>THIS IS **THE WAY**

>THIS IS NORTEL

Product Name **Ethernet Switch**
Product Number **460/470**

> Technical Configuration Guide for MAC Security

Enterprise Network Engineering
Document Date: July 5, 2005
Document Version: 1.1

Table of Contents

1. Overview: MAC Security Features

MAC address-based security

MAC addresses can be added to a MAC Security Table to control the MAC address or addresses allowed on a port. MAC addresses can be added either via static entries or automatically via MAC address learning with the ability to restrict the number of MAC entries per port.

The MAC address-based security auto-learning feature provides the ability to add allowed MAC addresses in the MAC Security Table automatically without user intervention. The user specifies the number of addresses between 1 and 25 to be added in the table per port. The switch forwards traffic only for those MAC addresses on the specified ports.

The user can configure an aging time period in minutes after which the entries are refreshed in the MAC Security Table. If the value is set to 0, the entries once learned are never aged-out; the user will need to reset the MAC Address Table for the specified port to force new addresses to be learned. The entries associated with a given port in the MAC Security Address Table will also be deleted from the table if a link down event occurs for the port.

The user cannot modify any MAC addresses which were automatically learned (added to the MAC Security Tool). The addresses added automatically are not saved in NVRAM but learned after the switch port becomes operational. The aging time and the number of MAC addresses per port are saved in the configuration file in non-volatile memory.

The user can reset the MAC address table for a port by disabling the security on the port and then re-enabling it.

If a MAC is already learned on a port migrates to another port on the switch or stack, then the MAC entry port association will be removed from the original port and associated with new port in the MAC Security Address Table. When the MAC address is learned on the new port, the aging timer for that MAC address entry will be reset.

When the user disables auto-learning on a port, all the MAC entries associated with that port in the MAC Security Address Table are removed. No traffic can then be permitted on the port until statically configured MAC addresses are added. User configured MAC addresses take precedence in the forwarding table over any other MAC learning on the switch or stack. This means that user settings have priority over automatic learning.

DA filtering using MAC address-based security

You can configure the Ethernet Switch 460/470 to drop all packets with specific Destination MAC Addresses (DAs). You can configure up to 10 specific MAC DAs as an enhancement to the current MAC address-based security system that allows you to filter MAC source addresses (SAs).

NOTE: You must use either the CLI or Web-based management to configure MAC DA filtering.

2. Nortel CLI Mode:

When you first connect to the Ethernet Switch via a local console port connection, you will be prompted to enter *Ctrl-Y* to begin. This will bring you to the *Enterprise Switch Main Menu* by default.

To access Nortel CLI, from the *Ethernet Switch Main Menu*, select *Command Line Interface.* Once you get the Nortel CLI prompt, enter the commands below.

1) Go to the privileged mode by entering the command below:

   - BS470_48>***enable***
   - BS470_48#

2) Go to configuration mode:

   - BS470_48#***configure terminal***
     Enter configuration commands, one per line. End with CNTL/Z.
     BS470_48(config)#

If you wish to go directly to Nortel CLI and avoid the *Ethernet Switch Main Menu*, enter the following command.

- BS470_48#***cmd-interface cli***

3. MAC Security Configuration:

MAC security on an ES470-460 can be configured using the following command:

Via Nortel CLI

- 470-24T(config)#***mac-security ?***

```
  auto-learning       Configure MAC Auto-Learning
  disable             Disable MAC Address Security.
  enable              Enable MAC Address Security.
  filtering           Enable/disable DA filtering
  intrusion-detect    Enable/disable partitioning on intrusion detection
  intrusion-timer     Set temporary partition time for intrusion detection.
  learning            Enable/disable MAC address learning
  learning-ports      Modify ports participation in MAC address learning.
  mac-address-table   Add addresses to MAC security address table
  mac-da-filter       Add/delete MAC DA filtering addresses
  security-list       Modify security list port membership.
  snmp-lock           Enable/disable SNMP lock on MAC address security
                      parameters.
  snmp-trap           Enable/disable SNMP trap generation on intrusion
                      detection.
```

Via Device Manager (JDM)

- Edit>Security>General

Where

Parameters and variables	Description

`Disable|enable`
 	
`SecurityStatus (JDM)`
	Disables or enables MAC address-based security.

`filtering {enable|disable}`
 	
`daFiltering (JDM)`
	Enables or disables destination address (DA) filtering on intrusion detected.

`intrusion-detect {enable|disable|forever}`
 	
`partitionPort (JDM)`
	Specifies partitioning of a port when an intrusion is detected:
	• `enable`—port is partitioned for a period of time
	• `disabled`—port is not partitioned on detection
	• `forever`—port is partitioned until manually changed

`intrusion-timer <1-65535>`
 	
`AuthCtlPartTime (JDM)`
	Specifies, in seconds, length of time a port is partitioned when an intrusion is detected; enter the number of you want.
	
	Specifies MAC address learning. Learned addresses are added to the table of allowed MAC addresses. Enter the ports you want to learn; it can be a single port, a range of ports, several ranges, all, or none.

`learning {enable|disable}`	Specifies MAC address learning: • `enable`—enables learning by ports • `disable`—disables learning by ports
`snmp-lock {enable|disable}`	Enables or disables a lock on SNMP write-access to the BaySecure MIBs.
`snmp-trap {enable|disable} trap (JDM)`	Enables or disables trap generation upon intrusion detection.

3.1 Security Lists:

MAC security lists can be used to group a number of ports. Up to 32 groups are supported and are configurable using the following command:

Via Nortel CLI

- 470-24T(config)#***mac-security security-list <1-32> ?***

```
add      Add ports
LINE     List of ports
remove   Remove ports
```

Via Device Manager (JDM)

- Edit>Security>Security List>Insert
  - *SecurityListIndx: 1..32*
  - *SecurityListMembers: <click on port members and click on OK>*

4. Configuration Examples:

4.1 Enabling MAC Auto-Learning with MAC Address Limit:

The following is an example on how to limit the number of MAC addresses that can be learned on a port. By default, the maximum MAC addresses is set for 2. For example, assuming that we wish to limit the number of MAC addresses learned on port 18 to 3 addresses, enter the following commands:

Via CLI

- 470-24T(config)#***interface fastEthernet 18***
- 470-24T(config-if)#***mac-security port 18 enable***
- 470-24T(config-if)#***mac-security auto-learning port 18 max-addrs 3***
- 470-24T(config-if)#***mac-security auto-learning port 18 enable***
- 470-24T(config-if)#***exit***
- 470-24T(config)#***mac-security enable***

To view the MAC security address table, enter the following command:

- 470-24T#***show mac-security mac-address-table***

```
Port Allowed MAC Address Automatic
---- ------------------- ---------
20   00-00-04-00-00-22   Yes
20   00-00-04-00-00-33   Yes
20   00-00-04-00-00-44   Yes

Security List Allowed MAC Address Automatic
------------- ------------------- ---------
```

Via Device Manager (JDM)

To configure MAC address security via Java Device Manager (JDM), use the following sequence:

- Edit>Security>AutoLearn>Insert
  - *Via Port 18 Enabled: true*
  - *Via Port 18 MaxMacs: 3*
- Edit>Security>General
  - *SecurityStatus: Check box*
  - *PortSecurityStatus: Select port 18*

To view the MAC security address table via JDM, enter the following sequence:

- Edit>Security>AutoConfig

4.1.1 Other Options – MAC Security Aging

By default, the MAC Security aging time is set for 60 minutes. You can change this time by using the following command:

Via Nortel CLI

- 470-24T(config)#***mac-security auto-learning aging-time ?***
  `<0-65535>  Aging-time period, 0 is Forever`

Via JDM

- Edit>Security>General
  - AutoLearningAgingTime: <0..65535 minutes; 0 = does not age out>

4.2 Destination MAC Filtering:

You can use destination MAC (DA) filters to filter up to 10 specific MAC DAs by using the following command:

Via Nortel CLI

- 470-24T(config)#***mac-security mac-da-filter ?***
  add Add MAC DA filtering address
  delete Delete MAC DA filtering address

For example, assuming we wish to block PVST+ BPDU, which uses a MAC DA address of 01-00-0C-CC-CC-CD, enter the following command:

- 470-24T(config)#***mac-security mac-da-filter add 01:00:0c:cc:cc:cd***

Via JDM

Destination MAC filtering is not configurable via JDM. You must use either CLI or WEB to configure this option.

4.3 Enabling Intrusion Detection:

MAC security intrusion detection is enabled by issuing the following commands:

Via Nortel CLI

- 470-24T(config)#***mac-security intrusion-detect ?***

```
  disable  Disable partition on intrusion detection.
  enable   Enable temporary partition on intrusion detection.
  forever  Enable permanent partition on intrusion detection.
```

If you select the *enable* option, this will enable the switch to shutdown the port when MAC intrusion. The intrusion detection time is configurable between 0 and 65535 seconds (18.2 hours) and specifies the time for which the port will be temporarily disabled when a MAC intrusion event occurs. By default, the intrusion detect timeout is set for 1 second. If you select the *forever* option or set the timer to 0, the port will be shutdown upon an intrusion and will require administrative intervention to enable the port again.

You can configure the intrusion timer using the following command:

- 470-24T(config)#***mac-security intrusion-timer ?***
  <0-65535> Temporary partition time, 0 is Forever

Finally, you can generate a SNMP trap upon detecting an intrusion by issuing the following command:

470-24T(config)#***mac-security intrusion-detect enable snmp-trap enable***

Example:

For example, let's assume we wish to enable intrusion detection with a time-out of 10 seconds and also generate a trap upon detection. This can be accomplished by entering the following commands:

Via Nortel CLI

- 470-24T(config)#***mac-security intrusion-detect enable***
- 470-24T(config)#***mac-security intrusion-timer 10***
- 470-24T(config)#***mac-security intrusion-detect enable snmp-trap enable***

Upon detecting an intrusion, this will generate a trap and show up in the log file as shown below

470-24T#***show logging sort-reverse***

```
Type Time                    Idx  Src Message
---- ----------------------- ---- --- -------
I    00:00:05:50             21       Link Up Trap Port: 20
I    00:00:05:38             20       Link Down Trap Port: 20
I    00:00:05:37             19       Trap:  s5EtrSbsMacAccessViolation
I    00:00:05:37             18       Trap:  s5EtrSbsMacAccessViolation
```

Via JDM

- Edit>Security>General
  - *Security Action: partitionPortAndsendTrap*
  - *AutoLearningAgingTime: 33*

4.4 Adding Static MAC Entries:

Static MAC Address security entries can be added by using the following command:

- 470-24T(config)#***mac-security mac-address-table address <MAC address to add> ?***

```
  port           Assign specific port to a MAC address.
  security-list  Assign a security list to a MAC address.
```

Example:

For this example, we wish to allow access on port 18 only for MAC addresses 00:00:02:00:00:01 and 00:00:02:00:00:11.

Via Nortel CLI

- 470-24T(config)#***mac-security mac-address-table address 00:00:02:00:00:01 port 18***
- 470-24T(config)#***mac-security mac-address-table address 00:00:02:00:00:11 port 18***
- 470-24T(config)#***mac-security enable***
- 470-24T(config)# ***interface fastEthernet 18***
- 470-24T(config-if)#***mac-security enable***

Via JDM

- Edit>Security>AuthConfig
  - Insert
    - *BrdIndx: 1*
    - *PortIndx: 18*
    - *MacIndx: 00:00:02:00:00:01*
    - *AccessCtrlType: allowed*
    - *Insert*
  - Insert
    - *BrdIndx: 1*
    - *PortIndx: 18*
    - *MacIndx: 00:00:02:00:00:11*
    - *AccessCtrlType: allowed*
    - *Insert*
- Edit>Security>General
  - *SecurityStatus: <check box>*
  - *PortSecurityStatus: 18*

4.4.1 Adding Static Entries via Security List

An alternative way to add MAC security addresses is to configure this to use MAC security lists capability. In the following example, we will set up a security list, list 1, with ports 14-18.

Via Nortel CLI

- 470-24T(config)#***mac-security security-list 1 add 14-18***
- 470-24T(config)#***mac-security mac-address-table address 00:00:02:00:00:01 security-list 1***
- 470-24T(config)#***mac-security mac-address-table address 00:00:02:00:00:11 security-list 1***
- 470-24T(config)#***mac-security enable***
- 470-24T(config)#***interface fastEthernet 14-18***
- 470-24T(config-if)#***mac-security port 14-18 enable***

Via JDM

- Edit>Security>SecurityList
  - Insert
    - *SecurityListIndx: 1*
    - *SecurityListMembers: 14-18*
    - *Insert*
- Edit>Security>AuthConfig
  - Insert
    - *BrdIndx: 0*
    - *PortIndx: 0*
    - *MacIndx: 00:00:02:00:00:01*
    - *AccessCtrlType: allowed*
    - *SecureList: 1*
    - *Insert*
  - Insert
    - *BrdIndx: 0*
    - *PortIndx: 0*
    - *MacIndx: 00:00:02:00:00:11*
    - *AccessCtrlType: allowed*
    - *SecureList: 1*
    - *Insert*
- Edit>Security>General
  - *SecurityStatus: <check box>*
  - *PortSecurityStatus: 18*

4.4.2 Viewing Security Lists and MAC Address Table

To view the MAC security list, use the following command:

Via Nortel CLI

- 470-24T(config)#***show mac-security security-lists***

```
Security List 1: 14-18
Security List 2: NONE
Security List 3: NONE
|
Security List 32: NONE
```

Via JDM

- Edit>Security>SecurityList

To view the MAC addresses associated with each security address table, enter the following command:

Via Nortel CLI

- 470-24T(config)#***show mac-security mac-address-table***

```
Port Allowed MAC Address Automatic
---- ------------------- ---------

Security List Allowed MAC Address Automatic
------------- ------------------- ---------
1             00-00-02-00-00-01   No
1             00-00-02-00-00-11   No
```

Via JDM

- Edit>Security>AuthConfig

5. Software Baseline:

This document is based on software release version 3.6.

6. Reference Documentation:

Document Title	Publication Number	Description
Configuring and Managing Security	217104-A	Nortel Ethernet Switches 460 and 470 Software Release 3.6

Contact Us:

For product support and sales information, visit the Nortel Networks website at:

http://www.nortel.com

In North America, dial toll-free 1-800-4Nortel, outside North America dial 987-288-3700.