BYOD Converged Access Configurations

Revised: March 6, 2014

What's New: The configurations have been updated to add the QoS configurations discussed in Converged Access QoS in Chapter 7, "Application Considerations and License Requirements for BYOD" and to add the application visibility configurations discussed in Converged Access Application Visibility in Chapter 24, "Mobile Traffic Engineering with Application Visibility and Control (AVC)."

Converged Access—Campus

The Converged Access Campus consists of CT5760 as the Mobility Controller (MC) and the Catalyst 3850 as the Mobility Agent (MA).

An example configuration of a CT5760 in a campus design acting as a MC is shown below. The QoS model shown below assumes a 2P4Q4T queueing model for the wired uplink port, an upstream client QoS policy which shows remarking only, and a static assignment of the upstream client QoS policy.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
!
aaa session-id common
!
ip device tracking
!
!
captive-portal-bypass
!
dot1x system-auth-control
!
!
table-map remarkToDefault
 default 0
!
```

```
!
mac access-list extended MAC_ALLOW
 permit any any
spanning-tree mode pvst
spanning-tree extend system-id
!
!
class-map match-any REALTIME-QUEUE
 match dscp ef
class-map match-any NETWORK-CONTROL-QUEUE
 match dscp cs6
class-map match-any SIGNALING-QUEUE
 match dscp cs3
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any SCAVENGER-QUEUE
  match  dscp cs1
class-map match-any BULK-DATA
  match access-group name BULK-DATA
class-map match-any INTERACTIVE-VIDEO
  match access-group name INTERACTIVE-VIDEO
class-map match-any RT2
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any RT1
  match  dscp ef
  match  dscp cs6
  match  dscp cs3
class-map match-any INTERACTIVE-VIDEO-QUEUE
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any BULK-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp af13
class-map match-any VOICE
  match  dscp ef
  match access-group name VOICE
class-map match-any SCAVENGER
  match access-group name SCAVENGER
class-map match-any non-client-nrt-class
  match non-client-nrt
class-map match-any SIGNALING
  match  dscp cs3
  match access-group name SIGNALING
class-map match-any TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-DATA
class-map match-any NETWORK-CONTROL
match dscp cs6
!
policy-map port_child_policy
 class non-client-nrt-class
    bandwidth remaining ratio 7
 class RT1
    priority level 1
    police rate percent 10 conform-action transmit exceed-action drop
 class RT2
    priority level 2
    police rate percent 20 conform-action transmit exceed-action drop
 class class-default
```

```
    bandwidth remaining ratio 63
policy-map REALTIME-DOWNSTREAM-CHILD
 class RT1
    priority level 1
    police 15000000   conform-action transmit exceed-action drop
 class RT2
    priority level 2
    police 30000000    conform-action transmit     exceed-action drop
 class class-default
policy-map EMPLOYEE-DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD
policy-map REMARK_UPSTREAM_CLIENT
 class VOICE
   set dscp ef
 class SIGNALING
   set dscp cs3
 class INTERACTIVE-VIDEO
   set dscp af41
 class TRANSACTIONAL-DATA
   set dscp af21
 class BULK-DATA
   set dscp af11
 class SCAVENGER
   set dscp cs1
 class class-default
   set dscp default
policy-map PROVISIONING_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map DEFAULT_UPSTREAM_CLIENT
 class class-default
   set dscp default
policy-map REALTIME-DOWNSTREAM-CHILD-PERSONAL
 class RT1
    priority level 1
    police 4500000    conform-action transmit     exceed-action drop
 class RT2
    priority level 2
    police 9000000    conform-action transmit     exceed-action drop
 class class-default
policy-map PERSONAL_DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD-PERSONAL
policy-map IT_DEVICES_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map GUEST_DOWNSTREAM
 class class-default
    shape average 6000000
    queue-buffers ratio 0
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map 2P6Q3T
 class REALTIME-QUEUE
    priority level 1
     police rate percent 10
 class INTERACTIVE-VIDEO-QUEUE
```

```
    priority level 2
     police rate percent 20
class NETWORK-CONTROL-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
class SIGNALING-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10 class BULK-DATA-QUEUE
    bandwidth remaining percent 20
    queue-buffers ratio 10
    queue-limit dscp  af11 percent 100
    queue-limit dscp  af12 percent 90
    queue-limit dscp  af13 percent 80
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 34
    queue-buffers ratio 10
    queue-limit dscp  af21 percent 100
    queue-limit dscp  af22 percent 90
    queue-limit dscp  af23 percent 80
 class SCAVENGER-QUEUE
    bandwidth remaining percent 1
    queue-buffers ratio 10
 class class-default
    bandwidth remaining percent 35
    queue-buffers ratio 25
!
!
!interface Vlan2
 description ### BYOD-Employee Vlan ###
 ip address 10.231.2.7 255.255.255.0
 load-interval 30
!
interface Vlan3
 description ### BYOD-Provisioning Vlan ###
 ip address 10.231.3.7 255.255.255.0
 load-interval 30
!
interface Vlan47
 description ### Mgmt Vlan ###
 ip address 10.225.47.2 255.255.255.0
 load-interval 30
!
interface TenGigabitEthernet 1/1/1
service-policy out 2P6Q3T
!
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended ACL_BLACKHOLE
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
!
ip access-list extended ACL_BLACKHOLE_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit ip any any
!
ip access-list extended ACL_Full_Access
 permit ip any any
!
ip access-list extended ACL_ISE_Remediate
```

```
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any 23.0.0.0 0.255.255.255
 permit ip any 17.0.0.0 0.255.255.255
 permit ip any 184.0.0.0 0.255.255.255
 permit ip any 8.0.0.0 0.255.255.255
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
 permit ip any host 10.225.100.10
 permit ip any 173.223.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL_ISE_Remediate_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any 23.0.0.0 0.255.255.255
 deny   ip any 17.0.0.0 0.255.255.255
 deny   ip any 184.0.0.0 0.255.255.255
 deny   ip any 8.0.0.0 0.255.255.255
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 deny   ip any host 10.225.100.10
 deny   ip any 173.223.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Internet_Only
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any host 10.225.100.10
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Internet_Redirect
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any host 10.225.100.10
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 172.16.0.0 0.15.255.255
 permit ip any 192.168.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL_Partial_Access
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 10.230.4.0 0.0.0.255
 permit ip any host 10.230.6.2
 permit ip any host 10.225.100.10
 deny   ip any 10.230.0.0 0.0.255.255
 deny   ip any 10.225.0.0 0.0.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
```

```
ip access-list extended ACL_Provisioning
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
ip access-list extended ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE_ACL
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
!
ip access-list extended VOICE
remark - CISCO-JABBER-REDUCED-PORT-RANGE
permit udp any any range 16384 17384
!
ip access-list extended INTERACTIVE-VIDEO
remark CISCO-JABBER-RTP
permit udp any any range 17385 32767
remark MICROSOFT-LYNC
permit tcp any any range 50000 59999
!
ip access-list extended SIGNALING
remark SCCP
permit tcp any any eq 2000
remark SIP
permit tcp any any range 5060 5061
!
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq 443
remark CITRIX
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
remark ORACLE
permit tcp any any eq 1521
permit tcp any any eq 1527
permit tcp any any eq 1575
permit tcp any any eq 1630
permit tcp any any eq 6200
!
ip access-list extended BULK-DATA
remark FTP
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark SSH/SFTP
permit tcp any any eq 22
remark SMTP/SECURE SMTP
permit tcp any any eq smtp
permit tcp any any eq 465
remark IMAP/SECURE IMAP
permit tcp any any eq 143
permit tcp any any eq 993
remark POP3/SECURE POP3
```

```
permit tcp any any eq pop3
permit tcp any any eq 995
remark CONNECTED PC BACKUP
permit tcp any eq 1914 any
!
ip access-list extended SCAVENGER
remark BITTORRENT
permit tcp any any range 6881 6999
remark APPLE ITUNES MUSIC SHARING
permit tcp any any eq 3689
permit udp any any eq 3689
remark MICROSOFT DIRECT X GAMING
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 5 tries 3
radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key 7 1237161E060E5D56797F71
!
wireless mobility controller peer-group 100
wireless mobility controller peer-group 100 bridge-domain-id 1
wireless mobility controller peer-group 100 member ip 10.203.61.5 public-ip 10.203.61.5
wireless mobility controller peer-group 100 member ip 10.203.71.5 public-ip 10.203.71.5
wireless mobility controller peer-group 200
wireless mobility controller peer-group 200 bridge-domain-id 1
wireless mobility controller peer-group 200 member ip 10.207.61.5 public-ip 10.207.61.5
wireless mobility controller peer-group 200 member ip 10.207.71.5 public-ip 10.207.71.5
wireless mobility controller peer-group 200 member ip 10.207.81.5 public-ip 10.207.81.5
wireless mobility controller peer-group 300
wireless mobility controller peer-group 300 bridge-domain-id 1
wireless mobility controller peer-group 300 member ip 10.211.61.5 public-ip 10.211.61.5
wireless mobility controller peer-group 300 member ip 10.211.71.5 public-ip 10.211.71.5
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group member ip 10.225.45.2 public-ip 10.225.45.2
wireless mobility group name byod
wireless mobility dscp 48
wireless management interface Vlan47
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless exclusionlist 1CB0.9414.9077 description gregg
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security web-auth parameter-map global
service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output EMPLOYEE-DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output GUEST_DOWNSTREAM
```

```
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD-Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PROVISIONING_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan BYOD_Personal_Device 4 BYOD_Personal_Device
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 security web-auth parameter-map global
service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PERSONAL_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan IT_Devices 5 IT_Devices
 aaa-override
 client vlan BYOD-Employee
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth parameter-map global
 service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output IT_DEVICES_DOWNSTREAM
 session-timeout 1800
 no shutdown
```

An example configuration of Converged Access Catalyst 3850 in a campus design acting as a Mobility Agent is shown below:

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 0525150635491F5B4A5142
 auth-type any
!
aaa session-id common
!
ip device tracking
!
!
captive-portal-bypass
!
!
```

```
dot1x system-auth-control
!
table-map remarkToDefault
 default 0
!
mac access-list extended MAC_ALLOW
 permit any any
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan 57
 name Employee
!
vlan 58
 name Provisioning
!
vlan 59-60
!
vlan 61
 name Access_Point
!
vlan 777
 name Guest
!
!
!
!
class-map match-any REALTIME-QUEUE
 match dscp ef
class-map match-any NETWORK-CONTROL-QUEUE
 match dscp cs6
class-map match-any SIGNALING-QUEUE
 match dscp cs3
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any SCAVENGER-QUEUE
  match  dscp cs1
class-map match-any BULK-DATA
  match access-group name BULK-DATA
class-map match-any INTERACTIVE-VIDEO
  match access-group name INTERACTIVE-VIDEO
class-map match-any RT2
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any RT1
  match  dscp ef
  match  dscp cs6
  match  dscp cs3
class-map match-any INTERACTIVE-VIDEO-QUEUE
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any BULK-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp af13
!
class-map match-any VOICE
  match  dscp ef
  match access-group name VOICE
class-map match-any SCAVENGER
```

```
  match access-group name SCAVENGER
class-map match-any non-client-nrt-class
  match non-client-nrt
class-map match-any SIGNALING
  match  dscp cs3
  match access-group name SIGNALING
class-map match-any TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-DATA
class-map match-any NETWORK-CONTROL
match dscp cs6
!
!
policy-map port_child_policy
 class non-client-nrt-class
    bandwidth remaining ratio 7
 class RT1
    priority level 1
    police rate percent 10 conform-action transmit exceed-action drop
 class RT2
    priority level 2
    police rate percent 20 conform-action transmit exceed-action drop
 class class-default
    bandwidth remaining ratio 63
policy-map REALTIME-DOWNSTREAM-CHILD
 class RT1
    priority level 1
    police 15000000   conform-action transmit exceed-action drop
class RT2
    priority level 2
    police 30000000    conform-action transmit     exceed-action drop
 class class-default
policy-map EMPLOYEE-DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD
policy-map REMARK_UPSTREAM_CLIENT
 class VOICE
   set dscp ef
 class SIGNALING
   set dscp cs3
 class INTERACTIVE-VIDEO
   set dscp af41
 class TRANSACTIONAL-DATA
   set dscp af21
 class BULK-DATA
   set dscp af11
 class SCAVENGER
   set dscp cs1
 class class-default
   set dscp default
policy-map PROVISIONING_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map DEFAULT_UPSTREAM_CLIENT
 class class-default
   set dscp default
policy-map REALTIME-DOWNSTREAM-CHILD-PERSONAL
 class RT1
    priority level 1
    police 4500000    conform-action transmit     exceed-action drop
 class RT2
    priority level 2
```

```
    police 9000000    conform-action transmit     exceed-action drop
 class class-default
policy-map PERSONAL_DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD-PERSONAL
policy-map IT_DEVICES_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map GUEST_DOWNSTREAM
 class class-default
    shape average 6000000
    queue-buffers ratio 0
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map 2P6Q3T
 class REALTIME-QUEUE
    priority level 1
     police rate percent 10
 class INTERACTIVE-VIDEO-QUEUE
    priority level 2
     police rate percent 20
class NETWORK-CONTROL-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
class SIGNALING-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
 class BULK-DATA-QUEUE
    bandwidth remaining percent 20
    queue-buffers ratio 10
    queue-limit dscp  af11 percent 100
    queue-limit dscp  af12 percent 90
    queue-limit dscp  af13 percent 80
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 34
    queue-buffers ratio 10
    queue-limit dscp  af21 percent 100
    queue-limit dscp  af22 percent 90
    queue-limit dscp  af23 percent 80
 class SCAVENGER-QUEUE
    bandwidth remaining percent 1
    queue-buffers ratio 10
 class class-default
    bandwidth remaining percent 35
    queue-buffers ratio 25
!
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 57
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
```

```
 dot1x timeout tx-period 3
 spanning-tree portfast
!
interface TenGigabitEthernet 1/1/1
service-policy out 2P6Q3T
!
interface Vlan61
 ip address 10.207.61.5 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
ip http active-session-modules none
!
ip access-list extended ACL-DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
 deny   ip any any log
ip access-list extended ACL_BLACKHOLE
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
ip access-list extended ACL_BLACKHOLE_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit ip any any
ip access-list extended ACL_Full_Access
 permit ip any any
ip access-list extended ACL_ISE_Remediate
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any 23.0.0.0 0.255.255.255
 permit ip any 17.0.0.0 0.255.255.255
 permit ip any 184.0.0.0 0.255.255.255
 permit ip any 8.0.0.0 0.255.255.255
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
 permit ip any host 10.225.100.10
 deny   ip any any
ip access-list extended ACL_ISE_Remediate_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any 23.0.0.0 0.255.255.255
 deny   ip any 17.0.0.0 0.255.255.255
 deny   ip any 184.0.0.0 0.255.255.255
 deny   ip any 8.0.0.0 0.255.255.255
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 deny   ip any host 10.225.100.10
 permit ip any any
ip access-list extended ACL_Internet_Only
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
```

```
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any host 10.225.100.10
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Internet_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any host 10.225.100.10
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 172.16.0.0 0.15.255.255
 permit ip any 192.168.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL_Partial_Access
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 10.230.4.0 0.0.0.255
 permit ip any host 10.230.6.2
 permit ip any host 10.225.100.10
 deny   ip any 10.230.0.0 0.0.255.255
 deny   ip any 10.225.0.0 0.0.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Provisioning
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
ip access-list extended ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 permit tcp any any eq www
 permit tcp any any eq 443
!
ip access-list extended VOICE
remark - CISCO-JABBER-REDUCED-PORT-RANGE
permit udp any any range 16384 17384
!
ip access-list extended INTERACTIVE-VIDEO
remark CISCO-JABBER-RTP
permit udp any any range 17385 32767
remark MICROSOFT-LYNC
permit tcp any any range 50000 59999
!
ip access-list extended SIGNALING
remark SCCP
permit tcp any any eq 2000
remark SIP
permit tcp any any range 5060 5061
```

```
!
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq 443
remark CITRIX
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
remark ORACLE
permit tcp any any eq 1521
permit tcp any any eq 1527
permit tcp any any eq 1575
permit tcp any any eq 1630
permit tcp any any eq 6200
!
ip access-list extended BULK-DATA
remark FTP
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark SSH/SFTP
permit tcp any any eq 22
remark SMTP/SECURE SMTP
permit tcp any any eq smtp
permit tcp any any eq 465
remark IMAP/SECURE IMAP
permit tcp any any eq 143
permit tcp any any eq 993
remark POP3/SECURE POP3
permit tcp any any eq pop3
permit tcp any any eq 995
remark CONNECTED PC BACKUP
permit tcp any eq 1914 any
!
ip access-list extended SCAVENGER
remark BITTORRENT
permit tcp any any range 6881 6999
remark APPLE ITUNES MUSIC SHARING
permit tcp any any eq 3689
permit udp any any eq 3689
remark MICROSOFT DIRECT X GAMING
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
!
!
ip radius source-interface Vlan61
logging 10.230.1.83
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 5 tries 3
radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key 7 153C1805102F7A767B6760
!
!
wireless mobility controller ip 10.225.47.2 public-ip 10.225.47.2
wireless mobility dscp 48
wireless management interface Vlan61
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless broadcast
wireless multicast
```

```
wireless mgmt-via-wireless
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan Employee
 nac
 session-timeout 300
 service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output EMPLOYEE-DOWNSTREAM
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
 service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output GUEST_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan Provisioning
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PROVISIONING_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan BYOD_Personal_Device 4 BYOD_Personal_Device
 client vlan Guest
 mobility anchor 10.225.50.36
 service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PERSONAL_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan IT_Devices 5 IT_Devices
 aaa-override
 client vlan Employee
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output IT_DEVICES_DOWNSTREAM
 session-timeout 1800
 no shutdown
```

Converged Access—Branch

An example configuration of a Converged Access Catalyst 3850 in a branch design is shown below. Note that in a branch design, the Catalyst 3850 acts both as a Mobility Controller (MC) and a Mobility Agent (MA) in a single switch. The configuration also shows the AVC configuration.

```
aaa new-model
!
!
aaa authentication login default enable
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
!
!
!
aaa server radius dynamic-author
 client 10.225.49.15 server-key 7 032A4802120A701E1D5D4C
 auth-type any
!
aaa session-id common
switch 1 provision ws-c3850-24p
!
ip device tracking
!
!
captive-portal-bypass
!
!
mac access-list extended MAC_ALLOW
 permit any any
!
flow record rodrec_av1
 description IPv4flow
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match flow direction
 match application name
 match wireless ssid
 collect counter bytes long
 collect counter packets long
 collect wireless ap mac address
 collect wireless client mac address
!
!
!
flow monitor rodmon_av1
 cache timeout inactive 200
 record rodrec_av1
!

!
table-map remarkToDefault
 default 0
!
vlan 10
 name BYOD-Employee
!
```

```
vlan 11
 name BYOD-Provisioning
!
vlan 17
 name AP_Management
!
vlan 18
!
vlan 777
 name BYOD_Guest
!
class-map match-any REALTIME-QUEUE
 match dscp ef
class-map match-any NETWORK-CONTROL-QUEUE
 match dscp cs6
class-map match-any SIGNALING-QUEUE
  match  dscp cs3
class-map match-any TRANSACTIONAL-DATA-QUEUE
  match  dscp af21
  match  dscp af22
  match  dscp af23
class-map match-any SCAVENGER-QUEUE
  match  dscp cs1
class-map match-any BULK-DATA
  match access-group name BULK-DATA
class-map match-any INTERACTIVE-VIDEO
  match access-group name INTERACTIVE-VIDEO
class-map match-any RT2
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any RT1
  match  dscp ef
  match  dscp cs3
  match  dscp cs6
class-map match-any INTERACTIVE-VIDEO-QUEUE
  match  dscp af41
  match  dscp af42
  match  dscp af43
class-map match-any BULK-DATA-QUEUE
  match  dscp af11
  match  dscp af12
  match  dscp af13
class-map match-any VOICE
  match  dscp ef
  match access-group name VOICE
class-map match-any SCAVENGER
  match access-group name SCAVENGER
class-map match-any non-client-nrt-class
  match non-client-nrt
class-map match-any SIGNALING
  match  dscp cs3
  match access-group name SIGNALING
class-map match-any TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-DATA
class-map match-any NETWORK-CONTROL
  match dscp cs6
!
policy-map port_child_policy
 class non-client-nrt-class
    bandwidth remaining ratio 7
 class RT1
    priority level 1
    police rate percent 10 conform-action transmit exceed-action drop
```

```
 class RT2
    priority level 2
    police rate percent 20 conform-action transmit exceed-action drop
 class class-default
    bandwidth remaining ratio 63
policy-map REALTIME-DOWNSTREAM-CHILD
 class RT1
    priority level 1
    police cir 15000000  conform-action transmit  exceed-action drop
 class RT2
    priority level 2
    police 50000000  conform-action transmit  exceed-action drop
 class class-default
policy-map EMPLOYEE-DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD
policy-map REMARK_UPSTREAM_CLIENT
 class VOICE
   set dscp ef
class SIGNALING
   set dscp cs3
class INTERACTIVE-VIDEO
   set dscp af41
 class TRANSACTIONAL-DATA
   set dscp af21
 class BULK-DATA
   set dscp af11
 class SCAVENGER
   set dscp cs1
 class class-default
   set dscp default
policy-map PROVISIONING_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map DEFAULT_UPSTREAM_CLIENT
 class class-default
   set dscp default
policy-map REALTIME-DOWNSTREAM-CHILD-PERSONAL
 class RT1
    priority level 1
    police 4500000    conform-action transmit     exceed-action drop
 class RT2
    priority level 2
    police 9000000    conform-action transmit     exceed-action drop
 class class-default
policy-map PERSONAL_DOWNSTREAM
 class class-default
    shape average percent 100
    queue-buffers ratio 0
   service-policy REALTIME-DOWNSTREAM-CHILD-PERSONAL
policy-map IT_DEVICES_DOWNSTREAM
 class class-default
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map GUEST_DOWNSTREAM
 class class-default
    shape average 6000000
    queue-buffers ratio 0
   set dscp dscp table remarkToDefault
   set wlan user-priority dscp table remarkToDefault
policy-map 2P6Q3T
```

```
 class REALTIME-QUEUE
    priority level 1
     police rate percent 10
 class INTERACTIVE-VIDEO-QUEUE
    priority level 2
     police rate percent 20
class NETWORK-CONTROL-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
class SIGNALING-QUEUE
    bandwidth remaining percent 5
    queue-buffers ratio 10
 class BULK-DATA-QUEUE
    bandwidth remaining percent 20
    queue-buffers ratio 10
    queue-limit dscp  af11 percent 100
    queue-limit dscp  af12 percent 90
    queue-limit dscp  af13 percent 80
 class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 34
    queue-buffers ratio 10
    queue-limit dscp  af21 percent 100
    queue-limit dscp  af22 percent 90
    queue-limit dscp  af23 percent 80
 class SCAVENGER-QUEUE
    bandwidth remaining percent 1
    queue-buffers ratio 10
class class-default
    bandwidth remaining percent 35
    queue-buffers ratio 25
!
!
!
interface GigabitEthernet1/0/1
 switchport access vlan 10
 switchport mode access
 ip access-group ACL-DEFAULT in
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto
 authentication violation restrict
 mab
 dot1x pae authenticator
 dot1x timeout tx-period 3
 spanning-tree portfast
!
...
....
!
interface GigabitEthernet1/0/6
!
interface TenGigabitEthernet 1/1/1
service-policy out 2P6Q3T
!
interface Vlan17
 ip address 10.200.17.5 255.255.255.0
!
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended ACL-DEFAULT
```

```
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
 deny   ip any any
ip access-list extended ACL_BLACKHOLE
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
ip access-list extended ACL_BLACKHOLE_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 permit ip any any
ip access-list extended ACL_Full_Access
 permit ip any any
ip access-list extended ACL_ISE_Remediate
 permit udp any eq bootpc any eq bootps
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any 23.0.0.0 0.255.255.255
 permit ip any 17.0.0.0 0.255.255.255
 permit ip any 184.0.0.0 0.255.255.255
 permit ip any 8.0.0.0 0.255.255.255
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
 permit ip any host 10.225.100.10
 permit ip any 173.223.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL_ISE_Remediate_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
 deny   ip any 23.0.0.0 0.255.255.255
 deny   ip any 17.0.0.0 0.255.255.255
 deny   ip any 184.0.0.0 0.255.255.255
 deny   ip any 8.0.0.0 0.255.255.255
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 deny   ip any host 10.225.100.10
 deny   ip any 173.223.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Internet_Only
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 63.128.76.0 0.0.0.255
 permit ip any host 10.225.100.10
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 10.0.0.0 0.255.255.255
 deny   ip any 172.16.0.0 0.15.255.255
 deny   ip any 192.168.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Internet_Redirect
 deny   ip any host 10.230.1.45
 deny   ip any host 10.225.49.15
 deny   ip any host 10.230.1.76
 deny   ip any 63.128.76.0 0.0.0.255
```

```
 deny   ip any host 10.225.100.10
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 172.16.0.0 0.15.255.255
 permit ip any 192.168.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL_Partial_Access
 permit ip any host 10.230.1.45
 permit ip any host 10.225.49.15
 permit ip any host 10.230.1.76
 permit ip any 10.230.4.0 0.0.0.255
 permit ip any host 10.230.6.2
 permit ip any host 10.225.100.10
 deny   ip any 10.230.0.0 0.0.255.255
 deny   ip any 10.225.0.0 0.0.255.255
 deny   ip any 10.200.0.0 0.0.255.255
 permit ip any any
ip access-list extended ACL_Provisioning
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
 permit ip any 74.125.0.0 0.0.255.255
 permit ip any 173.194.0.0 0.0.255.255
 permit ip any 206.111.0.0 0.0.255.255
ip access-list extended ACL_Provisioning_Redirect
 deny   udp any eq bootpc any eq bootps
 deny   udp any host 10.230.1.45 eq domain
 deny   ip any host 10.225.49.15
 deny   ip any 74.125.0.0 0.0.255.255
 deny   ip any 173.194.0.0 0.0.255.255
 deny   ip any 206.111.0.0 0.0.255.255
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE_ACL
 permit udp any eq bootpc any eq bootps
 permit udp any host 10.230.1.45 eq domain
 permit ip any host 10.225.49.15
!
ip access-list extended VOICE
remark - CISCO-JABBER-REDUCED-PORT-RANGE
permit udp any any range 16384 17384
!
ip access-list extended INTERACTIVE-VIDEO
remark CISCO-JABBER-RTP
permit udp any any range 17385 32767
remark MICROSOFT-LYNC
permit tcp any any range 50000 59999
!
ip access-list extended SIGNALING
remark SCCP
permit tcp any any eq 2000
remark SIP
permit tcp any any range 5060 5061
!
ip access-list extended TRANSACTIONAL-DATA
remark HTTPS
permit tcp any any eq 443
remark CITRIX
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
remark ORACLE
permit tcp any any eq 1521
permit tcp any any eq 1527
```

```
permit tcp any any eq 1575
permit tcp any any eq 1630
permit tcp any any eq 6200
!
ip access-list extended BULK-DATA
remark FTP
permit tcp any any eq ftp
permit tcp any any eq ftp-data
remark SSH/SFTP
permit tcp any any eq 22
remark SMTP/SECURE SMTP
permit tcp any any eq smtp
permit tcp any any eq 465
remark IMAP/SECURE IMAP
permit tcp any any eq 143
permit tcp any any eq 993
remark POP3/SECURE POP3
permit tcp any any eq pop3
permit tcp any any eq 995
remark CONNECTED PC BACKUP
permit tcp any eq 1914 any
!
ip access-list extended SCAVENGER
remark BITTORRENT
permit tcp any any range 6881 6999
remark APPLE ITUNES MUSIC SHARING
permit tcp any any eq 3689
permit udp any any eq 3689
remark MICROSOFT DIRECT X GAMING
permit tcp any any range 2300 2400
permit udp any any range 2300 2400
!
ip radius source-interface Vlan17
!
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 send nas-port-detail
radius-server dead-criteria time 5 tries 3
radius-server host 10.225.49.15 auth-port 1812 acct-port 1813 key 7 153C1805102F7A767B6760
!
!
wireless mobility controller
wireless mobility group member ip 10.225.50.36 public-ip 10.225.50.36
wireless mobility group name byod
wireless mobility dscp 48
wireless management interface Vlan17
wireless client fast-ssid-change
wireless rf-network byod
wireless security dot1x radius call-station-id macaddress
wireless exclusionlist 1CB0.9414.9077 description gregg
wireless broadcast
wireless multicast
wlan BYOD_Employee 1 BYOD_Employee
 aaa-override
 client vlan BYOD-Employee
 nac
 security dot1x authentication-list default
 session-timeout 1800
ip flow monitor wireless-avc-basic input
 ip flow monitor wireless-avc-basic output
service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output EMPLOYEE-DOWNSTREAM
```

```
 no shutdown
wlan BYOD_Guest 2 BYOD_Guest
 aaa-override
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth
service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output GUEST_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan BYOD_Provisioning 3 BYOD_Provisioning
 aaa-override
 client vlan BYOD-Provisioning
ip flow monitor wireless-avc-basic input
 ip flow monitor wireless-avc-basic output
service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PROVISIONING_DOWNSTREAM
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 session-timeout 1800
 no shutdown
wlan BYOD_Personal_Device 4 BYOD_Personal_Device
 client vlan BYOD_Guest
 mobility anchor 10.225.50.36
 security web-auth parameter-map global
service-policy client input REMARK_UPSTREAM_CLIENT
 service-policy output PERSONAL_DOWNSTREAM
 session-timeout 1800
 no shutdown
wlan IT_Devices 5 IT_Devices
 aaa-override
 client vlan BYOD-Employee
 mac-filtering MAC_ALLOW
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security web-auth parameter-map global
 service-policy client input DEFAULT_UPSTREAM_CLIENT
 service-policy output IT_DEVICES_DOWNSTREAM
 session-timeout 1800
 no shutdown
end
```