



Example Configurations for AP and RADIUS Server

AP Configuration

The following example shows a Cisco IOS configuration for an AP. The configuration and configuration commands in this example are valid for Cisco IOS version 12.2(15)JA. If you are using a newer version of Cisco IOS, some of the commands might be different or might be invalid. Refer to the latest configuration and command reference documentation for your version of Cisco IOS.

```
ap#sh run
Building configuration...

Current configuration : 4324 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ap
!
enable secret 5 $1$ZyA5$VTX31sQLnZ2cZnBnGhX6v/
!
username Cisco password 7 00271A150754
clock timezone U -8
clock summer-time U recurring
ip subnet-zero
!
aaa new-model
!
!
aaa group server radius rad_eap
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login eap_methods group rad_eap
```

```

aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
dot11 phone
dot11 arp-cache
!
policy-map data
  class class-default
    set cos 1
policy-map management
  class class-default
    set cos 7
policy-map voice
  class class-default
    set cos 6
!
!
bridge irb
!
!
interface Dot11Radio0
  no ip address
  no ip route-cache
  !
  encryption vlan 1 key 1 size 128bit 7 C6BDD88611D089948782B58DA1E4 transmit-key
  encryption vlan 1 mode wep mandatory
  !
  encryption vlan 2 key 1 size 128bit 7 9FD518A21653687A4251AEE12308 transmit-key
  encryption vlan 2 mode wep mandatory
  !
  encryption vlan 3 key 1 size 128bit 7 09E1230C15B678330C1A84143960 transmit-key
  encryption vlan 3 mode wep mandatory
  !
  ssid data
    vlan 2
      authentication open
  !
  ssid voice
    vlan 3
      authentication open
  !
  speed basic-11.0
  rts threshold 2312
  power local 20
  power client 20
  channel 2437
  station-role root
  !
interface Dot11Radio0.1
  encapsulation dot1Q 1 native
  no ip route-cache
  service-policy input management
  service-policy output management
  bridge-group 1
  bridge-group 1 subscriber-loop-control
  bridge-group 1 block-unknown-source
  no bridge-group 1 source-learning
  no bridge-group 1 unicast-flooding
  bridge-group 1 spanning-disabled
  !
interface Dot11Radio0.2
  encapsulation dot1Q 2

```

```

no ip route-cache
service-policy input data
service-policy output data
bridge-group 2
bridge-group 2 subscriber-loop-control
bridge-group 2 block-unknown-source
no bridge-group 2 source-learning
no bridge-group 2 unicast-flooding
bridge-group 2 spanning-disabled
!
interface Dot11Radio0.3
encapsulation dot1Q 3
no ip route-cache
service-policy input voice
service-policy output voice
bridge-group 3
bridge-group 3 subscriber-loop-control
bridge-group 3 block-unknown-source
no bridge-group 3 source-learning
no bridge-group 3 unicast-flooding
bridge-group 3 spanning-disabled
!
interface FastEthernet0
no ip address
no ip route-cache
duplex auto
speed auto
ntp broadcast client
!
interface FastEthernet0.1
encapsulation dot1Q 1 native
no ip route-cache
bridge-group 1
no bridge-group 1 source-learning
bridge-group 1 spanning-disabled
!
interface FastEthernet0.2
encapsulation dot1Q 2
no ip route-cache
bridge-group 2
no bridge-group 2 source-learning
bridge-group 2 spanning-disabled
!
interface FastEthernet0.3
encapsulation dot1Q 3
no ip route-cache
bridge-group 3
no bridge-group 3 source-learning
bridge-group 3 spanning-disabled
!
interface BVI1
ip address 10.0.0.5 255.255.255.0
no ip route-cache
!
ip default-gateway 10.0.0.1
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip http authentication local
ip radius source-interface BVI1
!
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting

```

```

bridge 1 route ip
!
!
line con 0
line vty 5 15
!
ntp clock-period 2860645
ntp server 10.0.0.1
end

```

Configuring a Fallback RADIUS Server for LEAP

The following steps illustrate how to configure the fallback RADIUS server on the AP for LEAP authentication.

Step 1 Configure the Network Access Server (NAS):

```

radius-server local
  nas 192.168.10.35 key Cisco
  nas 192.168.10.45 key Cisco

```

Step 2 Configure the user database:

```

radius-server local
  user BM-AP1200-one-SCM password Cisco
  user BM-AP1100-two-SCM password Cisco
  user testuser password Cisco

```

Step 3 Configure the local RADIUS server in the AP's RADIUS server list:

```

aaa group server radius rad_eap
  server 192.168.10.45 auth-port 1812 acct-port 1813
  radius-server host 192.168.10.45 auth-port 1812 acct-port 1813 key Cisco

```

Step 4 Configure the RADIUS server time-outs:

```

radius-server deadtime 10

```

Step 5 Disable client holdoff:

```

no dot11 holdoff-time

```
