



BYOD Converged Access Configurations

Revised: August 7, 2013

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:

```
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
!
!
qos wireless-default-untrust
captive-portal-bypass
!
dot1x system-auth-control
!
!
!
mac access-list extended MAC_ALLOW
  permit any any
spanning-tree mode pvst
spanning-tree extend system-id
!
!

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
!
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
!
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 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
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
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
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
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
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
!
!
qos wireless-default-untrust

captive-portal-bypass
!
!
dot1x system-auth-control
!
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 non-client-nrt-class
  match non-client-nrt
!
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
!
!

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 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 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 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
  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
  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
  session-timeout 1800
  no shutdown
wlan BYOD_Personal_Device 4 BYOD_Personal_Device
  client vlan Guest
  mobility anchor 10.225.50.36
  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
  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.

```
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
!
!
qos wireless-default-untrust
captive-portal-bypass
!
!
mac access-list extended MAC_ALLOW
  permit any any
!
vlan 10
  name BYOD-Employee
!
vlan 11
  name BYOD-Provisioning
!
vlan 17
  name AP_Management
!
vlan 18
!
vlan 777
  name BYOD_Guest
!

!
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 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 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 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
  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
  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
  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
  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
  session-timeout 1800
  no shutdown
end
```