Access Control on the Wired Network

This workflow describes a phased approach to deploy IEEE 802.1x port-based authentication to provide secure and identity-based access control at the edge of the switch stack network.

Prerequisites for Access Control on the Wired Network

- Before globally enabling IEEE 802.1x authentication, remove the EtherChannel configuration from all of the interfaces.
- Define the authenticator (switch) to RADIUS server communication.
- Initiate Extensible Authentication Protocol (EAP) over LAN (EAPoL) messaging to successfully authenticate the end device (or supplicant).
- Based on your requirements, choose an appropriate EAP method. For information, see the *Wired 802.1x Deployment Guide*.
- Automate the certificate enrollment process for supplicants, as described in the *Certificate Autoenrollment in Windows Server 2003*.
- Enable machine authentication for end points, such as printers, to ensure that user login is supported.

Restrictions for Access Control on the Wired Network

- You cannot configure an IEEE 802.1x port that is a member of an EtherChannel.
- Destination ports configured with Switched Port Analyzer (SPAN) and remote SPAN (RSPAN) cannot be enabled with IEEE 802.1x authentication.
- You cannot enable an IEEE 802.1x port on trunk or dynamic ports. Dynamic ports can negotiate with its neighbors to become a trunk.
- Do not use port security with IEEE 802.1x. When IEEE 802.1x is enabled, port security then becomes redundant and might interfere with the IEEE 802.1x functionality.

Identify Configuration Values

Cisco Systems, Inc.
www.cisco.com

We recommend that you identify certain switch configuration values in advance so that you can proceed without interruption. We recommend that you take a print out of Table 7, and, as you follow the configuration sequence, replace the values in column B with your values in column C.

Note Depending on your authentication server settings, the authentication and accounting ports could be assigned the values 1812 and 1813 respectively.

Note Replace the blue italicized example values with your own values.

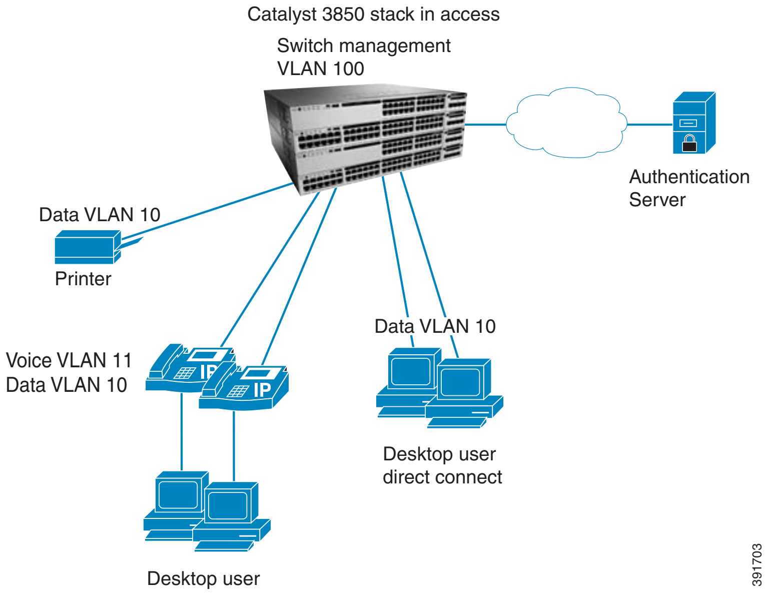
Table 7 Secure Access Control for Wired Network Values

A. Value Name	B. Example Value Names	C. Your Value
Interface range	***GigabitEthernet 1/0/1-1/0/24***	
RADIUS server	***AuthServer***	
RADIUS server IPv4 address	***192.168.254.14***	
Auth-port	***1656***	
Acct-port	***1646***	
RADIUS server encryption key	***cisco123***	
Data VLAN	***10***	
Voice VLAN	***11***	
Auth-server dead vlan	***20***	
Extended IP ACL	***LowImpactSecurity-acl***	

Note Configuration examples begin in global configuration mode, unless noted otherwise.

LAN Access Switch Topology with IEEE 802.1x Secure Access Control

Figure 9 LAN Access Switch Topology with IEEE 802.1x Secure Access Control



Securing Access Using 802.1x on a wired LAN

The following tasks are to be performed in the same order that is listed here.

- Recommendations for Configuring Security on a Wired LAN
- Provision Common Wired Security Access
- Provision in Monitor Mode
- Provision in Low-Impact Mode
- Provision in High-Impact Mode
-

Recommendations for Configuring Security on a Wired LAN

IEEE 802.1x permits or denies network connectivity based on the identity of users and devices. It provides a link between the user name and IP address, MAC address, and a port on a switch. It also provides customized network access based on the identity of the end device or user.

The main components of IEEE 802.1x are:

- Supplicant (end device)
- Authenticator (switch)
- Authentication server (RADIUS or ISE)

To provide secure access to your wired switch network, we recommend that you first provision your common wired security features. Provision security modes in phased deployments (monitor mode to high-security mode) of IEEE 802.1x authentication along with MAC Authentication Bypass (MAB), which uses the MAC address of the end device (or supplicant) to make decisions about access.

Note Each phased deployment should occur over time after ensuring that your network is ready to transition to the next security mode.

Table 8 describes the recommended IEEE 802.1x deployment scenarios that will have limited impact on network access. Test your network infrastructure while in monitor mode. If you are satisfied, then transition to low-impact mode and allow a subset of network traffic to pass through. Finally, transition to high-security mode, requiring authorization from all end devices.

Table 8 IEEE 802.1x Deployment Modes

Monitor Mode	Low-Impact Mode	High-Security Mode (Closed)
• Open access for unauthorized supplicants. • Extensive network visibility. • Monitor the network. • No impact to end devices.	• Limited access for unauthorized supplicants. • Differentiated access control using dynamic ACLs. • Limited impact to end devices.	• No access for unauthorized supplicants. • Heavily impacts supplicants.

Reference

For detailed information about wired mode deployments, see the *TrustSec Phased Deployment Configuration Guide*.

For basic information about IEEE 802.1x protocols, see the “8021X Protocols” section of the *Wired 802.1X Deployment Guide*.

Provision Common Wired Security Access

IEEE 802.1x port host modes determine whether more than one client can be authenticated on the port and how authentications is enforced:

Table 9 Types of IEEE 802.1x Port Host Modes

Single-Host	Multi-Host	Multi-Domain	Multi-Authentication
Allows only one end device to the IEEE 802.1x enabled switch port.	Authenticates the first MAC address and then allows an unlimited number of other MAC addresses.	Allows two endpoints on the port: one data endpoint and one voice endpoint.	Allows only one voice end device, but allows multiple data end devices. In this mode, all devices are authenticated.

Unless otherwise noted, we recommend that multiple-authentication mode be configured instead of single-host mode, for increased security:

- Multi-authentication mode authenticates all the devices that gain access to the network through a single switch port, such as devices connected through IP phones.
- Multi-authentication mode is more secure than multi-host mode (which also allows multiple data devices) because it authenticates all the devices that try to gain access to the network.

Step 1 Run the **show run** command on your switch to ensure that your access interface connections are set up.

This output is what you inherit after performing the "Access Interface Connectivity" workflow configuration for an interface connected to an IP phone.

```
Switch#show running-config int Te3/0/12
Building configuration...

Current configuration : 766 bytes
!
interface TenGigabitEthernet3/0/12
switchport mode access
switchport block unicast
switchport voice vlan 2
switchport port-security maximum 3
switchport port-security maximum 2 vlan access
switchport port-security violation restrict
switchport port-security aging time 1
switchport port-security aging type inactivity
switchport port-security
load-interval 30
trust device cisco-phone
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
auto qos voip cisco-phone
 macro description CISCO_PHONE_EVENT
spanning-tree portfast
spanning-tree bpduguard enable
service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
service-policy output AutoQos-4.0-Output-Policy
ip dhcp snooping limit rate 15
end
```

Step 2 (Optional) If you observe excessive timeouts, fine-tune the IEEE 802.1x timers and variables. Timers and variables are important for controlling the IEEE 802.1x authenticator process on the switch.

We recommend that you do not change the IEEE 802.1x timer and variable default settings, unless necessary.

Begin in interface configuration mode:

```
  dot1x timeout tx
-period 30
  dot1x max-reauth-req 2
  authentication timer restart 60
  dot1x timeout quiet-period 60
```

Step 3 Set the timers on the appropriate interfaces.

These timers and variables control IEEE 802.1x authenticator operations when end devices stop functioning during authentication.

Begin in interface configuration mode.

```
dot1x timeout supp-timeout 30
dot1x max-req 2
```

Reference

For detailed information about the IEEE 802.1x timers and variables, see the *Wired 802.1x Deployment Guide*.

Step 4 Enable MAC authentication bypass (MAB) from interface configuration mode to authenticate supplicants that do not support IEEE 802.1x authentication.

When MAB is enabled, the switch uses the MAC address of the device as its identity. The authentication has a database of MAC addresses that are allowed network access.

We recommend that you enable MAB to support non-802.1x-compliant devices. MAB also is an alternate authentication method when end devices fail IEEE 802.1x authentication due to restricted ACL access.

Begin in interface configuration mode.

```
mab
```

Step 5 Configure IEEE 802.1x on the appropriate interfaces.

When you configure an IEEE 802.1x parameter on a port, a dot1x authenticator is automatically created on the port. When that occurs, the **dot1x pae authenticator** command must also be configured to ensure that the dot1x authentication will work on legacy configurations.

Begin in interface configuration mode:

```
authentication port-control auto
dot1x pae authenticator
```

Step 6 Enable access control and IEEE 802.1x authentications.

Begin in global configuration mode.

```
!Enable new access control
!
aaa new-model
!
!Set authentication list for 802.1x
!
aaa authentication dot1x default group radius
!
!Enable 802.1x authentication
!
dot1x system-auth-control
```

Step 7 To establish the radius server, configure the RADIUS server with IP address, UDP port for authentication and accounting server, and server encryption key.

```
radius server AuthServer
address ipv4 192.168.254.14 auth-port 1656 acct-port 1646
key cisco123
```

Provision in Monitor Mode

Monitor mode enables IEEE 802.1x authentication without impacting the access of the end devices (supplicants) to a switch (authenticator). This mode allows you to continuously gather the following types of data for all the devices connected to your network:

- List of IEEE 802.1x-capable devices
- List of devices that are not capable of IEEE 802.1x
- Devices with good credentials
- Devices with bad credentials.
- List of valid MAC addresses (for MAB)
- List of unknown or invalid MAC addresses (for MAB)

We recommend monitor mode as a first-phase approach to provide secure access with IEEE 802.1x. Although this mode authenticates the end devices and users (supplicants), traffic is not impacted if authentication fails.

In monitor mode, IEEE 802.1x and MAB are enabled, but access is open to all users.

Step 8 To allow hosts to gain access to a controlled port, configure multi-authentication host mode and open authentication.

```
authentication host-mode multi-auth
authentication open
```

Step 9 Disable the Port Security feature, because when IEEE 802.1x is enabled, the Port Security feature becomes redundant and might interfere with the IEEE 802.1x functionality.

Begin in interface configuration mode.

```
  no switchport port-security
  no switchport port-security violation
  no switchport port-security aging type
  no switchport port-security aging time
  no switchport port-security maximum
```

Provision in Low-Impact Mode

The next deployment phase in securing your network is to provision in low impact mode, which allows differentiated network access to authenticated users while permitting basic network services for all users.

Note For information about configuration of multiple-authentication mode on IEEE 802.1x ports, see "Provision Common Wired Security Access".

Minimize the impact to your initial network access settings and add differentiated network access to authenticated users with low-impact mode provisioning. In low-impact mode, authentication is open and network access is contained using less restrictive port ACLs. After authentication, dACLs are used to allow full network access to end devices.

Step 10 configure multi-domain mode to prevent unauthorized users from accessing an interface after an authorized user has been authenticated.

```
authentication host-mode multi-domain
```

Step 11 Add a static ACL to allow basic network access.

Configure a restrictive port ACL that allows access for configuration and a Configured Trust List (CTL).

Begin in global configuration mode.

```
ip access-list extended LowImpactSecurity-acl
  permit tcp any any established
  permit udp any any eq bootps
  permit udp any any eq tftp
  permit udp any any eq domain
  exit
interface GigabitEthernet1/0/1
  ip access-group LowImpactSecurity-acl in
```

Provision in High-Impact Mode

The final deployment phase of securing your wired network is high-impact mode.

This phase goes beyond low-impact mode and provisions tight access control on the network port by configuring the default IEEE 802.1x authentication mode with dynamic VLAN for differentiated access.

Step 12 Configure multi-authentication host mode, and open authentication.

```
authentication host-mode multi-auth
authentication open
```

Step 13 Disable RADIUS for this deployment phase.

High-impact mode provides no network access to devices and users that fail authentication. In monitor mode and low-impact mode, we recommend that you identify and resolve the devices and user accounts that have failed authentication. Transition to high-impact mode when you are confident that end devices (that need network access) authenticate successfully, and authentication fails for devices and users that do not need access.

Begin in global configuration mode.

```
interface GigabitEthernet 1/0/1-1/0/24
  no authentication open
```

Step 14 Assign critical VLAN assignments for situations where the authentication server is unavailable.

The following command is used to configure a port to send both new and existing hosts to the critical VLAN when the RADIUS server is unavailable. Use this command for ports in multiple authentication (multiauth) mode or if the voice domain of the port is in MDA mode.

```
  authentication event server dead action authorize vlan 20
```

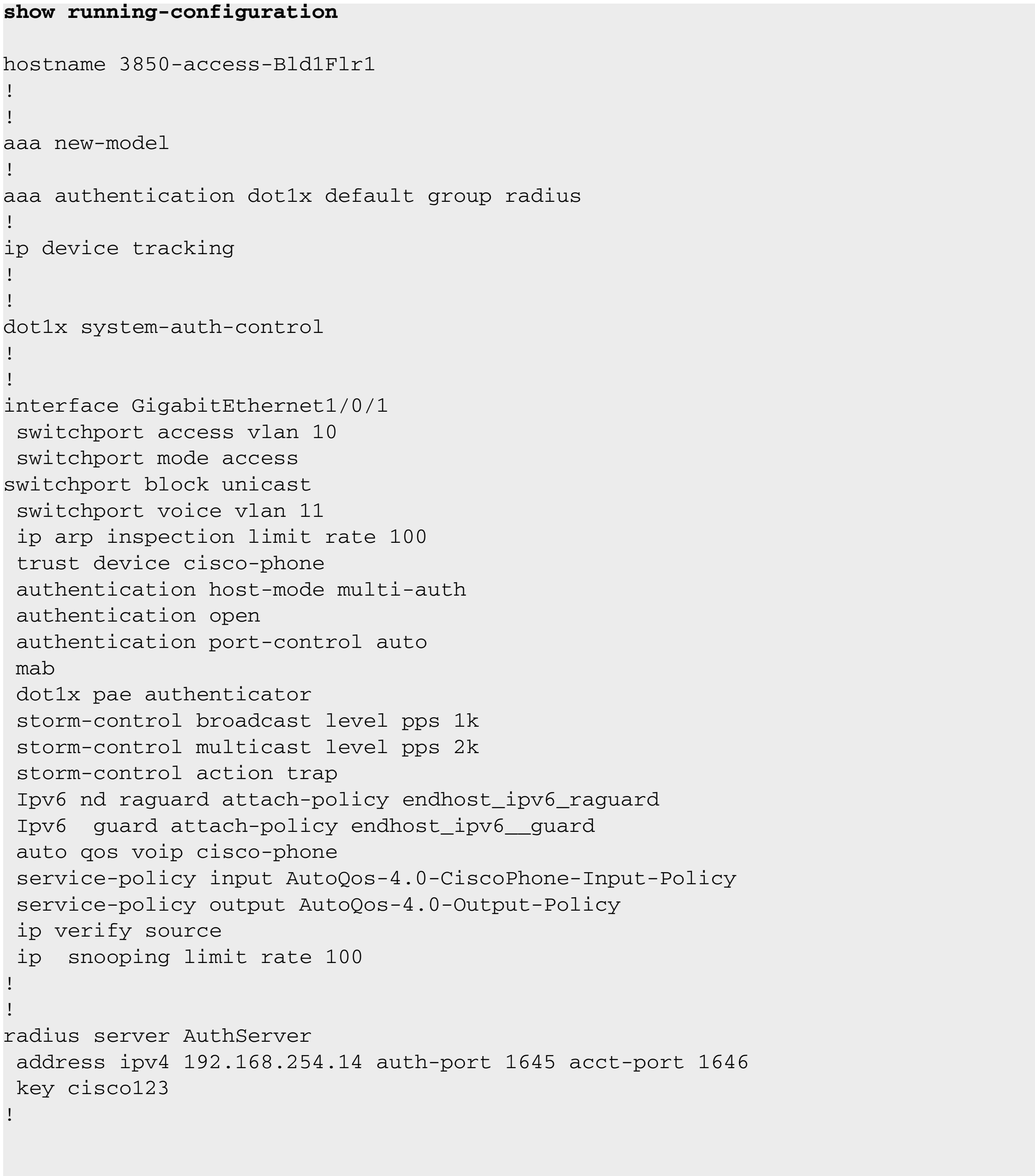
Step 15 If the authentication server does not respond, authorize voice.

```
  authentication dead action authorize voice
```

Show Running Configuration for Provisioning Modes

Step 1 Enter the **show running-configuration** command to display provisioning modes for the switch.

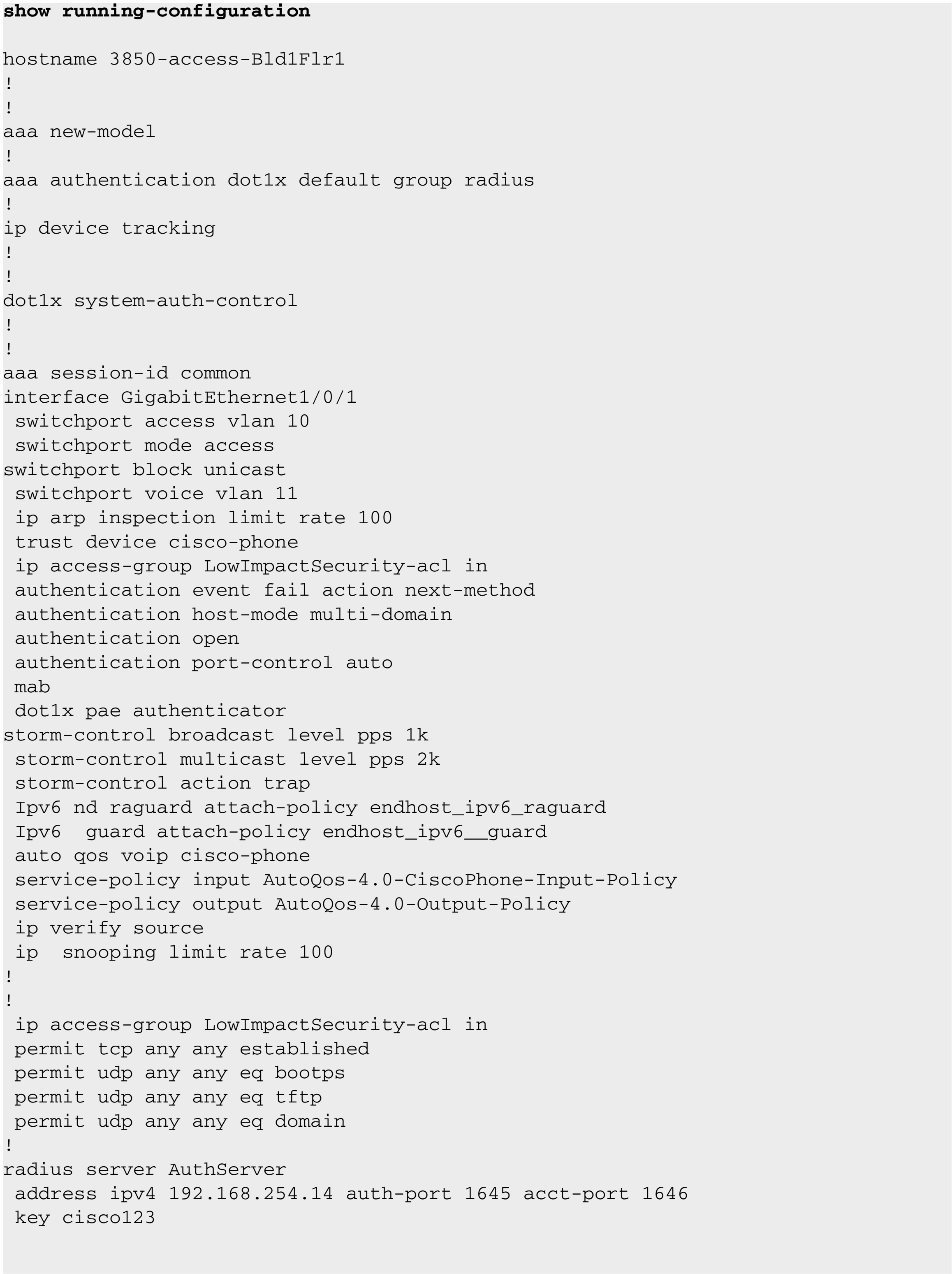
Figure 10 show running-configuration command for Provision in Monitor Mode



```
show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
switchport block unicast
 switchport voice vlan 11
 ip arp inspection limit rate 100
 trust device cisco-phone
 authentication host-mode multi-auth
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 Ipv6 nd raguard attach-policy endhost_ipv6_raguard
 Ipv6  guard attach-policy endhost_ipv6__guard
 auto qos voip cisco-phone
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
 ip verify source
 ip  snooping limit rate 100
!
!
radius server AuthServer
 address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
 key cisco123
!
```

Figure 11 how running-configuration command for Provision in Low-Impact Mode



```
show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
aaa session-id common
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
switchport block unicast
 switchport voice vlan 11
 ip arp inspection limit rate 100
 trust device cisco-phone
 ip access-group LowImpactSecurity-acl in
 authentication event fail action next-method
 authentication host-mode multi-domain
 authentication open
 authentication port-control auto
 mab
 dot1x pae authenticator
storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 Ipv6 nd raguard attach-policy endhost_ipv6_raguard
 Ipv6  guard attach-policy endhost_ipv6__guard
 auto qos voip cisco-phone
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
 ip verify source
 ip  snooping limit rate 100
!
!
 ip access-group LowImpactSecurity-acl in
 permit tcp any any established
 permit udp any any eq bootps
 permit udp any any eq tftp
 permit udp any any eq domain
!
radius server AuthServer
 address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
 key cisco123
```

Figure 12 how running-configuration command for Provision in High-Impact Mode

```
show running-configuration

hostname 3850-access-Bld1Flr1
!
!
aaa new-model
!
aaa authentication dot1x default group radius
!
ip device tracking
!
!
dot1x system-auth-control
!
!
aaa session-id common
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
switchport block unicast
 switchport voice vlan 11
 ip arp inspection limit rate 100
 trust device cisco-phone
 authentication event server dead action authorize vlan 20
 authentication event server dead action authorize voice
 authentication host-mode multi-auth
 authentication port-control auto
 mab
 dot1x pae authenticator
 storm-control broadcast level pps 1k
 storm-control multicast level pps 2k
 storm-control action trap
 Ipv6 nd raguard attach-policy endhost_ipv6_raguard
 Ipv6  guard attach-policy endhost_ipv6__guard
 auto qos voip cisco-phone
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
 ip verify source
 ip  snooping limit rate 100
!
!
radius server AuthServer
 address ipv4 192.168.254.14 auth-port 1645 acct-port 1646
 key cisco123
```

Monitoring IEEE 802.1x Status and Statistics

Step 1 Use the **show dot1x statistics** command to display switch-related and port-related IEEE 802.1x statistics.

To detect errors, filter the dot1x verbose messages that are enabled by default.

```
show dot1x statistics

Dot1x Global Statistics for
--------------------------------------------
RxStart = 7     RxLogoff = 0    RxResp = 0      RxRespID = 8
RxReq = 0       RxInvalid = 0   RxLenErr = 0
RxTotal = 29

TxStart = 0     TxLogoff = 0    TxResp = 0
TxReq = 0       ReTxReq = 0     ReTxReqFail = 0
TxReqID = 8     ReTxReqID = 0   ReTxReqIDFail = 0
TxTotal = 8
```

Step 2 Use the **show dot1x interface statistics** command to display IEEE 802.1x statistics for a specific port.

```
show dot1x  interface g1/0/1 statistics

Dot1x Authenticator Port Statistics for GigabitEthernet1/0/1
--------------------------------------------
RxStart = 10    RxLogoff = 0    RxResp = 0      RxRespID = 10
RxInvalid = 0   RxLenErr = 0    RxTotal = 37

TxReq = 0       TxReqID = 11    TxTotal = 11

RxVersion = 1   LastRxSrcMAC = 0023.33db.e970
```

Step 3 Use the **show dot1x all** command to display the IEEE 802.1x administrative and operational status for a switch.

```
show dot1x all

Sysauthcontrol              Enabled
Dot1x Protocol Version            3

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30
```

Step 4 Use the **show dot1x interface** command to display the IEEE 802.1x administrative and operational status for a specific port.

.

```
show dot1x interface g1/0/1

Dot1x Info for GigabitEthernet1/0/1
-----------------------------------
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```