Part No. 032662-00, Rev. A
April 2010

OmniSwitch 6250 User Guide Supplement

Release 6.6.1

Alcatel·Lucent

www.alcatel-lucent.com

This user guide supplement contains documentation updates for release 6.6.1 of the OmniSwitch 6250 Series. The information described in this supplement is subject to change without notice.

This OmniSwitch product contains components which may be covered by one or more of the following U.S. Patents:

- U.S. Patent No. 6,339,830
- U.S. Patent No. 6,070,243
- U.S. Patent No. 6,061,368
- U.S. Patent No. 5,394,402
- U.S. Patent No. 6,047,024
- U.S. Patent No. 6,314,106
- U.S. Patent No. 6,542,507
- U.S. Patent No. 6,874,090

26801 West Agoura Road
Calabasas, CA 91301
(818) 880-3500 FAX (818) 880-3505
support@ind.alcatel.com

US Customer Support—(800) 995-2696
International Customer Support—(818) 878-4507
Internet—service.esd.alcatel-lucent.com

Contents

1 User Documentation Addendum

This addendum includes information that should be added to or changed in the **6.6.1** release of the set of OmniSwitch 6250 user guides. The information provided documents new and enhanced features that were added to release 6.6.1.725.

OmniSwitch 6250 CLI Reference Guide

The following modifications should be made:

Chapter 13, "802.1AB Commands"

The 6.6.1.725 release provides support for LLDP Network Policy TLVs to advertise the VLAN ID, 802.1p, and DSCP for the following applications: voice, voice signaling, guest voice, guest voice signaling, soft phone voice, video conferencing, streaming voice and video signaling.

The OmniSwitch uses LLDP-MED Network Policies to advertise the Voice VLAN to the connected IP Phones through explicit definition of LLDP-MED Network Policies that contain information about the VLAN-ID and the associated L2 and L3 priorities. The binding of the network policies can be done globally or on a per port basis. The VLAN must be created explicitly. When using authenticated or mobile VLANs it is recommended to use mobile-tag rules to dynamically associate the devices according to the incoming tagged traffic.

The following new CLI commands were added to support the configuration of LLDP Network Policies:

lldp network-policy

Configures a local Network Policy on the switch for a specific application type.

lldp network-policy *policy_id* **-** [*policy_id2*] **application { voice | voice-signaling | guest-voice | guest-voice-signaling | softphone-voice | video-conferencing | streaming-video | video-signaling } vlan { untagged | priority-tag |** *vlan-id* **} [l2-priority** *802.1p_value* **] [dscp** *dscp_value* **]**

no lldp network-policy *policy_id* **-** [*policy_id2*]

Syntax Definitions

policy_id - [*policy_id2*]	A network policy identifier (0-31) which is associated to a port.
voice	Specifies a voice application type.
voice-signaling	Specifies a voice-signaling application type.
guest-voice	Specifies a guest-voice application type.
guest-voice-signaling	Specifies a guest-voice-signaling application type.
softphone-voice	Specifies a softphone-voice application type.
video-conferencing	Specifies a video-conferencing application type.
streaming-video	Specifies a streaming-video application type.
video-signaling	Specifies a video-signaling application type.
untagged	Specifies that a VLAN port is untagged.
priority-tag	Specifies the internal priority that would be assigned to the VLAN**.**
vlan_id	VLAN identifier. Valid range is 1–4094.
802.1p_value	The Layer-2 priority value assigned to the VLAN. Valid range is 0–7.
dscp_value	Priority value assigned to the DSCP (Differentiated Service Code Point) header. Valid range is 0–63.

Defaults

parameter	default
802.1p_value	**0**
dscp_value	**0**

- By default the 802.1p_value is 5 for voice application.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- Use the **no** form of this command to remove the configured network policy from the system.
- When a network policy is deleted, all the associated values and port bindings are also deleted.
- A maximum of 32 network policies can be configured on a single VLAN.
- Once a policy is created, the application type, VLAN ID, 802.1p, and DSCP values can be modified.
- If a network policy ID is bound to a port, it cannot be modified.
- Use a hyphen to specify a range of Policy IDs and a space to separate multiple Policy IDs in the command.
- The range for Policy IDs is supported only with the **no** form of this command.

Examples

```
-> lldp network-policy 10 application voice vlan 20
-> lldp network-policy 11 application guest-voice-signaling vlan untagged
l2-priority 3
-> lldp network-policy 20 application voice vlan priority-tag dscp 39
-> lldp network-policy 20 application voice-signaling vlan 23 l2-priority 2 dscp 43
-> no lldp network-policy 10
-> no lldp network-policy 10-20
```

Release History

Release 6.6.1.725; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the network policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

MIB Objects

```
aLldpXMedLocMediaPolicyTable
  alaLldpXMedLocMediaPolicyId
  alaLldpXMedLocMediaPolicyAppType
  alaLldpXMedLocMediaPolicyVlanType
  alaLldpXMedLocMediaPolicyVlanID
  alaLldpXMedLocMediaPolicyPriority
  alaLldpXMedLocMediaPolicyDscp
  alaLldpXMedLocMediaPolicyUnknown
  alaLldpXMedLocMediaPolicyTagged
  alaLldpXMedLocMediaPolicyRowStatus
```

lldp med network-policy

Associates an existing network policy to a port, slot, or chassis.

lldp {*slot/port* | *slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

no lldp {*slot/port* | *slot* | **chassis} med network-policy** *policy_id* - [*policy_id2*]

Syntax Definition

slot/port	The slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All switch ports.
policy_id - [*policy_id2*]	A network policy identifier (0–31).

Defaults

NA

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- Use the **no** form of this command to disassociate a network policy from a port.
- The network policy should already be configured in the system before associating it with a port.
- A maximum of 8 network policies can be associated to a port.
- Two or more network policy IDs with the same application type cannot be associated to a port.

Examples

```
-> lldp chassis med network-policy 22
-> lldp 1 med network-policy 1-4 5 6
-> lldp 2/3 med network-policy 12
-> no lldp 2/3 med network-policy 12
```

Release History

Release 6.6.1.725; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
show lldp network-policy	Displays the network policy details for a given policy ID.
show lldp med network-policy	Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
  alaLldpXMedLocMediaPolicyPortIfIndex
  alaLldpXMedLocMediaPolicyId
  alaLldpXMedLocMediaPolicyPortRowStatus
```

lldp transmit fast-start-count

Configures the fast start count for an LLDP Media Endpoint Device (MED).The fast start count specifies the number of LLDPDUs to be sent as soon as a MED is detected by the switch. The LLDPDUs contain the LLDP MED Network Policy TLVs.

lldp transmit fast-start-count *num*

Syntax Definitions

num	Specifies the number of LLDPDUs to send when a MED is detected. The valid range is 1–10.

Defaults

parameter	default
num	3

Platforms Supported

OmniSwitch 6250

Usage Guidelines

The LLDP MED fast start is only applicable when the MED is detected by the switch.

Examples

```
-> lldp transmit fast-start-count 4
```

Release History

Release 6.6.1.725; command introduced.

Related Commands

lldp network-policy	Configures a MED Network Policy on the switch for a specific application type.
lldp med network-policy	Associates an existing MED Network Policy with one or more LLDP ports.
show lldp local-system	Displays local system information.

MIB Objects

```
lldpXMedFastStartRepeatCount
```

show lldp config

Displays the general LLDP configuration information for LLDP ports.

show lldp {*slot* | *slot/port***} config**

Syntax Definitions

slot The slot number for a specific module.

slot/port Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).

Defaults

By default, a list of all LLDP ports with their configuration parameters is displayed.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

Use the *slot/port* or *slot* parameter to display information for a specific port or for all ports on a specific module.

Examples

```
-> show lldp config
----------+-------------------------------------------+-----------------+-------
          |  Admin   |  Notify  |  Std TLV |   Mgmt   |  802.1   |  802.3 |   MED
 Slot/Port|  Status  |   Trap   |   Mask   | Address  |   TLV    |   Mask |   Mask
----------+----------+----------+----------+----------+----------+------+------
   2/1      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/2      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/3      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/4      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
   2/5      Rx + Tx    Disabled     0x00     Disabled   Disabled     0x00 0x00
```

output definitions

Slot/Port The LLDP slot and port number.

Admin Status Indicates the Administrative status of the LLDP port.The options are **- Disabled**, **Rx**, **Tx**, and **Rx+Tx**.

Notify Trap Indicates if the Notify Trap feature is disabled or enabled on a particular port

Std TLV Mask The standard TLV mask set for the port.

Mgmt Address Indicates whether transmission of the per port IPv4 management address is enabled or disabled.

802.1 TLV Indicates whether 802.1 TLV status is enabled or disabled on the LLDP port.

output definitions

802.3 Mask	The standard 802.3 mask set for the port.
MED Mask	The standard MED mask set for the port.

Release History

Release 6.6.1.725; command was introduced.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp notification	Enables or disables the LLDP notification status for one or more switch ports. LLDP notifications are sent when there is a change to the remote systems MIB.
lldp tlv management	Specifies the switch to control per port management TLVs to be incorporated in the LLDPDUs.
lldp tlv dot3 mac-phy	Configures whether or not 802.3 TLVs are included in transmitted LLDPDUs.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
   lldpPortConfigAdminStatus
   lldpPortConfigNotificationEnable
   lldpLocPortPortNum
   lldpPortConfigTLVsTxEnable
lldpConfigManAddrTable
   lldpConfigManAddrPortsTxEnable
lldpXdot3PortConfigTable
   lldpXdot3PortConfigTLVsTxEnable
```

show lldp network-policy

Displays the MED Network Policy details for a given policy ID.

show lldp network-policy [*policy_id***]**

Syntax Definitions

policy_id	Policy identifier for a network policy definition. Valid range is between 0 and 31.

Defaults

By default, all configured policies are displayed.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- Network policy should be configured on the system before using this command.
- Enter a policy ID with this command to display information for a specific policy.

Examples

```
-> show lldp network-policy
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+----------------------+------+--------+-------
     1      voice                   4000   7        33
    12      guest-voice                -   -        44
    21      streaming-voice            0   4        11
    31      guest-voice-signaling     23   2        1

-> show lldp network-policy 1
Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
Policy ID        Type              Id    Priority  Value
-----------+----------------------+------+--------+-------
     1      voice                   4000   7        33
```

output definitions

Network Policy ID	Policy identifier for a network policy definition.
Application Type	Indicates the type of application configured on the port or VLAN.
VLAN ID	The VLAN ID assigned to the port on which the network policy is configured.
Layer2 Priority	Layer 2 priority to be used for the specified application type.
DSCP Value	DSCP value to be used to provide Diffserv node behavior for the specified application type.

Release History

Release 6.6.1.725; command introduced.

Related Commands

lldp network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyTable
  alaLldpXMedLocMediaPolicyId
  alaLldpXMedLocMediaPolicyAppType
  alaLldpXMedLocMediaPolicyVlanType
  alaLldpXMedLocMediaPolicyVlanId
  alaLldpXMedLocMediaPolicyPriority
  alaLldpXMedLocMediaPolicyDscp
  alaLldpXMedLocMediaPolicyUnknown
  alaLldpXMedLocMediaPolicyTagged
```

show lldp med network-policy

Displays the network policy configured on a slot or port. If no option is specified, network policies configured on all ports of the chassis are displayed.

show lldp [*slot* | *slot/port***] med network-policy**

Syntax Definitions

slot Specifies the slot number on a specific module or chassis.

slot/port Specifies the slot number for the module and physical port number on that module (e.g. 3/1 specifies port 1 of slot 3).

Defaults

By default, all ports with associated policies are displayed.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- Network policy should be configured on the system before using this command.
- Enter a slot or slot/port number with this command to display information for a specific slot or port.

Examples

```
-> show lldp med network-policy

  slot/port         Network Policy ID
--------------+-------------------------
    1/1            1 3 5 7 21 23 30 31
    1/2            1 2 3 4 7 8 9 10
    .
    .
    .
    2/1            1 3 5
    .
    .

-> show lldp 1/1 med network-policy

Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Slot/    Network         Application       Vlan    Layer2   DSCP
 Port    Policy ID        Type              Id    Priority  Value
-------+-----------+----------------------+------+--------+-------
  1/1       1      guest-voice-signaling  -      -        0
```

output definitions

Slot / Port	Slot number for the module and physical port number on that module.
Network Policy ID	Policy identifier for a network policy definition.
Application Type	Indicates the type of application configured on the port or VLAN.
VLAN ID	The VLAN ID assigned to the port on which the network policy is configured.
Layer2 Priority	Layer 2 priority to be used for the specified application type.

Release History

Release 6.6.1.725; command introduced.

Related Commands

lldp tlv med	Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.
lldp network-policy	Configures a local network policy on a switch for an application type.

MIB Objects

```
alaLldpXMedLocMediaPolicyPortTable
   alaLldpXMedLocMediaPolicyPortIfIndex
   alaLldpXMedLocMediaPolicyId
```

The following existing CLI commands were modified to support LLDP Network Policies:

lldp tlv med

Configures whether or not LLDP-MED TLVs are included in transmitted LLDPDUs.

lldp {*slot/port* | *slot* | **chassis} tlv med {power | capability | network policy} {enable | disable}**

Syntax Definitions

slot/port	Slot number for the module and physical port number on that module (e.g., 3/1 specifies port 1 on slot 3).
slot	The slot number for a specific module.
chassis	All ports on the switch.
power	Includes the extended POE TLV in transmitted LLDPDUs.
capability	Includes the Capabilities TLV in transmitted LLDPDUs.
network policy	Includes the Network Policy TLV in transmitted LLDPDUs.
enable	Enables the transmission of LLDP-MED TLV in LLDPDUs.
disable	Disables the transmission of LLDP-MED TLV in LLDPDUs.

Defaults

parameter	default
enable | disable	disable

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- The ports specified with this command must already be configured to transmit LLDPDUs.
- Using the *slot* or **chassis** parameter with this command overrides the existing configuration for any individual ports on the specified slot number or for all ports on the switch.
- The **lldp tlv med power** version of this command applies only to PoE units.
- Before enabling the Power MED TLV, use the **lanpower start** command to activate PoE on a port or on all ports in a specific slot.

Examples

```
-> lldp 4/4 tlv med power enable
-> lldp 4/3 tlv med capability enable
-> lldp 4 tlv med power disable
-> lldp 4 tlv med network-policy enable
-> lldp chassis tlv med network-policy enable
```

Release History

Release 6.6.1.725; **network policy** option added.

Related Commands

lldp lldpdu	Configures the LLDPDU status for one or more switch ports. The status determines if the specified switch ports will transmit, receive, transmit and receive, or drop LLDPDUs.
lldp tlv management	Configures whether or not management TLVs are included in transmitted LLDPDUs.
lldp tlv dot1	Configures whether or not 802.1 TLVs are included in transmitted LLDPDUs.
lldp tlv dot3 mac-phy	Configures whether or not 802.3 TLVs are included in transmitted LLDPDUs.
show lldp med network-policy	Displays the MED Network Policy configuration.

MIB Objects

```
lldpPortConfigTable
   lldpPortConfigPortNum
lldpXMedPortConfigTable
   lldpXMedPortConfigTLVsTxEnable
```

show lldp local-system

Displays local system information.

show lldp local-system

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6250

Usage Guidelines

N/A

Examples

```
-> show lldp local-system
Local LLDP Agent System Data:
  Chassis ID Subtype         = 4 (MAC Address),
  Chassis ID                 = 00:d0:95:e9:c9:2e,
  System Name                = Kite2_Stack_of_2,
  System Description         = 6.3.1.636.R01 Development, September 07, 2007.,
  Capabilites Supported      = Bridge, Router,
  Capabilites Enabled        = Bridge, Router,
  LLDPDU Transmit Interval    = 30 seconds,
  TTL Hold Multiplier        = 4,
  LLDPDU Transmit Delay      = 2 seconds,
  Reintialization Delay      = 2 seconds,
  MIB Notification Interval = 5 seconds,
  Fast Start Count           = 4,
  Management Address Type    = 1 (IPv4),
  Management IP Address      = 10.255.11.100,
```

output definitions

Chassis ID Subtype	The subtype that describe chassis ID.
Chassis ID	The chassis ID (MAC address).
System Name	The name of the system.
System Description	The description of the system.
Capabilites Supported	The capabilities of the system.
Capabilites Enabled	The enabled capabilities of the system.
LLDPDU Transmit Interval	The LLDPDU transmit interval.
TTL Hold Multiplier	The hold multiplier used to calculate TTL.

output definitions (continued)

LLDPDU Transmit Delay	The minimum transmit time between successive LLDPDUs.
Reintialization Delay	The minimum time interval before the reinitialization of local port objects between port status changes.
MIB Notification Interval	The minimum time interval between consecutive notifications of local system MIB change.
Fast Start Count	Specifies the number of LLDPDUs to be sent as soon as a MED is detected by system.
Management Address Type	The type of management address used in LLDPDU.
Management IP Address	The management IP address. This will be the Loopback0 IP address if configured, otherwise it is the first IP interface configured on the switch.

Release History

Release 6.6.1.725; **Fast Start Count** field added to output.

Related Commands

lldp transmit fast-start-count	Configures the fast start count for an LLDP Media Endpoint Device (MED).The fast start count specifies the number of LLDPDUs to be sent as soon as a MED is detected by the switch. The LLDPDUs contain the LLDP MED Network Policy TLVs.
lldp reinit delay	Sets the amount of time that must elapse before an LLDP port is re-initialized after the status for the port was disabled.
lldp transmit hold-multiplier	Sets the transmit hold multiplier value. This value is used to calculate the Time To Live (TTL) value that is advertised in an LLDPDU.
lldp transmit delay	Sets the minimum amount of time that must elapse between successive LLDPDUs that are transmitted as the result of a value or status change in the LLDP local systems MIB.

MIB Objects

```
lldpLocalSystemData
   lldpLocChassisIdSubtype
   lldpLocChassisId
   lldpLocSysName
   lldpLocSysDesc
   lldpLocSysCapSupported
   lldpLocSysEnabled
lldpPortConfigTable
   lldpMessageTxInterval
   lldpMessageTXHoldMultiplier
   lldpTxDelay
   lldpReinitDelay
   lldpNotificationInterval
lldpLocManAddrTable
   lldpLocManAddrSubtype
   lldpLocManAddr
   lldpXMedFastStartRepeatCount
```

Chapter 44, "802.1x Commands"

The 6.6.1.725 release supports the configuration of an 802.1x authentication server down policy. Users attempting to authenticate are classified by this policy when the RADIUS server is not available. This type of policy provides two options for classification: user is assigned to a User Network Profile (UNP) or user access is blocked on the port.

Users classified through the authentication server down policy are flagged for re-authentication when the RADIUS server becomes reachable. This policy is supported with 802.1x and MAC-based authentication, but not Captive Portal authentication.

The following new CLI commands were added to support the Auth-Server down policy enhancements:

802.1x auth-server-down

Enables or disables the authentication server down classification policy.

802.1x auth-server-down {enable | disable}

Syntax Definitions

enable	Enables the auth-server-down policy.
disable	Disables the auth-server-down policy.

Defaults

By default, authentication server down policy is disabled.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- This command is global and applies to all 802.1x ports on the switch.

Examples

```
-> 802.1x auth-server-down enable
-> 802.1x auth-server-down disable
```

Release History

Release 6.6.1.725; command was introduced.

Related Commands

show 802.1x auth-server-down	Displays the configured authentication server down policy.

MIB Objects

```
alaDot1xAuthSvrTimeoutStatus
```

802.1x auth-server-down policy

Configures the policy for classifying devices attempting to authenticate when the RADIUS servers are not reachable.

802.1x auth-server-down policy {user-network-profile *profile_name* **| block}**

Syntax Definitions

profile_name	The name of an existing User Network Profile (UNP) to use for device classification.
block	Blocks device access on the 802.1x port.

Defaults

By default, this policy is configured to block access to such devices and is disabled for the switch.

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- Use the **user-network-profile** parameter to classify device traffic into a specific profile when the RADIUS server is down.
- Use the **block** parameter to block device traffic on the 802.1x port when the RADIUS server is down.
- This command applies to all 802.1x-enabled ports on the switch.
- When device authentication fails due to an unreachable RADIUS server, an event message is sent to the switch logging utility (swlog). See the “Switch Logging Command” chapter for more information.

Examples

```
-> 802.1x auth-server-down policy user-network-profile unp1
-> 802.1x auth-server-down policy block
```

Release History

Release 6.6.1.725; command was introduced.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
802.1x auth-server-down re-authperiod	Configures the amount of time to wait before re-authentication is attempted for devices classified by the server down policy.
show 802.1x auth-server-down	Displays the configured authentication server down policy.

MIB Objects

```
alaDot1xAuthServerTimeout
alaDot1xAuthServerTimeoutPolicy
```

802.1x auth-server-down re-authperiod

Configures the amount of time to wait before re-authentication is attempted for devices that were classified by the authentication server down policy.

802.1x auth-server-down re-authperiod {*value***}**

Syntax Definitions

value	The value of re-authentication timer. The range is 1 to 9999 seconds.

Defaults

parameter	default
value	30

Platforms Supported

OmniSwitch 6250

Usage Guidelines

- This timer only applies to devices that were classified by the authentication server down policy. This policy classifies devices whenever RADIUS servers become unreachable.
- This command sets the time interval for all 802.1x-enabled ports on the switch.

Examples

```
-> 802.1x auth-server-down re-authperiod 500
```

Release History

Release 6.6.1.725; command was introduced.

Related Commands

802.1x auth-server-down policy	Configures the authentication server down policy.
show 802.1x auth-server-down	Displays the configured re-authentication time interval value.

MIB Objects

```
alaDot1xAuthSvrTimeoutReAuthPeriod
alaDot1xAuthServerTimeout
```

show 802.1x auth-server-down

Displays the configured authentication server down classification policy.

show 802.1x auth-server-down

Syntax Definitions

N/A

Defaults

N/A

Platforms Supported

OmniSwitch 6250

Usage Guidelines

N/A

Examples

```
-> show 802.1x auth-server-down

Status                        = Enabled
Re-authentication Interval    = 30 seconds
Classification policy         = block

-> show 802.1x auth-server-down

Status                        = Disabled
Re-authentication Interval    = 30 seconds
Classification policy         = block
```

output definitions

Status	Authentication server down policy status: **Enabled** or **Disabled**
Re-authentication Interval	The amount of time for the device to authenticate again with the RADIUS server when the device is classified according to the Auth-server-policy.
Classification Policy	The 802.1x device classification policy that was applied to the device.

Release History

Release 6.6.1.725; command was introduced.

Related Commands

802.1x auth-server-down	Enables or disables the authentication server down policy.
802.1x auth-server-down re-authperiod	Configures the re-authentication time for the device to authenticate again with the RADIUS server when it is classified according to the Auth-server-down policy
802.1x auth-server-down policy	Configures the policy for classifying the device when the authentication server is not reachable

MIB Objects

```
alaDot1xAuthSvrTimeout
  alaDot1xAuthSvrTimeoutStatus
  alaDot1xAuthSvrTimeoutReAuthPeriod
  alaDot1xAuthServerTimeoutPolicy
```

OmniSwitch 6250 Network Configuration Guide

The following modifications should be made:

Chapter 17, "Configuring 802.1AB"

The following sections were added or modified to provide information about the 6.6.1.725 implementation of LLDP Network Policies.

802.1AB Specifications

IEEE Specification	*IEEE 802.1AB-2005 Station and Media Access Control Connectivity Discovery*
TIA Specifications	TIA-1057 - Link Layer Discovery Protocol for Media Endpoint Devices
Platforms Supported (LLDP-MED added in 6.3.4)	OmniSwitch 6250
Transmit time interval for LLDPDUs	5 to 32768 in seconds
Transmit hold multiplier value	2 to 10
Transmit delay	1 to 8192 in seconds
Fast start count	1 to 10
Reinit delay	1 to 10 in seconds
Notification interval	5 to 3600 in seconds
Maximum number of network policies that can be associated with a port	8
Maximum number of network policies that can be configured on the switch	32
VLAN ID Range for assigning explicit LLDP-MED Network Policy	1 to 4094
DSCP range	0 to 63
802.1p priority range	0 to 7

802.1AB Defaults Table

The following table shows the default settings of the configurable 802.1AB parameters.

Parameter Description	Command	Default Value/Comments
Transmit time interval for LLDPDUs	**lldp transmit interval**	30 seconds
Transmit hold multiplier value	**lldp transmit hold-multiplier**	4
Transmit delay	**lldp transmit delay**	2 seconds
Transmit Fast Start Count	**lldp transmit fast-start-count**	3
Reinit delay	**lldp reinit delay**	2 seconds
Notification interval	**lldp notification interval**	5 seconds

Parameter Description	Command	Default Value/Comments
LLDPDUs transmission	**lldp lldpdu**	Transmission and Reception
LLDP Network Policy	**lldp network-policy**	802.1p value: 5 for voice application. 0 for other applications. DSCP value: 0
Per port notification	**lldp notification**	Disable
Management TLV	**lldp tlv management**	Disable
802.1 TLV	**lldp tlv dot1**	Disable
802.3 TLV	**lldp tlv dot3 mac-phy**	Disable
LLDP Media Endpoint Device	**lldp tlv med**	Disable

Quick Steps for Configuring LLDP-MED Network Policy

Note. A VLAN and VPA must be created for LLDP-MED to work on fixed, mobile or 802.1x ports. However, if the VLAN is not created and the VLAN is added in the LLDP-MED Network Policy, no error is displayed.

LLDP-MED Network Policy for Fixed Ports

Create a VLAN, and associate a port to the VLAN. Subsequently, a network policy ID can be created and associated to the related port. The **lldp tlv med**, **lldp network-policy**, and **lldp med network-policy** commands must be used to configure and enable network policy for fixed ports.

1 Enable the transmission of network policy through a VLAN port using the **lldp tlv med** command. Configure the LLDP-MED TLVs to be transmitted through a particular port using this command. For example:

```
-> lldp 1/10 tlv med network-policy enable
```

2 Configure a local network policy on the switch for a specific application type using the **lldp network-policy** command. Assign a network policy identifier (ID) to a particular application type using this command. For example:

```
-> lldp network-policy 1 application voice vlan 10 l2-priority 5
```

3 Bind the network policy to the VLAN port using the **lldp med network-policy** command. For example:

```
-> lldp 1/10 med network-policy 1
```

LLDP on Mobile Ports

For mobile VPA to be created, enable Group Mobility on a port and then define a MAC address rule for an existing VLAN. If the source MAC address of a device matches a MAC address specified in this rule, the device and its mobile port joins the VLAN when the device starts to send traffic.

1 Enable group mobility on a VLAN port using the **vlan port** command.

```
-> vlan port mobile 2/10
```

2 Define MAC address rule for the associated VLAN.

```
-> vlan 10 mac 11:11:11:11:11:11
```

3 Enable network policy using the **lldp tlv med** command. Configure LLDP-MED TLVs for a particular port using this command.

```
-> lldp 2/10 tlv med network-policy enable
```

4 Configure a local network policy on the switch for a specific application type using the **lldp network-policy** command.

```
-> lldp network-policy 1 application voice vlan 10 l2-priority 5
```

5 Bind the network policy to a port associated with a VLAN using the **lldp med network-policy** command.

```
-> lldp 2/10 med network-policy 1
```

LLDP-MED Network Policy on 802.1x Ports

1 Enable group mobility on a VLAN port using the **vlan port** command.

```
-> vlan port mobile 3/10
```

2 Enable 802.1x on the VLAN mobile port.

```
-> vlan port 3/10 802.1x enable
```

3 Use the **aaa radius-server** command to configure the radius server to be used for port authentication. Configure the radius server to return the VLAN ID for the incoming MAC address of the LLDP device.

```
-> aaa radius-server rad1 host 10.10.2.1 timeout 25
```

4 Associate the RADIUS server with authentication for 802.1X ports using the **aaa authentication** command.

```
-> aaa authentication 802.1x rad1
```

5 Configure the User Network Profile and add a classification rule for the MAC address using the following command.

```
-> aaa classification-rule mac-address <mac-address-of-the-lldp-device>
user-network-profile name engineering
```

6 Enable network policy using the **lldp tlv med** command. Configure LLDP-MED TLVs for a particular port using this command.

```
-> lldp 3/10 tlv med network-policy enable
```

7 Configure a local network policy on the switch for a specific application type using the **lldp network-policy** command.

```
-> lldp network-policy 1 application voice vlan 10 l2-priority 5
```

8 Bind the network policy to a port associated with a VLAN using the **lldp med** command.

```
-> lldp 3/10 med network-policy 1
```

If the authentication server returns a VLAN ID, then the client device is assigned to the related VLAN.

Note. *Optional*. Verify the LLDP network policies enabled with regard to different network policy IDs, by entering the **show lldp network-policy** command. For example:

```
-> show lldp network-policy

Legend: 0 Priority Tagged Vlan
        - Untagged Vlan

Network         Application       Vlan    Layer2   DSCP
 Policy ID        Type              Id    Priority  Value
-----------+----------------------+------+--------+-------
     1      voice                   10       5       -
     2      guest-voice              -        -       44
```

To verify the network policies enabled on different slots and ports, use the **show lldp med network-policy** command. For example:

```
-> show lldp med network-policy

  slot/port         Network Policy ID
--------------+-------------------------
    1/10                1 2
    2/10                1 2
    3/10                1 2
```

For more information about this display, see the *OmniSwitch CLI Reference Guide.*

LLDP-Media Endpoint Devices

LLDP-MED is an extension to 802.1ab (Link Layer Discovery Protocol - LLDP), a link-layer protocol that defines a method for network access devices using Ethernet connectivity to advertise device information, device capabilities and media specific configuration information periodically to peer devices attached to the same network.

The LLDP-MED feature facilitates the information sharing between Media Endpoint Devices and Network Infrastructure Devices. It is designed to allow the following functionality:

- Auto-discovery of LAN policies (such as VLAN, Layer 2 Priority and Diffserv settings) leading to "plug and play" networking. This is achieved by advertising the VLAN information.
- Device location discovery to allow creation of location databases for VoIP, E911 services.
- Extended and automated power management of Power-over-Ethernet endpoints.
- Inventory management, allowing network administrators to track their network devices, and determine their characteristics (manufacturer, software and hardware versions, and serial / asset number).
- Support for receiving, storing and advertising of VLAN information from and to remote Network Connectivity Devices and Media Endpoint Devices (MEDs). LLDP-MED Network Policy TLVs are used to let the OmniSwitch advertise the VLAN or multiple VLANs, one for each specific application type, towards the connected MEDs.
- Support for receiving and storing of Inventory Management TLVs from remote Media Endpoint Devices.

VLAN assignment through explicit LLDP-MED Network Policy is supported on the OmniSwitch AOS.

- The LLDP-MED service advertises the information over the Logical Link-Layer Control Frames and records higher layer management reachability and connection endpoint information from adjacent devices.
- The LLDP-MED service enabled on OmniSwitch operates in advertising mode. However, it does not support any means for soliciting information from the MEDs.

LLDP-MED Network Policy

The network policies for MED devices can be configured on the OmniSwitch using the LLDP-MED CLI commands. A maximum of 32 network policies (0 - 31) can be configured on OmniSwitch. For the feature to work on fixed, mobile and 802.1x ports, there must be a VLAN Port Association (VPA) setup between the VLAN port and the advertised VLAN.

Network Policy - Application Types Supported

Each network policy can be configured with one application type as a mandatory parameter. The following application types are supported:

- Voice
- Voice Signaling
- Guest Voice
- Guest Voice Signaling
- Soft phone voice
- Video Conferencing
- Streaming voice
- Video Signaling

LLDP-MED Network Policy for VLAN Advertisement

The following provisions are provided in the OmniSwitch AOS to assign LLDP-MED network policy for VLAN advertisement:

- The OmniSwitch AOS allows the configuration of a maximum of 32 network policy IDs.
- Each network policy identifier (ID) must be configured with an application type and VLAN-ID as mandatory parameters. Other parameters include L2 priority and DSCP.
- Up to 8 network policy IDs; one per each application type; can be configured for a given port.
- Two or more network policy IDs with the same application type can not be assigned to a port.
- The network policy ID can be configured on fixed, mobile and 802.1x ports.
- When any MED connects to a port with an explicit MED network policy configuration, the OmniSwitch advertises the policy in the LLDPDU along with the MED Network Policy TLVs. This advertisement occurs only if the transmission of the Network Policy TLV is enabled by the user. The Media Endpoint Device must configure itself according to the advertised policy.

Fast Restart of LLDP on Detection of MED

The Fast Restart (as described in IEEE 802.1ab rev) is implemented on the OmniSwitch to transmit the related LLDP-MED Network Policy TLV as soon as a new MED endpoint is detected. The MED TLVs are encapsulated in the LLDPDU. The transmission of LLDP-MED TLV starts only when the OmniSwitch detects a MED capable endpoint on the VLAN port.

LLDP-MED for IP Phones

The LLDP-MED feature on OmniSwitch for voice transmission and VoIP Phones provides a network friendly solution. The information received from and transmitted to IP phones is tagged with voice VLAN ID.

A VLAN can be explicitly assigned to IP Phones through explicit definition of an LLDP-MED network policy identifier. The LLDP-MED Network Policy for the voice and voice signalling application must be activated on the OmniSwitch to advertise the VLAN to the connected IP Phones. For example on how to setup LLDP-MED for IP Phones, see the “Enabling and Disabling Notification” in Chapter 17.

Enabling and Disabling MED TLV

The **lldp tlv med** command is used to control per port LLDP Media End Device (MED) TLVs transmission in the LLDPDUs on a specific port, a slot, or all ports on a switch. When enabled, the LLDPDU administrative status must be in the transmit state.

To enable the LLDP-MED TLV LLDPDU transmission on a switch, enter the **lldp tlv med** command, as shown:

```
-> lldp chassis tlv med power enable
```

To enable the MED TLV on port 4 of slot 4, enter the following command at the CLI prompt:

```
-> lldp 4/4 tlv med capability enable
```

To disable the MED TLV on a switch, enter the **lldp tlv med** command, as shown:

```
-> lldp chassis tlv med power disable
```

To disable MED TLV on port 3 of slot 4, enter the following command at the CLI prompt:

```
-> lldp 4/3 tlv med capability disable
```

To enable the voice application network policy for a MED TLV on the port 3 of slot 4, enter the following command at the CLI prompt:

```
-> lldp 4/3 tlv med network policy 1 enable
```

To disable a MED TLV voice network policy on the port 3 of slot 4, enter the following command at the CLI prompt:

```
-> lldp 4/3 tlv med network policy 1 disable
```

Setting the Transmit Fast Start Count

To set the fast start count in order to transmit the LLDP-MED Network Policy TLV in LLDPDU as soon as the OmniSwitch detects a new MED capable endpoint device, enter the **lldp transmit fast-start-count** command.

```
-> lldp transmit fast-start-count 3
```

Chapter 27, "Configuring Access Guardian"

The following sections were added or modified to provide information about the 6.6.1.725 implementation of the authentication server down policy.

Enabling an Authentication Server Down Policy

An authentication server down policy is used to classify devices attempting to authenticate through 802.1.x switch ports when the RADIUS server is unreachable. This type of policy offers two options:

- Assign the device to a pre-configured User Network Profile (UNP). See the "Configuring User Network Profiles" section in Chapter 27 for more information.
- Block access to the switch; device traffic is dropped.

A default authentication server down policy is configured to block device access. To change the policy configuration, use the **802.1x auth-server-down policy** command. For example:

```
-> 802.1x auth-server-down policy user-network-profile tem_unp1
```

The **802.1x auth-server-down** command is used to enable or disable a policy. For example:

```
-> 802.1x auth-server-down enable
-> 802.1x auth-server-down disable
```

After a device is classified according to an authentication server down policy, an attempt to re-authenticate the device is made after a specific period of time (30 seconds by default). This time value is configurable using the **802.1x auth-server-down re-authperiod** command. For example:

```
-> 802.1x auth-server-down re-authperiod 500
```

The authentication server down policy and re-authentication time period configuration applies to all 802.1x ports on the switch. To verify the authentication server down policy configuration, use the **show 802.1x auth-server-down** command.

Note that when device authentication fails due to an unreachable RADIUS server, an event message is sent to the switch logging utility (swlog). See Chapter 36, "Using Switch Logging," for more information.