



# **BorderGuard™ 6000 Series**

---

## **Release Notes Through FFW 7.4-17**

Version 14  
March 2007

Blue Ridge Networks, Inc.  
14120 Parke Long Court  
Chantilly, VA 20151

## 1.0 Introduction

The BorderGuard™ 6000 Release Notes describe the new features and differences found in the Blue Ridge Networks BorderGuard 6000 series VPN appliance products. This document is primarily intended as a reference for those familiar with the existing BorderGuard product line, and it assumes a familiarity with previous BorderGuard products. The BorderGuard 6000 family offers a range of capacity across multiple models as shown in the table below.

Model	10/100 Ethernet Ports	10/100/1000 Ethernet Ports	Nominal Maximum AES256 Throughput (Mbps)	Maximum Concurrent Tunnels	4096 bit RSA and Diffie-Hellman Keys
6100	2	0	20	150	no
6200	3	0	45	300	no
6400	3	0	100	600	no
6500	1	2	200	1,000	yes
6600	1	2	400	1,500	yes

Table 1-1 BorderGuard 6000 Series Products

## 2.0 BorderGuard 6000 Series Hardware

The BorderGuard 6000 is based on the same hardware as the BorderGuard 5000. It also has the same mounting, power and cabling requirements, and it is backwards compatible with previous models of the BorderGuard product line. Troubleshooting procedures for the BorderGuard 6000 are similar to those for the earlier products.

### 2.1 Processor Core

Models in the BorderGuard 6000 series use an IBM 440GX core processor running at 667MHz.

### 2.2 Memory

BorderGuard 6000 models are configured with 128 Mbytes of Double Data Rate (DDR) SDRAM operating at 166MHz. This RAM is used in executing code, processing packet data buffers and as working storage. Permanent storage of operating software and site configuration data is provided by 32Mbytes of Flash memory.

### 2.3 Cryptography

Some BorderGuard 6000 models (6400, 6500, and 6600) use a Hifn 7855 hardware encryption accelerator to improve the performance of the DES, Triple-DES, AES, LZS, MD5, and SHA1 cryptographic algorithms. The BorderGuard 6000 series also

optionally supports a removable USB-based Smart Card that is cryptographically mated to the chassis. Removing the USB Smart Card disables the chassis boot firmware to provide added security for units in transit or for unattended operation.

## 2.4 Interfaces

BorderGuard 6000 models provide up to three Ethernet interfaces with link speeds as shown in the table in section 1.0. The three external ports will use the same form of the RJ45 connector used on the BorderGuard 5000, and the LED indicating link speed provides dual color feedback. The green and amber colors will be used per the table listed below.

Link speed	RJ45 LED Color
10Mb/sec	OFF
100Mb/sec	Green
1000Mb/sec	Amber

Table 2-1 BorderGuard Interfaces

## 3.0 Firmware Release Notes

### 3.1 Firmware Release 7.4-17 (March 2007)

The following sections describe the changes incorporated in 7.4-17 firmware.

#### 3.1.1 DPF Segmentation

Special “segmentation” processing has been added to the firmware to avoid fragmentation of DPF packets. The “segmentation” feature uses a default MTU of 1400 for each tunnel, but an extension has been added to the `dpf set sleeve` command to allow each MTU value to be explicitly defined.

```
dpf set sleeve <sleeve name pattern> mtu_out <integer value>
```

In addition, the `dpf show sleeve_definitions` command will now display the mtu values of tunnels, if the remote devices support dpf “segmentation”. If the remote device does not support “segmentation”, this will be noted in the printout.

```
dpf show sleeve_definitions
Sleeve Name:sleeve0 Status:ENABLED MTU:1400
```

or

```
dpf show sleeve_definitions
Sleeve Name: sleeve0 Status:ENABLED MTU:remote device does
not support segmentation
```

### 3.2 Firmware Release 7.4-15 (November 2006)

The following sections describe the changes incorporated in 7.4-15 firmware.

### 3.2.1 X.509 Policy Processing

Note: Changes in processing X.509 policies are only relevant to BG6000 systems.

There is no longer a limit on the number of values associated with a certificate attribute when defining a policy rule. This is required to support “custom groups” or “green list” where field attributes (such as CN information) are imported from an external source and used to define a remote access user group. In addition, the BG6000 will examine each field in the certificate even if an attribute is repeated; e.g. OU=USA OU=Testing.

## 3.3 Firmware Release 7.4-14 (October 2006)

The following sections describe the changes incorporated in 7.4-14 firmware.

### 3.3.1 DHCP Operation

The BorderGuard's DHCP server will now start, even when interface links are down.

### 3.3.2 Command Enhancement

The `dpf show slan` command will now display the mode, topology, and current state. If the sleeve is up, the current state is “active” and the sleeve name will be shown. Typically, more than one sleeve is assigned to the LAN. If this is the case each sleeve will be listed.

```
700090 System 5> dpf show slan
Installed Sleeve LANs
LAN      Mode      Topology   Sleeve    Current
State
sp16     passive  mesh      <Undefined> DOWN
```

## 3.4 Firmware Release 7.4-12 (September 2006)

The following sections describe the changes incorporated in 7.4-12 firmware.

### 3.4.1 Expanded Range of UDP Ports

The range of allowable UDP ports has now been expanded to include ports between 1 and 65535.

## 3.5 Firmware Release 7.4-11 (September 2006)

The following sections describe the changes incorporated in 7.4-11 firmware.

### 3.5.1 RemoteLink Support

Two features have been added to the firmware to better enable configuration and management of BorderGuard remote access servers to work with the new BorderGuard RemoteLink product.

- ToS (Type of Service) settings have been added as DPF sleeve parameters. This enables modification of ToS settings on bridged traffic based on client requirements. The commands are fully compatible with ToS NetSentry filters and have the same semantics.

```
dpf define sleeve foo tos stamp <number>
dpf define sleeve foo tos or <number>
dpf define sleeve foo tos and <number>
```

- The RemoteLink serial number is included in console display text and log messages. This enables better tracking of these remote devices.

### 3.6 Firmware Release 7.4-10 (June 2006)

The following sections describe the changes incorporated in 7.4-10 firmware.

#### 3.6.1 Improved Performance

The maximum number of Hifn sessions has been increased. This was found to improve overall performance, allowing the BorderGuard to support up to 3000 simultaneous tunnels.

#### 3.6.2 Link Testing Facility

A link test facility is now operational for the BorderGuard and can be used to perform link-level checkout of the interfaces.

To enable testing, enter the following command from the system prompt:

```
System> Test ifs interface_name on
```

Testing will be enabled, but will not be initiated until you issue the following command:

```
System> Test ifs interface_name start
```

The format for the *test ifs* command is as follows:

```
Test ifs interface_name [count number_of_packets]
                        [delay milliseconds]
                        [[no]echo_test]
                        [fixed pattern]
                        [[no]halt]
                        [increment]
                        [length bytes]
                        [mac_dest MAC_address]
                        [max bytes]
                        [min bytes]
                        [off]
                        [on]
                        [random]
                        [received]
                        [[no]report]
                        [setup]
```

[start]  
[stats]  
[stop]  
[[no]sweep]  
[timeout seconds]  
[transmitted]  
[[no]verify]

**count**

The number of test packets that will be sent when the test is started. The default is 10 packets.

**delay**

The number of milliseconds that will elapse between sending each test packet. The default is 10 milliseconds.

**[no]echo\_test**

Indicates whether or not the test packet will be returned (echoed) to the sender. The default is to echo the packet.

**fixed**

Indicates that a fixed test pattern will be sent. The range of patterns is from 0x0 to 0xFFFFFFFF. The default pattern is 0xFFFFFFFF.

**[no]halt**

Indicates whether or not the test should be halted when an error occurs. The default is halt.

**increment**

Indicates that the test packets will contain data that increments with each packet sent.

**length**

The amount of data to be sent in each test packet. The data is repeated sets of the chosen data type.

**mac\_dest**

Specifies a MAC address for testing an Ethernet interface. Use of a multicast or broadcast address is only recommended when a single peer Ethernet node is connected.

**max**

The maximum length of a test packet when using the sweep option. The default is 1000 bytes.

**min**

The minimum length of a test packet when using the sweep option. The default is 50 bytes.

**off**

Disables interface testing.

**on**

Enables interface testing.

**random**

Generates a pseudo-random pattern for the test packets.

**received**

Displays the received PIB. (Packet Information Block; this is an internal data structure.)

**[no]report**

Indicates whether or not a report will be generated for the test facility. The default is to generate a report.

**setup**

Displays the current setting of the test parameters.

**start**

Initiates the test using the current parameter settings.

**stats**

Displays current statistics for the test in progress.

**stop**

Stops the test.

**[no]sweep**

Indicates whether or not the length of the data in each packet will be incremented from the minimum setting to the maximum setting. If the number of packets sent is such that the maximum length is reached, the size drops back to the minimum and the sweep begins again.

**timeout**

The number of seconds allowed between sending an echo packet and its return. If this timeout is exceeded, an error is returned. The default is 3 seconds.

**transmitted**

Displays the transmitted PIB.

**[no]verify**

Indicates whether or not the received test data will be checked with the transmitted test data. If the data does not match, an error is returned. The default is verify.

To alter these parameters, use the test command as shown in the following example:

```
System> test ifs en01 increment
```

This example will change the test parameters to use an incrementing bytes test instead of the fixed test pattern.

The current statistics for a test in progress can be checked, as shown in the following example:

```
BG5050 System> test ifs en01 stat
Run state = ON
transmit packets = 134472
retransmit packets = 0
receive packets = 134475
data errors = 0
size miscompare errors = 0
sequence errors = 0
test packet PIB address = 0x710428
```

This display provides the following information:

- Whether or not a test is currently running.
- The number of packets sent and received.
- The number of data, size, and sequence errors detected.
- The PIB address of the test packet.

### **3.6.3 Bug Fixes**

Bug fixes for this firmware release have resolved the following issues:

- Fixed a problem with ToS (Type of Service) Expediting where the stamping filter was not placing the correct value in the ToS field of the IP packet.
- Corrected an issue with command line processing of dotted decimal notation. IP address entries that had leading zeroes were erroneously treated as octal rather than decimal numbers.

### **3.6.4 Known Anomalies**

There are no known anomalies in this release.

## **3.7 Firmware Release 7.4-9 (May 2006)**

The following sections describe the changes incorporated in the 7.4-9 firmware.

### **3.7.1 Bug Fixes**

An issue with the contention logic for “originator”/ “responder” roles has been corrected to better enable secure tunnels to be established. In addition, this release addresses changes related to the use of “fixed packet length” settings with routed VPN configurations. It has corrected processing when “fixed packet length” settings are used with secure tunnel bridging.

### **3.7.2 Known Anomalies**

There are no known anomalies in this release.

## **3.8 Firmware Release 7.4-8 (March 2006)**

This release incorporates internal enhancements to the firmware including the improved processing of DHCP lease files. This eliminates an earlier issue with extremely large DHCP lease files. There are no new system features with this release.

### **3.8.1 Bug Fixes**

There are no bug fixes to report.

### **3.8.2 Known Anomalies**

There are no known anomalies in this release.

### 3.9 Firmware Release 7.4-6 (February 2006)

The following sections describe the changes incorporated in the 7.4-6 firmware. This firmware release is the initial release of firmware to fully support the Compact BorderGuard models.

#### 3.9.1 VLAN Tagging

Enhancements have been made to the firmware that will enable remote client PC's that have enabled IEEE 802.1Q VLAN tagging to communicate with their home networks using the BorderGuard and layer 2 cryptographic tunneling.

This is a very basic implementation in that it is not designed to give the BorderGuard any significant control over VLAN connectivity and VLAN tags. Rather, it provides the minimum needed so that 802.1Q aware remote client PCs can properly interact with 802.1Q aware hosts and switches on their home network.

Basically, the changes have two limited goals:

- The bridge code will successfully forward packets to other bridge ports that have VLAN tags within them. These VLAN capable bridge ports include sleeve ports for secure tunnel bridging and sleeve LAN's for PC clients. Routing of packets causes the VLAN tag to be stripped and its contents lost.
- Filtering of bridge packets will take place as if the VLAN tag were not present.

Specifically, the changes provide no means of generating, inspecting, or modifying VLAN tags in a bridged packet that flows through the BorderGuard.

#### 3.9.2 Type of Service (TOS) Expediting (all models)

Enhancements for VoIP (Voice over Internet Protocol) and other high-priority packets have been made to the firmware that will permit both preferential scheduling of packets with certain TOS values, and will permit the writer of packet filters to examine and alter the contents of the TOS field as described in RFC 791.

There are two command options to change the values of the TOS field that will qualify for higher priority queues on an individual interface basis:

- `set if enxx hitos <value>`
- `set if enxx midtos <value>`

The <value> here is usually entered as a hexadecimal number in the range 0-0xff.

This number simultaneously specifies:

- The minimum precedence that qualifies a packet for the High or Medium queue.
- A mask against the (D,T,R) bits. If the packets TOS and the (D,T,R) mask is nonzero, then the packet will also be placed into the respective queue.

In addition to the special facilities used to sort packets into priority queues, filtering can be used to identify packets by their IP Type of Service and modify the Type Of Service field in an enroute packet to correct the labeling policy on the part of site hosts.

The following filters can be used:

- `ip_tos` pattern - This filter pattern extracts the Type of Service field if the packet is an IP datagram, and compares it against a certain range of values. Further, filtering supports the extraction of bit fields within any packet field, which is quite useful in the case of type of service.
- `ip_stamp_tos` action - This filtering action takes an argument in the range 0 through 255 and places it in the Type Of Service field of an IP packet. It has no effect if the target packet is not IP.

`ip_stamp_tos <value>`

The `<value>` is entered as a decimal number (such as 224) or a hexadecimal number (in the form 0xe0).

- `ip_or_tos` action - This filtering action takes an argument in the range 0 through 255 and logically OR's it with the Type Of Service field of an IP packet. It has no effect if the target packet is not IP.

`ip_or_tos <value>`

The `<value>` is entered as a decimal number (such as 16) or a hexadecimal number (in the form 0x10).

- `ip_and_tos` action - This filtering action takes an argument in the range 0 through 255 and logically AND's it with the Type Of Service field of an IP packet. It has no effect if the target packet is not IP.

`ip_and_tos <value>`

The `<value>` is entered as a decimal number (such as 31) or a hexadecimal number (in the form 0x1F).

A more extensive description of Type Of Service (TOS) expediting is included in the latest BorderGuard reference manuals.

### 3.9.3 New and Enhanced Commands (all models)

The following commands have been added to the firmware:

#### 1. `system ifenv n-`

Similar to the `ifexists` command, the `ifenv` command does its comparison with an environmental variable. If the expression is true, the command file is executed. If both the variable and the target string are numeric, a numerical comparison is made; otherwise, a string comparison is made.

```

system ifenv <env name> eq <string>then<@command>
                        ne
                        lt
                        le
                        gt
                        ge
                        defined
                        not defined
                        !defined

```

Examples:

```

sys ifenv vpn_conf eq "bitw" then @bitw.cmd
sys ifenv num_ports ge 3 then @extra_ports.cmd

```

## 2. system echo <string>

The text string will be printed to the console (either serial or Telnet).

Example:

```

sys echo "test scenario #33"

```

## 3. system increment [from<number>|<ip>] to<number>|<ip> [by<number>|<ip>] format <format>

The increment command can be used to generate a large number of similar commands which differ only by an incrementing number or IP address. The format parameter can contain text and a single print "%" parameter. Results can be piped into a command file for later execution. The default for the *from* and *by* parameter is one. The command can also decrement by making the *from* parameter larger than the *to* parameter.

Examples:

```

sys increment to 10 format "dpf define sleeve
vpn%02d">sleeve.cmd

```

```

sys increment from 192.168.1.0 to 192.168.255.0 by
256
format "ip define route %I netmask
255.255.255.0" next 10.1>route.cmd

```

The following commands have been enhanced in the firmware:

## 4. dpf establish sleeve <pattern>[except<pattern>...]

Instead of a single sleeve name, a pattern can be used and optional exceptions applied.

**Examples:**

```
# all defined sleeves established (except the
predefined default sleeve)
dpf establish sleeve *

# establish all sleeves starting with 's' except
those starting with 'sa'
dpf establish sleeve s* except sa*
```

**5.** dpf set sleeve <pattern>[except<pattern>...]

Multiple sleeves can have their attributes changed.

**Examples:**

```
# all defined sleeves set to long keys (except the
predefined default sleeve)
dpf set sleeve * key long

# set all sleeves with a 'b' as the second
character except those starting with 'sb' or
those starting with 'xb'
dpf set sleeve?b* except sb* xb*
```

**6.** dpf terminate session <session  
#>|\*[except<pattern>...]

Multiple sessions can now be terminated with one command.

**Examples:**

```
# terminate all sessions
dpf terminate session *

# terminate all sessions except those whose sleeve
name starts with 'sa'
dpf terminate session * except sa*
```

**7.** dpf undefine sleeve <pattern>[except<pattern>...]

Multiple sleeves can be undefined.

Examples:

```
# all defined sleeves can be undefined (except the
predefined default sleeve)

dpf undefine sleeve *

# undefine sleeves except those starting with `sa`
dpf undefined sleeve * except sa
```

### 3.9.4 Factory Reset of BorderGuards (all models)

The new convention for firmware behavior for all BorderGuard models will be to react to a "reset to default settings"/"factory reset" by clearing the keys, formatting the low and high file systems (lfs and hfs), and enabling all possible ports (available ports are based on model designations) with a default IP/Subnet. The default IP/Subnet will be different for each port, and will be based on the following scheme:

192.168.25X.1

For example, on BorderGuard 6000 models 6500 and 6600 (3 ports), this will result in setting:

```
EN01 = 192.168.251.1
EN02 = 192.168.252.1
EN03 = 192.168.253.1
```

And on BorderGuard 6000 model 6100 (2 ports), this will result in setting:

```
EN01 = 192.168.251.1
EN02 = 192.168.252.1
```

### 3.9.5 Bug Fixes

There are no bug fixes to report.

### 3.9.6 Known Anomalies

Extremely large DHCP lease files can contribute to sluggish system response. This issue will be corrected in the next 7.4 release.

## 3.10 Firmware Release 7.3-10 (November 2005)

The following sections describe the changes incorporated in the 7.3-10 firmware.

### 3.10.1 DHCP Server

Enhancements have been added to DCHP start/stop and DHCP event logging.

### 3.10.2 Bug Fixes in 7.3-10

Bug fixes for this firmware release resolve an issue in the file system related to the condense processing during file edits.

## 3.11 Firmware Release 7.3-9 (September 2005)

The following sections describe the changes incorporated in the 7.3-9 firmware.

### 3.11.1 Firmware Encryption

Firmware encryption has been updated to include SHA256 as an option.

### 3.11.2 Firmware Commands Updates

The "\*" (asterisk) was added as an option when entering some commands on the command line of the terminal emulator. These commands include:

- Establish Session
- Terminate Session
- Define Sleeve
- Undefine Sleeve

For descriptions on these and other commands, please refer to the latest BorderGuard Reference Manual.

### 3.11.3 Multi-DPF

The command `dpf set address <ip>` has a slight change in its semantics. Prior to the new multi-dpf feature, if you set an ip address, it would replace the current ip address if any existed. Now the new address is added to a list of DPF addresses. If the address is already in the list, the new set address command is ignored.

### 3.11.4 DHCP Server

A Dynamic Host Configuration (DHCP) server has been incorporated in this release of BorderGuard firmware. The server daemon must be activated in a startup file or via the command line, and server options are declared in a config file, "dhcpd.conf." The syntax for declaring options, and the names and formats of the options that can be declared, are available in a separate document.

### 3.11.5 Reset Pin

The factory reset pin at the back of the BorderGuard has been tuned to enable two types of resets; a "soft" reset, or a full "factory reset." Depressing the reset pin for 10 seconds will result in a soft reset which will perform a re-boot of the BorderGuard. Depressing the reset pin for at least 30 seconds will cause a full factory reset which is exactly like a disk reformatting command. The factory reset erases all keys and data from the device rendering the data irretrievable. (Details on the reset options are documented in the BorderGuard Reference Manual, Appendix F.)

### 3.11.6 DPF Multi UDP Ports

The changes to multi UDP ports include an update to set udpports, and a new command, clear udpports. The system still supports the old syntax of dpf set udpports min <port> max <port>. Now, the command can be entered multiple times, and it will not replace, but rather add the new ports. A single port number can also be entered rather than a range, i.e., set udpport 820. The dpf clear udpports command can also be used to clear the port settings to start over. In addition, there are minor changes to the display where a comma delimited list form is used and ranges use the “..” notation.

### 3.11.7 TAR with Compression

A compress parameter when creating a tarball has been added. The extraction does not require the compress parameter as it queries the file to see if it is compressed.

```
Sys tar create test.tar .....compress.....
```

### 3.11.8 Command Line Macros

The command line processor and the filter compiler will now allow macros. The macros are defined with an environment variable prefixed with a % (percent sign). If the environment variable is defined, the variable will be expanded to its value when the command line is processed.

```
Sys set env IP = "192.168.1.1"
Ip start if en01 %IP
Dpf set address %IP
Filter my_ip ip_sa in (%IP) succeed; end
```

## 3.12 Firmware Release 7.3-6 (August 2005)

The following sections describe the changes incorporated in the 7.3-6 firmware. This firmware release is the first version to fully support the BorderGuard 6000 models.

### 3.12.1 Supports Standard (X.509) Certificates

The X.509 standard refers to a very commonly encountered form of digital certificates, where an X.509 digital certificate contains the holder's public key as well as the holder's identity information such as name, organization, etc. In X.509 deployments, a Certificate Authority, or CA, is responsible for verifying the identity of certificate holders, publishing the public key certificate for previously issued certificates, responding to authenticated requests for certificate revocation, and providing notification of any certificate revocations.

The BorderGuard 6000 family uses the BG6000 Management Console (MC) to provide CA functionality and to proxy enterprise information requests to external CAs. The MC provides information to the BorderGuard 6000 about the status of X.509 certificates that are presented from other BorderGuards or from VPN Client software.

The BG6000 MC can be configured to use either CRL (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) or both to perform certificate status checking.

The following commands have been added to the BorderGuard's new IPsec facility to support X.509 processing:

*ipsec load cert id "FileName"*

This command loads the identity certificate provided via file "FileName"

*ipsec load cert root "FileName"*

This command loads the root certificate provided via file "FileName"

*ipsec load rule "FileName"*

This command loads the rule provided via file "FileName"

*ipsec drop cert id "FileName"*

This command drops the identity certificate denoted via file "FileName"

*ipsec drop cert root "FileName"*

This command drops the root certificate denoted via file "FileName"

*ipsec drop rule*

This command drops all rules and policies.

*ipsec show cert id*

This command lists identity certs.

*ipsec show cert root*

This command lists root certs.

*ipsec show rule*

This command displays the current loaded rule and policy on the BG

*ipsec show OCSP*

This command lists configuration information for the OCSP server and the "Path Discover" URL.

The following command has been added to the BorderGuard's dpf facility to support X.509 processing:

*dpf show dsleeve*

This command provides details about dynamic sleeves

### 3.13 Firmware Release 7.33-1 (June 2005)

The following sections describe the changes incorporated in the 7.33-1 firmware.

#### 3.13.1 Protocol Conformance

This new feature addresses the external “signal” characteristics of the DPF packets being emitted by the BorderGuard and/or the Blue Ridge VPN Client. In the 7.33-1 firmware release, Protocol Conformance is only supported for remote access (no site-to-site), and the remote access solution must use UDP as the transport protocol. In addition, only the most recent VPN Client and VPN Manager releases (version 6.1 Win2K-WinXP clients and version 4.2 VPN Manager) support this feature. More details about Protocol Conformance can be found in the latest BorderGuard Reference Manual.

#### 3.13.2 ARP Aging

Currently a MAC address for an IP address is added to the route table when an ARP Request/Reply message is processed. Over a period of time this can lead to problems if an IP address is reused on a different host. The BorderGuard will only remember the old MAC address and will not ask for an updated MAC address. ARP Aging helps eliminate this problem by slowly aging the MAC addresses and eventually purging them from the system. The BorderGuard will check the MAC address entries every "interval" seconds and add to its age. If the age exceeds the "lifetime" entry, the MAC address is said to be "arp aged" and before the MAC address can be used again, a new ARP Request must be processed. If a MAC address remains in the "ARP aged" state for "purge" minutes, the MAC and IP address are purged from the BorderGuard.

The aging process is only performed on ARP learned MAC addresses and will not effect addresses entered by the user with the defined host command or if an entry is defined as static.

The age of an ARP MAC address can be rejuvenated by a number of events. If an ARP Request/Reply referencing the entry is processed by the BorderGuard, the ARP age is set to zero. If a data packet is received or sent by the BorderGuard that uses the MAC address, the ARP age is set to zero. This way, the most active entries are not purged from the system.

The following new ip commands have been added to support this capability:

*ip start arp\_aging*

This command manually starts ARP aging.

*ip stop arp\_aging*

ARP aging is automatically started at boot time but can be shut down with this stop command.

*ip clear arp\_aging*

This command resets all “ages to zero.

*ip set lifetime <minutes> purge <minutes> interval <seconds>*

This command adjusts the timeouts for the ARPs. The defaults are:

lifetime = 5 minutes

purge = 60 minutes

interval = 15 seconds (legal values are 15,20,30)

*ip display arp\_aging*

This command displays the ARP aging settings and a table of ARP entries.

### 3.14 Firmware Release 7.1 (March 2005)

The following sections describe the changes incorporated in the 7.1 firmware. This firmware release is the first version to fully support the BorderGuard 5000 models.

#### 3.14.1 Enhanced Self-Tests

Self-test logic for codec algorithms has been completely rewritten to use a codec transform. Cryptographic processors are automatically invoked during the “known answer tests.” In addition, the hardware self-tests for all FIPS-approved algorithms (AESxxx, DES, TDES, and HMAC-SHA1) are performed at initialization. The cryptographic processor is disabled if these self-tests fail.

#### 3.14.2 Expanded Discretionary Tests

Hardware (“HW”) and Software (“SW”) options have been added to all codec algorithms for discretionary tests (dpf test xxx hw/sw)

#### 3.14.3 Random Number Generation and Application

The random number seeding logic has been updated in 7.1 firmware. The seed is continually updated in NVRAM (nonvolatile RAM). Note that models with Hifn 7855 support use its hardware random number generation. This change affects the Borderguard 5100 and 5200 only. In addition, the Hifn 7855 processing has been updated to add random data to the next initialization vector after each message sent.

#### 3.14.4 Added TAR Utility

Support has been added for a Tape Archive (TAR) utility. This TAR utility can be used to create or extract an archive and is especially useful in transferring files between systems.

The following new system commands have been added to support this capability:

*system tar create [<tarball name>] [UTC <±n>] [verbose] [files <files name>...]*

This command will create a new archive of all the files in the low file system (/lfs) and the high file system (/hfs). The resultant file name is either user specified or the default of **tarball.tar** will be used and placed in the current file system.

A Coordinated Universal Time (UTC) constant can be specified when transferring files between different systems that may have different time settings. The default is that no time conversion will take place. If used, “n” is the number of hours difference from GMT.

If the verbose option is used, the files names will be listed as they are being included into the tarball.

The files option will restrict the archive to only include specified file names. Approximately 12 file names can be specified, and wild card characters can be used.

```
system tar extract [<tarball name>] [UTC <± n>] [verbose][files <file name>...]
```

The TAR extract command will extract files from an existing tarball and create them on the BorderGuard. Files extracted from a tarball will replace any existing files of the same name in the file system.

The resultant tarball file name is either user specified or the default of **tarball.tar** will be used and placed in the current file system.

Options for a Coordinated Universal Time (UTC) constant and verbose feedback can also be applied to this command.

The files option allows for the extraction of only the specified file names from the tarball. Approximately 12 file names can be specified. Wild card characters can also be used in the file names.

```
system tar list [<tarball name>] [UTC <±n>]
```

This command will list files from an existing archive. The archive file name is either user specified or the default of **tarball.tar** will be used.

A Coordinated Universal Time (UTC) constant can be specified for this command.

More information about the TAR capability can be found in the latest BorderGuard Reference Manual.

### 3.15 Firmware Release 7.0 (September 2004)

The following sections describe the changes incorporated in the 7.0 firmware, which is the initial release of firmware for the BorderGuard 6000.

#### 3.15.1 Extended RSA and Diffie-Hellman Values

Support for generating and using RSA authentication public and private keys 2048 and 4096 bits in length have been added. 2048 bit keys are supported in all BG6000 models. 4096 bit keys are supported in the high end 5500 and 5600 models.

Diffie-Hellman (D-H) key exchange has also been enhanced to service key exchanges that involve 2048 and 4096 bit primes and public D-H values.

Two enhancements to sleeve definitions have been made – adding more options for the key parameter, and the addition of the dhgroup parameter.

```
dpf set sleeve <name> key { short | long | 2k | 4k } dhgroup <number>
dpf define sleeve <name> key { short | long | 2k | 4k } dhgroup <number>
```

The additions to the **key** parameter and the **dhgroup** parameter are also accepted in files of sleeve definitions such as the **sleeves.dpf** file.

See document “Using Extended Keys in DPF” for more detailed information.

### 3.15.2 Address Change Subnet Roaming Feature

Subnet roaming DPF in Blue Ridge’s PC Client software has an entry to change the DPF Address, and sends an authenticated Address Change message field to the Responder for all connections where this DPF is the Originator. When the Responder receives and authenticates the message field, it adopts the IP address and UDP source port of the incoming message as the Originator's new address for all subsequent communications.

This feature is designed to support roaming across subnets within Wi-Fi networks without disrupting an existing DPF connection. It will also support the future client interface roaming capability.

### 3.15.3 ESP-DES and ESP-TDES Changed To Match IPSec Usage

The technique used to pad the last block has been changed to conform to IPSec specifications. This allows ESP-DES and ESP-TDES to be used with compression, and HMAC-SHA1 and HMAC-MD5 for single-pass encode and decode through the Hifn 7855. This padding technique is not compatible with the ESP-DES and ESP-TDES transforms provided with earlier Release 6.x versions of the BorderGuard firmware. Support for these earlier, incorrect ESP transforms is being discontinued by Blue Ridge.

### 3.15.4 Gigabit Ethernet Support on the BorderGuard 6000

Numerous commands have been modified to expand negotiation options and display BorderGuard 6000-specific Ethernet interface status.

### 3.15.5 Type of Service Priority Routing

IP packets arriving that have the "low latency" bit set in the TOS field of the header will be processed on arrival before all other queued packets with normal latency. If the hardware transmit queue is full and packets must be diverted to the software backing queue, packets with low latency TOS will be moved to the hardware queue before all normal packets.

### 3.15.6 Enhancements to "DPF Test Transform"

To better assist regression testing, and to make the tests more comprehensive, the transform tests have been enhanced. Additionally, the transform tests have been rewritten to generate packets that are arbitrarily fragmented.

### 3.15.7 Enhanced Site-to-Site Redundancy

An enhanced version of Virtual Router Redundancy Protocol (VRRP) is implemented for Site-to-Site redundancy. It includes full RFC compliance and multi-vendor interoperability. Blue Ridge's enhancements to VRRP provide sensing of connectivity to other Internet sites, and will fail over a BorderGuard device that is no longer successfully communicating on the Internet. Further details are documented in the VRRP section of the BorderGuard 6000 Reference Manual. .

### 3.15.8 Interface Set Command

The command "sys set if en0X on" must now be used to turn on the interface after it has been turned off and prior to an "ip start if en0X" or any other command using the interface.

### 3.15.9 New Ethernet Drivers

The Ethernet drivers, even those for 100BaseT, are effectively all new code for the BorderGuard 6000 family. There are no significant changes to Ethernet code for the BorderGuard 4000.

### 3.15.10 DPF Codec

The "codec," the module that applies transforms to messages for encoding and decoding, has been heavily rewritten to take full advantage of the Hifn 7855 cryptographic coprocessor. A different mechanism is used to schedule individual transforms (TDES decrypt, LZSB decompress, etc.).

### 3.15.11 Random Number Source

On the BorderGuard 6000 series, random numbers are obtained from the Hifn 7855 hardware random number generator and the Hifn software development kit (SDK).