Ethernet Routing Switch
5510/5520/5530/5698TFD(-PWR)/5650TD(-PWR)/5632FD
Software Release 6.0.3

1. Release Summary

Release Date: 09-February-2009
Purpose: Software patch release to address customer and internally found software issues.

2. Important Notes Before Upgrading to This Release

For customers upgrading from older software versions, a series of upgrades are required to prevent configuration corruption under certain circumstances. Customers upgrading to release 6.0.1 and later versions from software versions prior to Release 6.0, must first upgrade to Release 6.0. Please see "Ethernet Routing Switch 5000 Series Release Notes - Release 6.0" for details on how to upgrade your Ethernet Routing Switch to Release 6.0.

3. Platforms Supported

Ethernet Routing Switch 5510/5520/5530/5698TFD(-PWR)/5650TD(-PWR)/5632FD

4. Notes for Upgrade

Please see "Nortel Ethernet Routing Switch 5000 Series, Configuration – System, Software Release 6.0" (NN47200-500, available at http://www.nortel.com/support). Under Technical Support, select Routers & Routing Switches followed by Ethernet Routing Switch 5510, 5520, 5530-24TFD, 5698TFD(-PWR), 5650TD(-PWR) or 5632FD) for details on how to upgrade your Ethernet Routing Switch.

File Names for This Release

File Name	Module or File Type	File Size (bytes)
5xxx_60006_diags.bin	Diagnostic image	2,464,932
5xxx_603008.img	Agent code image	15,345,708
5xxx_603009s.img	Agent code image (SSH)	15,873,432

5. Version of Previous Release

Software Version 6.0.1

6. Compatibility

This software release is managed with Java Device Manager (JDM) Release 6.1 or later.

7. Changes in This Release

New Features in This Release

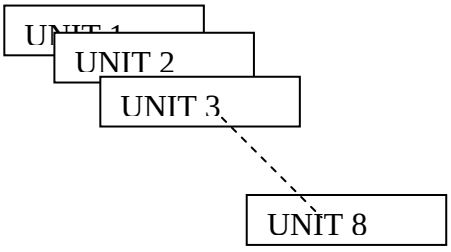
IGMP Selective Channel Block:

IGMP Selective Channel Block feature provides the network administrator the tool to block the streaming of specific channels on some ports.
In certain deployment scenarios, it might be required to disallow the multicast streaming from specific group addresses to users on specific ports. With IGMP selective channel block feature, this type of control can be exercised. When configured it will control the IGMP membership of ports by blocking IGMP reports received from users on that port, destined for the specific group addresses.
This feature will work irrespective of whether the switch is in Layer 2 IGMP snooping mode or the full IGMP mode as the blocking of channels is implemented by blocking the ports from joining an IGMP group. Also, it will be compatible with IGMP v1 and v2 but v3 will be supported in future releases.

The purpose of this feature is to block certain ports on the switch from receiving the multicast traffic from some specified group addresses. This is achieved by capturing the IGMP reports from all the ports and if the destination group address plus port combination matches any configured profile, then drop the report.
The configuration allows 240 profiles to be configured, each for a group address or a range of group addresses. For each group address or a range of group address, the user can configure a list of ports to be blocked. Each unit in the stack will store the configuration for the local ports in NVRAM but it passes the reports for processing to the base unit.
IGMP Selective channel block feature will be supported in the standalone as well as in the stacking mode.
This feature will work with full IGMP enabled in layer3 mode as well as with IGMP snooping on layer2; the implementation works on receiving the packets which will be independent of IGMP mode and will support both. It is also supported for trunk ports but for applying a profile to a trunk port, the user has to manually apply it on one of the members of the trunk.

Usage Example

Consider the following stack



Suppose UNIT 1 is the base unit.
Now consider the following scenarios:

1. Configuration on Unit 3 and packet on Unit 2
User configures a profile with Id 1 to block the address range 224.22.2.2 – 224.22.2.10 on unit 3. This configuration is propagated to all the units. Now all the units have the information for profile 1.
Now on the same unit user applies the profile to various ports – 1/2 – 1/5, 2/2 – 2/5, 3/2 – 3/5.

This information is sent to all units including the originator. Base Unit stores all the information for all these ports against profile 1. Unit 2 and Unit 3 store their local port list 2/2-2/5 and 3/2 – 3/5 respectively and ignore the other information. All other units will ignore this information.
Now an IGMP report arrives for a GA 224.22.2.2 at port 2/4. It is sent to the base unit where a valid match is found and the packet is dropped.

2. Configuration on Unit 3 and packet on Unit 3
In a similar fashion, now with the same above configuration, if an IGMP report packet is received on 3/3, it is sent from local CPU to base unit CPU. After a valid match is found in the profile table, the packet gets dropped.

3. A unit leaves and joins the stack

Let's say, a unit 3 leaves the stack. The base unit gets the message, and it clears information regarding the ports on Unit 3 from its profile table. (it still has all the profile information though). When a new unit 3 joins the stack with no previous configuration, it gets the profile information from the base unit during data base exchange and has all ports permit till any profile is applied on any of its ports.

4. A new Unit with previous configuration joins the stack.
A new unit, say unit 7 joins the stack with profile 1,2 and 3 configured for blocking certain group addresses. When the database exchange happens, all units in the stack get the new configuration for profile 2 and 3 with certain ports to be blocked.
Since profile 1 already exists, the base unit will resolve the conflict to overrule the profile 1 information.

IGMP selective channel block feature is configured using IGMP profiles. Following table provides a list of configurable parameters for a profile.

Parameters	Range	Default Value
Profile Id	1-65535	No default (Index)
Group Start Address	Multicast address range	0.0.0.0
Group End Address	Multicast address range.	Group Start Address
Action	Deny (for now only deny is supported, we can enhance it to support 'permit' for future)	Deny
Port List	Valid ports on all units 1/1 – 8/Max	None (No ports)

.

Limitations

This feature does not snoop the multicast streams that are being sent from any groups to any port. It solely relies on the fact that once the IGMP reports are dropped, ports are prevented from joining the groups so there will be no multicast streaming from those groups to those ports.

Profiles can not be directly applied to MLT trunks, they have to be applied to a member of the trunk.

When a profile is applied to a port in which the same group is already learned, the group is not immediately removed from that port. As a consequence, multicast stream continually flows to that port until Report expiry.

There will be JDM support for this feature and it will support NNCLI but Web configuration is not supported.

Command Syntax

1. Create IGMP profile

Switch(config)# **ip igmp profile** <profile number (1-65535)>
Switch(config-igmp-profile)# **deny**
Switch(config-igmp-profile)# **range** <ip multicast address> <ip multicast address>

2. Delete IGMP profile

Switch(config)#no ip igmp profile<profile number (1-65535)>

3. Applying the IGMP filter profile on interface

```
Switch(config)# interface <interface-id>
Switch(config-if)# ip igmp filter <profile number>
```

4. Remove a profile from an interface

```
Switch(config)# interface <interface-id>
Switch(config-if)#no ip igmp filter <profile number>
```

Old Features Removed From This Release

A feature enhancement **(Q01645430)** that changed the VLACP interoperability behavior with Passport 8600 was removed. For further details, please see the Technical Support Bulletin ID. 2008009238, Rev 1, published on 2008-12-12.

Problems Resolved in This Release

None

8. Outstanding Issues

None

9. Known Limitations

IGMP profile does not automatically propagate to all LACP ports. All LACP ports need to be added manually to the IGMP profile.

10. Documentation Corrections

For other known issues, please refer to the product release notes and technical documentation available from the Nortel Technical Support web site at: http://www.nortel.com/support .

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