Converged Access: Wireless QoS

This chapter describes how to configure the granular wireless quality of service (QoS) feature on a converged access network, which contains Cisco Catalyst 3850 Series and Cisco Catalyst 3650 Series Switches. This chapter also provides information on Wired QoS with reference to Wired AutoQoS.

Converged Access QoS

Converged Access QoS consists of Wired and a Wireless QoS components. In the context of wired QoS, you can use the Wired AutoQoS depending on the type of wired devices attached to the converged access switches (such as, Cisco-Phone, Cisco-Softphone, Cisco Telepresence System (CTS), Cisco video surveillance camera, Cisco Delivery Protocol (CDP)-capable Cisco digital media player, trusted devices, untrusted devices, and so on).

In the context of wireless QoS, the Cisco Catalyst 3850 Series and the Cisco Catalyst 3650 Series Switches have advanced wireless QoS capabilities. This ensures guaranteed bandwidth or services at a granular level, that includes access-point port, radio, SSID, and client levels. In the past, wireless networks lacked QoS visibility and enforcement and were vulnerable to unfair bandwidth allocation because QoS could not be applied inside the wireless tunnels. Converged Access switches terminate the wireless tunnels. Hence, QoS can be applied much closer to users.

For more information about configuring wired and wireless components, refer to the "Configuring Auto-QoS" chapter in the *QoS Configuration Guide*.

Note An Auto QOS policy, CAPWAP AP, is added on the AP connected port on Cisco Catalyst 4500 Series Switches, to prioritize wireless traffic.

```
Device# show run interface GigabitEthernet 1/43
Building configuration...

Current configuration : 196 bytes

!

interface GigabitEthernet 1/43

 switchport access vlan 60

 switchport mode access

 datalink flow monitor mac input

 spanning-tree portfast

 service-policy output Capwap-SRND4-Queuing-Policy

end

Policy Map Capwap-SRND4-Queuing-Policy

    Class Capwap-Priority-Queue

      priority

    Class Capwap-Control-Mgmt-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Multimedia-Conf-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Multimedia-Stream-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Trans-Data-Queue

      bandwidth remaining 10 (%)

    Class Capwap-Bulk-Data-Queue

      bandwidth remaining 4 (%)

    Class Capwap-Scavenger-Queue

      bandwidth remaining 1 (%)

    Class class-default

      bandwidth remaining 25 (%)
```

A converged access switch is capable of automatically allocating equal bandwidth among the connected users within a given SSID, with the help of the Approximate Fair Dropping (AFD) algorithm. This algorithm ensures that all the users within an SSID receive a fair share of the available bandwidth while they are connected to the network.

The purpose of the Converged Access: Wireless QoS chapter is to provide necessary guidance with the help of template policy definitions. These can either be utilized as-is or can be used as base policies that can be modified for a particular deployment.

To simplify the guidance, we have selected WLAN Enterprise, which is a commonly used SSID in most deployments, and also recommended the relevant Wireless QoS policies.

Supported Policies for Wireless Targets

Note

- Downstream Direction—From Controller to Access Point Traffic
- Upstream Direction—From Access Point to Controller Traffic

The following table provides information about the supported policies for wireless targets:

Table 1: Supported Policies for Wireless Targets

Wireless Target	Policy Supported on Wireless Targets	Policy Supported in Downstream Direction	Policy Supported in Upstream Direction
Wireless Port	Yes	Yes—User configurable	No
Radio	Yes	Yes—Not user configurable	No
SSID	Yes	Yes—User configurable	Yes—User configurable
Client	Yes	Yes—User configurable	Yes—User configurable

Note For more information on the Converged Access QoS concepts and configurations, refer to the "Configuring QoS" chapter in the *QoS Configuration Guide*.

Configuring ACL and Class Map

Configuring ACL Definitions

To configure ACL definitions, use the following commands:

```
!!
!!
!! Ingress Access Lists for QoS
!
!
Device(config)# ip access-list extended MultiEnhanced-Conf
```

```
 ! Real-Time Transport Protocol Traffic

Device(config-ext-nacl)# permit udp any any range 16384 32767
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Transactional-Data
 ! HTTPS

Device(config-ext-nacl)# permit tcp any any eq 443
 ! Oracle application

Device(config-ext-nacl)# permit tcp any any eq 1521
 ! nCube License Manager

Device(config-ext-nacl)# permit udp any any eq 1521
 ! Oracle Database common alternative

 Device(config-ext-nacl)# permit tcp any any eq 1526
 ! Prospero Data Access

 Device(config-ext-nacl)# permit udp any any eq 1526
 ! Oraclenames

 Device(config-ext-nacl)# permit tcp any any eq 1575
 ! Oraclenames

Device(config-ext-nacl)# permit udp any any eq 1575
 ! Oracle Net8 Cman

Device(config-ext-nacl)#  permit tcp any any eq 1630
 ! Oracle Net8 Cman

Device(config-ext-nacl)# permit udp any any eq 1630
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Bulk-Data
 ! SSH

Device(config-ext-nacl)# permit tcp any any eq 22
 ! SMTP-SSL

Device(config-ext-nacl)# permit tcp any any eq 465
 ! IMAP

Device(config-ext-nacl)# permit tcp any any eq 143
 ! IMAP-SSL

Device(config-ext-nacl)# permit tcp any any eq 993
 ! POP3-SSL

Device(config-ext-nacl)# permit tcp any any eq 995
 ! Elm-Momentum

Device(config-ext-nacl)# permit tcp any any eq 1914

 Device(config-ext-nacl)# permit tcp any any eq ftp

Device(config-ext-nacl)# permit tcp any any eq ftp-data

Device(config-ext-nacl)# permit tcp any any eq smtp

Device(config-ext-nacl)# permit tcp any any eq pop3
Device(config-ext-nacl)# exit

Device(config)# ip access-list extended Scavenger
 ! Chessmaster

Device(config-ext-nacl)# permit tcp any any range 2300 2400
 ! Chessmaster

Device(config-ext-nacl)# permit udp any any range 2300 2400
 ! Bit Torrent
```

```
Device(config-ext-nacl)# permit tcp any any range 6881 6999
 ! MSN Game Zone

Device(config-ext-nacl)#  permit tcp any any range 28800 29100
 ! Kazaa, Grokster

Device(config-ext-nacl)# permit tcp any any eq 1214
 ! Kazaa, Grokster

Device(config-ext-nacl)# permit udp any any eq 1214
 ! iTunes Music sharing

Device(config-ext-nacl)# permit tcp any any eq 3689
 ! Digital Audio Access Protocol

Device(config-ext-nacl)# permit udp any any eq 3689
 ! Yahoo Games

Device(config-ext-nacl)#  permit tcp any any eq 11999
```

Configuring Class Map Definitions

To configure class map definitions, use the following commands:

```
!!
!!
!! Class-Maps for Ingress Policies
!
!
Device(config)# class-map match-any Voip-Data-Class
Device(config-cmap)# match dscp ef
Device(config-cmap)# exit

Device(config)# class-map match-any Voip-Signal-Class
Device(config-cmap)# match dscp cs3
Device(config-cmap)# exit

Device(config)# class-map match-any Multimedia-Conf-Class
Device(config-cmap)# match access-group name MultiEnhanced-Conf
Device(config-cmap)# exit

Device(config)# class-map match-any Transaction-Class
Device(config-cmap)# match access-group name Transactional-Data
Device(config-cmap)# exit

Device(config)# class-map match-any Bulk-Data-Class
Device(config-cmap)# match access-group name Bulk-Data
Device(config-cmap)# exit

Device(config)# class-map match-any Scavenger-Class
Device(config-cmap)# match access-group name Scavenger
Device(config-cmap)# exit
!!
!!
!! Two realtime classes for Voice and Video used with egress policies
!
!
Device(config)# class-map match-any RT1-Class
Device(config-cmap)# match dscp ef
Device(config-cmap)# match dscp cs6
Device(config-cmap)# exit

Device(config)# class-map match-any RT2-Class
Device(config-cmap)# match dscp cs4
Device(config-cmap)# match dscp cs3
Device(config-cmap)# exit
```

Wireless Ingress QoS

For wireless ports, the default system behavior is non-trust, which implies that when the switch is booted, all markings for the wireless ports are defaulted to zero and no traffic is prioritized. Disable the non-trust configuration before you continue with the wireless ingress configuration.

To disable the default non-trust of QoS markings, use the following command:

```
Device(config)# no qos wireless-default-untrust
```

Enterprise WLAN Client Ingress Policy

Before you begin, make sure that the relevant Enterprise WLAN already exists on the switch.

In the context of Enterprise WLAN, the enterprise WLAN client ingress policy re-marks the ingress traffic as per the traffic type at the client level. We recommend that you re-mark the various types of ingress traffic at the client-level.

To re-mark the ingress traffic using enterprise WLAN client ingress policy, use the following commands:

```
Device(config)# policy-map client_input_policy
Device(config-pmap)# class Voip-Data-Class
Device(config-pmap-c)# set dscp ef
Device(config-pmap-c)# exit

Device(config-pmap)# class Voip-Signal-Class
Device(config-pmap-c)# set dscp cs3
Device(config-pmap-c)# exit

Device(config-pmap)# class Multimedia-Conf-Class
Device(config-pmap-c)# set dscp af41
Device(config-pmap-c)# exit

Device(config-pmap)# class Transaction-Class
Device(config-pmap-c)# set dscp af21
Device(config-pmap-c)# exit

Device(config-pmap)# class Bulk-Data-Class
Device(config-pmap-c)# set dscp af11
Device(config-pmap-c)# exit

Device(config-pmap)# class Scavenger-Class
Device(config-pmap-c)# set dscp cs1
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap-c)# set dscp default
Device(config-pmap-c)# exit
```

To apply the enterprise WLAN client ingress policy, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# service-policy client input client_input_policy <<<< The client keyword
 is included since this policy is applied at the client level.
```

Wireless Egress QoS

Wireless egress QoS can be applied at multiple places in the wireless egress path such as the port, radio, SSID, and Client levels. The wireless egress policy enables you to fine-tune the performance of the converged access switches during congestion.

An effective port-level egress QoS policy uses class maps to classify traffic into priority and nonpriority queues. The port-child-policy port-level egress policy defines the QoS policy of the directly connected access point. All the access points receive the same egress QoS policy. If you do not apply the QoS policies at instances such as radio and client, all the egress traffic for wireless interfaces are subjected to the same behavior, as per the policy.

At the port-child-policy port level, the policy model has four Egress Queues, two priority queues, and two non-priority queues. The policy model does not have any drop thresholds. The port-child-policy is a built-in policy map that is implicitly applied to the wireless interfaces. To modify the port-level policy, use the following commands:

```
Device(config)# class-map RTI-class
Device(config-cmap)# exit
Device(config)# class-map RT2-class
Device(config-pmap-c)# exit
!

Device(config)# policy-map port-child-policy
Device(config-pmap)# class non-client-nrt-class
Device(config-pmap-c)# bandwidth remaining ratio 7
Device(config-pmap-c)# exit
Device(config-pmap)#   class RTI-class
Device(config-pmap-c)# priority level 1 percent 10
Device(config-pmap-c)# exit
Device(config-pmap)#   class RT2-class
Device(config-pmap-c)# priority level 2 percent 20
Device(config-pmap-c)# exit
Device(config-pmap)#  class class-default
Device(config-pmap-c)# bandwidth remaining ratio 63
Device(config-pmap-c)# end
```

Note The port-child-policy is applied implicitly, as soon as an access point is connected and is detected on the interface.

Enterprise WLAN SSID Egress Policy

Use the SSID-level policy maps to allocate bandwidth as per the SSID. This enables you to prioritize the traffic of one SSID during congestion.

Enterprise WLAN SSID egress is a hierarchical policy in which the parent policy shapes up to 100% of the available radio bandwidth. The child policy defines the relevant policy values for the real time priority queues (for voice and video). The **bandwidth remaining ratio** command ensures that the required bandwidth is maintained as compared to the remaining SSIDs. You can change this value based on a specific requirement.

To run the Enterprise WLAN SSID egress policy, use the following commands:

```
Device(config)# policy-map SSID_child_policy
Device(config-pmap)# class RT1-Class
Device(config-pmap-c)# priority level 1
Device(config-pmap-c)# police 15000000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class RT2-Class
Device(config-pmap-c)# priority level 2
Device(config-pmap-c)# police 30000000 conform-action transmit exceed-action drop
Device(config-pmap-c-police)# exit
Device(config-pmap-c)# exit

Device(config-pmap)# class class-default
Device(config-pmap)# exit

Device(config)# policy-map SSID-output-policy
Device(config-pmap)# class class-default
Device(config-pmap-c)# shape average percent 100
Device(config-pmap-c)# queue-buffers ratio 0
Device(config-pmap-c)# bandwidth remaining ratio 70
Device(config-pmap-c)# service-policy SSID-child-policy
```

To apply the Enterprise VLAN SSID egress policy, use the following commands:

```
Device(config)# wlan profile-name
Device(config-wlan)# Service-policy output SSID-output-policy
```

Note After you configure the **bandwidth remaining ratio** command on one SSID, it must be configured on all the available SSIDs in the deployment in order to have a predictable behavior.

Note The radio-level egress policies and the client-level egress policies cannot be defined as already mentioned in this document.

Verifying a Policy Installation

To verify the port-level policy that is installed, use the following commands. The interface in the example below is the interface connected to the access point.

```
Device# show platform qos policies PORT

Loc Interface          IIF-ID             Dir Policy             State
--- ------------------ ------------------ --- ------------------ ---------------
.
.
.
L:1 interface          iif-id             OUT port_child_policy  INSTALLED IN HW

Device# show policy-map interface interface
 interface
.
.
.
        Class-map: non-client-nrt-class (match-any)
          Match: non-client-nrt
            0 packets, 0 bytes
            5 minute rate 0 bps
          Queueing

          (total drops) 0
          (bytes output) 68206789
          bandwidth remaining ratio 7

        Class-map: RT1-Class (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Match:  dscp cs6 (48)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Priority: 10% (60000 kbps), burst bytes 1500000,

          Priority Level: 1

        Class-map: RT2-Class (match-any)
          Match:  dscp cs4 (32)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Match:  dscp cs3 (24)
            0 packets, 0 bytes
            5 minute rate 0 bps
          Priority: 20% (120000 kbps), burst bytes 3000000,

          Priority Level: 2

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            5 minute rate 0 bps
          Queueing

          (total drops) 0
          (bytes output) 0
          bandwidth remaining ratio 63
```

To verify an SSID-level policy that is installed, use the following commands:

```
Device# show platform qos policies SSID

Loc Interface     IIF-ID   Dir Policy                        State
--- ------------- -------- --- ----------------------------- ---------------
.
.
.
L:1 interfaceID   iif-id   OUT SSID_output_policy            INSTALLED IN HW
L:1 interfaceID   iif-id   OUT SSID_child_policy             INSTALLED IN HW

Device# show policy-map interface wireless SSID name profileName

SSID profileName iifid: 0x0108B80000000025.0x00E447800000010B.0x00EF19000000012E

  Service-policy output: SSID_output_policy

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      shape (average) cir 200000000, bc 800000, be 800000
      target shape rate 200000000
      queue-buffers ratio 0
      bandwidth remaining ratio 70

      Service-policy : SSID_child_policy

        Class-map: RT1-Class (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            30 second rate 0 bps
          Match:  dscp cs6 (48)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 1
          police:
              cir 15000000 bps, bc 468750 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps

        Class-map: RT2-Class (match-any)
          Match:  dscp cs4 (32)
            0 packets, 0 bytes
            30 second rate 0 bps
          Match:  dscp cs3 (24)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 2
          police:
              cir 30000000 bps, bc 937500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
.
.
.
```

To verify a client-level policy that is installed, use the following commands:

```
Device# show platform qos policies CLIENT

Loc Interface        IIF-ID Dir Policy                        State
--- ---------------- ------ --- ----------------------------- ---------------
L:1 ClientMACAddress iif-id IN  client_input_policy INSTALLED IN HW
.
.
.

Device# show policy-map interface wireless client mac ClientMACAddress

Client ClientMACAddress ..
.
.
.

  Service-policy input: client-input-policy

    Class-map: Voip-Data-Class (match-any)
      Match:  dscp ef (46)
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp ef

    Class-map: Voip-Signal-Class (match-any)
      Match:  dscp cs3 (24)
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs3
    Class-map: Multimedia-Conf-Class (match-any)
      Match: access-group name MultiEnhanced-Conf
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af41

    Class-map: Transaction-Class (match-any)
      Match: access-group name Transactional-Data
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af21

    Class-map: Bulk-Data-Class (match-any)
      Match: access-group name Bulk-Data
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs1

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp default

Device# show policy-map client mac-address ClientMACAddress service-policy input

Wireless Client QoS Service Policy
Policy Name  : client_input_policy
Policy State : Installed
```

To verify a radio-level policy, which is on by default, use the following command:

```
Device# show platform qos policies RADIO

Loc Interface          IIF-ID             Dir Policy             State
--- ------------------ ------------------ --- ------------------ ---------------
L:1 R71187880340357388 0x00fce9000000010c OUT def-11an           INSTALLED IN HW
.
.
.
```

To verify a QoS policy based on the WLAN, use the following commands:

```
Device# show wlan name profileName | include Policy

AAA Policy Override                             : Disabled
QoS Service Policy - Input
  Policy Name                                   : unknown
  Policy State                                  : None
QoS Service Policy - Output
  Policy Name                                   : SSID-output-policy
  Policy State                                  : Validated
QoS Client Service Policy
  Input  Policy Name                            : client_input_policy
  Output Policy Name                            : unknown
Radio Policy                                    : All
```