NORTEL

Ethernet Routing Switch 4500
Software Release 5.2.2

1. Release Summary

Release Date: 08-May-2009
Purpose: Software patch release to address customer found software issues.

2. Important Notes Before Upgrading to This Release

None.

3. Platforms Supported

Ethernet Routing Switch 4500 (all models).

4. Notes for Upgrade

For details on updating the software on your Ethernet Routing Switch, please see "*Nortel Ethernet Routing Switch 4500 Series, Overview — System Configuration*" for software release 5.2 (NN47205-500 v04.0x). To download this document, go to http://www.nortel.com/support, and select **Routers & Routing Switches**. Under Ethernet Routing Switches, select your **Ethernet Routing Switch 4500 Series** model. Click on **Documentation** in the gray banner to view a list of all documentation for the product.

File Names For This Release

File Name	Module or File Type	File Size (bytes)
4500_5203_diag.bin	Diagnostic image	1,589,532
4500_522012.img	Agent code image	5,796,280
4500_522013s.img	Agent code image (SSH)	6,051,748

5. Version of Previous Release

Software Version 5.2.1.

6. Compatibility

This software release is managed with Java Device Manager (JDM) release 6.0.9.

7. Changes in This Release

New Features in This Release

Radius Assigned VLAN Update for 802.1x - Use most recent Radius VLAN Enhancement

Existing Functionality

If use-radius-assigned-vlan option is enabled, the first valid radius-assigned-vlan (by EAP or Non-EAP authentication) on that port will be honored. Subsequent radius-vlan assignments will be ignored, for any user on that port. Note: If EAP VLAN is assigned after the Non-EAP VLAN, then the EAP VLAN takes precedence over the non-EAP with the port being moved from the Non-EAP VLAN to the EAP VLAN.

New Functionality (as implemented in 5.2.2 release)

The new functionality introduced with release 5.2.2 is to honor the last received radius-vlan assignments on a port. The last radius-assigned VLAN (either EAP or Non-EAP) will determine the VLAN membership and PVID replacing any previous radius-assigned VLAN values for that port.
Functional examples:
1. NEAP (Non-EAP) device authenticates on port X, the VLAN membership and PVID will be changed according to radius-vlan assignment if any. For example, let's say it will be added to VLAN 50.
2. Next. a PC authenticates on the same port X. That port will be removed from the VLAN 50 and moved into the new radius-vlan assigned with the new PVID, if a VLAN is assigned from the radius server.
The VLAN and the PVID will be changed every time a new valid radius-vlan assignment is processed on the port as a result of a new authentication.

Other functional example:
1. Multiple EAP and NEAP (non-EAP) clients authenticate on a port.
2. The EAP clients perform re-authentication; the non-EAP clients age out and are re-authenticated; the last VLAN assigned setting for either EAP or ENEAP clients will always be applied (meaning there is a potential for the VLAN to swap based on re-authentication).
CLI, SNMP and ACG interfaces are supported (no WebUI is available for this function)

CLI commands:

```
eap multihost use-most-recent-radius-vlan enable
no eap multihost use-most-recent-radius-vlan enable
```

ACG support will be represented by the presence of either of the following lines in the EAP configuration section of the ASCII

```
eap multihost use-most-recent-radius-vlan enable
```

or

```
no eap multihost use-most-recent-radius-vlan enable
```

SNMP Support
Global:

```
bseeMultiHostUseMostRecentRadiusAssignedVlan OBJECT-TYPE
  SYNTAX TruthValue
  MAX-ACCESS read-write
  STATUS current
  DESCRIPTION "Controls whether to use most recent RADIUS-assigned VLAN."
  DEFVAL { false }
  ::= { bseeObjects 21 }
```

Per Interface:

```
        bseePortConfigMultiHostUseMostRecentRadiusAssignedVlan OBJECT-TYPE
          SYNTAX TruthValue
          MAX-ACCESS read-write
          STATUS current
          DESCRIPTION "Controls whether to use most recent RADIUS-assigned VLAN."
          DEFVAL { false }
          ::= { bseePortConfigEntry 18 }
```

BaySecure Sticky MAC Address (Q01992005)

Feature Synopsis

This feature is an extension of the BaySecure application, allowing the user to combine functionality from both static MAC addresses and auto-learning.
Static MAC address entries are tedious to manage as they require identification of a specific MAC for a device. The auto learning functionality simplified this for system management. The Sticky MAC feature combines these methods.

The learning mechanism used is the same as when auto-learning is enabled. But when the Sticky MAC feature is enabled, migration and auto-deletion on link down are blocked and addresses are not aged out.
When Sticky mode is enabled, the aging timer is automatically set to zero.

Sticky MAC Address characteristics:

The addresses are permanent.

Before the introduction of this feature enhancement, in auto-learning mode if a link-down event occurred on the receiving port the address was removed from the mac-security table. The same happened if the switch/stack was rebooted.

With the new enhancement the learned addresses are never removed from the mac-security address table. The user may configure up to 25 MAC addresses per port.

Example :

```
switch(config)#mac-security enable
switch(config)#mac-security auto-learning sticky

switch(config)#interface fastEthernet 2/2-3
switch(config-if)#mac-security enable
switch(config-if)#mac-security auto-learning max-addrs 2
switch(config-if)#mac-security auto-learning enable
switch(config-if)#exit
```

In this example the maximum number of addresses to be learned is 2, and the aging time is automatically set to 0 to forbid aging.

Suppose the switch learns the addresses 00-00-00-00-00-01 and 00-00-00-00-00-02.
After rebooting the unit/stack and checking the mac-security mac-address-table:

```
switch#show mac-security mac-address-table :

Unit Port Allowed MAC Address Automatic
---- ---- ------------------ ---------
2    3    00-00-00-00-00-01   Yes
2    3    00-00-00-00-00-02   Yes
```

Addresses are still present in the mac-security table.

Now, note that the switch has already learned 00-00-00-00-00-01 and 00-00-00-00-00-02; by removing the link from port 2/3 and displaying the mac-security mac-address-table:

```
switch#show mac-security mac-address-table :

Unit Port Allowed MAC Address Automatic
---- ---- ------------------- ---------
2    3    00-00-00-00-00-01   Yes
2    3    00-00-00-00-00-02   Yes
```

Addresses are still present in the table.
The link down event is ignored when sticky-mode is enabled.

The addresses can be removed from mac-security mac-address-table

The user can also remove a specific address or all addresses from the table even if MAC addresses are not static and were learned through auto-learning mode.
The user must use “no mac-security mac-address-table {address xx:xx:xx:xx:xx:xx} {port y}” command. The mechanism for deleting is similar as in the case for static addresses

Migration of addresses is not allowed

Another behavior is related to migration of addresses. Addresses are not migrated when sticky mode is enabled.

Example :

1.Enable auto-learning on port 4.

```
switch(config)#interface fast 4
switch(config-if)#mac-security enable
switch(config-if)#mac-security auto-learning enable
switch(config-if)#exit
```

The address 00-00-00-00-00-01 is learned on port 4. Check the mac-security table :

```
switch#show mac-security mac-address-table :

  Unit Port Allowed MAC Address Automatic
  ---- ---- ------------------- ---------
  2    3    00-00-00-00-00-01   Yes
  2    3    00-00-00-00-00-02   Yes
```

The address 00-00-00-00-00-01 is configured as allowed on port 3, and not on port 4. A security intrusion event is generated into the log file and the intrusion event is sent if syslog and SNMP traps are configured.

Security behavior

There are two distinct cases when syslog messages and SNMP traps are sent:

1) If the maximum number of the configured addresses is reached, the next incoming MAC address will not be forwarded or learned.

2) A learned address is removed from mac-security table.

In the first case the information sent along with the syslog message includes: the maximum number of addresses that is allowed to be learned on that particular port and the number of the port on which the event took place. If the switch is a member of the stack, then also the pair unit/port is included in the syslog message.

In the second case, the information includes: the port (or unit/port) on which the address was learned and the mac-address that was removed.

In both cases, SNMP traps are also sent if a snmp-server host is configured.

A Security Intrusion event is produced for MAC address migration when sticky MAC is enabled.

Observations:

A. Sticky-mac feature specific behavior becomes active immediately after setting sticky mode as enabled. It is not relevant if addresses were learned before or after the mode is enabled.

On the other hand disabling sticky-mac after some addresses were learned (through auto-learning) would make the learned addresses behave as normal auto-learned addresses: the addresses can migrate, cannot be deleted, and they are not saved in configuration files.

B. Also it is important that mac-security to be globally enabled and auto-learning to be enabled for the desired interfaces before enabling sticky mode. This is because sticky-mac-feature only affects addresses learned through auto-learning.
Otherwise activation of sticky-mac feature is useless.

User notes:

It is recommended that users disable auto-saving in NVRAM when sticky mode is enabled. Otherwise an increased number of NVRAM writes would slow down the entire application.

CLI Support

The following command will be added to perform the Sticky MAC feature functionality:

```
switch(config)# mac-security auto-learning sticky
```

The auto-learning mode should be configured previous to this command.
To disable sticky mac feature:

```
switch(config)# no mac-security auto-learning sticky
```

To remove the address from mac-security table :

```
switch(config)#no mac-security mac-address-table
switch(config)#no mac-security mac-address-table address xx:xx:xx:xx:xx:xx
switch(config)#no mac-security mac-address-table address xx:xx:xx:xx:xx:xx  port y
switch(config)#no mac-security mac-address-table  port y
```

SNMP Support

The following SNMP objects are related to Sticky MAC feature :

```
s5SbsAuthCfgStatus OBJECT-TYPE
   SYNTAX       INTEGER {
            valid(1),
            create(2),
            delete(3),
            modify(4),
            createSticky(5)
            }
   MAX-ACCESS       read-write
```

```
    STATUS        current
    DESCRIPTION
        "The status of the AuthCfg entry.  The primary use of
         this object is for modifying the AuthCfg table.  Values
         that can be written create(2), delete(3), modify(4).
         Values that can be read: valid(1).  Setting this entry
         to delete(3) causes the entry to be deleted from the
         table.  Setting a new entry with create(2) causes the
         entry to be created in the table. Setting an entry with
         modify(4) causes the entry to be modified. The response
         to a get request or get-next request will always indicate
         a status of valid (1), since invalid entries are removed
         from the table.

         This object cannot be modified for entries whose value of
         s5SbsAuthCfgSource is autoLearn(2) if the value of
         s5SbsAutoLearningSticky is false(2).  Any such attempt
         will generate an inconsistentValue error."
    ::= { s5SbsAuthCfgEntry 5 }



s5SbsAuthCfgSecureList OBJECT-TYPE
    SYNTAX        Integer32(0..65535)
    MAX-ACCESS  read-write
    STATUS  current
    DESCRIPTION
        "The index of the security list. This value is meaningful
         only if s5SbsAuthCfgBrdIndx and s5SbsAuthCfgPortIndx values
         are zero. For other board and port index values
         it should have the value of zero. This value is used
         as an index into s5SbsSecurityListTable.
         The corresponding MAC Address of this entry is allowed or blocked
         on all the ports of that port list.  Note that this value must
         be 0 for entries where the value of s5SbsAuthCfgSource is either
         autoLearn(2) or sticky(3)."
    ::= { s5SbsAuthCfgEntry 6 }

s5SbsAuthCfgSource OBJECT-TYPE
    SYNTAX      INTEGER {
                    static(1),
                    autoLearn(2),
                    sticky(3)
                }
    MAX-ACCESS  read-only
    STATUS  current
    DESCRIPTION
        "This object indicates the source of an entry.  A value of static(1)
         indicates that the entry was manually created by a user.  A value
         of autoLearn(2) indicates that the entry was auto-learned.

         Note that if the value of s5SbsAutoLearningSticky is false(2), then
         an auto-learned entry cannot be directly deleted, though disabling
         auto-learning for a port will delete all auto-learned MAC addresses
         for the port.  However, if the value of s5SbsAutoLearningSticky is
         true(1), then auto-learned addresses can be deleted normally."
    ::= { s5SbsAuthCfgEntry 7 }


s5SbsAutoLearningSticky OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "This object controls whether the 'sticky-mac' feature is enabled."
    ::= { s5SbsAuth 24 }
```

ASCII Generator
The sticky mode status will be saved in the ASCII-config file.
The auto-learned addresses will be saved in the ASCII-config file.

Old Features Removed From This Release

None.

Problems Resolved in This Release

After disabling the banner, a large amount of logs were displayed after 15 min (**Q01967905**)

Non-EAPOL Password format for MAC addresses should be without periods (**Q01955679**)

When VLACP made a port down then the next best route for the same network going through an alternate link is still unavailable until the ARP entry for original/previous next hop is cleared from the switch (**Q01978509**).

DMLT/MSTP traffic did not pass when a link was disconnected (**Q01971643**)

Protocol based user define VLAN 0xFEFE dropped packets (**Q01981082-01**)

DHCP Discover packets were not forwarded with snooping enabled and packet size greater than 590 bytes (**Q01931641-01**).

8. Outstanding Issues

None.

9. Known Limitations

None.

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 .

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