BayStack 450

Software Release 4.5.2

1. Release Summary

Release Date: 15-Feb-2005
Purpose: Software patch release to address customer found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

BayStack 350/450/410

4. Notes for Upgrade

Please see “Release Notes for the BayStack 450 10/100/1000 Series Switch Software Version 4.1.x.x” (Part No. 214110-D, available at http://www.nortel.com/support, select BayStack family, then Ethernet Switch 450-24T) for details on how to upgrade your Policy Switch.

File Names For This Release

File Name	Module or File Type	File Size (bytes)
b4504524.img	Agent code image	884,228

5. Version of Previous Release

Software Version 4.5.1

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 5.8.4.

7. Changes in This Release

New Features in This Release
None.

Old Features Removed From This Release
None.

Problems Resolved in This Release

With snooping disabled, IGMP v3 packets were not flooded to all ports **(Q00928271)**.

ICMP hello packets with less than 64 bytes were not properly padded with zeros. The additional bytes could contain internal switch information **(Q00950373).**

Link Flap Detection was not functional when a Gig MDA was inserted into a unit **(Q01001127).**

Station movements between edge stacks of BayStack 450 units connected via DMLT, could sporadically cause CAM corruptions **(Q00897788).**

When two Passport 8600 units and a BayStack 450 unit were connected in a triangular topology via DMLT, the Spanning Tree Protocol did not always behave properly **(Q01013722).**

IGMP reports would not be flooded if IGMP was disabled **(Q01064915).**

BS450 4.5.1: auto-negotiation disabled on GBIC MDA after reset **(Q00974923).**

Copyright information was updated to reflect the correct calendar year of 2005 **(Q01060342).**

8. Outstanding Issues

In a mixed stack with a 450 as the point connection to the network, downgrading the agent code to an older version or upgrading it to a newer, post-4.4 version may not always be successful. The workaround for this problem is to use a unit other than a 450 to carry out the code upgrade in a mixed stack **(Q01070410).**

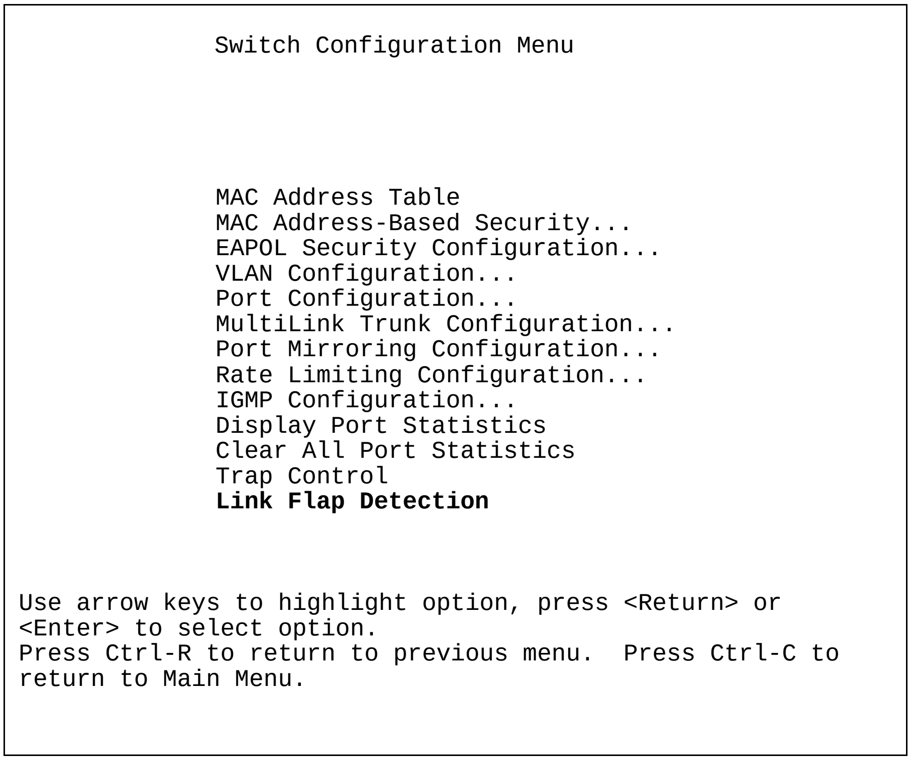
9. Known Limitations

10. Documentation Corrections

The 4.5.1 agent code and hence 4.5.2 include access to a feature from the Switch Menu for Link Flap Detection. This feature was not documented in the 4.5.1 readme. It is important to note that this feature is not supported in a mixed stack.

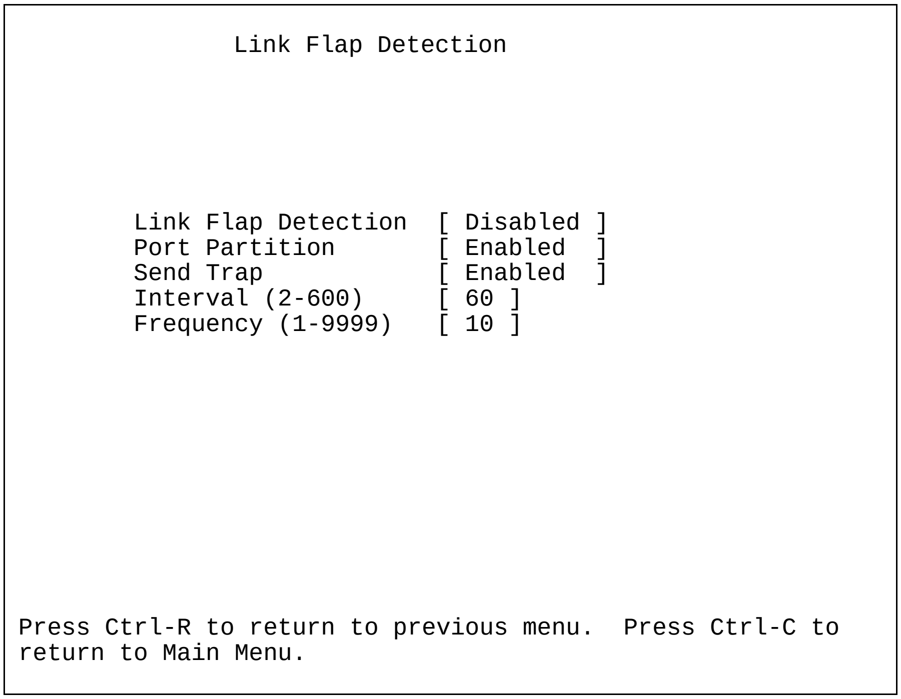
Link Flap Detection Menu Selection

The Switch Configuration Menu now includes a Link Flap Detection selection. This feature allows the automatic detection of links that are “flapping” (undergoing repeated link up and link down conditions). Link flaps could cause network instability and could also result in repeated Spanning Tree re-convergence and subsequent network delays. The Link Flap Detection functionality provides a number of parameters that are used to detect link flaps and prevent their undesirable side effects. The change to the Switch Configuration Menu is shown below.



```
                 Switch Configuration Menu




                 MAC Address Table
                 MAC Address-Based Security...
                 EAPOL Security Configuration...
                 VLAN Configuration...
                 Port Configuration...
                 MultiLink Trunk Configuration...
                 Port Mirroring Configuration...
                 Rate Limiting Configuration...
                 IGMP Configuration...
                 Display Port Statistics
                 Clear All Port Statistics
                 Trap Control
                 Link Flap Detection



Use arrow keys to highlight option, press <Return> or
<Enter> to select option.
Press Ctrl-R to return to previous menu.  Press Ctrl-C to
return to Main Menu.
```

Selection of the Link Flap Detection option will cause the display of the Link Flap Detection configuration display:



```
                Link Flap Detection





        Link Flap Detection  [ Disabled ]
        Port Partition       [ Enabled  ]
        Send Trap            [ Enabled  ]
        Interval (2-600)     [ 60 ]
        Frequency (1-9999)   [ 10 ]










Press Ctrl-R to return to previous menu.  Press Ctrl-C to
return to Main Menu.
```

The fields that could be set are outlined below:

Option	Discussion
Link Flap Detection	Controls the execution of the link flap detection algorithm
Port Partition	If enabled, flapping port(s) will be partitioned (non-trunk ports)
Send Trap	If enabled, a trap will be sent to configured trap receivers
Interval	Interval over which to check link flap behavior
Frequency	Acceptable frequency of occurrence for link up/down changes

Link flap detection is disabled by default (enabled in 4.5.1). When enabled, it is applied as a global setting to all ports. Detection of link flapping will cause the sending of traps and the partitioning of ports as configured. When a flapping port is part of a trunk, a trap will be sent for that port but the port will **not** be partitioned. This prevents disabling of a trunk and loss of connectivity to the switch/stack. The trap sent will use the SNMP OID of 1.3.6.1.4.1.2272.1.21.8 on a packet capture and
1.3.6.1.4.1.2272.1.21.0.8 if decoded in a trap receiver such as JDM.

The interval and frequency fields allow the user to tailor the behavior of the link flap detection algorithm. Using the values of 60 seconds and 10 occurrences shown above, any link up transition after 10 cycles within 60 seconds would cause the trap and partition actions to occur. Traps sent for an offending port will not be sent more than once per minute to limit the trap traffic from the switch for flapping links.

Other Known Issue References

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 .

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