address text box below.</p>
Connection	<p>Select Connect on Demand if you do not want the connection up all the time and specify an idle time-out (in seconds) in the Max. Idle Timeout field. The default setting selects Connection on Demand with 0 as the idle time-out, which means the Internet session does not timeout.</p> <p>Select Nailed-Up Connection if you want your connection up all the time. The BCM50a Integrated Router tries to bring up the connection automatically if it is disconnected.</p> <p>The schedule rules in SMT menu 26 has priority over your Connection settings.</p>
Network Address Translation	Select None , SUA Only , or Full Feature from the drop-down list box. For more details, see Chapter 8, "Network Address Translation (NAT) Screens," on page 121 .
Back	Click Back to go back to the first wizard screen.
Next	Click Next to continue to the next wizard screen.

DHCP setup

Using Dynamic Host Configuration Protocol (DHCP), individual clients can obtain TCP/IP configuration from a server. You can configure the BCM50a Integrated Router as a DHCP server. When configured as a server, the BCM50a Integrated Router provides the TCP/IP configuration for the clients. If you turn DHCP service off, you must have another DHCP server on your LAN, or else the computer must be manually configured. DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132)

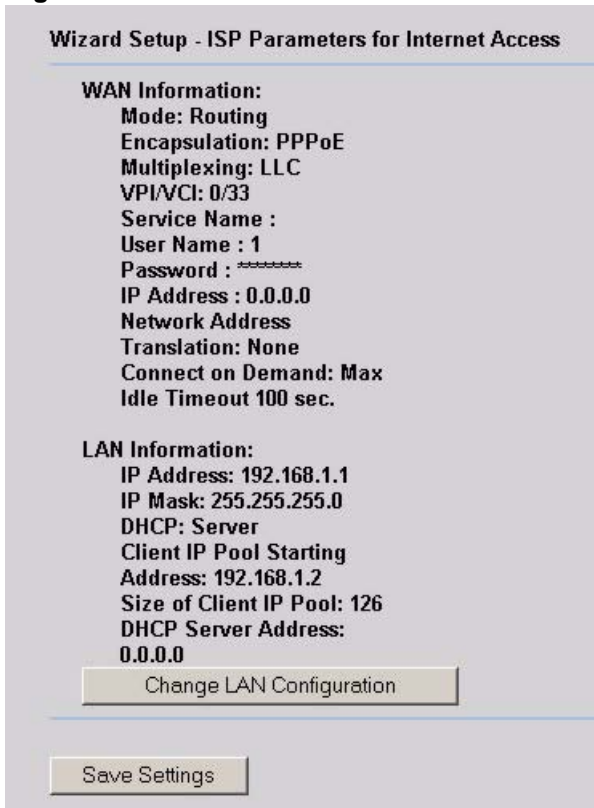
IP pool setup

The BCM50a Integrated Router is preconfigured with a pool of IP addresses for the client machines.

Wizard setup configuration: third screen

- 1 Verify the settings in the following screen. To change the LAN information on the BCM50a Integrated Router, click **Change LAN Configurations**. Otherwise click **Save Settings** to save the configuration and skip to [“Test your Internet connection”](#) on page 63.

Figure 12 Wizard Screen 3



- 2 To change your BCM50a Integrated Router LAN settings, click **Change LAN Configuration** to display the following screen.



Note: If you change the BCM50a Integrated Router LAN IP address, you must use the new IP address to access the WebGUI again.

Figure 13 Wizard: LAN configuration

Wizard Setup - ISP Parameters for Internet Access

LAN IP Address: 192.168.1.1
 LAN Subnet Mask: 255.255.255.0

DHCP

DHCP: Server
 Client IP Pool Starting Address: 192.168.1.2
 Size of Client IP Pool: 126
 DHCP Server Address: 0.0.0.0
 First DNS Server: Obtained From ISP 0.0.0.0
 Second DNS Server: Obtained From ISP 0.0.0.0
 Third DNS Server: Obtained From ISP 0.0.0.0

Back Finish

[Table 7](#) describes the fields in [Figure 13](#).

Table 7 Wizard: LAN configuration

Label	Description
LAN IP Address	Enter the IP address of your BCM50a Integrated Router in dotted decimal notation, for example, 192.168.1.1 (factory default).
LAN Subnet Mask	Enter a subnet mask in dotted decimal notation.
DHCP	

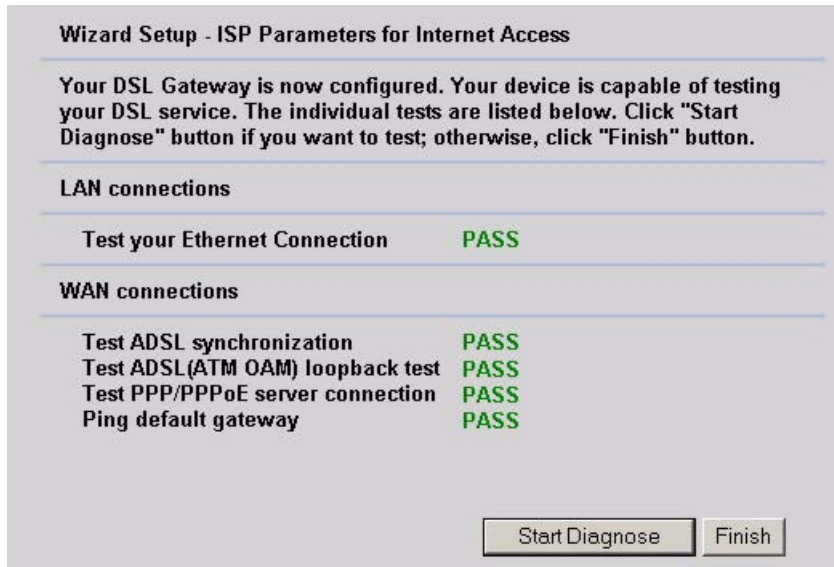
Table 7 Wizard: LAN configuration (continued)

Label	Description
DHCP	<p>With DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) individual clients (workstations) can obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to Server. When configured as a server, the BCM50a Integrated Router provides TCP/IP configuration for the clients. When set as a server, fill in the IP Pool Starting Address and Pool Size fields.</p> <p>Select Relay to have the BCM50a Integrated Router forward DHCP requests to another DHCP server. When set to Relay, fill in the DHCP Server Address field.</p> <p>Select None to stop the BCM50a Integrated Router from acting as a DHCP server. When you select None, you must have another DHCP server on your LAN, or else the computers must be manually configured.</p>
Client IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	This field specifies the size or count of the IP address pool.
DHCP Server Address	Type the IP address of the DHCP server in dotted decimal notation (like 192.168.1.5).
First DNS Server Second DNS Server Third DNS Server	<p>Select Obtained From ISP if your ISP dynamically assigns DNS server information (and the BCM50a Integrated Router WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select UserDefined if you have the IP address of a DNS server. Enter the DNS server IP address in the field to the right.</p> <p>Select DNS Relay to have the BCM50a Integrated Router act as a DNS proxy. The BCM50a Integrated Router LAN IP address displays in the field to the right (read-only). The BCM50a Integrated Router tells the DHCP clients on the LAN that the BCM50a Integrated Router itself is the DNS server. When a computer on the LAN sends a DNS query to the BCM50a Integrated Router, the BCM50a Integrated Router forwards the query to the BCM50a Integrated Router system DNS server (configured in the SYSTEM General screen) and relays the response back to the computer. You can only select DNS Relay for one of the three servers;</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP addresses of devices or web sites in order to access them.</p>
Back	Click Back to go back to the previous screen.
Finish	Click Finish to save the settings and proceed to the next wizard screen.

Wizard setup configuration: connection tests

The BCM50a Integrated Router automatically tests the connection to the computers connected to the LAN ports. To test the connection from the BCM50a Integrated Router to the ISP and the connected LAN devices, click **Start Diagnose**. Otherwise click **Finish** to go back to the site map screen.

Figure 14 Wizard Screen 4



Test your Internet connection

Launch your Web browser and navigate to www.nortel.com. Internet access is just the beginning. For more detailed information on the complete range of features for the BCM50a Integrated Router, see the rest of this guide. If you cannot access the Internet, open the WebGUI again to confirm that the Internet settings you configured in the Wizard Setup are correct.

Chapter 4

User Notes

General Notes

There are some router functions that, although performing as expected, might cause some confusion. These are summarized below.

General

1 Default Address Mapping Rules When First Enable NAT Full Feature.

When NAT Full Feature is first enabled, two address mapping rules are added to the address mapping table. This is done to facilitate programming, and matches the default SUA rule. The rules can be deleted.

2 Response to Invalid User ID or Password

When the wrong user ID or password is entered into the router login screen, no error message is displayed. Instead, the login screen is simply displayed again.

3 First DHCP Address Reserved for BCM50

The first address of the DHCP Address Pool is reserved for a BCM50 in the subnet, and will not be assigned to any other equipment. Once assigned to a BCM50, it is reserved for that BCM50, and will not be assigned to any other. If the BCM50 is changed, the following command must be used to enable the router to assign the first address to a different BCM50:

```
ip dhcp enif0 server m50mac clear
```

4 Login Requires Reboot

If the Administrator Timeout is set to 0, and an administration session is terminated without logging off, the router needs to be rebooted in order for the administrator to log in to the WebGUI again. Alternatively, the administrator can log in using a TelNet session, if TelNet access has been enabled in the Remote Management menu.

Firewall

1 Address Range Validation

In the firewall rules, the router does not confirm when given an address range, that the second address is higher than the first. If this type of address range is entered, the range is ignored.

2 Automatic Firewall Programming

Configurations to various areas of the router, such as remote management or adding a SUA Server, do not automatically add the appropriate rules to the Firewall, to enable the traffic to pass through the router. These need to be added separately.

Note: Firewall rules do not apply to IPSec tunnels.

NAT

1 Deleting NAT Rule Does Not Drop an Existing Connection

If a NAT rule is deleted, the router must be rebooted to apply the change to existing service connections. This is already noted in the GUI.

2 Confusing NAT Traversal Status

If NAT Traversal is enabled, but is not needed (because the client is not behind a NAT router), it will be shown as 'inactive' in the VPN Client Monitor. This may confuse some users.

VPN Client Termination

1 Change of User Account Does Not Drop Existing Connections

If a VPN Client user account is de-activated, deleted, or changed, and that user is currently connected, the connection is not automatically dropped. To drop the connection, the administrator needs to disconnect the user using the 'Disconnect' function in the VPN/SA Monitor GUI. This is consistent with other Nortel Contivity products.

2 User Name Restrictions

User names are limited to a maximum length of 63 characters.

3 VPN Client Account Password Restrictions

The password for a VPN Client user cannot contain the single- or double-quote characters.

4 IP Pool Address Overlap

When defining multiple VPN Client Termination IP pools, the router uses the IP Subnet mask, and not the pool size, to determine if the pools are overlapping. The subnet mask of each pool should be appropriate for the size of the VPN Client Termination IP pool.

5 VPN Client Termination - Failure In Specific Addressing Situation

If the Client has an assigned IP address that is the same as the IP address assigned for the Client Tunnel, the connection will fail to be established.

6 VPN Client Termination - Configuration Restrictions

This router has some restrictions when compared to larger Contivity Routers (1000 Series and above). In particular,

VPN Clients cannot be added to the LAN subnet. They must have addresses outside of the LAN subnet.

VPN Clients can have dynamically assigned IP addresses, or they can have a statically assigned addresses. However, the router does not support both modes at once. All addresses must either be dynamically assigned, or they must all be statically assigned.

Security

1 Exporting or Saving Self-Signed Certificate

To export or save a self-signed certificate, click details (the icon that looks like a paper note), then click 'Export' or copy the PEM text into the clipboard, and paste into a file.

Routing

1 RIP Version Advertisement Control

To change the version of generated RIP advertisements, the following CLI command needs to be used

```
ip rip mode [enif0|enif1] [in|out] [0|1|2|3]
```

where:

'enif0' is the LAN side, and 'enif1' is the WAN side

'in' affects recognition of received advertisements, and

'out' applies to generated advertisements

The number controls the operating mode:

None (disabled)

RIP-1 only

RIP-2 only

Both RIP-1 and RIP-2

Advanced Router Configuration

The following notes are intended to help with advanced router configuration.

Setting up the router when the system has a server

- 1 If you are using a Full-Feature NAT configuration, first, do the following...
 - a In SUA/NAT / Address Mapping, add a 'Server' rule, specifying the 'Public' IP address of the server.
- 2 For both SUA-Only and Full-Feature NAT configurations, do the following...
 - a In SUA/NAT : SUA Server, add server private IP address and port number(s) to the SUA/NAT Server table.
 - b In FIREWALL, add a WAN-to-LAN rule
 - c If the service is not in the list of available services, add it as a 'Custom Port'.
 - d Add the rule, selecting the service, and entering the server IP address as the destination IP address.

Connecting two sites to establish a virtual private network

The recommended method to do this is through a branch-to-branch IPsec tunnel.

- 1 In VPN / Summary, add a new tunnel by editing an unused rule. Create an Active, Branch Office tunnel.
 - a Select 'Nailed Up' if the tunnel should not be closed while not in use.
 - b Enter the authentication information, with either a pre-shared key or an imported certificate.
 - c Enter the IP Address assigned to the router WAN port. This should be a static address, or a dynamic DNS name, and the IP address of the remote router.
 - d Select the encryption and authentication algorithms.
 - e Add an IP policy, by specifying the IP address ranges of the local and remote hosts that will use the tunnel.
- 2 Repeat these steps at the other end of the branch.

Note: If VPN Client Termination is used on these sites, the client termination address range will need to be included in the tunnel policies in order for the VPN clients to see the other site.

Adding IP telephony to a multi-site network

Scenario 1: A BCM50 in the primary site acting as the gateway for both sites

- 1 Ensure that the DHCP Server in the BCM50 is disabled, that the BCM50 is connected to the router, and both have booted.
- 2 Add the IP phones to the primary site as per BCM50 installation guide.
- 3 Create a tunnel to the remote site, as described above.
- 4 In the remote site, set the S1 and S2 addresses to the IP address of the BCM50, which is identified in the router DHCP table or in the BCM50. This is done with a CLI command.

TELNET or SSH to the router. This needs TELNET or SSH enabled on that router. Select menu 24, select menu 8, and enter the commands:

```
ip dhcp enif0 server voipserver 1 <BCM50_IP_Address> 7000 1
```

```
ip dhcp enif0 server voipserver 2 <BCM50_IP_Address> 7000 1
```

- 5 Add the IP phones to the remote site, configured for full DHCP client mode.

Scenario 2: A BCM50 in each site, each acting as the backup call server for the other site

- 1 At each site,
 - a Ensure that the DHCP Server in the BCM50 is disabled, that the BCM50 is connected to the router, and both have booted.
 - b Add the IP phones to the site as per BCM50 installation guide.
 - c At each router, change the S2 address to the IP address of the remote BCM50, using TELNET or SSH, and the CLI command,

```
ip dhcp enif0 server voipserver 2 <Remote_BCM50_IP_Address> 7000 1
```
- 2 Create a tunnel between the sites, as described above.
- 3 Create an H.323 trunk between the BCM50s, as per the BCM50 User Guide.

Configuring the router to act as a Nortel VPN Server (Client Termination)

- 1 Under VPN / Client Termination,
 - a Enable Client Termination.
 - b Select authentication type and the encryption algorithms supported.
 - c If the clients are assigned IP addresses from a pool, define the pool, and enable it.
- 2 Assuming a Local User Database is used for authentication,
 - a Add user name and password to the local user database as an IPSec user, and activate it. If the hosts will be assigned a static IP address, enter the address that will be assigned to the user.

Configuring the router to connect to a Nortel VPN Server (Client Emulation)

- 1 Go to VPN / Summary, and select 'Edit'.
- 2 Select a connection type of Contivity Client, and fill in the web page with the relevant data.
- 3 If Group authentication or On-Demand Client Tunnels are needed, click the 'Advanced' button to configure this.

Configuring the router to allow remote management of a LAN-connected BCM50

- 1 Create the appropriate NAT server rules to add the BCM50.

Go to SUA/NAT / SUA Server, and create two server rules for HTTPS and Element Manager access:

One named BCM_HTTPS, with port number 443, and the IP address of the BCM50

One named BCM_EM, with the port number 5989, and the IP address of the BCM50

Note: In DHCP Server mode, the BCM50 IP address will be the lowest address in the pool.

- 2 Create the appropriate Firewall rules to add BCM50 access.

Go to FIREWALL / Summary, and create two WAN-to-LAN firewall rules:

One rule allowing access from allowed remote computer IP addresses, to the BCM50 IP address, for service type HTTPS(TCP:443)

One rule allowing access from allowed remote computer IP addresses, to the BCM50 IP address, for custom port TCP:5989

Setting up the router for guest access

The recommended approach to provide guest access is by creating an IP Alias, and using static addressing for the corporate equipment, to make it a member of the defined Alias subnet. Then use firewall rules to restrict access of the guest equipment. NOTE: if a BCM50 is used, it will also need to be assigned a static IP address.

- 1 Go to LAN / IP Alias, and Enable IP Alias 1.
- 2 Define a subnet for the corporate equipment.
- 3 Statically assign addresses to the corporate equipment that are within the IP Alias subnet.
- 4 Set up LAN / IP to enable DHCP Server, with an address range that will be used for guest equipment.
- 5 In the FIREWALL, set up a LAN-to-LAN rule to block traffic between the guest subnet (DHCP Pool) and the corporate subnet (IP Alias subnet).

Note: If branch tunnels are being used, the policies on these tunnels should exclude the guest subnet.

Preventing heavy data traffic from impacting telephone calls

To ensure voice quality during heavy data traffic, bandwidth needs to be reserved for voice traffic. Bandwidth needs to be reserved on both the WAN side, and the LAN side.

- 1 On BANDWIDTH MANAGEMENT / Summary, activate WAN- and LAN-side bandwidth management.

- 2** On BANDWIDTH MANAGEMENT / Class Setup, add a WAN subclass, and reserve sufficient bandwidth based on the number of telephones, for Protocol ID 17 (UDP Traffic).

The amount of bandwidth should be based on a reasonable peak number of simultaneous calls, and the data rate needed by the IP telephony CODECs. Refer to the BCM IP Telephony (or other call server) documentation for calculation details.

- 3** Set up a similar LAN subclass.

Chapter 5

System screens

This chapter provides information on the System screens.

System overview

This section provides background information on features that you cannot configure in the Wizard.

DNS overview

There are three places where you can configure DNS (Domain Name System) setup on the BCM50a Integrated Router.

Use the **System General** screen to configure the BCM50a Integrated Router to use a DNS server to resolve domain names for BCM50a Integrated Router system features like VPN, DDNS, and the time server.

Use the **LAN IP** screen to configure the DNS server information that the BCM50a Integrated Router sends to the DHCP client devices on the LAN.

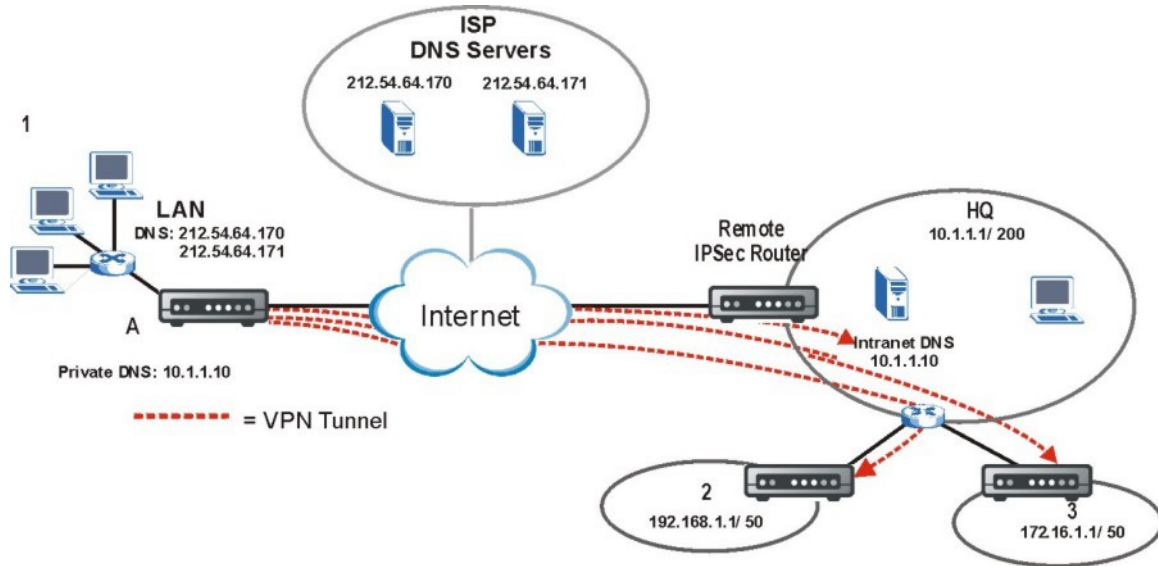
Use the **Remote Management DNS** screen to configure the BCM50a Integrated Router to accept or discard DNS queries.

Private DNS server

In cases where you want to use domain names to access Intranet servers on a remote private network that has a DNS server, you must identify that DNS server. You cannot use DNS servers on the LAN or from the ISP because these DNS servers cannot resolve domain names to private IP addresses on the remote private network.

Figure 15 depicts an example where three VPN tunnels are created from BCM50a Integrated Router A; one to branch office 2, one to branch office 3, and another to headquarters (HQ). In order to access computers that use private domain names on the HQ network, the BCM50a Integrated Router at branch office 1 uses the Intranet DNS server in headquarters.

Figure 15 Private DNS server example



Note: If you do not specify an Intranet DNS server on the remote network, then the VPN host must use IP addresses to access the computers on the remote private network.

Configuring General Setup

Click **SYSTEM** to open the **General** screen.

Figure 16 System general setup
SYSTEM

The screenshot shows the 'General' tab of the system configuration interface. It contains the following fields and controls:

- System Name:** A text input field.
- Domain Name:** A text input field.
- Administrator Inactivity Timer:** A text input field containing the value '5', with a note '(minutes, 0 means no timeout)'.
- System DNS Servers:** A section containing three rows:
 - First DNS Server:** A dropdown menu set to 'From ISP' and a text box containing '0.0.0.0'.
 - Second DNS Server:** A dropdown menu set to 'From ISP' and a text box containing '0.0.0.0'.
 - Third DNS Server:** A dropdown menu set to 'From ISP' and a text box containing '0.0.0.0'.
- Buttons:** 'Apply' and 'Reset' buttons are located at the bottom center.

Table 8 describes the fields in Figure 16.

Table 8 System general setup

Label	Description
System Name	Choose a descriptive name for identification purposes. Nortel recommends that you enter your computer name in this field. This name can be up to 30 alphanumeric characters long. Spaces, dashes (-) and underscores (_) are accepted.
Domain Name	Enter the domain name (if you know it) here. If you leave this field blank, the ISP assigns a domain name through DHCP. The domain name entered by you is given priority over the ISP-assigned domain name.
Administrator Inactivity Timer	Type how many minutes a management session (either through the WebGUI or SMT) can be left idle before the session times out. The default is 5 minutes. After it times out you have to log in with your password again. Very long idle timeouts can have security risks. A value of 0 means a management session never times out, no matter how long it has been left idle (not recommended).
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Table 8 System general setup

Label	Description
System DNS Servers (if applicable)	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. The DNS server is extremely important because without it, you must know the IP address of a machine before you can access it. The BCM50a Integrated Router uses a system DNS server (in the order you specify here) to resolve domain names for VPN, DDNS and the time server.
First DNS Server Second DNS Server Third DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the BCM50a Integrated Router WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns. If you chose From ISP, but the BCM50a Integrated Router has a fixed WAN IP address, From ISP changes to None after you click Apply. If you chose From ISP for the second or third DNS server, but the ISP does not provide a second or third IP address, From ISP changes to None after you click Apply.</p> <p>Select User-Defined if you have the IP address of a DNS server. The IP address can be public or a private address on your local LAN. Enter the DNS server's IP address in the field to the right.</p> <p>A User-Defined entry with the IP address set to 0.0.0.0 changes to None after you click Apply. A duplicate User-Defined entry changes to None after you click Apply.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a system DNS server, you must use IP addresses when configuring VPN, DDNS and the time server.</p> <p>Select Private DNS if the DNS server has a private IP address and is located behind a VPN peer. Enter the DNS server's IP address in the field to the right.</p> <p>With a private DNS server, you must also configure the first DNS server entry in the LAN IP screen to use DNS Relay.</p> <p>You must also configure a VPN branch office rule since the BCM50a Integrated Router uses a VPN tunnel when it relays DNS queries to the private DNS server. The rule must also have an IP policy that includes the LAN IP address of the BCM50a Integrated Router as a local IP address and the IP address of the DNS server as a remote IP address.</p> <p>A Private DNS entry with the IP address set to 0.0.0.0 changes to None after you click Apply. A duplicate Private DNS entry changes to None after you click Apply.</p>

Dynamic DNS

With Dynamic DNS, you can update your current dynamic IP address with one or many dynamic DNS services so that anyone can contact you (as in NetMeeting or CU-SeeMe). You can also access your FTP server or Web site on your own computer using a domain name (for instance, myhost.dhs.org, where myhost is a name of your choice) that will never change instead of using an IP address that changes each time you reconnect. Your friends or relatives can always call you even if they don't know your IP address.

First of all, you must register a dynamic DNS account with, for example www.dyndns.org. This is for people with a dynamic IP from their ISP or DHCP server that still wants a domain name. The Dynamic DNS service provider gives you a password or key.

DYNDNS wildcard

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

Configuring Dynamic DNS



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

To change the DDNS settings, click **SYSTEM**, then the **DDNS** tab. The screen illustrated in [Figure 17](#) appears.

Figure 17 DDNS
SYSTEM

The screenshot shows a configuration window for DDNS. The window has a title bar with tabs: General, DDNS, Password, Time and Date, and ALG. The DDNS tab is selected. The main area contains the following elements:

- Active
- Service Provider: WWW.DynDNS.ORG
- DDNS Type: Dynamic DNS (dropdown menu)
- Host Name 1: [Empty text box]
- Host Name 2: [Empty text box]
- Host Name 3: [Empty text box]
- Username: [Empty text box]
- Password: [Empty text box]
- Enable Wildcard
- Off Line

Below these fields is a section titled "IP Address Update Policy":

- DDNS Server Auto Detect IP Address
- Use Specified IP Address
- Use IP Address: 0.0.0.0 (text box)

At the bottom of the window are two buttons: "Apply" and "Reset".

Table 9 describes the fields in Figure 17.

Table 9 DDNS

Label	Description
Active	Select this check box to use dynamic DNS.
Service Provider	Select the name of your Dynamic DNS service provider.
DDNS Type	Select the type of service that you are registered for from your Dynamic DNS service provider.
Host Names 1~3	Enter the host names in the three fields provided. You can specify up to two host names in each field separated by a comma (,).
User	Enter your username (up to 31 characters).

Table 9 DDNS

Label	Description
Password	Enter the password associated with your username (up to 31 characters).
Enable Wildcard	Select the check box to enable DYNDNS Wildcard.
Off Line	This option is available when CustomDNS is selected in the DDNS Type field . Check with your Dynamic DNS service provider to have traffic redirected to a URL (that you can specify) while you are off line.
IP Address Update Policy:	
DDNS Server Auto Detect IP Address	Select this option only when there are one or more NAT routers between the BCM50a Integrated Router and the DDNS server. This feature has the DDNS server automatically detect and use the IP address of the NAT router that has a public IP address. Note: The DDNS server not be able to detect the proper IP address if there is an HTTP proxy server between the BCM50a Integrated Router and the DDNS server.
Use Specified IP Address	Select this option to update the IP address of the host names to the IP address specified below. Use this option if you have a static IP address.
Use IP Address	Enter the IP address if you select the User Specify option.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to return to the previously saved settings.

Configuring Password

To change the password of your BCM50a Integrated Router (recommended), click **SYSTEM**, then the **Password** tab. The screen illustrated in [Figure 18](#) appears. In this screen, you can change password of the BCM50a Integrated Router.

Figure 18 Password
SYSTEM

The screenshot shows a web-based configuration interface for a system. At the top, there are five tabs: 'General', 'DDNS', 'Password', 'Time and Date', and 'ALG'. The 'Password' tab is currently selected. Below the tabs, the page is divided into two main sections: 'Administrator Setting' and 'Client User Setting'. Each section contains three input fields. The 'Administrator Setting' section has fields for 'Old Password', 'New Password', and 'Retype to Confirm'. The 'Client User Setting' section has fields for 'User Name', 'New Password', and 'Retype to Confirm'. At the bottom of the page, there are two buttons: 'Apply' and 'Reset'.

Table 10 describes the fields in Figure 18.

Table 10 Password

Label	Description
Administrator Setting	The administrator can access and configure all of the BCM50a Integrated Router's features.
Old Password	Type your existing system administrator password ("PlsChgMe!" is the default password).
New Password	Type your new system password (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype your new system password for confirmation.

Table 10 Password

Label	Description
Client User Setting	<p>The client user is the person who uses the BCM50a Integrated Router's Contivity Client VPN tunnel.</p> <p>The client user can do the following:</p> <ul style="list-style-type: none"> • Configure the WAN ISP and IP screens. • Configure the VPN Contivity Client settings (except the Advanced screen exclusive use mode for client tunnel and MAC address allowed settings). • View the SA monitor. • Configure the VPN Global Setting screen. • View logs. • View the Maintenance Status screen. • Use the Maintenance F/W Upload and Restart screens.
User Name	Type a username for the client user (up to 31 characters).
New Password	Type a password for the client user (up to 31 characters). Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Retype the client user password for confirmation.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Predefined NTP time server list

The BCM50a Integrated Router uses the predefined list of NTP time servers listed in [Table 11](#) if you do not specify a time server or if it cannot synchronize with the time server you specified.

The BCM50a Integrated Router can use this predefined list of time servers regardless of the Time Protocol you select.

When the BCM50a Integrated Router uses the predefined list of NTP time servers, it randomly selects one server and tries to synchronize with it. If the synchronization fails, then the BCM50a Integrated Router goes through the rest of the list in order from the first one tried until either it is successful or all the predefined NTP time servers have been tried.

Table 11 Default Time Servers

ntp1.cs.wisc.edu
ntp1.gbg.netnod.se
ntp2.cs.wisc.edu
tock.usno.navy.mil
ntp3.cs.wisc.edu
ntp.cs.strath.ac.uk
ntp1.sp.se
time1.stupi.se
tick.stdtime.gov.tw
tock.stdtime.gov.tw
time.stdtime.gov.tw

Configuring Time and Date

To change the time and date of your BCM50a Integrated Router, click **SYSTEM**, and then **Time and Date**. The screen in [Figure 19](#) appears. Use this screen to configure the time based on your local time zone.

Figure 19 Time and Date
SYSTEM

General	DDNS	Password	Time and Date	ALG
----------------	-------------	-----------------	----------------------	------------

Current Time and Date

Current Time	00 : 49 : 34
Current Date	2000 - 01 - 01

Time and Date Setup

Manual

New Time (hh:mm:ss)	0 : 47 : 55
New Date (yyyy-mm-dd)	2000 - 1 - 1

Get from Time Server

Time Protocol	NTP (RFC-1305)
Time Server Address*	a.ntp.alphazed.net

* Optional. There is a pre-defined NTP time server list.

Time Zone Setup

Time Zone (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Enable Daylight Saving

Start Date	First	Saturday	of	January	(2000-01-01)	at	0	o'clock
End Date	First	Saturday	of	January	(2000-01-01)	at	0	o'clock

Table 12 describes the fields in Figure 19.

Table 12 Time and Date

Label	Description
Current Time and Date	
Current Time	This field displays the time on your BCM50a Integrated Router. Each time you reload this page, the BCM50a Integrated Router synchronizes the time with the time server.
Current Date	This field displays the date on your BCM50a Integrated Router. Each time you reload this page, the BCM50a Integrated Router synchronizes the date with the time server.
Time and Date Setup	
Manual	Select this radio button to enter the time and date manually. If you configure a new time and date, time zone and daylight saving at the same time, the new time and date you entered has priority and the Time Zone and Daylight Saving settings do not affect it.
New Time (hh:mm:ss)	This field displays the last updated time from the time server or the last time configured manually. After you set Time and Date Setup to Manual , enter the new time in this field and then click Apply .
New Date (yyyy-mm-dd)	This field displays the last updated date from the time server or the last date configured manually. After you set Time and Date Setup to Manual , enter the new date in this field and then click Apply .
Get from Time Server	Select this radio button to have the BCM50a Integrated Router get the time and date from the time server that you specified.
Time Protocol	Select the time service protocol that your time server sends when you turn on the BCM50a Integrated Router. Not all time servers support all protocols, so you need to check with your ISP or network administrator or use trial and error to find a protocol that works. The main difference between the protocols is the format. Daytime (RFC 867) format is day/month/year/time zone of the server. Time (RFC 868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0. The default, NTP (RFC 1305) , is similar to Time (RFC 868) .
Time Server Address	Enter the IP address or URL of your time server. Check with your ISP or network administrator if you are unsure of this information.
Synchronize Now	Click this button to have the BCM50a Integrated Router get the time and date from a time server (see the Time Server Address field). This also saves your changes (including the time server address).

Table 12 Time and Date

Label	Description
Time Zone Setup	
Time Zone	Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).
Enable Daylight Saving	Daylight Saving Time 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. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you select Enable Daylight Saving . The o'clock field uses the 24-hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the first Sunday of April. Each time zone in the United States starts using Daylight Saving Time at 2 a.m. local time. So, in the United States, select First, Sunday, April and type 2 in the o'clock field. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 a.m. GMT or UTC). So, in the European Union, select Last, Sunday, March . The time you type in the o'clock field depends on your time zone. In Germany, for instance, type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you select Enable Daylight Saving . The o'clock field uses the 24-hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 a.m. local time. So, in the United States, select Last, Sunday, October and type 2 in the o'clock field. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 a.m. GMT or UTC). So, in the European Union, select Last, Sunday, October . The time you type in the o'clock field depends on your time zone. In Germany for instance, type 2 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

ALG

With Application Layer Gateway (ALG), an application can pass through NAT and the firewall. You must also configure NAT and firewall rules depending upon the type of access you want to allow.



Note: You must enable the FTP ALG in order to use bandwidth management on that application.

Configuring ALG

To change the ALG settings of your BCM50a Integrated Router, click **SYSTEM** and then **ALG**. The screen appears as shown in [Figure 20](#).

Figure 20 ALG

SYSTEM

The screenshot shows a web interface for configuring the ALG settings. At the top, there are five tabs: 'General', 'DDNS', 'Password', 'Time and Date', and 'ALG'. The 'ALG' tab is active. Below the tabs, the text 'ALG Setting' is displayed. Underneath, there is a checkbox labeled 'Enable FTP ALG' which is checked. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

[Table 13](#) describes the labels in [Figure 20](#).

Table 13 ALG

Label	Description
Enable FTP ALG	Select this check box to allow FTP (File Transfer Protocol) to send and receive files through the BCM50a Integrated Router.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 6

LAN screens

This chapter describes how to configure LAN settings.

LAN overview

Local Area Network (LAN) is a shared communication system to which many computers are attached. The LAN screens can help you configure a LAN DHCP server, manage IP addresses, configure RIP and multicast settings, and partition your physical network into logical networks.

DHCP setup

Using DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132), individual clients can obtain TCP/IP configuration at start-up from a server. You can configure the BCM50a Integrated Router as a DHCP server or disable it. When configured as a server, the BCM50a Integrated Router provides the TCP/IP configuration for the clients. If DHCP service is disabled, you must have another DHCP server on your LAN, or else the computer must be configured manually.

IP pool setup

The BCM50a Integrated Router is preconfigured with a pool of IP addresses for the DHCP clients (DHCP Pool). Do not assign static IP addresses from the DHCP pool to your LAN computers.

DNS servers

Use the **LAN IP** screen to configure the DNS server information that the BCM50a Integrated Router sends to the DHCP client devices on the LAN.

LAN TCP/IP

The BCM50a Integrated Router has built in DHCP server capability that assigns IP addresses and DNS servers to systems that support DHCP client capability.

Factory LAN defaults

The LAN parameters of the BCM50a Integrated Router are preset in the factory with the following values:

- IP address of 192.168.1.1 with subnet mask of 255.255.255.0 (24 bits)
- DHCP server enabled with 126 client IP addresses starting from 192.168.1.2.

These parameters work for the majority of installations. If your ISP gives you explicit DNS server addresses, read the embedded WebGUI help regarding which fields need to be configured.

RIP setup

RIP (Routing Information Protocol, RFC 1058 and RFC 1389) allows a router to exchange routing information with other routers. **RIP Direction** controls the sending and receiving of RIP packets. When set to **Both** or **Out Only**, the BCM50a Integrated Router broadcasts its routing table periodically. When set to **Both** or **In Only**, it incorporates the RIP information that it receives; when set to **None**, it does not send any RIP packets and ignores any RIP packets received.

RIP Version controls the format and the broadcasting method of the RIP packets that the BCM50a Integrated Router sends (it recognizes both formats when receiving). **RIP-1** is universally supported; but **RIP-2** carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology.

Both **RIP-2B** and **RIP-2M** send routing data in RIP-2 format; the difference being that **RIP-2B** uses subnet broadcasting while **RIP-2M** uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

By default, **RIP Direction** is set to **Both** and **RIP Version** to **RIP-1**.

Multicast

Traditionally, IP packets are transmitted in one of two ways—Unicast (1 sender-1 recipient) or Broadcast (1 sender-everybody on the network). Multicast delivers IP packets to a group of hosts on the network—not everybody and not just 1.

IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of *Internet Group Management Protocol* (RFC 2236). The class D IP address is used to identify host groups and can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is not assigned to any group and is used by IP multicast computers. The address 224.0.0.1 is used for query messages and is assigned to the permanent group of all IP hosts (including gateways). All hosts must join the 224.0.0.1 group in order to participate in IGMP. The address 224.0.0.2 is assigned to the multicast routers group.

The BCM50a Integrated Router supports both IGMP version 1 (**IGMP-v1**) and IGMP version 2 (**IGMP-v2**). At start up, the BCM50a Integrated Router queries all directly connected networks to gather group membership. After that, the BCM50a Integrated Router periodically updates this information. IP multicasting can be enabled or disabled on the BCM50a Integrated Router LAN, WAN or both interfaces in the WebGUI (**LAN**; **WAN**). Select **None** to disable IP multicasting on these interfaces.

Configuring IP

Click **LAN** to open the **IP** screen.

Figure 21 LAN IP

LAN

The screenshot displays the LAN IP configuration interface with the following sections and fields:

- Static DHCP** (selected tab)
- DHCP Setup**
 - DHCP: Server (dropdown)
 - IP Pool Starting Address: 192.168.1.2
 - DHCP Server Address: 0.0.0.0
 - Pool Size: 126
- DNS Servers Assigned by DHCP Server**
 - First DNS Server: From ISP (dropdown), 0.0.0.0
 - Second DNS Server: From ISP (dropdown), 0.0.0.0
 - Third DNS Server: From ISP (dropdown), 0.0.0.0
- LAN TCP/IP**
 - IP Address: 192.168.1.1
 - IP Subnet Mask: 255.255.255.0
 - Multicast: None (dropdown)
 - RIP Direction: None (dropdown)
 - RIP Version: RIP-1 (dropdown)
- Windows Networking (NetBIOS over TCP/IP)**
 - Allow between LAN and WAN
- Buttons:** Apply, Reset

Table 14 describes the fields in Figure 21.

Table 14 LAN IP

Label	Description
DHCP	<p>With DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) individual clients (workstations) can obtain TCP/IP configuration at startup from a server. Unless you are instructed by your ISP, leave this field set to Server. When configured as a server, the BCM50a Integrated Router provides TCP/IP configuration for the clients. When set as a server, fill in the IP Pool Starting Address and Pool Size fields.</p> <p>Select Relay to have the BCM50a Integrated Router forward DHCP requests to another DHCP server. When set to Relay, fill in the DHCP Server Address field.</p> <p>Select None to stop the BCM50a Integrated Router from acting as a DHCP server. When you select None, you must have another DHCP server on your LAN, or else the computers must be manually configured.</p>
IP Pool Starting Address	This field specifies the first of the contiguous addresses in the IP address pool. The default is 192.168.1.2.
Pool Size	This field specifies the size, or count, of the IP address pool. The default is 126.
DHCP Server Address	Type the IP address of the DHCP server in dotted decimal notation (like 192.168.1.5).
DNS Servers Assigned by DHCP Server	The BCM50a Integrated Router passes a DNS (Domain Name System) server IP address (in the order you specify here) to the DHCP clients. The BCM50a Integrated Router only passes this information to the LAN DHCP clients when you select the DHCP Server check box. When you clear the DHCP Server check box, DHCP service is disabled and you must have another DHCP sever on your LAN, or else the computers must have their DNS server addresses manually configured.

Table 14 LAN IP

Label	Description
First DNS Server Second DNS Server Third DNS Server	<p>Select From ISP if your ISP dynamically assigns DNS server information (and the BCM50a Integrated Router's WAN IP address). The field to the right displays the (read-only) DNS server IP address that the ISP assigns.</p> <p>Select User-Defined if you have the IP address of a DNS server. Enter the DNS server's IP address in the field to the right.</p> <p>Select DNS Relay to have the BCM50a Integrated Router act as a DNS proxy. The BCM50a Integrated Router's LAN IP address displays in the field to the right (read-only). The BCM50a Integrated Router tells the DHCP clients on the LAN that the BCM50a Integrated Router itself is the DNS server. When a computer on the LAN sends a DNS query to the BCM50a Integrated Router, the BCM50a Integrated Router forwards the query to the BCM50a Integrated Router's system DNS server (configured in the SYSTEM General screen) and relays the response to the computer. You can only select DNS Relay for one of the three servers.</p> <p>Select None if you do not want to configure DNS servers. If you do not configure a DNS server, you must know the IP address of a machine in order to access it.</p>
LAN TCP/IP	
IP Address	Type the IP address of your BCM50a Integrated Router in dotted decimal notation (192.168.1.1 factory default).
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address. Your BCM50a Integrated Router automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50a Integrated Router 255.255.255.0.
RIP Direction	<p>With RIP (Routing Information Protocol, RFC 1058 and RFC 1389) a router can exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None. When set to Both or Out Only, the BCM50a Integrated Router broadcasts its routing table periodically. When set to Both or In Only, it incorporates the RIP information that it receives; when set to None, it does not send any RIP packets and ignores any RIP packets received. None is the default.</p>

Table 14 LAN IP

Label	Description
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the BCM50a Integrated Router sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so does not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Multicast	Select IGMP V-1 or IGMP V-2 or None . IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of <i>Internet Group Management Protocol</i> (RFC 2236).
Windows Networking (NetBIOS over TCP/IP)	
Allow between LAN and WAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you also need to create a WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. This field does the same as the Allow between WAN and LAN field in the WAN IP screen. Enabling one automatically enables the other.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Configuring Static DHCP

With Static DHCP, you can assign IP addresses on the LAN to specific individual computers based on their MAC Addresses.

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

To change the static DHCP settings, click **LAN**, then the **Static DHCP** tab. The screen appears as shown in [Figure 22](#).

Figure 22 Static DHCP

LAN

#	MAC Address	IP Address
1	<input type="text"/>	<input type="text" value="0.0.0.0"/>
2	<input type="text"/>	<input type="text" value="0.0.0.0"/>
3	<input type="text"/>	<input type="text" value="0.0.0.0"/>
4	<input type="text"/>	<input type="text" value="0.0.0.0"/>
5	<input type="text"/>	<input type="text" value="0.0.0.0"/>
6	<input type="text"/>	<input type="text" value="0.0.0.0"/>
7	<input type="text"/>	<input type="text" value="0.0.0.0"/>
8	<input type="text"/>	<input type="text" value="0.0.0.0"/>

[Table 15](#) describes the fields in [Figure 22](#).

Table 15 Static DHCP

Label	Description
#	This is the index number of the Static IP table entry (row).
MAC Address	Type the MAC address (with colons) of a computer on your LAN.
IP Address	This field specifies the size, or count of the IP address pool.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Configuring IP Alias

With IP Alias, you can partition a physical network into different logical networks over the same Ethernet interface. The BCM50a Integrated Router supports three logical LAN interfaces through its single physical Ethernet interface with the BCM50a Integrated Router itself as the gateway for each LAN network.



Note: Make sure that the subnets of the logical networks do not overlap.

To change the IP Alias settings of your BCM50a Integrated Router, click **LAN**, then the **IP Alias** tab. The screen appears as shown in [Figure 23](#).

Figure 23 IP Alias
LAN

The screenshot shows the configuration interface for IP Aliases. At the top, there are three tabs: "IP", "Static DHCP", and "IP Alias". The "IP Alias" tab is selected. Below the tabs, there are two sections for configuring IP Aliases, labeled "IP Alias 1" and "IP Alias 2". Each section starts with a checkbox that is currently unchecked. Below each checkbox are four fields: "IP Address", "IP Subnet Mask", "RIP Direction", and "RIP Version". For both IP Alias 1 and IP Alias 2, the "IP Address" and "IP Subnet Mask" fields are set to "0.0.0.0". The "RIP Direction" is set to "None" and the "RIP Version" is set to "RIP-1". At the bottom of the configuration area, there are two buttons: "Apply" and "Reset".

Table 16 describes the fields in Figure 23.

Table 16 IP Alias

Label	Description
IP Alias 1,2	Select the check box to configure another LAN network for the BCM50a Integrated Router.
IP Address	Enter the IP address of your BCM50a Integrated Router in dotted decimal notation.
IP Subnet Mask	Your BCM50a Integrated Router automatically calculates the subnet mask based on the IP address that you assign. Unless you are implementing subnetting, use the subnet mask computed by the BCM50a Integrated Router.
RIP Direction	With RIP (Routing Information Protocol, RFC 1058 and RFC 1389), a router can exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets. Select the RIP direction from Both/In Only/Out Only/None . When set to Both or Out Only , the BCM50a Integrated Router broadcasts its routing table periodically. When set to Both or In Only , it incorporates the RIP information that it receives; when set to None , it does not send any RIP packets and ignores any RIP packets received.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the BCM50a Integrated Router sends (it recognizes both formats when receiving). RIP-1 is universally supported but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines because they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, RIP direction is set to Both and the Version set to RIP-1 .
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 7

WAN screens

This chapter describes how to configure WAN settings.

WAN overview

This section provides background information on features that you cannot configure in the Wizard.

TCP/IP Priority (metric)

The metric represents the cost of transmission. A router determines the best route for transmission by choosing a path with the lowest cost. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number must be between 1 and 15; a number greater than 15 means the link is down. The smaller the number, the lower the cost.

- 1 The metric sets the priority for the BCM50a Integrated Router's routes to the Internet. Each route must have a unique metric.
- 2 The priority of the WAN port route must always be higher than the traffic redirect route priority.

If the WAN port route has a metric of 1 and the traffic redirect route has a metric of 2, then the WAN port route acts as the primary default route. If the WAN port route fails to connect to the Internet, the BCM50a Integrated Router tries the traffic redirect route next.

The traffic redirect route cannot take priority over the WAN route.

Configuring General

Click **WAN** to open the **General** screen.

Figure 24 WAN: General

WAN

General	WAN ISP	WAN IP	Traffic Redirect
---------	---------	--------	------------------

Route Selection

WAN	Priority (metric)	1	Priority = 1(highest)-15(lowest)
Traffic Redirect	Priority (metric)	14	Priority = 1(highest)-15(lowest)
Dial Backup	Priority (metric)	15	Priority = 1(highest)-15(lowest)

Connectivity Check

Check Period	5	5 ~ 300 (Seconds)
Check Timeout	3	1 ~ 10 (Seconds)
Check Fail Tolerance	3	1 ~ 10 (Successive Checks)

Check WAN Connectivity

- Ping Default Gateway 0.0.0.0
- Ping this Address (Domain Name or IP Address)

Check Traffic Redirection Connectivity

- Ping Default Gateway 0.0.0.0
- Ping this Address (Domain Name or IP Address)

Apply Reset

Table 17 describes the fields in Figure 24.

Table 17 WAN: General

Label	Description
WAN Traffic Redirect Dial Backup	<p>The default WAN connection is 1 as your broadband connection through the WAN port must always be your preferred method of accessing the WAN. The default priority of the routes is WAN, Traffic Redirect and then Dial Backup (dial backup does not apply to all models).</p> <p>You have two choices for an auxiliary connection in the event that your regular WAN connection goes down. If Dial Backup is preferred to Traffic Redirect, then type 14 in the Dial Backup Priority (metric) field (and leave the Traffic Redirect Priority (metric) at the default of 15).</p>
Connectivity Check	
Check Period	<p>The BCM50a Integrated Router tests a WAN connection by periodically sending a ping to either the default gateway or the address in the Ping this Address field.</p> <p>Type a number of seconds (5 to 300) to set the time interval between checks. Allow more time if your destination IP address handles lots of traffic.</p>
Check Timeout	<p>Type the number of seconds (1 to 10) for your BCM50a Integrated Router to wait for a response to the ping before considering the check to have failed. This setting must be less than the Check Period. Use a higher value in this field if your network is busy or congested.</p>
Check Fail Tolerance	<p>Type how many WAN connection checks can fail (1-10) before the connection is considered "down" (not connected). The BCM50a Integrated Router still checks a "down" connection to detect if it reconnects.</p>
Check WAN Connectivity	<p>Select the check box to have the BCM50a Integrated Router periodically test the WAN connection.</p> <p>Select Ping Default Gateway to have the BCM50a Integrated Router ping the WAN port's default gateway IP address.</p> <p>Select Ping this Address and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the BCM50a Integrated Router ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.</p>

Table 17 WAN: General

Label	Description
Check Traffic Redirection Connectivity	Select the check box to have the BCM50a Integrated Router periodically test the traffic redirect connection. Select Ping Default Gateway to have the BCM50a Integrated Router ping the backup gateway's IP address. Select Ping this Address and enter a domain name or IP address of a reliable nearby computer (for example, your ISP's DNS server address) to have the BCM50a Integrated Router ping that address. For a domain name, use up to 63 alphanumeric characters (hyphens, periods and the underscore are also allowed) without spaces.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

PPPoE encapsulation

The BCM50a Integrated Router supports PPPoE (Point-to-Point Protocol over Ethernet). PPPoE is an IETF Draft standard (RFC 2516) specifying how a personal computer (PC) interacts with a broadband modem (DSL, cable, wireless, etc.) connection. The **PPPoE** option is for a dial-up connection using PPPoE.

For the service provider, PPPoE offers an access and authentication method that works with existing access control systems (for example Radius). 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 you access one of multiple network services, a function known as dynamic service selection. This enables the service provider to easily create and offer new IP services for individuals.

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

By implementing PPPoE directly on the BCM50a Integrated Router (rather than individual computers), the computers on the LAN do not need PPPoE software installed, since the BCM50a Integrated Router does that part of the task. Furthermore, with NAT, all of the LAN computers will have access.

Configuring WAN ISP

To configure the WAN ISP settings for your BCM50a Integrated Router, click **WAN**, then the **WAN ISP** tab. The screen differs depending on the encapsulation.

Figure 25 WAN: WAN ISP

WAN

General	WAN ISP	WAN IP	Traffic Redirect
Name			
		ChangeMe	
Mode			
		Routing	
Encapsulation			
		PPPoE	
Multiplex			
		LLC	
Virtual Circuit ID			
VPI		0	
VCI		33	
Login Information			
Service Name			
User Name		1	
Password		*	
Connection			
<input type="radio"/> Keep Alive			
<input checked="" type="radio"/> Connect on Demand			
Max Idle Time		100 Sec.	
PPPoE Pass Through			
		No	
<input type="button" value="Apply"/> <input type="button" value="Reset"/>			

Table 18 describes the fields in Figure 25.

Table 18 WAN: WAN ISP

Label	Description
Name	Enter the name of your Internet Service Provider, for example, MyISP. This information is for identification purposes only.
Mode	Select Routing (default) from the drop-down list box if your ISP allows multiple computers to share an Internet account. Otherwise select Bridge .
Encapsulation	Select the method of encapsulation used by your ISP from the drop-down list box. Choices vary depending on the mode you select in the Mode field. If you select Bridge in the Mode field, select either PPPoA or RFC 1483 . If you select Routing in the Mode field, select PPPoA , RFC 1483 , ENET ENCAP or PPPoE .
Multiplex	Select the method of multiplexing used by your ISP from the drop-down list. Choices are VC or LLC .
Virtual Circuit ID	VPI (Virtual Path Identifier) and VCI (Virtual Channel Identifier) define a virtual circuit.
VPI	The valid range for the VPI is 0 to 255. Enter the VPI assigned to you.
VCI	The valid range for the VCI is 32 to 65 535 (0 to 31 is reserved for local management of ATM traffic). Enter the VCI assigned to you.
Login Information	(PPPoA and PPPoE encapsulation only)
Service Name	(PPPoE only) Type the name of your PPPoE service here.
User Name	Enter the username exactly as your ISP assigned. If assigned a name in the form user@domain , where domain identifies a service name, enter both components exactly as given.
Password	Enter the password associated with the username above.
Connection (PPPoA and PPPoE encapsulation only)	The schedule rules in SMT menu 26 have priority over your Connection settings.
Nailed-Up Connection	Select Nailed-Up Connection if you want your connection up all the time. The BCM50a Integrated Router tries to bring up the connection automatically if it is disconnected.
Connect on Demand	Select Connect on Demand if you don't want the connection up all the time and specify an idle time-out in the Max Idle Timeout field.

Table 18 WAN: WAN ISP (continued)

Label	Description
Max Idle Timeout	Specify an idle time-out in the Max Idle Timeout field when you select Connect on Demand . The default setting is 0, which means the Internet session does not timeout.
PPPoE Pass Through (PPPoE encapsulation only)	This field is available when you select PPPoE encapsulation. In addition to the BCM50a Integrated Router built-in PPPoE client, you can enable PPPoE pass through to allow up to ten hosts on the LAN to use PPPoE client software on their computers to connect to the ISP using the BCM50a Integrated Router. Each host can have a separate account and a public WAN IP address. PPPoE pass through is an alternative to NAT for applications where NAT is not appropriate. Disable PPPoE pass through if you do not need to allow hosts on the LAN to use PPPoE client software on their computers to connect to the ISP.
Subnet Mask (ENET ENCAP encapsulation only)	Enter a subnet mask in dotted decimal notation.
ENET ENCAP Gateway (ENET ENCAP encapsulation only)	You must specify a gateway IP address (supplied by your ISP) when you select ENET ENCAP in the Encapsulation field.
Apply	Click Apply to save the changes.
Reset	Click Reset to begin configuring this screen afresh.

Configuring WAN IP

To change the WAN IP settings of your BCM50a Integrated Router, click **WAN**, then the **WAN IP** tab. This screen varies according to the type of encapsulation you select.

If your ISP did *not* assign you a fixed IP address, click **Get automatically from ISP (Default)**; otherwise click **Use fixed IP Address** and enter the IP address in the field **My WAN IP Address**.

Figure 26 WAN: IP

WAN

The screenshot shows a configuration window for WAN settings. At the top, there are four tabs: 'General', 'WAN ISP', 'WAN IP', and 'Traffic Redirect'. The 'WAN IP' tab is currently selected. Below the tabs, the 'WAN IP Address Assignment' section contains two radio buttons: 'Get automatically from ISP (Default)' and 'Use fixed IP address'. The 'Use fixed IP address' option is selected. Below this, there are three input fields: 'My WAN IP Address', 'Remote IP Address', and 'Remote IP Subnet Mask', all containing the value '0.0.0.0'. The 'Network Address Translation' section includes a dropdown menu set to 'None', a 'Metric' input field with '1', a 'Private' dropdown set to 'No', and dropdown menus for 'RIP Direction' (None), 'RIP Version' (RIP-1), and 'Multicast' (None). The 'Call Schedule' section has four dropdown menus labeled '1st Schedule Set', '2nd Schedule Set', '3rd Schedule Set', and '4th Schedule Set', all set to 'None'. The 'Windows Networking (NetBIOS over TCP/IP)' section contains two checkboxes: 'Allow between WAN and LAN (You also need to create a firewall rule!)' and 'Allow Trigger Dial', both of which are unchecked. At the bottom of the window are 'Apply' and 'Reset' buttons.

Tab	Selected
General	No
WAN ISP	No
WAN IP	Yes
Traffic Redirect	No

WAN IP Address Assignment

Get automatically from ISP (Default)

Use fixed IP address

My WAN IP Address: 0.0.0.0

Remote IP Address: 0.0.0.0

Remote IP Subnet Mask: 0.0.0.0

Network Address Translation: None

Metric: 1

Private: No

RIP Direction: None

RIP Version: RIP-1

Multicast: None

Call Schedule

1st Schedule Set: None

2nd Schedule Set: None

3rd Schedule Set: None

4th Schedule Set: None

Windows Networking (NetBIOS over TCP/IP)

Allow between WAN and LAN (You also need to create a firewall rule!)

Allow Trigger Dial

Buttons: Apply, Reset

Table 19 describes the fields in Figure 26.

Table 19 WAN: IP

Label	Description
Get automatically from ISP	Select this option if your ISP did not assign you a fixed IP address. This is the default selection.
Use fixed IP address	Select this option if your ISP assigned a fixed IP address.
My WAN IP Address	Enter your WAN IP address in this field if you selected Use Fixed IP Address .
My WAN IP Subnet Mask (RFC1483 encapsulation only)	Type your network's IP subnet mask.
Remote IP Address (or Gateway IP Address)	Type the IP address of the remote network or gateway. The gateway is an immediate neighbor of your BCM50a Integrated Router that will forward the packet to the destination. On the LAN, the gateway must be a router on the same segment as your BCM50a Integrated Router; over the WAN, the gateway must be the IP address of one of the remote nodes.
Remote IP Subnet Mask (PPPoE and PPPoA encapsulation)	When using a LAN to LAN application, type the IP subnet mask of the destination network. 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.
Network Address Translation	<p>With Network Address Translation (NAT), the router translations an Internet protocol address used within one network (for example, a private IP address used in a local network) to a different IP address known within another network (for example, a public IP address used on the Internet). NAT is available when the device is in routing mode.</p> <p>Choose None to disable NAT.</p> <p>Choose SUA Only if you have a single public IP address. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server.</p> <p>Choose Full Feature if you have multiple public IP addresses. Full Feature mapping types include: One-to-One, Many-to-One (SUA/PAT), Many-to-Many Overload, Many- One-to-One and Server. After you select Full Feature, you must configure at least one address-mapping set.</p>

Table 19 WAN: IP

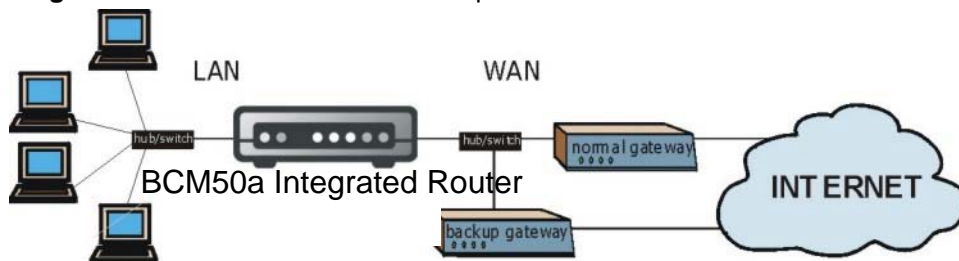
Label	Description
Metric (<p>This field sets this route's priority among the routes the BCM50a Integrated Router uses.</p> <p>The metric represents the cost of transmission. A router determines the best route for transmission by choosing a path with the lowest cost. RIP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. The number must be between 1 and 15; a number greater than 15 means the link is down. The smaller the number, the lower the cost.</p>
Private (PPPoE and PPPoA only)	<p>This parameter determines if the BCM50a Integrated Router includes the route to this remote node in its RIP broadcasts. If set to Yes, this route is kept private and not included in RIP broadcast. If No, the route to this remote node is propagated to other hosts through RIP broadcasts.</p>
RIP Direction	<p>With RIP (Routing Information Protocol), a router can exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets.</p> <p>Choose Both, None, In Only or Out Only.</p> <p>When set to Both or Out Only, the BCM50a Integrated Router broadcasts its routing table periodically.</p> <p>When set to Both or In Only, the BCM50a Integrated Router incorporates RIP information that it receives.</p> <p>When set to None, the BCM50a Integrated Router does not send any RIP packets and ignores any RIP packets received.</p> <p>By default, RIP Direction is set to Both.</p>
RIP Version	<p>The RIP Version field controls the format and the broadcasting method of the RIP packets that the BCM50a Integrated Router sends (it recognizes both formats when receiving).</p> <p>Choose RIP-1, RIP-2B or RIP-2M.</p> <p>RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines since they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also. By default, the RIP Version field is set to RIP-1.</p>

Table 19 WAN: IP

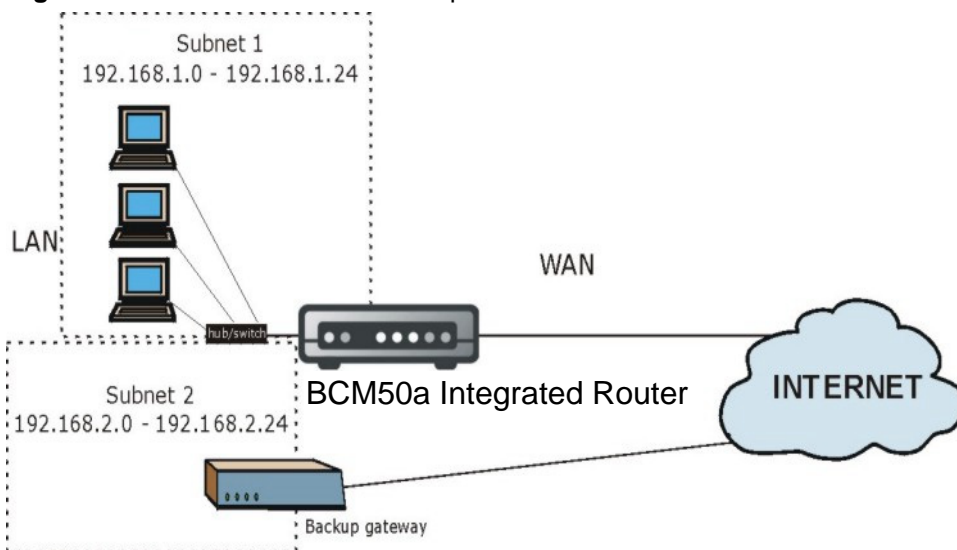
Label	Description
Multicast	Choose None (default), IGMP-V1 or IGMP-V2 . IGMP (Internet Group Multicast Protocol) is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data. IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. If you want to read more detailed information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of <i>Internet Group Management Protocol</i> (RFC 2236).
Call Schedule (PPPoE and PPPoA encapsulation)	Apply call schedule sets for this remote node. Use the Call Schedule screens to configure call schedule sets (see Chapter 20, "Call scheduling screens," on page 373).
Windows Networking (NetBIOS over TCP/IP):	Windows Networking (NetBIOS over TCP/IP): NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. For some dial-up services, such as PPPoE, NetBIOS packets cause unwanted calls.
Allow from WAN to LAN	Select this check box to forward NetBIOS packets from the LAN to the WAN and from the WAN to the LAN. If your firewall is enabled with the default policy set to block WAN to LAN traffic, you must also create a WAN to LAN firewall rule that forwards NetBIOS traffic. Clear this check box to block all NetBIOS packets going from the LAN to the WAN and from the WAN to the LAN. This field does the same as the Allow between LAN and WAN field in the LAN IP screen. Enabling one automatically enables the other.
Allow Trigger Dial	Select this option to allow NetBIOS packets to initiate calls.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Traffic redirect

Traffic redirect forwards WAN traffic to a backup gateway when the BCM50a Integrated Router cannot connect to the Internet through its normal gateway. Connect the backup gateway on the WAN so that the BCM50a Integrated Router still provides firewall protection. This feature is not available on all models.

Figure 27 Traffic Redirect WAN Setup

The network topology illustrated in [Figure 28](#) avoids triangle route security issues when the backup gateway is connected to the LAN. Use IP alias to configure the LAN into two or three logical networks with the BCM50a Integrated Router itself as the gateway for each LAN network. Put the protected LAN in one subnet (Subnet 1 in [Figure 28](#)) and the backup gateway in another subnet (Subnet 2). Configure a LAN to LAN/BCM50a Integrated Router firewall rule that forwards packets from the protected LAN (Subnet 1) to the backup gateway (Subnet 2).

Figure 28 Traffic Redirect LAN Setup

Configuring Traffic Redirect

To change the traffic redirect settings, click **WAN**, then the **Traffic Redirect** tab. The screen appears as shown in [Figure 29](#).

Figure 29 Traffic Redirect

WAN

The screenshot shows the WAN configuration interface. At the top, there are four tabs: 'General', 'WAN ISP', 'WAN IP', and 'Traffic Redirect'. The 'Traffic Redirect' tab is selected. Below the tabs, there is a section with a checkbox labeled 'Active' which is currently unchecked. Underneath the checkbox is a text input field labeled 'Backup Gateway IP Address' containing the value '0.0.0.0'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

[Table 20](#) describes the fields in [Figure 29](#).

Table 20 Traffic Redirect

Label	Description
Active	Select this check box to have the BCM50a Integrated Router use traffic redirect if the normal WAN connection goes down.
Backup Gateway IP Address	Type the IP address of your backup gateway in dotted decimal notation. The BCM50a Integrated Router automatically forwards traffic to this IP address if the BCM50a Integrated Router's Internet connection terminates.
Apply	Click Apply to save your changes back to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Configuring Dial Backup

To change the dial backup settings, click **WAN**, then the **Dial Backup** tab. The screen appears as shown in [Figure 30](#).



Note: To enable or disable Dial Back-up on the router, check or uncheck the 'Enable Dial Back-Up' function. None of the other Basic or Advanced Settings should be changed.

Figure 30 Dial Backup Setup
WAN

General	WAN ISP	WAN IP	Traffic Redirect	Dial Backup
<input type="checkbox"/> Enable Dial Backup				
Basic Settings				
Login Name	<input type="text"/>			
Password	<input type="password"/>			
Retype to Confirm	<input type="password"/>			
Authentication Type	CHAP/PAP			
Primary Phone Number	<input type="text"/>			
Secondary Phone Number	<input type="text"/> <small>Optional</small>			
Dial Backup Port Speed	115200			
AT Command Initial String	et&fs0=0			
Advanced Modem Setup	<input type="button" value="Edit"/>			
TCP/IP Options				
Priority (Metric)	15 <small>1(Highest) ~ 16(Lowest)</small>			
<input checked="" type="radio"/> Get IP Address Automatically from Remote Server				
<input type="radio"/> Use Fixed IP Address				
My WAN IP Address	<input type="text" value="0.0.0.0"/>			
Remote Node IP Address	<input type="text" value="0.0.0.0"/>			
Remote IP Subnet Mask	<input type="text" value="0.0.0.0"/>			
<input checked="" type="checkbox"/> Enable SUA				
<input type="checkbox"/> Enable RIP				
RIP Version	RIP-1			
RIP Direction	Both			
<input type="checkbox"/> Broadcast Dial Backup Route				
<input type="checkbox"/> Enable Multicast				
Multicast Version	IGMPv1			
PPP Options				
PPP Encapsulation	Standard PPP			
<input type="checkbox"/> Enable Compression				
Budget				
<input type="radio"/> Always On				
<input checked="" type="radio"/> Configure Budget				
Allocated Budget	<input type="text" value="0"/> <small>(Minutes)</small>			
Period	<input type="text" value="0"/> <small>(Hours)</small>			
Idle Timeout	<input type="text" value="100"/> <small>(Seconds)</small>			
Call Schedule				
1st Schedule Set	None			
2nd Schedule Set	None			
3rd Schedule Set	None			
4th Schedule Set	None			
<input type="button" value="Apply"/> <input type="button" value="Reset"/>				

Table 21 describes the fields in Figure 30.

Table 21 Dial Backup Setup

Label	Description
Enable Dial Backup	Select this check box to turn on dial backup.
Basic Settings	
Login Name	Type the logon name assigned by your ISP.
Password	Type the password assigned by your ISP.
Retype to Confirm	Type your password again in this field.
Authentication Type	Use the drop-down list to select an authentication protocol for outgoing calls. Options are: CHAP/PAP - Your BCM50a Integrated Router accepts either CHAP or PAP when requested by this remote node. CHAP - Your BCM50a Integrated Router accepts CHAP only. PAP - Your BCM50a Integrated Router accept PAP only.
Primary/ Secondary Phone Number	Type the first (primary) phone number from the ISP for this remote node. If the Primary Phone number is busy or does not answer, your BCM50a Integrated Router dials the Secondary Phone number, if available. Some areas require dialing the pound sign # before the phone number for local calls. Include a # symbol at the beginning of the phone numbers as required.
Dial Backup Port Speed	Use the drop-down list to select the speed of the connection between the Dial Backup port and the external device. Available speeds are: 9 600, 19 200, 38 400, 57 600, 115 200 or 230 400 b/s.
AT Command Initial String	Type the AT command string to initialize the WAN device. Consult the manual of your WAN device connected to your Dial Backup port for specific AT commands.
Advanced Modem Setup	Click this button to display the Advanced Setup screen and edit the details of your dial backup setup.
TCP/IP Options	
Priority (Metric)	This field sets this route's priority among the three routes the BCM50a Integrated Router uses (normal, traffic redirect and dial backup). Type a number (1 to 15) to set the priority of the dial backup route for data transmission. The smaller the number, the higher the priority. If the three routes have the same metrics, the priority of the routes is as follows: WAN, Traffic Redirect, Dial Backup .
Get IP Address Automatically from Remote Server	Select this check box if your ISP will automatically assign you an IP address (dynamic IP address).

Table 21 Dial Backup Setup

Label	Description
Used Fixed IP Address	Select this check box if your ISP assigned you a fixed IP address and then enter the IP address in the following field.
My WAN IP Address	Leave the field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) assign your WAN IP address, if you do not know it. Type your WAN IP address here, if you know it (static). This is the address assigned to your local BCM50a Integrated Router, not the remote router.
Remote IP Subnet Mask	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically send its subnet mask, if you do not know it. Type the remote gateway's subnet mask here, if you know it (static).
Remote Node IP Address	Leave this field set to 0.0.0.0 (default) to have the ISP or other remote router dynamically (automatically) send its IP address, if you do not know it. Type the remote gateway's IP address here, if you know it (static).
Enable SUA	Using Network Address Translation (NAT), the router translates an Internet protocol address used within one network to a different IP address known within another network. SUA (Single User Account) is a subset of NAT that supports two types of mapping: Many-to-One and Server. When you select this option the BCM50a Integrated Router uses Address Mapping Set 255. Clear this option to disable NAT.
Enable RIP	Select this check box to turn on RIP (Routing Information Protocol), which allows a router to exchange routing information with other routers.
RIP Version	The RIP Version field controls the format and the broadcasting method of the RIP packets that the BCM50a Integrated Router sends (it recognizes both formats when receiving). Choose RIP-1 , RIP-2B or RIP-2M . RIP-1 is universally supported; but RIP-2 carries more information. RIP-1 is probably adequate for most networks, unless you have an unusual network topology. Both RIP-2B and RIP-2M sends the routing data in RIP-2 format; the difference being that RIP-2B uses subnet broadcasting while RIP-2M uses multicasting. Multicasting can reduce the load on nonrouter machines because they generally do not listen to the RIP multicast address and so do not receive the RIP packets. However, if one router uses multicasting, then all routers on your network must use multicasting, also.

Table 21 Dial Backup Setup

Label	Description
RIP Direction	<p>RIP (Routing Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction field controls the sending and receiving of RIP packets.</p> <p>Choose Both, In Only or Out Only.</p> <p>When set to Both or Out Only, the BCM50a Integrated Router broadcasts its routing table periodically.</p> <p>When set to Both or In Only, the BCM50a Integrated Router incorporates RIP information that it receives.</p>
Broadcast Dial Backup Route	Select this check box to forward the backup route broadcasts to the WAN.
Enable Multicast	Select this check box to turn on IGMP (Internet Group Multicast Protocol). IGMP is a network layer protocol used to establish membership in a Multicast group—it is not used to carry user data.
Multicast Version	Select IGMP-v1 or IGMP-v2 . IGMP version 2 (RFC 2236) is an improvement over version 1 (RFC 1112) but IGMP version 1 is still in wide use. For more information about interoperability between IGMP version 2 and version 1, see sections 4 and 5 of <i>Internet Group Management Protocol</i> (RFC 2236).
Budget	
Always On	Select this check box to have the dial backup connection on all of the time.
Configure Budget	Select this check box to have the dial backup connection on during the time that you select.
Allocated Budget	Type the amount of time (in minutes) that the dial backup connection can be used during the time configured in the Period field. Set an amount that is less than the time period configured in the Period field.
Period	Type the time period (in hours) for how often the budget is reset. For example, to allow calls to this remote node for a maximum of 10 minutes every hour, set the Allocated Budget to 10 (minutes) and the Period to 1 (hour).
Idle Timeout	Type the number of seconds of idle time (when there is no traffic from the BCM50a Integrated Router to the remote node) for the BCM50a Integrated Router to wait before it automatically disconnects the dial backup connection. This option applies only when the BCM50a Integrated Router initiates the call. The dial backup connection never times out if you set this field to 0 (it is the same as selecting Always On).
Call Schedule Sets	Specify call schedule sets to use on the dial backup connection. The call schedule sets must already be configured (see Chapter 20, "Call scheduling screens," on page 373).

Table 21 Dial Backup Setup

Label	Description
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Advanced Modem Setup

AT Command Strings

For regular telephone lines, the default Dial string tells the modem that the line uses tone dialing. ATDT is the command for a switch that requires tone dialing. If your switch requires pulse dialing, change the string to ATDP.

For ISDN lines, there are many more protocols and operational modes. Consult the documentation of your TA. You need additional commands in both Dial and Init strings.

DTR Signal

The majority of WAN devices default to hanging up the current call when the DTR (Data Terminal Ready) signal is dropped by the DTE. If the **Drop DTR When Hang Up** check box is selected, the BCM50a Integrated Router uses this hardware signal to force the WAN device to hang up, in addition to issuing the drop command ATH.

Response Strings

The response strings tell the BCM50a Integrated Router the tags, or labels, immediately preceding the various call parameters sent from the WAN device. The response strings have not been standardized; consult the documentation of your WAN device to find the correct tags.

Configuring Advanced Modem Setup

Click the **Edit** button in the **Dial Backup** screen to display the **Advanced Setup** screen shown in [Figure 31](#).



Note: To ensure proper operation with the BCM50, none of the default settings should be changed.

Figure 31 Advanced Setup
WAN - ADVANCED MODEM SETUP

AT Command Strings	
Dial	atdt
Drop	^^+++^^ath
Answer	ata
<input checked="" type="checkbox"/> Drop DTR When Hang Up	

AT Response Strings	
CLID	NMBR
Called ID	
Speed	CONNECT

Call Control	
Dial Timeout (sec)	60
Retry Count	0
Retry Interval (sec)	10
Drop Timeout (sec)	20
Call Back Delay (sec)	15

Apply Cancel

Table 22 describes the fields in Figure 31.

Table 22 Advanced Setup

Label	Description	Example
AT Command Strings		
Dial	Type the AT Command string to make a call.	atdt
Drop	Type the AT Command string to drop a call. ~ represents a one-second wait. For example, ~~~+++~ath can be used if your modem has a slow response time.	~~~+++~ath
Answer	Type the AT Command string to answer a call.	ata
Drop DTR When Hang Up	Select this check box to have the BCM50a Integrated Router drop the DTR (Data Terminal Ready) signal after the AT Command String: Drop is sent out.	
AT Response Strings		
CLID	Type the keyword that precedes the CLID (Calling Line Identification) in the AT response string. This lets the BCM50a Integrated Router capture the CLID in the AT response string that comes from the WAN device. CLID is required for CLID authentication.	NMBR
Called ID	Type the keyword preceding the dialed number.	
Speed	Type the keyword preceding the connection speed.	CONNECT
Call Control		
Dial Timeout (sec)	Type a number of seconds for the BCM50a Integrated Router to try to set up an outgoing call before timing out (stopping).	60
Retry Count	Type a number of times for the BCM50a Integrated Router to retry a busy or no answer phone number before blacklisting the number.	0
Retry Interval (sec)	Type a number of seconds for the BCM50a Integrated Router to wait before trying another call after a call has failed. This applies before a phone number is blacklisted.	10
Drop Timeout (sec)	Type the number of seconds for the BCM50a Integrated Router to wait before dropping the DTR signal if it does not receive a positive disconnect confirmation.	20

Table 22 Advanced Setup

Label	Description	Example
Call Back Delay (sec)	Type a number of seconds for the BCM50a Integrated Router to wait between dropping a callback request call and dialing the corresponding callback call.	15
Apply	Click Apply to save your changes to the BCM50a Integrated Router.	
Reset	Click Reset to begin configuring this screen afresh.	

Chapter 8

Network Address Translation (NAT) Screens

This chapter discusses how to configure NAT on the BCM50a Integrated Router.

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, is changed to a different IP address known within another network.

NAT definitions

Inside/outside denotes where a host is located relative to the BCM50a Integrated Router. 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. [Table 23](#) summarizes this information.

Table 23 NAT definitions

Term	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.



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

What NAT does

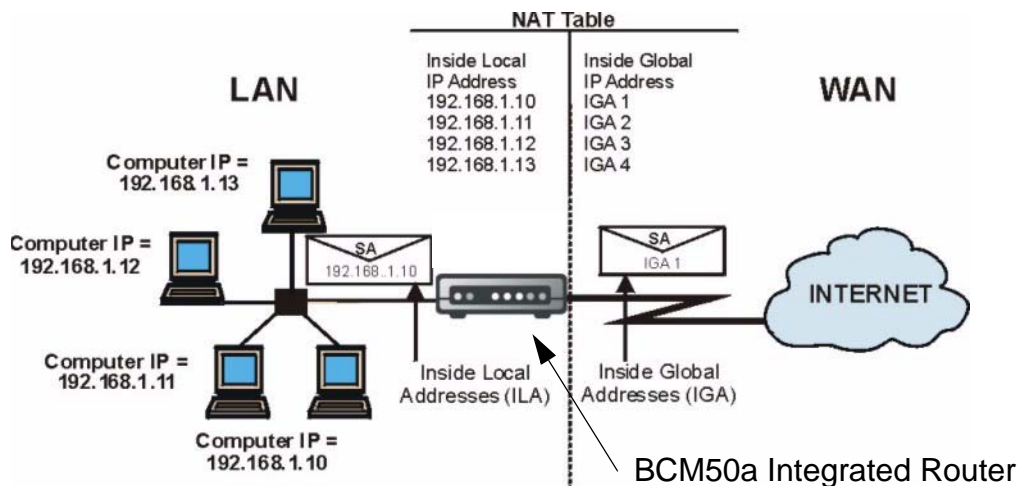
In the simplest form, NAT changes the source IP address in a packet received from a subscriber (the inside local address) to another (the inside global address) before forwarding the packet to the WAN side. When the response comes back, NAT translates the destination address (the inside global address) 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. You can make designated servers on the LAN accessible to the outside world. If you do not define any servers (for Many-to-One and Many-to-Many Overload mapping), NAT offers the additional benefit of firewall protection. With no servers defined, your BCM50a Integrated Router filters out all incoming inquiries, thus preventing intruders from probing your network. For more information about IP address translation, refer to *The IP Network Address Translator (NAT)* (RFC 1631).

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 (and TCP or UDP source port numbers for Many-to-One and Many-to-Many Overload NAT mapping) in each packet and then forwards it to the Internet. The BCM50a Integrated Router keeps track of the original addresses and port numbers so incoming reply packets can have their original values restored, as illustrated in [Figure 32](#).

Figure 32 How NAT works



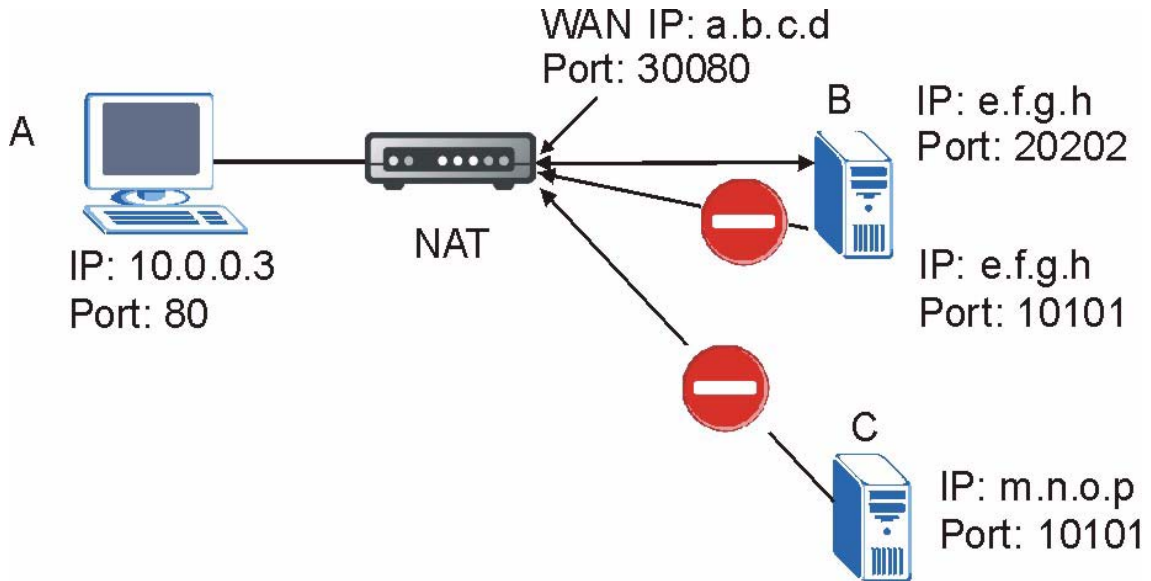
Port restricted cone NAT

The BCM50a Integrated Router uses port restricted cone NAT.

Port restricted cone NAT maps all requests from the same private IP address and port to the same public IP address and port. A host on the Internet can only send a packet to the private IP address and port if the private IP address and port has previously sent a packet to the IP address and port of that host.

In [Figure 33](#), B can send packets, with source IP address e.f.g.h and port 20202 to A because A previously sent a packet to IP address e.f.g.h and port 20202. B cannot send packets, with source IP address e.f.g.h and port 10101 to A because A has not sent a packet to IP address e.f.g.h and port 10101.

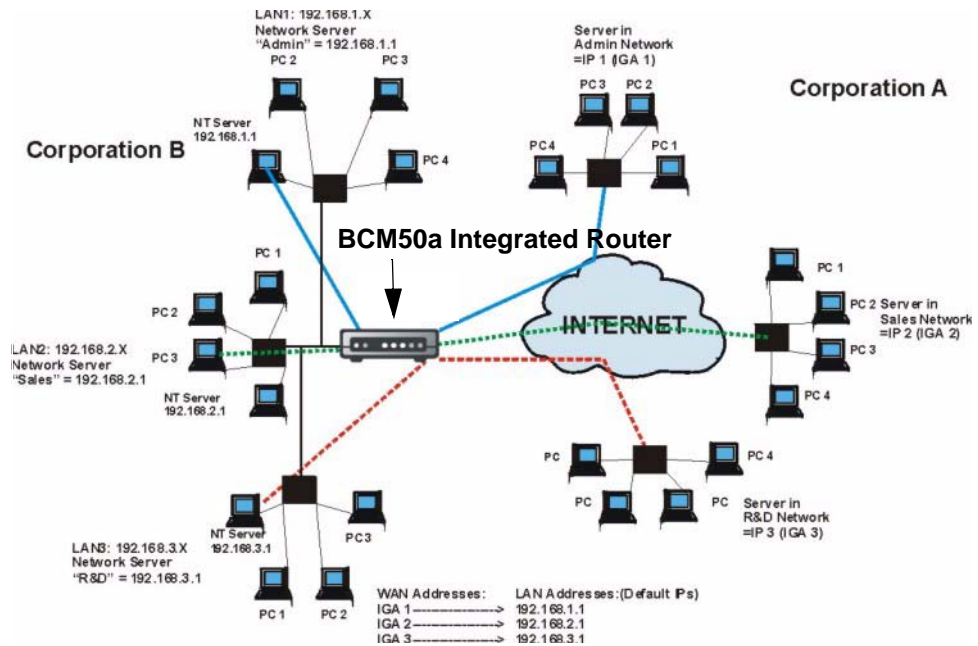
Figure 33 Port Restricted Cone NAT



NAT application

[Figure 34](#) illustrates a possible NAT application, where three inside LANs (logical LANs using IP Alias) behind the BCM50a Integrated Router can communicate with three distinct WAN networks. More examples follow at the end of this chapter.

Figure 34 NAT application with IP Alias



NAT mapping types

NAT supports five types of IP/port mapping. They are:

- **One to One:** In One-to-One mode, the BCM50a Integrated Router maps one local IP address to one global IP address.
- **Many to One:** In Many-to-One mode, the BCM50a Integrated Router maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the Single User Account feature (the SUA Only option).
- **Many to Many Overload:** In Many-to-Many Overload mode, the BCM50a Integrated Router maps the multiple local IP addresses to shared global IP addresses.
- **Many One to One:** In Many-One-to-One mode, the BCM50a Integrated Router maps each local IP address to a unique global IP address.
- **Server:** With this type you can specify inside servers of different services behind the NAT to be accessible to the outside world. Port numbers do **not** change for **One-to-One** and **Many-One-to-One** NAT mapping types.

Table 24 summarizes these types.

Table 24 NAT mapping type

Type	IP Mapping	SMT Abbreviations
One-to-One	ILA1 \leftrightarrow IGA1	1-1
Many-to-One (SUA/PAT)	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA1 ...	M-1
Many-to-Many Overload	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA1 ILA4 \leftrightarrow IGA2 ...	M-M Ov
Many-One-to-One	ILA1 \leftrightarrow IGA1 ILA2 \leftrightarrow IGA2 ILA3 \leftrightarrow IGA3 ...	M-1-1
Server	Server 1 IP \leftrightarrow IGA1 Server 2 IP \leftrightarrow IGA1 Server 3 IP \leftrightarrow IGA1	Server

Using NAT



Note: You must create a firewall rule in addition to setting up SUA/NAT, to allow traffic from the WAN to be forwarded through the BCM50a Integrated Router.

SUA (Single User Account) versus NAT

SUA (Single User Account) is an implementation of a subset of NAT that supports two types of mapping, **Many-to-One** and **Server**. The BCM50a Integrated Router also supports **Full Feature** NAT to map multiple global IP addresses to multiple private LAN IP addresses of clients or servers using mapping types. Select either **SUA Only** or **Full Feature** in **WAN IP**.

SUA Server

A SUA server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the outside world even though SUA makes your whole inside network appear as a single computer to the outside world.

You can enter a single port number or a range of port numbers to be forwarded, and the local IP address of the desired server. The port number identifies a service; for example, web service is on port 80 and FTP on port 21. In some cases, such as for unknown services or where one server can support more than one service (for example, both FTP and web service), it is better to specify a range of port numbers. You can allocate a server IP address that corresponds to a port or a range of ports.

With many residential broadband ISP accounts you cannot run any server processes (such as a Web or FTP server) from your location. Your ISP periodically checks for servers and can suspend your account if it discovers any active services at your location. If you are unsure, refer to your ISP.

Default server IP address

In addition to the servers for specified services, NAT supports a default server IP address. A default server receives packets from ports that are not specified in this screen.



Note: If you do not assign a Default Server IP Address, the BCM50a Integrated Router discards all packets received for ports that are not specified here or in the remote management setup.

Port forwarding: Services and Port Numbers

The most often used port numbers are shown in [Table 25](#). Refer to *Assigned Numbers* (RFC 1700) for further information about port numbers.

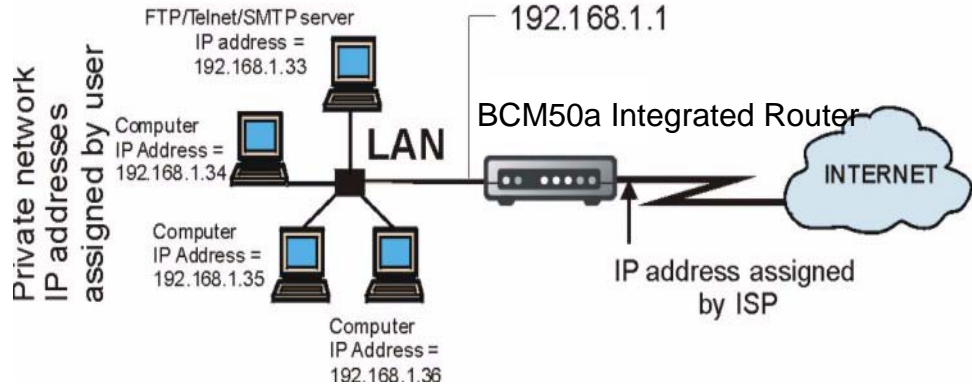
Table 25 Services and port numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Configuring servers behind SUA (example)

For example, you want to assign ports 22-25 to one server, port 80 to another and assign a default server IP address of 192.168.1.35, as shown in [Figure 35](#).

Figure 35 Multiple servers behind NAT example
The NAT network appears as a single host on the Internet



Configuring SUA Server



Note: If you do not assign a Default Server IP Address, then all packets received for ports not specified in this screen are discarded.

Click **SUA/NAT** to open the **SUA Server** screen.

Refer to [Chapter 10, “Firewalls,”](#) on page 145 and [Chapter 11, “Firewall screens,”](#) on page 161 for port numbers commonly used for particular services.

Figure 36 SUA/NAT setup

SUA/NAT

The screenshot shows the 'Address Mapping' tab of the SUA/NAT setup. At the top, there are three tabs: 'SUA Server', 'Address Mapping', and 'Trigger Port'. Below the tabs, there is a 'Default Server' field with the value '0.0.0.0'. Underneath is a table with 11 rows. The table has the following columns: '#', 'Active', 'Name', 'Start Port', 'End Port', and 'Server IP Address'. Each row has a checkbox in the 'Active' column, an empty text field in the 'Name' column, and '0' in the 'Start Port' and 'End Port' columns. The 'Server IP Address' column contains '0.0.0.0' for every row. At the bottom of the form, there are two buttons: 'Apply' and 'Reset'.

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

Table 26 describes the fields in Figure 36.

Table 26 SUA/NAT setup

Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, then all packets received for ports not specified in this screen are discarded.
#	Number of an individual SUA server entry.

Table 26 SUA/NAT setup

Label	Description
Active	Select this check box to enable the SUA server entry. Clear this check box to disallow forwarding of these ports to an inside server without having to delete the entry.
Name	Enter a name to identify this port forwarding rule.
Start Port	Enter a port number here. To forward only one port, enter it again in the End Port field. To specify a range of ports, enter the last port to be forwarded in the End Port No field
End Port	
Server IP Address	Enter the inside IP address of the server here.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to clear your changes.

Configuring Address Mapping

Ordering your rules is important because the BCM50a Integrated Router applies the rules in the order that you specify. When a rule matches the current packet, the BCM50a Integrated Router takes the corresponding action and the remaining rules are ignored. If there are any empty rules before your new configured rule, your configured rule is pushed up by that number of empty rules. For example, if you have already configured rules 1 to 6 in your current set and you configure rule number 9. In the set summary screen, the new rule becomes rule 7, not 9. If you delete rule 4, rules 5 to 7 are pushed up by 1 rule, so old rules 5, 6, and 7 become new rules 4, 5, and 6.

To change the NAT address mapping settings, click **SUA/NAT**, then the **Address Mapping** tab. The screen appears as shown in [Figure 37](#).

Figure 37 Address Mapping

SUA/NAT

SUA Server		Address Mapping		Trigger Port		
<p>Note: Change may not take effect on existing NAT sessions. A system restart will guarantee the change to take effect.</p>						
#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	
<input checked="" type="radio"/> 1	-	
<input type="radio"/> 2	-	
<input type="radio"/> 3	-	
<input type="radio"/> 4	-	
<input type="radio"/> 5	-	
<input type="radio"/> 6	-	
<input type="radio"/> 7	-	
<input type="radio"/> 8	-	
<input type="radio"/> 9	-	
<input type="radio"/> 10	-	
<input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>						

Table 27 describes the fields in Figure 37.

Table 27 Address Mapping

Label	Description
Local Start IP	This refers to the Inside Local Address (ILA), that is the starting local IP address. Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local Address (ILA). If the rule is for all local IP addresses, then this field displays 0.0.0.0 and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This refers to the Inside Global IP Address (IGA). 0.0.0.0 is for a dynamic IP address from your ISP with Many-to-One and Server mapping types.
Global End IP	This is the ending Inside Global Address (IGA), that is the starting global IP address. This field is N/A for One-to-One , Many-to-One and Server mapping types.

Table 27 Address Mapping

Label	Description
Type	<ol style="list-style-type: none">1. One-to-One mode maps one local IP address to one global IP address. Note that port numbers do not change for the One-to-one NAT mapping type.2. Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (that is, PAT, port address translation), the Single User Account feature.3. Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses.4. Many One-to-One mode maps each local IP address to unique global IP addresses.5. Server permits you to specify inside servers of different services behind the NAT to be accessible to the outside world.
Edit	Click Edit to go to the Address Mapping Rule screen.
Delete	Click Delete to delete an address mapping rule.
Insert	Click Insert to insert a new mapping rule before an existing one.

Configuring Address Mapping

To edit an Address Mapping rule, click the **Edit** button to display the screen shown in [Figure 38](#).

Figure 38 Address Mapping edit
SUA/NAT - Address Mapping

Address Mapping Rule

Type: One-to-One

Local Start IP: 0.0.0.0

Local End IP: N/A

Global Start IP: 0.0.0.0

Global End IP: N/A

Apply Reset

Table 28 describes the fields in Figure 38.

Table 28 Address Mapping edit

Label	Description
Type	Choose the port mapping type from one of the following. 1. One-to-One : One-to-one mode maps one local IP address to one global IP address. Note that port numbers do not change for One-to-one NAT mapping type. 2. Many-to-One : Many-to-One mode maps multiple local IP addresses to one global IP address. This is equivalent to SUA (for example, PAT, port address translation), the Single User Account feature. 3. Many-to-Many Ov (Overload): Many-to-Many Overload mode maps multiple local IP addresses to shared global IP addresses. 4. Many One-to-One : Many One-to-one mode maps each local IP address to unique global IP addresses. 5. Server : With this type, you can specify inside servers of different services behind the NAT to be accessible to the outside world.
Local Start IP	This is the starting Inside Local IP Address (ILA). Local IP addresses are N/A for Server port mapping.
Local End IP	This is the end Inside Local IP Address (ILA). If your rule is for all local IP addresses, then enter 0.0.0.0 as the Local Start IP address and 255.255.255.255 as the Local End IP address. This field is N/A for One-to-One and Server mapping types.
Global Start IP	This is the starting Inside Global IP Address (IGA). Enter 0.0.0.0 here if you have a dynamic IP address from your ISP.

Table 28 Address Mapping edit

Label	Description
Global End IP	This is the ending Inside Global IP Address (IGA). This field is N/A for One-to-One , Many-to-One and Server mapping types.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

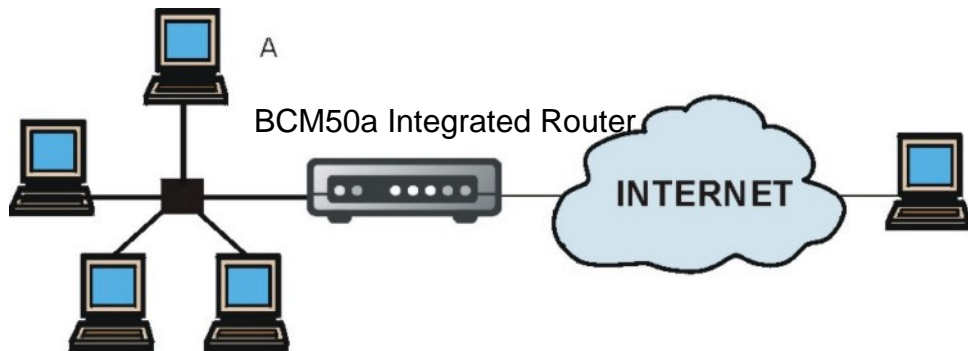
Trigger Port Forwarding

Some services use a dedicated range of ports on the client side and a dedicated range of ports on the server side. With regular port forwarding you set a forwarding port in NAT to forward a service (coming in from the server on the WAN) to the IP address of a computer on the client side (LAN). The problem is that port forwarding only forwards a service to a single LAN IP address. In order to use the same service on a different LAN computer, you have to manually replace the LAN computer's IP address in the forwarding port with another LAN computer's IP address,

Trigger port forwarding solves this problem by allowing computers on the LAN to dynamically take turns using the service. The BCM50a Integrated Router records the IP address of a LAN computer that sends traffic to the WAN to request a service with a specific port number and protocol (a trigger port). When the WAN port on the BCM50a Integrated Router receives a response with a specific port number and protocol (incoming port), the BCM50a Integrated Router forwards the traffic to the LAN IP address of the computer that sent the request. After that connection closes, another computer on the LAN can use the service in the same manner. This way, you do not need to configure a new IP address each time you want a different LAN computer to use the application.

Trigger Port Forwarding example

[Figure 39](#) illustrates an example of trigger port forwarding.

Figure 39 Trigger Port Forwarding process: example

- 1 Jane (A) requests a file from the Real Audio server (port 7070).
- 2 Port 7070 is a trigger port and causes the BCM50a Integrated Router to record Jane's computer IP address. The BCM50a Integrated Router associates Jane's computer IP address with the incoming port range of 6970-7170.
- 3 The Real Audio server responds using a port number ranging between 6970-7170.
- 4 The BCM50a Integrated Router forwards the traffic to Jane's computer IP address.
- 5 Only Jane can connect to the Real Audio server until the connection is closed or times out. The BCM50a Integrated Router times out in three minutes with UDP (User Datagram Protocol) or two hours with TCP/IP (Transfer Control Protocol/Internet Protocol).

Two points to remember about Trigger Ports

Trigger events only happen on data that is coming from inside the BCM50a Integrated Router and going to the outside.

If an application needs a continuous data stream, that port (range) is tied up so that another computer on the LAN cannot trigger it.

Configuring Trigger Port Forwarding

To change trigger port settings of your BCM50a Integrated Router, click **SUA/NAT** and the **Trigger Port** tab. The screen appears as shown in [Figure 40](#).



Note: Only one LAN computer can use a trigger port (range) at a time.

Figure 40 Trigger Port
SUA/NAT

SUA Server		Addr Mapping		Trigger Port	
#	Name	Incoming		Trigger	
		Start Port	End Port	Start Port	End Port
1		0	0	0	0
2		0	0	0	0
3		0	0	0	0
4		0	0	0	0
5		0	0	0	0
6		0	0	0	0
7		0	0	0	0
8		0	0	0	0
9		0	0	0	0
10		0	0	0	0
11		0	0	0	0
12		0	0	0	0

Apply Reset

Table 29 describes the fields in Figure 40.

Table 29 Trigger Port

Label	Description
No.	This is the rule index number (read-only).
Name	Type a unique name (up to 15 characters) for identification purposes. All characters are permitted, including spaces.
Incoming	Incoming is a port (or a range of ports) that a server on the WAN uses when it sends out a particular service. The BCM50a Integrated Router forwards the traffic with this port (or range of ports) to the client computer on the LAN that requested the service.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Trigger	The trigger port is a port (or a range of ports) that causes (or triggers) the BCM50a Integrated Router to record the IP address of the LAN computer that sent the traffic to a server on the WAN.
Start Port	Type a port number or the starting port number in a range of port numbers.
End Port	Type a port number or the ending port number in a range of port numbers.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 9

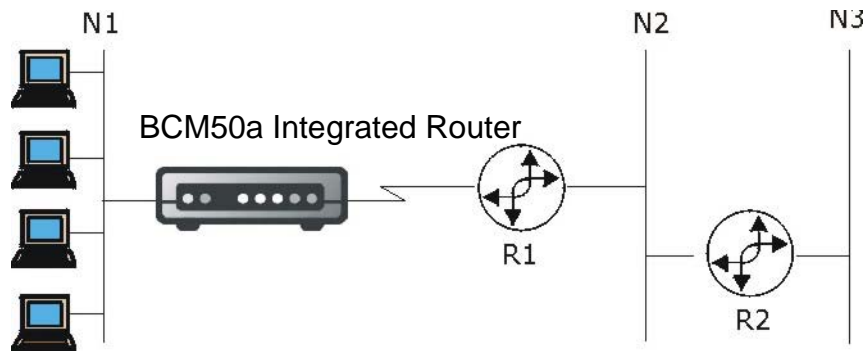
Static Route screens

This chapter shows you how to configure static routes for your BCM50a Integrated Router.

Static Route overview

Each remote node specifies only the network to which the gateway is directly connected, and the BCM50a Integrated Router has no knowledge of the networks beyond. For instance, the BCM50a Integrated Router knows about network N2 in [Figure 41](#) through remote node Router 1. However, the BCM50a Integrated Router is unable to route a packet to network N3 because it does not know that there is a route through the same remote node Router 1 (through gateway Router 2). The static routes are for you to tell the BCM50a Integrated Router about the networks beyond the remote nodes.

Figure 41 Example of Static Routing topology



Configuring IP Static Route

Click **STATIC ROUTE** to open the **Route Entry** screen.



Note: The first static route entry is for the default WAN route. You cannot modify or delete this static default route.

Figure 42 Static Route screen

STATIC ROUTE

IP Static Route

#	Name	Active	Destination	Gateway
1	Reserved	-
2	-	-
3	-	-
4	-	-
5	-	-
6	-	-
7	-	-
8	-	-
9	-	-
10	-	-
11	-	-
12	-	-

Edit Delete

Table 30 describes the fields in Figure 41.

Table 30 IP Static Route summary

Label	Description
#	Number of an individual static route.
Name	Name that describes or identifies this route.
Active	This field shows whether this static route is active (Yes) or not (No).
Destination	This parameter specifies the IP network address of the final destination. Routing is always based on network number.
Gateway	This is the IP address of the gateway. The gateway is a router or switch on the same network segment as the BCM50a Integrated Router LAN or WAN port. The gateway helps forward packets to their destinations.
Edit	Click a static route index number and then click Edit to set up a static route on the BCM50a Integrated Router.

Configuring Route entry

Select a static route index number and click **Edit**. The screen is illustrated in [Figure 43](#). Fill in the required information for each static route.

Figure 43 Edit IP Static Route

STATIC ROUTE - EDIT

The screenshot shows a web-based configuration interface titled "Route Entry". It contains the following fields and controls:

- Route Name:** A text input field.
- Active:** A checkbox.
- Destination IP Address:** A text input field containing "0.0.0.0".
- IP Subnet Mask:** A text input field containing "0.0.0.0".
- Gateway IP Address:** A text input field containing "0.0.0.0".
- Metric:** A text input field containing "2".
- Private:** A checkbox.
- Buttons:** "Apply" and "Reset" buttons at the bottom.

[Table 31](#) describes the fields in [Figure 43](#).

Table 31 Edit IP Static Route

Label	Description
Route Name	Enter the name of the IP static route. Leave this field blank to delete this static route.
Active	This field allows you to activate or deactivate this static route.
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.
IP Subnet Mask	Enter the IP subnet mask here.
Gateway IP Address	Enter the IP address of the gateway. The gateway is a router or switch on the same network segment as the BCM50a Integrated Router LAN or WAN port. The gateway helps forward packets to their destinations.

Table 31 Edit IP Static Route

Label	Description
Metric	Metric 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. Enter 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.
Private	This parameter determines if the BCM50a Integrated Router includes this route to a remote node in its RIP broadcasts. Select this check box to keep this route private and not included in RIP broadcasts. Clear this check box to propagate this route to other hosts through RIP broadcasts.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 10

Firewalls

This chapter gives some background information on firewalls and introduces the BCM50a Integrated Router firewall.

Firewall overview

Originally, the term firewall referred to a construction technique designed to prevent the spread of fire from one room to another. The networking term firewall is a system or group of systems that enforces an access control policy between two networks. It can also be defined as a mechanism used to protect a trusted network from an untrusted network. Of course, firewalls cannot solve every security problem. A firewall is one of the mechanisms used to establish a network security perimeter in support of a network security policy. It must never be the only mechanism or method employed. For a firewall to guard effectively, you must design and deploy it appropriately. This requires integrating the firewall into a broad information security policy. In addition, specific policies must be implemented within the firewall itself.

Types of firewalls

There are three main types of firewalls:

- 1 Packet Filtering firewalls
- 2 Application level firewalls
- 3 Stateful Inspection firewalls

Packet filtering firewalls

Packet filtering firewalls restrict access based on the source or destination computer network address of a packet and the type of application.

Application level firewalls

Application level firewalls restrict access by serving as proxies for external servers. Because they use programs written for specific Internet services, such as HTTP, FTP and Telnet, they can evaluate network packets for valid application specific data. Application level firewalls have a number of general advantages over the default mode of permitting application traffic directly to internal hosts:

- 1 Information hiding prevents the names of internal systems from being made known through DNS to outside systems, because the application gateway is the only host whose name must be made known to outside systems.
- 2 Robust authentication and logging preauthenticates application traffic before it reaches internal hosts and causes it to be logged more effectively than if it were logged with standard host logging. Filtering rules at the packet filtering router can be less complex than if the router needed to filter application traffic and direct it to a number of specific systems. The router need only allow application traffic destined for the application gateway and reject the rest.

Stateful Inspection firewalls

Stateful inspection firewalls restrict access by screening data packets against defined access rules. They make access control decisions based on IP address and protocol. They also inspect the session data to assure the integrity of the connection and to adapt to dynamic protocols. These firewalls generally provide the best speed and transparency; however, they often lack the granular application level access control or caching that some proxies support. For more information, see [“Stateful inspection” on page 153](#).

Firewalls, of one type or another, have become an integral part of standard security solutions for enterprises.

Introduction to the BCM50a Integrated Router firewall

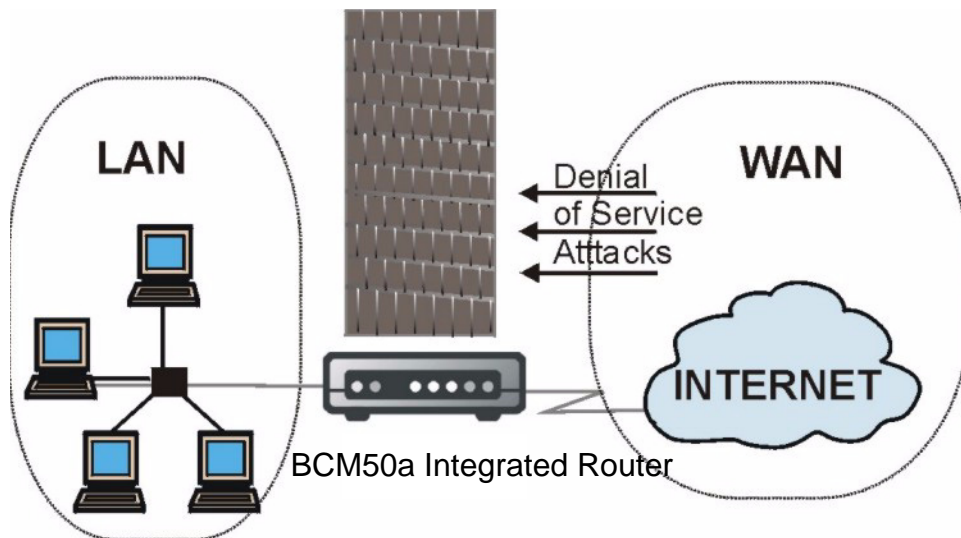
The BCM50a Integrated Router firewall is a stateful inspection firewall ¹ is designed to protect against Denial of Service attacks when activated (in SMT menu 21.2 or in the WebGUI). The BCM50a Integrated Router allows a private Local Area Network (LAN) to be securely connected to the Internet. The BCM50a Integrated Router can be used to prevent theft, destruction, and modification of data, as well as log events, which is important to the security of your network. The BCM50a Integrated Router also has packet filtering capabilities.

The BCM50a Integrated Router is installed between the LAN and a broadband modem connecting to the Internet, so that it can allow it to act as a secure gateway for all data passing between the Internet and the LAN.

The BCM50a Integrated Router has one Ethernet WAN port and one Ethernet LAN port, which are used to physically separate the network into two areas.

- The WAN (Wide Area Network) port attaches to the broadband modem (cable or ADSL) connecting to the Internet.
- The LAN (Local Area Network) port attaches to a network of computers, which needs security from the outside world. These computers have access to Internet services such as e-mail, FTP, and the World Wide Web. However, inbound access is not allowed unless the remote host is authorized to use a specific service.

1

Figure 44 BCM50a Integrated Router firewall application

Denial of Service

Denials of Service (DoS) attacks are aimed at devices and networks with a connection to the Internet. Their goal is not to steal information, but to disable a device or network so users no longer have access to network resources. The BCM50a Integrated Router is preconfigured to automatically detect and thwart currently known DoS attacks.

Basics

Computers share information over the Internet using a common language called TCP/IP. TCP/IP, in turn, is a set of application protocols that perform specific functions. An extension number, called the TCP port or UDP port, identifies these protocols, such as HTTP (Web), FTP (File Transfer Protocol), and POP3 (E-mail). For example, Web traffic uses TCP port 80, by default.

When computers communicate on the Internet, they use the client/server model, where the server listens on a specific TCP/UDP port for information requests from remote client computers on the network. For example, a Web server typically listens on port 80. Note that, while a computer can be intended for use over a single port, such as Web on port 80, other ports are also active and vulnerable to attack by hackers.

Some of the most common IP ports are:

Table 32 Common IP ports

21	FTP	53	DNS
23	Telnet	80	HTTP
25	SMTP	110	POP3

Types of DoS attacks

There are four types of DoS attacks:

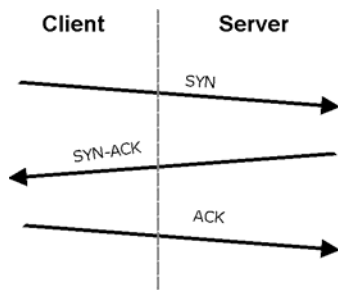
- Those that exploit bugs in a TCP/IP implementation.
 - Those that exploit weaknesses in the TCP/IP specification.
 - Brute force attacks that flood a network with useless data.
 - IP Spoofing.
- 1 Ping of Death and Teardrop attacks exploit bugs in the TCP/IP implementations of various computer and host systems.

Ping of Death uses a ping utility to create an IP packet that exceeds the maximum 65 536 bytes of data allowed by the IP specification. The oversize packet is then sent to an unsuspecting system, and can cause systems to crash, hang, or reboot.

Teardrop attack exploits weaknesses in the reassembly of IP packet fragments. As data is transmitted through a network, IP packets are often broken up into smaller chunks. Each fragment looks like the original IP packet except that it contains an offset field that says, for instance, “This fragment is carrying bytes 200 through 400 of the original (non fragmented) IP packet.” The Teardrop program creates a series of IP fragments with overlapping offset fields. After these fragments are reassembled at the destination, some systems crash, hang, or reboot.

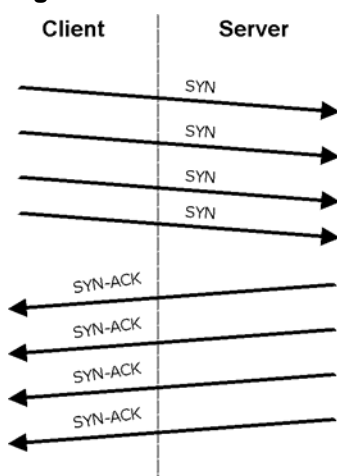
- Weaknesses in the TCP/IP specification leave it open to SYN Flood and LAND attacks. These attacks are executed during the handshake that initiates a communication session between two applications.

Figure 45 Three-way handshake



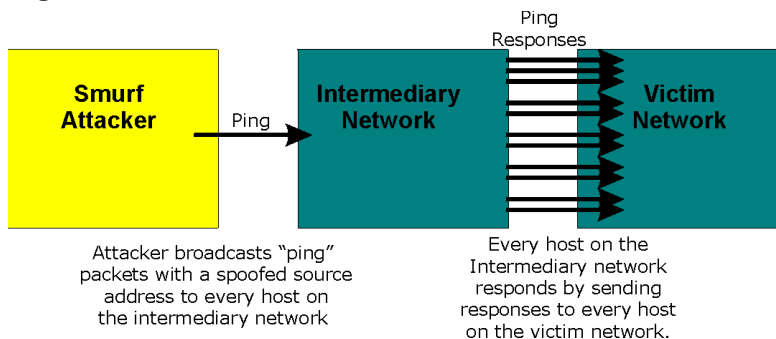
Under normal circumstances, the application that initiates a session sends a SYN (synchronize) packet to the receiving server. The receiver sends back an ACK (acknowledgment) packet and its own SYN, and then the initiator responds with an ACK (acknowledgment). After this handshake, a connection is established.

SYN Attack floods a targeted system with a series of SYN packets. Each packet causes the targeted system to issue a SYN-ACK response. While the targeted system waits for the ACK that follows the SYN-ACK, it queues up all outstanding SYN-ACK responses on what is known as a backlog queue. SYN-ACKs are moved off the queue only when an ACK comes back or when an internal timer (which is set at relatively long intervals) terminates the three-way handshake. Once the queue is full, the system ignores all incoming SYN requests, making the system unavailable for legitimate users.

Figure 46 SYN flood

In a LAND Attack, hackers flood SYN packets into the network with a spoofed source IP address of the targeted system. This makes it appear as if the host computer sent the packets to itself, making the system unavailable while the target system tries to respond to itself.

- 3** A brute force attack, such as a Smurf attack, targets a feature in the IP specification known as directed or subnet broadcasting, to quickly flood the target network with useless data. A Smurf hacker floods a router with Internet Control Message Protocol (ICMP) echo request packets (pings). Since the destination IP address of each packet is the broadcast address of the network, the router broadcasts the ICMP echo request packet to all hosts on the network. If there are numerous hosts, this creates a large amount of ICMP echo request and response traffic. If a hacker chooses to spoof the source IP address of the ICMP echo request packet, the resulting ICMP traffic not only clogs up the intermediary network, but also congests the network of the spoofed source IP address, known as the victim network. This flood of broadcast traffic consumes all available bandwidth, making communications impossible.

Figure 47 Smurf attack

- ICMP vulnerability

ICMP is an error reporting protocol that works in concert with IP. The following ICMP types trigger an alert:

Table 33 ICMP commands that trigger alerts

5	REDIRECT
13	TIMESTAMP_REQUEST
14	TIMESTAMP_REPLY
17	ADDRESS_MASK_REQUEST
18	ADDRESS_MASK_REPLY

- Illegal Commands (NetBIOS and SMTP)

The only legal NetBIOS commands are shown in [Table 34](#)— all others are illegal.

Table 34 Legal NetBIOS commands

MESSAGE:
REQUEST:
POSITIVE:
NEGATIVE:
RETARGET:
KEEPALIVE:

All SMTP commands are illegal except for those displayed in [Table 35](#).

Table 35 Legal SMTP commands

AUTH	DATA	EHLO	ETRN	EXPN	HELO	HELP	MAIL	NOOP
QUIT	RCPT	RSET	SAML	SEND	SOML	TURN	VERFY	

- Traceroute

Traceroute is a utility used to determine the path a packet takes between two endpoints. Sometimes, when a packet filter firewall is configured incorrectly, an attacker can traceroute the firewall and gain knowledge of the network topology inside the firewall.

- 4 Often, many DoS attacks also employ a technique known as IP Spoofing as part of their attack. IP Spoofing can be used to break into systems, to hide the hacker's identity, or to magnify the effect of the DoS attack. IP Spoofing is a technique used to gain unauthorized access to computers by tricking a router or firewall into thinking that the communications are coming from within the trusted network. To engage in IP spoofing, a hacker must modify the packet headers so that it appears that the packets originate from a trusted host and is allowed through the router or firewall. The BCM50a Integrated Router blocks all IP Spoofing attempts.

Stateful inspection

With stateful inspection, fields of the packets are compared to packets that are already known to be trusted. For example, if you access an outside service, the proxy server remembers things about your original request, like the port number and source and destination addresses. This remembering is called saving the state. When the outside system responds to your request, the firewall compares the received packets with the saved state to determine if they are allowed in. The BCM50a Integrated Router uses stateful packet inspection to protect the private LAN from hackers and vandals on the Internet. By default, the BCM50a Integrated Router stateful inspection allows all communications to the Internet that originate from the LAN, and blocks all traffic to the LAN that originates from the Internet.

In summary, stateful inspection:

- Allows all sessions originating from the LAN (local network) to the WAN (Internet).
- Denies all sessions originating from the WAN to the LAN.

Figure 48 Stateful inspection

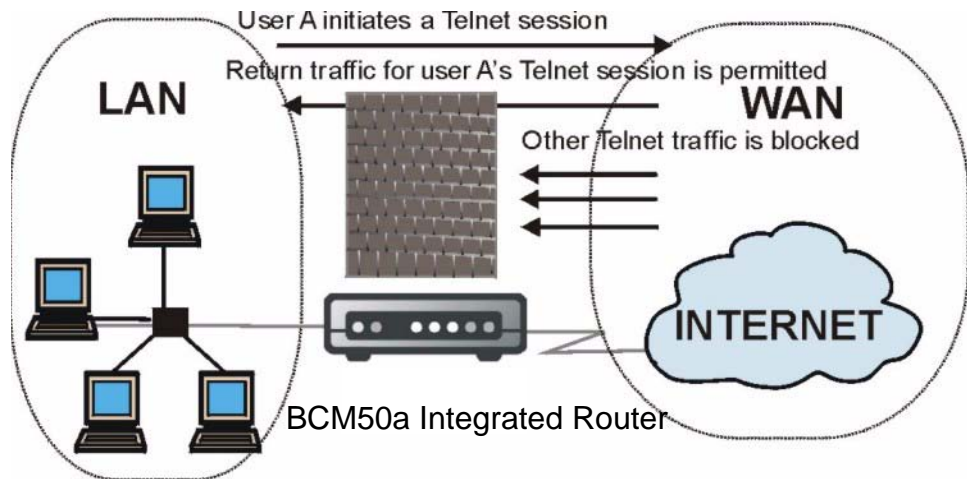


Figure 48 shows the BCM50a Integrated Router default firewall rules in action, and demonstrates how stateful inspection works. User A can initiate a Telnet session from within the LAN and responses to this request are allowed. However, other Telnet traffic initiated from the WAN is blocked.

Stateful inspection process

In the following example, the following sequence of events occurs when a TCP packet leaves the LAN network through the firewall's WAN interface. The TCP packet is the first in a session, and the packet's application layer protocol is configured for a firewall rule inspection:

- 1 The packet travels from the firewall's LAN to the WAN.
- 2 The packet is evaluated against the interface's existing outbound access list, and the packet is permitted (a denied packet is dropped at this point).

- 3 The packet is inspected by a firewall rule to determine and record information about the state of the packet's connection. This information is recorded in a new state table entry created for the new connection. If there is not a firewall rule for this packet and it is not an attack, the **Action for packets that don't match firewall rules** field determines the action for this packet.
- 4 Based on the obtained state information, a firewall rule creates a temporary access list entry that is inserted at the beginning of the WAN interface's inbound extended access list. This temporary access list entry is designed to permit inbound packets of the same connection as the outbound packet just inspected.
- 5 The outbound packet is forwarded out through the interface.
- 6 Later, an inbound packet reaches the interface. This packet is part of the connection previously established with the outbound packet. The inbound packet is evaluated against the inbound access list, and is permitted because of the temporary access list entry previously created.
- 7 The packet is inspected by a firewall rule, and the connection's state table entry is updated as necessary. You can modify the inbound extended access list temporary entries based on the updated state information, in order to permit only packets that are valid for the current state of the connection.
- 8 Any additional inbound or outbound packets that belong to the connection are inspected to update the state table entry and to modify the temporary inbound access list entries as required, and are forwarded through the interface.
- 9 When the connection terminates or times out, the connection's state table entry is deleted and the connection's temporary inbound access list entries are deleted.

Stateful inspection and the BCM50a Integrated Router

Additional rules can be defined to extend or override the default rules. For example, a rule can be created that will:

- Block all traffic of a certain type, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic from the Internet to specific hosts on the LAN.
- Allow access to a Web server to everyone but competitors.

- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by evaluating the network traffic source IP address, destination IP address, IP protocol type, and comparing these to rules set by the administrator.



Note: The ability to define firewall rules is a very powerful tool. Using custom rules, it is possible to disable all firewall protection or block all access to the Internet. Use extreme caution when creating or deleting firewall rules. Test changes after creating them to make sure they work correctly.

Below is a brief technical description of how these connections are tracked. Connections can either be defined by the upper protocols (for instance, TCP), or by the BCM50a Integrated Router itself (as with the virtual connections created for UDP and ICMP).

TCP security

The BCM50a Integrated Router uses state information embedded in TCP packets. The first packet of any new connection has its SYN flag set and its ACK flag cleared; these are initiation packets. All packets that do not have this flag structure are called subsequent packets, since they represent data that occurs later in the TCP stream.

If an initiation packet originates on the WAN, someone is trying to make a connection from the Internet into the LAN. Except in a few special cases, (see [“Upper layer protocols” on page 157](#)), these packets are dropped and logged.

If an initiation packet originates on the LAN, someone is trying to make a connection from the LAN to the Internet. Assuming that this is an acceptable part of the security policy (as is the case with the default policy), the connection is allowed. A cache entry is added, which includes connection information such as IP addresses, TCP ports, and sequence numbers.

After the BCM50a Integrated Router receives any subsequent packet (from the Internet or from the LAN), its connection information is extracted and checked against the cache. A packet is only allowed to pass through if it corresponds to a valid connection (that is, if it is a response to a connection that originated on the LAN).

UDP/ICMP security

UDP and ICMP do not contain any connection information (such as sequence numbers). However, at the very minimum, they contain an IP address pair (source and destination). UDP also contains port pairs, and ICMP has type and code information. All of this data can be analyzed in order to build virtual connections in the cache.

For instance, any UDP packet that originates on the LAN creates a cache entry. Its IP address and port pairs are stored. For a short period of time, UDP packets from the WAN that have matching IP and UDP information are allowed back in through the firewall.

A similar situation exists for ICMP, except that the BCM50a Integrated Router is even more restrictive. Specifically, only outgoing echoes allow incoming echo replies, outgoing address mask requests allow incoming address mask replies, and outgoing timestamp requests allow incoming timestamp replies. No other ICMP packets are allowed in through the firewall, simply because they are too dangerous and contain too little tracking information. For instance, ICMP redirect packets are never allowed in, since they can be used to reroute traffic through attacking machines.

Upper layer protocols

Some higher layer protocols (such as FTP and RealAudio) utilize multiple network connections simultaneously. In general terms, they usually have a control connection, which is used for sending commands between endpoints, and then data connections, which are used for transmitting bulk information.

Consider the FTP protocol. A user on the LAN opens a control connection to a server on the Internet and requests a file. At this point, the remote server opens a data connection from the Internet. For FTP to work properly, this connection must be allowed to pass through even though a connection from the Internet is normally rejected.

In order to achieve the above scenario, the BCM50a Integrated Router inspects the application level FTP data. Specifically, it searches for outgoing PORT commands, and when it sees these; it adds a cache entry for the anticipated data connection. This can be done safely, since the PORT command contains address and port information, which can be used to uniquely identify the connection.

Any protocol that operates in this way must be supported on a case-by-case basis. You can use the Custom Ports feature in the WebGUI to do this.

Guidelines for enhancing security with your firewall

- 1 Change the default password through SMT or WebGUI.
- 2 Think about access control before you connect your device to the network in any way.
- 3 Limit who can Telnet into your router.
- 4 Do not enable any local service (such as SNMP or NTP) that you do not use. Any enabled service can present a potential security risk. A determined hacker can find creative ways to misuse the enabled services to access the firewall or the network.
- 5 For local services that are enabled, protect against misuse. Protect by configuring the services to communicate only with specific peers, and protect by configuring rules to block packets for the services at specific interfaces.
- 6 Protect against IP spoofing by making sure the firewall is active.
- 7 Keep the firewall in a secured (locked) room.

Packet filtering vs. firewall

Below are some comparisons between the filtering and firewall functions of the BCM50a Integrated Router.

Packet filtering:

- The router filters packets as they pass through the router interface according to the filter rules you designed.
- Packet filtering is a powerful tool, yet can be complex to configure and maintain, especially if you need a chain of rules to filter a service.
- Packet filtering only checks the header portion of an IP packet.

When to use filtering

- 1 To block or allow LAN packets by their MAC addresses.
- 2 To block or allow special IP packets that are neither TCP nor UDP, nor ICMP packets.
- 3 To block or allow both inbound (WAN to LAN) and outbound (LAN to WAN) traffic between the specific inside host or network A and outside host or network B. If the filter blocks the traffic from A to B, it also blocks the traffic from B to A. Filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4 To block or allow IP trace route.

Firewall

- The firewall inspects packet contents as well as their source and destination addresses. Firewalls of this type employ an inspection module, applicable to all protocols, that understands data in the packet is intended for other layers, from the network layer (IP headers) up to the application layer.
- The firewall performs stateful inspection. It takes into account the state of the connections it handles, so that, for example, a legitimate incoming packet can be matched with the outbound request for that packet and allowed in. Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked.
- The firewall uses session filtering, or smart rules, that enhance the filtering process and control the network session rather than control individual packets in a session.
- The firewall provides e-mail service to notify you of routine reports and when alerts occur.

When to use the firewall

- 1** To prevent DoS attacks and prevent hackers cracking your network.
- 2** A range of source and destination IP addresses as well as port numbers can be specified within one firewall rule, making the firewall a better choice when complex rules are required.
- 3** To selectively block or allow inbound or outbound traffic between inside host or networks and outside host or networks. Remember that filters cannot distinguish traffic originating from an inside host or an outside host by IP address.
- 4** The firewall performs better than filtering if you need to check many rules.
- 5** Use the firewall if you need routine e-mail reports about your system or need to be alerted when attacks occur.
- 6** The firewall can block any specific URL traffic that occurs in the future. The URL can be saved in an Access Control List (ACL) database.

Chapter 11

Firewall screens

This chapter shows you how to configure your BCM50a Integrated Router firewall.

Access methods

The WebGUI is, by far, the most comprehensive firewall configuration tool your BCM50a Integrated Router has to offer. For this reason, Nortel recommends that you configure your firewall using the WebGUI. With SMT screens, you can activate the firewall. CLI commands provide limited configuration options and are only recommended for advanced users, refer to for firewall CLI commands.

Firewall policies overview

Firewall rules are grouped based on the direction of travel of packets to which they apply:

LAN to LAN/BCM50a Integrated Router	WAN to LAN
LAN to WAN	WAN to WAN/BCM50a Integrated Router

By default, BCM50a Integrated Router stateful packet inspection allows packets traveling in the following directions:

- LAN to LAN/BCM50a Integrated Router
This allows computers on the LAN to manage the BCM50a Integrated Router and communicate between networks or subnets connected to the LAN interface.
- LAN to WAN

By default, the BCM50a Integrated Router stateful packet inspection blocks packets traveling in the following directions:

- WAN to LAN
- WAN to WAN/BCM50a Integrated Router
This prevents computers on the WAN from using the BCM50a Integrated Router as a gateway to communicate with other computers on the WAN, or to manage the BCM50a Integrated Router, or both.

You can define additional rules and sets or modify existing ones, but exercise extreme caution in doing so.



Note: If you configure firewall rules without a good understanding of how they work, you can inadvertently introduce security risks to the firewall and to the protected network. Make sure you test your rules after you configure them.

For example, you can create rules to:

- Block certain types of traffic, such as IRC (Internet Relay Chat), from the LAN to the Internet.
- Allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN.
- Allow everyone except your competitors to access a Web server.
- Restrict use of certain protocols, such as Telnet, to authorized users on the LAN.

These custom rules work by comparing the Source IP address, Destination IP address and IP protocol type of network traffic to rules set by the administrator. Your customized rules take precedence and override the BCM50a Integrated Router default rules.

Rule logic overview



Note: Study these points carefully before configuring rules.

Rule checklist

- 1 State the intent of the rule. For example, “This restricts all IRC access from the LAN to the Internet.” Or, “This allows a remote Lotus Notes server to synchronize over the Internet to an inside Notes server.”
- 2 Is the intent of the rule to forward or block traffic?
- 3 What direction of traffic does the rule apply to?
- 4 What IP services are affected?
- 5 What computers on the LAN are affected (if any)?
- 6 What computers on the Internet are affected? The more specific, the better. For example, if traffic is allowed from the Internet to the LAN, it is better to allow only certain machines on the Internet to access the LAN.

Security ramifications

Once the logic of the rule has been defined, it is critical to consider the security ramifications created by the rule:

- 1 Does this rule stop LAN users from accessing critical resources on the Internet? For example, if IRC is blocked, are there users that require this service?
- 2 Is it possible to modify the rule to be more specific? For example, if IRC is blocked for all users, a rule that blocks just certain users can be more effective.
- 3 Does a rule that allows Internet users access to resources on the LAN create a security vulnerability? For example, if FTP ports (TCP 20, 21) are allowed from the Internet to the LAN, Internet users can connect to computers with running FTP servers.
- 4 Does this rule conflict with any existing rules?

Once these questions have been answered, adding rules is simply a matter of plugging the information into the correct fields in the WebGUI screens.

Key fields for configuring rules

Action

Set the action to either **Block** or **Forward**.



Note: Block means the firewall silently discards the packet.

Service

Select the service from the **Service** scrolling list box. If the service is not listed, it is necessary to first define it. For more information on predefined services, see [“Predefined services” on page 178](#).

Source address

What is the source address of the connection; is it on the LAN or WAN? Is it a single IP, a range of IPs, or a subnet?

Destination address

What is the destination address of the connection; is it on the LAN or WAN? Is it a single IP, a range of IPs or a subnet?

Connection direction examples

This section describes examples for firewall rules for connections going from LAN to WAN and from WAN to LAN.

LAN to LAN/BCM50a Integrated Router rules apply to packets coming in through the LAN interface that are destined for either the BCM50a Integrated Router LAN interface itself or a different subnet on the LAN. A management

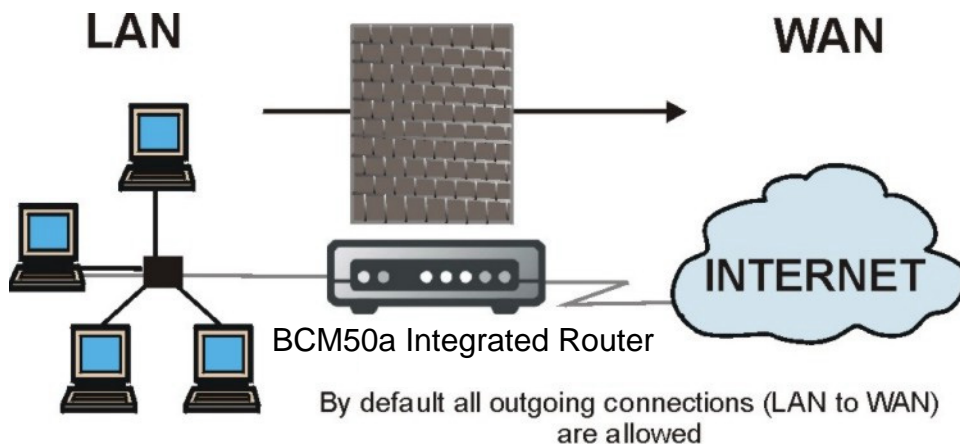
session through the LAN interface is an example of traffic destined for the BCM50a Integrated Router LAN interface itself. You can also use LAN to LAN/BCM50a Integrated Router rules with IP alias to control routing between two subnets on the LAN.

WAN to WAN/BCM50a Integrated Router rules apply to packets coming in through the WAN interface that are destined for either the BCM50a Integrated Router WAN interface itself or a different subnet on the WAN. A management session through the WAN interface is an example of traffic destined for the BCM50a Integrated Router WAN interface itself. By default, the BCM50a Integrated Router stops WAN computers from using the BCM50a Integrated Router as a gateway to communicate with other computers on the WAN. You can configure one of these rules to allow a WAN computer to manage the BCM50a Integrated Router.

LAN to WAN rules

The default rule for LAN to WAN traffic is that all users on the LAN are allowed unrestricted access to the WAN. When you configure a LAN to WAN rule, you in essence want to limit some or all users from accessing certain services on the WAN.

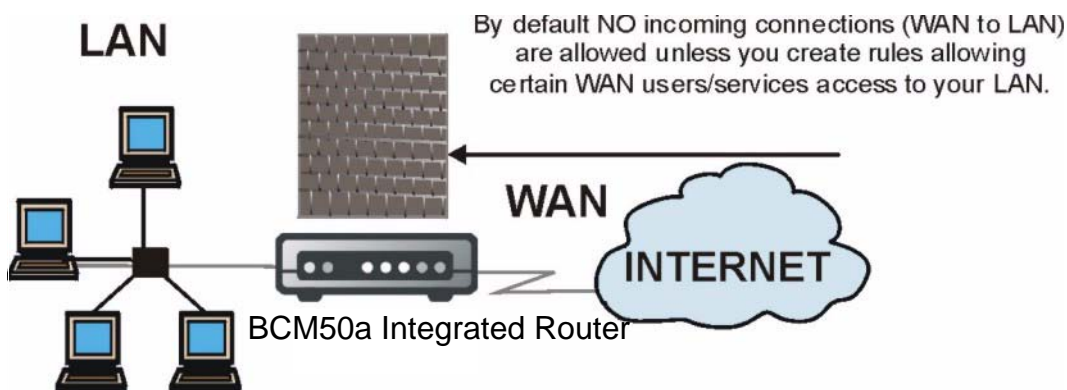
Figure 49 LAN to WAN traffic



WAN to LAN rules

The default rule for WAN to LAN traffic blocks all incoming connections (WAN to LAN). If you want to allow certain WAN users to have access to your LAN, you need to create custom rules to allow it.

Figure 50 WAN to LAN traffic



Configuring firewall

Click **FIREWALL** to open the **Summary** screen. Enable (or activate) the firewall by selecting the **Enable Firewall** check box as seen in [Figure 51](#).

The BCM50a Integrated Router applies the firewall rules in order, starting from the first rule for the direction of travel of a packet. When the traffic matches a rule, the BCM50a Integrated Router takes the action in the rule and stops checking the firewall rules.

For example, you have one general rule that blocks all LAN to WAN IRC (Internet Relay Chat). And you have another rule that allows IRC traffic from your company president's LAN IP address to go to the WAN. In order for the president's IRC traffic to get through, the rule for the president's IP address must come before the rule that blocks all LAN to WAN IRC traffic. If the rule that blocks all LAN to WAN IRC traffic comes first, all LAN to WAN IRC traffic matches that rule and the BCM50a Integrated Router drops the president's connection and does not check any other firewall rules.

If you list a general rule before a specific rule, traffic that you want to be controlled by the specific rule can get the general rule applied to it instead. Any traffic that does not match the first firewall rule matches the default rule and the BCM50a Integrated Router forwards the traffic.



Note: If an alternate gateway on the LAN has an IP address in the same subnet as the BCM50a Integrated Router LAN IP address, return traffic does not go through the BCM50a Integrated Router. This is called an asymmetrical or triangle route, and causes the BCM50a Integrated Router to reset the connection, as the connection has not been acknowledged.

Note: Allowing asymmetrical routes can let traffic from the WAN go directly to the LAN without passing through the BCM50a Integrated Router. A better solution is to use IP alias to put the BCM50a Integrated Router and the backup gateway on separate subnets. See the Appendix B “Triangle Route” of for more about triangle route topology.

Figure 51 Enabling the firewall

FIREWALL

Table 36 describes the fields in Figure 51.

Table 36 Firewall rules summary: First screen

Label	Description
Enable Firewall	Select this check box to activate the firewall. The BCM50a Integrated Router performs access control and protects against Denial of Service (DoS) attacks when the firewall is activated. The firewall allows traffic to go through your VPN tunnels.

Table 36 Firewall rules summary: First screen

Label	Description
Bypass Triangle Route	Select this check box to have the BCM50a Integrated Router permit the use of asymmetrical route topology on the network (not reset the connection).
Firewall Rules Storage Space in Use	This read-only bar shows how much of the BCM50a Integrated Router's memory for recording firewall rules is currently being used. The bar turns from green to red when the maximum is approached. You can typically configure up to ten rules per traffic direction.
Packet Direction	Use the drop-down list to select a direction of travel of packets for which you want to display firewall rules.
Block/Forward	Use the option buttons to select whether to Block (silently discard) or Forward (allow the passage of) packets that are traveling in the selected direction.
Log packets that don't match these rules.	Select the check box to create a log (when the above action is taken) for packets that are traveling in the selected direction and do not match any of the rules below.
	The following read-only fields summarize the rules you have created that apply to traffic traveling in the selected packet direction. The firewall rules that you configure (summarized below) take priority over the general firewall action settings above.
#	This is your firewall rule number. The ordering of your rules is important as rules are applied in turn. The Move field allows you to reorder your rules.
Status	This field displays whether a firewall is turned on (Active) or not (Inactive). Rules that have not been configured display Empty .
Source Address	This drop-down list displays the source addresses or ranges of addresses to which this firewall rule applies. Note that a blank source or destination address is equivalent to Any .
Destination Address	This drop-down list displays the destination addresses or ranges of addresses to which this firewall rule applies. Note that a blank source or destination address is equivalent to Any .
Service Type	This drop-down list displays the services to which this firewall rule applies. Note that a blank service type is equivalent to Any . For more information, see Table 40 on page 179 .
Action	This is the specified action for the selected rule, either Block or Forward . Note that Block means the firewall silently discards the packet.
Log	This field shows you if a log is created for packets that match the rule (Match), don't match the rule (Not Match), both (Both), or no log is created (None).
Alert	This field tells you whether this rule generates an alert (Yes) or not (No) when the rule is matched.

Table 36 Firewall rules summary: First screen

Label	Description
Insert	Type the index number for where you want to put a rule. For example, if you type "6", your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7. Click Insert to display the screen where you configure a firewall rule.
Move	Select the Index option button of a rule and type a number for where you want to put that rule. Click Move to move the rule to the number that you typed. The ordering of your rules is important as they are applied in order of their numbering.
Rule to (Rule Number)	Click a rule's option button and type the number for where you want to put that rule.
Edit	Click Edit to create or edit a rule.
Delete	Click Delete to delete an existing firewall rule. Note that subsequent firewall rules move up by one when you take this action.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Configuring firewall rules

Follow these directions to create a new rule.

In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type 1, your new rule becomes number 1 and the previous rule 1 (if there is one) becomes rule 2.

Click **Insert** to display the screen shown in [Figure 52](#).

Figure 52 Creating and editing a firewall rule
FIREWALL - EDIT RULE

Table 37 describes the fields in Figure 52.

Table 37 Creating and editing a firewall rule

Label	Description
Active	Check the Active check box to have the BCM50a Integrated Router use this rule. Leave it unchecked if you do not want the BCM50a Integrated Router to use the rule after you apply it.
Packet Direction	Use the drop-down list to select the direction of packet travel to which you want to apply this firewall rule.

Table 37 Creating and editing a firewall rule

Label	Description
Source Address	Click SrcAdd to add a new address, SrcEdit to edit an existing one or SrcDelete to delete one. The source address can be a particular (single) IP, a range of IP addresses (for example, 192.168.1.10 to 192.169.1.50), a subnet or any IP address. See the next section for more information about adding and editing source addresses.
Destination Address	Click DestAdd to add a new address, DestEdit to edit an existing one or DestDelete to delete one. The destination address can be a particular (single) IP, a range of IP addresses (for example, 192.168.1.10 to 192.169.1.50), a subnet or any IP address. See section “Configuring source and destination addresses” on page 173 for information about adding and editing destination addresses.
Services Available/ Selected Services	For more information on services available, see Table 40 on page 179 . Highlight a service from the Available Services box on the left, then click >> to add it to the Selected Services box on the right. To remove a service, highlight it in the Selected Services box on the right, then click << .
Custom Port	
Add	Click this button to bring up the screen that you use to configure a new custom service that is not in the predefined list of services.
Edit	Select a custom service (denoted by an “*”) from the Available Services list and click this button to edit the service.
Delete	Select a custom service (denoted by an “*”) from the Available Services list and click this button to remove the service.
Action for Matched Packets	Use the drop-down list to select whether to discard (Block) or allow the passage of (Forward) packets that match this rule.
Log	This field determines if a log is created for packets that match the rule (Match), don't match the rule (Not Match), both (Both) or no log is created (None). Go to the Log Settings page and select the Access Control logs category to have the BCM50a Integrated Router record these logs.
Alert	Check the Alert check box to determine that this rule generates an alert when the rule is matched.
Apply	Click Apply to save your changes to the BCM50a Integrated Router and exit this screen.
Cancel	Click Cancel to exit this screen without saving,

Configuring source and destination addresses

To add a new source or destination address, click **SrcAdd** or **DestAdd** from the previous screen. To edit an existing source or destination address, select it from the box and click **SrcEdit** or **DestEdit** from the previous screen. Either action displays the screen shown in [Figure 53](#).

Figure 53 Adding or editing source and destination addresses

FIREWALL - EDIT RULE - EDIT IP

The screenshot shows a configuration window titled "FIREWALL - EDIT RULE - EDIT IP". It contains the following fields and controls:

- Address Type:** A dropdown menu with "Any Address" selected.
- Start IP Address:** A text input field containing "0.0.0.0".
- End IP Address:** A text input field containing "0.0.0.0".
- Subnet Mask:** A text input field containing "0.0.0.0".
- Buttons:** "Apply" and "Cancel" buttons are located at the bottom of the window.

[Table 38](#) describes the fields in [Figure 53](#).

Table 38 Adding or editing source and destination addresses

Label	Description
Address Type	Select an option from the drop-down list that includes: Single Address , Range Address , Subnet Address and Any Address .
Start IP Address	Enter the single IP address or the starting IP address in a range here. Use a numerical IP address in dotted decimal notation (for example, 192.168.1.10).
End IP Address	Enter the ending IP address in a range here. Use a numerical IP address in dotted decimal notation (for example, 192.168.1.10).
Subnet Mask	Enter the subnet mask here, if applicable.
Apply	Click Apply to save your changes to the BCM50a Integrated Router and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

Configuring custom ports

You can also configure customized ports for services not predefined by the *BCM50a Integrated Router* (see “[Predefined services](#)” on page 178 for a list of predefined services). For a comprehensive list of port numbers and services, visit the IANA (Internet Assigned Number Authority) Web site.

Click the **Add** button under **Custom Port** while editing a firewall to configure a custom port. This displays the screen illustrated in [Figure 54](#).

Figure 54 Creating or editing a custom port
FIREWALL - EDIT RULE - EDIT CUSTOM PORT

[Table 39](#) describes the fields in [Figure 54](#).

Table 39 Creating/Editing A Custom Port

Label	Description
Service Name	Enter a unique name to identify the service (a service that is not predefined in the BCM50a Integrated Router).
Service Type	Choose the IP port (TCP , UDP or Both) that defines your customized port from the drop-down list.
Port Configuration Type	Click Single to specify one port only or Range to specify a span of ports that define your customized service.
Port Number	Enter a single port number or the range of port numbers that define your customized service.
Apply	Click Apply to save your changes to the BCM50a Integrated Router and exit this screen.
Cancel	Click Cancel to exit this screen without saving.

Example firewall rule

The following Internet firewall rule example allows a hypothetical My Service connection from the Internet.

- 1 Click the **Firewall** link and then the **Summary** tab.
- 2 In the **Summary** screen, type the index number for where you want to put the rule. For example, if you type “6”, your new rule becomes number 6 and the previous rule 6 (if there is one) becomes rule 7.
- 3 Click **Insert** to display the firewall rule configuration screen.

Figure 55 Firewall edit rule screen example

FIREWALL - EDIT RULE

The screenshot shows the 'FIREWALL - EDIT RULE' configuration window. At the top left, there is a checked checkbox for 'Active'. To its right is a dropdown menu for 'Packet Direction' set to 'WAN to LAN'. Below these are two text input fields: 'Source Address' containing '##### Source IP Address ##### Any' and 'Destination Address' containing '#### Destination IP Address ##### Any'. Each field has three buttons below it: 'SrcAdd', 'SrcEdit', 'SrcDelete' for the source and 'DestAdd', 'DestEdit', 'DestDelete' for the destination. In the center, there are two list boxes: 'Available Services' with a scrollable list of services (AIM/NEW_ICQ(TCP:5190), AUTH(TCP:113), BGP(TCP:179), BOOTP_CLIENT(UDP:68), BOOTP_SERVER(UDP:67)) and 'Selected Services' with a list of 'Any(UDP)' and 'Any(TCP)'. Between these lists are '<<' and '>>' buttons. Below the 'Available Services' list is a 'Custom Port' section with 'Add', 'Edit', and 'Delete' buttons. At the bottom, there is an 'Action for Matched Packets' dropdown set to 'Forward', and two unchecked checkboxes for 'Log' and 'Alert'. Finally, 'Apply' and 'Cancel' buttons are at the very bottom.

- 4 Select **WAN to LAN** as the **Packet Direction**.
- 5 Select **Any** in the **Destination Address** box and then click **DestEdit**.

- 6 Configure the **Firewall Rule Edit IP** screen as follows and click **Apply**.

Figure 56 Firewall rule edit IP example

FIREWALL - EDIT RULE - EDIT IP

The screenshot shows a configuration window titled "FIREWALL - EDIT RULE - EDIT IP". It contains the following fields:

- Address Type:** A dropdown menu set to "Range Address".
- Start IP Address:** A text input field containing "10.0.0.10".
- End IP Address:** A text input field containing "10.0.0.15".
- Subnet Mask:** A text input field containing "0.0.0.0".

At the bottom of the window, there are two buttons: "Apply" and "Cancel".

- 7 In the firewall rule configuration screen, click **Add** under **Custom Port** to open the **Edit Custom Port** screen. Configure it as shown in [Figure 57](#) and click **Apply**.

Figure 57 Edit custom port example

FIREWALL - EDIT RULE - EDIT CUSTOM PORT

The screenshot shows a configuration window titled "FIREWALL - EDIT RULE - EDIT CUSTOM PORT". It contains the following fields:

- Service Name:** A text input field containing "My Service".
- Service Type:** A dropdown menu set to "TCP/UDP".
- Port Configuration Type:** Two radio buttons, "Single" (selected) and "Range".
- Port Number:** Two text input fields, the first containing "123" and the second containing "0", separated by a hyphen.

At the bottom of the window, there are two buttons: "Apply" and "Cancel".

- 8 The firewall rule configuration screen displays. Use the arrows between **Available Services** and **Selected Services** to configure it as shown in [Figure 58](#). Click **Apply** after you are done.



Note: Custom ports show up with an * before their names in the Services list box and the Rule Summary list box. Click **Apply** after you have created your custom port.

Figure 58 MyService rule configuration example
FIREWALL - EDIT RULE

Active

Packet Direction: WAN to LAN

Source Address
Source IP Address #####
Any

Destination Address
Destination IP Address ###
10.0.0.10 - 10.0.0.15

SrcAdd SrcEdit SrcDelete DestAdd DestEdit DestDelete

Available Services
Any(TCP)
Any(UDP)
AIM/NEW_ICQ(TCP:5190)
AUTH(TCP:113)
BGP(TCP:179)

Selected Services
*My Service(TCP/UDP:123)

Custom Port :
Add Edit Delete

Action for Matched Packets: Forward Log Alert

Apply Cancel

After completing the configuration procedure for this Internet firewall rule, the **Rule Summary** screen will look like the one illustrated in [Figure 59](#). Rule 1: Allows a My Service connection from the WAN to IP addresses 10.0.0.10 through 10.0.0.15 on the LAN. Remember to click **Apply** after you finish configuring your rules to save your settings to the BCM50a Integrated Router.

Figure 59 My Service example rule summary
FIREWALL

Summary
Attack Alert

The firewall protects against Denial of Service (DoS) attacks when it is enabled.

Enable Firewall
 Bypass Triangle Route

Firewall Rules Storage Space in Use

0% 100%

Packet Direction: WAN to LAN

Configured rules for this packet direction are displayed in the summary table below.

Action for packets that don't match firewall rules. Block Forward

Log packets that don't match these rules.

#	Status	Source Address	Destination Address	Service Type	Action	Log	Alert
1	Active	Any	10.0.0.10 - 10.0.0.15	*My Service(TCP/UDP:123)	Forward	Disabled	No

Insert

New Rule Before (Rule Number).

Move

Selected Rule (select an Index Number) To (Rule Number).

Edit

Selected Rule

Delete

Selected Rule

Apply

Reset

Predefined services

The **Available Services** list box in the **Edit Rule** screen (see [Figure 52](#)) displays all predefined services that the BCM50a Integrated Router already supports. Next to the name of the service, two fields appear in brackets. The first field indicates the IP protocol type (TCP, UDP, or ICMP). The second field indicates the IP port number that defines the service. (Note that there can be more than one IP protocol

type. For example, look at the default configuration labeled “**(DNS)**”. (**UDP/TCP:53**) means UDP port 53 and TCP port 53. Custom services can also be configured using the **Custom Ports** function, which is discussed in “[Configuring custom ports](#)” on page 174.

Table 40 Predefined services

Service	Description
AIM/New-ICQ(TCP:5190)	AOL Internet Messenger service, used as a listening port by ICQ.
AUTH(TCP:113)	Authentication protocol used by some servers.
BGP(TCP:179)	Border Gateway Protocol.
BOOTP_CLIENT(UDP:68)	DHCP Client.
BOOTP_SERVER(UDP:67)	DHCP Server.
CU-SEEME(TCP/UDP:7648, 24032)	A popular videoconferencing solution from White Pines Software.
DNS(UDP/TCP:53)	Domain Name Server, a service that matches Web names (for example, www.nortel.com) to IP numbers.
FINGER(TCP:79)	Finger is a UNIX or Internet-related command that can be used to find out if a user is logged on.
FTP(TCP:20.21)	File Transfer Program is a program to enable fast transfer of files, including large files that cannot be sent by e-mail.
H.323(TCP:1720)	NetMeeting uses this protocol.
HTTP(TCP:80)	Hyper Text Transfer Protocol is a client/server protocol for the World Wide Web.
HTTPS(TCP:443)	HTTPS is a secured http session often used in e-commerce.
ICQ(UDP:4000)	This is a popular Internet chat program.
IKE(UDP:500)	The Internet Key Exchange algorithm is used for key distribution and management.
IPSEC_TUNNEL(AH:0)	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
IPSEC_TUNNEL(ESP:0)	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
IRC(TCP/UDP:6667)	This is another popular Internet chat program.
MSN Messenger(TCP:1863)	Microsoft Networks' messenger service uses this protocol.
MULTICAST(IGMP:0)	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.

Table 40 Predefined services

Service	Description
NEW-ICQ(TCP:5190)	An Internet chat program.
NEWS(TCP:144)	A protocol for news groups.
NFS(UDP:2049)	Network File System (NFS) is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP(TCP:119)	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING(ICMP:0)	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3(TCP:110)	Post Office Protocol version 3 lets a client computer receive e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP(TCP:1723)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL(GRE:0)	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the data channel.
RCMD(TCP:512)	Remote Command Service.
REAL_AUDIO(TCP:7070)	A streaming audio service that enables real time sound over the web.
REXEC(TCP:514)	Remote Execution Daemon.
RLOGIN(TCP:513)	Remote Logon.
RTELNET(TCP:107)	Remote Telnet.
RTSP(TCP/UDP:554)	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP(TCP:115)	Simple File Transfer Protocol.
SMTP(TCP:25)	Simple Mail Transfer Protocol is the message exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP(TCP/UDP:161)	Simple Network Management Program.
SNMP-TRAPS(TCP/UDP:162)	Traps for use with the SNMP (RFC:1215).
SQL-NET(TCP:1521)	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.

Table 40 Predefined services

Service	Description
SIP-V2(UDP:5060)	The Session Initiation Protocol (SIP) is an application layer control (signaling) protocol that handles the setting up, altering and tearing down of voice and multimedia sessions over the Internet. SIP is used in VoIP (Voice over IP), the sending of voice signals over the Internet Protocol.
SSH(TCP/UDP:22)	Secure Shell Remote Logon Program.
STRM WORKS(UDP:1558)	Stream Works Protocol.
SYSLOG(UDP:514)	Using syslog, you can send system logs to a UNIX server.
TACACS(UDP:49)	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET(TCP:23)	Telnet is the logon and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP(UDP:69)	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE(TCP:7000)	Another videoconferencing solution.

Alerts

Alerts are reports on events, such as attacks, that you want to know about right away. You can choose to generate an alert when an attack is detected in the **Attack Alert** screen (Figure 60, check the **Generate alert when attack detected** check box) or when a rule is matched in the **Rule Edit** screen (see Figure 52). Configure the **Log Settings** screen to have the BCM50a Integrated Router send an immediate e-mail message to you when an event generates an alert.

Configuring attack alert

Attack alerts are the first defense against DOS attacks. In the **Attack Alert** screen (Figure 60) you can choose to generate an alert whenever an attack is detected. For DoS attacks, the BCM50a Integrated Router uses thresholds to determine when to drop sessions that do not become fully established. These thresholds apply globally to all sessions.

You can use the default threshold values, or you can change them to values more suitable to your security requirements.

Threshold values

Tune these parameters when something is not working and after you have checked the firewall counters. These default values work fine for normal, small offices with ADSL bandwidth. Factors influencing choices for threshold values are:

- The maximum number of opened sessions
- The minimum capacity of server backlog in your LAN network
- The CPU power of servers in your LAN network
- Network bandwidth
- Type of traffic for certain servers

If your network is slower than average for any of these factors (especially if you have servers that are slow or handle many tasks and are often busy), then the default values must be reduced.

You must make any changes to the threshold values before you continue configuring firewall rules.

Half-open sessions

An unusually high number of half-open sessions (either an absolute number or measured as the arrival rate) indicates that a Denial of Service attack is occurring. For TCP, half-open means that the session has not reached the established state, and the TCP three-way handshake has not yet been completed (see Figure 45). For UDP, half-open means that the firewall has detected no return traffic.

The BCM50a Integrated Router measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

After the number of existing half-open sessions rises above a threshold (**max-incomplete high**), the BCM50a Integrated Router starts deleting half-open sessions as required to accommodate new connection requests. The BCM50a Integrated Router continues to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (**max-incomplete low**).

After the rate of new connection attempts rises above a threshold (**one-minute high**), the BCM50a Integrated Router starts deleting half-open sessions to accommodate new connection requests as required. The BCM50a Integrated Router continues to delete half-open sessions, as necessary, until the rate of new connection attempts drops below another threshold (**one-minute low**). The rate is the number of new attempts detected in the last one minute sample period.

TCP maximum incomplete and blocking period

An unusually high number of half-open sessions with the same destination host address indicates that a Denial of Service attack is being launched against the host.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (**TCP Maximum Incomplete**), the BCM50a Integrated Router starts deleting half-open sessions according to one of the following methods:

- If the **Blocking Period** timeout is 0 (the default), the BCM50a Integrated Router deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host never exceeds the threshold.
- If the **Blocking Period** timeout is greater than 0, the BCM50a Integrated Router blocks all new connection requests to the host giving the server time to handle the present connections. The BCM50a Integrated Router continues to block all new connection requests until the **Blocking Period** expires.

The BCM50a Integrated Router also sends alerts whenever **TCP Maximum Incomplete** is exceeded. The global values specified for the threshold and timeout apply to all TCP connections. Click the **Attack Alert** tab to bring up the screen shown in [Figure 60](#).

Figure 60 Attack alert

FIREWALL

[Table 41](#) describes the fields in [Figure 60](#).

Table 41 Attack alert

Label	Description
Generate alert when attack detected	A detected attack automatically generates a log entry. Check this box to generate an alert (as well as a log) whenever an attack is detected.
Denial of Service Thresholds	
One Minute Low	This is the rate of new half-open sessions that causes the firewall to stop deleting half-open sessions. The BCM50a Integrated Router continues to delete half-open sessions, as necessary, until the rate of new connection attempts drops below this number.

Table 41 Attack alert

Label	Description
One Minute High	<p>This is the rate of new half-open sessions that causes the firewall to start deleting half-open sessions. When the rate of new connection attempts rises above this number, the BCM50a Integrated Router deletes half-open sessions, as required, to accommodate new connection attempts.</p> <p>The numbers, for example, 80 in the One Minute Low field and 100 in this field, cause the BCM50a Integrated Router to start deleting half-open sessions when more than 100 session establishment attempts are detected in the last minute, and to stop deleting half-open sessions when fewer than 80 session establishment attempts are detected in the last minute.</p>
Maximum Incomplete Low	<p>This is the number of existing half-open sessions that causes the firewall to stop deleting half-open sessions. The BCM50a Integrated Router continues to delete half-open requests, as necessary, until the number of existing half-open sessions drops below this number.</p>
Maximum Incomplete High	<p>This is the number of existing half-open sessions that causes the firewall to start deleting half-open sessions. When the number of existing half-open sessions rises above this number, the BCM50a Integrated Router deletes half-open sessions, as required, to accommodate new connection requests. Do not set Maximum Incomplete High to lower than the current Maximum Incomplete Low number.</p> <p>The above values, say 80 in the Maximum Incomplete Low field and 100 in this field, cause the BCM50a Integrated Router to start deleting half-open sessions when the number of existing half-open sessions rises above 100, and to stop deleting half-open sessions with the number of existing half-open sessions drops below 80.</p>
TCP Maximum Incomplete	<p>This is the number of existing half-open TCP sessions with the same destination host IP address that causes the firewall to start dropping half-open sessions to that same destination host IP address. Enter a number between 1 and 256. As a general rule, choose a smaller number for a smaller network, a slower system or limited bandwidth.</p>
Blocking Period	<p>When TCP Maximum Incomplete is reached you can choose to either allow or block the next session. If you select the Blocking Period check box, any new sessions are blocked for the length of time you specify in the next field (min) and all old incomplete sessions are cleared during this period. If you want strong security, it is better to block the traffic for a short time, as it gives the server some time to digest the loading.</p>
(min)	Enter the length of Blocking Period in minutes.

Table 41 Attack alert

Label	Description
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 12

Content filtering

This chapter provides a brief overview of content filtering using the embedded WebGUI.

Introduction to content filtering

With Internet content filtering, you can create and enforce Internet access policies tailored to their needs. Content filtering is the ability to block certain web features or specific URL keywords and is not to be confused with packet filtering through SMT menu 21.1. To access these functions, from the **Main Menu**, click **Content Filter** to expand the Content Filter menus.

Restrict web features

The BCM50a Integrated Router can block web features such as ActiveX controls, Java applets, and cookies and disable web proxies.

Days and Times

With the BCM50a Integrated Router, you can also define time periods and days during which the BCM50a Integrated Router performs content filtering.

Configure Content Filtering

Click **Content Filter** on the navigation panel, to open the screen show in [Figure 61](#).

Figure 61 Content filter
CONTENT FILTERING

The screenshot shows a web-based configuration interface for content filtering. At the top, there is a tab labeled "Filter". Below the tab, the interface is organized into several sections:

- Restrict Web Features:** A horizontal row of five checkboxes: ActiveX, Java, Cookies, and Web Proxy.
- Enable URL Keyword Blocking:** A checkbox followed by the text "Enable URL Keyword Blocking".
- Keyword List Management:** A text input field labeled "Keyword" is positioned above a larger text area labeled "Keyword List". Below the "Keyword List" area are three buttons: "Add", "Delete", and "Clear All".
- Denied Access Message:** A text input field with the label "Denied Access Message" to its left.
- Day to Block:** A section with a checkbox "Everyday" and a row of checkboxes for the days of the week: Sun, Mon, Tue, Wed, Thu, Fri, and Sat.
- Time of Day to Block (24-Hour Format):** A section with a checkbox "All day" and a time selection interface. The interface includes labels "Start" and "End", each followed by two input fields for "hour" and "min".

At the bottom of the configuration area, there are two buttons: "Apply" and "Reset".

Table 42 describes the fields in Figure 61.

Table 42 Content filter

Label	Description
Restrict Web Features	Select the boxes to restrict a feature. When you download a page containing a restricted feature, that part of the web page appears blank or grayed out.
ActiveX	A tool for building dynamic and active Web pages and distributed object applications. When you visit an ActiveX Web site, ActiveX controls are downloaded to your browser, where they remain in case you visit the site again.
Java	A programming language and development environment for building downloadable Web components or Internet and intranet business applications of all kinds.
Cookies	Used by Web servers to track usage and provide service based on ID.
Web Proxy	A server that acts as an intermediary between a user and the Internet to provide security, administrative control, and caching service. When a proxy server is located on the WAN, it is possible for LAN users to circumvent content filtering by pointing to this proxy server.
Enable URL Keyword Blocking	The BCM50a Integrated Router can block Web sites with URLs that contain certain keywords in the domain name or IP address. For example, if the keyword bad was enabled, all sites containing this keyword in the domain name or IP address will be blocked, for example, URL http://www.website.com/bad.html is blocked. Select this check box to enable this feature.
Keyword	Type a keyword in this field. You can use any character (up to 64 characters). Wildcards are not allowed. You can also enter a numerical IP address.
Keyword List	This list displays the keywords already added.
Add	Click Add after you have typed a keyword. Repeat this procedure to add other keywords. Up to 64 keywords are allowed. When you try to access a web page containing a keyword, you will receive a message telling you that the content filter is blocking this request.
Delete	Highlight a keyword in the lower box and click Delete to remove it. The keyword disappears from the text box after you click Apply .
Clear All	Click this button to remove all of the listed keywords.
Day to Block	Select check boxes for the days that you want the BCM50a Integrated Router to perform content filtering. Select the Everyday check box to have content filtering turned on all days of the week.

Table 42 Content filter

Label	Description
Time of Day to Block	<p>Time of Day to Block allows the administrator to define during which time periods content filtering is enabled. Time of Day to Block restrictions only apply to the keywords (see above). Restrict web server data, such as ActiveX, Java, Cookies and Web Proxy are not affected.</p> <p>Enter the time period, in 24-hour format, during which content filtering will be enforced. Select the All Day check box to have content filtering always active on the days selected in Day to Block with time of day limitations not enforced.</p>
Apply	Click Apply to save your changes.
Reset	Click Reset to begin configuring this screen afresh

Chapter 13

VPN

This chapter introduces the basics of IPSec VPNs and covers the VPN WebGUI. See [Chapter 19, “Logs Screens,” on page 359](#) for information about viewing logs and the appendices for IPSec log descriptions.

VPN

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 or services used to transport traffic over the Internet or any insecure network that uses the TCP/IP protocol suite for communication.

Use the screens documented in this chapter to configure rules for VPN connections and manage VPN connections.

IPSec

Internet Protocol Security (IPSec) is a standards based VPN that offers flexible solutions for secure data communications across a public network like the Internet. IPSec is built around a number of standardized cryptographic techniques to provide confidentiality, data integrity and authentication at the IP layer.

BCM50a Integrated Router VPN functions

You can use the BCM50a Integrated Router as either:

- A Contivity Client (for an encrypted connection to a single VPN router).

or

- As a VPN router that can have encrypted connections to multiple remote VPN routers.

See [Table 1 on page 31](#) for details about the VPN specifications of the BCM50a Integrated Router.

VPN screens overview

[Table 43](#) summarizes the main functions of the VPN screens.

Security Association

A Security Association (SA) is a contract between two parties indicating which security parameters, such as keys and algorithms, they use.

Table 43 VPN Screens Overview

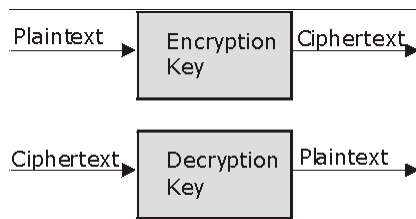
Screens		Description
Summary		This screen lists all of your VPN rules.
	Contivity Client Rule Setup	Use these screens to configure simple VPN rules that have the BCM50a Integrated Router operate as a VPN client.
	Branch Office Rule Setup	Use these screens to manually configure VPN rules that have the BCM50a Integrated Router operate as a VPN router.
SA Monitor		Use this screen to display and manage active VPN connections.
Global Setting		Use this screen to configure the IPSec timer settings.

Other terminology

Encryption

Encryption is a mathematical operation that transforms data from plaintext (readable) to ciphertext (scrambled text) using a key. The key and clear text are processed by the encryption operation, which leads to the data scrambling that makes encryption secure. Decryption is the opposite of encryption; it is a mathematical operation that transforms “ciphertext” to plaintext. Decryption also requires a key.

Figure 62 Encryption and decryption



Data confidentiality

The IPSec sender can encrypt packets before transmitting them across a network.

Data integrity

The IPSec receiver can validate packets sent by the IPSec sender to ensure that the data is not altered during transmission.

Data origin authentication

The IPSec receiver can verify the source of IPSec packets. This service depends on the data integrity service.

VPN applications

The BCM50a Integrated Router supports the following VPN applications:

- Linking Two or More Private Networks Together

Connect branch offices and business partners over the Internet with significant cost savings and improved performance when compared to leased lines between sites.

- Accessing Network Resources When NAT Is Enabled

When NAT is enabled between the WAN and the LAN, remote users are not able to access hosts on the LAN unless the host is designated a public LAN server for that specific protocol. Since the VPN tunnel terminates inside the LAN, remote users can access all computers that use private IP addresses on the LAN.

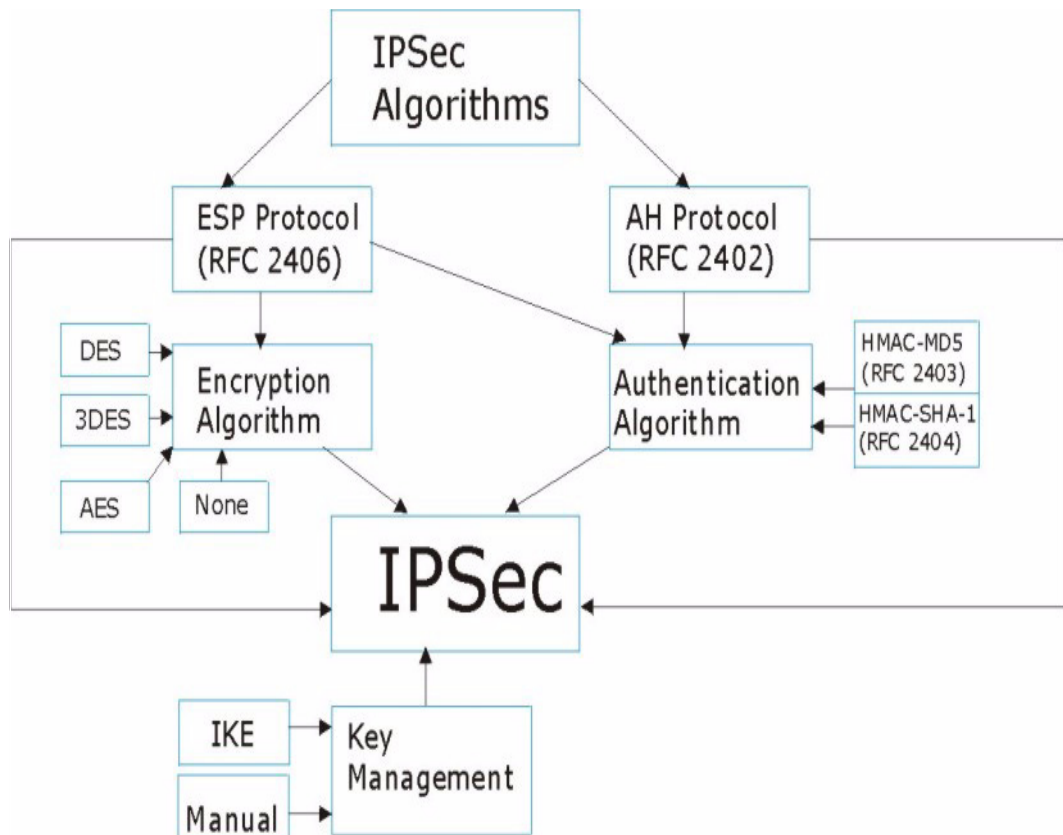
- Unsupported IP Applications

A VPN tunnel can be created to add support for unsupported emerging IP applications.

IPSec architecture

The overall IPSec architecture is shown as follows in [Figure 63](#).

Figure 63 IPsec architecture



IPsec algorithms

The **ESP** (Encapsulating Security Payload) Protocol (RFC 2406) and **AH** (Authentication Header) protocol (RFC 2402) describe the packet formats and the default standards for packet structure (including implementation algorithms).

The Encryption Algorithm describes the use of encryption techniques such as DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Triple DES algorithms.

The Authentication Algorithms, HMAC-MD5 (RFC 2403) and HMAC-SHA-1 (RFC 2404), provide an authentication mechanism for the **AH** and **ESP** protocols.

The **ESP** and **AH** protocols are necessary to create a Security Association (SA), the foundation of an IPsec VPN. An SA is built from the authentication provided by the **AH** and **ESP** protocols. The primary function of key management is to establish and maintain the SA between systems. After the SA is established, the transport of data can commence.

AH (Authentication Header) protocol

AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation but not for confidentiality, for which the **ESP** was designed.

In applications where confidentiality is not required or not sanctioned by government encryption restrictions, an **AH** can be employed to ensure integrity. This type of implementation does not protect the information from dissemination but can be used for verification of the integrity of the information and authentication of the originator.

ESP (Encapsulating Security Payload) protocol

The **ESP** protocol (RFC 2406) provides encryption, as well as the services offered by **AH**. **ESP** authenticating properties are limited compared to the **AH** due to the exclusion of the IP header information during the authentication process. However, **ESP** is sufficient if only the upper layer protocols need to be authenticated.

An added feature of the **ESP** is payload padding, which further protects communications by concealing the size of the packet being transmitted.

Table 44 AH and ESP

	ESP	AH
Encryption	DES (default) Data Encryption Standard (DES) is a widely used method of data encryption using a secret key. DES applies a 56-bit key to each 64-bit block of data.	
	3DES Triple DES (3DES) is a variant of DES, which iterates 3 times with 3 separate keys (3 x 56 = 168 bits), effectively doubling the strength of DES.	
	AES Advanced Encryption Standard is a newer method of data encryption that also uses a secret key. This implementation of AES applies a 128-bit key to 128-bit blocks of data during phase 1. You can configure the device to use a 128-bit, 192-bit or 256-bit key for phase 2. AES is faster than 3DES.	
	Select NULL to set up a phase 2 tunnel without encryption.	
Authentication	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.	MD5 (default) MD5 (Message Digest 5) produces a 128-bit digest to authenticate packet data.
	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.	SHA1 SHA1 (Secure Hash Algorithm) produces a 160-bit digest to authenticate packet data.
	Select MD5 for minimal security and SHA-1 for maximum security.	

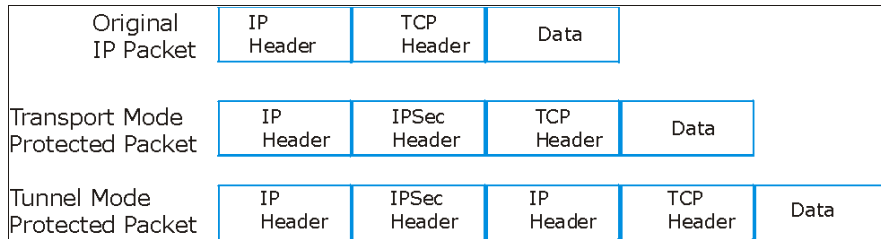
Key management

Your BCM50a Integrated Router uses IKE (ISAKMP) key management in order to set up a VPN.

Encapsulation

The two modes of operation for IPSec VPNs are **Transport** mode and **Tunnel** mode.

Figure 64 Transport and Tunnel mode IPSec encapsulation



Transport mode

Transport mode is used to protect upper layer protocols and only affects the data in the IP packet. In **Transport** mode, the IP packet contains the security protocol (**AH** or **ESP**) located after the original IP header and options, but before any upper layer protocols contained in the packet (such as TCP and UDP).

With **ESP**, protection is applied only to the upper layer protocols contained in the packet. The IP header information and options are not used in the authentication process. Therefore, the originating IP address cannot be verified for integrity against the data.

With the use of **AH** as the security protocol, protection is extended forward into the IP header to verify the integrity of the entire packet by use of portions of the original IP header in the hashing process.

Tunnel mode

Tunnel mode encapsulates the entire IP packet to transmit it securely. A **Tunnel** mode is required for gateway services to provide access to internal systems. **Tunnel** mode is fundamentally an IP tunnel with authentication and encryption. This is the most common mode of operation. **Tunnel** mode is required for BCM50a Integrated Router to BCM50a Integrated Router and host to BCM50a Integrated Router communications. **Tunnel** mode communications have two sets of IP headers:

Outside header: The outside IP header contains the destination IP address of the BCM50a Integrated Router.

Inside header: The inside IP header contains the destination IP address of the final system behind the BCM50a Integrated Router. The security protocol appears after the outer IP header and before the inside IP header.

IPSec and NAT

Read this section if you are running IPSec on a host computer behind the BCM50a Integrated Router.

NAT is incompatible with the **AH** protocol in both **Transport** and **Tunnel** mode. An IPSec VPN using the **AH** protocol digitally signs the outbound packet, both data payload and headers, with a hash value appended to the packet. When using **AH** protocol, packet contents (the data payload) are not encrypted.

A NAT device in between the IPSec endpoints rewrites either the source or destination address with one of its own choosing. The VPN device at the receiving end verifies the integrity of the incoming packet by computing its own hash value, and complains that the hash value appended to the received packet does not match. The VPN device at the receiving end does not know about the NAT in the middle, so it assumes that the data was maliciously altered.

IPSec using **ESP** in **Tunnel** mode encapsulates the entire original packet (including headers) in a new IP packet. The new IP packet's source address is the outbound address of the sending BCM50a Integrated Router, and its destination address is the inbound address of the VPN device at the receiving end. When using **ESP** protocol with authentication, the packet contents (in this case, the entire original packet) are encrypted. The encrypted contents, but not the new headers, are signed with a hash value appended to the packet.

Tunnel mode **ESP** with authentication is compatible with NAT because integrity checks are performed over the combination of the original header plus original payload, which is unchanged by a NAT device. **Transport** mode **ESP** with authentication is not compatible with NAT, although NAT traversal provides a way to use **Transport** mode **ESP** when there is a NAT router between the IPSec endpoints (see [“NAT Traversal” on page 205](#) for details).

Table 45 VPN and NAT

Security Protocol	Mode	NAT
AH	Transport	N
AH	Tunnel	N
ESP	Transport	N
ESP	Tunnel	Y

Secure Gateway Address

Secure Gateway Address is the WAN IP address or domain name of the remote secure gateway. You can specify this for a VPN rule in the **VPN Branch Office Rule Setup** screen (see [Figure 70 on page 214](#)).

If the remote secure gateway has a static WAN IP address, enter it in the **Secure Gateway Address** field. You can alternatively enter the domain name of the remote secure gateway (if it has one) in the **Secure Gateway Address** field.

You can also enter the domain name of the remote secure gateway in the **Secure Gateway Address** field if the remote secure gateway has a dynamic WAN IP address and is using DDNS. The BCM50a Integrated Router has to rebuild the VPN tunnel each time the WAN IP address of the remote secure gateway changes (there can be a delay until the DDNS servers are updated with the new WAN IP address of the remote secure gateway).

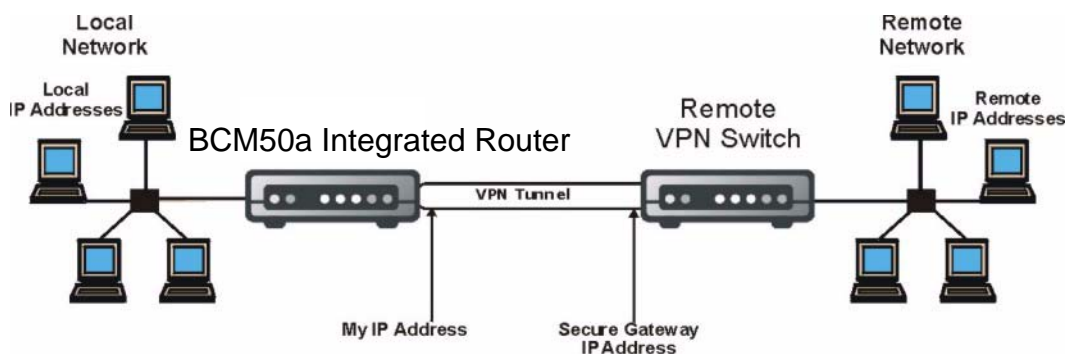
Dynamic Secure Gateway Address

If the remote secure gateway has a dynamic WAN IP address and does not use DDNS, enter 0.0.0.0 as the address of the remote secure gateway. In this case, only the remote secure gateway can initiate SAs. This is useful for telecommuters initiating a VPN tunnel to the company network.

Summary screen

[Figure 65](#) helps explain the main fields in the WebGUI.

Figure 65 IPSec summary fields



Click **VPN** to open the **Summary** screen. This is a read-only menu of your IPSec rules (tunnels). Edit or create an IPSec rule by selecting an index number and then clicking **Edit** to configure the associated submenus.

The firewall allows traffic to go through your VPN tunnels.

Figure 66 Summary
VPN

Summary										SA Monitor		Global Setting		Client Termination			
Contivity VPN Client										Connect							
#	Name	Active	Private / Local / Remote Policy IP Address			Encap.	IPSec Algorithm	Secure Gateway Address									
1	test	Yes	N/A	192.168.2.33	192.168.1.33	Tunnel	ESP SHA1	IP Policies									
2	test2	No	1.2.3.4	2.2.2.2	0.0.0.0	Tunnel	ESP SHA1										
3	test3	Yes	N/A	1.1.1.1	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0									
			N/A	1.1.1.2	0.0.0.0												
			N/A	1.1.1.3	0.0.0.0												
			N/A	1.1.1.4	0.0.0.0												
			N/A	1.1.1.5	0.0.0.0												
			N/A	1.1.1.6	0.0.0.0												
			N/A	1.1.1.7	0.0.0.0												
			N/A	1.1.1.8	0.0.0.0												
4	test4	No	-			Tunnel	ESP DES SHA1	0.0.0.0									
			N/A	1.1.2.1	0.0.0.0												
5	test5	Yes	N/A	1.1.2.2	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0									
			N/A	2.2.2.3	0.0.0.0												
			N/A	1.1.2.3	0.0.0.0												
			N/A	1.1.2.4	0.0.0.0												
6	test6	No	N/A	1.1.2.5	0.0.0.0	Tunnel	ESP DES SHA1	0.0.0.0									
			N/A	1.1.2.6	0.0.0.0												
			N/A	1.1.2.7	0.0.0.0												
			N/A	1.1.2.8	0.0.0.0												
			N/A	1.1.2.9	0.0.0.0												
			N/A	1.1.2.10	0.0.0.0												
			N/A	1.1.2.11	0.0.0.0												
			N/A	1.1.2.12	0.0.0.0												
7	test7	No	-			Tunnel	ESP DES SHA1	0.0.0.0									
8	test8	No	-			Tunnel	ESP DES SHA1	0.0.0.0									
9	test9	No	-			Tunnel	ESP DES SHA1	0.0.0.0									
10	test10	No	-			Tunnel	ESP DES SHA1	0.0.0.0									

Table 46 describes the fields in Figure 66.

Table 46 Summary

Label	Description
Contivity VPN Client	<p>The Contivity VPN Client is a simple VPN rule that lets you define and store connection information for accessing your corporate network using the BCM50a Integrated Router. The Contivity VPN Client uses the IPSec protocol to establish a secure end-to-end connection. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.</p> <p>When this button displays Connect, click it to create a VPN connection to the remote Contivity switch.</p> <p>When this button displays Disconnect, click it to drop the Contivity VPN connection.</p>
#	This is the VPN rule index number.
Name	This field displays the name you specified in the VPN Branch Office Rule Setup screen to identify this VPN policy.
Active	This field displays whether the VPN rule is active or not. A Yes signifies that this VPN rule is active. No signifies that this VPN rule is not active.
Private /Local / Remote Policy IP Address	<p>These are the IP addresses of the computers that can use the VPN tunnel. Ranges of IP addresses are indicated by the starting and ending IP addresses separated by a dash. You configure these IP addresses in the VPN Branch Office IP Policy screen. This field is empty if you do not configure the VPN branch office rule to use an IP policy.</p> <p>Private IP addresses are IP addresses of computers on your BCM50a Integrated Router's local network, for which you have configured the IP policy to use NAT for the VPN tunnel.</p> <p>Local IP addresses are the IP addresses of the computers on your BCM50a Integrated Router's local network that can use the VPN tunnel.</p> <p>Remote IP addresses are the IP addresses of the computers behind the remote IPSec router that can use the VPN tunnel. When 0.0.0.0 displays, only the remote IPSec router can initiate the VPN. The address 0.0.0.0 displays when the Secure Gateway Address field is configured to 0.0.0.0 or the IP policy's Remote Starting IP Address field is set to 0.0.0.0 in the IP Policy screen.</p>
Encap	This field displays Tunnel or Transport mode.
IPSec Algorithm	<p>This field displays the security protocols used for an SA.</p> <p>Both AH and ESP increase BCM50a Integrated Router processing requirements and communications latency (delay).</p>
Secure Gateway Address	<p>This is the static WAN IP address or URL of the remote IPSec router.</p> <p>This field displays 0.0.0.0 when you configure the Secure Gateway Address field in the VPN Branch Office screen to 0.0.0.0.</p>

Table 46 Summary

Label	Description
Edit	Click the radio button next to a VPN index number and then click Edit to edit a specific VPN policy.
Delete	Click the radio button next to a VPN policy number you want to delete and then click Delete . When a VPN policy is deleted, subsequent policies do not move up in the page list.

Keep Alive

When you initiate an IPSec tunnel with keep alive enabled, the BCM50a Integrated Router automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [“Configuring advanced Branch office setup” on page 233](#) section for more information about the IPSec SA lifetime). The keep alive option is available with the Contivity Client rule. See the **VPN Contivity Client Rule Setup** screen ([Figure 68 on page 207](#)). In effect, the IPSec tunnel becomes an always on connection after you initiate it. Both IPSec routers must have a BCM50a Integrated Router compatible keep alive feature enabled in order for this feature to work.

If the BCM50a Integrated Router has its maximum number of simultaneous IPSec tunnels connected to it and they all have keep alive enabled, then no other tunnels can take a turn connecting to the BCM50a Integrated Router because the BCM50a Integrated Router does not drop the tunnels that are already connected (unless there is outbound traffic with no inbound traffic).



Note: No matter whether or not keep alive is set, when there is outbound traffic with no inbound traffic, the BCM50a Integrated Router automatically drops the tunnel after two minutes.

Nailed up

The nailed up feature is similar to the keep alive feature. When you initiate an IPSec tunnel with nailed up enabled, the BCM50a Integrated Router automatically renegotiates the tunnel when the IPSec SA lifetime period expires (see [“Configuring advanced Branch office setup” on page 233](#) for more

information about the IPSec SA lifetime). The nailed up option is available with the branch office rules. See the **VPN Branch Office Rule Setup** screen (Figure 70 on page 214). Unlike keep alive, any time the BCM50a Integrated Router restarts, it also automatically renegotiates any nailed up tunnels. In effect, the IPSec tunnel becomes an “always on” connection after you initiate it. Also different from keep alive, the peer IPSec router does not have to have a BCM50a Integrated Router compatible nailed up feature enabled in order for this feature to work.

If the BCM50a Integrated Router has its maximum number of simultaneous IPSec tunnels connected to it and they all have nailed up enabled, no other tunnels can take a turn connecting to the BCM50a Integrated Router because the BCM50a Integrated Router does not drop the tunnels that are already connected (unless there is outbound traffic with no inbound traffic).

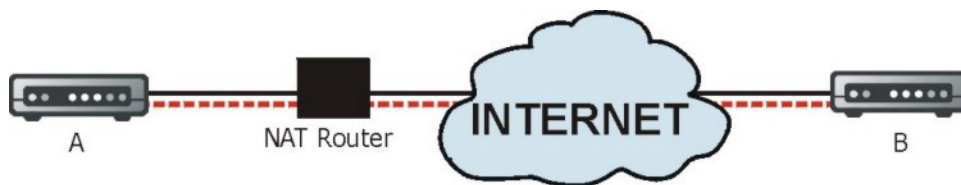


Note: No matter whether or not nailed up is set, when there is outbound traffic with no inbound traffic, the BCM50a Integrated Router automatically drops the tunnel after two minutes.

NAT Traversal

NAT traversal allows you to set up a VPN connection when there are NAT routers between the BCM50a Integrated Router and the remote IPSec router.

Figure 67 NAT router between IPSec routers



Normally, you cannot set up a VPN connection with a NAT router between the two IPSec routers because the NAT router changes the header of the IPSec packet. In the previous figure, IPSec router A sends an IPSec packet in an attempt to initiate a VPN. The NAT router changes the header of the IPSec packet so it does not match the header for which IPSec router B is checking. Therefore, IPSec router B does not respond and the VPN connection cannot be built.

NAT traversal solves the problem by adding a UDP port 500 header to the IPSec packet. The NAT router forwards the IPSec packet with the UDP port 500 header unchanged. IPSec router B checks the UDP port 500 header and responds. IPSec routers A and B build a VPN connection.

NAT Traversal configuration

Enable or disable NAT traversal in the **VPN Branch Office Rule Setup** screen (see [Figure 70 on page 214](#)). For NAT traversal to work, you must:

- Use ESP security protocol (in either transport or tunnel mode)
- Use IKE keying mode
- Enable NAT traversal on both IPSec endpoints

In order for IPSec router A (see [Figure 70 on page 214](#)) to receive an initiating IPSec packet from IPSec router B, set the NAT router to forward UDP port 500 to IPSec router A.

Preshared key

A preshared key identifies a communicating party during a phase 1 IKE negotiation (see [“IKE phases” on page 230](#) for more information). It is called preshared because you have to share it with another party before you can communicate with them over a secure connection. For Contivity Client VPN connections, the BCM50a Integrated Router generates the preshared key from the username and password.

Configuring Contivity Client VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. The **VPN Contivity Client Rule Setup** screen is shown in [Figure 68](#).

Figure 68 VPN Contivity Client rule setup**VPN - Contivity Client**
Table 47 VPN Contivity Client rule setup

Label	Description
Connection Type	Select Branch Office to manually configure a VPN rule. This has the BCM50a Integrated Router operate as a VPN router. Select Contivity Client to use a simple VPN rule that lets you define and store connection information for accessing your corporate network through a IPSec router. This has the BCM50a Integrated Router operate as a VPN client.
Active	Select this check box to turn on this rule. Clear this check box if you do not want to use this rule after you apply it. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive. To set a Contivity Client rule to active, all of the other VPN rules must be disabled.
Keep Alive	Select this check box to turn on the Keep Alive feature for this SA. Turn on Keep Alive to have the BCM50a Integrated Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The remote IPSec router must also have keep alive enabled in order for this feature to work.
Description	Enter a brief description about this rule for identification purposes.

Table 47 VPN Contivity Client rule setup

Label	Description
Destination	This field specifies the IP address or the domain name (up to 31 case-sensitive characters) of the remote IPSec router. You can use alphanumeric characters, the underscore, dash, period and the @ symbol in a domain name. No spaces are allowed.
User Name	Enter the username exactly as the IPSec router administrator gives it to you.
Password	Enter the password exactly as the IPSec router administrator gives it to you.
Advanced	Click Advanced to configure group authentication and on-demand client tunnel settings.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to return to the VPN Summary screen without saving your changes.

Configuring Advanced Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule. If the **Branch Office** screen is displayed, select **Contivity Client** from the **Connection Type** list box. Click **Advanced** to display the **VPN Contivity Client Advanced Rule Setup** screen as shown in [Figure 69](#).

Figure 69 VPN Contivity Client advanced rule setup**VPN - Contivity Client - Advanced**

Table 48 describes the fields in Figure 69.

Table 48 VPN Contivity Client advanced rule setup

Label	Description
Group Authentication	Enable Group Authentication to have the BCM50a Integrated Router send a Group ID and Group Password to the remote IPsec router for initial authentication. After a successful initial authentication, a RADIUS server associated with the remote IPsec router uses the User Name and Password to authenticate the BCM50a Integrated Router. You must also configure the Group ID and Group Password fields when you enable Group Authentication . After Group Authentication is not enabled, the remote IPsec router uses the User Name and Password to authenticate the BCM50a Integrated Router.
Group ID	Enter the group ID exactly as the IPsec router administrator gives it to you. This field only applies when you enable Group Authentication .
Group Password	Enter the group password exactly as the IPsec router administrator gives you. This field only applies when you enable Group Authentication .
On Demand Client Tunnel	Select this check box to have any outgoing packets automatically trigger a VPN connection to the remote IPsec router. When On Demand Client Tunnel is not enabled, you need to go to the VPN Summary screen and click the Connect button to create a VPN connection to the remote IPsec router.

Table 48 VPN Contivity Client advanced rule setup

Label	Description
Apply	Click Apply to temporarily save the settings and return to the VPN - Contivity Client screen. The Group Authentication settings are saved to the BCM50a Integrated Router if you click Apply in the VPN - Contivity Client screen.
Cancel	Click Cancel to return to the VPN Contivity Client Rule Setup screen without saving your changes.

ID Type and content

With aggressive negotiation mode (see [“Negotiation Mode” on page 232](#) for more information), the BCM50a Integrated Router identifies incoming SAs by ID type and content since this identifying information is not encrypted, so that it can distinguish between multiple rules for SAs that connect from remote IPsec routers that have dynamic WAN IP addresses. Telecommuters can use separate passwords to simultaneously connect to the BCM50a Integrated Router from IPsec routers with dynamic IP addresses.



Note: Regardless of the ID type and content configuration, you cannot save multiple active rules with overlapping local and remote IP addresses with the BCM50a Integrated Router.

With the main negotiation mode (see [“Negotiation Mode” on page 232](#) for more information), the ID type and content are encrypted to provide identity protection. In this case the BCM50a Integrated Router can only distinguish between up to 12 different incoming SAs that connect from remote IPsec routers that have dynamic WAN IP addresses. The BCM50a Integrated Router can distinguish up to 12 incoming SAs because you can select between two encryption algorithms (DES and 3DES), two authentication algorithms (MD5 and SHA1) and three key groups (DH1, DH2, and DH5) when you configure a VPN rule (see [“Configuring advanced Branch office setup” on page 233](#)). The ID type and content act as an extra level of identification for incoming SAs.

Configure the ID type and content in the **VPN Branch Office Rule Setup** screen (see [Figure 70 on page 214](#)). The type of ID can be a domain name, an IP address, or an e-mail address. The content is the IP address, domain name, or e-mail address.

Table 49 Local ID type and content fields

Local ID type=	Content=
IP	Type the IP address of your computer or leave the field blank to have the BCM50a Integrated Router automatically use its own IP address.
DNS	Type a domain name (up to 31 characters) by which to identify this BCM50a Integrated Router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify this BCM50a Integrated Router.
The domain name or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address.	

Table 50 Peer ID type and content fields

Peer ID type=	Content=
IP	Type the IP address of the computer with which you make the VPN connection or leave the field blank to have the BCM50a Integrated Router automatically use the address in the Secure Gateway field.
DNS	Type a domain name (up to 31 characters) by which to identify the remote IPSec router.
E-mail	Type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.
The domain name or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the IP address of the remote IPSec router or what you configure in the Secure Gateway Address field below.	

ID type and content examples

Two IPSec routers must have matching ID type and content configuration in order to set up a VPN tunnel.

The two BCM50a Integrated Routers shown in [Table 51](#) can complete negotiation and establish a VPN tunnel.

Table 51 Matching ID type and content configuration example

BCM50a Integrated Router A	BCM50a Integrated Router B
Local ID type: E-mail	Local ID type: IP
Local ID content: tom@yourcompany.com	Local ID content: 1.1.1.2
Peer ID type: IP	Peer ID type: E-mail
Peer ID content: 1.1.1.2	Peer ID content: tom@yourcompany.com

The two BCM50a Integrated Routers shown in [Table 52](#) cannot complete their negotiation because the **Local ID type** of BCM50a Integrated Router B is **IP**, but the **Peer ID type** in BCM50a Integrated Router A is set to **E-mail**. An “ID mismatched” message displays in the IPSEC LOG.

Table 52 Mismatching ID Type and Content Configuration Example

BCM50a Integrated Router A	BCM50a Integrated Router B
Local ID type: IP	Local ID type: IP
Local ID content: 1.1.1.10	Local ID content: 1.1.1.10
Peer ID type: E-mail	Peer ID type: IP
Peer ID content: aa@yahoo.com	Peer ID content: N/A

My IP Address

My IP Address is the WAN IP address of the BCM50a Integrated Router. The BCM50a Integrated Router has to rebuild the VPN tunnel if the **My IP Address** changes after setup.

The following applies if this field is configured as 0.0.0.0:

- The BCM50a Integrated Router uses the current BCM50a Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel.

Configuring Branch Office VPN Rule Setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule. The **VPN Branch Office Rule Setup** screen is shown in [Figure 70](#).

Figure 70 VPN Branch Office rule setup

VPN - Branch Office

Connection Type

Active NAT Traversal

Nailed Up

Name

Key Management

Negotiation Mode

Encapsulation Mode

Available IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
<input checked="" type="radio"/> 1	1.0.0.17	10.0.0.17	10.0.0.36-10.0.0.45

Selected IP Policy:

#	Private IP Address	Local IP Address	Remote IP Address
<input checked="" type="radio"/> 1	N/A	192.168.2.33	192.168.1.33

Authentication Method

Pre-Shared Key
Retype to Confirm

Certificate
(See [My Certificates](#))

Local ID Type
Content

Peer ID Type
Content

My IP Address
Secure Gateway Address

ESP AH

Encryption Algorithm Authentication Algorithm

Authentication Algorithm

Table 53 describes the fields in Figure 70.

Table 53 VPN Branch Office rule setup

Label	Description
Connection Type	Select Branch Office to manually configure a VPN rule. Select Contivity Client to use a simple VPN rule that lets you define and store connection information for accessing your corporate network using the BCM50a Integrated Router. You can only configure one Contivity client rule. If you want to set the Contivity Client rule to active, you must set all other VPN rules to inactive.
Active	Select this check box to activate this VPN tunnel. This option determines whether a VPN rule is applied.
Nailed Up	Select this check box to turn on the nailed up feature for this SA. Turn on nailed up to have the BCM50a Integrated Router automatically reinitiate the SA after the SA lifetime times out, even if there is no traffic. The BCM50a Integrated Router also reinitiates the SA when it restarts.
NAT Traversal	Select this check box to enable NAT traversal. With NAT traversal, you can set up a VPN connection when there are NAT routers between the two IPsec routers. The remote IPsec router must also have NAT traversal enabled. You can use NAT traversal with ESP protocol using Transport or Tunnel mode, but not with AH protocol. In order for a IPsec router behind a NAT router to receive an initiating IPsec packet, set the NAT router to forward UDP port 500 to the IPsec router behind the NAT router.
Name	Type a name to identify this VPN policy. You can use any character, including spaces, but the BCM50a Integrated Router drops trailing spaces.
Key Management	Your BCM50a Integrated Router uses IKE (ISAKMP) key management in order to set up a VPN.
Negotiation Mode	Select Main for identity protection. Select Aggressive to allow more incoming connections from dynamic IP addresses to use separate passwords. Multiple SAs connecting through a IPsec router must have the same negotiation mode.
Encapsulation Mode	Select Tunnel mode or Transport mode from the drop-down list. Tunnel is compatible with NAT, Transport is not.

Table 53 VPN Branch Office rule setup

Label	Description
Available/ Selected IP Policy	<p>The Available IP Policy table displays network routes. Use the Add, Edit and Delete buttons to configure this list.</p> <p>Move the network routes that you want to use the VPN tunnel down into the Selected IP Policy table.</p> <p>Select a network route's radio button in the Available IP Policy table, then click the down arrows to move it into the Selected IP Policy table. To remove a network route from the Selected IP Policy table, select its radio button in the Selected IP Policy table and click the up arrows.</p> <p>A network route that is already selected for a VPN tunnel does not display in the Available IP Policy table.</p>
Private IP Address	<p>This field displays the IP address (or a range of IP addresses) of the computers on your BCM50a Integrated Router's local network, for which you have configured this VPN rule. For a range of addresses, the starting and ending IP addresses are displayed separated by a dash.</p> <p>This field applies when you configure the IP policy to use a branch tunnel NAT address mapping rule in the IP Policy screen.</p> <p>This field displays a single (static) IP address when the IP policy's Branch Tunnel NAT Address Mapping Rule Type field is configured to One-to-One in the IP Policy screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's Branch Tunnel NAT Address Mapping Rule Type field is configured to Many-to-One or Many One-to-one in the IP Policy screen.</p>

Table 53 VPN Branch Office rule setup

Label	Description
Local IP Address	<p>This field displays the IP address (or range of IP addresses) of the computers on your BCM50a Integrated Router's local network, for which you have configured this IP policy.</p> <p>This field displays the IP policy's virtual IP address (or range of addresses) when you enable branch tunnel NAT address mapping in the IP Policy screen.</p> <p>This field displays a single (static) IP address when the IP policy's Branch Tunnel NAT Address Mapping Rule Type field is configured to One-to-one or Many-to-One in the IP Policy screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the policy's Branch Tunnel NAT Address Mapping Rule Type field is configured to Many One-to-one in the IP Policy screen.</p> <p>This field displays the policy's local IP address (or range of addresses) when you disable branch tunnel NAT address mapping in the IP Policy screen.</p> <p>This field displays a single (static) IP address when the IP policy's Local Address Type field is configured to Single Address in the IP Policy screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's Local Address Type field is configured to Range Address in the IP Policy screen.</p> <p>This field displays a (static) IP address and a subnet mask when the IP policy's Local Address Type field is configured to Subnet Address in the IP Policy screen.</p>

Table 53 VPN Branch Office rule setup

Label	Description
Remote IP Address	<p>This field displays the IP addresses of computers on the remote network behind the remote IPsec router.</p> <p>This field displays a single (static) IP address when the IP policy's Remote Address Type field is configured to Single Address in the IP Policy screen.</p> <p>This field displays the beginning and ending (static) IP addresses of a range of computers when the IP policy's Remote Address Type field is configured to Range Address in the IP Policy screen.</p> <p>This field displays a (static) IP address and a subnet mask when the IP policy's Remote Address Type field is configured to Subnet Address in the IP Policy screen.</p> <p>This field displays ALL whenever the Secure Gateway Address field is set to 0.0.0.0.</p> <p>This field also displays ALL whenever the IP policy's Remote Starting IP Address field is set to 0.0.0.0 in the IP Policy screen.</p> <p>When ALL displays, only the remote IPsec router can initiate the VPN.</p>
Add	Select Add to open a screen where you can configure an IP policy.
Edit	Select the radio button next to an IP policy and then click Edit to edit that IP policy.
Delete	Select the radio button next to an IP policy that you want to remove and then click Delete .
Authentication Method	<p>Select the Pre-Shared Key radio button to use a preshared secret key to identify the BCM50a Integrated Router.</p> <p>Select the Certificate radio button to identify the BCM50a Integrated Router by a certificate.</p>
Pre-Shared Key	<p>Type your preshared key in this field. A preshared key identifies a communicating party during a phase 1 IKE negotiation. It is called preshared because you must share it with another party before you can communicate with that party over a secure connection.</p> <p>Type from 8 to 32 case-sensitive ASCII characters or from 16 to 62 hexadecimal (0-9, A-F) characters. You must precede a hexadecimal key with a 0x (zero x), which is not counted as part of the 16 to 62 character range for the key. For example, in 0x0123456789ABCDEF, "0x" denotes that the key is hexadecimal and "0123456789ABCDEF" is the key itself.</p> <p>Both ends of the VPN tunnel must use the same preshared key. You see a "PYLD_MALFORMED" (payload malformed) log if the same preshared key is not used on both ends.</p>
Retype to Confirm	Type your preshared key again in this field.

Table 53 VPN Branch Office rule setup

Label	Description
Certificate	<p>Use the drop-down list to select the certificate to use for this VPN tunnel.</p> <p>You must have certificates already configured in the My Certificates screen. Click My Certificates to go to the My Certificates screen, where you can view the BCM50a Integrated Router's list of certificates.</p>
Local ID Type	<p>Select IP to identify this BCM50a Integrated Router by its IP address.</p> <p>Select DNS to identify this BCM50a Integrated Router by a domain name.</p> <p>Select E-mail to identify this BCM50a Integrated Router by an e-mail address.</p>
Local Content	<p>When you select IP in the Local ID Type field, type an IP address or leave the field blank to have the BCM50a Integrated Router automatically use its own IP address.</p> <p>When you select DNS in the Local ID Type field, type a domain name (up to 31 characters) by which to identify this BCM50a Integrated Router.</p> <p>When you select E-mail in the Local ID Type field, type an e-mail address (up to 31 characters) by which to identify this BCM50a Integrated Router.</p> <p>The IP address, domain name, or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address.</p>
Peer ID Type	<p>Select IP to identify the remote IPSec router by its IP address.</p> <p>Select DNS to identify the remote IPSec router by a domain name.</p> <p>Select E-mail to identify the remote IPSec router by an e-mail address.</p>

Table 53 VPN Branch Office rule setup

Label	Description
Peer Content	<p>When you select IP in the Peer ID Type field, type the IP address of the computer with which you make the VPN connection or leave the field blank to have the BCM50a Integrated Router automatically use the address in the Secure Gateway Address field.</p> <p>When you select DNS in the Peer ID Type field, type a domain name (up to 31 characters) by which to identify the remote IPSec router.</p> <p>When you select E-mail in the Peer ID Type field, type an e-mail address (up to 31 characters) by which to identify the remote IPSec router.</p> <p>The domain name or e-mail address that you use in the Content field is used for identification purposes only and does not need to be a real domain name or e-mail address. The domain name also does not have to match the remote router's IP address or what you configure in the Secure Gateway Address field.</p> <p>Regardless of how you configure the ID Type and Content fields, two active SAs cannot have both the local and remote IP address ranges overlap between rules.</p>
My IP Address	<p>Enter the WAN IP address of your BCM50a Integrated Router. The VPN tunnel has to be rebuilt if this IP address changes.</p> <p>The following applies if this field is configured as 0.0.0.0 (the default):</p> <ul style="list-style-type: none"> • The BCM50a Integrated Router uses the current BCM50a Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel.
Secure Gateway Address	<p>Type the WAN IP address or the domain name (up to 31 characters) of the IPSec router with which you are making the VPN connection. Set this field to 0.0.0.0 if the remote IPSec router has a dynamic WAN IP address (the Key Management field must be set to IKE). The remote address fields do not apply when the Secure Gateway Address field is configured to 0.0.0.0. In this case, only the remote IPSec router can initiate the VPN.</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the full IP address range of the LAN as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p>

Table 53 VPN Branch Office rule setup

Label	Description
ESP	Select ESP if you want to use ESP (Encapsulation Security Payload). The ESP protocol (RFC 2406) provides encryption as well as the services offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields (described next).
AH	Select AH if you want to use AH (Authentication Header Protocol). The AH protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation, but not for confidentiality, for which the ESP was designed. If you select AH here, you must select options from the Authentication Algorithm field.
Encryption Algorithm	<p>Select DES, 3DES, AES 128, AES 192, AES 256 or NULL from the drop-down list.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of AES. AES is faster than 3DES.</p> <p>Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>
Authentication Algorithm	Select SHA1 or MD5 from the drop-down list. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5 , but is slower. Select MD5 for minimal security and SHA-1 for maximum security.
Advanced	Click Advanced to go to a screen where you can configure detailed IKE (Internet Key Exchange) negotiation—phase 1 (Authentication) and phase 2 (Key Exchange) settings for the rule.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to return to the VPN Summary screen without saving your changes.

Configuring an IP Policy

Select one of the IP policies in the **VPN Branch Office** screen and click **Add** or **Edit** to configure the policy. The **Branch Office – IP Policy** setup screen is shown in [Figure 71](#).

Figure 71 VPN Branch Office — IP Policy

VPN - Branch Office - IP Policy

Protocol	<input type="text" value="0"/>
<input checked="" type="checkbox"/> Enable Control Ping	
Control Ping IP Address	<input type="text" value="10.0.0.37"/>
<input checked="" type="checkbox"/> Active	
Branch Tunnel NAT Address Mapping Rule:	<input type="text" value="Port Forwarding Server"/>
Type	<input type="text" value="One-to-One"/>
Private Starting IP Address	<input type="text" value="1.0.0.17"/>
Private Ending IP Address	<input type="text"/>
Virtual Starting IP Address	<input type="text" value="10.0.0.17"/>
Virtual Ending IP Address	<input type="text"/>
Local :	
Address Type	<input type="text" value="Single Address"/>
Starting IP Address	<input type="text" value="0.0.0.0"/>
Ending IP Address / Subnet Mask	<input type="text" value="0.0.0.0"/>
Port	<input type="text" value="0"/>
Remote :	
Address Type	<input type="text" value="Range Address"/>
Starting IP Address	<input type="text" value="10.0.0.36"/>
Ending IP Address / Subnet Mask	<input type="text" value="10.0.0.45"/>
Port	<input type="text" value="0"/>
<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>

Table 54 describes the fields in Figure 71.

Table 54 VPN Branch Office — IP Policy

Label	Description
Protocol	<p>Enter a number to specify what type of traffic is allowed to go through the VPN tunnel that is built using this IP policy. For example, use 1 for ICMP, 6 for TCP, 17 for UDP. 0 is the default and signifies any protocol. For example, if you select 1 (ICMP), only ICMP packets can go through the tunnel.</p> <p>If you specify a protocol other than 1 (ICMP) or 0 (any protocol), you cannot use the control ping feature.</p> <p>If you set this field to 6 (TCP) or 17 (UDP), you can use the Port field to specify the port number of the allowed traffic.</p>
Enable Control Ping	<p>Select the check box and configure an IP address in the Control Ping IP Address field to have the BCM50a Integrated Router periodically test the VPN tunnel to the branch office.</p> <p>The BCM50a Integrated Router pings the IP address every minute. The BCM50a Integrated Router starts the IPsec connection idle timeout timer when it sends the ping packet. If there is no traffic from the remote IPsec router by the time the timeout period expires, the BCM50a Integrated Router disconnects the VPN tunnel.</p>
Control Ping IP Address	<p>If you select Enable Control Ping, enter the IP address of a computer at the branch office. The computer's IP address must be in this IP policy's remote range (see the Remote fields).</p>
Branch Tunnel NAT Address Mapping Rule	
Port Forwarding Server	<p>Click Port Forwarding Server to configure a list of inside (behind NAT on the LAN) servers, for example, web or FTP. The BCM50a Integrated Router makes these servers visible to the devices using the VPN branch NAT tunnel (from behind the remote IPsec router) even though NAT makes your inside network appear as a single machine. This option applies when the Type field is configured to Many-to-One.</p>
Active	<p>Enable this feature to have the BCM50a Integrated Router use a different (virtual) IP address for the VPN connection. When you enable branch tunnel NAT address mapping, you do not configure the local section.</p>

Table 54 VPN Branch Office — IP Policy

Label	Description
Type	<p>Select one of the following port mapping types.</p> <ol style="list-style-type: none"> 1. One-to-One: One-to-one mode maps one private IP address to one virtual IP address. Port numbers do not change with one-to-one NAT mapping. 2. Many-to-One: Many-to-One mode maps multiple private IP addresses to one virtual IP address. This is equivalent to SUA (for example, PAT, port address translation), BCM50a Integrated Router's Single User Account feature. 3. Many One-to-one: Many One-to-one mode maps each private IP address to a unique virtual IP address. Port numbers do not change with many one-to-one NAT mapping.
Private Starting IP Address	<p>When the Type field is configured to One-to-one, enter the (static) IP address of the computer on your BCM50a Integrated Router's LAN that is to use the VPN tunnel.</p> <p>When the Type field is configured to Many-to-One or Many One-to-one, enter the beginning (static) IP address of the range of computers on your BCM50a Integrated Router's LAN that are to use the VPN tunnel.</p>
Private Ending IP Address	<p>When the Type field is configured to One-to-one, this field is N/A.</p> <p>When the Type field is configured to Many-to-One or Many One-to-one, enter the ending (static) IP address of the range of computers on your BCM50a Integrated Router's LAN that are to use the VPN tunnel.</p>
Virtual Starting IP Address	<p>Virtual addresses must be static and correspond to the remote IPsec router's configured remote IP addresses.</p> <p>The computers on the BCM50a Integrated Router's LAN and the remote network can function as if they were on the same subnet when the virtual IP address(es) is on the same subnet as the remote IP addresses.</p> <p>Two active SAs can have the same virtual or remote IP address, but not both. You can configure multiple SAs between the same virtual and remote IP addresses, as long as only one is active at a time.</p> <p>When the Type field is configured to One-to-one or Many-to-One, enter the (static) IP address that you want to use for the VPN tunnel.</p> <p>When the Type field is configured to Many One-to-one, enter the beginning (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.</p>

Table 54 VPN Branch Office — IP Policy

Label	Description
Virtual Ending IP Address	<p>When the Type field is configured to One-to-one or Many-to-One, this field is N/A.</p> <p>When the Type field is configured to Many One-to-one, enter the ending (static) IP address of the range of IP addresses that you want to use for the VPN tunnel.</p>
Local	<p>Local IP addresses must be static and correspond to the remote IPsec router's configured remote IP addresses.</p> <p>Two active SAs can have the same local or remote IP address, but not both. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at a time.</p> <p>Two IP policies can have the same local or remote IP address, but not both.</p> <p>In order to have more than one active rule with the Secure Gateway Address field set to 0.0.0.0, the ranges of the local IP addresses cannot overlap between rules.</p> <p>If you configure an active rule with 0.0.0.0 in the Secure Gateway Address field and the full IP address range of the LAN as the local IP address, then you cannot configure any other active rules with the Secure Gateway Address field set to 0.0.0.0.</p>
Address Type	<p>Use the drop-down menu to choose Single Address, Range Address, or Subnet Address. Select Single Address for a single IP address. Select Range Address for a specific range of IP addresses. Select Subnet Address to specify IP addresses on a network by their subnet mask.</p>
Starting IP Address	<p>When the Address Type field is configured to Single Address, enter a (static) IP address on the LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Range Address, enter the beginning (static) IP address, in a range of computers on your LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Subnet Address, this is a (static) IP address on the LAN behind your BCM50a Integrated Router.</p>
Ending IP Address / Subnet Mask	<p>When the Address Type field is configured to Single Address, this field is N/A. When the Address Type field is configured to Range Address, enter the end (static) IP address, in a range of computers on the LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Subnet Address, this is a subnet mask on the LAN behind your BCM50a Integrated Router.</p>

Table 54 VPN Branch Office — IP Policy

Label	Description
Protocol	<p>Enter a number to specify what type of traffic is allowed to go through the VPN tunnel that is built using this IP policy. For example, use 1 for ICMP, 6 for TCP, 17 for UDP. 0 is the default and signifies any protocol. For example, if you select 1 (ICMP), only ICMP packets can go through the tunnel.</p> <p>If you specify a protocol other than 1 (ICMP) or 0 (any protocol), you cannot use the control ping feature.</p> <p>If you set this field to 6 (TCP) or 17 (UDP), you can use the Port field to specify the port number of the allowed traffic.</p>
Port	<p>This field is available when you set the Protocol field to 6 (TCP) or 17 (UDP). Use this field to specify the port number of the traffic that is allowed to go through the VPN tunnel that is built using this IP policy.</p> <p>The default is 0 and it signifies any port. Type a port number from 0 to 65 535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.</p> <p>Do this if you want to allow only traffic of a particular port number to go through the VPN tunnel. For example, if you only wanted to allow FTP traffic to go through the VPN tunnel, specify 6 (TCP) in the Protocol field and 21 (FTP) in the Port field.</p>
Remote	<p>Remote IP addresses must be static and correspond to the remote IPSec router's configured local IP addresses. The remote fields do not apply when the Secure Gateway Address field is configured to 0.0.0.0. In this case, only the remote IPSec router can initiate the VPN.</p> <p>Two active SAs cannot have the local and remote IP addresses both the same. You can configure multiple SAs between the same local and remote IP addresses, as long as only one is active at any time.</p> <p>Two IP policies can have the same local or remote IP address, but not both.</p>
Address Type	<p>Use the drop-down menu to choose Single Address, Range Address, or Subnet Address. Select Single Address for a single IP address. Select Range Address for a specific range of IP addresses. Select Subnet Address to specify IP addresses on a network by their subnet mask.</p>
Starting IP Address	<p>When the Address Type field is configured to Single Address, enter a (static) IP address on the LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Range Address, enter the beginning (static) IP address, in a range of computers on your LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Subnet Address, this is a (static) IP address on the LAN behind your BCM50a Integrated Router.</p>

Table 54 VPN Branch Office — IP Policy

Label	Description
Ending IP Address / Subnet Mask	When the Address Type field is configured to Single Address , this field is N/A. When the Address Type field is configured to Range Address , enter the end (static) IP address, in a range of computers on the LAN behind your BCM50a Integrated Router. When the Address Type field is configured to Subnet Address , this is a subnet mask on the LAN behind your BCM50a Integrated Router.
Port	By default, 0 signifies any port. Type a port number from 0 to 65 535. Some of the most common IP ports are: 21, FTP; 53, DNS; 23, Telnet; 80, HTTP; 25, SMTP; 110, POP3.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to return to the VPN Branch Office screen without saving your changes.

Port forwarding server

A NAT server set is a list of inside (behind NAT on the LAN) servers, for example, web or FTP, that you can make visible to the devices using the VPN branch NAT tunnel (from behind the remote IPSec router) even though NAT makes your inside network appear as a single machine. The servers must be using the VPN branch NAT tunnel (from behind the BCM50a Integrated Router).

You can enter a single port or a range of ports to be forwarded and then the local IP address of the desired inside servers.

Configuring a port forwarding server

Select one of the IP Policies in the **VPN Branch Office** screen and click **Edit** to display the **Branch Office – IP Policy** setup screen. For the Mapping Rule Type, select **Many-to-One**, enter the private and virtual IP addresses and click the **Port Forwarding Server** button to display the screen shown in [Figure 72](#).

Figure 72 VPN Branch Office — IP Policy - Port Forwarding Server
 VPN - Branch Office - IP Policy - Port Forwarding Server

Default Server: 0.0.0.0

#	Active	Name	Start Port	End Port	Server IP Address
1	<input type="checkbox"/>		0	0	0.0.0.0
2	<input type="checkbox"/>		0	0	0.0.0.0
3	<input type="checkbox"/>		0	0	0.0.0.0
4	<input type="checkbox"/>		0	0	0.0.0.0
5	<input type="checkbox"/>		0	0	0.0.0.0
6	<input type="checkbox"/>		0	0	0.0.0.0
7	<input type="checkbox"/>		0	0	0.0.0.0
8	<input type="checkbox"/>		0	0	0.0.0.0
9	<input type="checkbox"/>		0	0	0.0.0.0
10	<input type="checkbox"/>		0	0	0.0.0.0
11	<input type="checkbox"/>		0	0	0.0.0.0

Buttons: Apply, Reset, Cancel

Table 55 describes the fields in Figure 72.

Table 55 VPN Branch Office — IP Policy - Port Forwarding Server

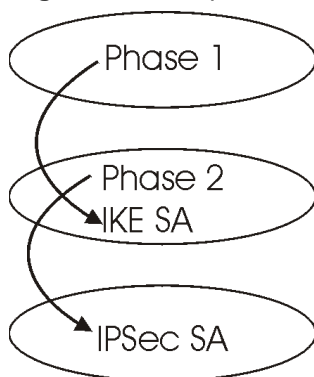
Label	Description
Default Server	In addition to the servers for specified services, NAT supports a default server. A default server receives packets from ports that are not specified in this screen. If you do not assign a default server IP address, all packets received for ports not specified in this screen are discarded.
#	Number of an individual port forwarding server entry.
Active	Select this check box to activate the port forwarding server entry.
Name	Enter a descriptive name for identifying purposes.

Table 55 VPN Branch Office — IP Policy - Port Forwarding Server

Label	Description
Start Port	Type a port number in this field. To forward only one port, type the port number again in the End Port field. To forward a series of ports, type the start port number here and the end port number in the End Port field.
End Port	Type a port number in this field. To forward only one port, type the port number in the Start Port field above and then type it again in this field. To forward a series of ports, type the last port number in a series that begins with the port number in the Start Port field above.
Server IP Address	Type your server IP address in this field.
Apply	Click this button to save these settings and return to the VPN Branch Office - IP Policy screen.
Reset	Click this button to begin configuring this screen afresh.
Cancel	Click this button to return to the VPN Branch Office - IP Policy screen without saving your changes.

IKE phases

There are two phases to every IKE (Internet Key Exchange) negotiation—phase 1 (Authentication) and phase 2 (Key Exchange). A phase 1 exchange establishes an IKE SA and the second one uses that SA to negotiate SAs for IPSec.

Figure 73 Two phases to set up the IPsec SA

In Phase 1 you must:

- Choose a negotiation mode.
- Authenticate the connection by entering a preshared key.
- Choose an encryption algorithm.
- Choose an authentication algorithm.
- Choose a Diffie-Hellman public-key cryptography key group (**DH1**, **DH2**, and **DH5**).
- Set the IKE SA lifetime. In this field you can determine how long an IKE SA will stay up before it times out. An IKE SA times out when the IKE SA lifetime period expires. If an IKE SA times out when an IPsec SA is already established, the IPsec SA stays connected.

In Phase 2 you must:

- Choose which protocol to use (**ESP** or **AH**) for the IKE key exchange.
- Choose an encryption algorithm.
- Choose an authentication algorithm
- Choose whether to enable Perfect Forward Secrecy (PFS) using Diffie-Hellman public-key cryptography—see [“Perfect Forward Secrecy \(PFS\)” on page 233](#). Select **None** (the default) to disable PFS.
- Choose **Tunnel** mode or **Transport** mode.

- Set the IPsec SA lifetime. In this field, you can determine how long the IPsec SA will stay up before it times out. The BCM50a Integrated Router automatically renegotiates the IPsec SA if there is traffic when the IPsec SA lifetime period expires. The BCM50a Integrated Router also automatically renegotiates the IPsec SA if both IPsec routers have keep alive enabled, even if there is no traffic. If an IPsec SA times out, the IPsec router must renegotiate the SA the next time someone attempts to send traffic.

Negotiation Mode

The phase 1 **Negotiation Mode** you select determines how the Security Association (SA) is established for each connection through IKE negotiations.

Main Mode ensures the highest level of security when the communicating parties are negotiating authentication (phase 1). It uses six messages in three round trips: SA negotiation, Diffie-Hellman exchange, and an exchange of nonces (a nonce is a random number). This mode features identity protection (your identity is not revealed in the negotiation).

Aggressive Mode is quicker than **Main Mode** because it eliminates several steps when the communicating parties are negotiating authentication (phase 1). However the trade-off is that faster speed limits its negotiating power and it also does not provide identity protection. It is useful in remote access situations where the address of the initiator is not known by the responder and both parties want to use preshared key authentication.

Preshared key

A preshared key identifies a communicating party during a phase 1 IKE negotiation. It is called preshared because you have to share it with another party before you can communicate with the party over a secure connection.

Diffie-Hellman (DH) Key Groups

Diffie-Hellman (DH) is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communications channel. Diffie-Hellman is used within IKE SA setup to establish session keys. 768-bit (Group 1 - **DH1**), 1 024-bit (Group 2 – **DH2**) and 1 536-bit (Group 5 - **DH5**) Diffie-Hellman groups are supported. Upon completion of the Diffie-Hellman exchange, the two peers have a shared secret, but the IKE SA is not authenticated. For authentication, use preshared keys.

Perfect Forward Secrecy (PFS)

Enabling PFS means that the key is transient. The key is thrown away and replaced by a brand new key using a new Diffie-Hellman exchange for each new IPsec SA setup. With PFS enabled, if one key is compromised, previous and subsequent keys are not compromised, because subsequent keys are not derived from previous keys. The (time consuming) Diffie-Hellman exchange is the trade-off for this extra security.

This can be unnecessary for data that does not require such security, so PFS is disabled (**None**) by default in the BCM50a Integrated Router. Disabling PFS means new authentication and encryption keys are derived from the same root secret (which can have security implications in the long run) but allows faster SA setup (by bypassing the Diffie-Hellman key exchange).

Configuring advanced Branch office setup

Select one of the VPN rules in the **VPN Summary** screen and click **Edit** to configure the rule. The basic IKE rule setup screen displays.

In the **VPN Branch Office Rule Setup** screen, click the **Advanced** button to display the **VPN Branch Office Advanced Rule Setup** screen.

Figure 74 VPN Branch Office advanced rule setup**VPN - Branch Office - Advanced**

Enable Replay Detection NO

Phase 1

Multiple Proposal

Negotiation Mode Main

Encryption Algorithm DES

Authentication Algorithm MD5

SA Life Time (Seconds) 28800

Key Group DH1

Phase 2

Multiple Proposal

Active Protocol ESP

Encryption Algorithm DES

Authentication Algorithm SHA1

SA Life Time (Seconds) 28800

Encapsulation Tunnel

Perfect Forward Secrecy(PFS) NONE

Apply Cancel

Table 56 describes the fields in Figure 74.

Table 56 VPN Branch Office Advanced Rule Setup

Label	Description
Enable Replay Detection	As a VPN setup is processing intensive, the system is vulnerable to Denial of Service (DoS) attacks. The IPsec receiver can detect and reject old or duplicate packets to protect against replay attacks. Enable replay detection by setting this field to YES .
Phase 1	A phase 1 exchange establishes an IKE SA (Security Association).

Table 56 VPN Branch Office Advanced Rule Setup

Label	Description
Multiple Proposal	<p>Select this check box to allow the BCM50a Integrated Router to use any of its phase 1 encryption and authentication algorithms when negotiating an IKE SA.</p> <p>Clear this check box to have the BCM50a Integrated Router use only the phase 1 encryption and authentication algorithms configured below when negotiating an IKE SA.</p>
Negotiation Mode	<p>Select Main for identity protection. Select Aggressive to allow more incoming connections from dynamic IP addresses to use separate passwords. The BCM50a Integrated Router's negotiation mode must be identical to that on the remote IPSec router. Multiple SAs connecting through a IPSec router must have the same negotiation mode.</p>
Encryption Algorithm	<p>Select DES, 3DES or AES from the drop-down list.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. This implementation of AES uses a 128-bit key. AES is faster than 3DES.</p>
Authentication Algorithm	<p>Select SHA1 or MD5 from the drop-down list. The BCM50a Integrated Router's authentication algorithm must be identical to the remote IPSec router. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate the source and integrity of packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select SHA-1 for maximum security.</p>
SA Life Time	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It can range from 60 to 3 000 000 seconds (almost 35 days). A short SA life time increases security by forcing the two IPSec routers to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Key Group	<p>You must choose a key group for phase 1 IKE setup.</p> <p>DH1 (default) refers to Diffie-Hellman Group 1, a 768-bit random number.</p> <p>DH2 refers to Diffie-Hellman Group 2, a 1 024-bit (1Kb) random number.</p> <p>DH5 refers to Diffie-Hellman Group 5, a 1 536-bit random number.</p>
Phase 2	<p>A phase 2 exchange uses the IKE SA established in phase 1 to negotiate the SA for IPSec.</p>

Table 56 VPN Branch Office Advanced Rule Setup

Label	Description
Multiple Proposal	<p>Select this check box to allow the BCM50a Integrated Router to use any of its phase 2 encryption and authentication algorithms when negotiating an IPSec SA.</p> <p>Clear this check box to have the BCM50a Integrated Router use only the phase 2 encryption and authentication algorithms when negotiating an IPSec SA.</p>
Active Protocol	<p>Select ESP or AH from the drop-down list. The BCM50a Integrated Router's IPSec Protocol must be identical to the remote IPSec router. The ESP (Encapsulation Security Payload) protocol (RFC 2406) provides encryption as well as the authentication offered by AH. If you select ESP here, you must select options from the Encryption Algorithm and Authentication Algorithm fields. The AH protocol (Authentication Header Protocol) (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation, but not for confidentiality, for which the ESP was designed. If you select AH here, you must select options from the Authentication Algorithm field.</p>
Encryption Algorithm	<p>Select DES, 3DES, AES or NULL from the drop-down list.</p> <p>When you use one of these encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code. The DES encryption algorithm uses a 56-bit key. Triple DES (3DES) is a variation on DES that uses a 168-bit key. As a result, 3DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput. You can select a 128-bit, 192-bit, or 256-bit key with this implementation of AES. AES is faster than 3DES.</p> <p>Select NULL to set up a tunnel without encryption. When you select NULL, you do not enter an encryption key.</p>
Authentication Algorithm	<p>Select SHA1 or MD5 from the drop-down list. MD5 (Message Digest 5) and SHA1 (Secure Hash Algorithm) are hash algorithms used to authenticate packet data. The SHA1 algorithm is generally considered stronger than MD5, but is slower. Select MD5 for minimal security and SHA-1 for maximum security.</p>
SA Life Time	<p>Define the length of time before an IKE SA automatically renegotiates in this field. It can range from 60 to 3 000 000 seconds (almost 35 days). A short SA life time increases security by forcing the two IPSec routers to update the encryption and authentication keys. However, every time the VPN tunnel renegotiates, all users accessing remote resources are temporarily disconnected.</p>
Encapsulation	<p>Select Tunnel mode or Transport mode from the drop-down list. The BCM50a Integrated Router's encapsulation mode must be identical to the remote IPSec router. Tunnel is compatible with NAT, Transport is not.</p>

Table 56 VPN Branch Office Advanced Rule Setup

Label	Description
Perfect Forward Secrecy (PFS)	Perfect Forward Secrecy (PFS) is disabled (None) by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not as secure. Choose from DH1 , DH2 , or DH5 to enable PFS. DH1 refers to Diffie-Hellman Group 1, a 768-bit random number. DH2 refers to Diffie-Hellman Group 2, a 1 024-bit (1Kb) random number (more secure, yet slower). DH5 refers to Diffie-Hellman Group 5, a 1 536-bit random number.
Apply	Click Apply to temporarily save the settings and return to the VPN - Branch Office Rule Setup screen. The advanced settings are saved to the BCM50a Integrated Router if you click Apply in the VPN - Branch Office Rule Setup screen.
Cancel	Click Cancel to return to the VPN Branch Office screen without saving your changes.

SA Monitor

In the WebGUI, click **VPN** and the **SA Monitor** tab. Use this screen to display and manage all of the active VPN connections (IPsec sessions).

A Security Association (SA) is the group of security settings related to a specific VPN tunnel. This screen displays active VPN connections. Use **Refresh** to display active VPN connections. This screen is read-only. [Table 57](#) describes the fields in this tab.



Note: When there is outbound traffic but no inbound traffic, the SA times out automatically after two minutes. A tunnel with no outbound or inbound traffic is idle and does not time out until the SA lifetime period expires. See the section [“Keep Alive” on page 204](#) about keep alive to have the BCM50a Integrated Router renegotiate an IPsec SA when the SA lifetime expires, even if there is no traffic.

Figure 75 VPN SA Monitor

VPN

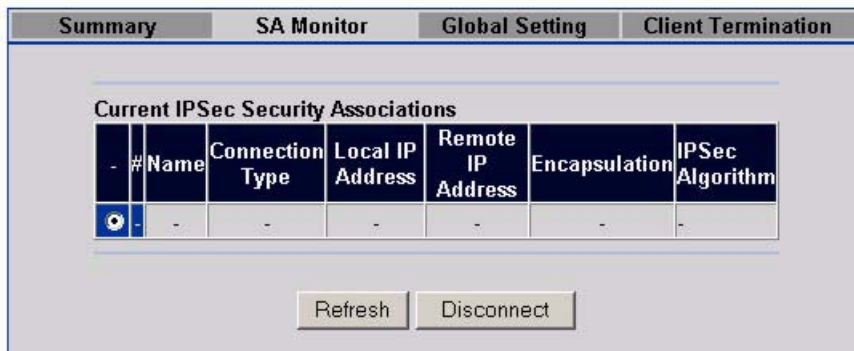


Table 57 describes the fields in Figure 75.

Table 57 VPN SA Monitor

Label	Description
#	This is the security association index number.
Name	This field displays the identification name for this VPN policy.
Connection Type	This field displays whether this is a connection to another IPSec router or to a Contivity VPN client.
Local IP Address	This field displays the IP address of the computer using the VPN IPSec feature of your BCM50a Integrated Router.
Remote IP Address	This field displays IP address (in a range) of computers on the remote network behind the remote IPSec router.
Encapsulation	This field displays Tunnel or Transport mode.
IPSec Algorithm	This field displays the security protocols used for an SA. Both AH and ESP increase BCM50a Integrated Router processing requirements and communications latency (delay).
Refresh	Click Refresh to display the current active VPN connections. This button is available when you have active VPN connections.
Disconnect	Select a security association index number that you want to disconnect and then click Disconnect . This button is available when you have active VPN connections.
Next Page (if applicable)	Click Next Page to view more items in the summary (if you have a summary list that exceeds this page)

Global settings

In the WebGUI, click **VPN** on the navigation panel, then click the **Global Setting** tab.

Figure 76 VPN Global Setting
VPN

Table 58 describes the fields in Figure 76.

Table 58 VPN Global Setting

Label	Description
Windows Networking (NetBIOS over TCP/IP)	NetBIOS (Network Basic Input/Output System) are TCP or UDP packets that enable a computer to connect to and communicate with a LAN. It is sometimes necessary to allow NetBIOS packets to pass through VPN tunnels in order to allow local computers to find computers on the remote network and vice versa.
Allow Through IPsec Tunnel	Select this check box to send NetBIOS packets through the VPN connection.
Exclusive Use Mode for Client Tunnel	Select this check box to permit only the computer with the MAC address that you specify to set up a VPN connection to the remote IPsec router.

Table 58 VPN Global Setting

Label	Description
MAC Address Allowed	Enter the MAC address of the computer you want to allow to use the VPN tunnel.
Contivity Client Fail-Over	The Contivity Client fail-over feature allows a Contivity client to establish a VPN connection to a backup IPsec router when the default remote IPsec router (specified in the Destination field) is not accessible. The VPN fail-over feature must also be set up in the remote IPsec router.
First Gateway Second Gateway Third Gateway	These read-only fields display the IP addresses of the backup IPsec routers. The BCM50a Integrated Router automatically gets this information from the default remote IPsec router. After the remote IPsec router is unreachable or fails to respond to IKE negotiation, the BCM50a Integrated Router tries to establish a VPN connection to a backup IPsec router.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

VPN Client Termination

Use these screens to configure the BCM50a Integrated Router for VPN connections from computers using Nortel Contivity VPN Client software. In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the screen illustrated in [Figure 77](#). This screen sets the general settings for use with all of the Contivity VPN client tunnels.

Figure 77 VPN Client Termination
VPN

Summary	SA Monitor	Global Setting	Client Termination
<input type="checkbox"/> Enable Client Termination			
<hr/>			
Authentication			
<input type="checkbox"/> Local User Database (Configure Local User Database)			
<input type="checkbox"/> User Name and Password/Pre-Shared Key			
<input type="checkbox"/> RADIUS Server (Configure RADIUS Server)			
Group ID and Password			
Group ID		<input type="text"/>	
Group Password		<input type="text"/>	
Retype to Confirm		<input type="text"/>	
Authentication Type			
<input type="checkbox"/> User Name and Password			
<hr/>			
Encryption			
<input type="checkbox"/> ESP - 128-bit AES with SHA1 Integrity			
<input type="checkbox"/> ESP - Triple DES with SHA1 Integrity			
<input type="checkbox"/> ESP - Triple DES with MD5 Integrity			
<input type="checkbox"/> ESP - 56-bit DES with SHA1 Integrity			
<input type="checkbox"/> ESP - 56-bit DES with MD5 Integrity			
<input type="checkbox"/> AH - Authentication Only (HMAC-SHA1)			
<input type="checkbox"/> AH - Authentication Only (HMAC-MD5)			
<hr/>			
IKE Encryption and Diffie-Hellman Group			
<input type="checkbox"/> 56-bit DES with Group 1 (768-bit prime)			
<input type="checkbox"/> Triple DES with Group 2 (1024-bit prime)			
<input type="checkbox"/> 128-bit AES with Group 5 (1536-bit prime)			
<hr/>			
Assignment of Client IP			
<input type="checkbox"/> Use Static Addresses (Configured in eWIC>>AUTH SERVER>>Local User Database)			
IP Address Pool		<input type="text" value="(None selected)"/> (Configure IP Address Pool)	
<hr/>			
<input type="checkbox"/> Enable Perfect Forward Secrecy			
<hr/>			
Rekey Timeout		<input type="text" value="08:00:00"/> (Range 00:02:00 - 23:59:59)	
Rekey Data Count		<input type="text" value="0"/> (Kbytes, minimum is 5 Kbytes, and 0 means disable)	
<hr/>			
<input type="button" value="Advanced"/>		<input type="button" value="Apply"/>	
<input type="button" value="Reset"/>			

Table 59 describes the fields in Figure 77.

Table 59 VPN Client Termination

Label	Description
Enable Client Termination	Turn on the client termination feature if you want the BCM50a Integrated Router to support VPN connections from computers using Contivity VPN Client software.
Local User Database	Select this option to have the BCM50a Integrated Router use its internal list of users to authenticate the Contivity VPN clients. Click Configure Local User Database to edit the list of users and their usernames and passwords.
User Name and Password/ Pre-Shared Key	Select this option to have the BCM50a Integrated Router use the Contivity VPN clients' usernames and passwords as a preshared key to identify them during phase 1 IKE negotiations.
RADIUS Server	Select this option to have the BCM50a Integrated Router use an external RADIUS server to identify the Contivity VPN clients during phase 1 IKE negotiations. Click Configure RADIUS Server to specify the associated external RADIUS server.
Group ID	The Contivity VPN clients send the group ID and group password to the BCM50a Integrated Router for or initial authentication. After a successful initial authentication, the associated external RADIUS server uses the username and password from the Contivity VPN client to authenticate the Contivity VPN client. Enter a group ID of up to 31 ASCII characters.
Group Password Retype to Confirm	Enter a group password of up to 31 ASCII characters. Enter it a second time to make sure you have entered it correctly.
Authentication Type	Select User Name and Password to have the external RADIUS server use the Contivity VPN clients' usernames and passwords to authenticate them during phase 1 IKE negotiations.

Table 59 VPN Client Termination

Label	Description
Encryption	<p>Select the combinations of protocol and encryption and authentication algorithms that the BCM50a Integrated Router is to use for the phase 2 VPN connections (VPN tunnels) with Contivity VPN clients.</p> <p>The ESP (Encapsulation Security Payload) protocol (RFC 2406) uses encryption as well as the services offered by AH.</p> <p>The AH (Authentication Header Protocol) protocol (RFC 2402) was designed for integrity, authentication, sequence integrity (replay resistance), and nonrepudiation but not for confidentiality, for which the ESP was designed. It does not use encryption.</p> <p>When you use one of the encryption algorithms for data communications, both the sending device and the receiving device must use the same secret key, which can be used to encrypt and decrypt the message or to generate and verify a message authentication code.</p> <p>The DES encryption algorithm uses a 56-bit key.</p> <p>Triple DES is a variation on DES that uses a 168-bit key. Triple DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.</p> <p>You can select a 128-bit key implementation of AES. AES is faster than 3DES.</p> <p>SHA1 (Secure Hash Algorithm) and MD5 (Message Digest 5) are hash algorithms used to authenticate packet data. SHA1 algorithm is generally considered stronger than MD5, but is slower.</p>
IKE Encryption and Diffie-Hellman Group	<p>Select the combinations of encryption algorithm and Diffie-Hellman key group that the BCM50a Integrated Router is to use for phase 1 IKE setup with Contivity VPN clients.</p> <p>The DES encryption algorithm uses a 56-bit key.</p> <p>Triple DES is a variation on DES that uses a 168-bit key. Triple DES is more secure than DES. It also requires more processing power, resulting in increased latency and decreased throughput.</p> <p>You can select a 128-bit key implementation of AES. AES is faster than 3DES.</p> <p>Diffie-Hellman (DH) is a public-key cryptography protocol that is used within IKE SA setup to establish session keys. The larger the Diffie-Hellman Group, the higher the security.</p> <p>Diffie-Hellman Group 1 uses a 768-bit random number.</p> <p>Diffie-Hellman Group 2 uses a 1 024-bit (1Kb) random number.</p> <p>Diffie-Hellman Group 5 uses a 1 536-bit random number.</p>
Assignment of Client IP	<p>Select Use Static Addresses if the Contivity VPN clients are using static IP addresses. You must specify these in the remote user profiles.</p>

Table 59 VPN Client Termination

Label	Description
IP Address Pool	Have the BCM50a Integrated Router assign IP addresses to the Contivity VPN clients from a pool of IP address that you define. Select the pool to use. Click Configure IP Address Pool to define the ranges of IP addresses that you can select from.
Enable Perfect Forward Secrecy	Perfect Forward Secrecy (PFS) is disabled by default in phase 2 IPsec SA setup. This allows faster IPsec setup, but is not so secure. Turn on PFS to use the Diffie-Hellman exchange to create a new key for each IPsec SA setup.
Rekey Timeout	Set the allowed lifetime for an individual key used for data encryption before negotiating a new key. A setting of 00:00:00 disables the rekey timeout.
Rekey Data Count	Set how much data can be transmitted through the VPN tunnel before negotiating a new key. A setting of 0 disables the rekey data count.
Advanced	Click Advanced to configure detailed VPN client tunnel termination settings.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

VPN Client Termination IP pool summary

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Configure IP Address Pool** link to open the screen in [Figure 78](#). Use this screen to manage the list of ranges of IP addresses to assign to the Contivity VPN clients.

Figure 78 VPN Client Termination IP pool summary

IP Pool

[Return to VPN->Client Termination Page](#)

IP Pool Summary

#	Name	Active	Starting Address	Subnet mask	Pool size
<input checked="" type="radio"/> 1	-	-	-	-	-
<input type="radio"/> 2	-	-	-	-	-
<input type="radio"/> 3	-	-	-	-	-

Table 60 describes the fields in Figure 78.

Table 60 VPN Client Termination IP pool summary

Label	Description
Return to ->Client Termination Page	Click this link to return to the screen used to configure the general settings for use with all of the Contivity VPN Client tunnels.
#	These numbers are an incremental value. The position of the IP address pool in the list does not matter.
Name	This field displays the label that you configure for the IP address pool.
Active	This field displays whether or not the IP address pool is turned on.
Starting Address	This field displays the first IP address in the IP address pool.
Subnet mask	This field displays the subnet mask that you specified to define the IP address pool.
Pool size	This field displays how many IP addresses you set the BCM50a Integrated Router to give out from the pool created by the starting address and subnet mask.
Edit	Click the radio button next to an IP address pool entry and click Edit to open the screen where you can configure the entry.
Delete	Click the radio button next to an IP address pool entry and click Delete to remove it.

VPN Client Termination IP pool edit

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Configure IP Address Pool** link to open the **VPN Client Termination IP Pool Summary** screen. Click the radio button next to an IP address pool entry and click **Edit** to open the following screen where you can configure the entry. Use this screen to configure a range of IP addresses to assign to the Contivity VPN clients.

Figure 79 VPN Client Termination IP pool edit
IP Pool Edit

The screenshot shows a web form for editing an IP pool. It features a checkbox labeled 'Active' which is currently unchecked. Below this are four input fields: 'IP Pool Name' (an empty text box), 'Starting Address' (a text box containing '0.0.0.0'), 'Subnet Mask' (a text box containing '0.0.0.0'), and 'Pool Size' (a text box containing '0'). At the bottom of the form are two buttons: 'Apply' and 'Cancel'.

[Table 61](#) describes the fields in [Figure 79](#).

Table 61 VPN Client Termination IP pool edit

Label	Description
Active	Turn on the IP pool if you want the BCM50a Integrated Router to use it in assigning IP addresses to the Contivity VPN clients.
IP Pool Name	Specify a label for the IP address pool.
Starting Address	Specify the first of the IP addresses in the IP address pool.
Subnet Mask	Specify a subnet mask to define the IP address pool.

Table 61 VPN Client Termination IP pool edit

Label	Description
Pool Size	Specify how many IP addresses the BCM50a Integrated Router is to give out from the pool created by the starting address and subnet mask. 256 is the maximum.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to return to the IP Pool Summary screen without saving your changes.

VPN Client Termination advanced

In the WebGUI, click **VPN** on the navigation panel and the **Client Termination** tab to open the **VPN Client Termination** screen. Then click the **Advanced** button to open the following screen. Use this screen to configure detailed settings for use with all of the Contivity VPN Client tunnels.

Figure 80 VPN Client Termination advanced

VPN - Client Termination - Advanced

NAT Traversal

Enabled

Disable Client IKE Source Port Switching

UDP Port

Fail-Over

First Gateway

Second Gateway

Third Gateway

Client Failover Tuning (Keepalive)

Enable Failover Tuning

Interval (Range 00:00:10 - 23:59:59)

Max Number of Retransmissions

Accept ISAKMP Initial Contact Payload

Idle Timeout (00:00:00 means no idle timeout.)

Domain Name

Primary DNS

Secondary DNS

Primary WINS

Secondary WINS

Client Minimum Version Requirement

Action

Message

Display Banner

Banner

Allow Password Storage on Client

Password Management

Alpha-Numeric Password Required

Maximum Password Age (Range 0 - 180 days, 0 means never expire)

Minimum Password Length (Range 3 - 16)

Table 62 describes the fields in Figure 80.

Table 62 VPN Client Termination advanced

Label	Description
NAT Traversal	Select Enabled in order to Use NAT traversal when there is a NAT router between the BCM50a Integrated Router and the Contivity VPN clients. The Contivity VPN clients must also have NAT traversal enabled. You also need to specify the UDP port that is used for the VPN traffic.
Disable Client IKE Source Port Switching	With client IKE source port switching, if the BCM50a Integrated Router detects that traffic is going through NAT, it asks the client to use a UDP port higher than the standard of 500 (such as port 1023). Turn off client source port switching if the NAT router requires IKE to use port 500.
UDP Port	Specifies the UDP port to use for the VPN traffic. In order for a Contivity VPN client behind a NAT router to receive an initiating IPSec packet, set the NAT router to forward this UDP port to the VPN Contivity client behind the NAT router.
Fail-Over	The fail-over feature allows a Contivity VPN client to establish a VPN connection to a backup IPSec router when the BCM50a Integrated Router is not accessible. The VPN fail-over feature must also be set up in the Contivity VPN clients.
First Gateway Second Gateway Third Gateway	Enter the IP addresses of the backup IPSec routers. When the BCM50a Integrated Router is unreachable or fails to respond to IKE negotiation, the Contivity VPN client tries to establish a VPN connection to a backup IPSec router.
Enable Failover Tuning	Enable the VPN fail-over feature to have the BCM50a Integrated Router keep sending keep-alive packets to the Contivity VPN clients in order to check the connection and keep the connection alive.
Interval	Specifies how long the VPN Contivity client waits between VPN connection checks.
Max Number of Retransmissions	Specifies the maximum number of retransmissions (0~255) of the keep-alive packets. This is how many times the VPN Contivity client can resend the keep-alive packet to the BCM50a Integrated Router to check the connection before attempting to use the first fail-over gateway.

Table 62 VPN Client Termination advanced

Label	Description
Accept ISAKMP Initial Contact Payload	The BCM50a Integrated Router can accept the INITIAL-CONTACT status messages to inform it that the Contivity VPN client is establishing a first SA. The BCM50a Integrated Router then deletes the existing SAs because it assumes that the sending Contivity VPN client has restarted and no longer has access to any of the existing SAs.
Idle Timeout	Specifies how long the Contivity VPN client connection can go without traffic before the BCM50a Integrated Router terminates the session. The BCM50a Integrated Router does not time out idle connections when this field is set to 00:00:00.
Domain Name	Specifies the domain name that is used while the VPN tunnel is connected.
Primary DNS Secondary DNS	Specifies the first and second DNS server IP addresses to assign to the Contivity VPN clients.
Primary WINS Secondary WINS	Specifies the first and second WINS server IP addresses to assign to the Contivity VPN clients.
Client Minimum Version Requirement	Selects the lowest version of Contivity VPN client software that you require the clients to use.
Action	<p>Specifies what the BCM50a Integrated Router does when it detects a noncompliant version of Contivity VPN client software.</p> <p>Select None to allow the VPN tunnel without displaying any messages to tell the user where to download the required version of the Contivity VPN client software.</p> <p>Select Send Message to allow the VPN tunnel, but display a message to tell the user where to download the required version of the Contivity VPN client software.</p> <p>Select Send Message and Force Logoff to disconnect the VPN tunnel and display a message to tell the user where to download the required version of the Contivity VPN client software.</p>
Message	Enter a message that tells where to download the required version of the Contivity VPN client software. Use from 1 to 255 ASCII characters.
Display Banner	Select Enabled to have the BCM50a Integrated Router show the Contivity VPN client users a message across the top of the screen after they log on.
Banner	Enter the message (such as the name of your company) that you want to show at the top of the Contivity VPN client users' screens after they log on. Use from 1 to 255 ASCII characters.
Allow Password Storage on Client	Use this to let the Contivity VPN clients save their logon passwords instead of always having to enter them manually.

Table 62 VPN Client Termination advanced

Label	Description
Password Management	You can have the BCM50a Integrated Router use some password requirements to enhance security.
Alpha-Numeric Password Required	Use this to have the BCM50a Integrated Router require the Contivity VPN client passwords to have both numbers and letters.
Maximum Password Age	Enter the maximum number of days that a Contivity VPN client can use a password before it has to be changed. 0 means that a password never expires.
Minimum Password Length	Enter the minimum number of characters that can be used for a Contivity VPN client password.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 14

Certificates

This chapter gives background information about public-key certificates and explains how to use them.

Certificates overview

The BCM50a Integrated Router can use certificates (also called digital IDs) to authenticate users. Certificates are based on public-private key pairs. A certificate contains the identity and public key of the certificate owner. Certificates provide a way to exchange public keys for use in authentication.

A Certification Authority (CA) issues certificates and guarantees the identity of each certificate owner. There are commercial certification authorities like CyberTrust or VeriSign and government certification authorities. You can use the BCM50a Integrated Router to generate certification requests that contain identifying information and public keys and then send the certification requests to a certification authority.

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

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

The BCM50a Integrated Router uses certificates based on public-key cryptology to authenticate users attempting to establish a connection, not to encrypt the data that is sent after establishing a connection. The method used to secure the data that is sent through an established connection depends on the type of connection. For example, a VPN tunnel can use the triple DES encryption algorithm.

The certification authority uses its private key to sign certificates. Anyone can use the certification authority's public key to verify the certificates.

A certification path is the hierarchy of certification authority certificates that validate a certificate. The BCM50a Integrated Router does not trust a certificate if any certificate on its path has expired or been revoked.

Certification authorities maintain directory servers with databases of valid and revoked certificates. A directory of certificates that have been revoked before the scheduled expiration is called a CRL (Certificate Revocation List). The BCM50a Integrated Router can check a peer's certificate against a list of revoked certificates on a directory server. The framework of servers, software, procedures, and policies that handles keys is called PKI (public-key infrastructure).

Advantages of certificates

Certificates offer the following benefits:

- The BCM50a Integrated Router only has to store the certificates of the certification authorities that you decide to trust, no matter how many devices you need to authenticate.
- Key distribution is simple and very secure because you can freely distribute public keys and you never need to transmit private keys.

Self-signed certificates

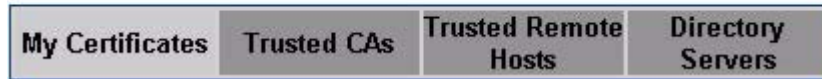
Until public-key infrastructure becomes more mature, it is not available in some areas. You can have the BCM50a Integrated Router act as a certification authority and sign its own certificates.

Configuration summary

This section summarizes how to manage certificates on the BCM50a Integrated Router.

Figure 81 Certificate configuration overview

CERTIFICATES



Use the **My Certificate** screens to generate and export self-signed certificates or certification requests and import the CA-signed certificates.

Use the **Trusted CA** screens to save CA certificates to the BCM50a Integrated Router.

Use the **Trusted Remote Hosts** screens to import self-signed certificates.

Use the **Directory Servers** screen to configure a list of addresses of directory servers (that contain lists of valid and revoked certificates).

My Certificates

Click **CERTIFICATES**, **My Certificates** to open summary list of certificates and certification requests stored on the BCM50a Integrated Router. Certificates display in black and certification requests display in gray, as shown in [Figure 82](#).

Figure 82 My Certificates

My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers

PKI Storage Space in Use

0% 12% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to Business Secure Router models. Click Replace to create a certificate using your Business Secure Router's MAC address that will be specific to this device.

My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=Business Secure Router Factory Default Certificate	CN=Business Secure Router Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	

Table 63 describes the labels in Figure 82.

Table 63 My Certificates

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the PKI storage space that is currently in use. The bar turns from green to red when the maximum is being approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
Replace	This button displays when the BCM50a Integrated Router has the factory default certificate. The factory default certificate is common to all BCM50a Integrated Routers that use certificates. Nortel recommends that you use this button to replace the factory default certificate with one that uses your BCM50a Integrated Router's MAC address.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate. Nortel recommends that you give each certificate a unique name.
Type	This field displays what kind of certificate this is. REQ represents a certification request and is not yet a valid certificate. Send a certification request to a certification authority, which then issues a certificate. Use the My Certificate Import screen to import the certificate and replace the request. SELF represents a self-signed certificate. *SELF represents the default self-signed certificate, which the BCM50a Integrated Router uses to sign imported trusted remote host certificates. CERT represents a certificate issued by a certification authority.
Subject	This field displays identifying information about the owner of the certificate, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). Nortel recommends that each certificate have unique subject information.
Issuer	This field displays identifying information about the certification authority that issued the certificate, such as a common name, organizational unit or department, organization, or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.

Table 63 My Certificates

Label	Description
Modify	<p>Click the details icon to open a screen with an in-depth list of information about the certificate.</p> <p>Click the delete icon to remove the certificate. A window displays, asking you to confirm that you want to delete the certificate.</p> <p>You cannot delete a certificate that one or more features are configured to use.</p> <p>Do the following to delete a certificate that shows *SELF in the Type field.</p> <ol style="list-style-type: none"> 1. Make sure that no other features, such as HTTPS, VPN, or SSH are configured to use the *SELF certificate. 2. Click the details icon next to another self-signed certificate (see the description on the Create button if you need to create a self-signed certificate). 3. Select the Default self-signed certificate which signs the imported remote host certificates check box. 4. Click Apply to save the changes and return to the My Certificates screen. 5. The certificate that originally showed *SELF displays SELF and you can delete it now. <p>Note that subsequent certificates move up by one when you take this action.</p>
Import	<p>Click Import to open a screen where you can save the certificate that you have enrolled from a certification authority from your computer to the BCM50a Integrated Router.</p>
Create	<p>Click Create to go to the screen where you can have the BCM50a Integrated Router generate a certificate or a certification request.</p>
Refresh	<p>Click Refresh to display the current validity status of the certificates.</p>

Certificate file formats

The certification authority certificate that you want to import has to be in one of these file formats:

- **Binary X.509:** This is an ITU-T recommendation that defines the formats for X.509 certificates.
- **PEM (Base-64) encoded X.509:** This Privacy Enhanced Mail format uses 64 ASCII characters to convert a binary X.509 certificate into a printable form.

- **Binary PKCS#7:** This is a standard that defines the general syntax for data (including digital signatures) that can be encrypted. The BCM50a Integrated Router currently allows the importation of a PKCS#7 file that contains a single certificate.
- **PEM (Base-64) encoded PKCS#7:** This Privacy Enhanced Mail (PEM) format uses 64 ASCII characters to convert a binary PKCS#7 certificate into a printable form.

Importing a certificate

Click **CERTIFICATES**, **My Certificates** and then **Import** to open the **My Certificate Import** screen. Follow the instructions on the screen shown in [Figure 83](#) to save an existing certificate to the BCM50a Integrated Router.



Note: 1. You can only import a certificate that matches a corresponding certification request generated by the BCM50a Integrated Router.

Note: 2. The certificate you import replaces the corresponding request in the **My Certificates** screen.

Note: 3. You must remove any spaces from the certificate filename before you can import it.

Figure 83 My Certificate Import
CERTIFICATES - MY CERTIFICATE - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

For my certificate importation to be successful, a certification request corresponding to the imported certificate must already exist on BSR50e. After the importation, the certification request will automatically be deleted.

File Path:

Table 64 describes the labels in Figure 83.

Table 64 My Certificate Import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate to the BCM50a Integrated Router.
Cancel	Click Cancel to quit and return to the My Certificates screen.

Creating a certificate

Click **CERTIFICATES**, **My Certificates** and then **Create** to open the **My Certificate Create** screen. Use this screen to have the BCM50a Integrated Router create a self-signed certificate, enroll a certificate with a certification authority, or generate a certification request. For more information, see [Figure 84](#).

Figure 84 My Certificate create
CERTIFICATES - MY CERTIFICATE - CREATE

Certificate Name

Subject Information

Common Name

- Host IP Address
- Host Domain Name
- E-Mail

Organizational Unit

Organization

Country

Key Length bits

Enrollment Options

- Create a self-signed certificate
- Create a certification request and save it locally for later manual enrollment
- Create a certification request and enroll for a certificate immediately online

Enrollment Protocol

CA Server Address

CA Certificate (See [Trusted CAs](#))

Request Authentication

Key

Table 65 describes the labels in the Figure 84.

Table 65 My Certificate create

Label	Description
Certificate Name	Type up to 31 ASCII characters (not including spaces) to identify this certificate.
Subject Information	Use these fields to record information that identifies the owner of the certificate. You do not have to fill in every field, although the Common Name is mandatory. The certification authority can add fields (such as a serial number) to the subject information when it issues a certificate. Nortel recommends that each certificate have unique subject information.
Common Name	Select a radio button to identify the owner of the certificate by IP address, domain name, or e-mail address. Type the IP address (in dotted decimal notation), domain name, or e-mail address in the field provided. The domain name or e-mail address can be up to 31 ASCII characters. The domain name or e-mail address is for identification purposes only and can be any string.
Organizational Unit	Type up to 127 characters to identify the organizational unit or department to which the certificate owner belongs. You can use any character, including spaces, but the BCM50a Integrated Router drops trailing spaces.
Organization	Type up to 127 characters to identify the company or group to which the certificate owner belongs. You can use any character, including spaces, but the BCM50a Integrated Router drops trailing spaces.
Country	Type up to 127 characters to identify the nation where the certificate owner is located. You can use any character, including spaces, but the BCM50a Integrated Router drops trailing spaces.
Key Length	Select a number from the drop-down list to determine how many bits are used for the key (512 to 2 048). The longer the key, the more secure it is. A longer key also uses more PKI storage space.
Enrollment Options	These radio buttons deal with how and when the certificate is to be generated.
Create a self-signed certificate	Select Create a self-signed certificate to have the BCM50a Integrated Router generate the certificate and act as the Certification Authority (CA) itself. This way you do not need to apply to a certification authority for certificates.

Table 65 My Certificate create

Label	Description
Create a certification request and save it locally for later manual enrollment	<p>Select Create a certification request and save it locally for later manual enrollment to have the BCM50a Integrated Router generate and store a request for a certificate. Use the My Certificate Details screen to view the certification request and copy it to send to the certification authority.</p> <p>Copy the certification request from the My Certificate Details screen (see “My Certificate details” on page 265) and then send it to the certification authority.</p>
Create a certification request and enroll for a certificate immediately online	<p>Select Create a certification request and enroll for a certificate immediately online to have the BCM50a Integrated Router generate a request for a certificate and apply to a certification authority for a certificate.</p> <p>You must have the certification authority certificate already imported in the Trusted CAs screen.</p> <p>When you select this option, you must select the certification authority enrollment protocol and the certification authority certificate from the drop-down list and enter the certification authority server address (or URL). You also need to fill in the Reference Number and Key if the certification authority requires it.</p>
Enrollment Protocol	<p>Select the certification authority enrollment protocol from the drop-down list.</p> <p>Simple Certificate Enrollment Protocol (SCEP) is a TCP-based enrollment protocol that was developed by VeriSign and Cisco.</p> <p>Certificate Management Protocol (CMP) is a TCP-based enrollment protocol that was developed by the Public Key Infrastructure X.509 working group of the Internet Engineering Task Force (IETF) and is specified in RFC 2510.</p>
CA Server Address	Enter the IP address (or URL) of the certification authority server.
CA Certificate	<p>Select the certification authority certificate from the CA Certificate drop-down list.</p> <p>You must have the certification authority certificate already imported in the Trusted CAs screen. Click Trusted CAs to go to the Trusted CAs screen where you can view (and manage) the BCM50a Integrated Router's list of certificates of trusted certification authorities.</p>
Request Authentication	When you select Create a certification request and enroll for a certificate immediately online , the certification authority can require you to include a reference number and key to identify you when you send a certification request. Fill in both the Reference Number and the Key fields if your certification authority uses CMP enrollment protocol. Just fill in the Key field if your certification authority uses the SCEP enrollment protocol.
Key	Type the key that the certification authority gave you.

Table 65 My Certificate create

Label	Description
Apply	Click Apply to begin certificate or certification request generation.
Cancel	Click Cancel to quit and return to the My Certificates screen.

After you click **Apply** in the **My Certificate Create** screen, you see a screen that tells you the BCM50a Integrated Router is generating the self-signed certificate or certification request.

After the BCM50a Integrated Router successfully enrolls a certificate or generates a certification request or a self-signed certificate, you see a screen with a **Return** button that takes you back to the **My Certificates** screen.

If you configured the **My Certificate Create** screen to have the BCM50a Integrated Router enroll a certificate and the certificate enrollment is not successful, you see a screen with a **Return** button that takes you back to the **My Certificate Create** screen. Click **Return** and check your information in the **My Certificate Create** screen. Make sure that the certification authority information is correct and that your Internet connection is working properly if you want the BCM50a Integrated Router to enroll a certificate online.

My Certificate details

Click **CERTIFICATES**, and then **My Certificates** to open the **My Certificates** screen (see [Figure 82](#)). Click the details icon to open the **My Certificate Details** screen. You can use this screen (see [Figure 85](#)) to view in-depth certificate information and change the name of the certificate. In the case of a self-signed certificate, you can set it to be the one that the BCM50a Integrated Router uses to sign the trusted remote host certificates that you import to the BCM50a Integrated Router.

Table 66 describes the labels in Figure 85.

Table 66 My Certificate details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this certificate. You can use any character (not including spaces).
Property Default self-signed certificate that signs the imported remote host certificates.	<p>Select this check box to have the BCM50a Integrated Router use this certificate to sign the trusted remote host certificates that you import to the BCM50a Integrated Router. This check box is only available with self-signed certificates.</p> <p>If this check box is already selected, you cannot clear it in this screen, you must select this check box in the details screen of another self-signed certificate. This automatically clears the check box in the details screen of the certificate that was previously set to sign the imported trusted remote host certificates.</p>
Certification Path	<p>Click the Refresh button to have this read-only text box display the hierarchy of certification authorities that validate the certificate (and the certificate itself).</p> <p>If the issuing certification authority is one that you have imported as a trusted certification authority, it can be the only certification authority in the list (along with the certificate itself). If the certificate is a self-signed certificate, the certificate itself is the only one in the list. The BCM50a Integrated Router does not trust the certificate and displays “Not trusted” in this field if any certificate on the path has expired or been revoked.</p>
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the owner of the certificate signed the certificate (not a certification authority). “X.509” means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the identification number of the certificate given by the certification authority or generated by the BCM50a Integrated Router.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O) or Country (C).

Table 66 My Certificate details

Label	Description
Issuer	This field displays identifying information about the certification authority that issued the certificate, such as Common Name, Organizational Unit, Organization or Country. With self-signed certificates, this is the same as the Subject Name field.
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. The BCM50a Integrated Router uses rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Some certification authorities can use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the key pair (the BCM50a Integrated Router uses RSA encryption) of the certificate and the length of the key set in bits (1 024 bits for example).
Subject Alternative Name	This field displays the certificate owner's IP address (IP), domain name (DNS) or e-mail address (EMAIL).
Key Usage	This field displays for what functions the key of the certificate can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certification path of the certificate.
MD5 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the MD5 algorithm.
SHA1 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the SHA1 algorithm.

Table 66 My Certificate details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste a certification request into a certification authority Web page, an e-mail that you send to the certification authority or a text editor and save the file on a management computer for later manual enrollment. You can copy and paste a certificate into an e-mail to send to friends or colleagues or you can copy and paste a certificate into a text editor and save the file on a management computer for later distribution (through floppy disk, for example).
Export	Click this button and then Save in the File Download screen. The Save As screen displays, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes to the BCM50a Integrated Router. You can only change the name, except in the case of a self-signed certificate, which you can also set to be the default self-signed certificate that signs the imported trusted remote host certificates.
Cancel	Click Cancel to quit and return to the My Certificates screen.

Trusted CAs

Click **CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen, shown in [Figure 86](#). This screen displays a summary list of certificates of the certification authorities that you have set the BCM50a Integrated Router to accept as trusted. The BCM50a Integrated Router accepts any valid certificate signed by a certification authority on this list as being trustworthy; thus you do not need to import any certificate that is signed by one of these certification authorities.

Figure 86 Trusted CAs
CERTIFICATES

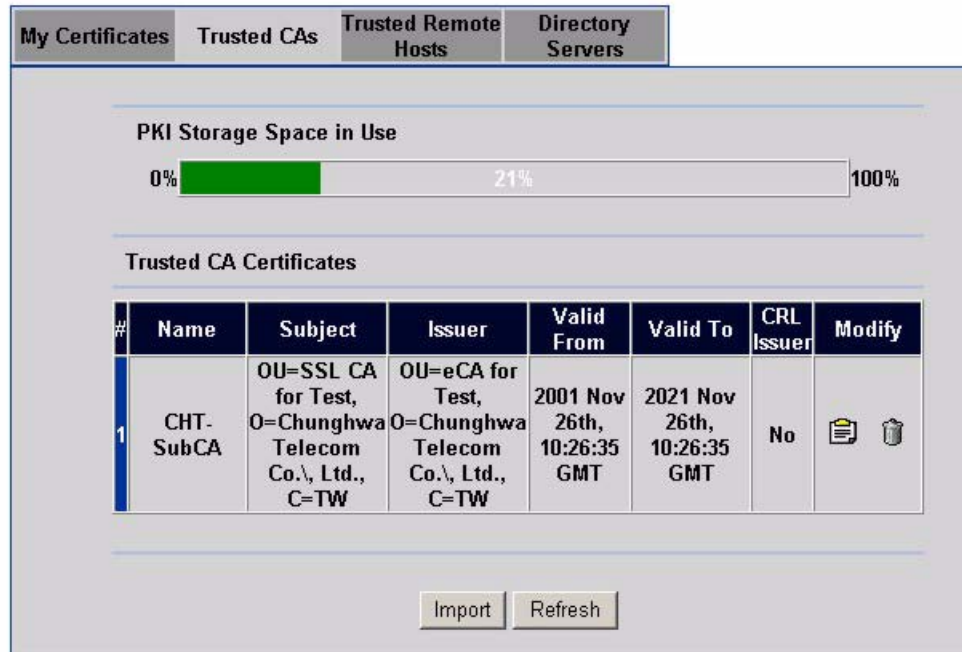


Table 67 describes the labels in Figure 86.

Table 67 Trusted CAs

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the owner of the, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) or C (Country). Nortel recommends that each certificate have unique subject information.

Table 67 Trusted CAs

Label	Description
Issuer	This field displays identifying information about the certification authority that issued the certificate, such as a common name, organizational unit or department, organization, or company and country. With self-signed certificates, this is the same information as in the Subject field.
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
CRL Issuer	This field displays Yes if the certification authority issues Certificate Revocation Lists for the certificates that it has issued and you have selected the Issues certificate revocation lists (CRL) check box in the certificate details screen to have the BCM50a Integrated Router check the CRL before trusting any certificates issued by the certification authority. Otherwise the field displays "No".
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window appears asking you to confirm that you want to delete the certificates. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Import	Click Import to open a screen where you can save the certificate of a certification authority that you trust, from your computer to the BCM50a Integrated Router.
Refresh	Click this button to display the current validity status of the certificates.

Importing a Trusted CA certificate

Click **CERTIFICATES**, **Trusted CAs** to open the **Trusted CAs** screen and then click **Import** to open the **Trusted CA Import** screen, shown in [Figure 87](#). Follow the instructions in this screen to save a trusted certification authority certificate to the BCM50a Integrated Router.



Note: You must remove any spaces from the certificate filename before you can import the certificate.

Figure 87 Trusted CA import

CERTIFICATES - TRUSTED CA - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

[Table 68](#) describes the labels in [Figure 87](#).

Table 68 Trusted CA import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.

Table 68 Trusted CA import

Label	Description
Apply	Click Apply to save the certificate on the BCM50a Integrated Router.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

Trusted CA Certificate details

Click **CERTIFICATES, Trusted CAs** to open the **Trusted CAs** screen. Click the details icon to open the **Trusted CA Details** screen, shown in [Figure 88](#). Use this screen to view in-depth information about the certification authority certificate, change the certificate name, and set whether or not you want the BCM50a Integrated Router to check a certification authority list of revoked certificates before trusting a certificate issued by the certification authority.

Figure 88 Trusted CA details
 CERTIFICATES - TRUSTED CA - DETAILS

Name

Property
 Check incoming certificates issued by this CA against a CRL

Certification Path

Searching...

Certificate Information

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	88735430130868711293164270205497631363
Subject	OU=SSL CA for Test, O=Chunghwa Telecom Co., Ltd., C=TW
Issuer	OU=eCA for Test, O=Chunghwa Telecom Co., Ltd., C=TW
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2001 Nov 26th, 10:26:35 GMT
Valid To	2021 Nov 26th, 10:26:35 GMT
Key Algorithm	rsaEncryption (1024 bits)
Key Usage	KeyCertSign, CRLSign
Basic Constraint	Subject Type=CA
CRL Distribution Points	[1]CRL Distribution Point Full Name: URI=http://10.144.133.196/crl/ca.crl
MD5 Fingerprint	41:83:77:e7:9f:7d:49:ed:41:a5:83:e2:43:af:9e:c1
SHA1 Fingerprint	64:49:d3:7e:5a:39:6e:ff:d3:1b:36:13:dd:13:fl:1c:11:29:7e:0f

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN CERTIFICATE-----
MIIDSTCCAjGgAwIBAgIQQsHSe8+4XoqmNPpexbHigzANBgkqhkiG9w0BAQUFADBJ
MQswCQYDVQQGEwJUVzEjMCEGA1UEChMaQ2h1bmdod2EgVGVSZWVvSDBby4sIEExO
ZC4xFTATBgNVBAsTDGVDQS8mb3IgdGVzZDQeFw0wMTEyMzYsY2h3YSBUZDw1
MjY2tENvLiwgTHRkLjEYMBYGA1UECwNPU1NMIENBIGZvc1BUZXNOMIGfMAOGCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQDkqWFAKPZzZmoaNEYst6gROVByE2S3ZJKEoemvu
Lf6h/EgWVJh7Iw79kpYfXTEOFQbHVWmoruVjH/NQDAa9nGNbaNMY6jwH8nweMRwi
NSA5B8UMhqusLW7tN5UAdZ1UyQJk3k4Q/eJQc2pYNSTa+G6ImbqnPxdlWdZx3xOF
uWEEEWIDAQABo4GtMIGqMB8GA1UdIwQYMBaAFN5DTnfpmpTaW+54KvOp1R4n7y2P
-----
```

Table 69 describes the labels in Figure 88.

Table 69 Trusted CA details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You can use any character (not including spaces).
Property Check incoming certificates issued by this CA against a CRL	Select this check box to have the BCM50a Integrated Router check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL). Clear this check box to have the BCM50a Integrated Router not check incoming certificates that are issued by this certification authority against a Certificate Revocation List (CRL).
Certification Path	Click the Refresh button to have this read-only text box display the certificate of the end entity and a list of certification authority certificates that shows the hierarchy of certification authorities that validate the end entity certificate. If the issuing certification authority is one that you have imported as a trusted certification authority, it can be the only certification authority in the list (along with the certificate of the end entity). The BCM50a Integrated Router does not trust the end entity certificate and displays "Not trusted" in this field if any certificate on the path has expired or been revoked.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. CA-signed means that a Certification Authority signed the certificate. Self-signed means that the owner of the certificate signed the certificate (not a certification authority). X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate identification number given by the certification authority.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), or Country (C).
Issuer	This field displays identifying information about the certification authority that issued the certificate, such as Common Name, Organizational Unit, Organization or Country. With self-signed certificates, this is the same information as in the Subject Name field.

Table 69 Trusted CA details

Label	Description
Signature Algorithm	This field displays the type of algorithm that was used to sign the certificate. Some certification authorities use rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm). Other certification authorities can use rsa-pkcs1-md5 (RSA public-private key encryption algorithm and the MD5 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate key pair (the BCM50a Integrated Router uses RSA encryption) and the length of the key set in bits (1 024-bits, for example).
Subject Alternative Name	This (optional) field displays the IP address (IP), domain name (DNS), or e-mail address (EMAIL) of the owner of the certificate.
Key Usage	This field displays for what functions the certificate key can be used. For example, "DigitalSignature" means that the key can be used to sign certificates and "KeyEncipherment" means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority certificate and "Path Length Constraint=1" means that there can only be one certification authority in the certification path.
CRL Distribution Points	This field displays how many directory servers with Lists of revoked certificates the issuing certification authority of this certificate makes available. This field also displays the domain names or IP addresses of the servers.
MD5 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the MD5 algorithm. You can use this value to verify with the certification authority (over the phone, for example) that this is actually a valid certificate.
SHA1 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the SHA1 algorithm. You can use this value to verify with the certification authority (over the phone, for example) that this is actually a valid certificate.

Table 69 Trusted CA details

Label	Description
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through floppy disk for example).
Export	Click this button and then Save in the File Download screen. The Save As screen displays, browse to the location that you want to use and click Save .
Apply	Click Apply to save your changes to the BCM50a Integrated Router. You can only apply changes to the name, set the BCM50a Integrated Router to check the CRL issued by the certification authority before trusting a certificate issued, or both.
Cancel	Click Cancel to quit and return to the Trusted CAs screen.

Trusted remote hosts

Click **CERTIFICATES, Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen (see [Figure 89](#)). This screen displays a list of the certificates of peers that you trust but which are not signed by one of the certification authorities on the **Trusted CAs** screen.

You do not need to add any certificate that is signed by one of the certification authorities on the **Trusted CAs** screen because the BCM50a Integrated Router automatically accepts any valid certificate signed by a trusted certification authority as being trustworthy.

Figure 89 Trusted remote hosts
CERTIFICATES

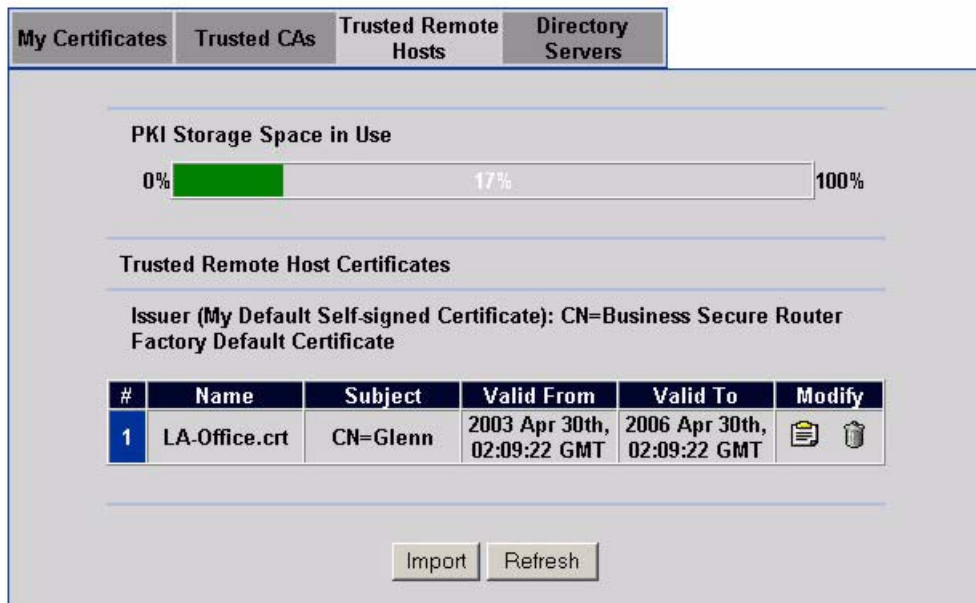


Table 70 describes the labels in Figure 89.

Table 70 Trusted Remote Hosts

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
Issuer (My Default Self-signed Certificate)	This field displays identifying information about the default self-signed certificate on the BCM50a Integrated Router that the BCM50a Integrated Router uses to sign the trusted remote host certificates.
#	This field displays the certificate index number. The certificates are listed in alphabetical order.
Name	This field displays the name used to identify this certificate.
Subject	This field displays identifying information about the owner of the certificate, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company), or C (Country). Nortel recommends that each certificate have unique subject information.

Table 70 Trusted Remote Hosts

Label	Description
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Modify	Click the details icon to open a screen with an in-depth list of information about the certificate. Click the delete icon to remove the certificate. A window displays asking you to confirm that you want to delete the certificate. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Import	Click Import to open a screen where you can save the certificate of a remote host (which you trust) from your computer to the BCM50a Integrated Router.
Refresh	Click this button to display the current validity status of the certificates.

Verifying a certificate of a trusted remote host

Certificates issued by certification authorities have the signature of the certification authority for you to check. Self-signed certificates only have the signature of the host itself. This means that you must be very careful when deciding to import (and thereby trust) the self-signed certificate of a remote host.

Trusted remote host certificate fingerprints

Certificate fingerprints are message digests calculated using the MD5 or SHA1 algorithms. The following procedure describes how to use a certificate fingerprint to verify that you have the remote host's actual certificate.

- 1 Browse to where you have the remote host's certificate saved on your computer.

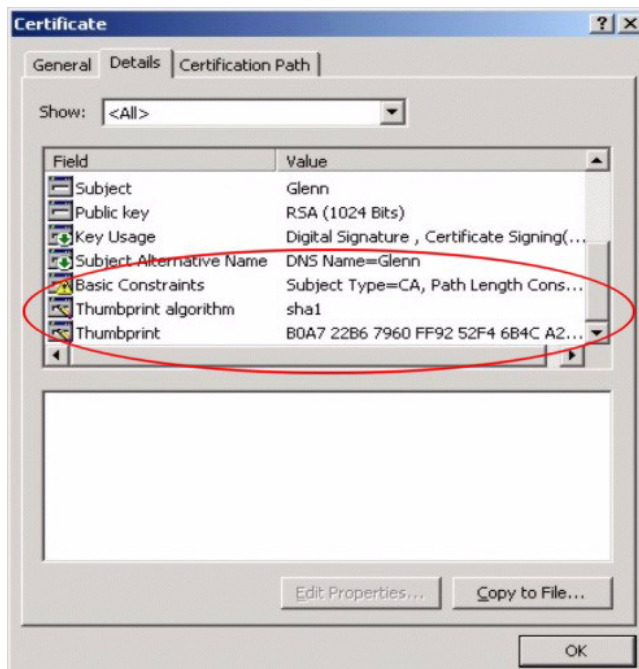
- 2 Make sure that the certificate has a “.cer” or “.crt” file name extension.

Figure 90 Remote host certificates



- 3 Double-click the certificate icon to open the **Certificate** window. Click the **Details** tab and scroll down to the **Thumbprint Algorithm** and **Thumbprint** fields.

Figure 91 Certificate details



Verify (over the phone, for example) that the remote host has the same information in the **Thumbprint Algorithm** and **Thumbprint** fields.

Importing a certificate of a trusted remote host

Click **CERTIFICATES, Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen and then click **Import** to open the **Trusted Remote Host Import** screen. Follow the instructions in this screen to save a trusted host certificate to the BCM50a Integrated Router, see [Figure 92](#).



Note: The trusted remote host certificate must be a self-signed certificate; and you must remove any spaces from its file name before you can import it.

Figure 92 Trusted remote host import

CERTIFICATES - TRUSTED REMOTE HOST - IMPORT

Import

Please specify the location of the certificate file to be imported. The certificate file must be in one of the following formats.

- Binary X.509
- PEM (Base-64) encoded X.509
- Binary PKCS#7
- PEM (Base-64) encoded PKCS#7

File Path:

Table 71 describes the labels in Figure 92.

Table 71 Trusted remote host import

Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse to find it.
Browse	Click Browse to find the certificate file you want to upload.
Apply	Click Apply to save the certificate on the BCM50a Integrated Router.
Cancel	Click Cancel to quit and return to the Trusted Remote Hosts screen.

Trusted remote host certificate details

Click **CERTIFICATES, Trusted Remote Hosts** to open the **Trusted Remote Hosts** screen. Click the details icon to open the **Trusted Remote Host Details** screen. You can use this screen to view in-depth information about the trusted remote host certificate and change the certificate name.

Figure 93 Trusted remote host details
CERTIFICATES - TRUSTED REMOTE HOST - DETAILS

Name

Certification Path

[CN=Business Secure Router Factory Default Certificate]
 [CN=Glenn]

Certificate Information

Type	CA-signed X.509 Certificate
Version	V3
Serial Number	105175496253
Subject	CN=Glenn
Issuer	CN=Business Secure Router Factory Default Certificate
Signature Algorithm	rsa-pkcs1-sha1
Valid From	2003 Apr 30th, 02:09:22 GMT
Valid To	2006 Apr 30th, 02:09:22 GMT
Key Algorithm	rsaEncryption (1024 bits)
Subject Alternative Name	DNS=Glenn
Key Usage Basic Constraint	DigitalSignature Path Length Constraint=10
MD5 Fingerprint	67:e0:c7:7c:ef:bf:99:b5:b3:63:a4:c8:e3:da:5e:58
SHA1 Fingerprint	e9:85:41:d2:7c:99:47:d6:b8:71:79:d9:70:af:3a:6f:c3:9f:0f:e3

Certificate in PEM (Base-64) Encoded Format

```

-----BEGIN CERTIFICATE-----
MIIBuzCCAwwGawIBAgIFGHzytjOwDQYJKoZIhvcNAQEFBQAwpPTE7MDkGA1UEAxMy
QnVzaW5lc3MgU2VjdXJlIFJvdXRlcjBGMWNOB3J5IERlZmF1bHQQQ2VydG1maWNh
dGUwHhcNMDMwNDMwMDIwOTIyWbcNMDYwNDMwMDIwOTIyWjAQMq4wDAYDVQQDEwVH
bGVubjCBnzANBgkqhkiG9w0BAQEFAA0BjQAwYkCgYEAq47bO90jSmORVbmzonzqH
zz7Rumqrqo8JNZPzZaoK8qfL6JiWsmqOTmvAOuae01eWNj6wDirJCsHEDa8F8/ec
+epKiyE2/GCM6nqMrb3OuxjP9wEIAtC27rUeah9ZSmuxLEAsbzdPbwHByNqBQAZ3
jjDBXLXo7SKoVLZF IqABp08CAwEAAAM1MDMwCwYDVROPB&QD&gKEMBA GA1UdEQQJ
MAeCBUdsZW5uMBIGA1UdEwEBAAQIMAYBAQAC&QowDQYJKoZIhvcNAQEFBQAQDQCP
RYbuEEUeG6c1Xru3qOrOvoUPR9+7ln5Zk2MaScOCEjTzOTft0CPD89N/t8uZ7Gnk

```

Table 72 describes the labels in Figure 93.

Table 72 Trusted remote host details

Label	Description
Name	This field displays the identifying name of this certificate. If you want to change the name, type up to 31 characters to identify this key certificate. You can use any character (not including spaces).
Certification Path	Click the Refresh button to have this read-only text box display the end entity's own certificate and a list of certification authority certificates in the hierarchy of certification authorities that validate a the certification authority that issued the certificate. For a trusted host, the list consists of the certificate of the end entity and the default self-signed certificate that the BCM50a Integrated Router uses to sign remote host certificates. Since the BCM50a Integrated Router considers its own self-signed certificate to be a certification authority, the chain of certificates is complete and the BCM50a Integrated Router trusts the certificate.
Refresh	Click Refresh to display the certification path.
Certificate Information	These read-only fields display detailed information about the certificate.
Type	This field displays general information about the certificate. With trusted remote host certificates, this field always displays CA-signed. The BCM50a Integrated Router is the Certification Authority that signed the certificate. X.509 means that this certificate was created and signed according to the ITU-T X.509 recommendation that defines the formats for public-key certificates.
Version	This field displays the X.509 version number.
Serial Number	This field displays the certificate identification number given by the device that created the certificate.
Subject	This field displays information that identifies the owner of the certificate, such as Common Name (CN), Organizational Unit (OU), Organization (O), or Country (C).
Issuer	This field displays identifying information about the default self-signed certificate on the BCM50a Integrated Router that the BCM50a Integrated Router uses to sign the trusted remote host certificates.
Signature Algorithm	This field displays the type of algorithm that the BCM50a Integrated Router used to sign the certificate, which is rsa-pkcs1-sha1 (RSA public-private key encryption algorithm and the SHA1 hash algorithm).
Valid From	This field displays the date that the certificate becomes applicable. The text displays in red and includes a Not Yet Valid! message if the certificate has not yet become applicable.

Table 72 Trusted remote host details

Label	Description
Valid To	This field displays the date that the certificate expires. The text displays in red and includes an Expiring! or Expired! message if the certificate is about to expire or has already expired.
Key Algorithm	This field displays the type of algorithm that was used to generate the certificate key pair (the BCM50a Integrated Router uses RSA encryption) and the length of the key set in bits (1 024-bits, for example).
Subject Alternative Name	This (optional) field displays the certificate owner's IP address (IP), domain name (DNS), or e-mail address (EMAIL).
Key Usage	This field displays for what functions the certificate key can be used. For example, DigitalSignature means that the key can be used to sign certificates and KeyEncipherment means that the key can be used to encrypt text.
Basic Constraint	This field displays general information about the certificate. For example, Subject Type=CA means that this is a certification authority certificate and Path Length Constraint=1 means that there can only be one certification authority in the certification path of the certificate.
MD5 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the MD5 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the BCM50a Integrated Router has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See "Verifying a certificate of a trusted remote host" on page 279 for how to verify a remote host's certificate.
SHA1 Fingerprint	This is the message digest of the certificate that the BCM50a Integrated Router calculated using the SHA1 algorithm. You cannot use this value to verify that this is the remote host's actual certificate because the BCM50a Integrated Router has signed the certificate; thus causing this value to be different from that of the remote host's actual certificate. See "Verifying a certificate of a trusted remote host" on page 279 for how to verify a remote host's certificate.
Certificate in PEM (Base-64) Encoded Format	This read-only text box displays the certificate or certification request in Privacy Enhanced Mail (PEM) format. PEM uses 64 ASCII characters to convert the binary certificate into a printable form. You can copy and paste the certificate into an e-mail to send to friends or colleagues or you can copy and paste the certificate into a text editor and save the file on a management computer for later distribution (through floppy disk for example).
Export	Click this button and then Save in the File Download screen. The Save As screen displays. Browse to the location that you want to use and click Save .

Table 72 Trusted remote host details

Label	Description
Apply	Click Apply to save your changes to the BCM50a Integrated Router. You can only change the name of the certificate.
Cancel	Click Cancel to quit configuring this screen and return to the Trusted Remote Hosts screen.

Directory servers

Click **CERTIFICATES, Directory Servers** to open the **Directory Servers** screen (Figure 94). This screen displays a summary list of directory servers (that contain lists of valid and revoked certificates) that have been saved into the BCM50a Integrated Router. If you decide to have the BCM50a Integrated Router check incoming certificates against the issuing certification authority's list of revoked certificates, the BCM50a Integrated Router first checks the servers listed in the **CRL Distribution Points** field of the incoming certificate. If the certificate does not list a server or the listed server is not available, the BCM50a Integrated Router checks the servers listed here.

Figure 94 Directory servers

CERTIFICATES

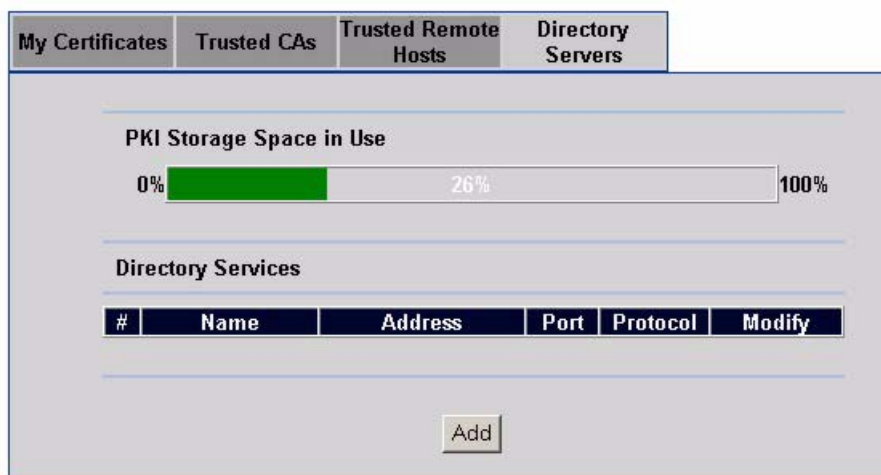


Table 73 describes the labels in Figure 94.

Table 73 Directory Servers

Label	Description
PKI Storage Space in Use	This bar displays the percentage of the PKI storage space that is currently in use. The bar turns from green to red when the maximum is approached. When the bar is red, consider deleting expired or unnecessary certificates before adding more certificates.
#	The index number of the directory server. The servers are listed in alphabetical order.
Name	This field displays the name used to identify this directory server.
Address	This field displays the IP address or domain name of the directory server.
Port	This field displays the port number that the directory server uses.
Protocol	This field displays the protocol that the directory server uses.
Modify	Click the details icon to open a screen where you can change the information about the directory server. Click the delete icon to remove the directory server entry. A window displays asking you to confirm that you want to delete the directory server. Note that subsequent certificates move up by one when you take this action. You cannot delete a certificate that is currently in use.
Add	Click Add to open a screen where you can configure information about a directory server so that the BCM50a Integrated Router can access it.

Add or edit a directory server

Click **CERTIFICATES, Directory Servers** to open the **Directory Servers** screen. Click **Add** (or the details icon) to display the screen shown in Figure 95. Use this screen to configure information about a directory server that the BCM50a Integrated Router can access.

Figure 95 Directory server add
CERTIFICATES - DIRECTORY SERVER - ADD

Table 74 describes the labels in Figure 95.

Table 74 Directory server add

Label	Description
Directory Service Setting	
Name	Type up to 31 ASCII characters (spaces are not permitted) to identify this directory server.
Access Protocol	Use the drop-down list to select the access protocol used by the directory server. LDAP (Lightweight Directory Access Protocol) is a protocol over TCP that specifies how clients access directories certificates and lists of revoked certificates. ¹
Server Address	Type the IP address (in dotted decimal notation) or the domain name of the directory server.

Table 74 Directory server add

Label	Description
Server Port	This field displays the default server port number of the protocol that you select in the Access Protocol field. You can change the server port number if needed, however, you must use the same server port number that the directory server uses. The default server port number for LDAP is 389.
Login Setting	
Login	The BCM50a Integrated Router must authenticate itself in order to assess the directory server. Type the logon name (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Password	Type the password (up to 31 ASCII characters) from the entity maintaining the directory server (usually a certification authority).
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to quit configuring this screen and return to the Directory Servers screen.

- 1 At the time of writing, LDAP is the only choice for directory server access protocol.

Chapter 15

Bandwidth management

This chapter describes the functions and configuration of bandwidth management.

Bandwidth management overview

With bandwidth management, you can allocate the outgoing capacity of an interface to specific types of traffic. It can also help you make sure that the BCM50a Integrated Router forwards certain types of traffic (especially real-time applications) with minimum delay. With the use of real-time applications such as Voice-over-IP (VoIP) increasing, the requirement for bandwidth allocation is also increasing.

Bandwidth management addresses questions such as:

- Who gets how much access to specific applications?
- Which traffic must have guaranteed delivery?
- How much bandwidth is allotted to guarantee delivery?

With bandwidth management, you can configure the allowed output for an interface to match what the network can handle. This helps reduce delays and dropped packets at the next routing device. For example, you can set the WAN interface speed to 1 024 kb/s (or less) if the broadband device connected to the WAN port has an upstream speed of 1 024 kb/s.

Bandwidth classes and filters

Use bandwidth subclasses to allocate specific amounts of bandwidth capacity (bandwidth budgets). Configure a bandwidth filter to define a bandwidth subclass based on a specific application or subnet. Use the **Class Setup** tab (see [“Bandwidth Manager Class Configuration” on page 297](#)) to set up a bandwidth class name, bandwidth allotment, and filter specifics. Each bandwidth subclass consists of a single filter you can define by editing the subclass.

Unallocated bandwidth, bandwidth that is not controlled by a subclass you specify, is allocated to traffic not controlled by any subclass. View your configured bandwidth subclasses for a given interface in the **Class Setup** tab (see [“Configuring class setup” on page 295](#) for details). The total of the configured bandwidth budgets cannot exceed the configured bandwidth budget for the interface, as specified in [“Configuring summary” on page 294](#).

Proportional bandwidth allocation

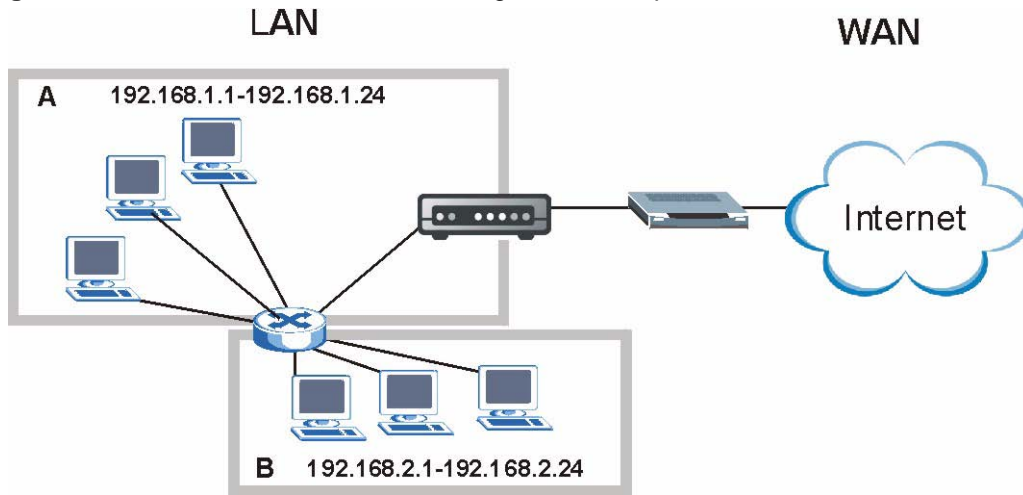
With bandwidth management, you can define how much bandwidth each class gets; however, the actual bandwidth allotted to each class decreases or increases in proportion to actual available bandwidth.

Application based bandwidth management

You can create bandwidth classes based on individual applications (like FTP, H.323, and SIP).

Subnet based bandwidth management

You can create bandwidth classes based on subnets. [Figure 96](#) shows LAN subnets. You can configure one bandwidth class for subnet A and another for subnet B.

Figure 96 Subnet based bandwidth management example

Application and subnet based bandwidth management

You can also create bandwidth classes based on a combination of a subnet and an application. [Table 75](#) shows bandwidth allocations for application specific traffic from separate LAN subnets.

Table 75 Application and Subnet based Bandwidth Management Example

Traffic Type	From Subnet A	From Subnet B
FTP	64 Kb/s	64 Kb/s
H.323	64 Kb/s	64 Kb/s
SIP	64 Kb/s	64 Kb/s

Reserving bandwidth for nonbandwidth class traffic

If you want to allow bandwidth for traffic that is not defined in a bandwidth filter, leave some of the bandwidth on the interface unbudgeted.

Configuring summary

Click **BW MGMT** to open the **Summary** screen.

Enable bandwidth management on an interface and set the maximum allowed bandwidth for that interface.

Figure 97 Bandwidth Manager: Summary

BANDWIDTH MANAGEMENT

Class	Active	Speed (kbps)
WAN	<input type="checkbox"/>	100000
LAN	<input type="checkbox"/>	100000

Table 76 describes the labels in Figure 97.

Table 76 Bandwidth Manager: Summary

Label	Description
WAN LAN	These read-only labels represent the physical interfaces. Select the check box next to an interface to enable bandwidth management on that interface. Bandwidth management applies to all traffic flowing out of the router through the interface, regardless of the traffic source. Traffic redirect or IP alias can cause LAN-to-LAN traffic to pass through the BCM50a Integrated Router and be managed by bandwidth management.
Active	Select a check box to enable bandwidth management on that interface.

Table 76 Bandwidth Manager: Summary

Label	Description
Speed (kbps)	Enter the amount of bandwidth for this interface that you want to allocate using bandwidth management. This appears as the bandwidth budget of the interface root class (see “Configuring class setup” on page 295). Nortel recommends that you set this speed to match what the device connected to the port can handle. For example, set the WAN interface speed to 1 000 kb/s (or less) if the broadband device connected to the WAN port has an upstream speed of 1 000 kb/s.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Configuring class setup

The class setup screen displays the configured bandwidth classes by individual interface. Select an interface and click the buttons to perform the actions described next. Click + to expand the class tree or click - to collapse the class tree. Each interface has a permanent root class. The bandwidth budget of the root class is equal to the speed you configured on the interface (see [“Configuring summary” on page 294](#) to configure the speed of the interface). Configure subclass layers for the root class.

To add or delete child classes on an interface, click **BW MGMT**, then the **Class Setup** tab. The screen appears as shown in [Figure 98](#).

Figure 98 Bandwidth Manager: Class setup
BANDWIDTH MANAGEMENT

Class Setup

Interface

Bandwidth Management: Active

Root Class: 100000 kbps

----- WAN-1: 1000 kbps

----- WAN-2: 1000 kbps

Filter List

#	Filter Name	Service	Destination IP Address	Destination Port	Source IP Address	Source Port	Protocol ID
1	WAN-1	FTP	0.0.0.0/0	0	0.0.0.0/0	0	0
2	WAN-2	SIP	0.0.0.0/0	0	192.168.1.33/0	0	0

filter to filter (filter number).

Table 77 describes the labels in Figure 98.

Table 77 Bandwidth Manager: Class Setup

Label	Description
Interface	Select an interface from the drop-down list for which you wish to set up classes.
Bandwidth Management	This field displays whether bandwidth management on the interface you selected in the field above is enabled (Active) or not (Inactive).
Add Sub-Class	Click Add Sub-Class to add a subclass.
Edit	Click Edit to go to a screen where you can configure the selected subclass. You cannot edit the root class.
Delete	Click Delete to remove the selected subclass. You cannot delete the root class.
Statistics	Click Statistics to display the status of the selected class.

Table 77 Bandwidth Manager: Class Setup

Label	Description
#	This is the number of a filter entry. The ordering of your filters is important, as they are applied in turn. Use the Move button to reorder your filters.
Filter Name	This is the Class Name that you configured in the Edit Class screen.
Service	If you selected a predefined application (FTP, H.323 or SIP), it displays here.
Destination IP Address	This field displays the destination IP address in dotted decimal notation followed by the subnet mask. The IP 0.0.0.0/0 means all.
Destination Port	This field displays the port number of the destination. 0 means all ports.
Source IP Address	This field displays the source IP address in dotted decimal notation followed by the subnet mask. The IP 0.0.0.0/0 means all.
Source Port	This field displays the port number of the source. The 0 means all ports.
Protocol ID	This field displays the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP. The 0 means all protocols.
Move	Type the number of a filter entry and the number for where you want to put it. Click Move to move the filter to the number that you typed. The ordering of your filters is important, as they are applied in order of their numbering. The filter entry numbers are not static names for the entries. A filter entry's number changes as you move the filter entry up or down in the list. Also, only the existing filter entries are counted, you cannot have any blank filter entries. For example, if you have only three filters and try to move number one to seven, it becomes filter three.

Bandwidth Manager Class Configuration

Configure a bandwidth management class in the **Class Setup** screen. You must use the **Summary** screen to enable bandwidth management on an interface before you can configure subclasses for that interface.

To add a subclass, click **BW MGMT**, and then the **Class Setup** tab. Click the **Add Sub-Class** button to open the screen shown in [Figure 99](#).

Figure 99 Bandwidth Manager: Edit class**BANDWIDTH MANAGEMENT - EDIT CLASS**

Class Configuration

Class Name: WAN-2

Bandwidth Budget: 1000 (kbps)

Filter Configuration

Enable Bandwidth Filter

Service: SIP

Destination IP Address: 0.0.0.0

Destination Subnet Mask: 0.0.0.0

Destination Port: 0

Source IP Address: 192.168.1.33

Source Subnet Mask: 0.0.0.0

Source Port: 0

Protocol ID: 0

Apply Cancel

Table 78 describes the labels in Figure 99.

Table 78 Bandwidth Manager: Edit class

Label	Description
Class Configuration	
Class Name	Use the autogenerated name or enter a descriptive name of up to 20 alphanumeric characters, including spaces.
Bandwidth Budget (kbps)	Specify the maximum bandwidth allowed for the class in kb/s. The recommendation is a setting between 20 kbps and 20 000 kbps for an individual class. The bandwidth you specify cannot cause the total allocated bandwidths of this and all other subclasses to exceed the bandwidth for the interface.

Table 78 Bandwidth Manager: Edit class

Label	Description
Filter Configuration	
Enable Bandwidth Filter	<p>Select Enable Bandwidth Filter to have the BCM50a Integrated Router use this bandwidth filter when it performs bandwidth management.</p> <p>You must enter a value in at least one of the following fields (other than the Subnet Mask fields, which are only available when you enter the destination or source IP address).</p>
Service	<p>This field simplifies bandwidth class configuration by allowing you to select a predefined application. When you select a predefined application, you do not need to configure the rest of the bandwidth filter fields (other than the Active check box).</p> <p>FTP (File Transfer Program) is a program to enable fast transfer of files, including large files that are not possible by e-mail. Select FTP from the drop-down list to configure the bandwidth filter for FTP traffic.</p> <p>If you select FTP, make sure you also turn on the FTP ALG. For more information about ALG, see “ALG” on page 88.</p> <p>H.323 is a protocol standard used for multimedia communications over networks, for example, NetMeeting. Select H.323 from the drop-down list to configure the bandwidth filter for H.323 traffic.</p> <p>SIP (Session Initiation Protocol) is a signaling protocol used in Internet telephony, instant messaging, events notification, and conferencing. The BCM50a Integrated Router supports SIP traffic pass through. Select SIP from the drop-down list to configure this bandwidth filter for SIP traffic. This option makes it easier to manage bandwidth for SIP traffic and is useful for example when there is a VoIP (Voice over Internet Protocol) device on your LAN.</p> <p>Select All from the drop-down list if you do not want to use a predefined application for the bandwidth class. When you select All, you must configure at least one of the following fields (other than the Subnet Mask fields, which you only enter if you also enter a corresponding destination or source IP address).</p>
Destination IP Address	Enter the destination IP address in dotted decimal notation.
Destination Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a Destination IP Address .
Destination Port	Enter the port number of the destination. See “Predefined services” on page 178 in Chapter 11 Firewall screens for a table of services and port numbers.
Source IP Address	Enter the source IP address.
Source Subnet Mask	Enter the destination subnet mask. This field is N/A if you do not specify a Source IP Address .

Table 78 Bandwidth Manager: Edit class

Label	Description
Source Port	Enter the port number of the source. See Table 79 for some common services and port numbers.
Protocol ID	Enter the protocol ID (service type) number, for example: 1 for ICMP, 6 for TCP or 17 for UDP.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to exit this screen without saving.

Table 79 Services and port numbers

Services	Port Number
ECHO	7
FTP (File Transfer Protocol)	21
SMTP (Simple Mail Transfer Protocol)	25
DNS (Domain Name System)	53
Finger	79
HTTP (Hyper Text Transfer protocol or WWW, Web)	80
POP3 (Post Office Protocol)	110
NNTP (Network News Transport Protocol)	119
SNMP (Simple Network Management Protocol)	161
SNMP trap	162
PPTP (Point-to-Point Tunneling Protocol)	1723

Bandwidth management statistics

Use the **Bandwidth Management Statistics** screen to view network performance for the interface (root class) or a specific subclass. Select the root or subclass from the **Class Setup** screen and then click **Statistics** to see how it is performing.

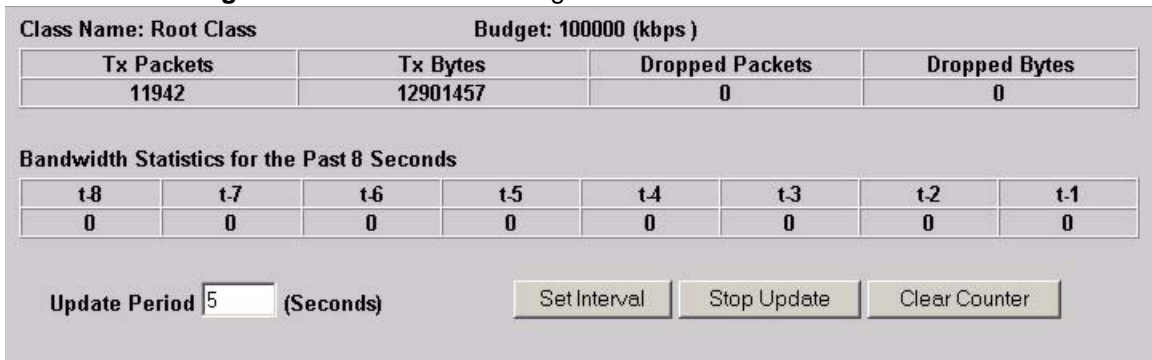
Figure 100 Bandwidth management statistics

Table 80 describes the labels in Figure 100.

Table 80 Bandwidth management statistics

Label	Description
Class Name	This field displays the name of the class the statistics page is showing.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Tx Packets	This field displays the total number of packets transmitted.
Tx Bytes	This field displays the total number of bytes transmitted.
Dropped Packets	This field displays the total number of packets dropped.
Dropped Bytes	This field displays the total number of bytes dropped.
Bandwidth Statistics for the Past 8 Seconds (t-8 to t-1)	
This field displays the bandwidth statistics (in b/s) for the past one to eight seconds. For example, t-1 means one second ago.	
Update Period (Seconds)	Enter the time interval, in seconds, to define how often the information is refreshed.
Set Interval	Click Set Interval to apply the new update period you entered in the Update Period field above.
Stop Update	Click Stop Update to stop the browser from refreshing bandwidth management statistics.
Clear Counter	Click Clear Counter to clear all of the bandwidth management statistics.

Monitor

To view bandwidth usage and allotments, click **BW MGMT**, then the **Monitor** tab. The screen appears as shown in [Figure 101](#).

Figure 101 Bandwidth manager monitor

BANDWIDTH MANAGEMENT

Class	Budget (kbps)	Current Usage (kbps)
Root Class	100000	0
WAN-1	1000	0
WAN-2	1000	0
Default Class	98000	0

[Table 81](#) describes the labels in [Figure 101](#).

Table 81 Bandwidth manager monitor

Label	Description
Interface	Select an interface from the drop-down list to view the bandwidth usage of its bandwidth classes.
Class	This field displays the name of the class.
Budget (kbps)	This field displays the amount of bandwidth allocated to the class.
Current Usage (kbps)	This field displays the amount of bandwidth that each class is using.
Refresh	Click Refresh to update the page.

Chapter 16

Authentication server

The BCM50a Integrated Router can use either the local user database internal to the BCM50a Integrated Router or an external RADIUS server for an unlimited number of users.

Introduction to Local User database

By storing user profiles locally on the BCM50a Integrated Router, your BCM50a Integrated Router is able to authenticate users without interacting with a network RADIUS server. However, there is a limit on the number of users you can authenticate in this way.

Local User database

To see the local user list, click **AUTH SERVER**. The **Local User Database** screen appears as shown in [Figure 102](#).

Figure 102 Local User database**Local User Database**

Local User Database		RADIUS					
-	#	User ID	Active	User type	Last Name	First Name	Status <small>(IPSec user only)</small>
	1	-	-	-	-	-	-
	2	-	-	-	-	-	-
	3	-	-	-	-	-	-
	4	-	-	-	-	-	-
	5	-	-	-	-	-	-
	6	-	-	-	-	-	-
	7	-	-	-	-	-	-
	8	-	-	-	-	-	-
	9	-	-	-	-	-	-
	10	-	-	-	-	-	-
	11	-	-	-	-	-	-
	12	-	-	-	-	-	-
	13	-	-	-	-	-	-
	14	-	-	-	-	-	-
	15	-	-	-	-	-	-
	16	-	-	-	-	-	-
	17	-	-	-	-	-	-
	18	-	-	-	-	-	-
	19	-	-	-	-	-	-
	20	-	-	-	-	-	-
	21	-	-	-	-	-	-
	22	-	-	-	-	-	-
	23	-	-	-	-	-	-
	24	-	-	-	-	-	-
	25	-	-	-	-	-	-
	26	-	-	-	-	-	-
	27	-	-	-	-	-	-
	28	-	-	-	-	-	-
	29	-	-	-	-	-	-
	30	-	-	-	-	-	-
	31	-	-	-	-	-	-
	32	-	-	-	-	-	-

Table 82 describes the labels in Figure 102.

Table 82 Local User database

Label	Description
User ID	This field displays the logon name for the user account.
Active	This field displays Yes if the user account is enabled or No if it is disabled.
User type	This field displays whether the user account can be used for a IEEE 802.1X or IPSec logon (or both).
Last Name	This field displays the user's last name.
First Name	This field displays the user's first name.

Table 82 Local User database

Label	Description
Status	This field displays the status of IPSec user accounts. A dash appears for all other accounts. Valid displays if an IPSec user can use the account to logon. Expired displays if an IPSec user can no longer use the account to logon. This happens when you have enabled Password Management in the VPN Client Termination Advanced screen and the account password has exceeded the time that you configured as the Maximum Password Age .
Edit	Select a user account and click Edit to go to the screen where you can configure the account settings.
Delete	Select a user account and click Delete to remove the account.

Edit Local User Database

To change a local user database entry, click **AUTH SERVER**. In the **Local User Database** screen, select the radio button of an entry and click the **Edit** button to display the **Local User Database Edit** screen, as shown in [Figure 103](#).

Figure 103 Local User database edit

User Edit

Active

User Type: 802.1X/IPSec

User Name: [Text Input]

Password: [Text Input]

Retype to Confirm: [Text Input]

IPSec User Profile

Account Name: [Text Input]

First Name: [Text Input]

Last Name: [Text Input]

Remote User

Static IP Address: 0.0.0.0

Static Subnet Mask: 0.0.0.0

Split Tunneling: Enabled (Configure Network)

Split Tunnel Network: example

Inverse Split Tunnel Network: (None selected)

Apply Cancel

Table 83 describes the labels in Figure 103.

Table 83 Local User database edit

Label	Description
Active	Select this check box to turn on the user account. Clear this check box to turn off the user account.
User Type	Select 802.1X to set this user account to be used for a IEEE 802.1X logon. Select IPSec to set this user account to be used for an IPSec logon. Select 802.1X/IPSec to set this user account to be used for both IEEE 802.1X and IPSec logons.
User Name	Specify the user ID to be used as the logon name for the user account.
Password	Enter a password up to 31 characters long for this user account. Note that as you type a password, the screen displays a (*) for each character you type.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
IPSec User Profile	The following fields display when you select IPSec or 802.1X/IPSec in the User Type field.
First Name	Enter the user's first name.
Last Name	Enter the user's last name.
Static IP Address	Enter the IP address of the remote user in dotted decimal notation.
Static Subnet Mask	Enter the subnet mask of the remote user.
Split Tunneling	Enable or disable split tunneling or inverse split tunneling. Select Disable to force all traffic to be encrypted and go through the VPN tunnel. Select Enabled to allow traffic not going through the VPN tunnel to go through the WAN interface without being encrypted. This reduces the processing load on the BCM50a Integrated Router but is less secure since the Contivity VPN clients' unencrypted sessions make them vulnerable to attacks. Select Enabled - Inverse to force traffic not going to the network subnets that you specify to be encrypted and sent through the VPN tunnel. Select Enable - Inverse (locally connected) to force traffic not going to directly connected networks, or the network subnets that you specify, to be encrypted and sent through the VPN tunnel.
Configure Network	Click this link to set up the list of networks to use as split or inverse split networks.

Table 83 Local User database edit

Label	Description
Split Tunnel Networks	This field applies when you select Enabled in the Split Tunneling field. Select the network for which you force traffic to be encrypted and go through the VPN tunnel.
Inverse Split Tunnel Network	This field applies when you select Enabled - Inverse or Enabled - Inverse (locally connected) in the Split Tunneling field. Select the network for which you do not force traffic to be encrypted and go through the VPN tunnel.
Apply	Click Apply to save the user account settings.
Cancel	Click Cancel to exit this screen without saving.

Current split networks

In the **Local User Database Edit** screen, click **Configure Network** to display the **Current Split Networks** screen as shown in [Figure 104](#). This screen displays a list of networks that are configured for use with split and inverse split VPN tunnels.

Figure 104 Current split networks

Current Split Networks



Table 84 describes the labels in Figure 104.

Table 84 Current split networks

Label	Description
Return to Local User Database -> User Edit Page	Click this link to return to the screen where you configure a local user database entry.
Current Split Networks	This is the list of names of split or inverse split networks.
Add	Click Add to open another screen where you can specify split or inverse split networks.
Edit	Select the name of a split or inverse split network and click Edit to open a screen where you can change the network settings.
Delete	Select the name of a split or inverse split network and click Delete to remove the network entry.

Current split networks edit

In the **Local User Database Edit** screen, click **Configure Network** to display the **Current Split Networks** screen. Click **Add** or select a network and click **Edit** in order to display the **Current Networks Edit** screen. Use this screen shown in Figure 105 to configure a set of subnets to use with split or inverse split VPN tunnels.

Figure 105 Current split networks edit**Current Split Networks Edit**

The screenshot shows a dialog box titled "Current Split Networks Edit". At the top, there is a "Network Name" label followed by a text input field containing the word "example". Below this is a horizontal separator line. Underneath, there are two labels: "IP Address" and "Netmask", each followed by a text input field containing "0.0.0.0". Below these is another label: "Current Subsets for Network: example", followed by a list box containing the text "192.168.1.0/24". Below the list box are three buttons: "Add", "Delete", and "Clear". At the bottom of the dialog are two more buttons: "Apply" and "Cancel".

[Table 85](#) describes the labels in [Figure 105](#).

Table 85 Current split networks edit

Label	Description
Network Name	Enter a name to identify the split network.
IP Address	Enter the IP address for the split network in dotted decimal notation.
Netmask	Enter the netmask for the split network in dotted decimal notation.

Table 85 Current split networks edit

Label	Description
Current Subnets for Network:	This box displays the subnets that belong to this split network.
Add	Click Add to save your split network configuration.
Delete	Select a network subset and click Delete to remove it.
Clear	Click Clear to remove all of the configuration field and subnet settings.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to exit this screen without saving your changes.

Configuring RADIUS

Use RADIUS if you want to authenticate users using an external server.

To set up RADIUS server settings, click **AUTH SERVER**, then the **RADIUS** tab. The screen appears, as shown in [Figure 106](#).

Figure 106 RADIUS
AUTH SERVER

The screenshot shows a configuration window for RADIUS authentication and accounting servers. The window has two tabs: 'Local User Database' and 'RADIUS'. The 'RADIUS' tab is selected. The window is divided into two main sections: 'Authentication Server' and 'Accounting Server'. Each section contains a checkbox for 'Active', a text field for 'Server IP Address', a text field for 'Port Number', a text field for 'Key', and a text field for 'Retype to Confirm'. The 'Authentication Server' section has 'Server IP Address' set to 0.0.0.0 and 'Port Number' set to 1812. The 'Accounting Server' section has 'Server IP Address' set to 0.0.0.0 and 'Port Number' set to 1813. At the bottom of the window are two buttons: 'Apply' and 'Reset'.

Table 86 describes the labels in Figure 106.

Table 86 RADIUS

Label	Description
Authentication Server	
Active	Select the check box to enable user authentication through an external authentication server. Clear the check box to enable user authentication using the local user profile on the BCM50a Integrated Router.
Server IP Address	Enter the IP address of the external authentication server in dotted decimal notation.

Table 86 RADIUS

Label	Description
Port Number	The default port of the RADIUS server for authentication is 1812. You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external authentication server and the BCM50a Integrated Router. Note that, as you type a password, the screen displays an * for each character you type. The key is not sent over the network. This key must be the same on the external authentication server and BCM50a Integrated Router.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Accounting Server	
Active	Select the check box to enable user accounting through an external authentication server.
Server IP Address	Enter the IP address of the external accounting server in dotted decimal notation.
Port Number	The default port of the RADIUS server for accounting is 1813 . You need not change this value unless your network administrator instructs you to do so with additional information.
Key	Enter a password (up to 31 alphanumeric characters) as the key to be shared between the external accounting server and the BCM50a Integrated Router. Note that as you type a password, the screen displays a (*) for each character you type. The key is not sent over the network. This key must be the same on the external accounting server and BCM50a Integrated Router.
Retype to Confirm	Enter the password again to make sure that you have entered it correctly.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 17

Remote management screens

This chapter provides information on the **Remote Management** screens.

Remote management overview

Remote management allows you to determine which services and protocols can access which BCM50a Integrated Router interface (if any) from which computers.



Note: When you configure remote management to allow management from the WAN, you still need to configure a firewall rule to allow access.

You can manage your BCM50a Integrated Router from a remote location through:

- Internet (WAN only)
- LAN only
- ALL (LAN and WAN)
- Neither (Disable)



Note: If you choose WAN only or ALL (LAN & WAN), you still need to configure a firewall rule to allow access.

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

Remote management limitations

Remote management over LAN or WAN does not work if:

- 1 A filter in SMT menu 3.1 (LAN) or in menu 11.1.4 (WAN) is applied to block a Telnet, FTP, or Web service.
- 2 A service is disabled in one of the remote management screens.
- 3 The IP address in the **Secured Client IP** field does not match the client IP address. If it does not match, the BCM50a Integrated Router disconnects the session immediately.
- 4 Another remote management session of the same type (web, FTP or Telnet) is running. You can only have one remote management session of the same type running at one time.
- 5 A web remote management session is running with a Telnet session. A web session is disconnected if you begin a Telnet session; nor does it begin if a Telnet session is already running.
- 6 A firewall rule blocks access to device.

Remote management and NAT

When NAT is enabled:

- Use the BCM50a Integrated Router WAN IP address when configuring from the WAN.
- Use the BCM50a Integrated Router LAN IP address when configuring from the LAN.

System timeout

There is a system timeout of 5 minutes (300 seconds) for the Telnet, web, or FTP connections. Your BCM50a Integrated Router automatically logs you off if you do nothing in this timeout period, except when it is continuously updating the status in menu 24.1 or when `sys studio` was changed on the command line. Use the **System** screen to change the timeout period in the **Administrator Inactivity Timer** field.

Introduction to HTTPS

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

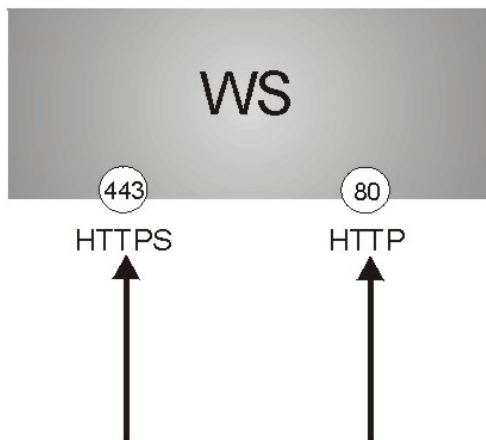
HTTPS relies upon certificates, public keys, and private keys (see [Chapter 14, “Certificates,”](#) on page 253 for more information).

HTTPS on the BCM50a Integrated Router is used so that you can securely access the BCM50a Integrated Router using the WebGUI. The SSL protocol specifies that the SSL server (the BCM50a Integrated Router) must always authenticate itself to the SSL client (the computer that requests the HTTPS connection with the BCM50a Integrated Router), whereas the SSL client only authenticates itself when the SSL server requires it to do so (select **Authenticate Client Certificates** in the **REMOTE MGMT, WWW** screen). **Authenticate Client Certificates** is optional and, if selected, means the SSL-client must send the BCM50a Integrated Router a certificate. You must apply for a certificate for the browser from a trusted CA on the BCM50a Integrated Router.

Refer to [Figure 107](#) about HTTPS implementation.

- 1 HTTPS connection requests from an SSL-aware Web browser go to port 443 (by default) on the BCM50a Integrated Router WS (Web server).
- 2 HTTP connection requests from a Web browser go to port 80 (by default) on the BCM50a Integrated Router WS (Web server).

Figure 107 HTTPS implementation



Note: If you disable **HTTP Server Access (Disable)** in the **REMOTE MGMT WWW** screen, the BCM50a Integrated Router blocks all HTTP connection attempts.

Configuring WWW

To change your BCM50a Integrated Router Web settings, click **REMOTE MGMT** to open the **WWW** screen.

Figure 108 WWW

REMOTE MANAGEMENT

Table 87 describes the labels in Figure 108.

Table 87 WWW

Label	Description
HTTPS	
Server Certificate	Select the Server Certificate that the BCM50a Integrated Router uses to identify itself. The BCM50a Integrated Router is the SSL server and must always authenticate itself to the SSL client (the computer that requests the HTTPS connection with the BCM50a Integrated Router).
Authenticate Client Certificates	Select Authenticate Client Certificates (optional) to require the SSL client to authenticate itself to the BCM50a Integrated Router by sending the BCM50a Integrated Router a certificate. To do that, the SSL client must have a CA-signed certificate from a CA that has been imported as a trusted CA on the BCM50a Integrated Router (see the appendix on importing certificates for details).

Table 87 WWW

Label	Description
Server Port	The HTTPS proxy server listens on port 443 by default. If you change the HTTPS proxy server port to a different number on the BCM50a Integrated Router, for example, 8443, you must notify people who need to access the BCM50a Integrated Router WebGUI to use https://BCM50a Integrated Router IP Address:8443 as the URL.
Server Access	Select a BCM50a Integrated Router interface from Server Access on which incoming HTTPS access is allowed. You can allow only secure WebGUI access by setting the HTTP Server Access field to Disable and setting the HTTPS Server Access field to an interface.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
HTTP	
Server Port	You can change the server port number for a service, if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the BCM50a Integrated Router using this service.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

HTTPS example

To change the default HTTPS port on the BCM50a Integrated Router, in your browser, enter “https://BCM50a Integrated Router IP Address/” as the Web site address, where “BCM50a Integrated Router IP Address” is the IP address or domain name of the BCM50a Integrated Router you wish to access.

Internet Explorer warning messages

When you attempt to access the BCM50a Integrated Router HTTPS server, a Windows dialog box appears, asking if you trust the server certificate. Click **View Certificate** if you want to verify that the certificate is from the BCM50a Integrated Router.

The **Security Alert** screen shown in [Figure 109](#) appears in Internet Explorer. Select **Yes** to proceed to the WebGUI logon screen; if you select **No**, then WebGUI access is blocked.

Figure 109 Security Alert dialog box (Internet Explorer)



Netscape Navigator warning messages

When you attempt to access the BCM50a Integrated Router HTTPS server, a **Website Certified by an Unknown Authority** screen (shown in [Figure 110](#)) appears asking if you trust the server certificate. Click **Examine Certificate** if you want to verify that the certificate is from the BCM50a Integrated Router.

If you select **Accept this certificate temporarily for this session**, then click **OK** to continue in Netscape.

Select **Accept this certificate permanently** to import the BCM50a Integrated Router certificate into the SSL client.

Figure 110 Figure 18-4 Security Certificate 1 (Netscape)



Figure 111 Security Certificate 2 (Netscape)

Avoiding the browser warning messages

The following section describes the main reasons that your browser displays warnings about the BCM50a Integrated Router HTTPS server certificate and what you can do to avoid seeing the warnings.

- The issuing certificate authority of the BCM50a Integrated Router HTTPS server certificate is not a trusted certificate authority in the browser. The issuing certificate authority of the BCM50a Integrated Router's factory default certificate is the BCM50a Integrated Router itself since the certificate is a self-signed certificate.
 - For the browser to trust a self-signed certificate, import the self-signed certificate into your operating system as a trusted certificate.
 - To have the browser trust the certificates issued by a certificate authority, import the certificate authority's certificate into your operating system as a trusted certificate.
- The actual IP address of the HTTPS server (the IP address of the BCM50a Integrated Router port that you are trying to access) does not match the common name specified in the BCM50a Integrated Router HTTPS server certificate that your browser received. To check the common name specified in the certificate that your BCM50a Integrated Router sends to HTTPS clients:

- a** Click **REMOTE MGMT**. Write down the name of the certificate displayed in the **Server Certificate** field.
- b** Click **CERTIFICATES**. Find the certificate that was displayed in the Server Certificate field and check its **Subject** column. **CN** stands for the common name of the certificate (see [Figure 115 on page 328](#) for an example).

Use this procedure to have the BCM50a Integrated Router use a certificate with a common name that matches the actual IP address of the BCM50a Integrated Router. You cannot use this procedure if you need to access the WAN port and it uses a dynamically assigned IP address.

- a** Create a new certificate for the BCM50a Integrated Router that uses the IP address (of the BCM50a Integrated Router port that you are trying to access) as the common name of the certificate. For example, to use HTTPS to access a LAN port with IP address 192.168.1.1, create a certificate that uses 192.168.1.1 as the common name.
- b** Go to the remote management **WWW** screen and select the newly created certificate in the **Server Certificate** field. Click **Apply**.

Logon screen

After you accept the certificate, the BCM50a Integrated Router logon screen appears. The lock displayed in the bottom right of the browser status bar denotes a secure connection.

Figure 112 Logon screen (Internet Explorer)

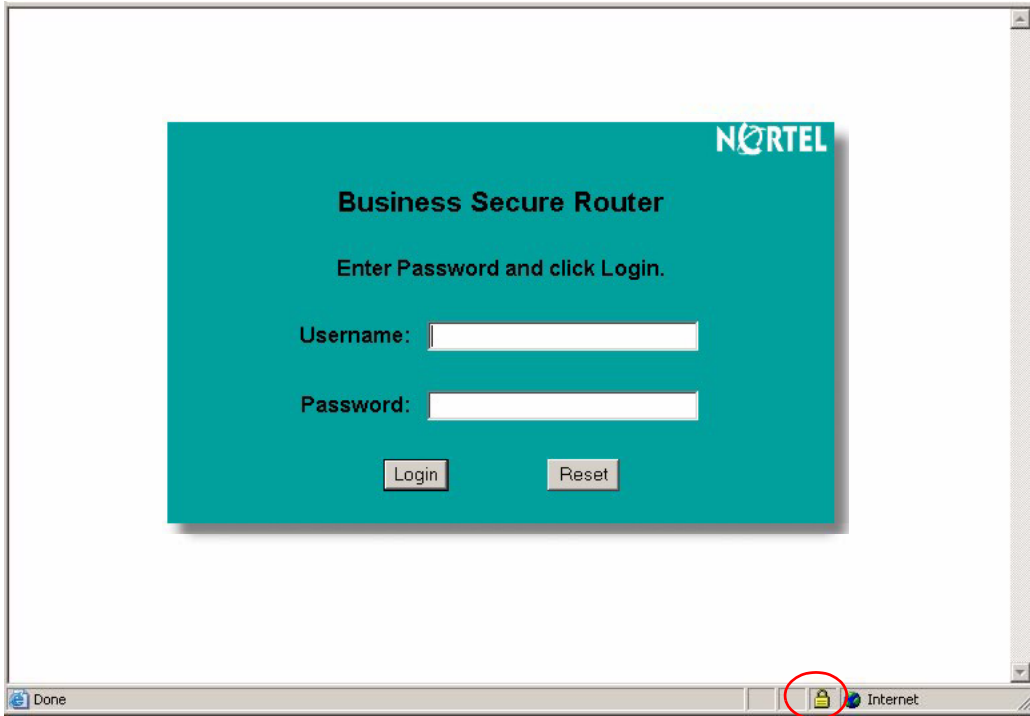
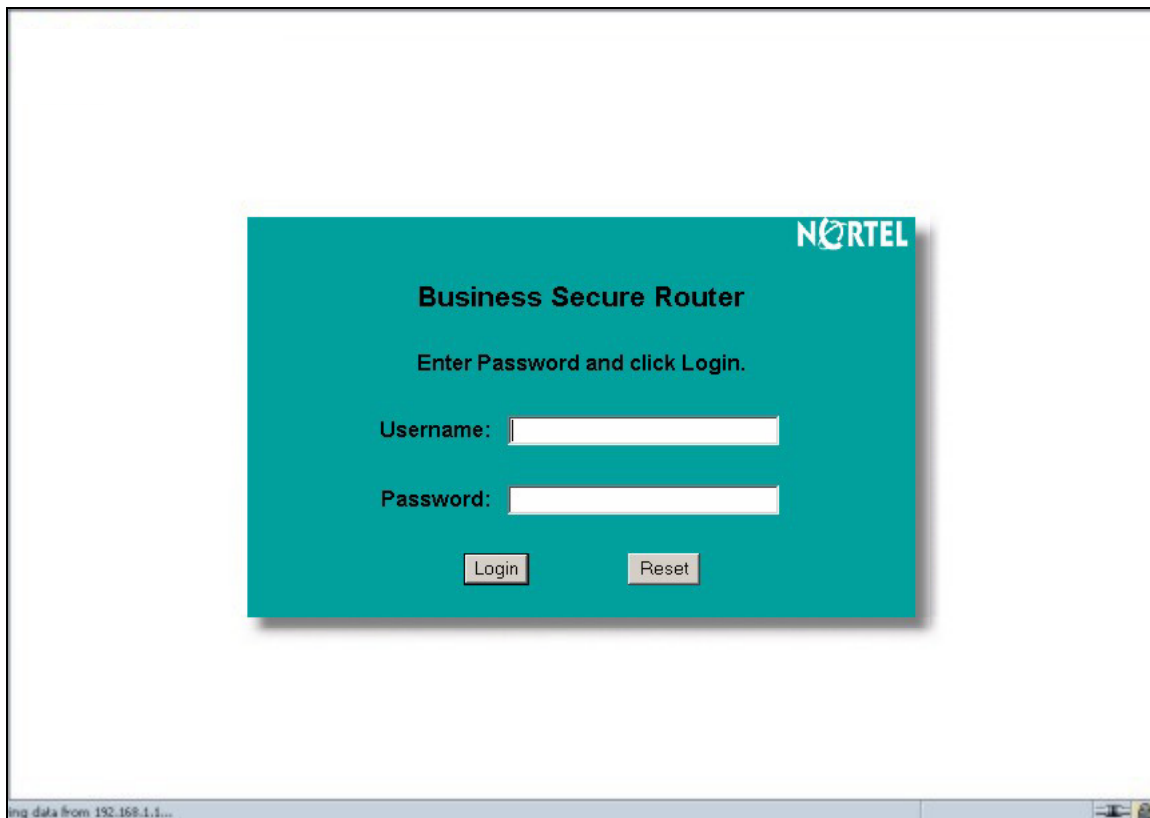


Figure 113 Login screen (Netscape)



Click **Login** to proceed. The screen shown in [Figure 114](#) appears.

The factory default certificate is a common default certificate for all BCM50a Integrated Router models.

Figure 114 Replace certificate

Click **Apply** in the **Replace Certificate** screen to create a certificate using your BCM50a Integrated Router MAC address that is specific to this device. Click **CERTIFICATES** to open the **My Certificates** screen. You see information similar to that shown in [Figure 115](#).

Figure 115 Device-specific certificate
CERTIFICATES

My Certificates Trusted CAs Trusted Remote Hosts Directory Servers

PKI Storage Space in Use

0% 12% 100%

My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Mo
1	auto_generated_self_signed_cert	SELF	CN=Business Secure Router 50 001349000001	CN=Business Secure Router 50 001349000001	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	

Import Create Refresh

Click **Ignore** in the **Replace Certificate** screen to use the common BCM50a Integrated Router certificate. The **My Certificates** screen appears (Figure 116).

Figure 116 Common BCM50a Integrated Router certificate

My Certificates
Trusted CAs
Trusted Remote Hosts
Directory Servers

PKI Storage Space in Use

0% 12% 100%

Replace Factory Default Certificate

Factory Default Certificate Name: auto_generated_self_signed_cert

The factory default certificate is common to Business Secure Router models. Click Replace to create a certificate using your Business Secure Router's MAC address that will be specific to this device.

My Certificates

#	Name	Type	Subject	Issuer	Valid From	Valid To	Modify
1	auto_generated_self_signed_cert	*SELF	CN=Business Secure Router Factory Default Certificate	CN=Business Secure Router Factory Default Certificate	2000 Jan 1st, 00:00:00 GMT	2030 Jan 1st, 00:00:00 GMT	

SSH overview

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

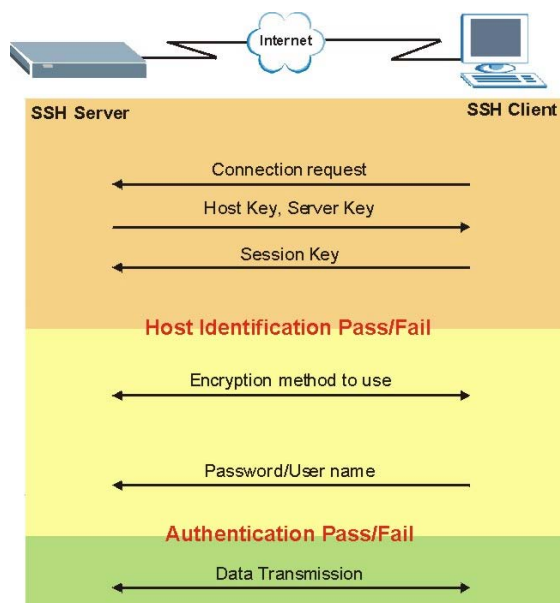
Figure 117 SSH Communication Example



How SSH works

Figure 118 summarizes how a secure connection is established between two remote hosts.

Figure 118 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (username and password) to the server to log on to the server.

SSH implementation on the BCM50a Integrated Router

Your BCM50a Integrated Router supports SSH version 1.5 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the BCM50a Integrated Router for remote SMT management and file transfer on port 22. Only one SSH connection is allowed at a time.

Requirements for using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the BCM50a Integrated Router over SSH.

Configuring SSH

To change the Secure Shell settings, click **REMOTE MGMT**, and then the **SSH** tab. The screen shown in [Figure 119](#) appears.

Figure 119 SSH
REMOTE MANAGEMENT

Table 88 describes the labels in Figure 119.

Table 88 SSH

Label	Description
Server Host Key	Select the certificate whose corresponding private key is to be used to identify the BCM50a Integrated Router for SSH connections. You must have certificates already configured in the My Certificates screen (Click My Certificates and see Chapter 14, "Certificates," on page 253 for details).
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the BCM50a Integrated Router using this service.
Secure Client IP Address	A secure client is a trusted computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.



Note: Nortel recommends that you disable Telnet and FTP when you configure SSH for secure connections.

Secure Telnet using SSH examples

This section shows two examples using a command interface and a graphical interface SSH client program to remotely access the BCM50a Integrated Router. The configuration and connection steps are similar for most SSH client programs. For more information about SSH client programs, refer to your SSH client program user's guide.

Example 1: Microsoft Windows

This section describes how to access the BCM50a Integrated Router using the Secure Shell Client program.

- 1 Launch the SSH client and specify the connection information (IP address, port number, or device name) for the BCM50a Integrated Router.
- 2 Configure the SSH client to accept connection using SSH version 1.
- 3 A window appears, prompting you to store the host key in you computer. Click **Yes** to continue.

Figure 120 SSH Example 1: Store Host Key



Enter the password to log on to the BCM50a Integrated Router. The SMT main menu appears.

Example 2: Linux

This section describes how to access the BCM50a Integrated Router using the OpenSSH client program that comes with most Linux distributions.

- 1 Test whether the SSH service is available on the BCM50a Integrated Router.

Enter “telnet 192.168.1.1 22” at a terminal prompt and press [ENTER]. The computer attempts to connect to port 22 on the BCM50a Integrated Router (using the default IP address of 192.168.1.1).

A message displays indicating the SSH protocol version supported by the BCM50a Integrated Router.

Figure 121 SSH Example 2: Test

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

- 2 Enter “ssh -1 192.168.1.1”. This command forces your computer to connect to the BCM50a Integrated Router using SSH version 1. If this is the first time you are connecting to the BCM50a Integrated Router using SSH, a message appears prompting you to save the host information of the BCM50a Integrated Router. Type yes and press [ENTER].

Enter the password to log on to the BCM50a Integrated Router.

Figure 122 SSH Example 2: Log on

```
$ ssh -l 192.168.1.1
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
```

- 3 The SMT main menu displays.

Secure FTP using SSH example

This section shows an example of file transfer using the OpenSSH client program. The configuration and connection steps are similar for other SSH client programs. For more information about using FTP, refer to your SSH client program user's guide.

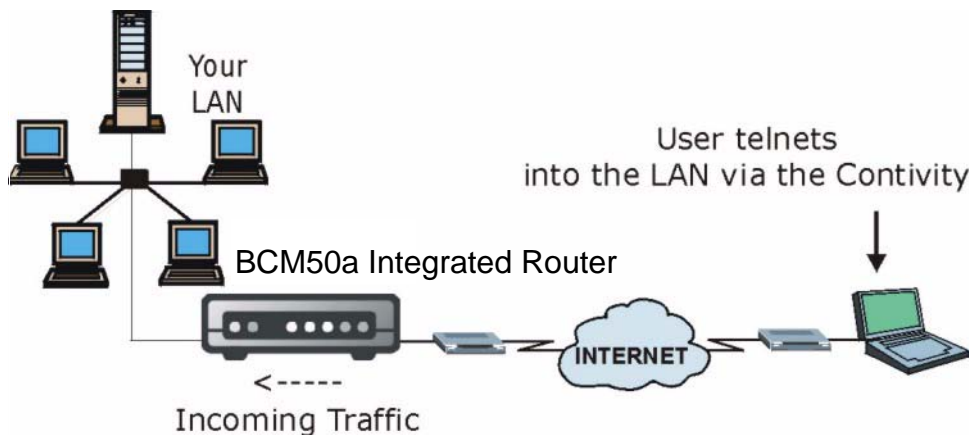
- 1 Enter `sftp -l 192.168.1.1`. This command forces your computer to connect to the BCM50a Integrated Router for secure file transfer using SSH version 1. If this is the first time you are connecting to the BCM50a Integrated Router using SSH, a message displays, prompting you to save the host information of the BCM50a Integrated Router. Type `yes` and press [ENTER].
- 2 Enter the password to log on to the BCM50a Integrated Router.
- 3 Use the `put` command to upload a new firmware to the BCM50a Integrated Router.

Figure 123 Secure FTP: Firmware Upload Example

```
$ sftp -l 192.168.1.1
Connecting to 192.168.1.1...
The authenticity of host '192.168.1.1 (192.168.1.1)' can't be
established.
RSA1 key fingerprint is
21:6c:07:25:7e:f4:75:80:ec:af:bd:d4:3d:80:53:d1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.1' (RSA1) to the list of
known hosts.
Administrator@192.168.1.1's password:
sftp> put firmware.bin ras
Uploading firmware.bin to /ras
Read from remote host 192.168.1.1: Connection reset by peer
Connection closed
$
```

Telnet

You can configure your BCM50a Integrated Router for remote Telnet access as shown in [Figure 124](#).

Figure 124 Telnet configuration on a TCP/IP network

Configuring TELNET

Click **REMOTE MANAGEMENT** to open the **TELNET** screen.

Figure 125 Telnet

REMOTE MANAGEMENT

The screenshot shows the TELNET configuration interface. At the top, there are navigation tabs: HTTP, SSH, TELNET, FTP, SNMP, DNS, and Security. The TELNET tab is selected. Below the tabs, the TELNET configuration options are displayed:

- Server Port:** A text input field containing the value '23'.
- Server Access:** A dropdown menu currently set to 'Disable'.
- Secured Client IP Address:** Two radio buttons are present: 'All' (which is unselected) and 'Selected' (which is selected). To the right of the 'Selected' radio button is a text input field containing the IP address '0.0.0.0'.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

[Table 89](#) describes the fields in [Figure 125](#).

Table 89 Telnet

Label	Description
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (If any) through which a computer can access the BCM50a Integrated Router using this service.
Secured Client IP Address	A secured client is a “trusted” computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Configuring FTP

You can upload and download the BCM50a Integrated Router firmware and configuration files using FTP. To use this feature, your computer must have an FTP client.

To change your BCM50a Integrated Router FTP settings, click **REMOTE MANAGEMENT**, and then the **FTP** tab. The screen appears as shown in [Figure 126](#).

Figure 126 FTP

REMOTE MANAGEMENT

The screenshot shows the 'REMOTE MANAGEMENT' configuration page with the 'FTP' tab selected. The configuration options are as follows:

- Server Port:** A text input field containing the value '21'.
- Server Access:** A dropdown menu currently set to 'Disable'.
- Secured Client IP:** Two radio buttons are present: 'All' (which is selected) and 'Selected'.
- Address:** A text input field containing the value '0.0.0.0'.

At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

[Table 90](#) describes the fields in [Figure 126](#).

Table 90 FTP

Label	Description
Server Port	You can change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Server Access	Select the interfaces (if any) through which a computer can access the BCM50a Integrated Router using this service.

Table 90 FTP

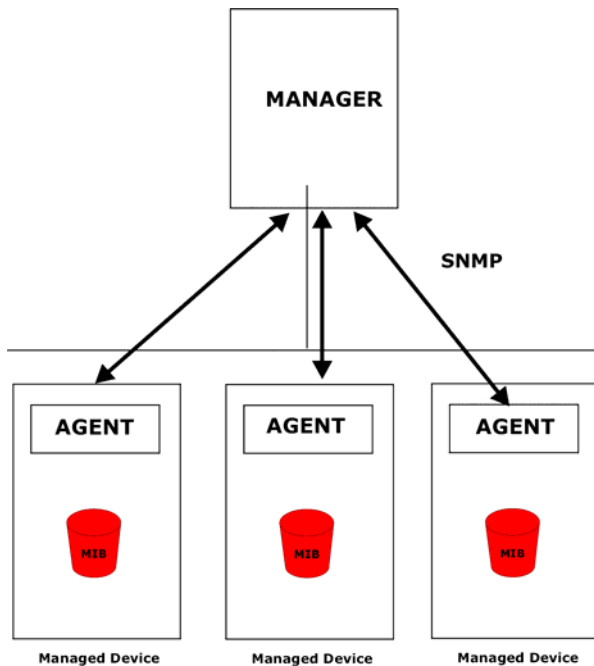
Label	Description
Secured Client IP Address	A secured client is a trusted computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Configuring SNMP

Simple Network Management Protocol is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. Your BCM50a Integrated Router supports SNMP-agent functionality, which allows a manager station to manage and monitor the BCM50a Integrated Router through the network. The BCM50a Integrated Router supports SNMP version 1 (SNMPv1). [Figure 127](#) illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured. The default get and set communities are public.



Note: SNMP is only available if TCP/IP is configured.

Figure 127 SNMP Management Model

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

An agent is a management software module that resides in a managed device (the BCM50a Integrated Router). 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 and managed objects that define each piece of information to be collected about a device. Examples of variables include number of packets received and node port status. 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 and response protocol based on the manager and 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.

Supported MIBs

The BCM50a Integrated Router supports MIB II, which is defined in RFC 1213 and RFC 1215. The focus of the MIBs is to let administrators collect statistical data and monitor status and performance.

SNMP Traps

The BCM50a Integrated Router sends traps to the SNMP manager when any one of the following events occurs:

Table 91 SNMP traps

Trap #	Trap Name	Description
0	coldStart (defined in <i>RFC 1215</i>)	A trap is sent after booting (power on).
1	warmStart (defined in <i>RFC 1215</i>)	A trap is sent after booting (software reboot).
4	authenticationFailure (defined in <i>RFC 1215</i>)	A trap is sent to the manager when receiving any SNMP get or set requirements with the wrong community (password).
6	whyReboot (defined in MIB)	A trap is sent with the reason of restart before rebooting when the system is going to restart (warm start).
6a	For intentional reboot:	A trap is sent with the message System reboot by user! if reboot is done intentionally, (for example, download new files, and CI command sys reboot).
6b	For fatal error:	A trap is sent with the message of the fatal code if the system reboots because of fatal errors.

REMOTE MANAGEMENT: SNMP

To change your BCM50a Integrated Router SNMP settings, click **REMOTE MANAGEMENT**, and then the **SNMP** tab. The screen appears as shown in [Figure 128](#).

Figure 128 SNMP

REMOTE MANAGEMENT

The screenshot shows the 'REMOTE MANAGEMENT' interface with the 'SNMP' tab selected. The configuration is organized into two main sections:

- SNMP Configuration:**
 - Get Community: [Text Input Field]
 - Set Community: [Text Input Field]
 - Trap Community: [Text Input Field]
 - Destination: [Text Input Field] (0.0.0.0)
- SNMP:**
 - Service Port: [Text Input Field] (161)
 - Service Access: [Dropdown Menu] (Disable)
 - Secured Client IP Address: [Radio Buttons] (All Selected) [Text Input Field] (0.0.0.0)

Buttons for 'Apply' and 'Reset' are located at the bottom of the configuration area.

[Table 92](#) describes the fields in [Figure 128](#).

Table 92 SNMP

Label	Description
SNMP Configuration	
Get Community	Enter the Get Community , which is the password for the incoming Get and GetNext requests from the management station. The default is "PlsChgMe!RO".
Set Community	Enter the Set community , which is the password for incoming Set requests from the management station. The default is "PlsChgMe!RW".

Table 92 SNMP

Label	Description
Trusted Host	If you enter a trusted host, your BCM50a Integrated Router only responds to SNMP messages from this address. In the field, 0.0.0.0 (default) means your BCM50a Integrated Router responds to all SNMP messages it receives, regardless of source.
Trap	
Community	Type the trap community, which is the password sent with each trap to the SNMP manager. The default is public and allows all requests.
Destination	Type the IP address of the station to send your SNMP traps to.
SNMP	
Service Port	You change the server port number for a service if needed, however, you must use the same port number in order to use that service for remote management.
Service Access	Select the interfaces (If any) through which a computer can access the BCM50a Integrated Router using this service.
Secured Client IP Address	A secured client is a trusted computer that is allowed to communicate with the BCM50a Integrated Router using this service. Select All to allow any computer to access the BCM50a Integrated Router using this service. Choose Selected to just allow the computer with the IP address that you specify to access the BCM50a Integrated Router using this service.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Configuring DNS

Use DNS (Domain Name System) to map a domain name to its corresponding IP address and vice versa, for example, the IP address of www.nortel.com is 47.249.48.20.

To change your BCM50a Integrated Router DNS settings, click **REMOTE MANAGEMENT**, and then the **DNS** tab. The screen appears as shown in [Figure 129](#).

Figure 129 DNS
REMOTE MANAGEMENT

The screenshot shows a web-based configuration interface for a BCM50a Integrated Router. At the top, there are seven tabs: HTTP, SSH, TELNET, FTP, SNMP, DNS, and Security. The 'DNS' tab is selected. Below the tabs, the title 'DNS' is displayed. The configuration area contains three main fields: 'Service Port' with a text input containing '53'; 'Service Access' with a dropdown menu showing 'LAN'; and 'Secured Client IP Address' with two radio buttons, 'All' (which is selected) and 'Selected', followed by a text input containing '0.0.0.0'. At the bottom of the configuration area, there are two buttons: 'Apply' and 'Reset'.

Table 93 describes the fields in Figure 129.

Table 93 DNS

Label	Description
Server Port	The DNS service port number is 53 and cannot be changed here.
Server Access	Select the interfaces (if any) through which a computer can send DNS queries to the BCM50a Integrated Router.
Secured Client IP Address	A secured client is a trusted computer that is allowed to send DNS queries to the BCM50a Integrated Router. Select All to allow any computer to send DNS queries to the BCM50a Integrated Router. Choose Selected to just allow the computer with the IP address that you specify to send DNS queries to the BCM50a Integrated Router.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Configuring Security

To change your BCM50a Integrated Router security settings, click **REMOTE MANAGEMENT**, and then the **Security** tab. The screen appears as shown in Figure 130.

If an outside user attempts to probe an unsupported port on your BCM50a Integrated Router, an ICMP response packet is automatically returned. This allows the outside user to know the BCM50a Integrated Router exists. The BCM50a Integrated Router series support antiprobing, which prevents the ICMP response packet from being sent. This keeps outsiders from discovering your BCM50a Integrated Router when unsupported ports are probed.



Note: In order to allow Ping on the WAN, you must also configure a WAN to WAN/ BCM50a Integrated Router rule that allows PING(ICMP:0) traffic.

Figure 130 Security
REMOTE MANAGEMENT

Table 94 describes the fields in Figure 130.

Table 94 Security

Label	Description
ICMP	Internet Control Message Protocol is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the TCP/IP software and directly apparent to the application user.
Respond to Ping on	The BCM50a Integrated Router does not respond to any incoming Ping requests when Disable is selected. Select LAN to reply to incoming LAN Ping requests. Select WAN to reply to incoming WAN Ping requests. Otherwise, select LAN & WAN to reply to both incoming LAN and WAN Ping requests.

Table 94 Security

Label	Description
Do not respond to requests for unauthorized services	Select this option to prevent hackers from finding the BCM50a Integrated Router by probing for unused ports. If you select this option, the BCM50a Integrated Router does not send ICMP response packets to port requests for unused ports, thus leaving the unused ports and the BCM50a Integrated Router unseen. If the firewall blocks a packet from the WAN, the BCM50a Integrated Router sends a TCP reset packet. Use the <code>sys firewall tcsrst rst off</code> command in the command interpreter if you want to stop the BCM50a Integrated Router from sending TCP reset packets.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Chapter 18

UPnP

This chapter introduces the Universal Plug and Play feature.

Universal Plug and Play overview

Universal Plug and Play (UPnP) is a distributed, open networking standard that uses TCP/IP for simple peer-to-peer network connectivity between devices. A UPnP device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about other devices on the network. In turn, a device can leave a network smoothly and automatically when it is no longer in use.

How do I know if I am using UPnP?

UPnP hardware is identified as an icon in the Network Connections folder (Windows XP). Each UPnP compatible device installed on your network appears as a separate icon. By selecting the icon of a UPnP device, you can access the information and properties of that device.

NAT Traversal

UPnP NAT traversal automates the process of allowing an application to operate through NAT. UPnP network devices can automatically configure network addressing, announce their presence in the network to other UPnP devices, and enable exchange of simple product and service descriptions. With NAT traversal, the device can do the following:

- Dynamic port mapping
- Learning public IP addresses
- Assigning lease times to mappings

Windows Messenger is an example of an application that supports NAT traversal and UPnP.

Cautions with UPnP

The automated nature of NAT traversal applications in establishing their own services and opening firewall ports can present network security issues. Network information and configuration can also be obtained and modified by users in some network environments.

All UPnP-enabled devices can communicate freely with each other without additional configuration. If this is not your intention, disable UPnP.

UPnP implementation

The device has UPnP certification from the Universal Plug and Play Forum Creates UPnP™ Implementers Corp. (UIC). This UPnP implementation supports IGD 1.0 (Internet Gateway Device). At the time of writing, the UPnP implementation supports Windows Messenger 4.6 and 4.7 while Windows Messenger 5.0 and Xbox are still being tested.

The BCM50a Integrated Router only sends UPnP multicasts to the LAN.

Configuring UPnP

Click **UPnP** to display the screen shown in [Figure 131](#).

Figure 131 Configuring UPnP
UPnP

The screenshot shows a web configuration interface for UPnP. At the top, there are two tabs: 'UPnP' and 'Ports'. The 'UPnP' tab is active. Below the tabs, the 'Device Name' is set to 'Business Secure Router'. There are three checkboxes: 'Enable the Universal Plug and Play (UPnP) feature' (unchecked), 'Allow users to make configuration changes through UPnP' (unchecked), and 'Allow UPnP to pass through Firewall' (unchecked). A note below the checkboxes states: 'Note: For UPnP to function normally, the [HTTP](#) service must be available for LAN computers using UPnP.' At the bottom of the form are two buttons: 'Apply' and 'Reset'.

Table 95 describes the fields in Figure 131.

Table 95 Configuring UPnP

Label	Description
Device Name	This identifies the device in UPnP applications.
Enable the Universal Plug and Play (UPnP) feature	Select this check box to activate UPnP. Be aware that anyone can use a UPnP application to open the WebGUI's logon screen without entering the BCM50a Integrated Router's IP address (although you must still enter the password to access the WebGUI).
Allow users to make configuration changes through UPnP	Select this check box to allow UPnP-enabled applications to automatically configure the BCM50a Integrated Router so that they can communicate through the BCM50a Integrated Router. For example, by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; eliminating the need to manually configure port forwarding for the UPnP enabled application.
Allow UPnP to pass through firewall	Select this check box to allow traffic from UPnP-enabled applications to bypass the firewall. Clear this check box to have the firewall block all UPnP application packets (for example, MSN packets).

Table 95 Configuring UPnP

Label	Description
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

Displaying UPnP port mapping

Click **UPnP** and then **Ports** to display the screen as shown in [Figure 132](#). Use this screen to view the NAT port mapping rules that UPnP creates on the BCM50a Integrated Router.

Figure 132 UPnP Ports

[Table 96](#) describes the labels in [Figure 132](#).

Table 96 UPnP Ports

Label	Description
Retain UPnP port forwarding	Select this check box to have the BCM50a Integrated Router retain UPnP created NAT rules even after restarting. If you use UPnP and you set a port on your computer to be fixed for a specific service (for example, FTP for file transfers), the BCM50a Integrated Router can keep a record when your computer uses UPnP to create a NAT forwarding rule for that service.
The following read-only table displays information about the UPnP-created NAT mapping rule entries in the NAT routing table.	

Table 96 UPnP Ports

Label	Description
#	This is the index number of the UPnP-created NAT mapping rule entry.
Remote Host	This field displays the source IP address (on the WAN) of inbound IP packets. Because this is often a wildcard, the field can be blank. When the field is blank, the BCM50a Integrated Router forwards all traffic sent to the External Port on the WAN interface to the Internal Client on the Internal Port . When this field displays an external IP address, the NAT rule has the BCM50a Integrated Router forward inbound packets to the Internal Client from that IP address only.
External Port	This field displays the port number that the BCM50a Integrated Router listens on (on the WAN port) for connection requests destined for the Internal Port and Internal Client of the NAT rule. The BCM50a Integrated Router forwards incoming packets (from the WAN) with this port number to the Internal Client on the Internal Port (on the LAN). If the field displays "0", the BCM50a Integrated Router ignores the Internal Port value and forwards requests on all external port numbers (that are otherwise unmapped) to the Internal Client .
Protocol	This field displays the protocol of the NAT mapping rule (TCP or UDP).
Internal Port	This field displays the port number on the Internal Client to which the BCM50a Integrated Router forwards incoming connection requests.
Internal Client	This field displays the DNS host name or IP address of a client on the LAN. Multiple NAT clients can use a single port simultaneously if the internal client field is set to 255.255.255.255 for UDP mappings.
Enabled	This field displays whether or not this UPnP-created NAT mapping rule is turned on. The UPnP-enabled device that connected to the BCM50a Integrated Router and configured the UPnP-created NAT mapping rule on the BCM50a Integrated Router determines whether or not the rule is enabled.
Description	This field displays a text explanation of the NAT mapping rule.
Lease Duration	This field displays the time to live (in seconds) for a dynamic port-mapping rule. It displays "0" if the port mapping is static.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Refresh	Click Refresh to update the table.

Installing UPnP in Windows example

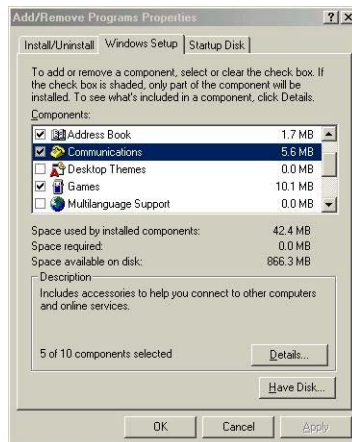
This section shows how to install UPnP in Windows Me and Windows XP.

Installing UPnP in Windows Me

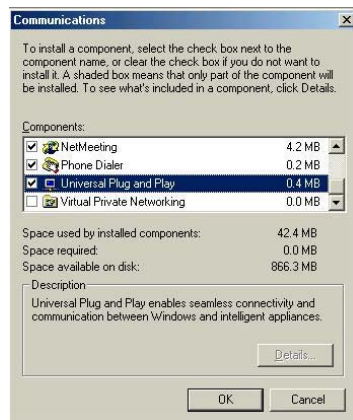
Follow the steps below to install UPnP in Windows Me.

- 1 Click **Start** and **Control Panel**. Double-click **Add/Remove Programs**.
- 2 Click on the **Windows Setup** tab and select **Communication** in the **Components** selection box. Click **Details**.

Figure 133 Add/Remove programs: Windows setup



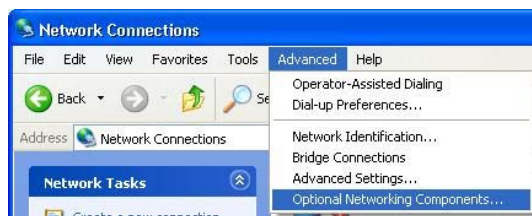
- 3 In the **Communications** window, select the **Universal Plug and Play** check box in the **Components** selection box.
- 4 Click **OK** to return to the **Add/Remove Programs Properties** window and click **Next**.
- 5 Restart the computer when prompted.

Figure 134 Communications

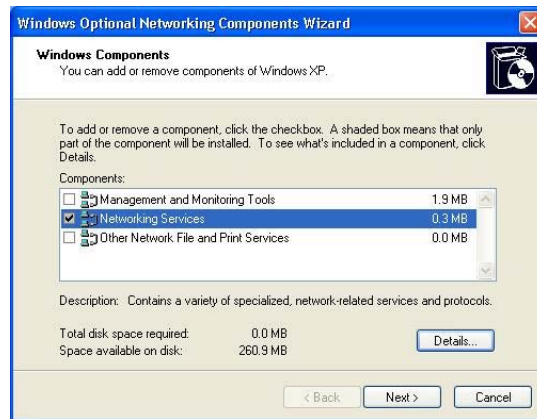
Installing UPnP in Windows XP

Follow the steps below to install UPnP in Windows XP.

- 1 Click **Start** and **Control Panel**.
- 2 Double-click **Network Connections**.
- 3 In the **Network Connections** window, click **Advanced** in the main menu and select **Optional Networking Components**
 The **Windows Optional Networking Components Wizard** window appears.

Figure 135 Network connections

- 4 Select **Networking Service** in the **Components** selection box and click **Details**.

Figure 136 Windows optional networking components wizard

- 5 In the **Networking Services** window, select the **Universal Plug and Play** check box.

Figure 137 Windows XP networking services

- 6 Click **OK** to return to the **Windows Optional Networking Component Wizard** window and click **Next**.

Using UPnP in Windows XP example

This section shows you how to use the UPnP feature in Windows XP. You must already have UPnP installed in Windows XP and UPnP activated on the device.

Make sure the computer is connected to a LAN port of the device. Turn on your computer and the BCM50a Integrated Router.

Autodiscover Your UPnP-enabled Network Device

- 1 Click **Start** and **Control Panel**. Double-click **Network Connections**. An icon displays under Internet Gateway.
- 2 Right-click the icon and select **Properties**.

Figure 138 Internet gateway icon



- 3 In the **Internet Connection Properties** window, click **Settings** to see the port mappings that were automatically created.

Figure 139 Internet connection properties



- 4 You can edit or delete the port mappings or click **Add** to manually add port mappings.

Figure 140 Internet connection properties advanced setup

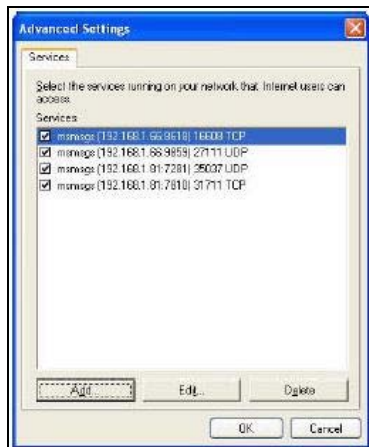
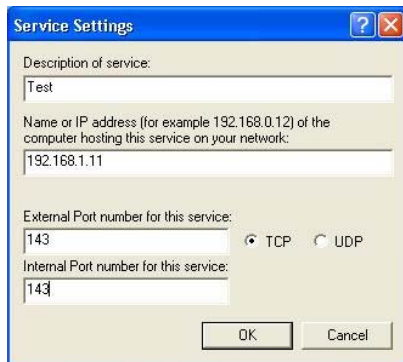


Figure 141 Service settings



Note: When the UPnP-enabled device is disconnected from your computer, all port mappings are deleted automatically.

- 5 Select the **Show icon in notification area when connected** check box and click **OK**. An icon displays in the system tray.

Figure 142 Internet connection icon



- 6 Double-click the icon to display your current Internet connection status.

Figure 143 Internet connection status



WebGUI easy access

With UPnP, you can access the WebGUI without first finding out its IP address. This is helpful if you do not know the IP address of your BCM50a Integrated Router.

Follow the steps below to access the WebGUI.

- 1 Click **Start** and then **Control Panel**.
- 2 Double-click **Network Connections**.

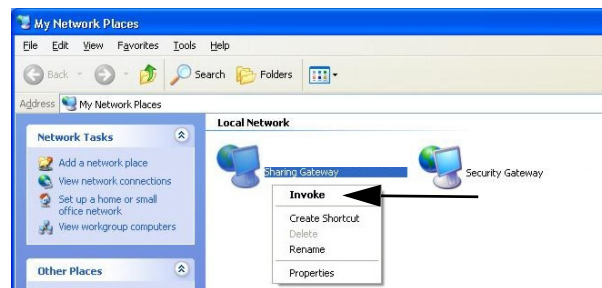
3 Select My Network Places under Other Places

Figure 144 Network connections



- 4 An icon with the description for each UPnP-enabled device displays under **Local Network**.
- 5 Right-click the icon for your BCM50a Integrated Router and select **Invoke**. The WebGUI logon screen displays.

Figure 145 My Network Places: Local network



Chapter 19

Logs Screens

This chapter contains information about configuring general log settings and viewing the BCM50a Integrated Router logs. Refer to [Appendix B, “Log Descriptions,”](#) on page 413 for example log message explanations.

Configuring View Log

With the WebGUI, you can look at all of the BCM50a Integrated Router logs in one location.

Click **LOGS** to open the **View Log** screen. Use the **View Log** screen to see the logs for the categories that you selected in the **Log Settings** screen (see [“Configuring Log settings”](#) on page 361). Options include logs about system maintenance, system errors, access control, allowed or blocked Web sites, blocked Web features (such as ActiveX controls, Java and cookies), attacks (such as DoS), and IPSec.

Log entries in red indicate system error logs. The log wraps around and deletes the old entries after it fills. Click a column heading to sort the entries. A triangle indicates ascending or descending sort order.

Figure 146 View Log
LOGS

The screenshot shows a web interface with three tabs: "View Log" (selected), "Log Settings", and "Reports". Below the tabs is a "Display" dropdown menu set to "All Logs", and three buttons: "Email Log Now", "Refresh", and "Clear Log". The main content is a table with the following data:

#	Time ▲	Message	Source	Destination	Note
1	02/21/2006 06:33:52	Successful HTTP login	192.168.1.3		User:admin
2	02/21/2006 06:33:46	HTTP login failed	192.168.1.3		User:admin
3	02/21/2006 06:33:37	Successful TELNET login	192.168.1.3		User:admin
4	02/21/2006 06:33:35	TELNET login failed	192.168.1.3		User:admin

Table 97 describes the fields in Figure 146.

Table 97 View Log

Label	Description
Display	The categories that you select in the Log Settings page display in the drop-down list. Select a category of logs to view; select All Logs to view logs from all of the log categories that you selected in the Log Settings page.
Time	This field displays the time the log was recorded. Refer to " Configuring Time and Date " on page 84 for information about configuring the time and date.
Message	This field states the reason for the log.
Source	This field lists the source IP address and the port number of the incoming packet.
Destination	This field lists the destination IP address and the port number of the incoming packet.
Note	This field displays additional information about the log entry.
Email Log Now	Click Email Log Now to send the log screen to the e-mail address specified in the Log Settings page (make sure that you have first filled in the Address Info fields in Log Settings).

Table 97 View Log

Label	Description
Refresh	Click Refresh to renew the log screen.
Clear Log	Click Clear Log to delete all the logs.

Configuring Log settings

To change your BCM50a Integrated Router log settings, click **Logs**, then the **Log Settings** tab. The screen appears as shown in [Figure 147](#).

Use the **Log Settings** screen to configure to where the BCM50a Integrated Router sends logs; the schedule for when the BCM50a Integrated Router is to send the logs and which logs and immediate alerts the BCM50a Integrated Router is to send.

An alert is a type of log that warrants more serious attention including system errors, attacks (access control), and attempted access to blocked Web sites or Web sites with restricted Web features such as cookies or Active X. Some categories, such as **System Errors**, consist of both logs and alerts. You can differentiate between logs and alerts by their color in the **View Log** screen. Alerts display in red and logs display in black.



Note: Alerts are e-mailed as soon as they happen. Logs can be e-mailed as soon as the log is full. Selecting many alert and log categories (especially Access Control) can result in many e-mails being sent.

Figure 147 Log settings

LOGS

View Log	Log Settings	Reports																																								
Address Info																																										
Mail Server	<input type="text"/>	(Outgoing SMTP Server Name or IP Address)																																								
Server Port:	<input type="text" value="0"/>	(SMTP Server Port Number)																																								
Mail Subject	<input type="text"/>																																									
Send Log to	<input type="text"/>	(E-Mail Address)																																								
Send Alerts to	<input type="text"/>	(E-Mail Address)																																								
Syslog Logging																																										
<input type="checkbox"/> Active																																										
Syslog Server	<input type="text" value="0.0.0.0"/>	(Server Name or IP Address)																																								
Log Facility	<input type="text" value="Local 1"/>																																									
Send Log																																										
Log Schedule	<input type="text" value="None"/>																																									
Day for Sending Log	<input type="text" value="Sunday"/>																																									
Time for Sending Log	<input type="text" value="0"/> (Hour): <input type="text" value="0"/> (Minute)																																									
<table border="0"> <thead> <tr> <th>Log</th> <th>Send Immediate Alert</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> System Maintenance</td> <td><input type="checkbox"/> System Errors</td> </tr> <tr> <td><input checked="" type="checkbox"/> System Errors</td> <td><input type="checkbox"/> Access Control</td> </tr> <tr> <td><input checked="" type="checkbox"/> Access Control</td> <td><input type="checkbox"/> Blocked Web Sites</td> </tr> <tr> <td><input checked="" type="checkbox"/> TCP Reset</td> <td><input type="checkbox"/> Blocked Java etc.</td> </tr> <tr> <td><input checked="" type="checkbox"/> Packet Filter</td> <td><input type="checkbox"/> Attacks</td> </tr> <tr> <td><input checked="" type="checkbox"/> ICMP</td> <td><input type="checkbox"/> IPSec</td> </tr> <tr> <td><input checked="" type="checkbox"/> Remote Management</td> <td><input type="checkbox"/> IKE</td> </tr> <tr> <td><input checked="" type="checkbox"/> Call Record</td> <td><input type="checkbox"/> PKI</td> </tr> <tr> <td><input checked="" type="checkbox"/> PPP</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> UPnP</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Forward Web Sites</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Blocked Web Sites</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Blocked Java etc.</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> Attacks</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> IPSec</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> IKE</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> PKI</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> SSL/TLS</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/> 802.1X</td> <td></td> </tr> </tbody> </table>			Log	Send Immediate Alert	<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors	<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites	<input checked="" type="checkbox"/> TCP Reset	<input type="checkbox"/> Blocked Java etc.	<input checked="" type="checkbox"/> Packet Filter	<input type="checkbox"/> Attacks	<input checked="" type="checkbox"/> ICMP	<input type="checkbox"/> IPSec	<input checked="" type="checkbox"/> Remote Management	<input type="checkbox"/> IKE	<input checked="" type="checkbox"/> Call Record	<input type="checkbox"/> PKI	<input checked="" type="checkbox"/> PPP		<input checked="" type="checkbox"/> UPnP		<input checked="" type="checkbox"/> Forward Web Sites		<input checked="" type="checkbox"/> Blocked Web Sites		<input checked="" type="checkbox"/> Blocked Java etc.		<input checked="" type="checkbox"/> Attacks		<input checked="" type="checkbox"/> IPSec		<input checked="" type="checkbox"/> IKE		<input checked="" type="checkbox"/> PKI		<input checked="" type="checkbox"/> SSL/TLS		<input checked="" type="checkbox"/> 802.1X	
Log	Send Immediate Alert																																									
<input checked="" type="checkbox"/> System Maintenance	<input type="checkbox"/> System Errors																																									
<input checked="" type="checkbox"/> System Errors	<input type="checkbox"/> Access Control																																									
<input checked="" type="checkbox"/> Access Control	<input type="checkbox"/> Blocked Web Sites																																									
<input checked="" type="checkbox"/> TCP Reset	<input type="checkbox"/> Blocked Java etc.																																									
<input checked="" type="checkbox"/> Packet Filter	<input type="checkbox"/> Attacks																																									
<input checked="" type="checkbox"/> ICMP	<input type="checkbox"/> IPSec																																									
<input checked="" type="checkbox"/> Remote Management	<input type="checkbox"/> IKE																																									
<input checked="" type="checkbox"/> Call Record	<input type="checkbox"/> PKI																																									
<input checked="" type="checkbox"/> PPP																																										
<input checked="" type="checkbox"/> UPnP																																										
<input checked="" type="checkbox"/> Forward Web Sites																																										
<input checked="" type="checkbox"/> Blocked Web Sites																																										
<input checked="" type="checkbox"/> Blocked Java etc.																																										
<input checked="" type="checkbox"/> Attacks																																										
<input checked="" type="checkbox"/> IPSec																																										
<input checked="" type="checkbox"/> IKE																																										
<input checked="" type="checkbox"/> PKI																																										
<input checked="" type="checkbox"/> SSL/TLS																																										
<input checked="" type="checkbox"/> 802.1X																																										
Log Consolidation																																										
<input checked="" type="checkbox"/> Active																																										
Log Consolidation Period	<input type="text" value="10"/>	1 ~ 600 (Seconds)																																								
<input type="button" value="Apply"/> <input type="button" value="Reset"/>																																										

Table 98 describes the fields in Figure 147.

Table 98 Log settings

Label	Description
Address Info	
Mail Server	Enter the server name or the IP address of the mail server for the e-mail addresses specified below. If this field is left blank, logs and alert messages are not sent through e-mail.
Server Port	Enter the port number that the mail server uses.
Mail Subject	Type a title that you want to be in the subject line of the log e-mail message that the BCM50a Integrated Router sends.
Send Log To	Logs are sent to the e-mail address specified in this field. If this field is left blank, logs are not sent through e-mail.
Send Alerts To	Alerts are sent to the e-mail address specified in this field. If this field is left blank, alerts are not sent through e-mail.
Syslog Logging	Syslog logging sends a log to an external syslog server used to store logs.
Active	Click Active to enable syslog logging.
Syslog Server IP Address	Enter the server name or IP address of the syslog server that logs the selected categories of logs.
Log Facility	Select a location from the drop-down list. In the log facility, you can log the messages to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Send Log	
Log Schedule	This drop-down menu is used to configure the frequency of log messages being sent as e-mail: Daily Weekly Hourly When the Log is Full None If you select Weekly or Daily , specify a time of day when the e-mail will be sent. If you select Weekly , you must also specify which day of the week the e-mail is to be sent. If you select When Log is Full , an alert is sent when the log fills up. If you select None , no log messages are sent.
Day for Sending Log	Use the drop-down list to select which day of the week to send the logs.

Table 98 Log settings

Label	Description
Time for Sending Log	Enter the time of the day in 24-hour format (for example 23:00 equals 11:00 p.m.) to send the logs.
Log	Select the categories of the logs that you want to record. Logs include alerts. ¹
Send Immediate Alert	Select the categories of alerts for which you want the BCM50a Integrated Router to instantly e-mail alerts to the e-mail address specified in the Send Alerts To field.
Log Consolidation	
Active	Some logs (such as the Attacks logs) can be so numerous that it becomes easy to ignore other important log messages. Select this check box to merge logs with identical messages into one log. You can use the <code>sys log consolidate msglist</code> command to see which log messages are consolidated.
Log Consolidation Period	Specify the time interval during which to merge logs with identical messages into one log.
Apply	Click Apply to save your customized settings and exit this screen.
Reset	Click Reset to begin configuring this screen afresh.

¹ 802.1x logs are not available in this release.

Configuring Reports

To change your BCM50a Integrated Router log reports, click **Logs**, and then the **Reports** tab. The screen appears as shown in [Figure 148](#).

The **Reports** page displays which computers on the LAN send and receive the most traffic, what kinds of traffic are used the most, and which Web sites are visited the most often. Use the **Reports** screen to have the BCM50a Integrated Router record and display the following network usage details:

- Web sites visited the most often
- Number of times the most visited Web sites were visited
- The most-used protocols or service ports
- The amount of traffic for the most used protocols or service ports

- The LAN IP addresses to and from which the most traffic has been sent
- How much traffic has been sent to and from the LAN IP addresses to and from which the most traffic has been sent



Note: The Web site hit count not be 100% accurate because sometimes when an individual Web page loads, it can contain references to other Web sites that also get counted as hits.

The BCM50a Integrated Router records Web site hits by counting the HTTP GET packets. Many Web sites include HTTP GET references to other Web sites and the BCM50a Integrated Router can count these as hits, thus the Web hit count is not (yet) 100% accurate.

Figure 148 Reports

LOGS

Setup

Collect Statistics
 Send Raw Traffic Statistics to Syslog Server for Analysis

Apply Reset

Statistics Report

Report Type: Web Site Hits Refresh Flush

#	Web Site	Hits
1	ad.doubleclick.net	2
2	en.wikipedia.org	1
3	m2.2mdn.net	1
4	pagead2.google syndication.com	1
5	m3.doubleclick.net	1
6	www.google.com.tw	1
7	www.google.com	1
8	www.webopedia.com	1



Note: Enabling the reporting function decreases the overall throughput by about 1 Mb/s.

Table 99 describes the fields in Figure 148.

Table 99 Reports

Label	Description
Collect Statistics	Select the check box and click Apply to have the BCM50a Integrated Router record report data.
Send Raw Traffic Statistics to Syslog Server for Analysis	Select the check box and click Apply to have the BCM50a Integrated Router send unprocessed traffic statistics to a syslog server for analysis. You must have the syslog server already configured in the Log Settings screen.

Table 99 Reports

Label	Description
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Reset	Click Reset to begin configuring this screen afresh.
Report Type	Use the drop-down list to select the type of reports to display. Web Site Hits displays the Web sites that have been visited the most often from the LAN and how many times they have been visited. Protocol/Port displays the protocols or service ports that have been used the most and the amount of traffic for the most used protocols or service ports. LAN IP Address displays the LAN IP addresses to and from which the most traffic has been sent and how much traffic has been sent to and from those IP addresses.
Refresh	Click Refresh to update the report display. The report also refreshes automatically when you close and reopen the screen.
Flush	Click Flush to discard the old report data and update the report display.



Note: All of the recorded reports data is erased when you turn off the BCM50a Integrated Router.

Viewing Web site hits

In the Reports screen, select **Web Site Hits** from the **Report Type** drop-down list to have the BCM50a Integrated Router record and display which Web sites have been visited the most often and how many times they have been visited.

Figure 149 Web site hits report example
LOGS

The screenshot shows a web interface with three tabs: 'View Log', 'Log Settings', and 'Reports'. The 'Reports' tab is active. Under the 'Setup' section, there are two checkboxes: 'Collect Statistics' (checked) and 'Send Raw Traffic Statistics to Syslog Server for Analysis' (unchecked). Below these are 'Apply' and 'Reset' buttons. The 'Statistics Report' section has a 'Report Type' dropdown menu set to 'Web Site Hits', with 'Refresh' and 'Flush' buttons to its right. Below this is a table with the following data:

#	Web Site	Hits
1	ad.doubleclick.net	2
2	en.wikipedia.org	1
3	m2.2mdn.net	1
4	pagead2.google syndication.com	1
5	m3.doubleclick.net	1
6	www.google.com.tw	1
7	www.google.com	1
8	www.webopedia.com	1

Table 100 describes the fields in Figure 149.

Table 100 Web site hits report

Label	Description
Web Site	This column lists the domain names of the Web sites visited most often from computers on the LAN. The names are ranked by the number of visits to each Web site and listed in descending order with the most visited Web site listed first. The BCM50a Integrated Router counts each page viewed in a Web site as another hit on the Web site.
Hits	This column lists how many times each Web site has been visited. The count starts over at 0 if a Web site passes the hit count limit.

Viewing Protocol/Port

In the **Reports** screen, select **Protocol/Port** from the **Report Type** drop-down list to have the BCM50a Integrated Router record and display which protocols or service ports have been used the most and the amount of traffic for the most used protocols or service ports.

Figure 150 Protocol/Port report example
LOGS

The screenshot shows the 'Reports' tab in a web interface. Under the 'Setup' section, there are two checkboxes: 'Collect Statistics' (checked) and 'Send Raw Traffic Statistics to Syslog Server for Analysis' (unchecked). Below these are 'Apply' and 'Reset' buttons. The 'Statistics Report' section features a 'Report Type' dropdown menu set to 'Protocol / Port', along with 'Refresh' and 'Flush' buttons. A table displays the following data:

#	Protocol / Port	Direction	Amount
1	HTTP(TCP:80)	Incoming	2610 (bytes)
2	HTTP(TCP:80)	Outgoing	1217 (bytes)
3	DNS (TCP/UDP:53)	Incoming	255 (bytes)
4	DNS (TCP/UDP:53)	Outgoing	123 (bytes)

Table 101 describes the fields in Figure 150.

Table 101 Protocol/ Port Report

Label	Description
Protocol/Port	This column lists the protocols or service ports for which the most traffic has gone through the BCM50a Integrated Router. The protocols or service ports are listed in descending order with the most used protocol or service port listed first.
Direction	This column lists the direction of travel of the traffic belonging to each protocol or service port listed. Incoming refers to traffic that is coming into the BCM50a Integrated Router LAN from the WAN. Outgoing refers to traffic that is going out from the BCM50a Integrated Router LAN to the WAN.
Amount	This column lists how much traffic has been sent and received for each protocol or service port. The measurement unit shown (bytes, Kilobytes, Megabytes or Gigabytes) varies with the amount of traffic for the particular protocol or service port. The count starts over at 0 if a protocol or port passes the bytes count limit (see Table 103 on page 372).

Viewing LAN IP address

In the **Reports** screen, select **LAN IP Address** from the **Report Type** drop-down list to have the BCM50a Integrated Router record and display the LAN IP addresses that the most traffic has been sent to and from and how much traffic has been sent to and from those IP addresses.



Note: Computers take turns using dynamically assigned LAN IP addresses. The BCM50a Integrated Router continues recording the bytes sent to or from a LAN IP address when it is assigned to a different computer.

Figure 151 LAN IP address report example
LOGS

Setup

Collect Statistics
 Send Raw Traffic Statistics to Syslog Server for Analysis

Apply Reset

Statistics Report

Report Type: LAN IP Address Refresh Flush

#	IP Address	Direction	Amount
1	192.168. 1. 3	Incoming	382170 (bytes)
2	192.168. 1. 3	Outgoing	52386 (bytes)

Table 102 describes the fields in Figure 151.

Table 102 LAN IP Address Report

Label	Description
IP Address	This column lists the LAN IP addresses to and from which the most traffic has been sent. The LAN IP addresses are listed in descending order with the LAN IP address to and from which the most traffic was sent listed first.
Amount	This column displays how much traffic has gone to and from the listed LAN IP addresses. The measurement unit shown (bytes, Kilobytes, Megabytes or Gigabytes) varies with the amount of traffic sent to and from the LAN IP address. The count starts over at 0 if the total traffic sent to and from a LAN IP passes the bytes count limit (see Table 103 on page 372).

Reports specifications

[Table 103](#) lists detailed specifications on the reports feature.

Table 103 Report Specifications

Label	Description
Number of Web sites/protocols or ports/IP addresses listed:	20
Hit count limit:	Up to 2^{32} hits can be counted per Web site. The count starts over at 0 if it passes four billion.
Bytes count limit:	Up to 2^{64} bytes can be counted per protocol/port or LAN IP address. The count starts over at 0 if it passes 2^{64} bytes.

Chapter 20

Call scheduling screens

With call scheduling (applicable for PPPoA or PPPoE encapsulation only), you can dictate when a remote node is to be called and for how long.

Call scheduling introduction

Using the call scheduling feature, the BCM50a Integrated Router can manage a remote node and dictate when a remote node is to be called and for how long. This feature is similar to the scheduler in a video cassette recorder (you can specify a time period for the VCR to record). Apply schedule sets in the **WAN IP** screen .

Lower numbered sets take precedence over higher numbered sets, thereby avoiding scheduling conflicts. For example, if sets 1, 2, 3, and 4 are applied in the remote node, set 1 takes precedence over set 2, 3, and 4 as the BCM50a Integrated Router, by default, applies the lowest numbered set first. Set 2 takes precedence over sets 3 and 4.

You can design up to 12 schedule sets. You can apply up to four schedule sets for a remote node.

Call schedule summary

Click **CALL SCHEDULE** to open the **Call Schedule Summary** screen.

Figure 152 Call schedule summary
CALL SCHEDULE

Summary									
#	Name	Active	How Often	Start Date	Week Day	Start Time	Duration Time	Action	
1	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-
4	-	-	-	-	-	-	-	-	-
5	-	-	-	-	-	-	-	-	-
6	-	-	-	-	-	-	-	-	-
7	-	-	-	-	-	-	-	-	-
8	-	-	-	-	-	-	-	-	-
9	-	-	-	-	-	-	-	-	-
10	-	-	-	-	-	-	-	-	-
11	-	-	-	-	-	-	-	-	-
12	-	-	-	-	-	-	-	-	-

Table 104 describes the fields in Figure 152.

Table 104 Call Schedule Summary

Label	Description
#	This is the call schedule set number.
Name	This field displays the name of the call schedule set.
Active	This field shows whether the call schedule set is turned on (Yes) or off (No).
Start Date	This is the date (in year-month-day format) that the call schedule set takes effect.
Duration Date	This is the date (in year-month-day format) that the call schedule set ends.

Table 104 Call Schedule Summary

Label	Description
Start Time	This is the time (in hour-minute format) when the schedule set takes effect.
Duration Time	This is the maximum length of time (in hour-minute format) that the schedule set applies the action displayed in the Action field.
Action	Forced On means that the connection is maintained whether or not there is a demand call on the line and persists for the time period specified in the Duration field. Forced Down means that the connection is blocked whether or not there is a demand call on the line. Enable Dial-On-Demand means that this schedule permits a demand call on the line. Disable Dial-On-Demand means that this schedule prevents a demand call on the line.
Edit	Click Edit to change a call schedule set.
Delete	Select the a call schedule set's radio button and click Delete to remove that call schedule set.

Call scheduling edit

To configure a schedule set, click the **Edit** button to display the screen shown in [Figure 153](#).

Figure 153 Call schedule edit

CALL SCHEDULE - EDIT

The screenshot shows a dialog box titled "Edit Set" with the following fields and controls:

- Schedule Name:** A text input field.
- Active:** A checkbox.
- How Often:** A dropdown menu set to "Once".
- Start Time (24-Hour Format):** Three input fields showing "2000 / 1 / 1".
- Duration Time (24-Hour Format):** Two input fields showing "0 (hour) 0 (min)".
- Action:** A dropdown menu set to "Forced On".
- Buttons:** "Apply" and "Cancel" buttons at the bottom.

If a connection has been already established, your BCM50a Integrated Router will not drop it. After the connection is dropped manually or it times out, that remote node can not be triggered again until the end of the **Duration**.

Table 105 Call schedule edit

Label	Description
Schedule Name	Enter a name (up to 16 characters) for the call schedule set. You can use numbers, the letters A-Z (upper or lower case) and the underscore (_) and @ symbols.
Active	Select this check box to turn on this call schedule set. Clear this check box to turn this call schedule set off.
Start Date	Set the date (in year-month-day format) when you want this call schedule set to take effect.
How Often	Select Once to use this schedule set only one time. Select Weekly to use this schedule every week. If you select Once , then enter the date the set will activate in year-month-day format. If you selected Weekly in the How Often field, then select the day or days of the week when the set will activate.
Start Time (24-Hour Format)	Enter the start time (in hour-minute format) when you want the schedule set to take effect.
Duration Time (24-Hour Format)	Enter the maximum length of time (in hour-minute format) that the schedule set is to apply the action configured in the Action field. The limit is 24 hours.
Action	Select an action for the schedule set to take. Forced On means that the connection is maintained whether or not there is a demand call on the line and persists for the time period specified in the Duration field. Forced Down means that the connection is blocked whether or not there is a demand call on the line. Enable Dial-On-Demand means that this schedule permits a demand call on the line. Disable Dial-On-Demand means that this schedule prevents a demand call on the line.
Apply	Click Apply to save your changes to the BCM50a Integrated Router.
Cancel	Click Cancel to exit this screen without saving.

Applying Schedule Sets to a remote node

Once your schedule sets are configured, you must then apply them. Apply schedule sets in the **WAN IP** screen.

Chapter 21

Maintenance

This chapter displays system information such as firmware, port IP addresses, and port traffic statistics.

Maintenance overview

The maintenance screens can help you view system information, upload new firmware, manage configuration, and restart your BCM50a Integrated Router.

Status screen

Click **MAINTENANCE** to open the **Status** screen, where you can monitor your BCM50a Integrated Router. Note that these fields are **READ-ONLY** and only used for diagnostic purposes.

Figure 154 System Status
MAINTENANCE

Status	DHCP Table	Diagnostic	F/W Upload	Configuration	Restart
System Name :					
Nortel Firmware Version: VBCM252_2.6.0.0.001b4 07/31/2006					
DSL FW Version: STMI 2.6.4					
Standard: Multi-Mode					
WAN Information					
IP Address : 0.0.0.0					
IP Subnet Mask : 0.0.0.0					
Default Gateway: 0.0.0.0					
VPI/VCI: 0 / 33					
LAN Information					
MAC Address: 00:13:49:00:00:01					
IP Address : 192.168.1.1					
IP Subnet Mask: 255.255.255.0					
DHCP: Server					
DHCP Start IP: 192.168.1.2					
DHCP Pool Size: 126					
<input type="button" value="Show Statistics"/>					

Table 106 describes the fields in Figure 154.

Table 106 System Status

Label	Description
System Name	This is the System Name you chose in the first Internet Access Wizard screen. It is for identification purposes
Nortel Firmware Version	The release of firmware currently on the BCM50a Integrated Router and the date the release was created.
DSL FW Version	This is the DSL firmware version currently on the BCM50a Integrated Router.
Standard	This is the ADSL standard that your BCM50a Integrated Router is using.
WAN Information	

Table 106 System Status

Label	Description
IP Address	This is the WAN port IP address.
IP Subnet Mask	This is the WAN port subnet mask.
Default Gateway	This is the IP address of the default gateway, if applicable.
VPI/VCI	This is the Virtual Path Identifier and Virtual Channel Identifier that you entered in the first Wizard screen.
LAN Information	
MAC Address	This is the MAC (Media Access Control) or Ethernet address unique to your BCM50a Integrated Router.
IP Address	This is the LAN port IP address.
IP Subnet Mask	This is the LAN port IP subnet mask.
DHCP	This is the LAN port DHCP role - Server, Relay or None .
DHCP Start IP	This is the first of the contiguous addresses in the IP address pool.
DHCP Pool Size	This is the number of IP addresses in the IP address pool.
Show Statistics	Click Show Statistics to see router performance statistics such as number of packets sent and number of packets received for each port.

System statistics

Read-only information here includes port status and packet specific statistics. Also provided are system up time and poll intervals. The **Poll Interval(s)** field is configurable.

Figure 155 System Status: Show statistics

System Up Time: 0:19:47
CPU Load: 0.00%

WAN Port Statistics:
Link Status: Initializing
Upstream Speed: 0 kbps
Downstream Speed: 0 kbps

Node-Link	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
1-ENET	N/A	0	0	0	0	0	0:00:00

LAN Port Statistics:

Interface:	Status	TxPkts	RxPkts	Collisions
Ethernet	100M/Full	829	868	0

Poll Interval(s) :

Table 107 describes the fields in Figure 155.

Table 107 System Status: Show Statistics

Label	Description
System up Time	This is the elapsed time the system has been up.
CPU Load	This field specifies the percentage of CPU utilization.
LAN or WAN Port Statistics	This is the WAN or LAN port.
Link Status	This is the status of your WAN link.
Upstream Speed	This is the upstream speed of your BCM50a Integrated Router.
Downstream Speed	This is the downstream speed of your BCM50a Integrated Router.
Node-Link	This field displays the remote node index number and link type. Link types are PPPoA , ENET , RFC 1483 and PPPoE .
Interface	This field displays the type of port.

Table 107 System Status: Show Statistics (continued)

Label	Description
Status	For the WAN port, this displays the port speed and duplex setting if you're using Ethernet encapsulation and down (line is down), idle (line (ppp) idle), dial (starting to trigger a call) and drop (dropping a call) if you're using PPPoE encapsulation. For a LAN port, this shows the port speed and duplex setting.
TxPkts	This field displays the number of packets transmitted on this port.
RxPkts	This field displays the number of packets received on this port.
Errors	This field displays the number of error packets on this port.
Tx B/s	This field displays the number of bytes transmitted in the last second.
Rx B/s	This field displays the number of bytes received in the last second.
Up Time	This field displays the elapsed time this port has been up.
Collisions	This is the number of collisions on this port.
Poll Interval(s)	Type the time interval for the browser to refresh system statistics.
Set Interval	Click this button to apply the new poll interval you entered in the Poll Interval field above.
Stop	Click this button to halt the refreshing of the system statistics.

DHCP Table screen

With DHCP (Dynamic Host Configuration Protocol, RFC 2131 and RFC 2132) individual clients can obtain TCP/IP configuration at start-up from a server. You can configure the BCM50a Integrated Router as a DHCP server or disable it. When configured as a server, the BCM50a Integrated Router provides the TCP/IP configuration for the clients. If set to **None**, DHCP service is disabled and you must have another DHCP server on your LAN, or else the computer must be configured manually.

Click **MAINTENANCE**, and then the **DHCP Table** tab. Read-only information here relates to your DHCP status. The DHCP table shows current DHCP Client information (including **IP Address**, **Host Name**, and **MAC Address**) of all network clients using the DHCP server.

Figure 156 DHCP Table

MAINTENANCE

Status	DHCP Table	Diagnostic	F/W Upload	Configuration	Restart
#	IP Address	Host Name	MAC Address	Reserve	
1	192.168.1.2	Tw11746	00:0f:fe:1e:4a:e0	<input type="checkbox"/>	

Table 108 describes the fields in Figure 156.

Table 108 DHCP Table

Label	Description
#	This is the index number of the host computer.
IP Address	This field displays the IP address relative to the # field listed above.
Host Name	This field displays the computer host name.
MAC Address	This field shows the MAC address of the computer with the name in the Host Name field. Every Ethernet device has a unique MAC (Media Access Control) address. The MAC address is assigned at the factory and consists of six pairs of hexadecimal characters, for example, 00:A0:C5:00:00:02.
Reserve	Select the check box to have the BCM50a Integrated Router always assign the displayed IP address to the corresponding MAC address (and host name). After you click Apply , the MAC address and IP address also display in the LAN Static DHCP screen (where you can edit them).
Refresh	Click Refresh to renew the screen.

Diagnostic Screen

From the **Site Map** screen, click **Diagnostic** to open the screen shown next.

Figure 157 Diagnostic

Diagnostic

The screenshot shows the Diagnostic configuration page. At the top, there are tabs for Status, DHCP Table, Diagnostic, F/W Upload, Configuration, and Restart. Below the tabs is a large text area containing the text "- Info -". Underneath the text area, there are several sections:

- General**: This section is currently empty.
- TCP/IP**: This section contains an "Address" input field and a "Ping" button.
- System**: This section contains a "Reset System" button.
- DSL Line**: This section contains five buttons: "Reset ADSL Line", "Upstream Noise Margin", "ATM Status", "Downstream Noise Margin", and "ATM Loopback Test".

Table 109 describes the fields in Figure 157.

Table 109 Diagnostic

Label	Description
General	
TCP/IP Address	Type the IP address of a computer that you want to ping in order to test a connection.

Table 109 Diagnostic

Label	Description
Ping	Click this button to ping the IP address that you entered.
Reset System	Click this button to reboot the BCM50a Integrated Router. A warning dialog box is then displayed asking you if you're sure you want to reboot the system. Click OK to proceed.
DSL Line	
Reset ADSL Line	Click this button to reinitialize the ADSL line. The large text box above then displays the progress and results of this operation, for example: "Start to reset ADSL Loading ADSL modem F/W... Reset ADSL Line Successfully!"
ATM Status	Click this button to view ATM status.
ATM Loopback Test	Click this button to start the ATM loopback test. Make sure you have configured at least one PVC with proper VPIs/VCI before you begin this test. The BCM50a Integrated Router sends an OAM F5 packet to the DSLAM/ATM switch and then returns it (loops it back) to the BCM50a Integrated Router. The ATM loopback test is useful for troubleshooting problems with the DSLAM and ATM network.
Upstream Noise Margin	Click this button to display the upstream noise margin.
Downstream Noise Margin	Click this button to display the downstream noise margin.

F/W Upload screen

Find firmware at www.nortel.com/index.html in a file that usually uses the system model name with a *.bin extension. The upload process uses FTP (File Transfer Protocol) and can take up to two minutes. After a successful upload, the system reboots.

Click **MAINTENANCE**, and then the **F/W UPLOAD** tab. Follow the instructions to upload firmware to your BCM50a Integrated Router.



Note: Only upload firmware for your specific model!

Figure 158 Firmware upload

MAINTENANCE

Table 110 describes the fields in Figure 158.

Table 110 Firmware Upload

Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.
Browse...	Click Browse... to find the .bin file you want to upload. Remember that you must decompress compressed (.zip) files before you can upload them.
Upload	Click Upload to begin the upload process. This process can take up to two minutes.

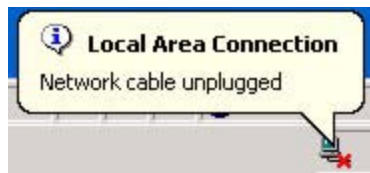


Note: Do not turn off the device while firmware upload is in progress!

After you see the **Firmware Upload in Process** (Figure 159) screen, wait two minutes before logging on to the device again.

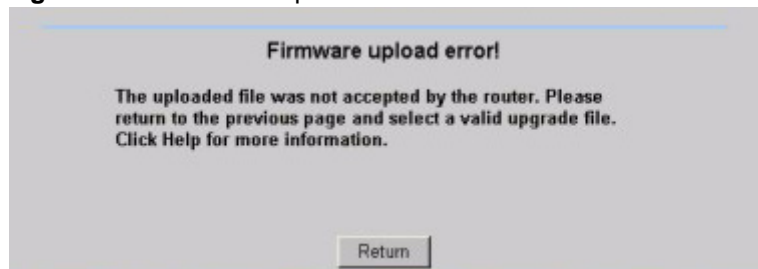
Figure 159 Firmware Upload In Process

The device automatically restarts in this time, causing a temporary network disconnect. In some operating systems, you can see the icon Shown in [Figure 160](#) on your desktop.

Figure 160 Network Temporarily Disconnected

After two minutes, log on again and check your new firmware version in the **System Status** screen.

If the upload was not successful, the screen shown in [Figure 161](#) appears. Uploading the wrong firmware file or a corrupted firmware file can cause this error. Click **Return** to return to the **F/W Upload** screen.

Figure 161 Firmware upload error

Configuration screen

Click **MAINTENANCE**, and then the **Configuration** tab. Information related to factory defaults, backup configuration, and restoring configuration appears as shown in [Figure 162](#).

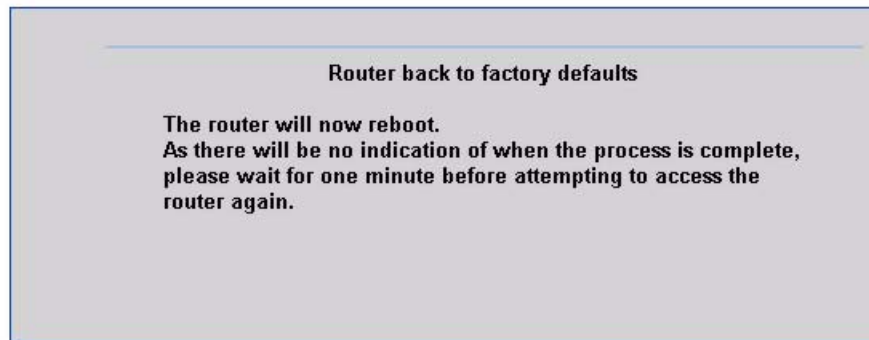
Figure 162 Configuration

MAINTENANCE

Status	DHCP Table	Diagnostic	F/W Upload	Configuration	Restart
Backup Configuration					
Click Backup to save the current configuration of your system to your computer.					
<input type="button" value="Backup"/>					
Restore Configuration					
To restore a previously saved configuration file to your system, browse to the location of the configuration file and click Upload.					
File Path: <input type="text"/> <input type="button" value="Browse..."/>					
<input type="button" value="Upload"/>					
Back to Factory Defaults					
Click Reset to clear all user-entered configuration information and return to factory defaults. After resetting, the					
- Password will be "PlsChgMe!"					
- LAN IP address will be 192.168.1.1					
- DHCP will be reset to server					
<input type="button" value="Reset"/>					

Back to Factory Defaults

Pressing the **Reset** button in this section clears all user-entered configuration information and returns the BCM50a Integrated Router to its factory defaults. The warning screen will appear (see [Figure 163](#)).

Figure 163 Reset warning message**CONFIGURATION**

The BCM50a Integrated Router LAN IP address changes back to 192.168.1.1 and the password reverts to “PlsChgMe!”.

Backup configuration

With backup configuration, you can back up and save the current device configuration to a 104 KB file on your computer. After your device is configured and functioning properly, Nortel recommends that you back up your configuration file before making configuration changes. The backup configuration file is useful in case you need to return to your previous settings.

Click **Backup** to save the current device configuration to your computer.

Restore configuration

With restore configuration, you can upload a new or previously saved configuration file from your computer to your BCM50a Integrated Router.

Table 111 Restore configuration

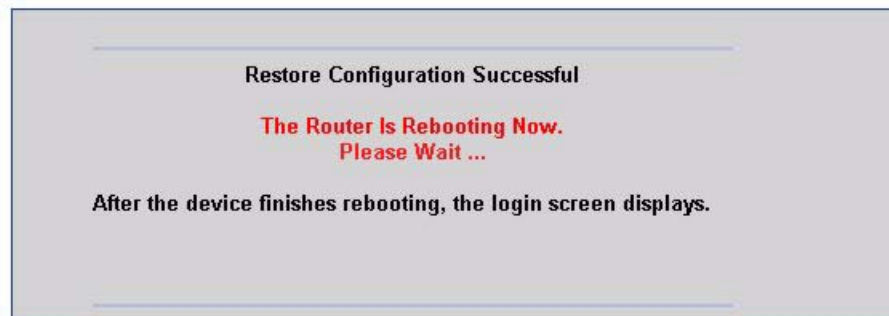
Label	Description
File Path	Type in the location of the file you want to upload in this field or click Browse... to find it.

Table 111 Restore configuration

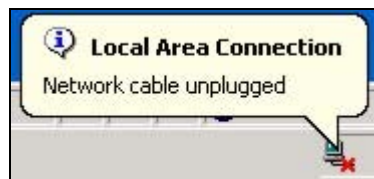
Browse...	Click Browse... to find the file you want to upload. Remember that you must decompress compressed (.ZIP) files before you can upload them.
Upload	Click Upload to begin the upload process.

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

After you see a “configuration upload successful” screen, you must then wait one minute before logging on to the device again.

Figure 164 Configuration Upload Successful**RESTORE CONFIGURATION**

The device automatically restarts in this time, causing a temporary network disconnect. In some operating systems, you see the icon shown in [Figure 165](#) on your desktop.

Figure 165 Network Temporarily Disconnected

If you uploaded the default configuration file, you need to change the IP address of your computer to be in the same subnet as that of the default device IP address (192.168.1.1). See your [guide](#) for details about how to set up your computer IP address.

If the upload was not successful, click **Return** to return to the **Configuration** screen.

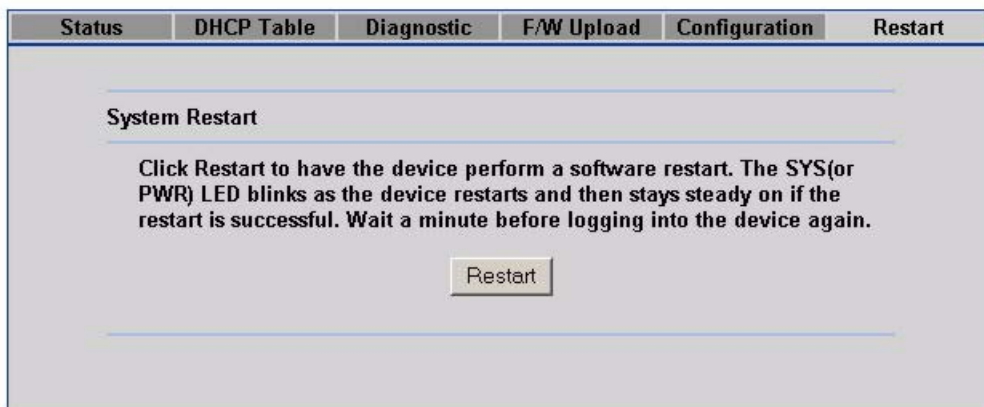
Restart screen

With system restart, you can reboot the BCM50a Integrated Router without turning the power off.

Click **MAINTENANCE**, and then **Restart**. Click **Restart** to have the BCM50a Integrated Router reboot. This does not affect the BCM50a Integrated Router's configuration.

Figure 166 Restart screen

MAINTENANCE



Appendix A

Troubleshooting

This chapter covers potential problems and the corresponding remedies.

Problems Starting Up the BCM50a Integrated Router

Table 112 Troubleshooting the Start-Up of your BCM50a Integrated Router

Problem	Corrective Action
None of the LEDs turn on when I turn on the BCM50a Integrated Router.	Make sure that the BCM50 power adaptor is connected to the BCM50a Integrated Router and plugged in to an appropriate power source. Check that the BCM50a Integrated Router and the power source are both turned on. Turn the BCM50a Integrated Router off and on. If the error persists, you have a hardware problem. In this case, contact your vendor.

Problems with the LAN LED

Table 113 Troubleshooting the LAN LED

Problem	Corrective Action
The LAN LEDs do not turn on.	Check your Ethernet cable connections.
	Check for faulty Ethernet cables.
	Make sure the Ethernet Card in your computer is working properly.

Problems with the LAN interface

Table 114 Troubleshooting the LAN interface

Problem	Corrective Action
I cannot access the BCM50a Integrated Router from the LAN.	Check your Ethernet cable type and connections.
	Make sure the Ethernet adapter is installed in the computer and functioning properly.
I cannot ping any computer on the LAN.	Check the 10M/100M LAN LEDs on the front panel. If they are all off, check the cables between your BCM50a Integrated Router and hub or the computer.
	Verify that the IP address and the subnet mask of the BCM50a Integrated Router and the computers are on the same subnet.

Problems with the WAN interface

Table 115 Troubleshooting the WAN Interface

Problem	Corrective Action
Cannot get WAN IP address from the ISP.	The ISP provides the WAN IP address after authentication. Authentication can be through the username and password, the MAC address, or the host name. Use the following corrective actions to make sure the ISP can authenticate your connection.
	You need a username and password if you are using PPPoE or PPPoA encapsulation. Make sure that you have entered the correct service type, username, and password (the username and password are case-sensitive). Use the WAN screens in the WebGUI.
	If your ISP requires host name authentication, configure your computer name as the system name of the BCM50a Integrated Router (use the System General screen to configure the system name).

Problems with Internet access

Table 116 Troubleshooting Internet access

Problem	Corrective Action
Cannot access the Internet.	Check your cable connections.
	Verify your settings in the WAN screens.
Internet connection disconnects.	Check the call-scheduling rules.
	If you use PPPoA or PPPoE encapsulation, check the idle time-out setting in the WAN screens.
	Contact your ISP.

Problems accessing an Internet Web site

Table 117 Troubleshooting Web Site Internet Access

Problem	Corrective Action
Cannot connect to a Web site on the Internet.	Disable content filtering and clear your browser cache. Try connecting to the Web site again. If you can now connect to this site, the content filter blocked original access. Check your content filter settings if this was not your intention.
	If you cannot connect to the site even after you disable content filtering, check your device connections and Internet access settings. Your username and password can be case-sensitive. If device connections and Internet access settings are correct, contact your ISP.

Problems with the password

Table 118 Troubleshooting the password

Problem	Corrective Action
I cannot access the BCM50a Integrated Router.	The administrator username is "nadmin". The default password is "PlsChgMe!". The Password and Username fields are case-sensitive. Make sure that you enter the correct password and username using the proper casing.

Problems with the WebGUI

Problems with Remote Management

Table 119 Troubleshooting Remote Management

Problem	Corrective Action
---------	-------------------

Table 119 Troubleshooting Remote Management

I cannot remotely manage the BCM50a Integrated Router from the LAN or the WAN.	Check your remote management and firewall configuration.
	Use the BCM50a Integrated Router WAN IP address when configuring from the WAN.
	Use the BCM50a Integrated Router LAN IP address when configuring from the LAN.
	Refer to “Problems with the LAN interface” on page 394 for instructions about checking your LAN connection.
	Refer to the “Problems with the WAN interface” on page 395 for instructions about checking your WAN connection.
See also “Problems with the WebGUI” on page 396 .	

Allowing Pop-up Windows, JavaScript and Java Permissions

In order to use the WebGUI, you must allow:

- Web browser pop-up windows from your device
- JavaScript
- Java permissions

Internet Explorer Pop-up Blockers



Note: Internet Explorer 6 screens are used here. Screens for other Internet Explorer versions vary

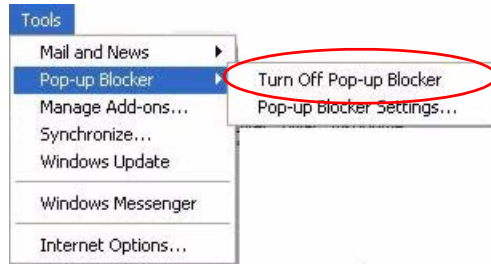
Disable pop-up blocking to log on to your device, if necessary.

Either disable pop-up blocking (enabled by default in Windows XP SP (Service Pack) 2) or enable pop-up blocking and create an exception for your device IP address.

Allowing Pop-ups

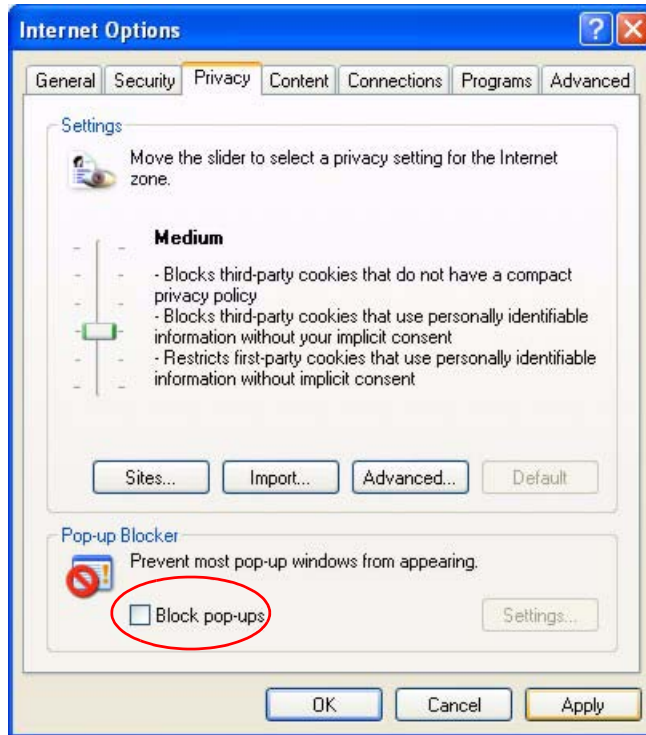
- 1 In Internet Explorer, select **Tools, Pop-up Blocker** and then select **Turn Off Pop-up Blocker**.

Figure 167 Pop-up Blocker



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

- 1 In Internet Explorer, select **Tools, Internet Options, Privacy**.
- 2 Clear the **Block pop-ups** check box in the **Pop-up Blocker** section of the screen.

Figure 168 Internet Options

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

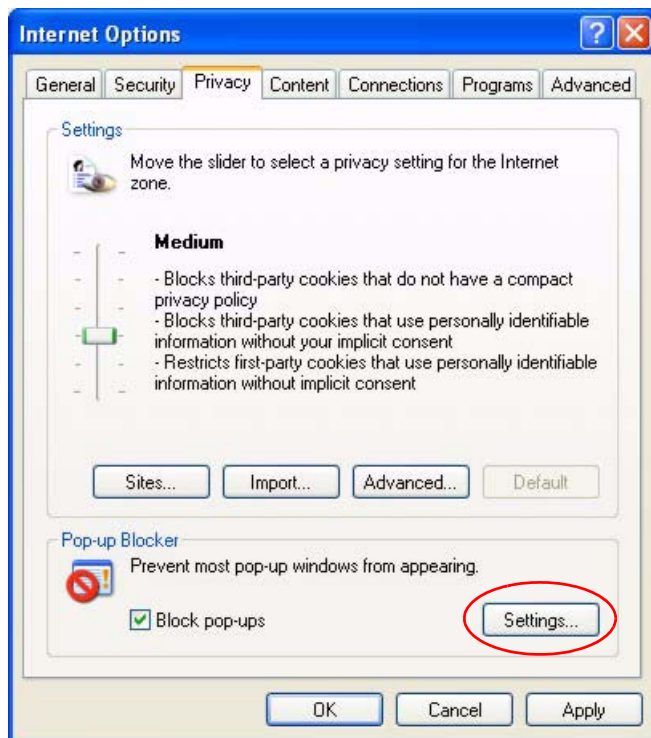
Enabling Pop-up Blockers with Exceptions

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

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

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

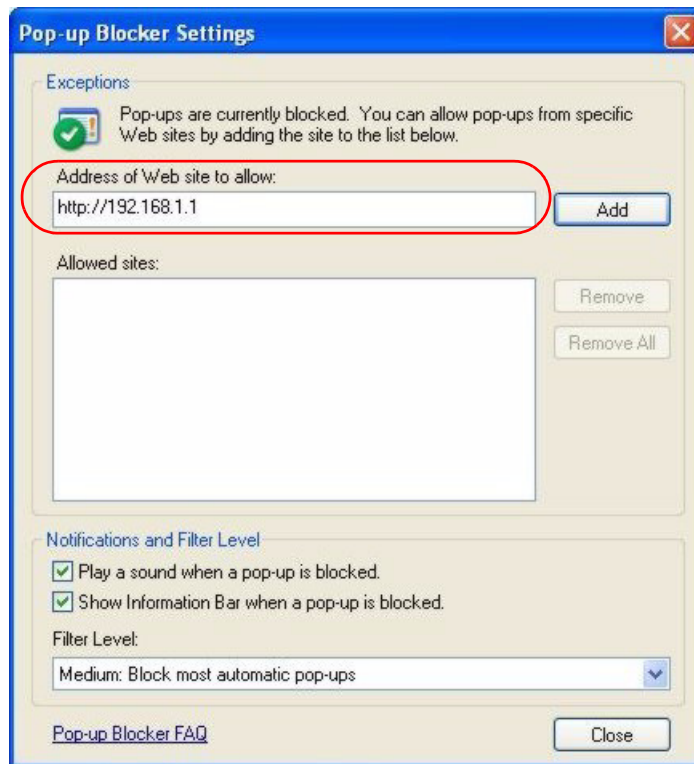
Figure 169 Internet options



- 3 Type the IP address of your device (the Web page that you do not want to have blocked) with the prefix “http://”. For example, http://192.168.1.1.

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

Figure 170 Pop-up Blocker settings



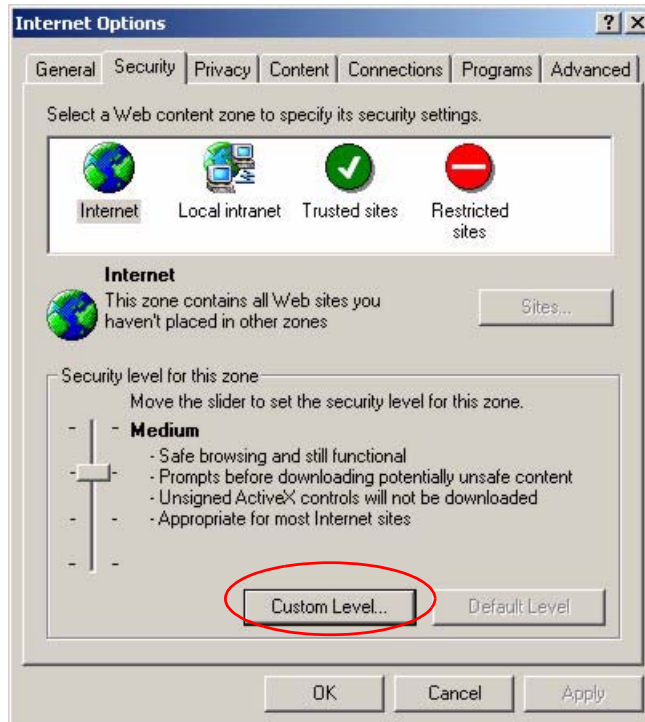
- 5 Click **Close** to return to the **Internet Options** screen.
- 6 Click **Apply** to save this setting.

Internet Explorer JavaScript

If pages of the WebGUI do not display properly in Internet Explorer, check that JavaScript and Java permissions are enabled.

- 1 In Internet Explorer, click **Tools, Internet Options**, and then the **Security** tab.

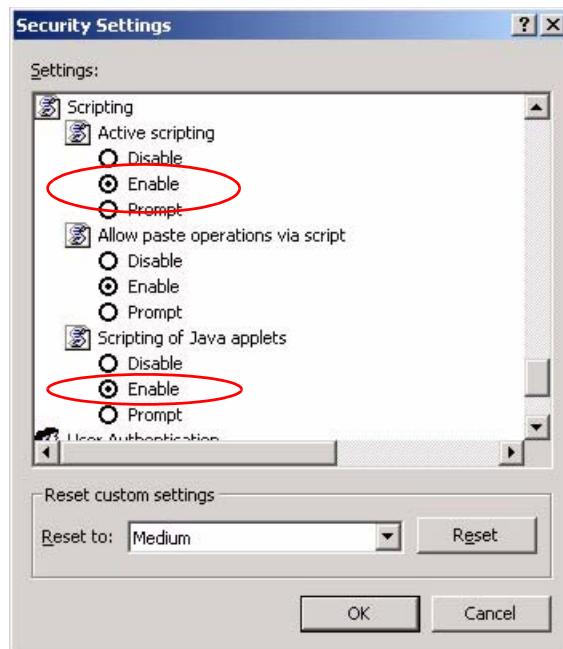
Figure 171 Internet options



- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Scripting**.
- 4 Under **Active scripting** make sure that **Enable** is selected (the default).
- 5 Under **Scripting of Java applets** make sure that **Enable** is selected (the default).

- 6 Click **OK** to close the window.

Figure 172 Security Settings - Java Scripting

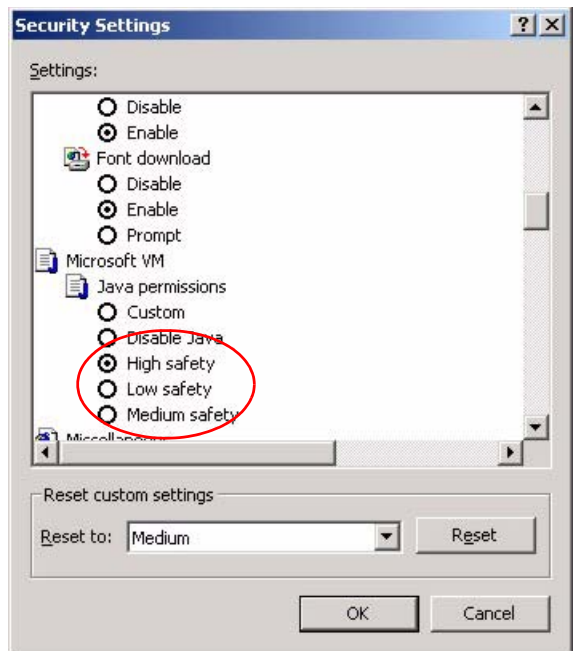


Internet Explorer Java Permissions

- 1 From Internet Explorer, click **Tools, Internet Options**, and then the **Security** tab.
- 2 Click the **Custom Level...** button.
- 3 Scroll down to **Microsoft VM**.
- 4 Under **Java permissions** make sure that a safety level is selected.

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

Figure 173 Security Settings - Java

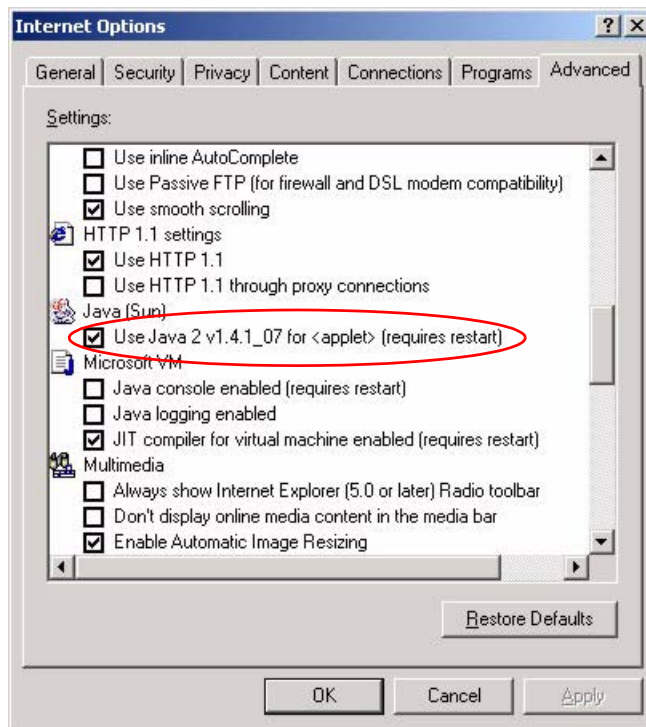


JAVA (Sun)

- 1 From Internet Explorer, click **Tools, Internet Options**, and then the **Advanced** tab.
- 2 Make sure that **Use Java 2 for <applet>** under **Java (Sun)** is selected.
- 3 Click **OK** to close the window.

- 4 Close your existing browser session and open a new browser.

Figure 174 Java (Sun)



Netscape Pop-up Blockers



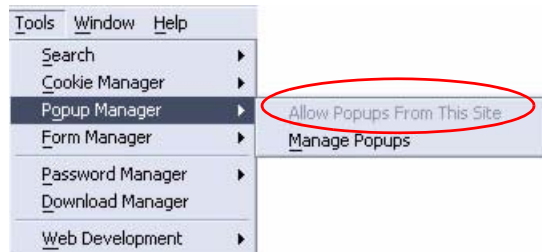
Note: Netscape 7.2 screens are used here. Screens for other Netscape versions vary

Either disable the blocking of unrequested pop-up windows (enabled by default in Netscape) or allow pop-ups from Web sites by creating an exception for your device IP address.

Allowing Pop-ups

- 1 In Netscape, click **Tools, Popup Manager** and then select **Allow Popups From This Site**.

Figure 175 Allow Popups from this site



- 2 In the Netscape search toolbar, you can enable and disable pop-up blockers for Web sites.

Figure 176 Netscape Search Toolbar

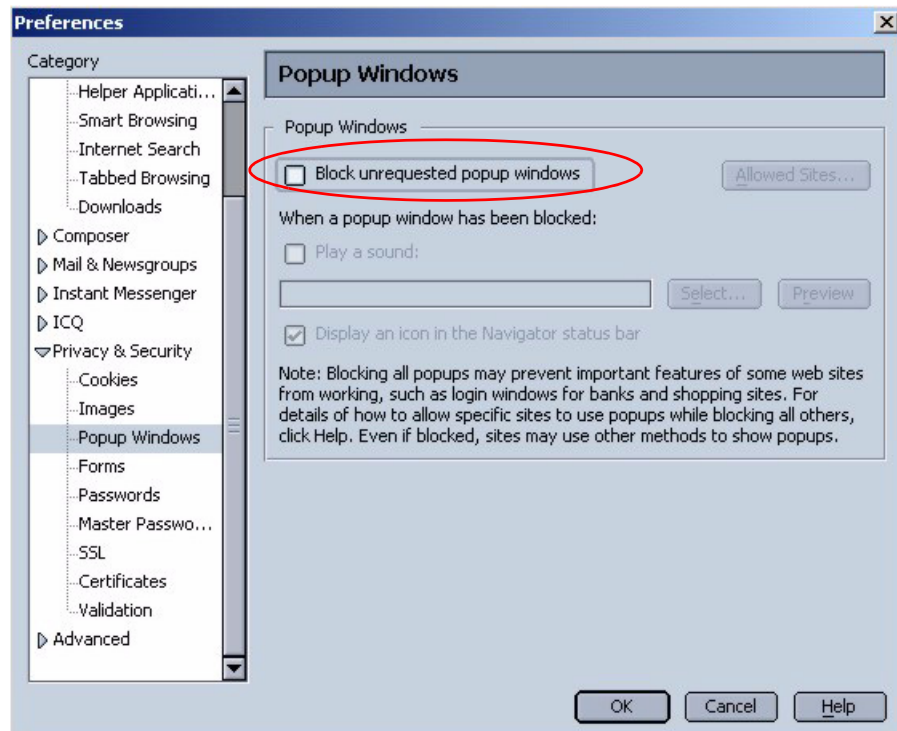


You can also check if pop-up blocking is disabled in the **Popup Windows** screen in the **Privacy & Security** directory.

- 1 In Netscape, click **Edit** and then **Preferences**.
- 2 Click the **Privacy & Security** directory and then select **Popup Windows**.

- 3 Clear the **Block unrequested popup windows** check box.

Figure 177 Popup Windows



- 4 Click **OK** to save this setting.

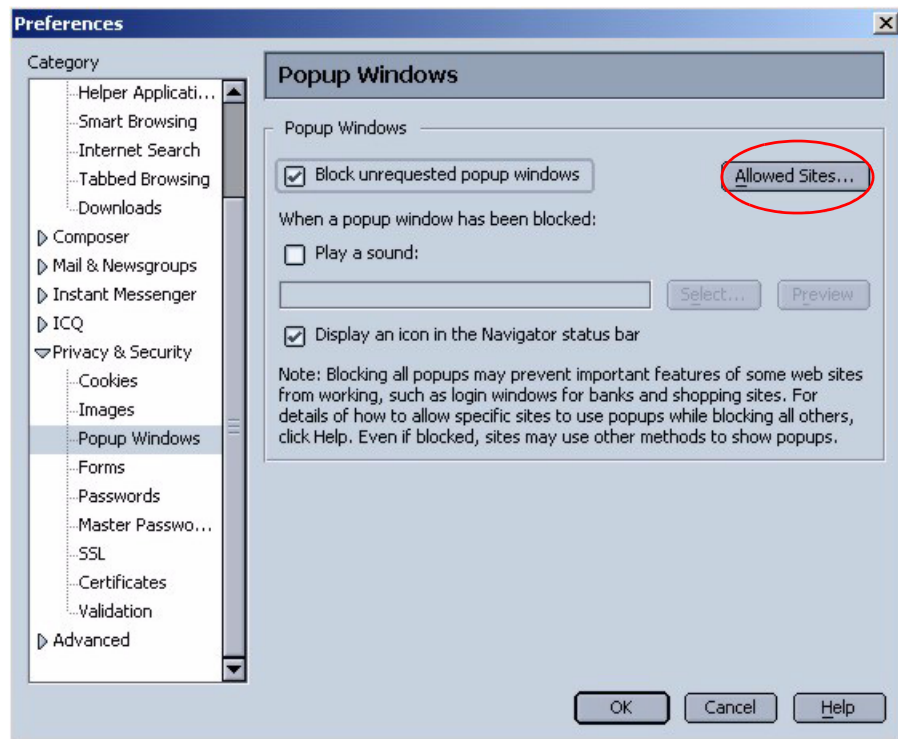
Enable Pop-up Blockers with Exceptions

Alternatively, if you only want to allow pop-up windows from your device, follow these steps:

- 1 In Netscape, click **Edit**, and then **Preferences**.
- 2 In the **Privacy & Security** directory, select **Popup Windows**.
- 3 Make sure the **Block unrequested popup windows** check box is selected.

- 4 Click the **Allowed Sites...** button.

Figure 178 Popup Windows



- 5 Type the IP address of your device (the Web page that you do not want to have blocked) with the prefix `http://`. For example, `http://192.168.1.1`.

- 6 Click **Add** to move the IP address to the **Site** list.

Figure 179 Allowed Sites



- 7 Click **OK** to return to the **Popup Windows** screen.
- 8 Click **OK** to save this setting.

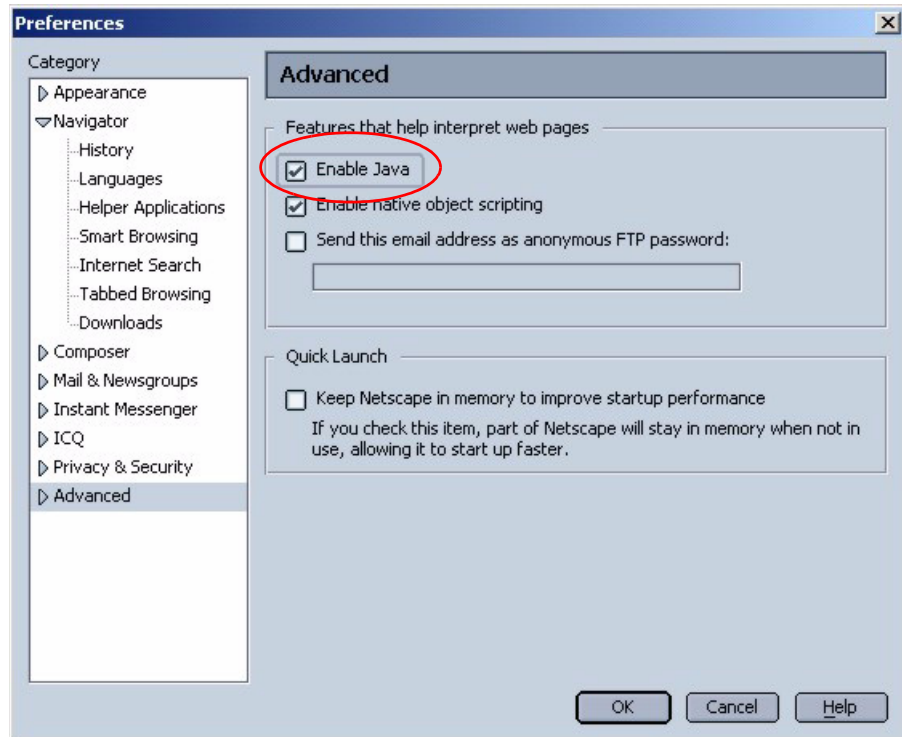
Netscape Java Permissions and JavaScript

If pages of the WebGUI do not display properly in Netscape, check that JavaScript and Java permissions are enabled.

- 1 In Netscape, click **Edit** and then **Preferences**.
- 2 Click the **Advanced** directory.
- 3 In the **Advanced** screen, make sure the **Enable Java** check box is selected.

- 4 Click **OK** to close the window.

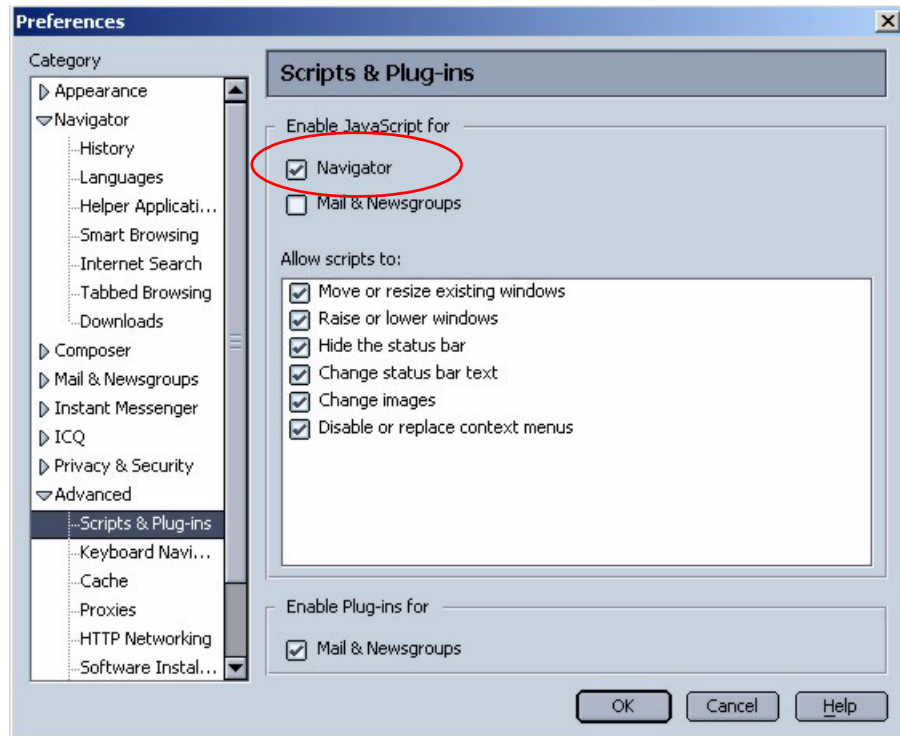
Figure 180 Advanced



- 5 Click the **Advanced** directory and then select **Scripts & Plug-ins**.
- 6 Make sure the **Navigator** check box is selected in the enable JavaScript section.

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

Figure 181 Scripts & Plug-ins



Appendix B

Log Descriptions

This appendix provides descriptions of example log messages.

Table 120 System Error Logs

Log Message	Description
<code>%s exceeds the max. number of session per host!</code>	This attempt to create a SUA/NAT session exceeds the maximum number of SUA/NAT session table entries allowed to be created per host.

Table 121 System Maintenance Logs

Log Message	Description
<code>Time calibration is successful</code>	The router has adjusted its time based on information from the time server.
<code>Time calibration failed</code>	The router failed to get information from the time server.
<code>DHCP client gets %s</code>	A DHCP client got a new IP address from the DHCP server.
<code>DHCP client IP expired</code>	A DHCP client's IP address has expired.
<code>DHCP server assigns %s</code>	The DHCP server assigned an IP address to a client.
<code>SMT Login Successfully</code>	Someone has logged on to the router's SMT interface.
<code>SMT Login Fail</code>	Someone has failed to log on to the router's SMT interface.
<code>WEB Login Successfully</code>	Someone has logged on to the router's WebGUI interface.
<code>WEB Login Fail</code>	Someone has failed to log on to the router's WebGUI interface.
<code>TELNET Login Successfully</code>	Someone has logged on to the router through Telnet.

Table 121 System Maintenance Logs

Log Message	Description
TELNET Login Fail	Someone has failed to log on to the router through Telnet.
FTP Login Successfully	Someone has logged on to the router through FTP.
FTP Login Fail	Someone has failed to log on to the router through FTP.
NAT Session Table is Full!	The maximum number of SUA/NAT session table entries has been exceeded and the table is full.

Table 122 UPnP Logs

Log Message	Description
UPnP pass through Firewall	UPnP packets can pass through the firewall.

Table 123 Content Filtering Logs

Category	Log Message	Description
URLFOR	IP/Domain Name	The BCM50a Integrated Router allows access to this IP address or domain name and forwarded traffic addressed to the IP address or domain name.
URLBLK	IP/Domain Name	The BCM50a Integrated Router blocked access to this IP address or domain name due to a forbidden keyword. All Web traffic is disabled except for trusted domains, untrusted domains, or the cybernot list.
JAVBLK	IP/Domain Name	The BCM50a Integrated Router blocked access to this IP address or domain name because of a forbidden service such as: ActiveX, a Java applet, a cookie, or a proxy.

Table 124 Attack Logs

Log Message	Description
attack TCP	The firewall detected a TCP attack.
attack UDP	The firewall detected an UDP attack.
attack IGMP	The firewall detected an IGMP attack.

Table 124 Attack Logs

Log Message	Description
attack ESP	The firewall detected an ESP attack.
attack GRE	The firewall detected a GRE attack.
attack OSPF	The firewall detected an OSPF attack.
attack ICMP (type:%d, code:%d)	The firewall detected an ICMP attack; see the section about ICMP messages for type and code details.
land TCP	The firewall detected a TCP land attack.
land UDP	The firewall detected an UDP land attack.
land IGMP	The firewall detected an IGMP land attack.
land ESP	The firewall detected an ESP land attack.
land GRE	The firewall detected a GRE land attack.
land OSPF	The firewall detected an OSPF land attack.
land ICMP (type:%d, code:%d)	The firewall detected an ICMP land attack; see the section about ICMP messages for type and code details.
ip spoofing - WAN TCP	The firewall detected a TCP IP spoofing attack on the WAN port.
ip spoofing - WAN UDP	The firewall detected an UDP IP spoofing attack on the WAN port.
ip spoofing - WAN IGMP	The firewall detected an IGMP IP spoofing attack on the WAN port.
ip spoofing - WAN ESP	The firewall detected an ESP IP spoofing attack on the WAN port.
ip spoofing - WAN GRE	The firewall detected a GRE IP spoofing attack on the WAN port.
ip spoofing - WAN OSPF	The firewall detected an OSPF IP spoofing attack on the WAN port.
ip spoofing - WAN ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack on the WAN port.
icmp echo ICMP (type:%d, code:%d)	The firewall detected an ICMP echo attack.
syn flood TCP	The firewall detected a TCP syn flood attack.
ports scan TCP	The firewall detected a TCP port scan attack.
teardrop TCP	The firewall detected a TCP teardrop attack.
teardrop UDP	The firewall detected an UDP teardrop attack.

Table 124 Attack Logs

Log Message	Description
teardrop ICMP (type:%d, code:%d)	The firewall detected an ICMP teardrop attack.
illegal command TCP	The firewall detected a TCP illegal command attack.
NetBIOS TCP	The firewall detected a TCP NetBIOS attack.
ip spoofing - no routing entry TCP	The firewall detected a TCP IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry UDP	The firewall detected an UDP IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry IGMP	The firewall detected an IGMP IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry ESP	The firewall detected an ESP IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry GRE	The firewall detected a GRE IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry OSPF	The firewall detected an OSPF IP spoofing attack while the BCM50a Integrated Router did not have a default route.
ip spoofing - no routing entry ICMP (type:%d, code:%d)	The firewall detected an ICMP IP spoofing attack while the BCM50a Integrated Router did not have a default route.
vulnerability ICMP (type:%d, code:%d)	The firewall detected an ICMP vulnerability attack.
traceroute ICMP (type:%d, code:%d)	The firewall detected an ICMP traceroute attack.

For type and code details, see [Table 127](#).

Table 125 Access Logs

Log Message	Description
Firewall default policy: TCP (set:%d)	TCP access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: UDP (set:%d)	UDP access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.

Table 125 Access Logs

Log Message	Description
Firewall default policy: ICMP (set:%d, type:%d, code:%d)	ICMP access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: IGMP (set:%d)	IGMP access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: ESP (set:%d)	ESP access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: GRE (set:%d)	GRE access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: OSPF (set:%d)	OSPF access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall default policy: (set:%d)	Access matched the default policy of the listed ACL set and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the ACL set.
Firewall rule match: TCP (set:%d, rule:%d)	TCP access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: UDP (set:%d, rule:%d)	UDP access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: ICMP (set:%d, rule:%d, type:%d, code:%d)	ICMP access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: IGMP (set:%d, rule:%d)	IGMP access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: ESP (set:%d, rule:%d)	ESP access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: GRE (set:%d, rule:%d)	GRE access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule match: OSPF (set:%d, rule:%d)	OSPF access matched the listed a firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.

Table 125 Access Logs

Log Message	Description
Firewall rule match: (set:%d, rule:%d)	Access matched the listed firewall rule and the BCM50a Integrated Router blocked or forwarded it according to the configuration of the rule.
Firewall rule NOT match: TCP (set:%d, rule:%d)	TCP access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: UDP (set:%d, rule:%d)	UDP access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: ICMP (set:%d, rule:%d, type:%d, code:%d)	ICMP access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: IGMP (set:%d, rule:%d)	IGMP access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: ESP (set:%d, rule:%d)	ESP access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: GRE (set:%d, rule:%d)	GRE ac access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: OSPF (set:%d, rule:%d)	OSPF access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Firewall rule NOT match: (set:%d, rule:%d)	Access did not match the listed firewall rule and the BCM50a Integrated Router logged it.
Filter default policy DROP!	TCP access matched a default filter policy and the BCM50a Integrated Router dropped the packet to block access.
Filter default policy DROP!	UDP access matched a default filter policy and the BCM50a Integrated Router dropped the packet to block access.
Filter default policy DROP!	ICMP access matched a default filter policy and the BCM50a Integrated Router dropped the packet to block access.
Filter default policy DROP!	Access matched a default filter policy and the BCM50a Integrated Router dropped the packet to block access.

Table 125 Access Logs

Log Message	Description
Filter default policy DROP!	Access matched a default filter policy (denied LAN IP) and the BCM50a Integrated Router dropped the packet to block access.
Filter default policy FORWARD!	TCP access matched a default filter policy. Access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	UDP access matched a default filter policy. Access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	ICMP access matched a default filter policy. Access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	Access matched a default filter policy. Access was allowed and the router forwarded the packet.
Filter default policy FORWARD!	Access matched a default filter policy (denied LAN IP). Access was allowed and the router forwarded the packet.
Filter match DROP <set %d/rule %d>	TCP access matched the listed filter rule and the BCM50a Integrated Router dropped the packet to block access.
Filter match DROP <set %d/rule %d>	UDP access matched the listed filter rule and the BCM50a Integrated Router dropped the packet to block access.
Filter match DROP <set %d/rule %d>	ICMP access matched the listed filter rule and the BCM50a Integrated Router dropped the packet to block access.
Filter match DROP <set %d/rule %d>	Access matched the listed filter rule and the BCM50a Integrated Router dropped the packet to block access.
Filter match DROP <set %d/rule %d>	Access matched the listed filter rule (denied LAN IP) and the BCM50a Integrated Router dropped the packet to block access.
Filter match FORWARD <set %d/rule %d>	TCP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	UDP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	ICMP access matched the listed filter rule. Access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	Access matched the listed filter rule. Access was allowed and the router forwarded the packet.
Filter match FORWARD <set %d/rule %d>	Access matched the listed filter rule (denied LAN IP). Access was allowed and the router forwarded the packet.

Table 125 Access Logs

Log Message	Description
(set:%d)	With firewall messages, this is the number of the ACL policy set and denotes the packet's direction (see Table 126). With filter messages, this is the number of the filter set.
(rule:%d)	With firewall messages, the firewall rule number denotes the number of a firewall rule within an ACL policy set. With filter messages, this is the number of an individual filter rule.
Router sent blocked web site message	
Triangle route packet forwarded	The firewall allowed a triangle route session to pass through.
Firewall sent TCP packet in response to DoS attack	The firewall detected a DoS attack and sent a TCP packets in response.
Firewall sent TCP reset packets	The firewall sent out TCP reset packets.
Packet without a NAT table entry blocked	The router blocked a packet that did not have a corresponding SUA/NAT table entry.
Out of order TCP handshake packet blocked	The router blocked a TCP handshake packet that came out of the proper order.
Drop unsupported/ out-of-order ICMP	The BCM50a Integrated Router generates this log after it drops an ICMP packet due to one of the following two reasons: 1. The BCM50a Integrated Router does not support the ICMP packet's protocol. 2. The ICMP packet is an echo reply for which there was no corresponding echo request.
Router sent ICMP response packet (type:%d, code:%d)	The router sent an ICMP response packet. This packet automatically bypasses the firewall.

For type and code details, see [Table 127](#).

Table 126 ACL Setting Notes

ACL Set Number	Direction	Description
1	LAN to WAN	ACL set 1 for packets traveling from the LAN to the WAN.
2	WAN to LAN	ACL set 2 for packets traveling from the WAN to the LAN.
7	LAN to LAN/BCM50a Integrated Router	ACL set 7 for packets traveling from the LAN to the LAN or the BCM50a Integrated Router.
8	WAN to WAN/BCM50a Integrated Router	ACL set 8 for packets traveling from the WAN to the WAN or the BCM50a Integrated Router.

Table 127 ICMP Notes

Type	Code	Description
0		Echo reply
	0	Echo reply message
3		Destination unreachable
	0	Net unreachable
	1	Host unreachable
	2	Protocol unreachable
	3	Port unreachable
	4	A packet that needed fragmentation was dropped because the packet was set to Don't Fragment (DF)
	5	Source route failed
4		Source quench
	0	A gateway discard internet datagrams if it does not have the buffer space needed to queue the datagrams for output to the next network on the route to the destination network.
5		Redirect
	0	Redirect datagrams for the Network
	1	Redirect datagrams for the Host
	2	Redirect datagrams for the Type of service and network

Table 127 ICMP Notes

Type	Code	Description
	3	Redirect datagrams for the Type of service and host
8		Echo
	0	Echo message
11		Time exceeded
	0	Time to live exceeded in transit
	1	Fragment reassembly time exceeded
12		Parameter problem
	0	Pointer indicates the error
13		Timestamp
	0	Timestamp request message
14		Timestamp reply
	0	Timestamp reply message
15		Information request
	0	Information request message
16		Information reply
	0	Information reply message

Table 128 Sys log

LOG MESSAGE	DESCRIPTION
Mon dd hr:mm:ss hostname src="<srcIP:srcPort>" dst="<dstIP:dstPort>" msg="<msg>" note="<note>"	This message is sent by the RAS when this syslog is generated. The messages and notes are defined in this appendix.

VPN/IPSec Logs

To view the IPSec and IKE connection log, type 3 in menu 27 and press [ENTER] to display the IPSec log, as shown in [Figure 182](#), which shows a typical log from the initiator of a VPN connection.

Figure 182 Example VPN Initiator IPsec Log

```
Index:      Date/Time:      Log:
-----
001      01 Jan 08:02:22      Send Main Mode request to <192.168.100.101>
002      01 Jan 08:02:22      Send:<SA>
003      01 Jan 08:02:22      Recv:<SA>
004      01 Jan 08:02:24      Send:<KE><NONCE>
005      01 Jan 08:02:24      Recv:<KE><NONCE>
006      01 Jan 08:02:26      Send:<ID><HASH>
007      01 Jan 08:02:26      Recv:<ID><HASH>
008      01 Jan 08:02:26      Phase 1 IKE SA process done
009      01 Jan 08:02:26      Start Phase 2: Quick Mode
010      01 Jan 08:02:26      Send:<HASH><SA><NONCE><ID><ID>
011      01 Jan 08:02:26      Recv:<HASH><SA><NONCE><ID><ID>
012      01 Jan 08:02:26      Send:<HASH>
Clear IPsec Log (y/n):
```

VPN Responder IPsec Log

[Figure 183](#) shows a typical log from the VPN connection peer.

Figure 183 Example VPN Responder IPSec Log

```

Index:      Date/Time:      Log:
-----
001      01 Jan 08:08:07      Recv Main Mode request from <192.168.100.100>
002      01 Jan 08:08:07      Recv:<SA>
003      01 Jan 08:08:08      Send:<SA>
004      01 Jan 08:08:08      Recv:<KE><NONCE>
005      01 Jan 08:08:10      Send:<KE><NONCE>
006      01 Jan 08:08:10      Recv:<ID><HASH>
007      01 Jan 08:08:10      Send:<ID><HASH>
008      01 Jan 08:08:10      Phase 1 IKE SA process done
009      01 Jan 08:08:10      Recv:<HASH><SA><NONCE><ID><ID>
010      01 Jan 08:08:10      Start Phase 2: Quick Mode
011      01 Jan 08:08:10      Send:<HASH><SA><NONCE><ID><ID>
012      01 Jan 08:08:10      Recv:<HASH>
Clear IPSec Log (y/n):

```

This menu is useful for troubleshooting your BCM50a Integrated Router. A log index number, the date and time the log was created, and a log message are displayed.



Note: Double exclamation marks (!!) denote an error or warning message.

[Table 129](#) shows sample log messages during IKE key exchange.



Note: A PYLD_MALFORMED packet usually means that the two ends of the VPN tunnel are not using the same preshared key.

Table 129 Sample IKE Key Exchange Logs

Log Message	Description
Send <Symbol> Mode request to <IP>Send <Symbol> Mode request to <IP>	The BCM50a Integrated Router started negotiation with the peer.
Recv <Symbol> Mode request from <IP>Recv <Symbol> Mode request from <IP>	The BCM50a Integrated Router received an IKE negotiation request from the peer.
Recv:<Symbol>	IKE uses the ISAKMP protocol (refer to RFC 2408 – ISAKMP) to transmit data. Each ISAKMP packet contains payloads of different types that show in the log (see Table 131).
Phase 1 IKE SA process done	Phase 1 negotiation finished.
Start Phase 2: Quick Mode	Phase 2 negotiation begins using Quick Mode.
!! IKE Negotiation is in process	The BCM50a Integrated Router has begun negotiation with the peer for the connection, but the IKE key exchange has not completed.
!! Duplicate requests with the same cookie	The BCM50a Integrated Router received multiple requests from the same peer but is still processing the first IKE packet from that peer.
!! No proposal chosen	The parameters configured for Phase 1 or Phase 2 negotiations do not match. Check all protocols and settings for these phases. For example, one party uses 3DES encryption, but the other party uses DES encryption, so the connection fails.
!! Verifying Local ID failed!! Verifying Remote ID failed	During IKE Phase 2 negotiation, both parties exchange policy details, including local and remote IP address ranges. If these ranges differ, the connection fails.
!! Local / remote IPs of incoming request conflict with rule <#d>	If the security gateway is “0.0.0.0”, the BCM50a Integrated Router uses the peer “Local Addr” as its “Remote Addr”. If this IP (range) conflicts with a previously configured rule, the connection is not allowed.
!! Invalid IP <IP start>/<IP end>	The peer “Local IP Addr” range is invalid.

Table 129 Sample IKE Key Exchange Logs

Log Message	Description
!! Remote IP <IP start> / <IP end> conflicts	If the security gateway is "0.0.0.0", the BCM50a Integrated Router uses the peer "Local Addr" as its "Remote Addr". If a peer "Local Addr" range conflicts with other connections, the BCM50a Integrated Router does not accept VPN connection requests from this peer.
!! Active connection allowed exceeded	The BCM50a Integrated Router limits the number of simultaneous Phase 2 SA negotiations. The IKE key exchange process fails if this limit is exceeded.
!! IKE Packet Retransmit	The BCM50a Integrated Router did not receive a response from the peer and retransmits the last packet sent.
!! Failed to send IKE Packet	The BCM50a Integrated Router cannot send IKE packets due to a network error.
!! Too many errors! Deleting SA	The BCM50a Integrated Router deletes an SA when too many errors occur.
!! Phase 1 ID type mismatch	The ID type of an incoming packet does not match the local's peer ID type.
!! Phase 1 ID content mismatch	The ID content of an incoming packet does not match the local's peer ID content.
!! No known phase 1 ID type found	The ID type of an incoming packet does not match any known ID type.
Peer ID: IP address type <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the IP address type and IP address of the incoming packet.
vs. My Remote <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the configured remote IP address type or IP address for this router that the incoming packet did not match.
vs. My Local <IP address>	The IP address type or IP address of an incoming packet does not match the peer IP address type or IP address configured on the local router. The log displays the configured local IP address type or IP address that the incoming packet did not match.

Table 129 Sample IKE Key Exchange Logs

Log Message	Description
-> <symbol>	The router sent a payload type of IKE packet.
Error ID Info	The parameters configured for Phase 1 ID content do not match or the parameters configured for the Phase 2 ID (IP address of single, range, or subnet) do not match. Check all protocols and settings for these phases.

[Table 130](#) shows sample log messages during packet transmission.

Table 130 Sample IPsec Logs During Packet Transmission

LOG MESSAGE	DESCRIPTION
!! WAN IP changed to <IP>	If the BCM50a Integrated Router WAN IP changes, all configured My IP Addr change to 0.0.0.0. If this field is configured as 0.0.0.0, the BCM50a Integrated Router uses the current BCM50a Integrated Router WAN IP address (static or dynamic) to set up the VPN tunnel.
!! Cannot find IPsec SA	The BCM50a Integrated Router cannot find a phase 2 SA that corresponds with the SPI of an inbound packet (from the peer); the packet is dropped.
!! Cannot find outbound SA for rule <%d>	The packet matches the rule index number (#d), but Phase 1 or Phase 2 negotiation for outbound (from the VPN initiator) traffic is not finished yet.
!! Discard REPLAY packet	The BCM50a Integrated Router discards any packets received with the wrong sequence number.
!! Inbound packet authentication failed	The authentication configuration settings are incorrect. Check them.
!! Inbound packet decryption failed	The decryption configuration settings are incorrect. Check them.
Rule <#d> idle time out, disconnect	If an SA has no packets transmitted for a period of time (configurable through CI command), the BCM50a Integrated Router drops the connection.

[Table 131](#) shows RFC 2408 ISAKMP payload types that the log displays. Refer to RFC 2408 for detailed information about each type.

Table 131 RFC 2408 ISAKMP Payload Types

Log Display	Payload Type
SA	Security Association
PROP	Proposal
TRANS	Transform
KE	Key Exchange
ID	Identification
CER	Certificate
CER_REQ	Certificate Request
HASH	Hash
SIG	Signature
NONCE	Nonce
NOTFY	Notification
DEL	Delete
VID	Vendor ID

Table 132 PKI Logs

Log Message	Description
Enrollment successful	The SCEP online certificate enrollment succeeded. The Destination field records the certification authority server IP address and port.
Enrollment failed	The SCEP online certificate enrollment failed. The Destination field records the certification authority server IP address and port.
Failed to resolve <SCEP CA server url>	The SCEP online certificate enrollment failed because the certification authority server address cannot be resolved.
Enrollment successful	The CMP online certificate enrollment was succeeded. The Destination field records the certification authority server IP address and port.
Enrollment failed	The CMP online certificate enrollment failed. The Destination field records the certification authority server IP address and port.

Table 132 PKI Logs

Log Message	Description
Failed to resolve <CMP CA server url>	The CMP online certificate enrollment failed because the certification authority server IP address cannot be resolved.
Rcvd ca cert: <subject name>	The router received a certification authority certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd user cert: <subject name>	The router received a user certificate, with subject name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd CRL <size>: <issuer name>	The router received a CRL (Certificate Revocation List), with size and issuer name as recorded, from the LDAP server whose IP address and port are recorded in the Source field.
Rcvd ARL <size>: <issuer name>	The router received an ARL (Authority Revocation List), with size and issuer name as recorded, from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ca cert	The router received a corrupted certification authority certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received user cert	The router received a corrupted user certificate from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received CRL	The router received a corrupted CRL (Certificate Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Failed to decode the received ARL	The router received a corrupted ARL (Authority Revocation List) from the LDAP server whose address and port are recorded in the Source field.
Rcvd data <size> too large! Max size allowed: <max size>	The router received directory data that was too large (the size is listed) from the LDAP server whose address and port are recorded in the Source field. The maximum size of directory data that the router allows is also recorded.
Cert trusted: <subject name>	The router has verified the path of the certificate with the listed subject name.
Due to <reason codes>, cert not trusted: <subject name>	Due to the reasons listed, the certificate with the listed subject name did not pass the path verification. The recorded reason codes are only approximate reasons for not trusting the certificate. See Table 133 for the corresponding descriptions of the codes.

Table 133 Certificate Path Verification Failure Reason Codes

Code	Description
1	Algorithm mismatch between the certificate and the search constraints.
2	Key usage mismatch between the certificate and the search constraints.
3	Certificate was not valid in the time interval.
4	(Not used)
5	Certificate is not valid.
6	Certificate signature was not verified correctly.
7	Certificate was revoked by a CRL.
8	Certificate was not added to the cache.
9	Certificate decoding failed.
10	Certificate was not found (anywhere).
11	Certificate chain looped (did not find trusted root).
12	Certificate contains critical extension that was not handled.
13	Certificate issuer was not valid (CA specific information missing).
14	(Not used)
15	CRL is too old.
16	CRL is not valid.
17	CRL signature was not verified correctly.
18	CRL was not found (anywhere).
19	CRL was not added to the cache.
20	CRL decoding failed.
21	CRL is not currently valid, but in the future.
22	CRL contains duplicate serial numbers.
23	Time interval is not continuous.
24	Time information not available.
25	Database method failed due to timeout.
26	Database method failed.
27	Path was not verified.
28	Maximum path length reached.

Log Commands

Go to the command interpreter interface (the Command Interpreter Appendix explains how to access and use the commands).

Configuring what you want the BCM50a Integrated Router to log

Use the `sys logs load` command to load the log setting buffer that allows you to configure which logs the BCM50a Integrated Router is to record.

Use `sys logs category` followed by a log category and a parameter to decide what to record.

Table 134 Log categories and available settings

Log Categories	Available Parameters
access	0, 1, 2, 3
attack	0, 1, 2, 3
error	0, 1, 2, 3
ike	0, 1, 2, 3
ipsec	0, 1, 2, 3
javablocked	0, 1, 2, 3
mten	0, 1
upnp	0, 1
urlblocked	0, 1, 2, 3
urlforward	0, 1
	Use 0 to record no logs for a selected category, 1 to record only logs a selected category, 2 to record only alerts for a selected category, and 3 to record both logs and alerts for a selected category.

Use the `sys logs save` command to store the settings in the BCM50a Integrated Router (you must do this in order to record logs).

Displaying Logs

Use the `sys logs display` command to show all of the logs in the BCM50a Integrated Router log.

Use the `sys logs category display` command to show the log settings for all of the log categories.

Use the `sys logs display [log category]` command to show the logs in an individual BCM50a Integrated Router log category.

Use the `sys logs clear` command to erase all of the BCM50a Integrated Router logs.

Log Command Example

This example shows how to set the BCM50a Integrated Router to record the access logs and alerts and then view the results.

```

ras> sys logs load
ras> sys logs category access 3
ras> sys logs save
ras> sys logs display access

```

#	.time	source	destination	notes
0	11/11/2002 15:10:12	172.22.3.80:137	172.22.255.255:137	ACCESS
	BLOCK			
	Firewall default policy: UDP(set:8)			
1	11/11/2002 15:10:12	172.21.4.17:138	172.21.255.255:138	ACCESS
	BLOCK			
	Firewall default policy: UDP(set:8)			
2	11/11/2002 15:10:11	172.17.2.1	224.0.1.60	ACCESS BLOCK
	Firewall default policy: IGMP(set:8)			
3	11/11/2002 15:10:11	172.22.3.80:137	172.22.255.255:137	ACCESS
	BLOCK			
	Firewall default policy: UDP(set:8)			
4	11/11/2002 15:10:10	192.168.10.1:520	192.168.10.255:520	ACCESS
	BLOCK			
	Firewall default policy: UDP(set:8)			
5	11/11/2002 15:10:10	172.21.4.67:137	172.21.255.255:137	ACCESS
	BLOCK			

Index

Numbers

3DES 197

4-Port Switch 33

A

Action 169

Action for Matched Packets 172

ActiveX 189

Administrator Inactivity Timer 77

ADSL standards 32

AES 197

AH 196

AH Protocol 196

Alert 169

Allocated Budget 116

Allow Through IPSec Tunnel 239

Allow Trigger Dial 109

Always On 116

Answer 119

Application-level Firewalls 146

Applications 39

AT Command Initial String 114

AT Command Strings 117, 119

AT Response Strings 119

ATDP 117

ATH 117

ATM loopback test 386

Attack Alert 182, 184

Attack Types 152

Authentication Header 196

Authentication Type 114

Autonegotiating 10/100 Mb/s Ethernet LAN 34

Autosensing 10/100 Mb/s Ethernet LAN 34

B

Backup 390

Bandwidth Class 292

Bandwidth Filter 292, 299

Bandwidth Management 291

Bandwidth Management Statistics 300

Bandwidth Manager Class Configuration 297

Bandwidth Manager Class Setup 295

Bandwidth Manager Monitor 302

Bandwidth Manager Summary 294

Blocking Time 183, 185

Branch Office 213

Branch Tunnel NAT Address Mapping Rule 224

Broadcast Dial Backup Route 116

Brute force Attack 151

Brute Force Password Guessing Protection 35

Budget 116

Bypass Triangle Route 169

C

Cable Modem 147

Call Back Delay 120

Call Control 119

Call Scheduling 36, 373

- Maximum Number of Schedule Sets 373, 377
- Precedence 373
- Precedence Example 373

Called ID 119

Calling Line Identification 119

Central Network Management 37

CHAP 114

CLID 119

Client IKE Source Port Switching 249

Client Minimum Version 250

Client Termination 240, 247

Client Termination IP Pool 246

Configuration 383

Content Filtering 36, 187

- Days and Times 187

- Restrict Web Features 187

Contivity Client 206

Contivity VPN Client 203

Contivity VPN Client Software 34, 240

conventions, text 27

Cookies 189

copyright 2

CPU utilization 382

Custom Port 172

Custom Ports

- Creating/Editing 174

D

Data Terminal Ready 117

DDNS Type 80

Default 389

Default Policy Log 169

Default Server 130

Default Server IP Address 129

Denial of Service 147, 148, 182, 183

DES 197

Destination Address 164, 172

DHCP 59, 79, 89, 90, 383

DHCP (Dynamic Host Configuration Protocol) 38

DHCP Server 93

diagnostic 384

Dial 119

Dial Backup 112

Dial Backup Port Speed 114

Dial Timeout 119

DNS 75, 343

DNS Relay 62

DNS Server

- For VPN Host 75

DNS server 62

DNS Servers 90

Domain Name 77, 128

DoS

- Basics 148

- Types 149

DoS (Denial of Service) 35

downstream noise margin 386

Drop 119

Drop DTR When Hang Up 119

Drop Timeout 119

DTE 117

DTR 117

DTR Signal 117

Dynamic DNS 79

Dynamic DNS Service Provider 80

Dynamic DNS Support 36

Dynamic Host Configuration Protocol 89

dynamic IP address 54

DYNDNS Wildcard 79, 81

E

ECHO 128

Enable Wildcard 81
Encapsulating Security Payload 196
Encapsulation 47, 50
 ENET ENCAP 47
 PPP over Ethernet 48
 PPPoA 48
 RFC 1483 48
encapsulation 33
encapsulation method 47
ENET ENCAP 47
ESP 196
ESP Protocol 196

F

Factory LAN Defaults 90
Failover Tuning 249
Features 31
Finger 128
Firewall 35
 Access Methods 161
 Address Type 173
 Alerts 181
 Connection Direction 164
 Creating/Editing Rules 170
 Custom Ports 174
 Enabling 161
 Firewall Vs. Filters 158
 Guidelines For Enhancing Security 158
 Introduction 147
 LAN to WAN Rules 165
 Policies 161
 Rule Checklist 163
 Rule Logic 163
 Rule Security Ramifications 163
 Services 178
 Types 145
 When To Use 160
Firmware Version 380
 380
First DNS Server 78

FTP 79, 127, 128, 315, 338
FTP Restrictions 315
FTP Server 39
Full Feature 107
Full Network Management 38

G

General Setup 76
Global 122
Global End IP 132, 135
Global Start IP 132, 134
Group Authentication 209
Group ID 209, 242
Group Password 209, 242

H

Half-Open Sessions 182
Host 82
Host Names 80
How SSH works 330
HTTP 128, 146, 148, 149
HTTPS 35, 317
HTTPS Example 320

I

IANA 52
ICMP Commands That Trigger Alerts 152
ICMP echo 151
ICMP Vulnerability 152
Idle Timeout 116
IGMP 91, 109, 116
IGMP-V1 109
IGMP-v1 116
IGMP-V2 109
IGMP-v2 116

Illegal Commands 152
Initial Contact Payload 250
Inside 122
Inside Global Address 122
Inside Local Address 122
Internet access 32
Internet Assigned Number Authority (IANA) 51
Internet Assigned Numbers Authority 52
Internet Control Message Protocol (ICMP) 151
Internet Group Multicast Protocol 91, 109
IP Address 51, 127, 383
IP Address Assignment 51
 ENET ENCAP 52
 PPPoA or PPPoE 52
 RFC 1483 52
IP Alias 37, 97
IP Multicast 37
 Internet Group Management Protocol
 (IGMP) 37
IP Pool Setup 59, 89
IP Ports 149
IP Spoofing 149, 153
IP Static Route 140
IPSec VPN Capability 34, 35
ISAKMP Initial Contact Payload 250

J

Java 189

K

Key Fields For Configuring Rules 164

L

LAN IP Address 367, 370
LAN Setup 89, 99
LAN TCP/IP 90

LAN to WAN Rules 165
LAND 150, 151
Local 122
Local End IP 132, 134
Local Start IP 132, 134
Log 169
Logging 38
Logs 359

M

MAC Addresses 95
MAC Encapsulated Routing Link Protocol 47
MAIN MENU 45
Management Information Base (MIB) 340
Many One-to-One 133, 134
Many to Many No Overload 125
Many to Many Overload 125
Many to One 125
Many-to-Many Ov 134
Many-to-Many Overload 133, 134
Many-to-On 134
Many-to-One 133
Maximum Incomplete High 185
Maximum Incomplete Low 185
Max-incomplete High 183
Max-incomplete Low 183, 185
MD5 197
Media Access Control 95
Metric 99, 108, 114, 143
Mode 50
Multicast 91, 109, 116
Multicast Version 116
Multiplexing 33, 48
 LLC-based 49
 VC-based 49
multiplexing method 48, 50

Multiprotocol Encapsulation 48

My Password 307, 313

N

Nailed-Up Connection 53

NAT 53, 107, 115, 127, 128, 129, 130

Application 124

Definitions 121

How NAT Works 123

Mapping Types 125

Port Restricted Cone 123

Restricted Cone 123

What NAT does 122

NAT Traversal 249, 347, 348, 349

NetBIOS commands 152

NetBIOS over TCP/IP 109, 239

Network Address Translation 53, 107, 115

Network Address Translation (NAT) 37

Network Management 128

NNTP 128

Number of Retransmissions 249

O

Obtained From ISP 62

Off Line 81

On Demand Client Tunnel 209

One Minute High 185

One Minute Low 184

One to One 125

One-Minute High 183

One-to-One 134

Outside 122

P

Packet Direction 169, 171

Packet Filtering 36, 159

Packet Filtering Firewalls 146

PAP 114

Password 42, 81, 307, 313

Password Management 251

PAT 134

Permanent Virtual Circuit 48

Phone Number 114

ping 386

Ping of Death 149

Point to Point Protocol over ATM Adaptation
Layer 5 48

Point-to-Point Protocol over Ethernet 102

Point-to-Point Tunneling Protocol 128

POP3 128, 148, 149

Port Configuration 174

Port Forwarding 38

Port Restricted Cone NAT 123

PPP over Ethernet 48

PPPoE 36, 48

PPPoE Encapsulation 102

PPPoE Pass Through 105

PPTP 128

Predefined NTP Time Server List 83

Preshared Key 206, 232

Primary Phone Number 114

Priority 114

Private 108, 143

private IP address 51

Proportional Bandwidth Allocation 292

Protocol/Port 367, 369

publications

hard copy 28

related 28

PVC 48

R

- reboot 386
- regulatory information 2
- reinitialize the ADSL line 386
- Remote Management and NAT 316
- Remote Management Limitations 315
- Reports 364
- reset 386
- Reset Button 34
- Response Strings 117
- Restore 390
- Restrict Web Features 189
- Retransmissions 249
- Retry Count 119
- Retry Interval 119
- RFC 2516 48
- RIP 90, 91, 115
 - RIP Direction 91, 108
 - RIP Version 90, 108, 115
 - RIP-1 90, 108, 115
 - RIP-2 90
 - RIP-2B 91, 108, 115
 - RIP-2M 91, 108, 115
- Root Class 295
- Routing Information Protocol 90
- Rule Summary 177
- Rules 161, 166
 - Checklist 163
 - Creating Custom 161
 - Key Fields 164
 - LAN to WAN 165
 - Logic 163
 - Predefined Services 178
 - Source and Destination Addresses 173

S

- SA Monitor 237
- Saving the State 153
- Schedule Sets
 - Duration 376
- Second DNS Server 78
- Secondary Phone Number 114
- Secure FTP Using SSH Example 335
- Secure Telnet Using SSH Example 333
- Security Ramifications 163
- Server 86, 125, 126, 133, 134
 - Server Auto-detect 81
- Service 164
- Service Type 169, 174
- Services 128
 - setup a schedule 375
- SHA1 197
- Single User Account 115, 134
- SMTP 128
- Smurf 151, 152
- SNMP 37, 128, 339
 - Get 341
 - Manager 340
 - MIBs 341
 - Trap 341
- SNMP (Simple Network Management Protocol) 37
- Source & Destination Addresses 173
- Source Address 164, 172
- SSH 35, 329
 - SSH Implementation 331
- Start Port 138
- Stateful Inspection 35, 145, 146, 153, 154, 155
 - Process 154
- Static DHCP 95
- static IP address 54

Static Route 139, 140
SUA 127, 128, 130
SUA (Single User Account) 126
SUA Only 107
SUA Server 129
Subclass Layers 295
Subnet Mask 51, 173
subnet mask 51
SYN Flood 150, 151
SYN-ACK 150
Syslog 177
System DNS Servers 78
System General Setup 77
System Name 77
System Screens 75
System Timeout 316
System up Time 382

T

TA 117
TCP Maximum Incomplete 183, 184, 185
TCP Security 156
TCP/IP 148, 149, 150, 336
Teardrop 149
technical publications 28
Telnet 336
Telnet Configuration 336
text conventions 27
TFTP Restrictions 315
Third DNS Server 78
Threshold Values 182
Time and Date 34
Time Setting 84
Traceroute 153
Tracing 38

trademarks 2
Traffic Redirect 38, 109, 110
Trigger Port Forwarding
Process 135

U

UDP/ICMP Security 157
Universal Plug and Play 36
Universal Plug and Play (UPnP) 347, 349
Upgradeable Firmware 39
UPnP 36
UPnP Examples 351
UPnP Port Mapping 350
Upper Layer Protocols 157
upstream noise margin 386
URL Keyword Blocking 189
User defined DNS server 62
User Profiles 303
Username 42

V

VCI 49, 50
Virtual Channel Identifier (VCI) 49
virtual circuit (VC) 48
Virtual Path Identifier (VPI) 49
VPI 49, 50
VPI & VCI 49

W

WAN to LAN Rules 166
Web Proxy 189
Web Site Hits 367
WebGUI 41, 44, 147, 158, 164
Windows Networking 109, 239
Wizard Setup 47

[WWW](#) 318