NORTEL

Secure Router 1001,1001S, 1002, 1004, and 3120

Software Release 9.3.2
Readme Notes

1. Release Summary

Release Date:	21-Aug-2008
Purpose:	Software maintenance release to address customer found software issues.

2. Important Notes before Upgrading to This Release

For Secure Router customers who are upgrading to v9.3.2 from a Secure Router version earlier than v9.3.0, it is highly recommended to refer to the v9.2.0 and v9.3.0 release notes for details on upgrading, converting units running Tasman branded code, and changes to the default settings. The Secure Router 1000/3120 v9.2.0 release notes can be found here:

v9.2.0 Release Notes:
http://www130.nortelnetworks.com/go/main.jsp?cscat=DOCDETAIL&DocumentOID=523853&RenditionID=REND832949&poid=15961

v9.3.0 Release Notes:
https://support.nortel.com/go/main.jsp?cscat=DOCDETAIL&id=681775&poid=15961

For users upgrading to v9.3.2 from a release earlier than v9.2.0, it is recommended that you install the v9.3.1 software upgrade through the console port since telnet, SNMP agent and WebUI enabled settings are not retained during the upgrade process. Starting with v9.2.0, the default settings for telnet and WebUI are now specifically disabled. Another option would be to enable SSH and save the configuration prior to the upgrade. Once the router has been upgraded to v9.2.0 or higher, users must explicitly enable these settings and save the configuration. Please refer to the v9.2.0 release notes for additional details.

Note: **IMPORTANT** - If your Secure Router unit is configured for RADIUS or TACACS Service, you must follow these upgrade procedures when upgrading from an earlier release to v9.3.1.

To make the handling of RADIUS and TACACS work properly when changing the shared key it requires that the RADIUS/TACACS are disabled when setting it. In the previous release the enabling aaa facility came prior to the RADIUS settings. Under the r9.2.6 release the AAA service enable command is stored after both the TACACS and RADIUS sections to insure that the service is disable prior to setting the key.

1)Before loading the v9.3.2 release you must enter the following commands

```
configure t
aaa
no enable
save local
```

2)Boot the v9.3.2 release. Enter the following commands:

```
Configure t
aaa
enable
save local
```

Stored configuration is saved in the proper order.

BGP Upgrade for SR 3120

Prior to upgrading to Release r9.3.2 (from 9.3 or earlier release) check that the each of your BGP peers does not send more than 5K prefixes. If so set the maximum_prefix parameter under the BGP peer section to the proper amount and store the configuration prior to upgrading.

3. Platforms Supported

Nortel Secure Router 3120
Nortel Secure Router 1001
Nortel Secure Router 1001S
Nortel Secure Router 1002
Nortel Secure Router 1004

4. Notes for Upgrade

Please see the technical documentation for the Secure Router 1000 and 3120 version 9.3 available at: http://www.nortel.com/support for details on how to upgrade your Secure Router unit.

File Names for This Release

Description	File Size	Version	File Name
Secure Router 3120	9480397	r9.3.2	H1000.Z
Secure Router 1002/1004	8792227	r9.3.2	T1000.Z
Secure Router 1001	9488905	r9.3.2	J1100.Z
Secure Router 1001S	9943114	r9.3.2	JP1010.Z

5. Version of Previous Release

Software Version 9.3.1

6. Compatibility

N/A

7. New Features in the 9.3.2 Release

7. 1 IGMP Snooping

IGMP snooping allows a SR Router to read (snoop) IGMP packets transferred between IP multicast routers and IP multicast hosts to learn the IP Multicast group membership. Without IGMP Snooping, SR Router handles IP multicast traffic in the same manner as network broadcast traffic and forward frames received on one interface to all other interfaces. This creates excessive traffic on the network and affects network performance. IGMP Snooping allows routers to monitor network traffic and determine hosts that want to receive multicast traffic.

IGMP snooping currently supports following configuration:

a) Global enabling or disabling of IGMP snooping. When disabled, IGMP snooping will not process any IGMP related packets. When enabled, the packets will be processed only on the VLANs on which IGMP snooping is enabled
b) Enabling or disabling of IGMP snooping on a specified VLAN. The default is that all vlans are disabled from IGMP snooping.
c) Configuring the Router to specify the interface and VLAN on which a layer 3 multicast router is configured
d) Enabling or disabling of querier on a VLAN. On enabling this, router will send a periodic query messages on the VLAN
e) Enabling or disabling of fast leave. If enabled, the VLAN will leave the group immediately after receiving a membership leave message. If disabled, the router will send query messages 3 times to check any host is still interested to receive the multicast stream on this VLAN.
f) Configuring IGMP version on a VLAN. This will specify the version of IGMP message to be used on a VLAN. Version 1 and 2 are supported.
g) Configuring query interval on a VLAN. This will specify query interval in milliseconds for query messages to be sent on a VLAN (default 125,000 milliseconds)
h) Configuring last member query interval. This will specify interval in millisecond of the query message to be sent upon receiving a membership leave message. (default 1,000 milliseconds)
i) Configuring maximum response time in centi-seconds (default 100 centi-seconds or 1,000 milliseconds). This value is used to calculate membership expiry timer using the formula:
   Membership expiry = 2 x query interval + maximum response time in seconds

CLI

To enable IGMP Snooping globally

```
Host/configure #igs
Host/configure/igs# snooping-enable
```

To disable IGMP Snooping globally

```
Host/configure #igs
Host/configure/igs# no snooping-enable
```

To enable IGMP Snooping on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs /vlan 10 # snooping-enable
```

To disable IGMP Snooping on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs /vlan 10 # no snooping-enable
```

To configure a multicast router port for a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs /vlan 10 # mrouter wan1
```

To enable querier on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # querier-enable
```

To disable querier on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # no querier-enable
```

To enable fast leave on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # fast-leave-enable
```

To disable fast leave on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # no fast-leave-enable
```

To configure version on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 #version 1
```

To configure query interval on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 #query-interval 150000
```

To configure last member query interval on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # last-member-query-interval 1500
```

To configure max response time on a VLAN

```
Host/configure #igs
Host/configure/igs#vlan 10
Host/configure/igs/vlan 10 # max-response-time 150
```

CLI Display commands

To display configuration details

```
Host # show igs config
```

Output:

```
Config
IGMP Snooping: ENABLED



     Vid   Snooping  Fast      Querier   IGMP  Query     Last      Max
                      Leave               Ver  Interval  Query     Resp
                                                         Interval  Time
       10  ENABLED   ENABLED   ENABLED   1     150000    1500      150
```

To display multicast groups learned by IGMP snooping on a particular interface

```
Host # show igs groups interface wan2
```

Output:

```
    Groups:
     Vid   GroupIPAddress     Interface
       10   227.1.1.1            wan2
       10   227.1.1.10           wan2
```

To display interfaces on which a particular multicast IP address is learned by IGMP snooping

```
Host # show igs groups ip 227.1.1.1
```

Output:

```
    Groups:
     Vid   GroupIPAddress     Interface
      10    227.1.1.1           wan2
      10    227.1.1.1           ethernet0/1
```

To display multicast groups learned by IGMP snooping on a particular VLAN

```
Host # show igs groups vlan 10
```

Output:

```
    Groups:
     Vid   GroupIPAddress     Interface
      10    227.1.1.1           wan2
      10    227.1.1.1           ethernet0/1
      10    227.1.1.10          wan2
```

To display all groups learned by IGMP snooping

```
Host # show igs groups all
```

Output:

```
    Groups:
     Vid   GroupIPAddress     Interface
      10    227.1.1.1           wan2
      10    227.1.1.1           ethernet0/1
      10    227.1.1.10          wan2
```

To display multicast routers learned or configured for IGMP snooping

```
Host # show igs mrouters
```

Output:

```
    Mrouters:
     Vid   Interface
      10    wan1
```

To display IGMP snooping packet statistics

```
Host # show igs statistics
```

Output:

```
    Statistics:

    RXCNT:
    Interface    Join  Leave Query Invalid
    wan1           15     2    25       0
    wan2            2     0     0       0

    TXCNT:
    Interface    Join  Leave Query Invalid
    wan1           15    1    25       0
    wan2            0    0    25       0
```

To display IGMP snooping in detail

```
Host # show igs detail
```

Output:

```
    Config
    IGMP Snooping: ENABLED

     Vid   Snooping  Fast      Querier   IGMP  Query     Last      Max
                     Leave               Ver   Interval  Query     Resp
                                                         Interval  Time
       10  ENABLED   ENABLED   ENABLED   1     150000    1500      150


    Groups:
     Vid   GroupIPAddress     Interface
      10    227.1.1.1           wan2
      10    227.1.1.1           ethernet0/1
      10    227.1.1.10          wan2
```

```
Mrouters:
 Vid   Interface
   10  wan1

Statistics:

RXCNT:
Interface    Join  Leave Query Invalid
wan1           15     2     25       0
wan2            2     0      0       0

TXCNT:
Interface    Join  Leave Query Invalid
wan1           15    1    25       0
wan2            0    0    25       0
```

CLI Debug commands

To redirect debug messages to "/flash1/IgsDbg.txt" and to disable console printing of debug messages

```
Host # debug igs file-logging
```

To disable file logging and enable console printing of debug messages

```
Host # no debug igs file-logging
```

To print configuration related debug messages

```
Host # debug igs configurations
```

To disable configuration related debug messages

```
Host # no debug igs configurations
```

To enable error/failure related debug messages

```
Host # debug igs errors
```

To disable error/failure related debug messages

```
Host # no debug igs errors
```

To enable events related debug messages

```
Host # debug igs events
```

To disable events related debug messages

```
Host # no debug igs events
```

To enable interface related debug messages

```
Host # debug igs interface
```

To disable interface related debug messages

```
Host # no debug igs interface
```

To enable memory related debug messages

```
Host # debug igs memory
```

To disable memory related debug messages

```
Host # no debug igs memory
```

To enable packets related debug messages

```
Host # debug igs packets
```

To disable packets related debug messages

```
    Host # no debug igs packets
```

To enable timer related debug messages

```
    Host # debug igs timer
```

To disable timer related debug messages

```
    Host # no debug igs timer
```

To enable all debug messages

```
    Host # debug igs all
```

To disable all debug messages

```
    Host # no debug igs all
```

7.2 ISDN Enhancements

7.2.1 Interface Based backup

Interface based backup feature which will enable the user to configure an ISDN interface as backup for the primary WAN link. When the Primary link goes down it will bring up the backup interface. ISDN call will be triggered as soon as the primary WAN link goes down. Once the ISDN call is established all the traffic will start flowing through the ISDN interface with the static routes configured. When the primary link is restored, ISDN call is dropped and the traffic passes through the Primary link as it was before.

CLI

Configuration details for backup interface are as below,

```
Host/configure > interface bundle bri
configuring existing WAN bundle interface bri
Host/configure/interface/bundle bri > isdn
Host/configure/interface/bundle bri/isdn > backup ?
NAME
  backup - Configure interface to backup (bundle name)
SYNTAX
  backup bundle_name <cr>
DESCRIPTION
  bundle_name         -- bundle name to backup
                         (enter a word )
Host/configure/interface/bundle bri/isdn > backup wan
Warning: Idle timer will be disabled...
```

Note: The above configuration will configure the bri bundle as backup for wan interface which is the primary link.

7.2.2 Filtering idle timeout

Routing updates and keep-alive packets can be filtered so that these packets do no impact the idle timer of ISDN connection. CLI has been introduced to allow filters to be configured for incoming and outgoing packets.

CLI

Filtering can be enabled for incoming and outgoing packets using the following CLI commands.

```
Host/configure/interface/bundle bri/isdn > filter
Host/configure/interface/bundle bri/isdn/filter > ?

NAME
  filter              -- Configures the ISDN command

SYNTAX
  COMMANDS <cr>



DESCRIPTION
  COMMANDS            -- Any of the following commands can be used

      incoming        -- Configure incoming filter
      outgoing        -- Configure outgoing filter

Host/configure/interface/bundle bri/isdn/filter > incoming ?

NAME
  incoming - Configure incoming filter

SYNTAX
  incoming enable <cr>

DESCRIPTION
  enable -- enable or disable the filter for IGRP, OSPF, VRRP,
                         ICMP, IGMP, PIM, RIP, BGP
    The parameter may have any of the following values:
        enable        -- enable
        IGRP          -- IGRP
        OSPF          -- OSPF
        VRRP          -- VRRP
        ICMP          -- ICMP
        IGMP          -- IGMP
        PIM           -- PIM
        RIP           -- RIP
        BGP           -- BGP


Host/configure/interface/bundle bri/isdn/filter > outgoing ?

NAME
  outgoing - Configure outgoing filter

SYNTAX
  outgoing enable <cr>

DESCRIPTION
  enable -- enable or disable the filter for IGRP, OSPF, VRRP,
                         ICMP, IGMP, PIM, RIP, BGP
```

```
The parameter may have any of the following values:
        enable        -- enable
        IGRP          -- IGRP
        OSPF          -- OSPF
        VRRP          -- VRRP
        ICMP          -- ICMP
        IGMP          -- IGMP
        PIM           -- PIM
        RIP           -- RIP
        BGP           -- BGP
```

By default all the filtering will be in the disabled state. User can enable the filtering for any specific multicast protocol. On enabling the filtering for a particular protocol, keep alive and control packets specific to that protocol will not impact the idle timer.

7.2.3 Multiple Bundles

User will be able to configure two 64kbps BRI bundles, which was not possible in earlier releases. Both bundles should be configured identical.

7.2.4 Numbering plan and Type of Number

CLI is provided to configure the Numbering Plan and Type of Number. This will enable the user to select the Numbering Plan and Type of Number for the Called Party Number.

```
Host/configure/interface/bundle bri/isdn > numplan ?
NAME
  numplan - Configure the ISDN Type Of Number
SYNTAX
  numplan numplan <cr>
DESCRIPTION
  numplan             -- numplan
    The parameter may have any of the following values:
        unknown       -- Unknown plan
        isdn          -- ISDN/Telephony Numbering plan(default)
        reserved      -- Telephony Numbering plan
        data          -- Data Numbering plan
        telex         -- Telex Numbering plan
        national      -- National Standard Numbering plan
        privacy       -- Private Numbering plan

Host/configure/interface/bundle bri/isdn > typeofnum ?
NAME
  typeofnum - Configure the ISDN Type Of Number
SYNTAX
  typeofnum typeofnum <cr>
```

```
DESCRIPTION
  typeofnum           -- type of number
    The parameter may have any of the following values:
        unknown       -- Unknown type
        international -- International type(default)
        national      -- National type
        network       -- Network Specific type
        subscriber    -- Subscriber type
        abbreviated   -- Abbreviated type
        reserved      -- Reserved value 5
```

7.2.5 Time of the day scheduling

User can configure the date and time for triggering any ISDN call. This feature will allow the user to configure the time schedule in 2 different ways, periodic and absolute. With periodic schedule, user can configure the time range which reoccurs every week and with absolute schedule, specific time range on the calendar. This feature will work with backup feature. When the Serial interface is down, ISDN call will be triggered which will be based on the configured schedule. If the current time is within the time range schedule which is configured on the bundle then only the ISDN call will be triggered, else ISDN call will not be initiated.

CLI Display

The threshold for triggering the 2nd bundle can be configured using the following CLI.

```
Host/configure >time-range <time-range name>
NAME
  time-range - configure time-range
SYNTAX
  time-range timeRangeName <cr>
DESCRIPTION
        timeRangeName -- Time-Range name, max 8 characters ( enter a word )

Host/configure/time-range test> ?
  COMMANDS            -- Any of the following commands can be used
      absolute        -- Configure specific scheduling for isdn
      periodic        -- Configure periodic scheduling for isdn

Host/configure/time-range test > absolute ?
NAME
  absolute - Configure specific scheduling
SYNTAX
  absolute start startdate starttime end enddate endtime <cr>
```

```
DESCRIPTION
  start               -- start
    The parameter may have any of the following values:
        start         -- start
  startdate           -- start date in the format of dd/mm/yyyy
                         ( enter a word )
  starttime  -- start time in the format of hh:mm (24 hours time format)
                         ( enter a word )
  end                 -- end
    The parameter may have any of the following values:
        end           -- end
  enddate             -- end date in the format of dd/mm/yyyy
                         ( enter a word )
  endtime    -- end time in the format of hh:mm (24 hours time format)
                         ( enter a word )
```

Host/configure/time-range test > periodic ?

```
NAME
  periodic - Configure periodic scheduling
SYNTAX
  periodic days starttime to endtime <cr>
DESCRIPTION
  days                -- list of days : weekdays weekends, monday, tuesday,
                         wednessday, thursday, friday, saturday, sunday
    The parameter may have any of the following values:
        daily         -- daily
        weekdays      -- weekdays
        weekends      -- weekends
        monday        -- monday
        tuesday       -- tuesday
        wednessday    -- wednessday
        thursday      -- thursday
        friday        -- friday
        saturday      -- saturday
        sunday        -- sunday
  starttime -- start time in the format of hh:mm (24 hours time format)
                         ( enter a word )
  to                  -- time range
```

```
          The parameter may have any of the following values:
              to            -- specify the end time
        endtime  -- end time in the format of hh:mm (24 hours time format)
                              ( enter a word )
      Host/configure/interface/bundle bri/isdn > trigger-schedule ?
      NAME
        trigger-schedule - Configure time schedule for ISDN
      SYNTAX
        trigger-schedule timeRangeName <cr>

      DESCRIPTION
        timeRangeName       -- Time Range name for ISDN time scheduling
                              ( enter a word )
```

Examples:

Periodic Configuration example:

```
configure# time-range periodic
configure/time-range periodic# periodic weekdays 9:00 to 20:30
configure/time-range periodic# exit
```

Absolute Configuration example:

```
configure# time-range absolute
configure/time-range absolute# absolute start 17/07/2008 12:00 end 18/07/2008 12:45
configure/time-range absolute# exit
configure#
```

7.3 Problems Resolved

Bug Reference	Subsystem	Description
Q01589244	Multicast	Unable to access the commands under ip multicast static
Q01730732	ISDN	No ISDN Time Of Day schedule feature to restrict when ISDN can call out when the primary link is down as backup
Q01771017	SSH	Router would run out of memory from SSH Server over long period of time from a SSH cleint attack
Q01818768	Security	Router crash caused by Firewall NetBIOS ALG even though the ALG is disabled
Q01851133	QOS-FR	After creating the first Frame Relay PVC with CBQ there is no warning message for subsequent PVCs that are created without CBQ. The subsequent PVCs that do not have CBQ will not pass data.
Q01853246	FR	Multi-link Frame Relay bundle had minor packet loss due to improper handling of the PVC sequence numbers in certain conditions
Q01856761	QoS	Unable to access remote router over a ppp vlan bridged bundle with QOS enabled
Q01858162	Firewall	An invalid Error message is display of "invalid policy protocol specified" when adding a firewall policy to allow protocol 4 (IP) to self.

Q01861309-01	SNMP	Command: (snmp-source) deprecated; replaced with (source-address)
Q01863063-01	VPN	Enhancement - bypass encrypting self traffic to trusted interface
Q01867821-01	CLI	Command: (ip multicast static) missing CLI help
Q01867935-01	PIM-SM	Command: (ip multicast static) not functional
Q01883844	IPSec	IPSec 'initial contact' timing issue with VPN Router
Q01889348	DHCP	DHCP altvlan not working when phone requests previous IP address
Q01893315	PPPoE	PPPoE-IPSec memory leak
Q01896244	RIP	RIP-Poison Reverse next hop field should be 0.0.0.0
Q01896245	Multicast	Command: (clear ip mfc) not functional

8. Outstanding Issues

a) Refer to the Secure Router 1000/3120 version 9.3.1 Release notes

9. Known Limitations

1. Refer to the Secure Router 1000/3120 version 9.3.1 Release notes
2. Q01917083 - IGMP Snooping - Forward all IP Multicast Traffic to mrouter port
   In this release, the IGS module forwards IP multicast traffic *only* to ports that have learned about IGMP group registration. However, there is a need to forward all IP multicast streams to “multicast router port” configured in the box.

10. Documentation Corrections

Earlier versions of the Secure Router 1000 and 3120 documentation set state that Multicast over GRE is supported. This statement is not correct. Multicast over GRE is not currently supported on the Secure Router 1000 and 3120 products.

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.

To access more technical documentation, search our knowledge base, or open a service request online, please visit Nortel Technical Support on the web at: http://www.nortel.com/support